SIEMENS

RUGGEDCOM ROX II v2.12

Web Interface User Guide

For RX1500, RX1501, RX1510, RX1511, RX1512

Continued on next page

05/2018
RC1399-EN-01

SIEMENS

RUGGEDCOM ROX II v2.12

Web Interface User Guide

For RX1500, RX1501, RX1510, RX1511, RX1512

05/2018
RC1399-EN-01

Disclaimer Of Liability

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

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

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

Registered Trademarks

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

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

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

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

Open Source

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

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

Security Information

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

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

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

Warranty

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

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

Contacting Siemens

Address
Siemens Canada Ltd
Industry Sector
300 Applewood Crescent
Concord, Ontario
Canada, L4K 5C7

Telephone
Toll-free: 1 888 264 0006
Tel: +1 905 856 5288
Fax: +1 905 856 1995

E-mail
ruggedcom.info.i-ia@siemens.com

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

Table of Contents

Preface

This guide describes the Web-based user interface for RUGGEDCOM ROX II v2.12 running on the RUGGEDCOM RX1500/RX1501/RX1510/RX1511/RX1512. It contains instructions and guidelines on how to use the software, as well as some general theory.

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

CONTENTS

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

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

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

Product Notes

Document Title	Link
Delivery Release for RUGGEDCOM ROX II 2.12.0	https://support.industry.siemens.com/cs/ww/en/view/109755291

User/Reference Guides

Document Title	Link
RUGGEDCOM ROX II v2.12 CLI User Guide	https://support.industry.siemens.com/cs/ww/en/view/109755285
RUGGEDCOM APE User Guide	https://support.industry.siemens.com/cs/ww/en/view/81193317
RUGGEDCOM ROX II NETCONF Reference Guide	https://support.industry.siemens.com/cs/ww/en/view/109737085
RUGGEDCOM NMS v2.1 User Guide for Windows	https://support.industry.siemens.com/cs/ww/en/view/109737564
RUGGEDCOM NMS v2.1 User Guide for Linux	https://support.industry.siemens.com/cs/ww/en/view/109737563
RUGGEDCOM CROSSBOW User Guide	Available upon request

Catalogs

Document Title	Link
RUGGEDCOM Modules Catalog for the RUGGEDCOM RX1500/ RX1501/RX1510/RX1511/RX1512	https://support.industry.siemens.com/cs/ww/en/view/109747072
RUGGEDCOM SFP Transceivers Catalog	https://support.industry.siemens.com/cs/ww/en/view/109482309

FAQs/Application Examples

Document Title	Link
How to Change the Log Level?	https://support.industry.siemens.com/cs/ww/en/view/109744203
How to Upgrade the U-Boot Binary?	https://support.industry.siemens.com/cs/ww/en/view/109744203
Mean Time Between Failures (MTBF) – List for RUGGEDCOM Products	https://support.industry.siemens.com/cs/ww/en/view/109479200
How Can You Upgrade the GNU C Library? (Security Advisory SSA-994726)	https://support.industry.siemens.com/cs/ww/en/view/109474273

Document Title	Link
How Do You Calculate the Latency on a Switched Ethernet Network with RUGGEDCOM Switches or Routers?	https://support.industry.siemens.com/cs/ww/en/view/94772587
What Should You Watch Out For When Configuring a Link Aggregation Between SCALANCE X Switches and RUGGEDCOM Switches?	https://support.industry.siemens.com/cs/ww/en/view/76798136
What Should You Watch Out For When Ordering and Installing Interface Modules For RUGGEDCOM Switches?	https://support.industry.siemens.com/cs/ww/en/view/77896782
What Options Do You Have For Connecting an (R)STP Segment To a Ring Structure and How Can You Reduce the Ring Reconfiguration Time Through the EPLC Procedure?	https://support.industry.siemens.com/cs/ww/en/view/77363773
How to Implement Robust Ring Networks using RSTP and eRSTP?	https://support.industry.siemens.com/cs/ww/en/view/109738240
How to Change the Log Level?	https://support.industry.siemens.com/cs/ww/en/view/109744203
What is the Difference Between RSTP (Rapid Spanning Tree Protocol) and eRSTP (enhanced Rapid Spanning Tree Protocol 4) PBDU (Bridge Protocol Data Unit)?	https://support.industry.siemens.com/cs/ww/en/view/109476379
How to Regenerate Keys and Certificates?	https://support.industry.siemens.com/cs/ww/en/view/109738241
Using BGP Route Reflection with VPNv4 Clients	https://support.industry.siemens.com/cs/ww/en/view/109757209

Installation Guides

Document Title	Link
RUGGEDCOM RX1500 Installation Guide	https://support.industry.siemens.com/cs/ww/en/view/82166529
RUGGEDCOM RX1501 Installation Guide	https://support.industry.siemens.com/cs/ww/en/view/82164308
RUGGEDCOM RX1510 Installation Guide	https://support.industry.siemens.com/cs/ww/en/view/82164310
RUGGEDCOM RX1511 Installation Guide	https://support.industry.siemens.com/cs/ww/en/view/82166915
RUGGEDCOM RX1512 Installation Guide	https://support.industry.siemens.com/cs/ww/en/view/82167597

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 RX1500/RX1501/RX1510/RX1511/RX1512
- 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 v2.12 is available online at https://www.siemens.com/ruggedcom. To request or inquire about a user document, contact Siemens Customer Support.

License Conditions

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

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

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

Training

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

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

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

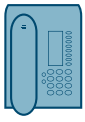
For more information about training services and course availability, visit https://www.siemens.com/ruggedcom or contact a Siemens Sales representative.

Customer Support

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

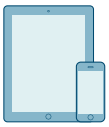
Online

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



Telephone

Call a local hotline center to submit a Support Request (SR). To locate a local hotline center, visit http://www.automation.siemens.com/mcms/aspa-db/en/automation-technology/Pages/default.aspx.



Mobile App

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

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

1 Introduction

Welcome to the RUGGEDCOM ROX II (Rugged Operating System on Linux®) v2.12 Web Interface User Guide for the RUGGEDCOM RX1500/RX1501/RX1510/RX1511/RX1512. This document details how to configure the RX1500 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.

CONTENTS

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:

Passwords	Multi-level user passwords secures against unauthorized configuration
SSH/SSL	Extends capability of password protection to add encryption of passwords and data as they cross the network
Enable/Disable Ports	Capability to disable ports so that traffic cannot pass
802.1Q VLAN	Provides the ability to logically segregate traffic between predefined ports on switches
SNMPv3	Encrypted authentication and access security
HTTPS	For secure access to the Web interface

Firewall	Integrated stateful firewall provides protected network zones
VPN/IPSEC	Allows creation of secure encrypted and authenticated tunnels

- **Enhanced Rapid Spanning Tree Protocol (eRSTP)™**
  Siemens's eRSTP allows the creation of fault-tolerant ring and mesh Ethernet networks that incorporate redundant links that are *pruned* to prevent loops. eRSTP implements both STP and RSTP to promote interoperability with commercial switches, unlike other proprietary *ring* solutions. The fast root failover feature of eRSTP provides quick network convergence in case of an RSTP root bridge failure in a mesh topology.
- **Quality of Service (IEEE 802.1p)**
  Some networking applications such as real-time control or VoIP (Voice over IP) require predictable arrival times for Ethernet frames. Switches can introduce latency in times of heavy network traffic due to the internal queues that buffer frames and then transmit on a first come first serve basis. RUGGEDCOM ROX II supports *Class of Service*, which allows time critical traffic to jump to the front of the queue, thus minimizing latency and reducing *jitter* to allow such demanding applications to operate correctly. RUGGEDCOM ROX II allows priority classification by port, tags, MAC address, and IP Type of Service (ToS). A configurable *weighted fair queuing* algorithm controls how frames are emptied from the queues.
- **VLAN (IEEE 802.1Q)**
  Virtual Local Area Networks (VLAN) allow the segregation of a physical network into separate logical networks with independent broadcast domains. A measure of security is provided since hosts can only access other hosts on the same VLAN and traffic storms are isolated. RUGGEDCOM ROX II supports 802.1Q tagged Ethernet frames and VLAN trunks. Port based classification allows legacy devices to be assigned to the correct VLAN. GVRP support is also provided to simplify the configuration of the switches on the VLAN.
- **Simple Network Management Protocol (SNMP)**
  SNMP provides a standardized method for network management stations to interrogate devices from different vendors. RUGGEDCOM ROX II supports v1, v2c and v3. SNMPv3 is generally recommended, as it provides security features (such as authentication, privacy, and access control) not present in earlier SNMP versions.

  RUGGEDCOM ROX II also supports numerous standard MIBs (Management Information Base) allowing for easy integration with any Network Management System (NMS). A feature of SNMP supported by RUGGEDCOM ROX II is the ability to generate *traps* upon system events. RUGGEDCOM NMS, the Siemens management solution, can record traps from multiple devices providing a powerful network troubleshooting tool. It also provides a graphical visualization of the network and is fully integrated with all Siemens products.
- **Remote Monitoring and Configuration with RUGGEDCOM NMS**
  RUGGEDCOM NMS (RNMS) is Siemens's Network Management System software for the discovery, monitoring and management of RUGGEDCOM products and other IP enabled devices on a network. This highly configurable, full-featured product records and reports on the availability and performance of network components and services. Device, network and service failures are quickly detected and reported to reduce downtime.

  RNMS is especially suited for remotely monitoring and configuring RUGGEDCOM routers, switches, serial servers and WiMAX wireless network equipment. For more information, contact a Siemens Sales representative.
- **NETCONF Configuration Interface**
  The NETCONF configuration interface allows administrators to set device parameters and receive device updates through the use of XML-based commands. This standard, supported by multiple vendors, makes it possible to greatly simplify the task of network management.

  For more information about how to use NETCONF to configure RUGGEDCOM ROX II, refer to the *RUGGEDCOM RUGGEDCOM ROX II NETCONF Reference Guide* available on https://www.siemens.com/ruggedcom.
- **NTP (Network Time Protocol)**
  NTP automatically synchronizes the internal clock of all RUGGEDCOM ROX II devices on the network. This allows for correlation of time stamped events for troubleshooting.

- **Port Rate Limiting**
  RUGGEDCOM ROX II supports configurable rate limiting per port to limit unicast and multicast traffic. This can be essential to managing precious network bandwidth for service providers. It also provides edge security for Denial of Service (DoS) attacks.
- **Broadcast Storm Filtering**
  Broadcast storms wreak havoc on a network and can cause attached devices to malfunction. This could be disastrous on a network with mission critical equipment. RUGGEDCOM ROX II limits this by filtering broadcast frames with a user-defined threshold.
- **Port Mirroring**
  RUGGEDCOM ROX II can be configured to duplicate all traffic on one port to a designated mirror port. When combined with a network analyzer, this can be a powerful troubleshooting tool.
- **Port Configuration and Status**
  RUGGEDCOM ROX II allows individual ports to be *hard* configured for speed, duplex, auto-negotiation, flow control and more. This allows proper connection with devices that do not negotiate or have unusual settings. Detailed status of ports with alarm and SNMP trap on link problems aid greatly in system troubleshooting.
- **Port Statistics and RMON (Remote Monitoring)**
  RUGGEDCOM ROX II provides continuously updating statistics per port that provide both ingress and egress packet and byte counters, as well as detailed error figures.

  Also provided is full support for RMON statistics. RMON allows for very sophisticated data collection, analysis and detection of traffic patterns.
- **Event Logging and Alarms**
  RUGGEDCOM ROX II records all significant events to a non-volatile system log allowing forensic troubleshooting. Events include link failure and recovery, unauthorized access, broadcast storm detection, and self-test diagnostics among others. Alarms provide a snapshot of recent events that have yet to be acknowledged by the network administrator. An external hardware relay is de-energized during the presence of critical alarms, allowing an external controller to react if desired.
- **HTML Web Browser User Interface**
  RUGGEDCOM ROX II provides a simple, intuitive user interface for configuration and monitoring via a standard graphical Web browser or via a standard telecom user interface. All system parameters include detailed online Help to facilitate setup and configuration. RUGGEDCOM ROX II presents a common look and feel and standardized configuration process, allowing easy migration to other RUGGEDCOM managed products.
- **Command Line Interface (CLI)**
  A command line interface used in conjunction with remote shell to automate data retrieval, configuration updates, and firmware upgrades. A powerful Telecom Standard style Command Line Interface (CLI) allows expert users the ability to selectively retrieve or manipulate any parameters the device has to offer.
- **Link Backup**
  Link backup provides an easily configured means of raising a backup link upon the failure of a designated main link. The main and backup links can be Ethernet, Cellular, T1/E1, DDS or T3. The feature can back up to multiple remote locations, managing multiple main: backup link relationships. The feature can also back up a permanent high speed WAN link to a permanent low speed WAN link and can be used to migrate the default route from the main to the backup link.
- **OSPF (Open Shortest Path First)**
  OSPF is a routing protocol that determines the best path for routing IP traffic over a TCP/IP network based on link states between nodes and several quality parameters. OSPF is an Interior Gateway Protocol (IGP), which is designed to work within an autonomous system. It is also a link state protocol, meaning the best route is determined by the type and speed of the inter-router links, not by how many router hops they are away from each other (as in distance-vector routing protocols such as RIP).

- **BGP (Border Gateway Protocol)**
  BGPv4 is a path-vector routing protocol where routing decisions are made based on the policies or rules laid out by the network administrator. It is typically used where networks are multi-homed between multiple Internet Service Providers, or in very large internal networks where internal gateway protocols do not scale sufficiently.
- **RIP (Routing Information Protocol)**
  RIP version 1 and version 2 are distance-vector routing protocols that limit the number of router hops to 15 when determining the best routing path. This protocol is typically used on small, self-contained networks, as any router beyond 15 hops is considered unreachable.
- **IS-IS (Intermediate System - Intermediate System)**
  IS-IS is one of a suite of routing protocols tasked with sharing routing information between routers. The job of the router is to enable the efficient movement of data over sometimes complex networks. Routing protocols are designed to share routing information across these networks and use sophisticated algorithms to decide the shortest route for the information to travel from point A to point B. One of the first link-state routing protocols was IS-IS developed in 1985 and adopted by the ISO in 1998 (ISO/IEC 10589:2002). It was later republished as an IETF standard (RFC 1142 [http://tools.ietf.org/html/rfc1142]).
- **Brute Force Attack Prevention**
  Protection against Brute Force Attacks (BFAs) is standard in RUGGEDCOM ROX II. If an external host fails to log in to the CLI, NETCONF or Web interfaces after a fixed number of attempts, the host's IP address will be blocked for a period of time. That period of time will increase if the host continues to fail on subsequent attempts.
- **USB Mass Storage**
  Use a removable USB Mass Storage drive to manage important files and configure RUGGEDCOM ROX II.
  - Upgrade/Downgrade Firmware – Use the USB Mass Storage drive as a portable repository for new or legacy versions of the RUGGEDCOM ROX II firmware.
  - Backup Files – Configure RUGGEDCOM ROX II to backup important information to the USB Mass Storage drive, such as rollbacks, log files, feature keys and configuration files.
  - Share Files – Quickly configure or upgrade other RUGGEDCOM RX1500 devices by copying files using the same microSD/microSDHC Flash drive.

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

  NOTE
  Only USB Mass Storage drives with one partition are supported.
- **Hot Swapping Modules and SFP Transceivers**
  Power Modules (PM), Line Modules (LM) and individual SFP transceivers can be safely replaced with modules/transceivers of exactly the same type while the device is running, with minimal disruption to the network. The device only needs to be restarted after swapping a module/transceiver with a different type, such as an Ethernet module with a serial module, or a 1000Base-X transceiver with a 100Base-FX transceiver.

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

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

Section 1.2

Feature Keys

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

The following feature keys are currently available:

- Layer 3 Standard Edition with Layer 3 Hardware (L3SEL3HW)
- Layer 3 Standard Edition with Layer 2 Hardware (L3SEL2HW)
- Layer 3 Security Edition with Layer 3 Hardware (L3SECL3HW)
- Layer 3 Security Edition with Layer 2 Hardware (L3SECL2HW)

By default, each new RUGGEDCOM RX1500/RX1501/RX1510/RX1511/RX1512 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 (L2SE)	L3SEL3HW	L3SEL2HW	L3SECL3HW	L3SECL2HW
VLANs (802.1Q)	✓	✓	✓	✓	✓
QoS (802.1p)	✓	✓	✓	✓	✓
MSTP (802.1Q-2005)	✓	✓	✓	✓	✓
RSTP	✓	✓	✓	✓	✓
eRSTP™	✓	✓	✓	✓	✓
NTP	✓	✓	✓	✓	✓
L2TPv2 and L2TPv3	✓	✓	✓	✓	✓
Port Rate Limiting	✓	✓	✓	✓	✓
Broadcast Storm Filtering	✓	✓	✓	✓	✓
Port Mirroring	✓	✓	✓	✓	✓
SNMP v1/v2/v3	✓	✓	✓	✓	✓
RMON	✓	✓	✓	✓	✓
CLI	✓	✓	✓	✓	✓
HTML User Interface	✓	✓	✓	✓	✓
MPLS		✓	✓	✓	✓
DHCP		✓	✓	✓	✓
VRRPv2 and VRRPv3		✓	✓	✓	✓

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

For information about installing and viewing the contents of feature keys, refer to Section 4.8, "Managing Feature Keys".

Section 1.3

Security Recommendations

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

Authentication

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

- Replace the default passwords for all user accounts, access modes (e.g. maintenance mode) and processes (where applicable) before the device is deployed.
- Use strong passwords. Avoid weak passwords (e.g. *password1*, *123456789*, *abcdefgh*) or repeated characters (e.g. *abcabc*). For more information about creating strong passwords, refer to the password requirements in Section 5.9, "Managing Passwords and Passphrases".

  This recommendation also applies to pre-shared keys (PSK) configured on the device.
- Make sure passwords are protected and not shared with unauthorized personnel.
- Do not re-use passwords across different user names and systems, or after they expire.
- Record passwords in a safe, secure, off-line location for future retrieval should they be misplaced.

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

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 6.3, "Enabling/Disabling Brute Force Attack Protection".
- SSH and SSL keys are accessible to users who connect to the device via the serial console. Make sure to take appropriate precautions when shipping the device beyond the boundaries of the trusted environment:
  - Replace the SSH and SSL keys with *throwaway* keys prior to shipping.
  - Take the existing SSH and SSL keys out of service. When the device returns, create and program new keys for the device.
- Replace all default and auto-generated SSL certificates with certificates and keys signed by a trusted Certificate Authority (CA). Default and auto-generated certificates are self-signed by RUGGEDCOM ROX II.
- Restrict physical access to the device to only trusted personnel. A person with malicious intent in possession of the flash card could extract critical information, such as certificates, keys, etc. (user passwords are protected by hash codes), or reprogram the card.
- Passwords/passphrases for service mode and maintenance mode should only be given to a limited number of trusted users. These modes provide access to private keys and certificates.
- 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 15.2, "Managing SNMP".
  - Make sure the default community strings are changed to unique values.
- When using RUGGEDCOM ROX II as a client to securely connect to a server (such as, in the case of a secure upgrade or a secure syslog transfer), make sure the server side is configured with strong ciphers and protocols.
- Limit the number of simultaneous Web Server, CLI, SFTP and NETCONF sessions allowed.
- If a firewall is required, configure and start the firewall before connecting the device to a public network. Make sure the firewall is configured to accept connections from a specific domain. For more information, refer to Section 6.8, "Managing Firewalls".
- Modbus is deactivated by default in RUGGEDCOM ROX II. If Modbus is required, make sure to follow the security recommendations outlined in this 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 4.10, "Managing Logs".

- Configuration files are provided in either NETCONF or CLI format for ease of use. Make sure configuration files are properly protected when they exist outside of the device. For instance, encrypt the files, store them in a secure place, and do not transfer them via insecure communication channels.
- It is highly recommended that critical applications be limited to private networks, or at least be accessible only through secure services, such as IPsec. Connecting a RUGGEDCOM ROX II device to the Internet is possible. However, the utmost care should be taken to protect the device and the network behind it using secure means such as firewall and IPsec. For more information about configuring firewalls and IPsec, refer to Section 6.8, "Managing Firewalls" and Section 12.8, "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.
- Make sure the device is fully decommissioned before taking the device out of service. For more information, refer to Section 4.7, "Decommissioning the Device".
- Configure port security features on access ports to prevent an unauthorized third-party from physically connecting to the device. For more information, refer to Section 6.5.2, "Configuring Port Security".

Hardware/Software

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

- Make sure the latest firmware version is installed, including all security-related patches. For the latest information on security patches for Siemens products, visit the Industrial Security website [https://www.siemens.com/global/en/home/company/topic-areas/future-of-manufacturing/industrial-security.html] or the ProductCERT Security Advisories website [http://www.siemens.com/innovation/en/technology-focus/siemens-cert/cert-security-advisories.htm]. Updates to Siemens Product Security Advisories can be obtained by subscribing to the RSS feed on the Siemens ProductCERT Security Advisories website, or by following @ProductCert on Twitter.
- Only enable the services that will be used on the device, including physical ports. Unused physical ports could potentially be used to gain access to the network behind the device.
- Use the latest Web browser version compatible with RUGGEDCOM ROX II to make sure the most secure Transport Layer Security (TLS) versions and ciphers available are employed. Additionally, 1/n-1 record splitting is enabled in the latest Web browser versions of Mozilla Firefox, Google Chrome and Internet Explorer, and mitigates against attacks such as SSL/TLS Protocol Initialization Vector Implementation Information Disclosure Vulnerability (e.g. BEAST).
- For optimal security, use SNMPv3 whenever possible and apply strong passwords.
- Validate the integrity of the firmware often. This task can be automated by scheduling a job to repeat every day or week. Firmware integrity can also be checked automatically at start-up.

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

For more information about checking the firmware integrity, refer to Section 4.13, "Monitoring Firmware Integrity".

» Policy

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

Section 1.4

Available Services by Port

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

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

Services	Port Number	Port Open	Port Default	Access Authorized
SSH	TCP/22	Open (if configured with login)	Open	Yes
SSH (Service Mode)	TCP/222	Open (if configured with login)	Closed	Yes
NETCONF	TCP/830	Open (if configured with login)	Open	Yes
SFTP	TCP/2222	Open (if configured with login)	Closed	Yes
HTTP	TCP/80	Open (if configured with login)	Open	N/A
NTP	UDP/123	Open (if configured)	Closed	No
SNMP	UDP/161	Open (if configured with login)	Closed	Yes
HTTPS	TCP/443	Open (if configured with login)	Open	Yes
TCP Modbus	TCP/502	Open (if configured)	Closed	No
IPSec IKE	UDP/500	Open (if configured)	Closed	Yes
IPSec NAT-T	UDP/4500	Open (if configured)	Closed	Yes
DNPv3	TCP/20000	Open (if configured)	Closed	No
RawSocket	TCP/configured	Open (if configured)	Closed	No
DHCP Agent	UDP/67	Open (if configured)	Closed	No

Services	Port Number	Port Open	Port Default	Access Authorized
DHCP Server	UDP/67 listening, 68 responding	Open (if configured)	Closed	No
RADIUS	UDP/1812 to send, opens random port to listen	Open (if configured)	Closed	Yes
TACACS+	TCP/49 to send, opens random port to listen	Open (if configured)	Closed	Yes
L2TP	Random Port	Open (if configured)	Closed	Yes
BGP	TCP/179	Open (if configured)	Closed	No
RIP	UDP/520	Open (if configured)	Closed	No
MPLS-Ping	UDP/3503	Open (if configured)	Closed	No
LDP	TCP/646 and UDP/646	Open (if configured)	Closed	No
L2TPv3	UDP/1701	Open (if configured)	Closed	No

Section 1.5

User Permissions

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

Types of user access:

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

Commands/Paths Permitted	Access			Notes
	Administrator	Operator	Guest	
config private | exclusive | no-confirm	Allowed	Allowed	No	
/admin/software-upgrade	R/U	R	No	
/admin/rox-imaging	R/U	R	No	
/admin/authentication	R/U	No	No	
/admin/authentication/password-complexity	R/U	No	No	
/admin/logging	C/R/U	No	No	
/admin/alarms (status)	R	R	No	Administrator and operator can see status of active-alarms, acknowledge and clear alarms
/admin/alarms-config/	R/U	R/U	No	Administrator and operator cannot create or delete alarm-lists

Commands/Paths Permitted	Access			Notes
	Administrator	Operator	Guest	
/admin/users	C/R/U	No	No	
/admin/users/userid	R/U	R/U	No	Operator can only change own password and cannot create users.
/admin/cli	R/U	R/U	No	
/admin/snmp	C/R/U	No	No	
/admin/netconf	R/U	No	No	
/admin/dns	C/R/U	No	No	
/admin/webui	R/U	R/U	No	
/admin/scheduler	C/R/U	No	No	
/admin/contact	R/U	No	No	
/admin/hostname	R/U	No	No	
/admin/location	R/U	No	No	
/admin/session-limits	R/U	No	No	
/admin/session-security	R/U	No	No	
/admin/sftp	R/U	No	No	
/admin/time (status)	R	R	No	
/admin/switch-config (status)	R/U	R	No	
/admin/system	R/U	No	No	
/admin/sytem-name	R/U	No	No	
/admin/timezone	R/U	No	No	
/admin/clear-all-alarms (action)	E	C/R/U	No	
/admin/backup-files (action)	E/R/U	No	No	
/admin/delete-all-ssh-known-hosts (action)	E	No	No	
/admin/delete-logs (action)	E	No	No	
/admin/delete-ssh-known-host (action)	E	No	No	
/admin/full-configuration-load (action)	E/U	No	No	
/admin/full-configuration-save (action)	E/U	No	No	
/admin/install-files (action)	E/U	No	No	
/admin/reboot (action)	E	E	No	
/admin/restore-factory-defaults (action)	E/U	No	No	
/admin/set-system-clock (action)	E/U	No	No	
/admin/shutdown (action)	E	E	No	
/apps	C/R/U	C/R/U	R	
/chassis/part-list	R/U	R	R	

Commands/Paths Permitted	Access			Notes
	Administrator	Operator	Guest	
/chassis/fixed-modules	C/R/U	No	R	
/chassis/line-module-list	R/U	R	R	
/chassis/line-modules/line-module	R/U	No	R	
/interfaces	R	C/R/U	R	
/interface	C/R/U	R/U	R	
/routing	C/R/U	C/R/U	R	
/routing/dynamic/ospf/interface	C/R/U	C/R/U	R	
/routing/dynamic/rip/interface	C/R/U	C/R/U	R	
/routing/multicast/dynamic/pim-sm/interface	C/R/U	C/R/U	R	
/routing/dynamic/isis/interface	C/R/U	C/R/U	R	
/security/firewall	C/R/U	C/R/U	R	
/security/crypto	C/R/U	R	R	
/security/crypto/private-key	C/R/U	No	No	
/services	C/R/U	C/R/U	R	
/services/time/ntp/key/	C/R/U	No	No	
/tunnel/ipsec	C/R/U	No	No	
/ip	C/R/U	C/R/U	R	
/mpls	C/R/U	C/R/U	R	
/mpls/interface-mpls	C/R/U	C/R/U	R	
/mpls/ldp/interface-ldp	C/R/U	C/R/U	R	
/switch	C/R/U	C/R/U	R	
/switch/vlans/all-vlans	C/R/U	C/R/U	R	
/switch/port-security	R/U	No	No	
/qos	C/R/U	C/R/U	R	
/global	C/R/U	No	No	
hints	E	E	E	
monitor	E	E	No	
mpls-ping	E	E	No	
mpls-traceroute	E	E	No	
ping	E	E	No	
ping6	E	E	No	
reportstats	E	E	No	
ssh	E	No	No	

Commands/Paths Permitted	Access			Notes
	Administrator	Operator	Guest	
tcpdump	E	E	No	
telnet	E	E	No	
traceroute	E	E	No	
traceroute6	E	E	No	
traceserial	E	E	No	
wizard	E	No	No	

Section 1.6

Removable Memory

The RUGGEDCOM RX1500 features a user-accessible memory slot that supports a USB Mass Storage device. The drive can be used to manage configuration, firmware and other files on the device or a fleet of devices.

- Upgrade/Downgrade Firmware – Use the USB Mass Storage device as a portable repository for new or legacy versions of the RUGGEDCOM ROX II firmware.
- Backup Files – Configure RUGGEDCOM ROX II to backup important information to the USB Mass Storage device, such as rollbacks, log files, feature keys and configuration files.
- Share Files – Quickly configure or upgrade other RUGGEDCOM RX1500/RX1501/RX1510/RX1511/RX1512 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 RX1500/RX1501/RX1510/RX1511/RX1512.

2 Using RUGGEDCOM ROX II

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

CONTENTS

Section 2.1

Default User Names and Passwords

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

CAUTION!
Security hazard – risk of unauthorized access and/or exploitation. To prevent unauthorized access to the device, change the default passwords before commissioning the device. For more information, refer to Section 5.9, "Managing Passwords and Passphrases".

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

Section 2.2

Logging In

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

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

Figure 1: 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 5.8.2, "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 2.1, "Default User Names and Passwords".

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

Siemens strongly recommends that BFA protection be enabled. For more information about enabling BFA protection, refer to Section 6.3, "Enabling/Disabling Brute Force Attack Protection".

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

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

Section 2.3
Logging Out

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

Figure 2: Logout

1. Logout Link

Section 2.4

Navigating the Interface

RUGGEDCOM ROX II features a unique, but easy-to-use Web-based user interface.

CONTENTS

Section 2.4.1

Menus

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

Figure 3: 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 2.4.2
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.

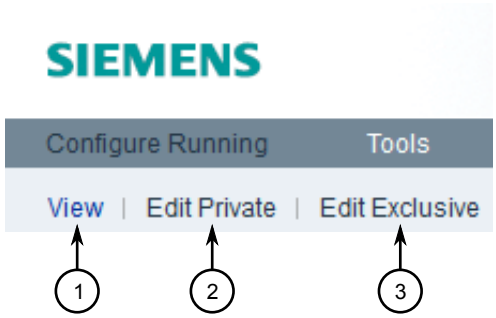


Figure 4: Modes Toolbar

1. View Mode **2.** Edit Private Mode **3.** Edit Exclusive Mode

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 2.4.3
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.

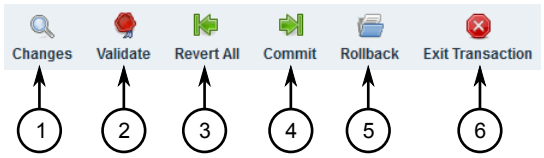


Figure 5: Edit Toolbar

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

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

Section 2.4.4
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).

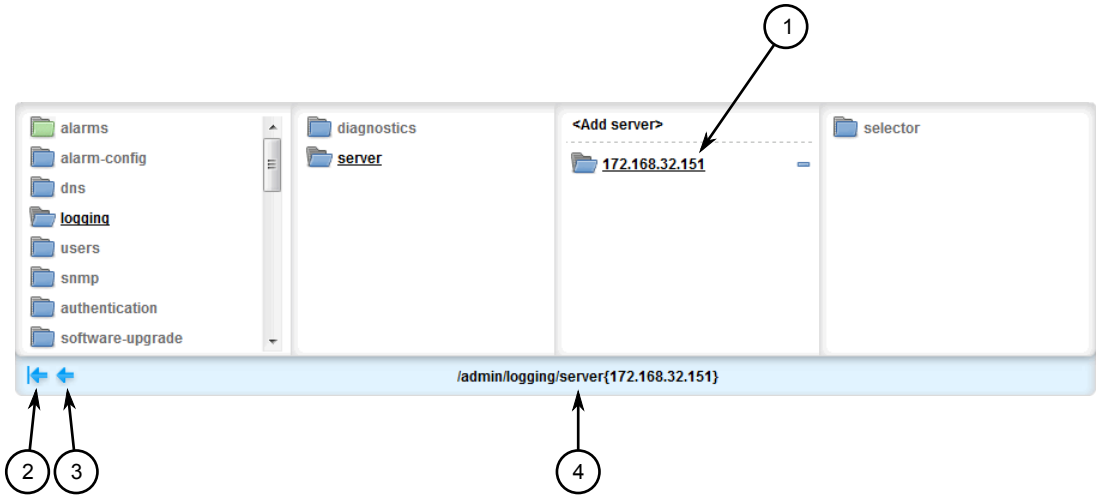


Figure 6: Navigation Menu

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 2.4.5

Icons

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

Figure 7: Icon In a Form

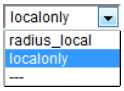
The following icons appear in RUGGEDCOM ROX II:

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

Section 2.4.6

Common Controls

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

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

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

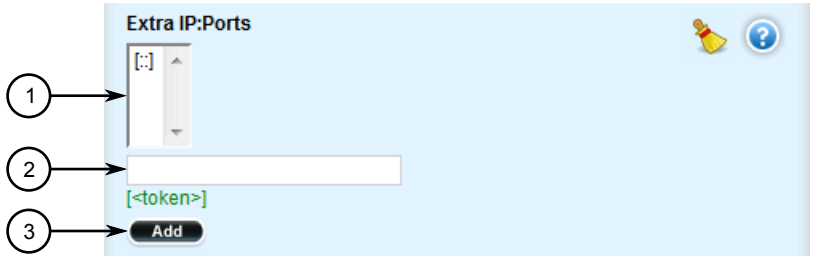


Figure 8: Example - Complex Control

1. List **2.** Box **3.** Button

Section 2.5

Using Network Utilities

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

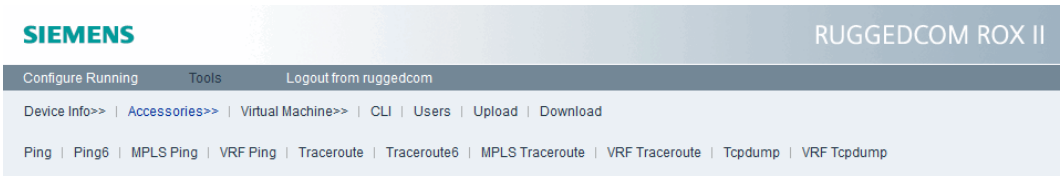


Figure 9: Accessories Menu

CONTENTS

Section 2.5.1

Pinging an IPv4 Address or Host

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

1. Select the **Tools** menu, click **Accessories**, and then click **Ping**. The ping console appears.

Figure 10: Ping Console

1. New Button **2.** Stop Button **3.** Current Ping Session List

2. Click **New**. A dialog box appears.

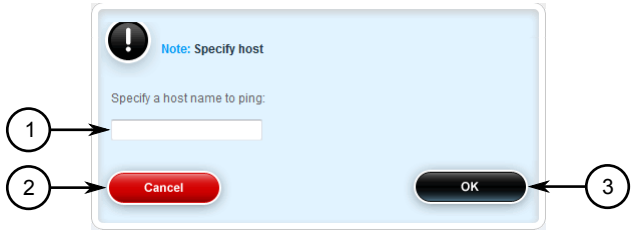


Figure 11: Dialog Box

1. Specify Host Box **2.** Cancel Button **3.** OK Button

3. Type the host name or IPv4 address and then click **OK**. The dialog box disappears and the ping results are displayed.

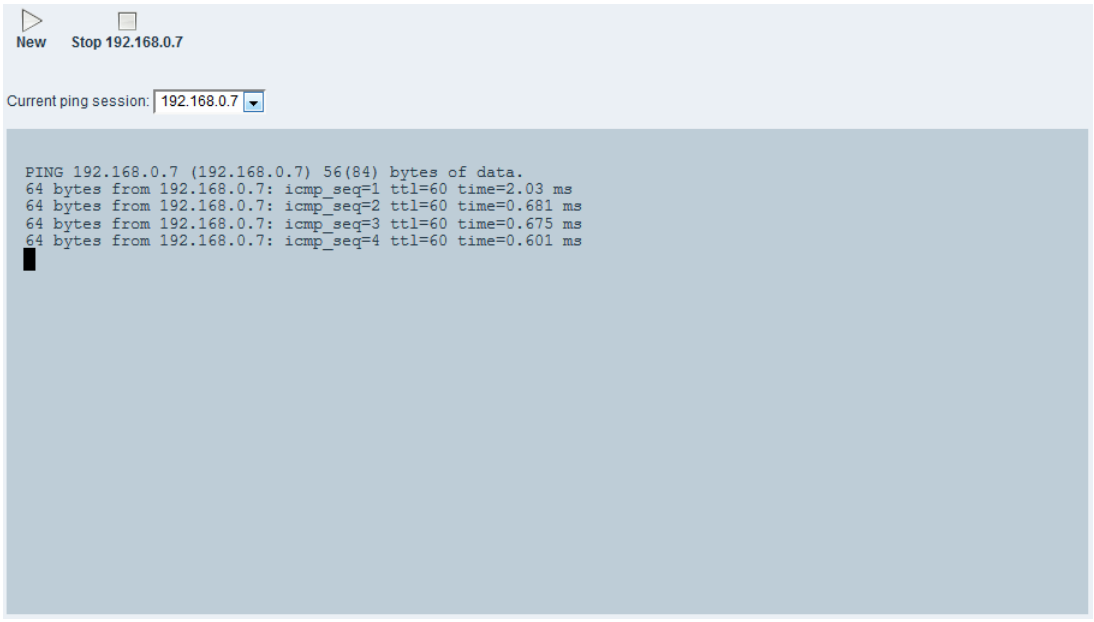


Figure 12: Example

NOTE
*The target IPv4 address or host name appears in the **Current Ping Session** list while the device is actively pinging the target.*

4. [Optional] Repeat Step 2 to Step 3 to start a new session, or select another active sessions from the **Current Ping Session** list.
5. Click **Stop {address}** to stop the ping request. The ping results are removed automatically.

Section 2.5.2
Pinging an IPv6 Address or Host

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

1. Select the **Tools** menu, click **Accessories**, and then click **Ping6**. The **ping6** console appears.

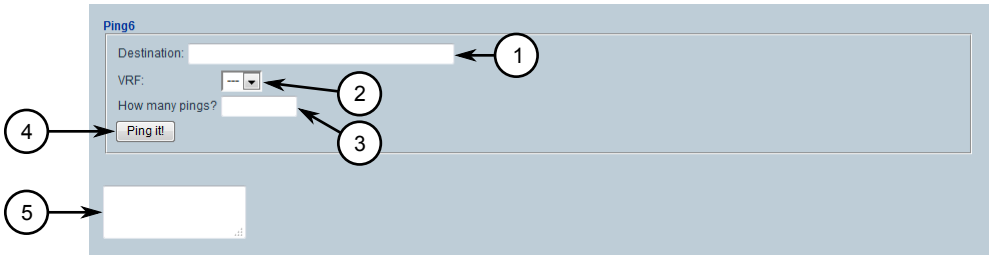


Figure 13: Ping6 Console

1. Destination Box **2.** VRF List **3.** How Many Pings Box **4.** Ping It Button **5.** Ping Results

2. Configure the following parameters as required:

Parameter	Description
Destination	The IPv6 address or name of the host.
VRF	The target VRF. Only required when pinging VRF routes.
How Many Pings	The number of ping attempts.

3. Click **Ping It**. The results of the ping action are displayed in the box below.

Section 2.5.3
Pinging MPLS Endpoints

To ping an MPLS endpoint, do the following:

1. Select the **Tools** menu, click **Accessories**, and then click **MPLS Ping**. The **mplsPing** console appears.

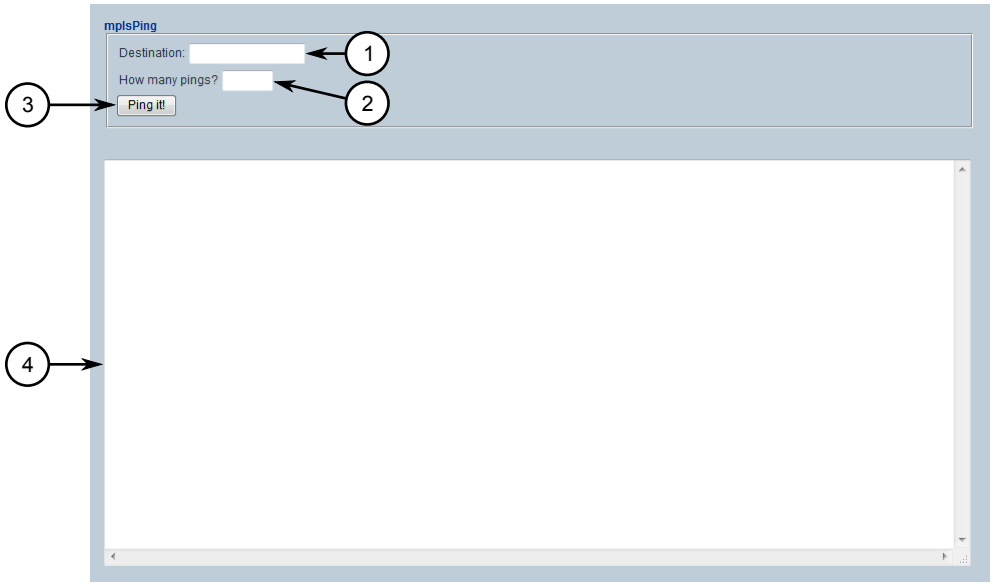


Figure 14: mplsPing Screen

1. Destination Box **2.** How Many Pings Box **3.** Ping It Button **4.** Ping Results

2. Configure the following parameters as required:

Parameter	Description
Destination	The IPv4 address and prefix of the MPLS endpoint.
How Many Pings	The number of ping attempts.

3. Click **Ping It**. The results of the ping action are displayed in the box below.

Section 2.5.4

Pinging VRF Endpoints

To ping an VRF endpoint, do the following:

1. Select the **Tools** menu, click **Accessories**, and then click **VRF Ping**. The **vrf Ping** console appears.

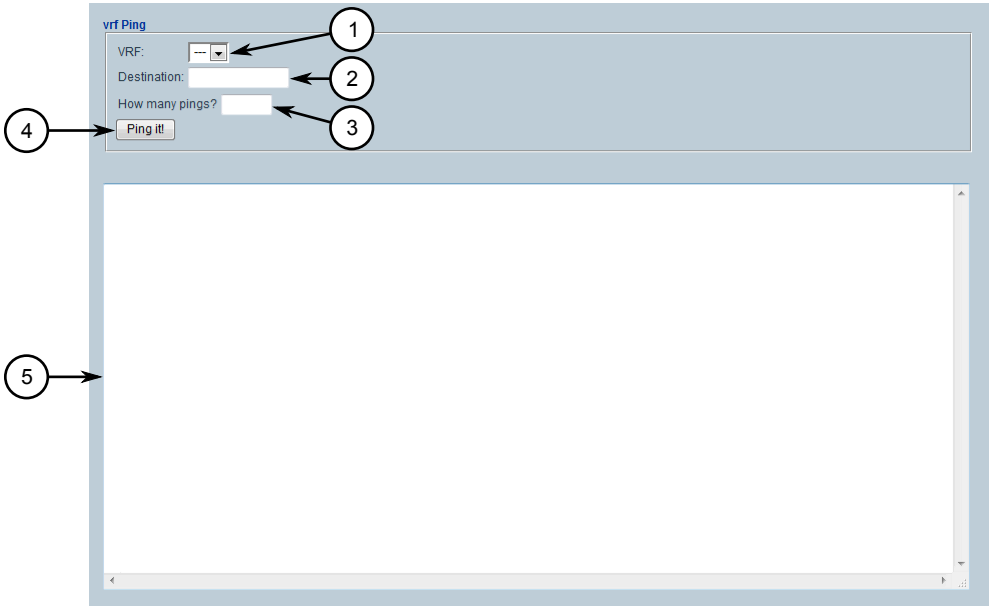


Figure 15: vrf Ping Screen

1. VRF List **2.** Destination Box **3.** How Many Pings Box **4.** Ping It Button **5.** Ping Results

2. Configure the following parameters as required:

Parameter	Description
VRF	The target VRF.
Destination	The IPv4 address and prefix of the VRF endpoint.
How Many Pings	The number of ping attempts.

3. Click **Ping It**. The results of the ping action are displayed in the box below.

Section 2.5.5

Tracing a Route to an IPv4 Host

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

1. Select the **Tools** menu, click **Accessories**, and then click **Traceroute**. The **Traceroute** console appears.

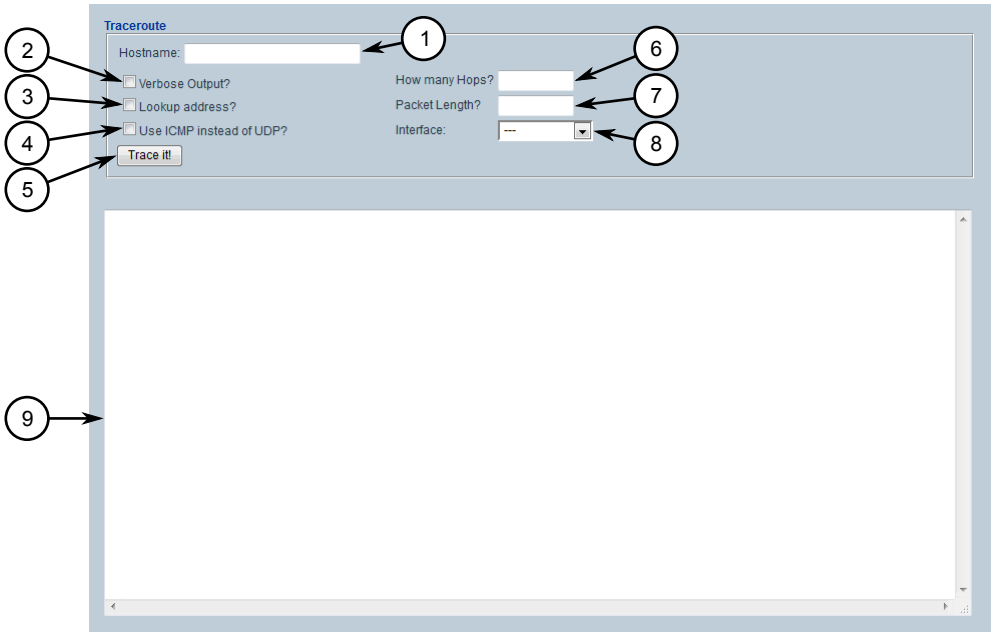


Figure 16: Traceroute Console

1. Hostname Box **2.** Verbose Output Check Box **3.** Lookup Address Check Box **4.** Use ICMP Instead of UDP Check Box **5.** Trace It Button **6.** How Many Hops Box **7.** Packet Length Box **8.** Interface List **9.** Trace Results

2. 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.
Packet Length	The maximum length of each packet.
Interface	The interface connected to the remote host.

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

Section 2.5.6

Tracing a Route to an IPv6 Host

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

1. Select the **Tools** menu, click **Accessories**, and then click **Traceroute6**. The **Traceroute for IPV6** console appears.

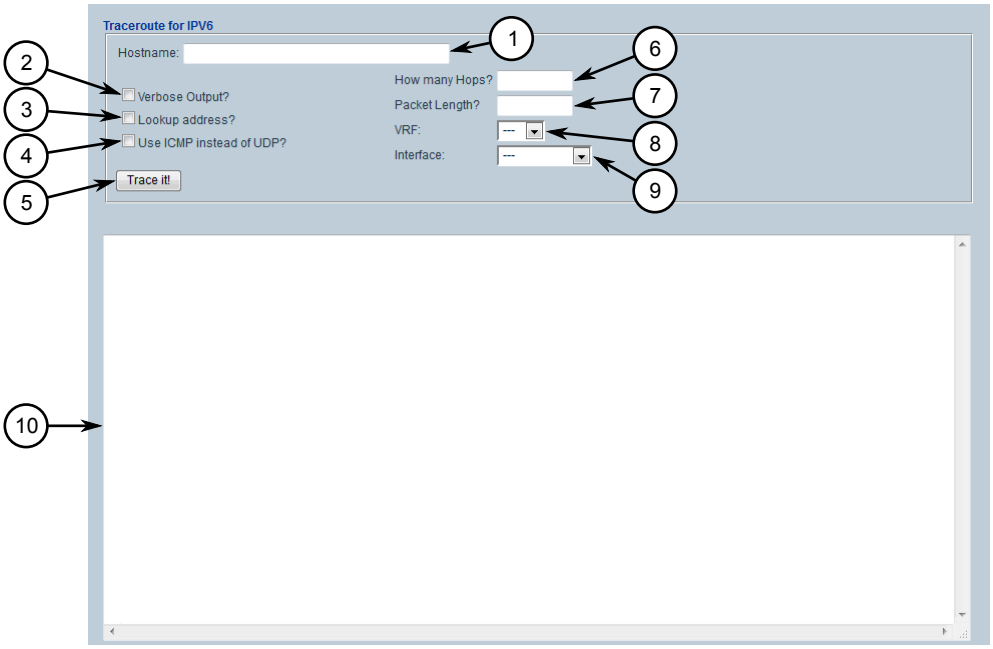


Figure 17: Traceroute for IPV6 Console

1. Hostname Box **2.** Verbose Output Check Box **3.** Lookup Address Check Box **4.** Use ICMP Instead of UDP Check Box **5.** Trace It Button **6.** How Many Hops Box **7.** Packet Length Box **8.** VRF List **9.** Interface List **10.** Trace Results

2. 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.
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.

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

Section 2.5.7

Tracing a Route to an MPLS Endpoint

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

1. Select the **Tools** menu, click **Accessories**, and then click **MPLS Traceroute**. The **mplsTrace** console appears.

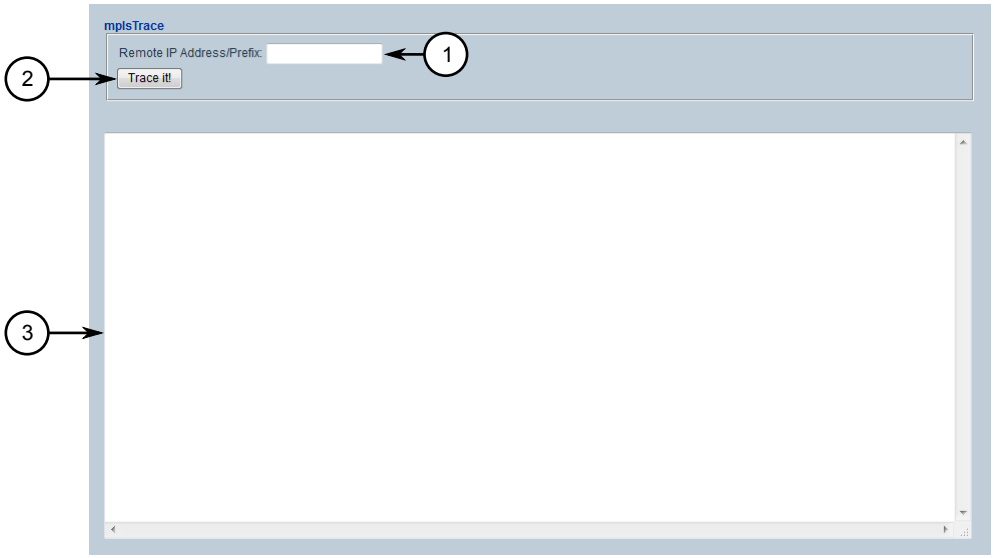


Figure 18: mplsTrace Console

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

2. Type the IPv4 address in the **Remote IP Address/Prefix** box and then click **Start**. The results of the trace are displayed below.

Section 2.5.8

Tracing a Route to a VRF Endpoint

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

1. Select the **Tools** menu, click **Accessories**, and then click **VRF Traceroute**. The **VRF Traceroute** console appears.

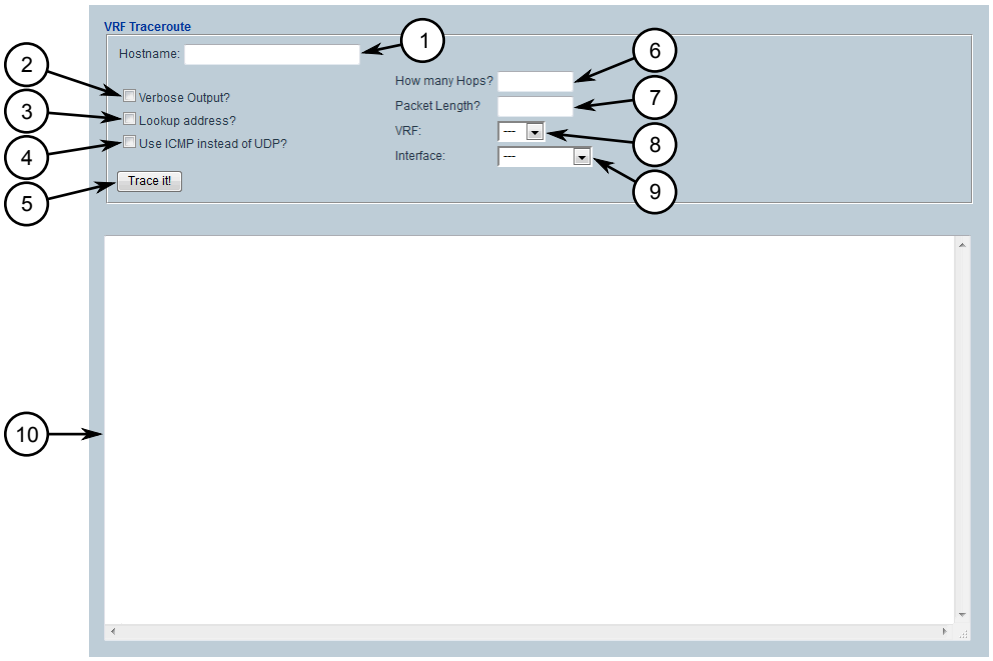


Figure 19: mplsTrace Console

1. Hostname Box **2.** Verbose Output Check Box **3.** Lookup Address Check Box **4.** Use ICMP Instead of UDP Check Box **5.** Trace It Button **6.** How Many Hops Box **7.** Packet Length Box **8.** VRF List **9.** Interface List **10.** Trace Results

2. 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.
Packet Length	The maximum length of each packet.
VRF	The target VRF.
Interface	The interface connected to the remote host.

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

Section 2.5.9

Capturing Packets from a Network Interface

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

To capture packets, do the following:

1. Select the **Tools** menu, click **Accessories**, and then click **Tcpdump**. The **Tcpdump a Network Interface** console appears.

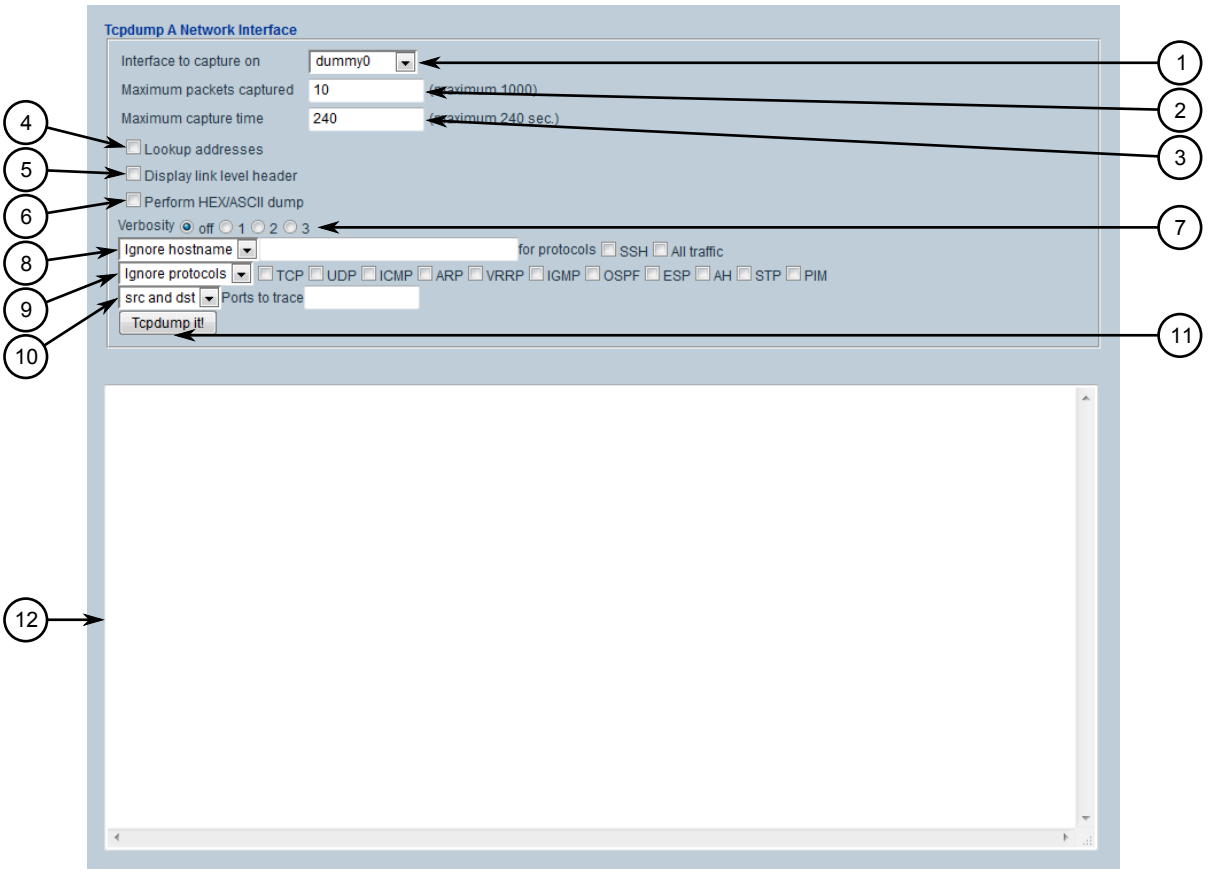


Figure 20: Tcpdump a Network Interface console

1. Interface To Capture On List **2.** Maximum Packets Captured Box **3.** Maximum Capture Time Box **4.** Lookup Addresses Check Box **5.** Display Link Level Header Check Box **6.** Perform HEX/ASCII Dump Check Box **7.** Verbosity Options **8.** Hostname Controls **9.** Protocol Controls **10.** Source/Destination Controls **11.** Tcpdump It Button

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

12. Click **Tcpdump It!** to start the dump. The results are displayed in the box below.

Section 2.5.10

Capturing Packets from a VRF Network Interface

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

To capture packets, do the following:

1. Select the **Tools** menu, click **Accessories**, and then click **VRF Tcpdump**. The **VRF Tcpdump** console appears.

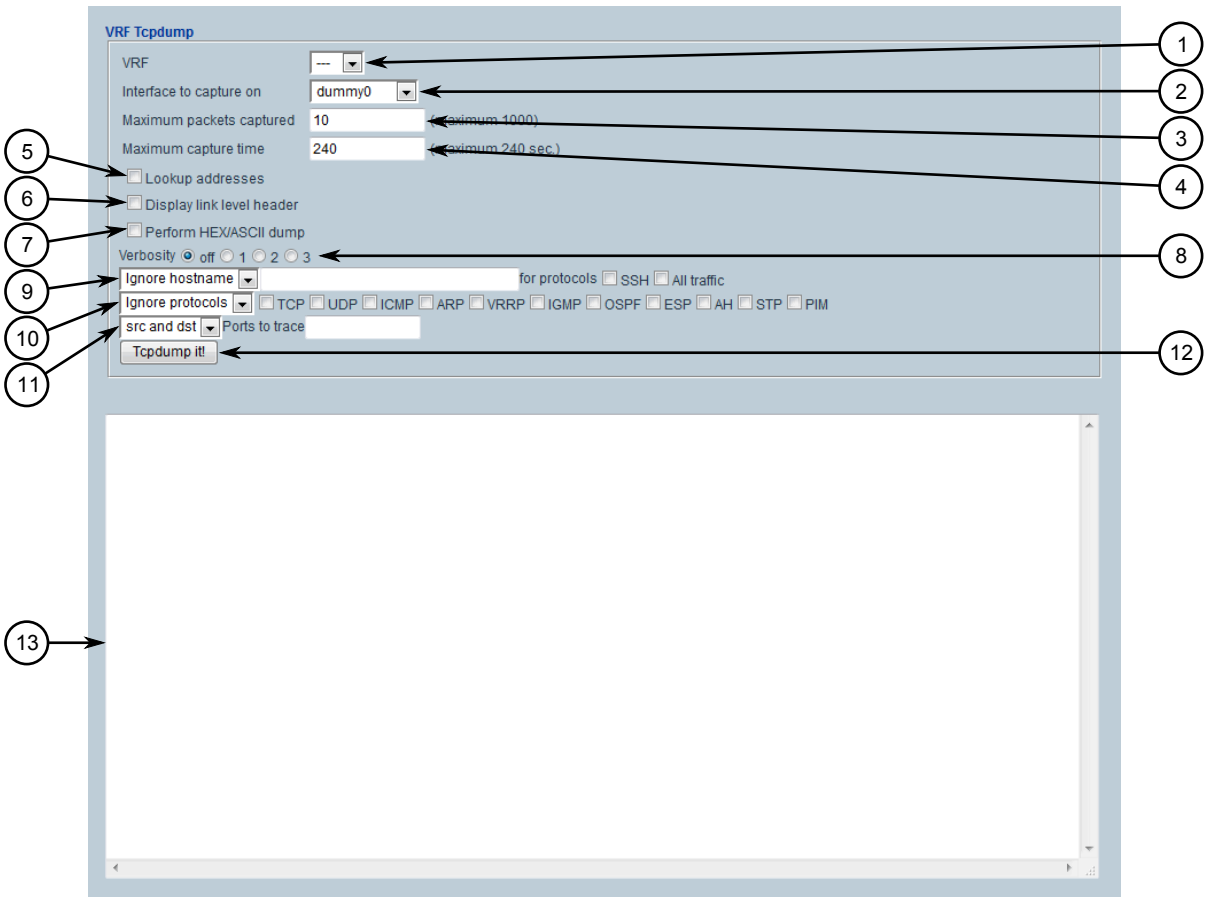


Figure 21: VRF Tcpdump

1. VRF List **2.** Interface To Capture On List **3.** Maximum Packets Captured Box **4.** Maximum Capture Time Box **5.** Lookup Addresses Check Box **6.** Display Link Level Header Check Box **7.** Perform HEX/ASCII Dump Check Box **8.** Verbosity Options **9.** Hostname Controls **10.** Protocol Controls **11.** Source/Destination Controls **12.** Tcpdump It Button

2. Under **Interface To Capture On**, select the interface to capture data from.
3. Under **Maximum Packets Captured**, set the maximum number of packets to capture.
4. Under **Maximum Capture Time**, set the maximum time to capture packets.
5. [Optional] Select **Lookup Addresses** to display the source IP for each packet.

6. [Optional] Select **Display Link Level Header** to display the link level header information for each packet.
7. [Optional] Select **Perform HEX/ASCII Dump** to convert the data to hexadecimal or ASCII characters.
8. Set the verbosity level to control how much information is dumped.
9. If a specific host name should be ignored, define the name of the host.
10. If a specific protocol(s) should be ignored, define the protocol type(s).
11. If packets are to be captured on a particular port, define the port.
12. Click **Tcpdump It!** to start the dump. The results are displayed in the box below.

Section 2.6

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.

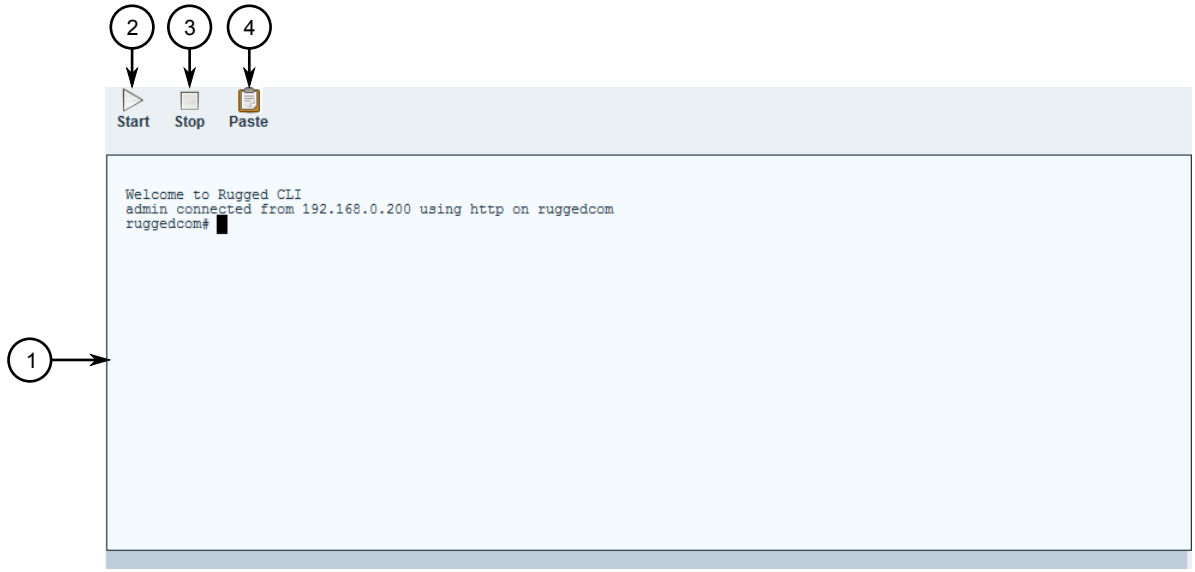


Figure 22: CLI Screen

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 v2.12 CLI User Guide*.

Section 2.7

Accessing Different Modes

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

3 Getting Started

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

CONTENTS

Section 3.1

Accessing RUGGEDCOM ROX II with Specific Web Browsers

At the time of release, default settings for certain Web browsers prevent users from accessing the RUGGEDCOM ROX II Web User Interface via HTTPS. The following describes how to configure these browsers.

NOTE
The following procedures were tested with the Web browser versions indicated and may not be compatible with previous or future versions. If problems are encountered, contact Siemens Customer Support for further assistance.

» Microsoft Internet Explorer®

Current versions of Microsoft Internet Explorer do not properly load Javascript when in Compatibility mode. This mode must be disabled to view the RUGGEDCOM ROX II Web User Interface.

To disable Compatibility mode in Microsoft Internet Explorer, do the following:

NOTE
The following steps were tested using Microsoft Internet Explorer v11.0.

1. Open Internet Explorer, press **Alt-X** and then click **Compatibility View Settings**. The **Compatibility View Settings** dialog box appears.
2. Clear the **Display intranet sites in Compatibility View** and **Use Microsoft compatibility lists** check boxes.
3. Click **Close** to close the dialog box.
4. Click **Start**, type **`gpedit.msc`** in the **Start Search** box, and then press **Enter**. The **Local Group Policy Editor** snap-in appears.

5. In the left pane, expand ***Local Computer Policy » Computer Configuration » Administrative Templates » Network*** and the click **SSL Configuration Settings**.
6. In the right pane, double click **SSL Cipher Suite Order**. The **SSL Cipher Suite Order** dialog box appears.
7. Select **Enabled**. The field under **Options** below **SSL Cipher Suites** automatically populates with a list of available cipher suites.
8. Replace the list of cipher suites with the following list:

   IMPORTANT!
   Cipher suites must be listed in a single comma-separated line without spaces.

   NOTE
   *The **Options** box supports up to 1023 characters.*

```
TLS_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA256,
TLS_RSA_WITH_AES_256_CBC_SHA,TLS_RSA_WITH_RC4_128_SHA,TLS_RSA_WITH_3DES_EDE_CBC_SHA,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P256,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P384,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P256,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P384,
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P256,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P384,
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256_P256,TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256_P256,
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384_P384,TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384_P384,
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA_P256,TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA_P384,
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA_P256,TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA_P384,
TLS_RSA_WITH_RC4_128_MD5,SSL_CK_RC4_128_WITH_MD5,SSL_CK_DES_192_EDE3_CBC_WITH_MD5,
TLS_RSA_WITH_NULL_MD5,TLS_RSA_WITH_NULL_SHA,TLS_RSA_WITH_NULL_SHA256,TLS_RSA_WITH_DES_CBC_SHA
```

9. Click **OK** to apply the changes
10. Reboot the workstation.

» Mozilla Firefox®

Some versions of Mozilla Firefox may produce an error message similar to the following when attempting to access the RUGGEDCOM ROX II Web User Interface:

```
An error occurred during a connection to 192.168.0.2. A PKCS #11 module returned
 CKR_DEVICE_ERROR, indicating that a problem has occurred with the token or slot. (Error code:
 sec_error_pkcs11_device_error)
```

To resolve this issue, download the latest version of Mozilla Firefox, then verify if connectivity to RUGGEDCOM ROX II is successful.

If the error persists, specific encryption ciphers must be disabled. To disable the ciphers, do the following:

NOTE
The following steps were tested using Mozilla Firefox v50.0.2.

1. Open Mozilla Firefox, type **`about:config`** in the address bar, and then press **Enter**. A confirmation message appears.
2. Click **I'll be careful, I promise!** to proceed. A list of preferences appears.
3. In the **Search** box at the top of the window, type **`security.ssl3.dhe_rsa_aes`**. The following preferences appear:
   - security.ssl3.dhe_rsa_aes_128_sha

- security.ssl3.dhe_rsa_aes_256_sha

4. Double-click each preference. The **Value** setting changes from `true` to `false`.

Section 3.2
Connecting to RUGGEDCOM ROX II

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

CONTENTS

Section 3.2.1
Default IP Address

The default IP address for the device is as follows:

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

Section 3.2.2
Connecting Directly

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

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

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

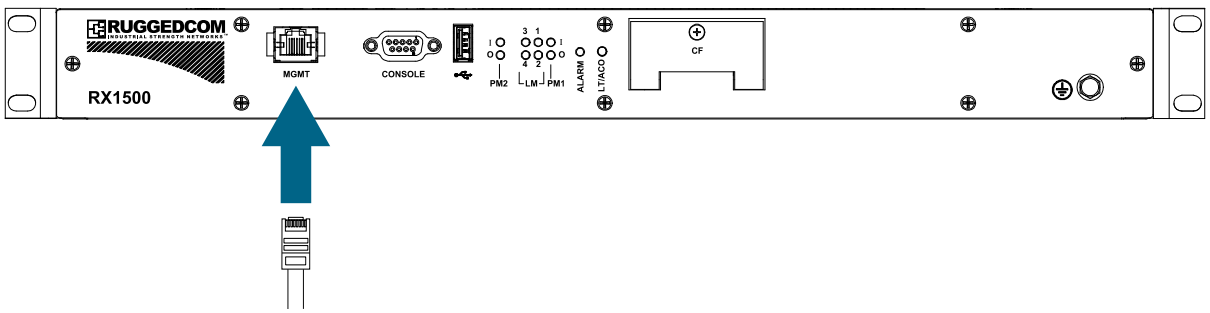


Figure 23: MGMT Port (RUGGEDCOM RX1500 Model Shown)

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

   For example, if the device's IP address is 192.168.0.2, configure the workstation's Ethernet port with an IPv4 address in the range of 192.168.0.3 to 192.168.0.254.
3. Launch a Web browser.
4. If using a proxy server, make sure the IP address and subnet for the device are included in the list of exceptions.
5. In the address bar, enter the host name or IP address for the device, and then press **Enter**.
6. If the device's SSH key has not been cached to the workstation's registry, a confirmation message will appear asking if the host is trusted. Click **Yes** to continue. The login prompt appears.
7. Log in to RUGGEDCOM ROX II. For more information, refer to Section 2.2, “Logging In”.

Section 3.2.3
Connecting Remotely

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

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

1. Launch a Web browser.
2. If using a proxy server, make sure the IP address and subnet for the device are included in the list of exceptions.
3. In the address bar, enter the host name or IP address for the device, and then press **Enter**.
4. If the device's SSH key has not been cached to the workstation's registry, a confirmation message will appear asking if the host is trusted. Click **Yes** to continue. The login prompt appears.
5. Log in to RUGGEDCOM ROX II. For more information, refer to Section 2.2, “Logging In”.

Section 3.3
Configuring a Basic Network

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

The following table lists the default IP addresses.

Interface	IP Address
switch.0001	192.168.0.2/24
fe-cm-1	192.168.1.2/24

CONTENTS

Section 3.3.1
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 6.3, “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 3.3.2
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 6.3, "Enabling/Disabling Brute Force Attack Protection".
7. Enable IPv6 Neighbor Discovery. For more information, refer to Section 7.1.5, "Configuring IPv6 Neighbor Discovery".
8. Make sure all computers connected to the device can ping one another.

4 Device Management

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

CONTENTS

Section 4.1

Displaying Device and Software Information

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

To display general information about the device and its software, navigate to ***chassis***. The **Chassis Status** form appears.

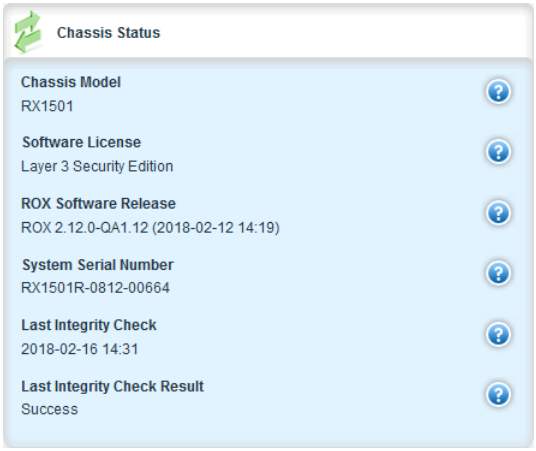


Figure 24: Chassis Status Form

This form provides the following information:

Parameter	Description
Chassis Model	**Synopsis:** A string The RuggedCom device model name.
Software License	**Synopsis:** A string The current software capability.
ROX Software Release	**Synopsis:** A string The release of ROX running on the chassis. This parameter is mandatory.
System Serial Number	**Synopsis:** A string 1 to 32 characters long The system serial number on the chassis label. This parameter is mandatory.
Last Integrity Check	**Synopsis:** A string 1 to 32 characters long The last time the firmware integrity was checked.
Last Integrity Check Result	**Synopsis:** A string The result of the last integrity check.

Section 4.2

Viewing Chassis Information and Status

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

CONTENTS

Section 4.2.1

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 Hardware

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 25: Slot Hardware Table

This table provides the following information:

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

Section 4.2.2
Viewing Module Information

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

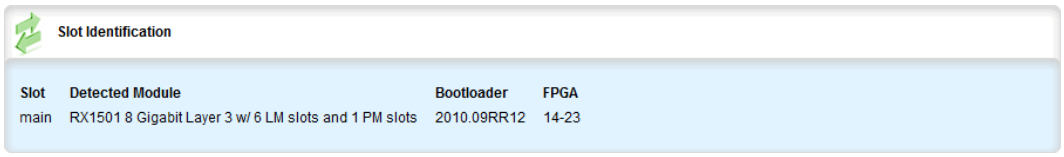


Figure 26: Slot Identification Table

This table provides the following information:

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

Section 4.2.3
Viewing Flash Card Storage Utilization

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

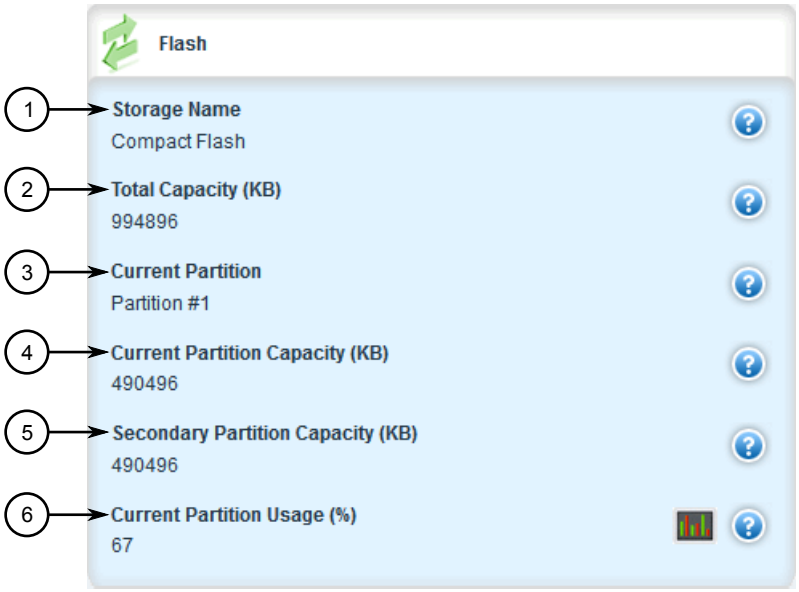


Figure 27: Flash Form

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	**Synopsis:** A string 0 to 32 characters long The type of storage.
Total Capacity (KiB)	**Synopsis:** A 32-bit unsigned integer between 0 and 4294967295 The total capacity of the flash storage in KB. This parameter is mandatory.
Current Partition	**Synopsis:** A string 0 to 32 characters long The partition ROX is currently running on and booted from. This parameter is mandatory.
Current Partition Capacity (KiB)	**Synopsis:** A 32-bit unsigned integer between 0 and 4294967295 The capacity of the current partition in KB. This parameter is mandatory.
Secondary Partition Capacity (KiB)	**Synopsis:** A 32-bit unsigned integer between 0 and 4294967295 The capacity of the secondary partition in KB. This parameter is mandatory.
Current Partition Usage (%)	**Synopsis:** A 32-bit signed integer between 0 and 100 The %usage of the current partition. This parameter is mandatory.

Section 4.2.4
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.

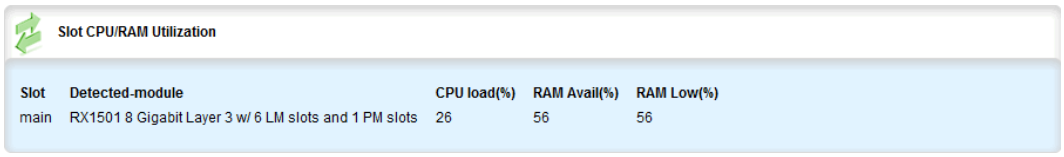


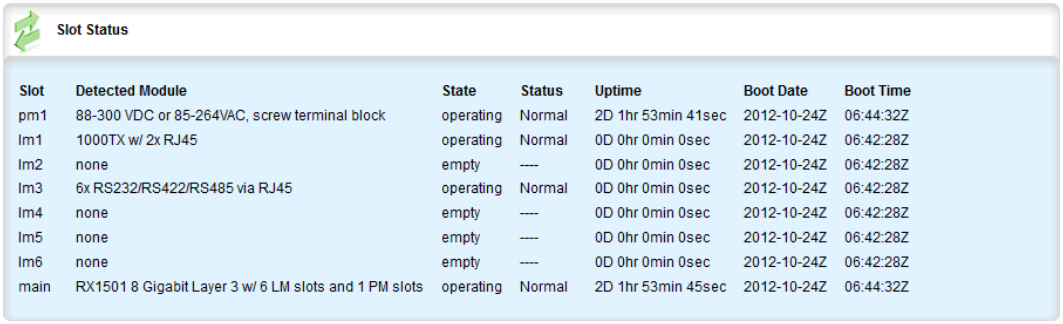
Figure 28: Slot CPU/RAM Utilization Table

This table provides the following information:

Parameter	Description
slot	**Synopsis:** { { --- }{ pm1, pm2, main }{ sm, lm1, lm2, lm3, lm4, lm5, lm6, swport, eth, serport, celport, wlanport }{ cm, em }{ trnk } } The slot name, as marked on the silkscreen across the top of the chassis.
Detected Module	**Synopsis:** A string 1 to 60 characters long The installed module's type specifier. This parameter is mandatory.
CPU load(%)	**Synopsis:** A 32-bit signed integer between 0 and 100 The CPU load, in percent, on the installed module.
RAM Avail(%)	**Synopsis:** A 32-bit signed integer between 0 and 100 The proportion of memory (RAM) currently unused, in percent, on the installed module.
RAM Low(%)	**Synopsis:** A 32-bit signed integer between 0 and 100 The lowest proportion of unused memory (RAM), in percent, recorded for the installed module since start-up.

Section 4.2.5
Viewing the Slot Status

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



Slot Status

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 29: Slot Status Table

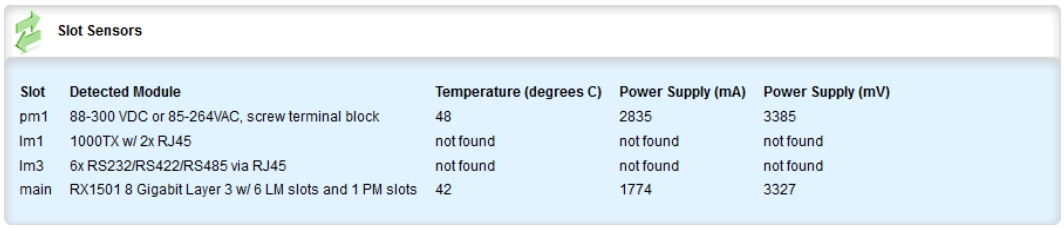
This table provides the following information:

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

Section 4.2.6

Viewing the Slot Sensor Status

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



Slot Sensors

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 30: Slot Sensors Table

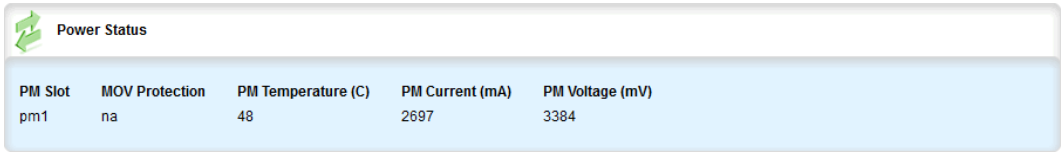
This table provides the following information:

Parameter	Description
slot	**Synopsis:** { { --- }{ pm1, pm2, main }{ sm, lm1, lm2, lm3, lm4, lm5, lm6, swport, eth, serport, celport, wlanport }{ cm, em }{ trnk } } The slot name, as marked on the silkscreen across the top of the chassis.
Detected Module	**Synopsis:** A string 1 to 60 characters long The installed module's type specifier. This parameter is mandatory.
Temperature (degrees C)	**Synopsis:** A 32-bit signed integer between -55 and 125 The temperature, in degrees C, of the installed module. If multiple temperature sensors are present on the board, the maximum reading is reported. This parameter is mandatory.
Power Supply (mA)	**Synopsis:** A 32-bit signed integer between 0 and 15000 The power supply current, in mA, being drawn by the installed module.
Power Supply (mV)	**Synopsis:** A 32-bit signed integer between 0 and 15000 The power supply voltage, in mV, seen by the installed module.

Section 4.2.7

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 31: Power Status Table

This table provides the following information:

Parameter	Description
PM Slot	**Synopsis:** { pm1, pm2 }

Parameter	Description
	The name of the power module slot as labeled on the chassis.
MOV Protection	**Synopsis:** { na, working, damaged } The state of the MOV protection circuit.
PM Temperature (C)	**Synopsis:** A 32-bit signed integer between -55 and 125 The temperature (Celsius) inside the power module.
PM Current (mA)	**Synopsis:** A 32-bit signed integer between 0 and 15000 The current (mA) sourced by the power module.
PM Voltage (mV)	**Synopsis:** A 32-bit signed integer between 0 and 15000 The voltage (mV) sourced by the power module.

Section 4.3
Viewing the Parts List

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

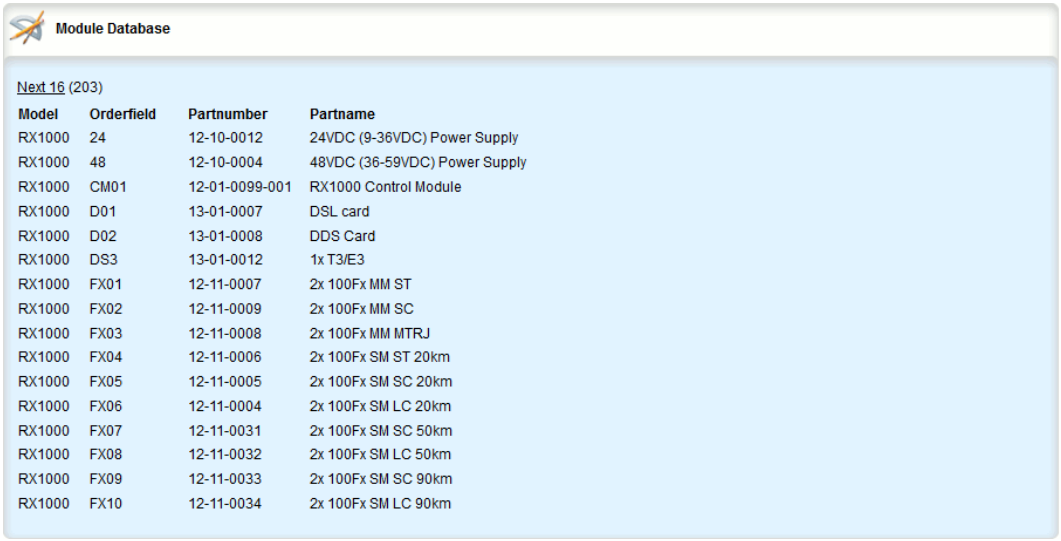


Figure 32: Module Database Table

Section 4.4
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 devices shuts down and provides a time-out period during which power can be disconnected from the device. The default time-out period is 300 seconds (five minutes). At the end of the time-out period, the device reboots and restarts.

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

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

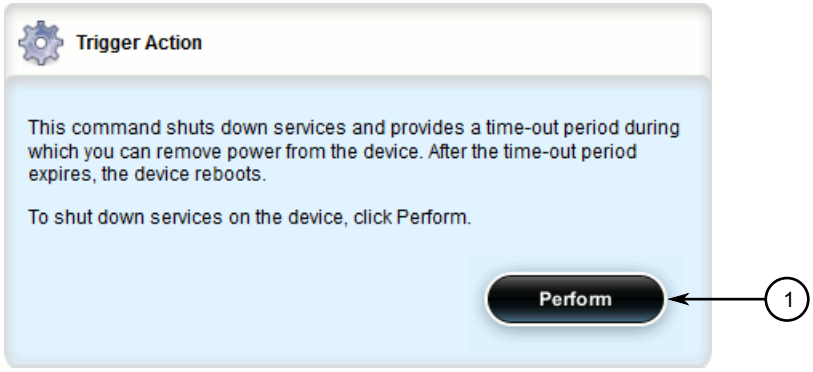


Figure 33: Trigger Action Form

1. Perform Button

2. Click **Perform**.

Section 4.5
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.

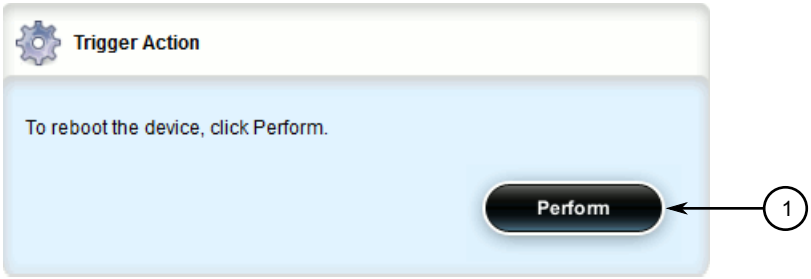


Figure 34: Trigger Action Form

1. Perform Button

2. Click **Perform**.

Section 4.6

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 35: 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

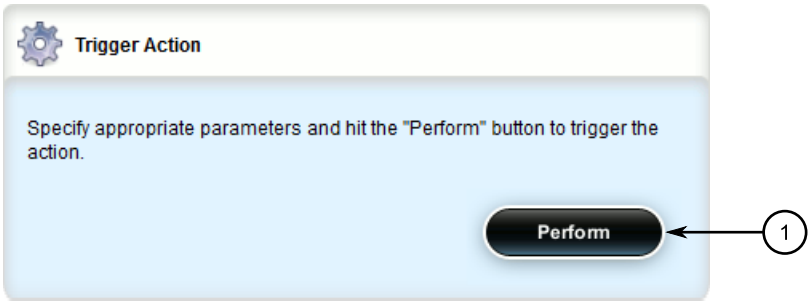


Figure 36: Trigger Action Form

1. Perform Button

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

Parameter	Description
Delete Logs	**Synopsis:** { true, false } **Default:** false Delete system logs as well as restoring default settings.
Default Both Partitions	**Synopsis:** { true, false } **Default:** false Perform the operation on both partitions.
Delete Saved Configurations	**Synopsis:** { true, false } **Default:** false Delete saved configuration files (works with default-both-partitions option).
shutdown	**Synopsis:** { true, false } **Default:** false Shutdown rather than reboot after restoring factory defaults.

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

Section 4.7

Decommissioning the Device

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

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 v2.12 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 2.2, "Logging In".
6. Flash the RUGGEDCOM ROX II firmware obtained in Step 1 to the inactive partition and reboot the device. For more information, refer to Section 4.12.5.2, "Downgrading Using ROXflash".
7. Repeat Step 5 and Step 6 to flash the RUGGEDCOM ROX II firmware obtained in Step 1 to the other partition and reboot the device.
8. Shut down the device. For more information, refer to Section 4.4, "Shutting Down the Device".

Section 4.8

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 https://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 an 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 for the device. An upgraded feature key file will be provided that is licensed to the device. For information on how to determine the *main* serial number, refer to Section 4.1, "Displaying Device and Software Information".

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 4.9.3, "Installing Files".

For information on how to backup a feature key, refer to Section 4.9.4, "Backing Up Files".

To view the contents of a feature key, refer to the *RUGGEDCOM ROX II v2.12 CLI Web Interface User Guide* for the RX1500/RX1501/RX1510/RX1511/RX1512.

Section 4.9

Managing Files

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

- **Upload**
  Allows users to upload files from a PC.

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

CONTENTS

Section 4.9.1

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.

Figure 37: Upload Screen

1. File Type List **2.** File Box **3.** Browse Button **4.** Send Button

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 4.9.2
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 38: 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 4.9.3
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 RX1500/RX1501/RX1510/RX1511/RX1512 Installation Guide*.
2. Navigate to ***admin*** and click **install-files** in the menu. The **Install Files** and **Trigger Action** forms appear.

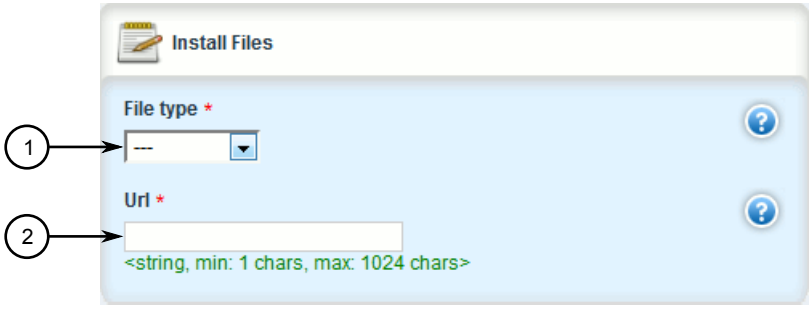


Figure 39: Install Files Form

1. File Type List **2.** URL Box

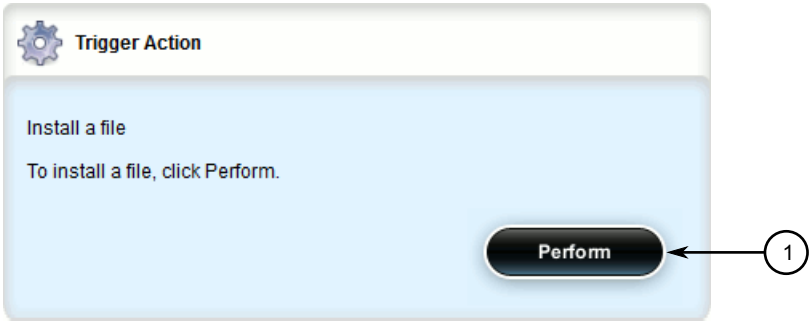


Figure 40: Trigger Action Form

1. Perform Button

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

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

Parameter	Description
File type	**Synopsis:** { config, featurekey, vmfile } The file types to be copied. This parameter is mandatory.
url	**Synopsis:** A string 1 to 1024 characters long The URL of the ROX II file to copy. Supported URIs are HTTP, SCP, SFTP, FTPS and FTP. To install from a USB flash drive or microSD card (if applicable), the URL format is "usb://{usb-device-name}/path-to-file-on-system" or "sd://sd-1//path-to-file-on-system". Run "show chassis" to determine the name of the USB device. Note that only one single partition is supported for either data medium. For all other protocols, the format is "protocol://user:password@host:port/path-to-file". If "port" is not specified, the default port for the protocol is used. This parameter is mandatory.

4. On the **Trigger Action** form, click **Perform**.
5. If the VPE feature key (VIRTUALM) was installed, reboot the device to reveal the virtualization features. For more information, refer to Section 4.5, "Rebooting the Device".

Section 4.9.4
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 RX1500/RX1501/RX1510/RX1511/RX1512 Installation Guide*.
2. Navigate to ***admin*** and click **backup-files** in the menu. The **Backup Files** and **Trigger Action** forms appear.

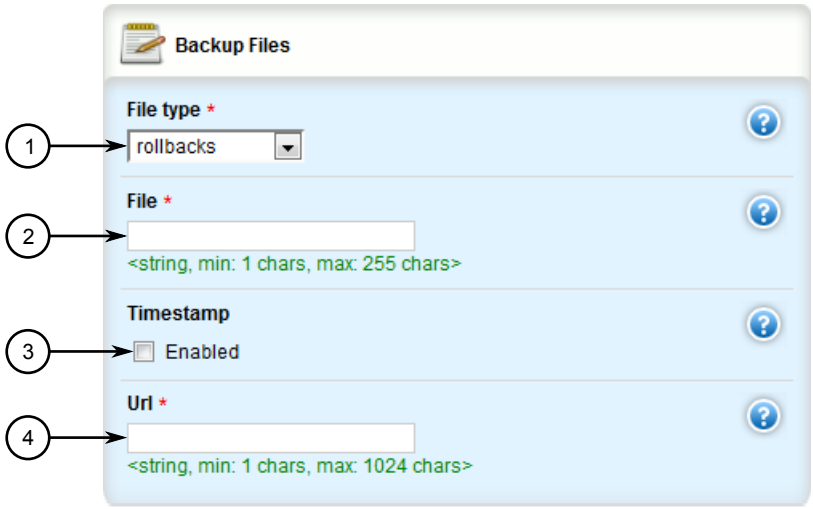


Figure 41: Backup Files Form

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

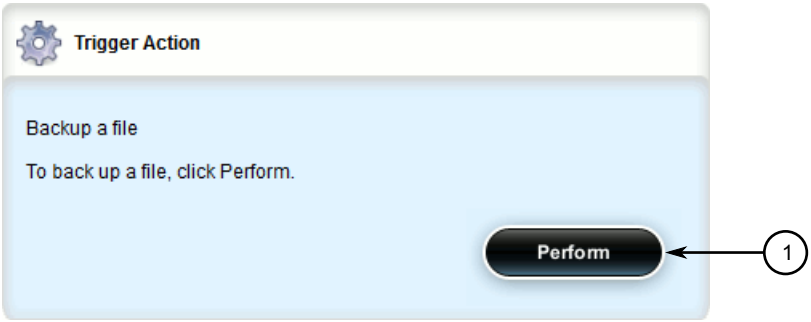


Figure 42: Trigger Action

1. Perform Button

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

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

Parameter	Description
File type	**Synopsis:** { config, featurekey, logfiles, rollbacks, licenses, logarchive } The file types to copy. This parameter is mandatory.
file	**Synopsis:** A string 1 to 255 characters long The name of the logarchive or a list of file names to copy. For logarchive, only 1 file name is accepted to name the tar-archive that will be used to backup of the entire /var/log directory. The archive is created in /tmp directory and will be automatically deleted. This parameter is mandatory.
timestamp	**Synopsis:** { true, false } **Default:** false If enabled, a time stamp will be appended to the file name. This option is not applicable to file names that contain '*'.
url	**Synopsis:** A string 1 to 1024 characters long The URL of the ROX II file to copy. Supported URIs are HTTP, SCP, SFTP, FTPS and FTP. To save to a USB flash drive or microSD card (if applicable), the URL format is "usb://{usb-device-name}/path-to-file" or "sd://sd-1//path-to-file". Run "show chassis" to determine the name of the USB device. Note that only one single partition is supported for either data medium. For all other protocols, the format is "protocol://user:password@host:port/path-to-file". If using a path only, close it with '/'. If "port" is not specified, the default port for the protocol is used. This parameter is mandatory.

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

Section 4.10
Managing Logs

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

Security Event Logs

Information related to the following security events are logged by RUGGEDCOM ROX II:

NOTE
Passwords can be retried up to 3 times before the login attempt is considered a security event.

- Successful and unsuccessful login attempts
- Local and remote (RADIUS) authentication
- Security-sensitive commands (whether successful or unsuccessful)
- An optionally configurable SNMP Authentication Failure Trap (disabled by default) in accordance with SNMPv2-MIB

All security event logs are recorded in `var/log/auth.log` and can be viewed in the Authlog Viewer. For more information about viewing logs, refer to Section 4.10.1, "Viewing Logs".

Syslogs	Syslog allows users to configure local and remote syslog connections to record important, non-security event information. The remote Syslog protocol, defined in RFC 3164 [http://tools.ietf.org/html/rfc3164], is a UDP/IP-based transport that enables a device to send event notification messages across IP networks to event message collectors, also known as Syslog servers. The protocol is designed to simply transport these event messages from the generating device to the collector. All log files are organized in the log directory (`/var/log`) according to the facility and priority at which they have been logged. Remote Syslog sends the requested logs to the remote server(s) at whichever facility and priority they were initially logged, after filtering the logs based on the selectors configured for the server. The following log files are setup with the following default selectors: • `syslog` catches all logs except daemon.debug, auth or authpriv logs • `daemon.log` catches all *err* level (and above) logs written to the daemon facility • `messages` catches all *info*, *notice* and *warn* level logs for all facilities except auth, authpriv, cron, daemon, mail and news A selector setup using the following facilities at level *info* and up is recommended: • daemon • user • kern • syslog
Diagnostic Logs	Diagnostic logs record system information for the purposes of troubleshooting.

CONTENTS

Section 4.10.1

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 4.9.4, “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:

Messages Viewer	Displays all events from `/var/log/messages`
Syslog Viewer	Displays syslog events from `/var/log/syslog`
Authlog Viewer	Displays authentication events from `/var/log/auth.log`
Layer2log Viewer	Displays Layer 2 events from `/var/log/layer2`

Kernlog Viewer	Displays kernel events from `/var/log/kern.log`

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

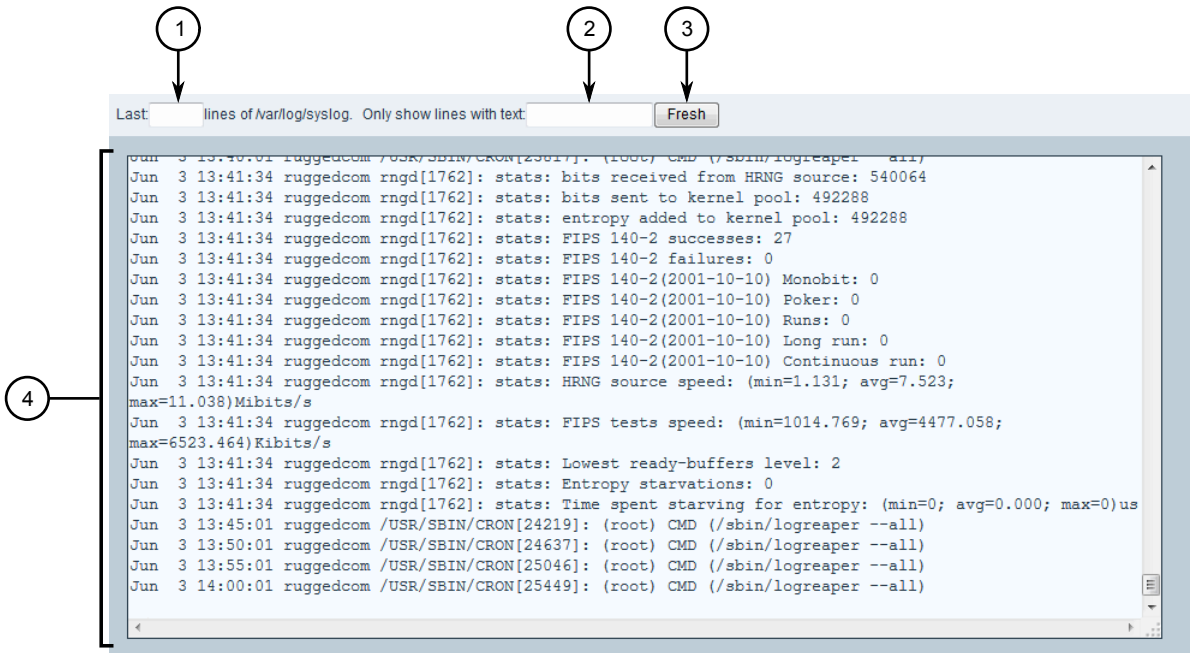


Figure 43: Syslog Viewer (Example)

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 4.10.2

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.

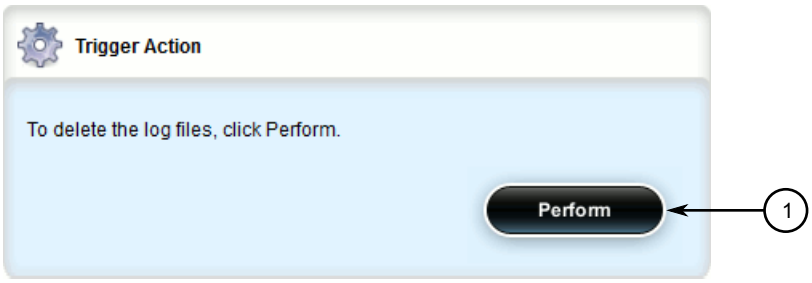


Figure 44: Trigger Action Form

1. Perform Button

2. Click **Perform**.

Section 4.10.3
Configuring Secure Remote Syslog

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

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

CONTENTS

Section 4.10.3.1
Enabling/Disabling Secure Remote Syslog

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

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to ***admin » logging » secure-remote-syslog***. The **Secure Remote Syslog** form appears.

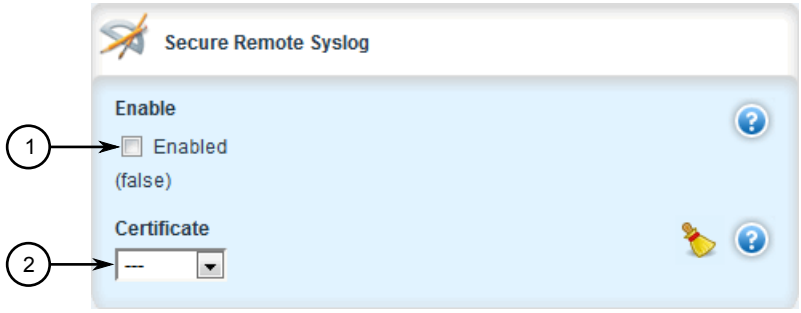


Figure 45: Secure Remote Syslog Form

1. Enable Check Box **2.** Certificate List

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 6.7.7.3, "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 4.10.3.3, "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 4.10.3.2
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 4.10.3.3, "Adding a Permitted Peer".

Section 4.10.3.3
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.

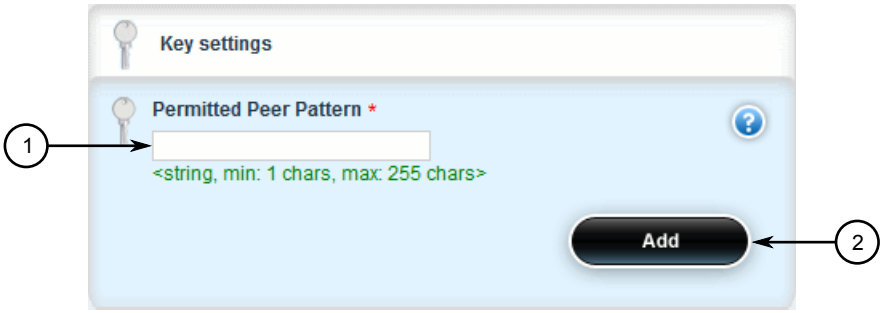


Figure 47: Key Settings Form

1. Permitted Peer Pattern Box **2.** Add Button

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

Parameter	Description
Permitted Peer Pattern	**Synopsis:** 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 4.10.3.4
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.

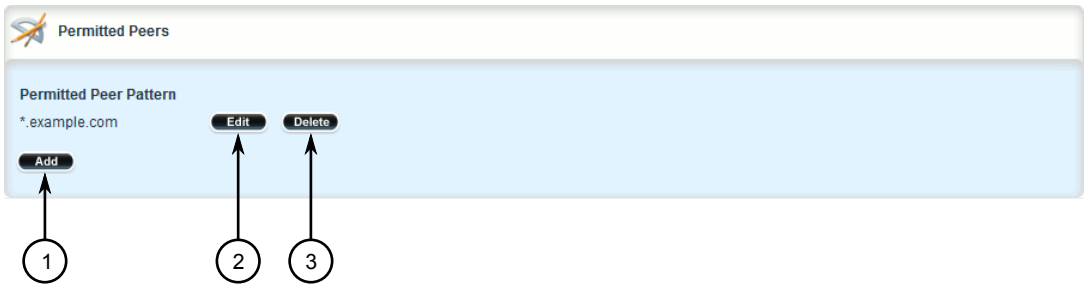


Figure 48: Permitted Peers Table

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

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 4.10.3.5

Configuring a Source IP Address for Remote Syslog Messages

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

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

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Make sure an IP address is first defined for the desired interface. For more information, refer to either Section 7.1.3.2, “Adding an IPv4 Address” or Section 7.1.4.2, “Adding an IPv6 Address”.
3. Navigate to ***admin » logging***. The **Remote Logging** form appears.

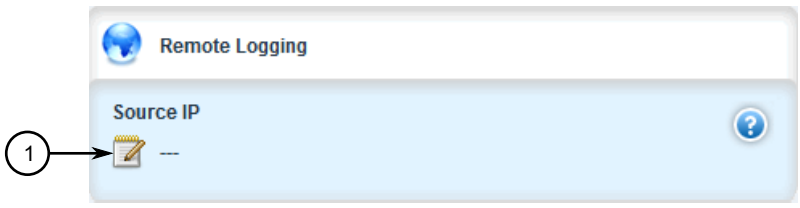


Figure 49: Remote Logging Form

1. Source IP Address Box

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 4.10.4
Managing Diagnostic Logs

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

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

CAUTION!
Configuration hazard – risk of reduced performance. Enabling diagnostic logging will significantly affect the performance of RUGGEDCOM ROX II. Only enable diagnostic logging when directed by Siemens.

CONTENTS

Section 4.10.4.1
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.

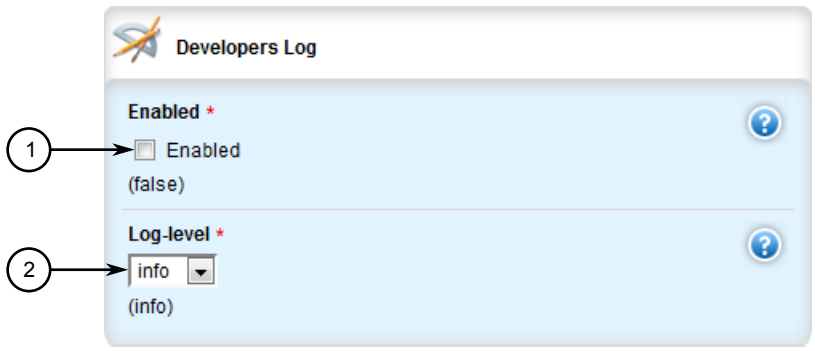


Figure 50: Developer's Log Form

1. Enabled Check Box **2.** Log-Level List

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

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

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 4.10.4.2
Enabling/Disabling the SNMP Log

The SNMP log records all SNMP related events.

CAUTION!
Configuration hazard – risk of reduced performance. Enabling diagnostic logging will significantly affect the performance of RUGGEDCOM ROX II. Only enable diagnostic logging when directed by Siemens.

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

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

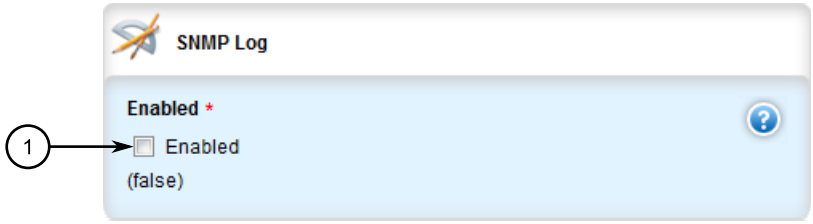


Figure 51: SNMP Log Form

1. Enabled Check Box

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

Parameter	Description
Enabled	**Synopsis:** { true, false } **Default:** 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 4.10.4.3

Enabling/Disabling the NETCONF Summary Log

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

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

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.

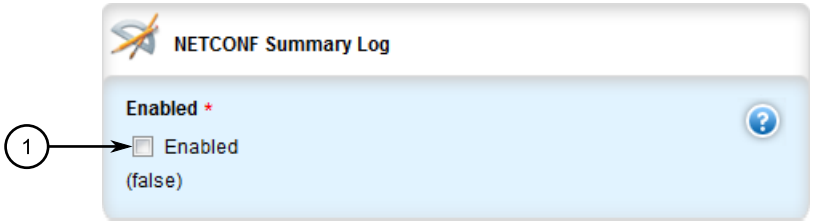


Figure 52: NETCONF Summary Log Form

1. Enabled Check Box

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

Parameter	Description
Enabled	**Synopsis:** { true, false } **Default:** false Enables/Disables NETCONF logging to the netconf.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 4.10.4.4

Enabling/Disabling the NETCONF Trace Log

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

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

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

CAUTION!
Configuration hazard – risk of reduced performance. Enabling diagnostic logging will significantly affect the performance of RUGGEDCOM ROX II. Only enable diagnostic logging when directed by Siemens.

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

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

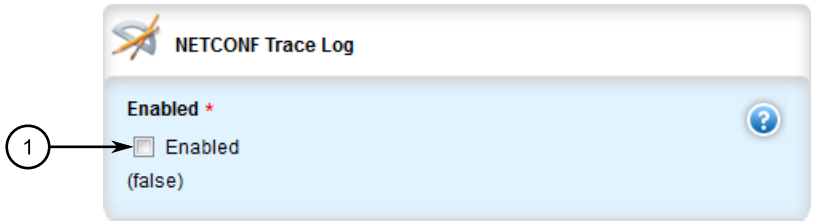


Figure 53: NETCONF Trace Log Form

1. Enabled Check Box

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

Parameter	Description
Enabled	**Synopsis:** { true, false } **Default:** false Enables/disables NETCONF Trace logging to netconf-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 4.10.4.5
Enabling/Disabling the XPATH Trace Log

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

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.

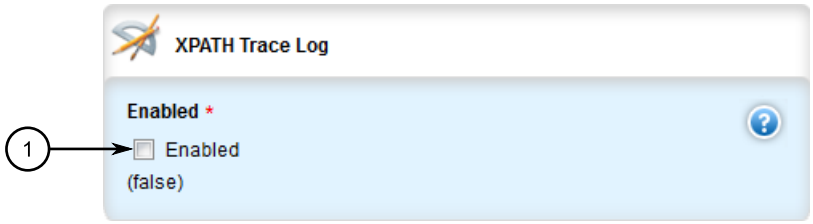


Figure 54: XPATH Trace Log Form

1. Enabled Check Box

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

Parameter	Description
Enabled	**Synopsis:** { true, false } **Default:** 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 4.10.4.6

Enabling/Disabling the WebUI Trace Log

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

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

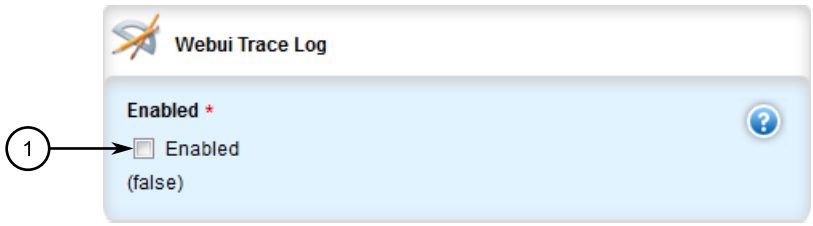


Figure 55: WebUI Trace Log Form

1. Enabled Check Box

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

Parameter	Description
Enabled	**Synopsis:** { true, false } **Default:** false Enables/disables WebUI Trace logging to the webui-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 4.10.5

Managing Remote Syslog Servers

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

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

CONTENTS

Section 4.10.5.1

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.

Figure 56: Remote Server Table

If no remote servers have been configured, add servers as needed. For more information, refer to Section 4.10.5.2, "Adding a Remote Server".

Section 4.10.5.2
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.

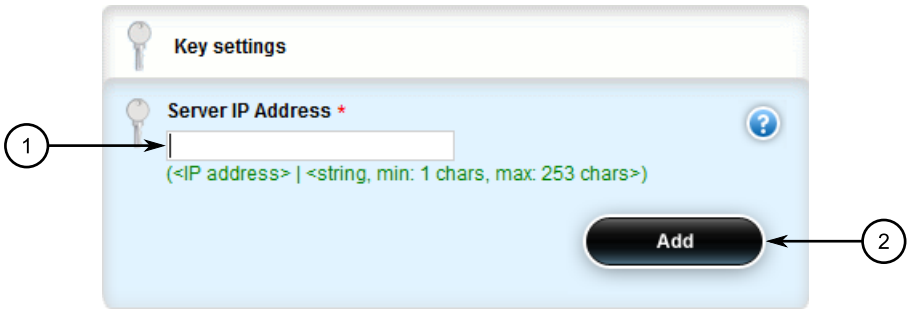


Figure 57: Key Settings Form

1. Server IP Address Box **2.** Add Button

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

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

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

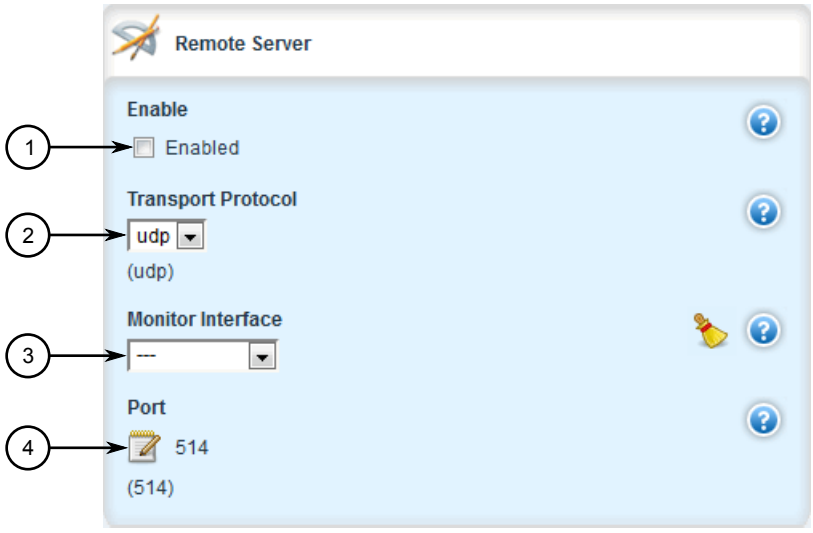


Figure 58: Remote Server Form

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	Enables/disables the feed to the remote logging server.
Transport Protocol	**Synopsis:** { udp, tcp } **Default:** udp TCP or UDP.
Monitor Interface	**Synopsis:** A string The interface to monitor. If the IP address is changed on the interface, the logging daemon will restart.
Port	**Synopsis:** A 16-bit unsigned integer between 1 and 65535 **Default:** 514 Port number.

6. Configure one or more selectors for the server. For more information, refer to Section 4.10.6.2, "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 4.10.5.3
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.

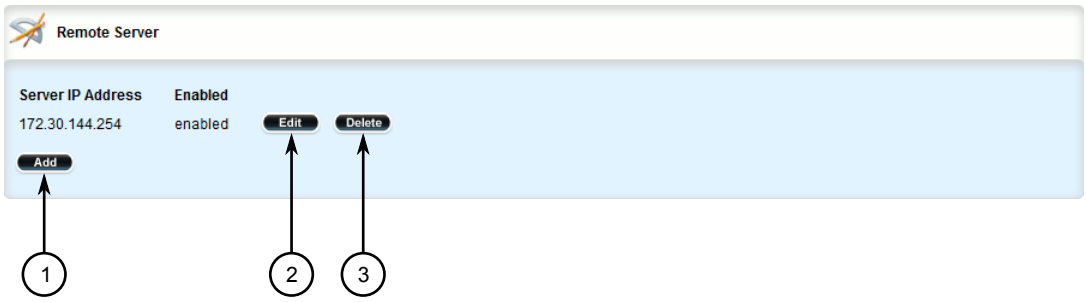


Figure 59: Remote Server Table

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

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 4.10.6

Managing Remote Server Selectors

Remote server selectors filter the information sent to specific servers.

CONTENTS

Section 4.10.6.1

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.

Figure 60: Remote Server Selector Table

If no remote server selectors have been configured, add selectors as needed. For more information, refer to Section 4.10.6.2, "Adding a Remote Server Selector".

Section 4.10.6.2
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.

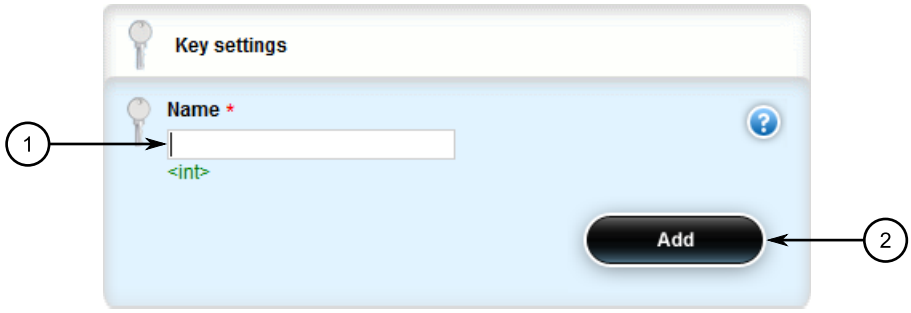


Figure 61: Key Settings Form

1. Name Box **2.** Add Button

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

Parameter	Description
Name	**Synopsis:** A 32-bit signed integer 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.

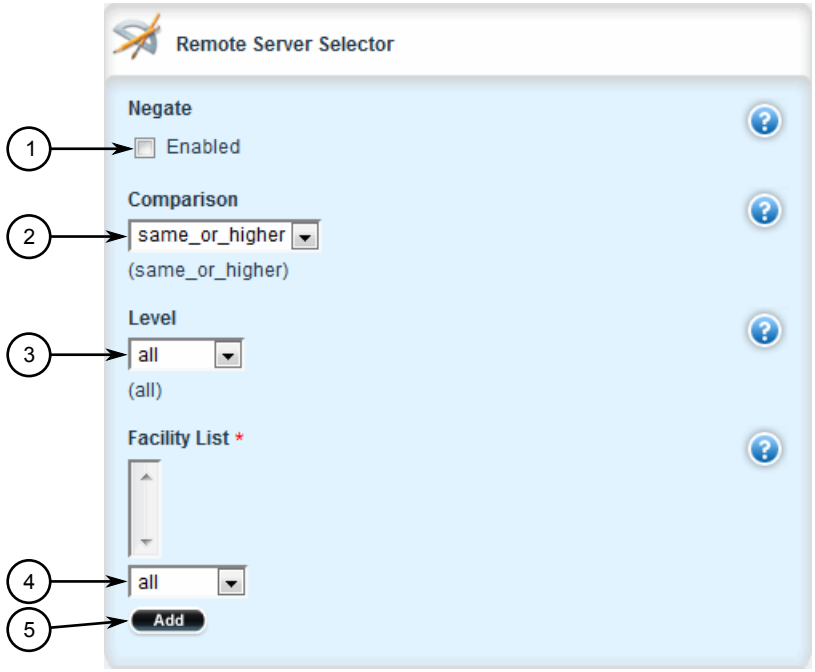


Figure 62: Remote Server Selector Form

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	Excludes messages defined in the *Remote Server Selector* fields from the log. Selecting this option acts as a logical NOT for the selector definition. For example: Selecting **same**, **debug**, and **mail** in the *Comparison*, *Level*, and *Facility-list* fields includes debug messages from the mail subsystem in the log. Selecting **Negate** *excludes* debug messages from the mail subsystem from the log.
Comparison	**Synopsis:** { same_or_higher, same } **Default:** same_or_higher The message severity levels to include in the log: • **same:** includes only messages of the severity level selected in the *Level* field. • **same_or_higher:** includes messages of the severity level selected in the *Level* field, and all messages of higher severity. For example: • Selecting **debug** in the *Level* field and **same** in the *Comparison* field includes only debug messages in the log. • Selecting **debug** in the *Level* field and **same_or_higher** in the *Comparison* field includes debug and all higher severity messages in the log.
Level	**Synopsis:** { emerg, alert, crit, err, warning, notice, info, debug, none, all } **Default:** all The base message severity level to include in the log. **all** includes all messages. **none** excludes all messages. Other levels are listed in order of increasing severity.
Facility List	**Synopsis:** { auth, authpriv, cron, daemon, ftp, kern, lpr, mail, news, security, syslog, user, uucp, local0, local1, local2, local3, local4, local5, local6, local7, all }

Parameter	Description
	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.

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 4.10.6.3
Deleting a Remote Server Selector

To delete 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. The **Remote Server Selector** table appears.

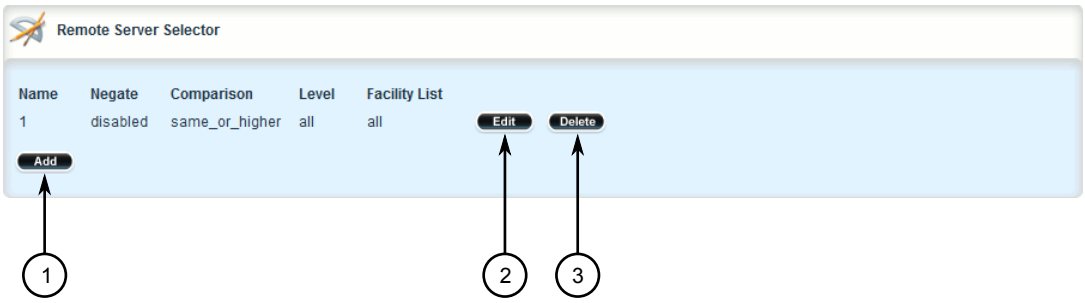


Figure 63: Remote Server Selector Table

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

3. 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 4.11
Managing the Software Configuration

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

CONTENTS

Section 4.11.1
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.

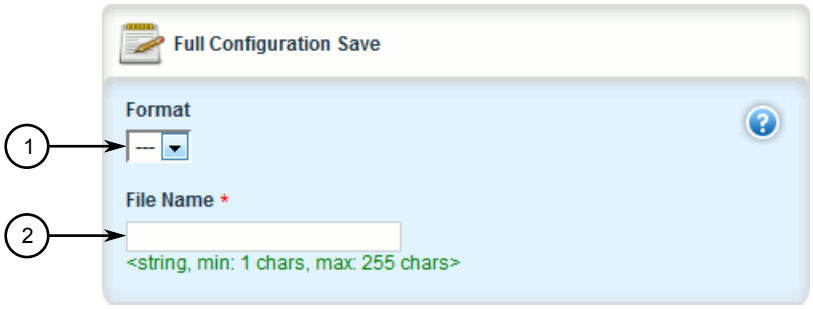


Figure 64: Full Configuration Save Form

1. Format List **2.** Filename Box

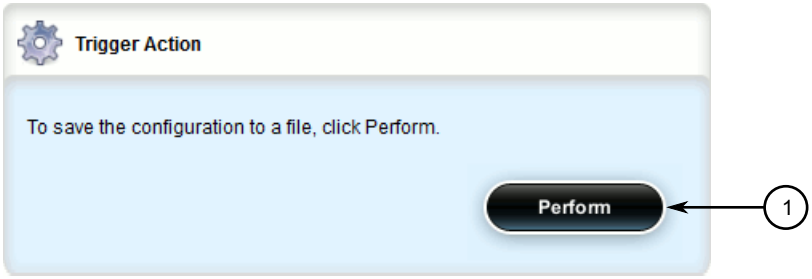


Figure 65: Trigger Action

1. Perform Button

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

Parameter	Description
format	**Synopsis:** { cli } Save full configuration to a file.
File Name	**Synopsis:** A string 1 to 255 characters long This parameter is mandatory.

3. On the **Trigger Action** form, click **Perform**.
4. [Optional] Backup the configuration file to a USB mass storage drive. For more information, refer to Section 4.9.4, “Backing Up Files”.

Section 4.11.2

Loading a Configuration

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

IMPORTANT!
RUGGEDCOM ROX II only accepts configuration files from devices with the same hardware profile running the same software version. It is recommended to only load configuration files from the same device.

1. [Optional] Install the configuration file on the device. For more information, refer to Section 4.9.3, "Installing Files".
2. Navigate to ***admin*** and click **full-configuration-load** in the menu. The **Load Full Configuration** and **Trigger Action** forms appear.

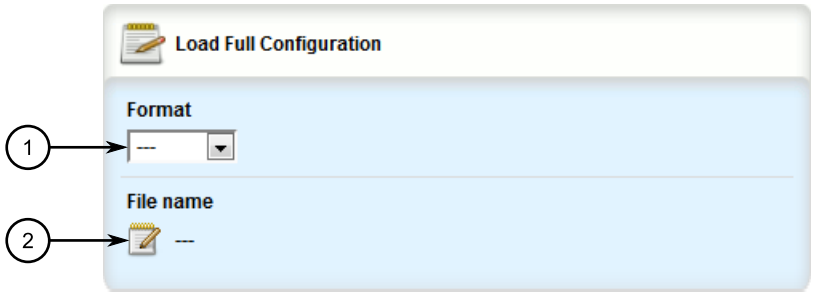


Figure 66: Load Full Configuration

1. Format List **2.** Filename Box

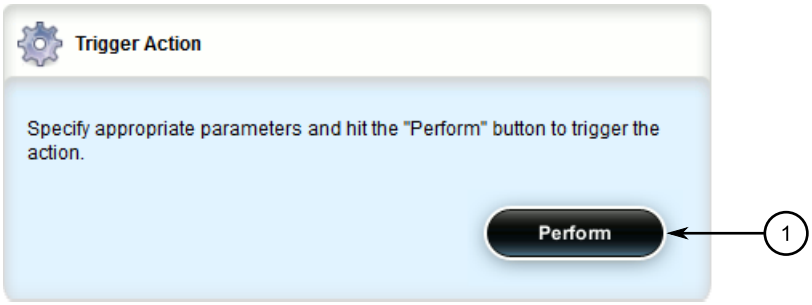


Figure 67: Trigger Action

1. Perform Button

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

Parameter	Description
format	**Synopsis:** { cli } Load a full configuration from a file
File Name	**Synopsis:** A string 1 to 255 characters long

Parameter	Description
	This parameter is mandatory.

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

Section 4.12
Upgrading/Downgrading the RUGGEDCOM ROX II Software

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

CONTENTS

Section 4.12.1
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 4.12.2, "Setting Up an Upgrade Server".

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

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

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

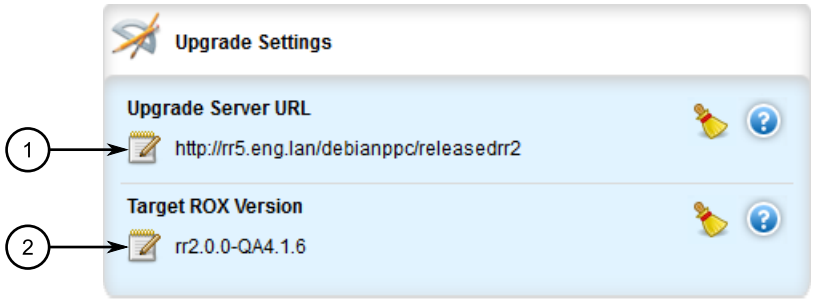


Figure 68: Upgrade Settings Form

1. Upgrade Server URL Box **2.** Target ROX Version Box

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

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

4. Add the server's SSH/RSA public key to RUGGEDCOM ROX II and add the server to the Known Hosts list. For more information, refer to Section 6.7.8.2, "Adding a Known Host".
5. Click **Exit Transaction** or continue making changes.

Section 4.12.2

Setting Up an Upgrade Server

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

The upgrade server must meet the following requirements:

- Each device that will be upgraded/downgraded must have access to a host that acts as a Web server or FTP server.
- The server must have sufficient disk space for at least two full software releases. Each full software release is approximately 75 MB, although most upgrades are typically much smaller.
- The server must have sufficient bandwidth. The bandwidth requirements will be based on the number of devices, the size of the upgrade, and when the devices launch an upgrade. The bandwidth is also limited by

default for each device to 500 kbps. A modest (e.g. 486 class machine) Web server should be able to serve files up to the limit of the network interface bandwidth.

- The server must be able to accept at least as many HTTP, HTTPS or FTP connections as there are devices on the network.
- The server must contain and publish a directory specifically for RUGGEDCOM ROX II software releases. The name of this directory will be specified in the upgrade settings for each device.
- Communication between the server and the device must be along a secure channel, such as IPsec.
- For upgrades via HTTPS, the server's public key must be signed by a trusted Certificate Authority (CA). A list of recognized CA's is available under `/etc/ssl/certs/`, 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 v2.12 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.

CONTENTS

Section 4.12.2.1
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,* ***2.12.1****.*

File Type	File Name	MIME Type
RUGGEDCOM ROX II Image Archive	imagerr2.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
GNU Privacy Guard (GPG)	imagerr2.x.y.tar.bz2.gpg	text/plain

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

- **Enable Double-Escaping**
  Double-escaping allows special double-encoded characters, such as +, % and &, in a URI. As some files in RUGGEDCOM ROX II upgrade/downgrade packages may contain a + sign in their file names, double-escaping

must be enabled for the upgrade server. If double-escaping is not enabled, some files will be un-retrievable and the upgrade will fail.

In the case of Microsoft's Internet Information Services (IIS) Manager, double-escaping is enabled by setting the **allowDoubleEscaping** attribute in `web.config` to `true`.

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

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

Section 4.12.2.2
Adding Software Releases to the Upgrade Server

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

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

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

   NOTE
   *Software release filenames take the form of **rrX.Y.Z.zip**, where **X** represents the major release number, **Y** represents the minor release number, and **Z** represents the patch release number.*
3. Extract the compressed ZIP file within the directory. The file will extract to a folder that has the same name as the major release (i.e. /rr2/dists/rr2.12.0). Subsequent releases will also be extracted to this folder (i.e. /rr2/dists/rr2.12.1).

Section 4.12.2.3
Adding Firmware Releases to the Upgrade Server

When configured, RUGGEDCOM ROX II can access the upgrade server to remotely upgrade firmware for the LTE modem. For more information, refer to Section 11.6.6, “Managing Firmware Updates”.

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

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

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

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

Section 4.12.3

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 4.12.4, "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 RX1500/RX1501/RX1510/RX1511/RX1512 Installation Guide*.
2. Make sure the source of the software upgrade has been configured. For more information, refer to Section 4.12.1, "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.

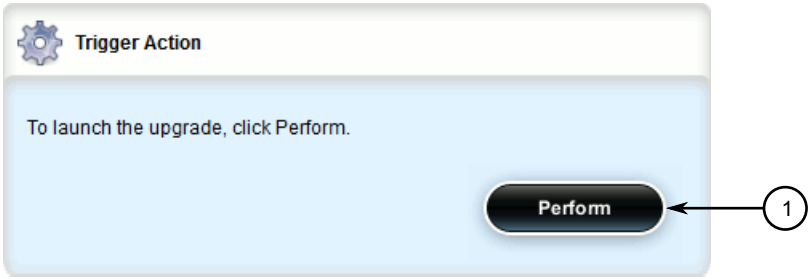


Figure 69: Trigger Action Form

1. Perform Button

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

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

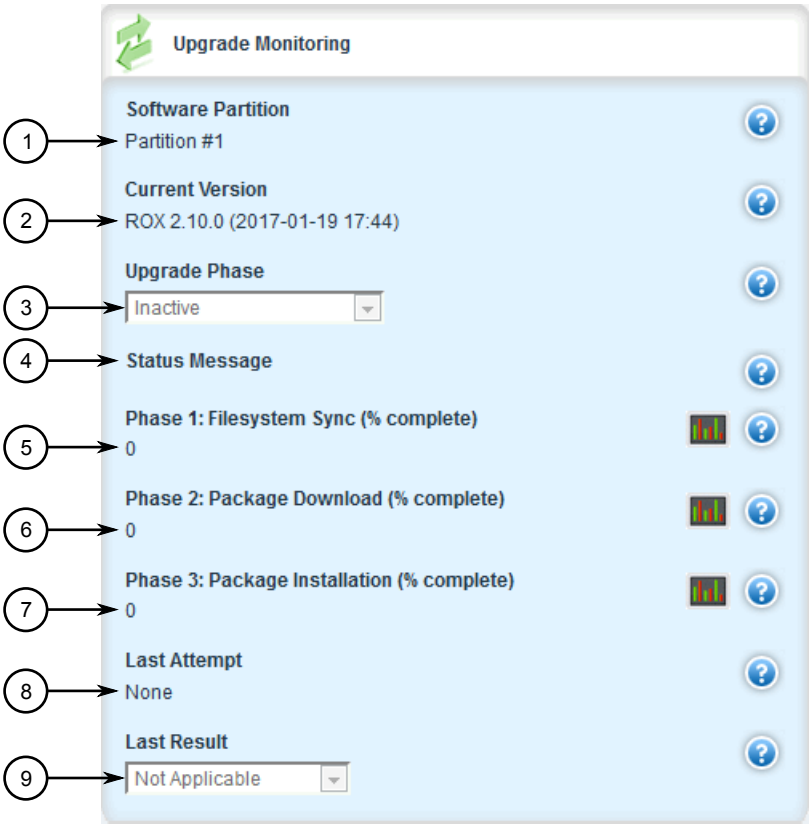


Figure 70: Upgrade Monitoring Form

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	**Synopsis:** A string 1 to 31 characters long The current active partition number. The unit has two software partitions: #1 and #2. Upgrades are always peformed to the other partition.
Current Version	**Synopsis:** A string 1 to 31 characters long The current operating software version. This parameter is mandatory.
Upgrade Phase	**Synopsis:** { Inactive, Estimating upgrade size, Copying filesystem, Downloading packages, Installing packages, Unknown state, Completed successfully, Failed, Uninstalling packages } 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. This parameter is mandatory.
Status Message	**Synopsis:** A string Additional details on the status of the upgrade. This parameter is mandatory.
Phase 1: Filesystem Sync (% complete)	**Synopsis:** A 32-bit signed integer between 0 and 100 Phase 1 of the upgrade involves synchronizing the filesystem with the partition you are upgrading to. This reflects the estimated percentage complete. This parameter is mandatory.
Phase 2: Package Download (% complete)	**Synopsis:** A 32-bit signed integer between 0 and 100 Phase 2 of the upgrade downloads all packages that require an update. This reflects the estimated percentage complete. This parameter is mandatory.
Phase 3: Package Installation (% complete)	**Synopsis:** A 32-bit signed integer between 0 and 100 Phase 3 of the upgrade installs all packages that require an update. This reflects the estimated percentage complete. This parameter is mandatory.
Last Attempt	**Synopsis:** A string 1 to 64 characters long The date and time of the completion of the last upgrade attempt. This parameter is mandatory.
Last Result	**Synopsis:** { Upgrade Successful, Upgrade Failed, Unknown, Reboot Pending, Not Applicable, Declined, Interrupted } Indicates whether or not the last upgrade was completed successfully This parameter is mandatory.

6. If the software upgrade is successful, reboot the device or decline the software upgrade. For more information about rebooting the device, refer to Section 4.5, “Rebooting the Device”.

Section 4.12.4

Stopping/Declining a Software Upgrade

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

IMPORTANT!
A software upgrade can only be declined before the device is rebooted. If the software upgrade has already been activated following a reboot, the previous software version installed on the other partition can be activated. For more information, refer to Section 4.12.5.1, "Rolling Back a Software Upgrade".

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

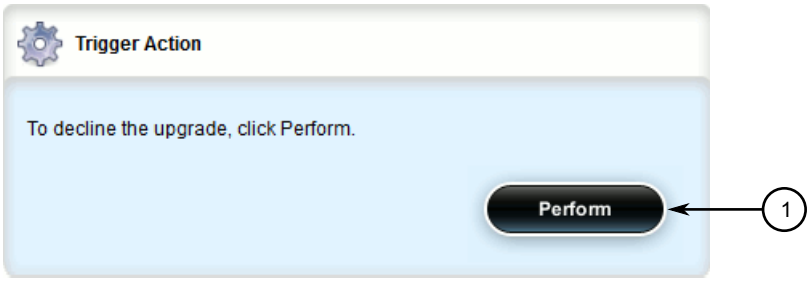


Figure 71: Trigger Action Form

1. Perform Button

2. Click **Perform**.

Section 4.12.5
Downgrading the RUGGEDCOM ROX II Software

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

CONTENTS

Section 4.12.5.1
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.

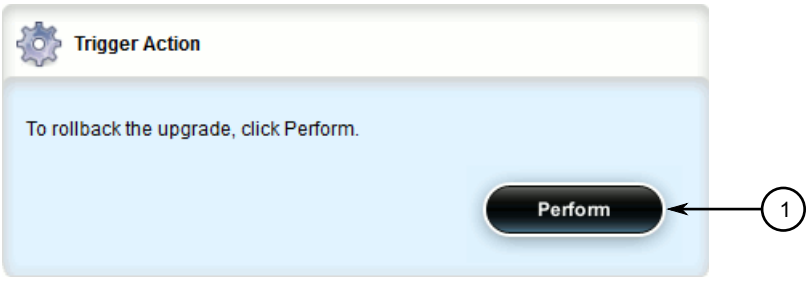


Figure 72: Trigger Action Form

1. Perform Button

2. 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 4.12.5.2

Downgrading Using ROXflash

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

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

IMPORTANT!
Use ROXflash only to install earlier versions of the RUGGEDCOM ROX II software. Newer software versions should be installed using the software upgrade functions. For more information about upgrading the RUGGEDCOM ROX II software, refer to Section 4.12.3, "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:

1. Contact Siemens Customer Support and obtain the required firmware version. Two tarball files (*.tar.bz2) are provided: the firmware image and a GPG (GNU Private Guard) signature file.
2. Add both files to the upgrade repository or place them on a USB Mass Storage drive.
3. 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 RX1500/RX1501/RX1510/RX1511/RX1512 Installation Guide*.
4. Navigate to ***admin » rox-imaging*** and click **roxflash** in the menu. The **ROXflash** and **Flash a ROXII image to the other partition** forms appear.

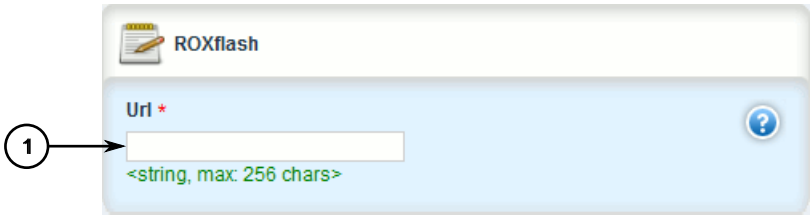


Figure 73: ROXflash Form

1. URL Box

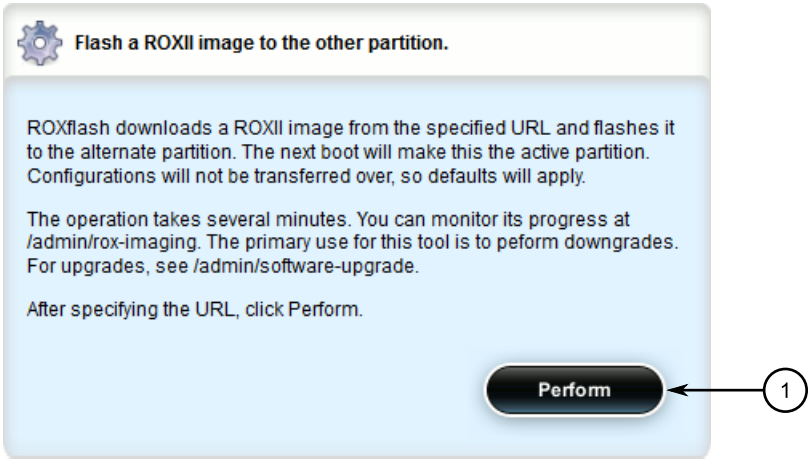


Figure 74: Flash a ROXII image to the other partition Form

1. Perform Button

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

IMPORTANT!
For downgrades via HTTPS (SSL), a custom or trusted Certificate Authority (CA) must be configured on the device. For more information, refer to Section 6.7.4.3, "Adding a CA Certificate and CRL".

Parameter	Description
url	**Synopsis:** A string 1 to 256 characters long The URL of the ROX II image to download. Supported URIs are HTTP, HTTPS, FTP, FTPS, SFTP, USB and SD. To flash from a USB flash drive or microSD card (if applicable), the URL format is "usb://device-name/path-to-file-on-system" or "sd://device-name/path-to-file-on-system". To determine the device name, insert your device and in the web ui, go to "chassis", "storage", "removable", OR, in the cli, type "show chassis". Note that only one single partition is supported for either data medium. 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". This parameter is mandatory.

6. 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.

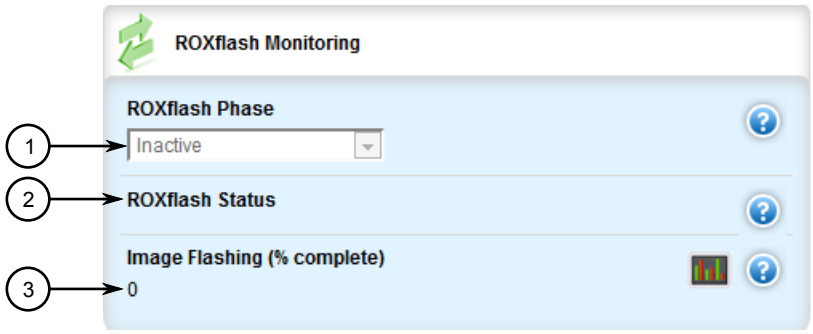


Figure 75: ROXflash Monitoring Form

1. ROXflash Phase List **2.** ROXflash Status **3.** Image Flashing

This form contains the following parameters:

Parameter	Description
ROXflash Phase	**Synopsis:** { 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. This parameter is mandatory.
ROXflash Status	**Synopsis:** A string 1 to 1024 characters long Detailed messages about ROXflash progress or errors. This parameter is mandatory.
Image Flashing (% complete)	**Synopsis:** A 32-bit signed integer between 0 and 100 Indicates the imaging progress and the percentage that is complete. This parameter is mandatory.

7. If the software is successfully downgraded, reboot the device. For more information about rebooting the device, refer to Section 4.5, “Rebooting the Device”.

Section 4.13

Monitoring Firmware Integrity

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

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

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

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

CAUTION!
Security hazard – risk of unauthorized access and/or exploitation. For the firmware integrity check to be meaningful, appropriate care must be taken to protect the device. Make sure physical access to the device is restricted to authorized personnel only and that administrator login credentials are kept secure.

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

CONTENTS

Section 4.13.1

Enabling/Disabling the Boot Time Firmware Integrity

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

To enable or disable this feature, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **admin**. The **Boot Time Firmware Integrity Check** form appears.

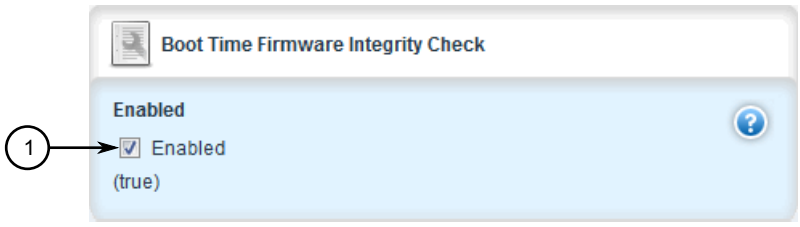


Figure 76: Boot Time Firmware Integrity Check Form

1. Enabled Check Box

3. Select **Enabled** to enable the boot time integrity check, or clear the check box to disable the feature.
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 4.13.2
Checking the Firmware Integrity

To check the firmware integrity manually, do the following:

1. Navigate to **admin** and then click **check-integrity**. The **Trigger Action** form appears.

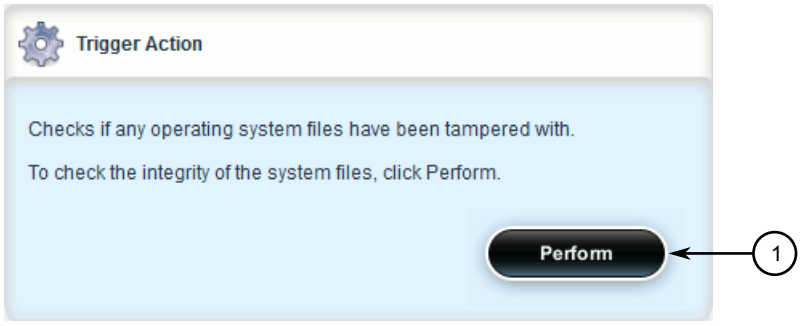


Figure 77: Trigger Action Form

1. Perform Button

2. Click **Perform** and allow a few seconds for the integrity check to complete. If no unauthorized/unexpected modifications were detected, the message **Success** is displayed.

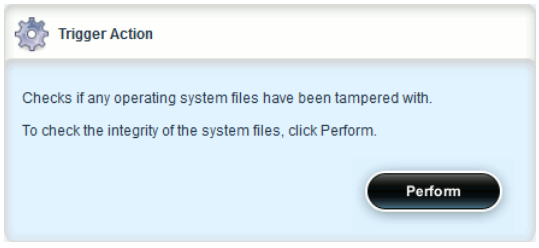


Figure 78: Trigger Action Form

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

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

Section 4.13.3

Scheduling a Recurring Firmware Integrity Check

Using the RUGGEDCOM ROX II scheduler, the firmware integrity check can be scheduled to run automatically at a specific time and date, either once or on a recurring schedule. For more information about scheduling the firmware integrity check, refer to Section 5.10, "Scheduling Jobs".

Section 4.13.4

Viewing the Status of the Firmware Integrity Check

To view the status of the last firmware integrity check, navigate to **chassis**. The results of the last integrity check are detailed on the **Chassis Status** form.

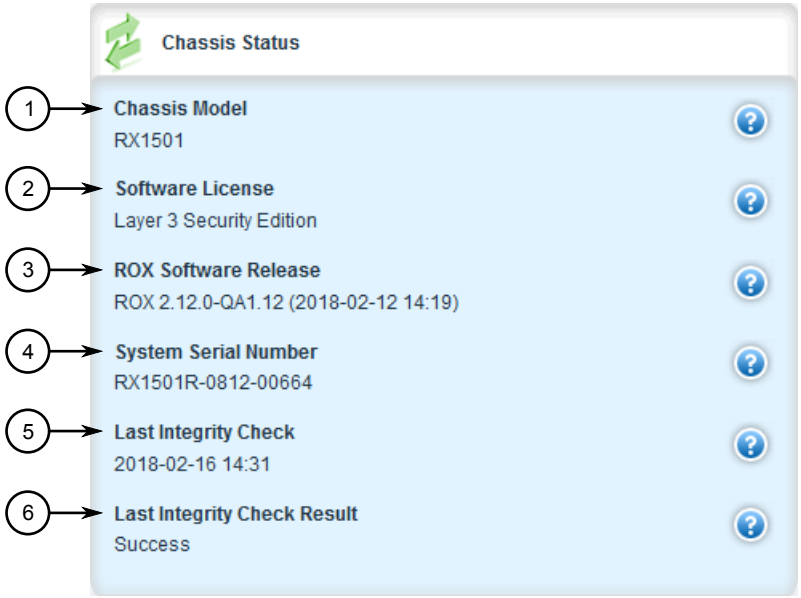


Figure 79: Chassis Status

1. Chassis Model **2.** Software License **3.** System Serial Number **4.** Last Integrity Check **5.** Last Integrity Check Result

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

```
Success
```

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

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

Section 4.14
Managing Fixed Modules

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

CONTENTS

Section 4.14.1
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.

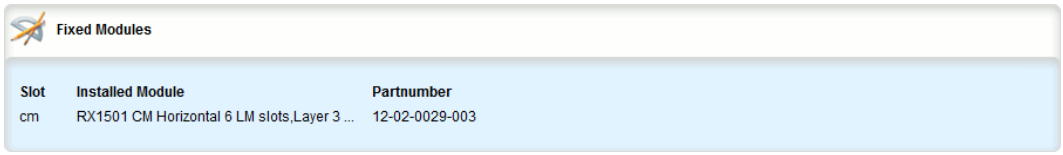


Figure 80: Fixed Modules Table

If no fixed modules have been configured, add fixed module configurations as needed. For more information, refer to Section 4.14.2, "Adding a Fixed Module Configuration".

Section 4.14.2
Adding a Fixed Module Configuration

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

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

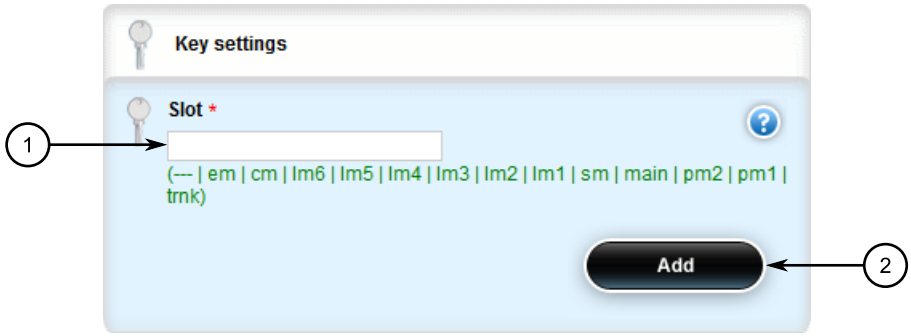


Figure 81: Key Settings Form

1. Slot Box **2.** Add Button

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

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

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

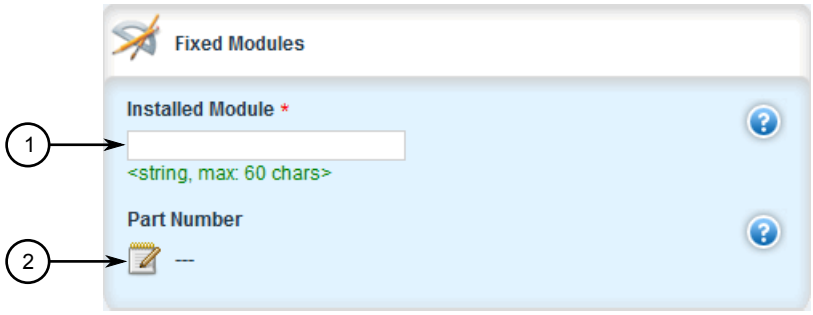


Figure 82: Fixed Modules Form

1. Installed Module Box **2.** Part Number Box

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

Parameter	Description
Installed Module	**Synopsis:** A string 1 to 60 characters long The module type to be used in this slot. This parameter is mandatory.
Part Number	**Synopsis:** A string 1 to 74 characters long The part number of the module type in this slot.

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 4.14.3
Deleting a Fixed Module Configuration

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

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

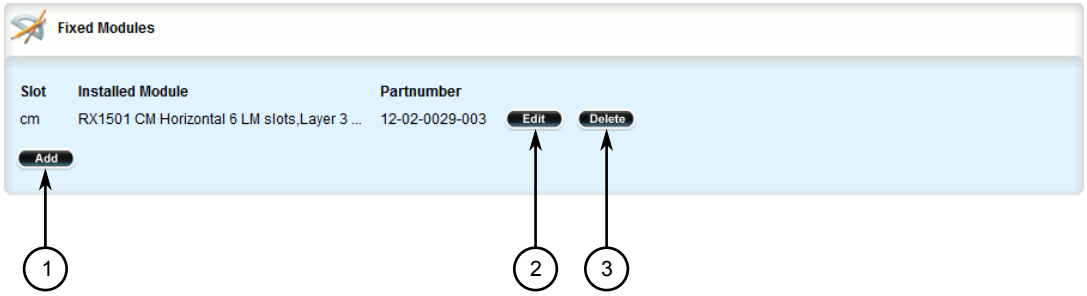


Figure 83: Fixed Modules Table

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

3. Click **Delete** next to the chosen fixed module 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 4.15
Managing Line Modules

RUGGEDCOM RX1500 series devices feature slots for field-replaceable line modules, which can be used to expand and customize the capabilities of the device to suit specific applications. A variety of modules are available, each featuring a specific type of communication port. For information about available line modules, refer to the *Modules Catalog* for the device family.

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

CONTENTS

Section 4.15.1
Removing a Line Module

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

1. Shut down the device. The device will shutdown for a period of time before rebooting and restarting. The default time-out period is 300 seconds (five minutes). If more time is required to complete the procedure, disconnect power from the device during the time-out period. For more information on how to shutdown the device, refer to Section 4.4, "Shutting Down the Device".
2. Remove the line module from the device.

Section 4.15.2
Installing a New Line Module

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

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

1. If equipped, remove the line module currently installed in the slot. For more information, refer to Section 4.15.1, "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.

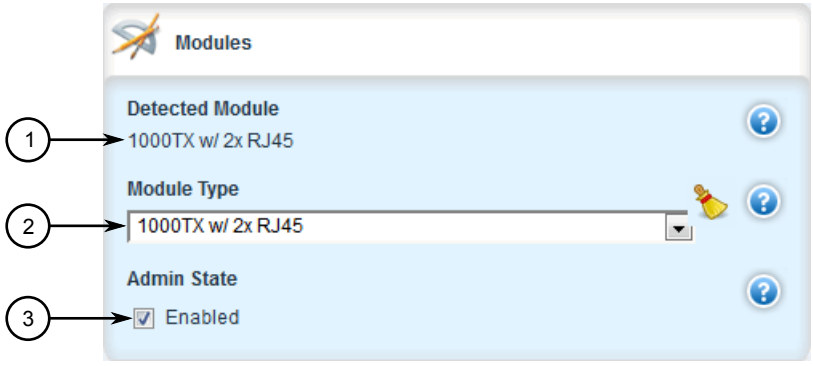


Figure 84: Modules Form

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

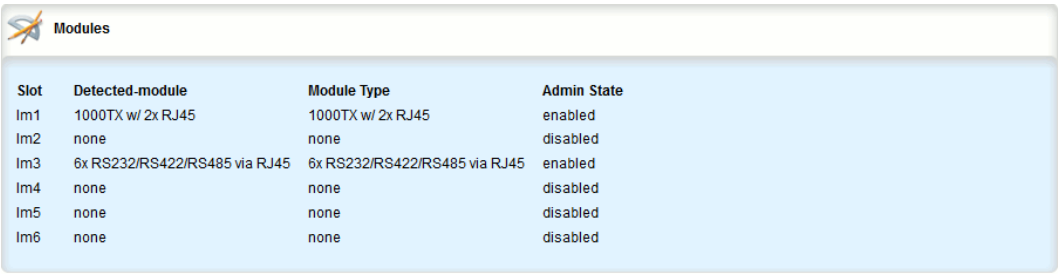
4. Under **Module Type**, select **none** from the list. This allows RUGGEDCOM ROX II to automatically detect the new module during the next startup.
5. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
6. Click **Exit Transaction** or continue making changes.
7. Insert the new line module into the empty slot in the chassis.
8. Reboot the device. For more information, refer to Section 4.5, "Rebooting the Device".

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

9. 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 4.15.4, "Configuring a Line Module".

Section 4.15.3
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.



Modules

Slot	Detected-module	Module Type	Admin State
lm1	1000TX w/ 2x RJ45	1000TX w/ 2x RJ45	enabled
lm2	none	none	disabled
lm3	6x RS232/RS422/RS485 via RJ45	6x RS232/RS422/RS485 via RJ45	enabled
lm4	none	none	disabled
lm5	none	none	disabled
lm6	none	none	disabled

Figure 85: Modules Table

If no line modules have been configured, install line module as needed. For more information, refer to Section 4.15.2, "Installing a New Line Module".

Section 4.15.4
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.

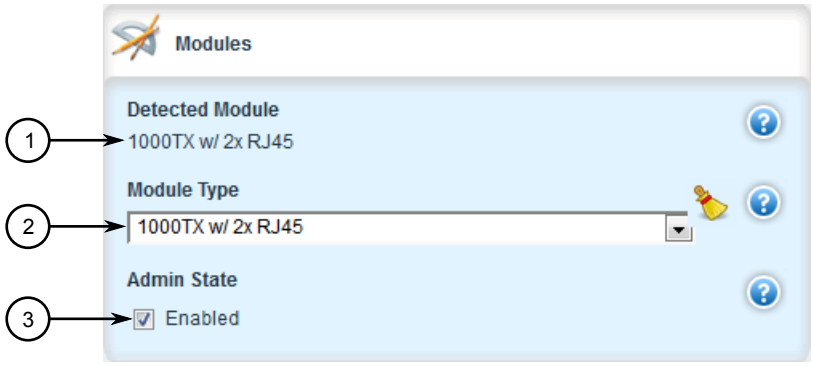


Figure 86: Modules Form

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

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

Parameter	Description
slot	**Synopsis:** { sm, lm1, lm2, lm3, lm4, lm5, lm6, swport, eth, serport, celport, wlanport } The slot name, as marked on the silkscreen across the top of the chassis.
Detected Module	**Synopsis:** A string 1 to 60 characters long The installed module's type specifier. This parameter is mandatory.
Module Type	**Synopsis:** A string Sets the module type to be used in this slot.
Admin State	Sets the administrative state for a module. Enabling the module powers it on.

4. 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.*

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

Section 4.15.5

Enabling/Disabling Controlled Bypass for M12 Line Modules

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

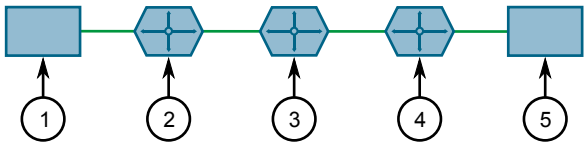


Figure 87: Sample Controlled Bypass Diagram

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

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

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

1. Log in to the defective router.
2. Change the mode to **Edit Private** or **Edit Exclusive**.
3. Navigate to ***chassis » line-modules » {module} » bypass***, where *{module}* is the M12 line module. The **Bypass Control and Status** form appears.

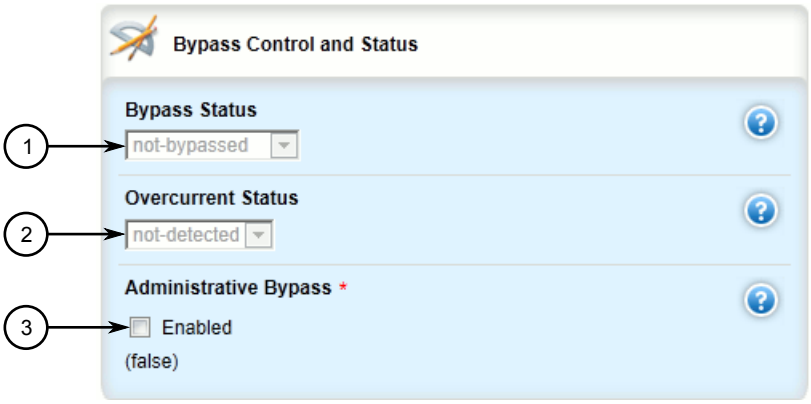


Figure 88: Bypass Control and Status Form

1. Bypass Status List **2.** Overcurrent Status List **3.** Administrative Bypass Check Box

NOTE
*The default status is **not bypassed**.*

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

4. Select the **Administrative Bypass** check box to enable controlled bypass, or clear the check box to disable it.
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.

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

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

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

Section 4.16
Managing SFP Transceivers

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

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

CONTENTS

Section 4.16.1
SFP Transceiver Support

RUGGEDCOM ROX II offers the following support for SFP transceivers.

Hot Swappable

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

Automatic Detection

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

Smart SFP For Select Transceivers

Smart SFP mode is available for any port on the RUGGEDCOM RX1500PN LM FG50 line module. This mode is enabled by default.

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

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

For information about disabling (or enabling) Smart SFP mode, refer to Section 4.16.3, "Enabling/Disabling Smart SFP Mode".

Section 4.16.2
Viewing SFP Information

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

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

```
ID: Unknown FF
```

1. Navigate to ***interfaces » switch » {module}***, where *module* is the slot name and port number for the SFP transceiver port.
2. Click **sfp**. The **Trigger Action** form appears.

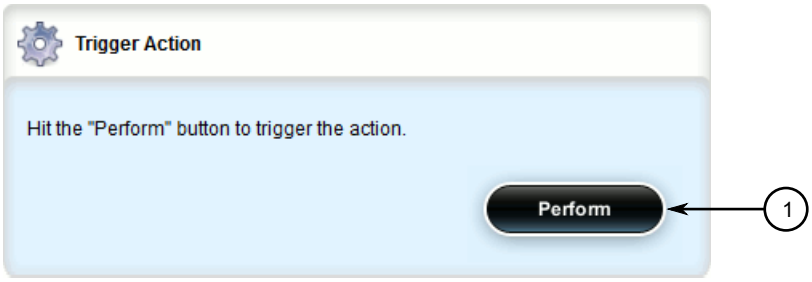


Figure 89: Trigger Action Form

1. Perform Button

3. Click the **Perform** button. The **SFP Information** form appears detailing the technical specifications of the selected transceiver.

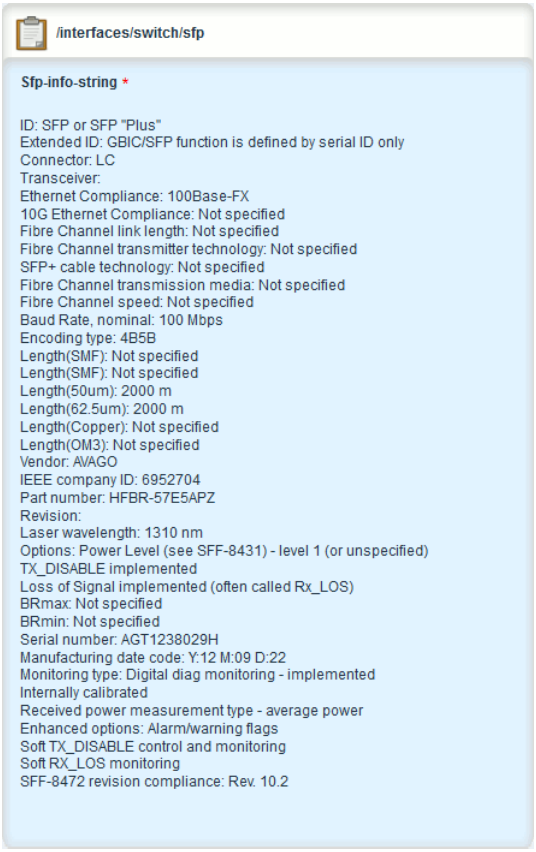


Figure 90: SFP Information Form

Section 4.16.3

Enabling/Disabling Smart SFP Mode

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

NOTE
Smart SFP mode is only available for any port on the RUGGEDCOM RX1500PN LM FG50 line module.

NOTE
To determine if an SFP transceiver has been marked as ***Unidentified****, refer to the* `Media` *parameter on the* ***Switched Ethernet Port Status*** *form associated with the port. For more information, refer to Section 8.1.4, "Viewing the Status of a Switched Ethernet Port". The parameter will display the following if the SFP transceiver is marked as* ***Unidentified****:*

```
SFP - Unidentified
```

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

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

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

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

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to ***interface » switch » {interface}***, where *{interface}* is the switched Ethernet port. The **Small Form Factor Pluggable Ports** form appears.

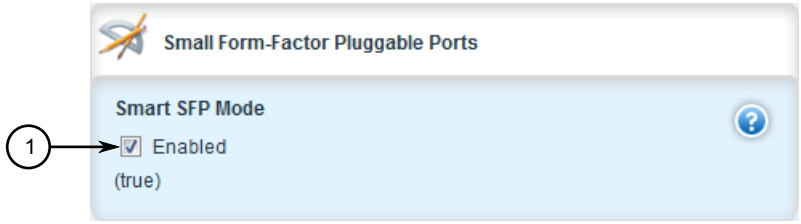


Figure 91: Small Form Factor Pluggable Ports Form

1. Smart SFP Mode Check Box

3. Select **Smart SFP Mode** to enable Smart SFP mode, or clear the check box to disable the feature.
4. If Smart SFP mode is disabled, review the configuration for the SFP transceiver socket. Some settings may need to be adjusted manually to suit the capabilities of the installed SFP transceiver. For more information, refer to Section 8.1.2, "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 4.17

Managing Routable Ethernet Ports

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

CONTENTS

Section 4.17.1
Viewing a List of Routable Ethernet Ports

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

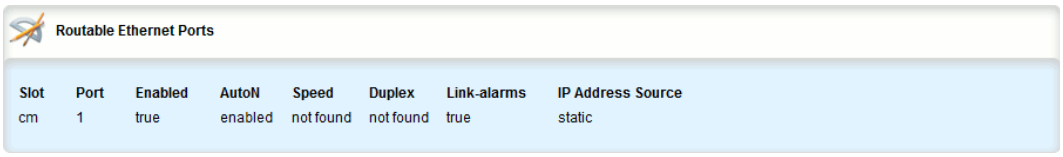


Figure 92: Routable Ethernet Ports Table

Section 4.17.2
Configuring a Routable Ethernet Port

To configure a routable 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.

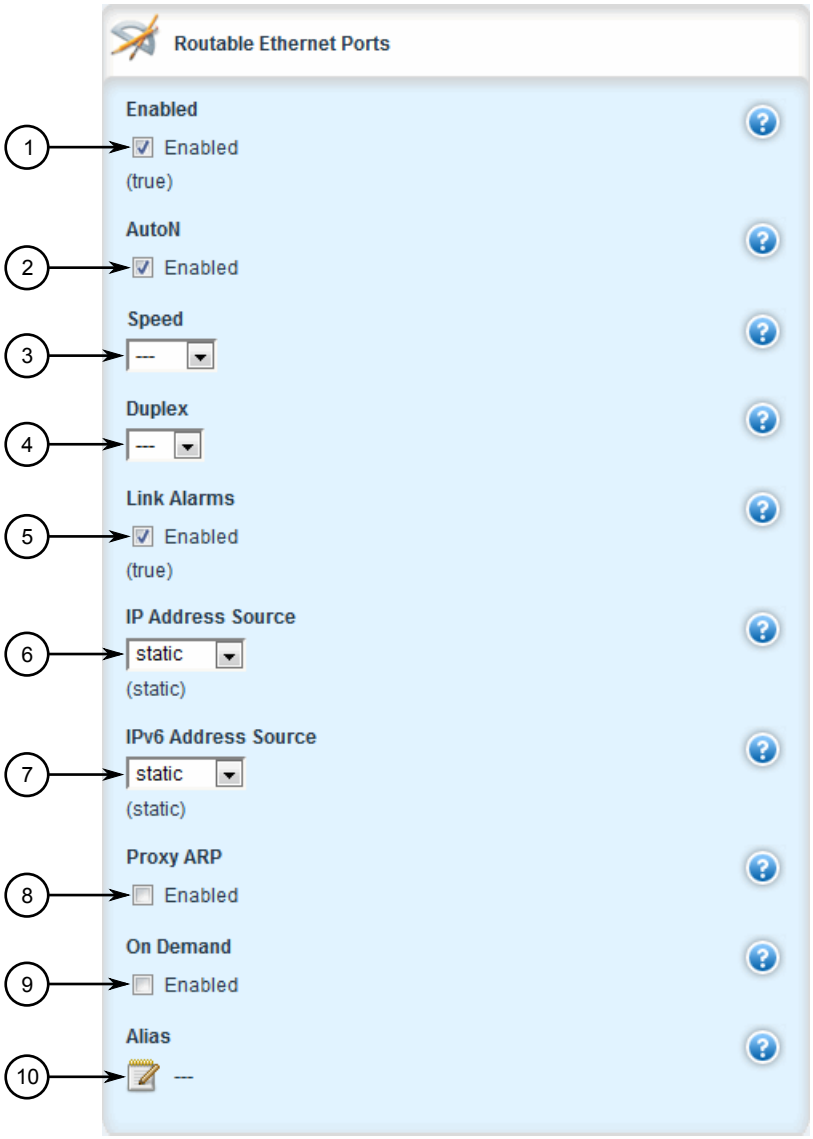


Figure 93: Routable Ethernet Ports Form

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.** IPv6 Address Source List **8.** ProxyARP Check Box **9.** On-Demand Check Box **10.** Alias Box

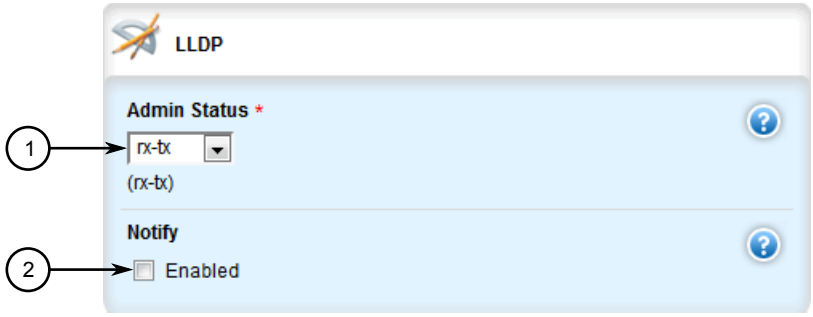


Figure 94: LLDP Form

1. Admin Status List **2.** Notify Check Box

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

Parameter	Description
Slot	**Synopsis:** { { cm, em }{ sm, lm1, lm2, lm3, lm4, lm5, lm6, swport, eth, serport, celport, wlanport } } The name of the module location provided on the silkscreen across the top of the device.
Port	**Synopsis:** A 32-bit signed integer between 1 and 16 The port number as seen on the front plate silkscreen of the switch (or a list of ports, if aggregated in a port trunk).
Enabled	**Synopsis:** { true, false } **Default:** true Enables/Disables the network communications on this port.
AutoN	Enables or disables IEEE 802.3 auto-negotiation. Enabling auto-negotiation results in speed and duplex being negotiated upon link detection; both end devices must be auto-negotiation compliant for the best possible results.
Speed	**Synopsis:** { 10, 100, 1000 } Speed (in Megabit-per-second or Gigabit-per-second). If auto-negotiation is enabled, this is the speed capability advertised by the auto-negotiation process. If auto-negotiation is disabled, the port is explicitly forced to this speed mode. AUTO means advertise all supported speed modes.
Duplex	**Synopsis:** { half, full } If auto-negotiation is enabled, this is the duplex capability advertised by the auto-negotiation process. If auto-negotiation is disabled, the port is explicitly forced to this duplex mode. AUTO means advertise all supported duplex modes.
Link Alarms	**Synopsis:** { true, false } **Default:** true Disabling link-alarms will prevent alarms and LinkUp and LinkDown SNMP traps from being sent for that interface. Link alarms may also be controlled for the whole system under admin / alarm-cfg.
IP Address Source	**Synopsis:** { static, dynamic } **Default:** static Determines whether the IP address is static or dynamically assigned via DHCP or BOOTP. The DYNAMIC option is a common case of a dynamically assigned IP address. It switches between BOOTP and DHCP until it gets the response from the relevant server. It must be static for non-management interfaces.
IPv6 Address Source	**Synopsis:** { static, dynamic }

Parameter	Description
	Default: static Determines whether the IPv6 address is static or dynamically assigned via DHCPv6. The DYNAMIC option is a common case of a dynamically assigned IPv6 address. This must be static for non-management interfaces.
Proxy ARP	Enables/Disables whether the port will respond to ARP requests for hosts other than itself.
On Demand	This interface is up or down on demand of link fail over.
Alias	**Synopsis:** A string 1 to 64 characters long The SNMP alias name of the interface
Admin Status	**Synopsis:** { tx-only, rx-only, rx-tx, no-lldp } **Default:** rx-tx • no-lldp : The local LLDP agent can neither transmit nor receive LLDP frames. • rxTx : The local LLDP agent can both transmit and receive LLDP frames through the port. • txOnly : The local LLDP agent can only transmit LLDP frames. • rxOnly : The local LLDP agent can only receive LLDP frames.
Notify	Disabling notifications will prevent sending notifications and generating alarms for a particular interface from the LLDP agent.

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

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

5. Add a VLAN ID (VID) for the port. For more information, refer to Section 4.17.3.2, "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 4.17.3
Managing VLANs for Routable Ethernet Ports

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

CONTENTS

- Section 4.17.3.3, "Deleting a VLAN for a Routable Ethernet Port"

Section 4.17.3.1
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.

Figure 95: 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 4.17.3.2, "Adding a VLAN to a Routable Ethernet Port".

Section 4.17.3.2
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.

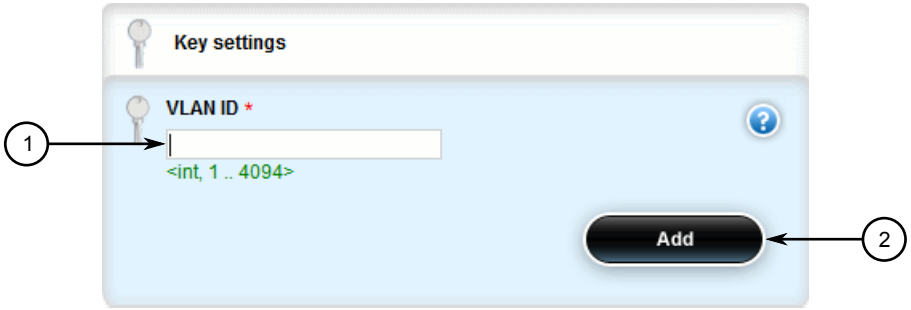


Figure 96: Key Settings Form

1. VLAN ID Box **2.** Add Button

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

Parameter	Description
VLAN ID	**Synopsis:** A 32-bit signed integer between 1 and 4094

Parameter	Description
	The VLAN ID for this routable logical interface.

5. Click **Add** to create the new VLAN. The **VLANs** form appears.

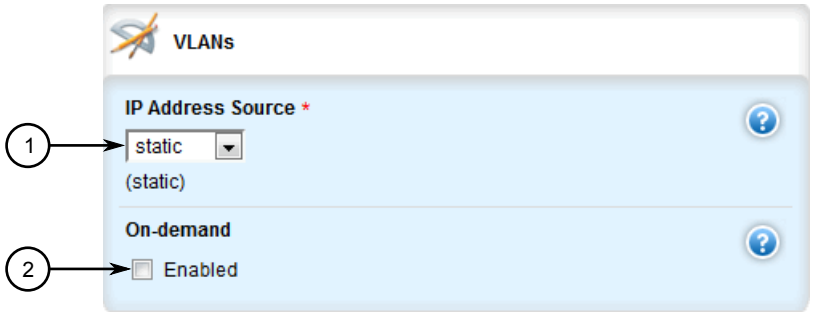


Figure 97: VLANs Form

1. IP Address Source Box **2.** On-Demand Check Box

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

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

7. Add a QoS map for the VLAN. For more information, refer to Section 16.2.7.2, "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 4.17.3.3
Deleting a VLAN for a Routable Ethernet Port

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

1. 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.

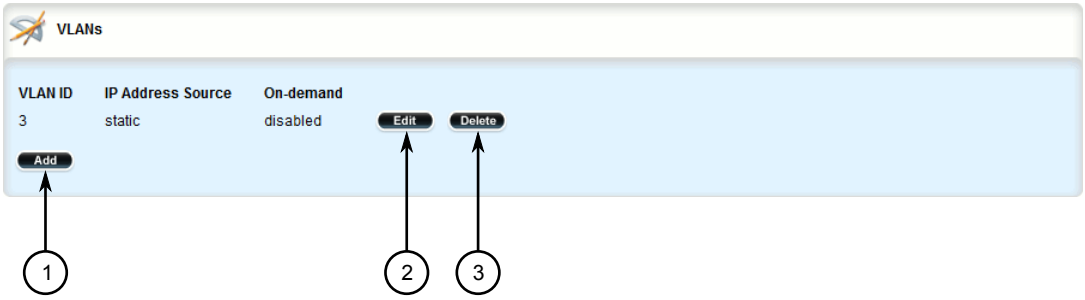


Figure 98: VLANs Table

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.

5 System Administration

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

CONTENTS

Section 5.1

Configuring the System Name and Location

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.

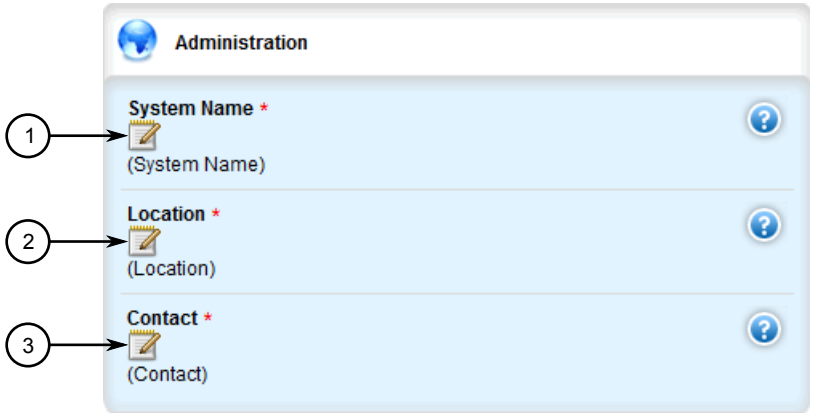


Figure 99: Administration Form

1. System Name Box **2.** Location Box **3.** Contact Box

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

Parameter	Description
System Name	**Synopsis:** A string 1 to 255 characters long **Default:** System Name An administratively-assigned name for this managed node. By convention, this is the node's fully-qualified domain name. If the name is unknown, the value is the zero-length string.
Location	**Synopsis:** A string 1 to 255 characters long **Default:** Location The physical location of this node (e.g., 'telephone closet, 3rd floor'). If the location is unknown, the value is the zero-length string.
Contact	**Synopsis:** A string 1 to 255 characters long **Default:** Contact The textual identification of the contact person for this managed node, together with information on how to contact this person. If no contact information is known, the value is the zero-length string.

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 5.2

Configuring the Host Name

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

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to ***admin***. The **Hostname** form appears.

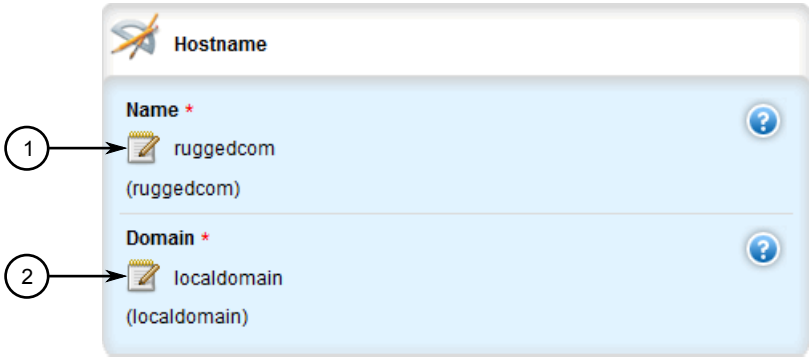


Figure 100: Hostname Form

1. Name Box **2.** Domain Box

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

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

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

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

Customizing the Welcome Screen

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

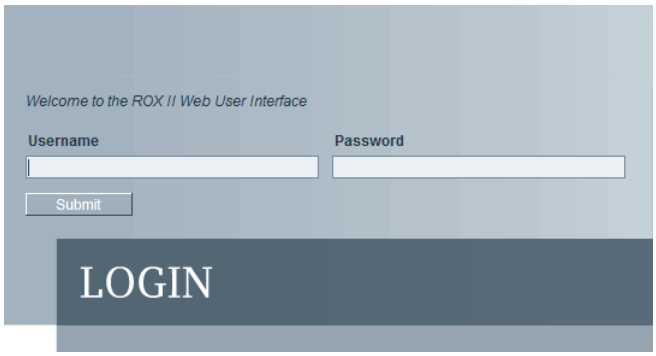


Figure 101: A Customized Welcome Screen

To add a welcome message, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to ***admin » authentication***. The **Authentication** form appears.

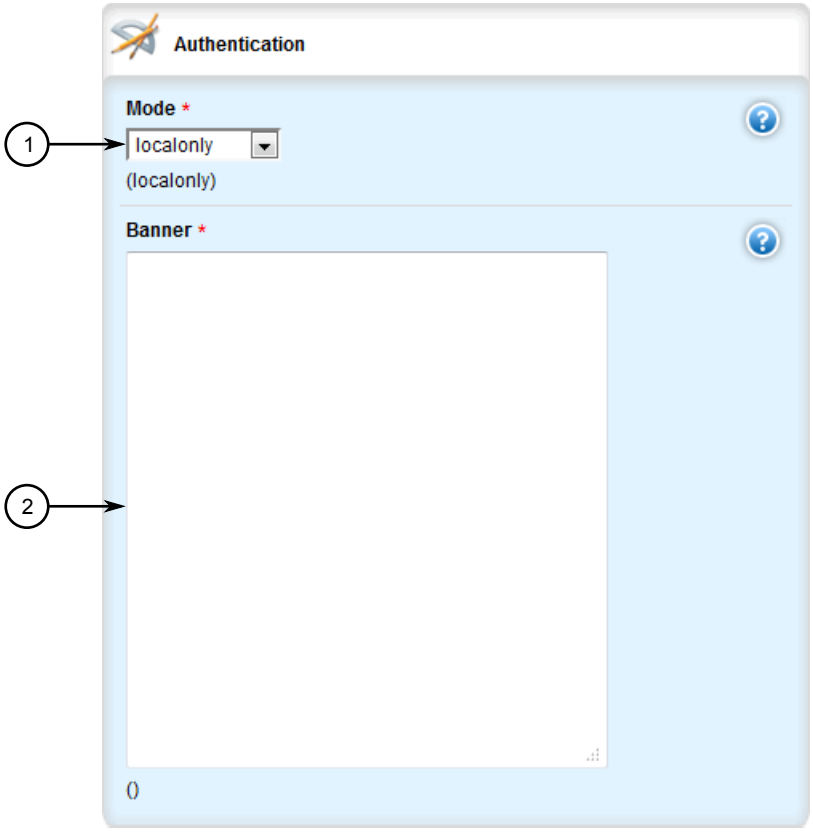


Figure 102: Authentication Form

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 5.4
Setting the Maximum Number of Sessions

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

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to ***admin***. The **Session Limits** form appears.

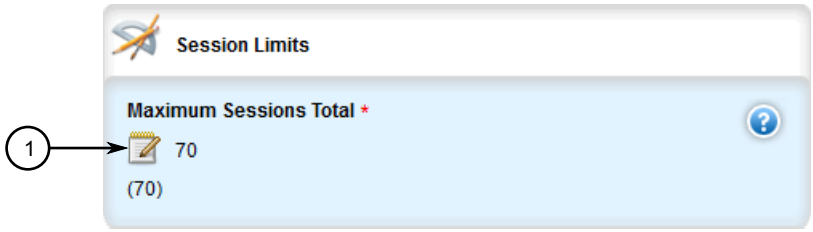


Figure 103: Session Limits Form

1. Maximum Sessions Total Box

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

Parameter	Description
Maximum Sessions Total	**Synopsis:** a 32-bit unsigned integer **Default:** 70 Puts a limit on the total number of concurrent sessions to ROX.

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 5.5
Enabling and Configuring WWW Interface Sessions

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

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to ***admin***. The **WWW Interface Sessions** form appears.

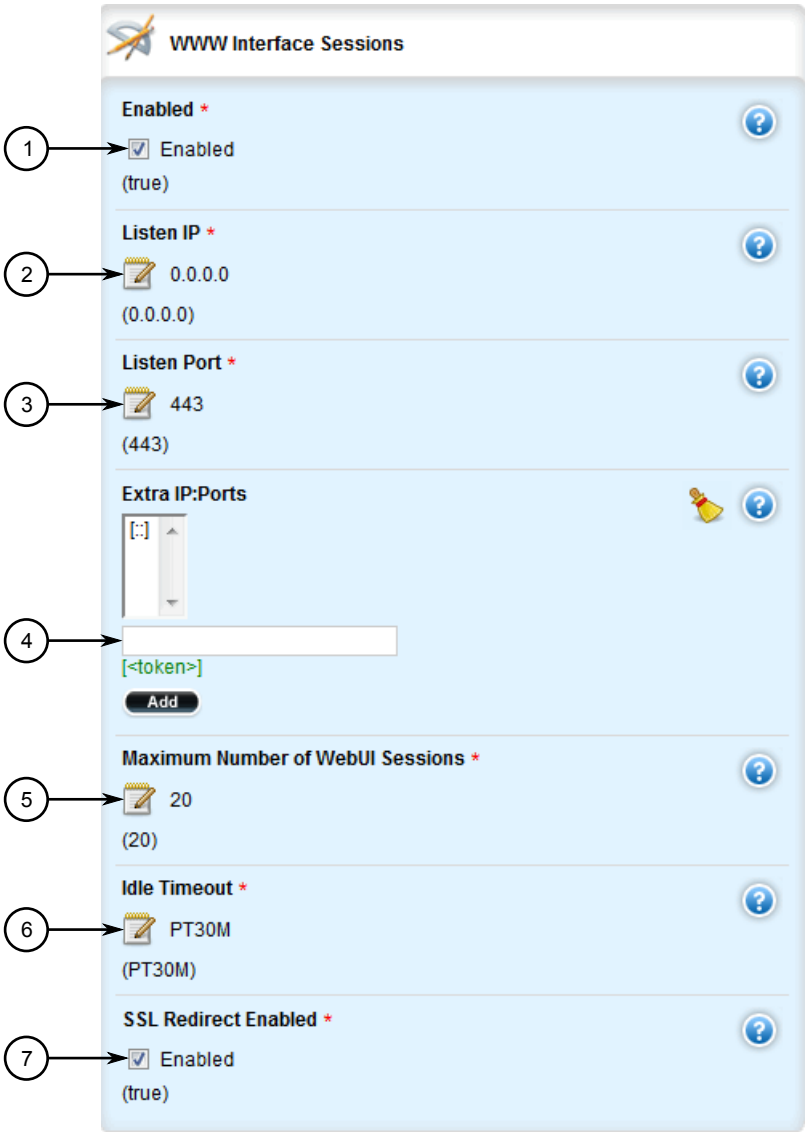


Figure 104: WWW Interface Sessions

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	**Synopsis:** { true, false } **Default:** true Provides the ability to configure WebUI features on the device.
Listen IP	**Synopsis:** A string **Default:** 0.0.0.0 The IP Address the CLI will listen on for WebUI requests.
Listen Port	**Synopsis:** A 16-bit unsigned integer between 0 and 65535

Parameter	Description
	Default: 443 The port on which the WebUI listens for WebUI requests.
Extra IP:Ports	**Synopsis:** A string The WebUI will also listen on these IP Addresses. For port values, add ':#' to set non-default port value. (ie. xxx.xxx.xxx.xxx:19343 [::] [::]:16000). If using the default address, do not specify another listen address with the same port.
Maximum Number of WebUI Sessions	**Synopsis:** a 32-bit unsigned integer **Default:** 20 The maximum number of concurrent WebUI sessions
Idle Timeout	**Synopsis:** A string **Default:** PT30M The maximum idle time before terminating a WebUI session. If the session is waiting for notifications, or has a pending confirmed commit, the idle timeout is not used. A value of 0 means no timeout. PT30M means 30 minutes.
SSL Redirect Enabled	**Synopsis:** { true, false } **Default:** true Redirects traffic from port 80 to port 443. If disabled, port 80 will be closed.
Client Certificate Verification	**Synopsis:** { none, peer, fail-if-no-peer-cert } **Default:** none Level of verification the server does on client certificates • none - It does not do any verification. • peer - The server will ask the client for a client-certificate but not fail if the client does not supply a client-certificate. • fail-if-no-peer-cert - The server requires the client to supply a client certificate.

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 5.6

Enabling/Disabling Remote Access Through a VRF Interface

A VRF interface can be used to remotely access the CLI and Web interface, or as an interface for SNMP. This capability is available on a per-interface basis and is disabled by default.

IMPORTANT!
This feature does not support some services. Note the following restrictions:

- *DHCP is not supported. As such, the VRF interface must not derive its IP address from an DHCP server.*
- *HTTP redirects to HTTPS are not supported. As such, HTTPS must be entered explicitly when accessing the Web user interface via a browser (e.g. https://x.x.x.x).*
- *HTTP is not supported on SNMP connections.*

To enable or disable this function on a VRF instance, do the following:

1. Make sure at least one VRF instance has been configured. For information about configuring a VRF instance, refer to Section 13.11.3, "Configuring VRF".
2. Change the mode to **Edit Private** or **Edit Exclusive**.
3. Navigate to ***global » vrf***. The **VRF Definition List Configuration** table appears.

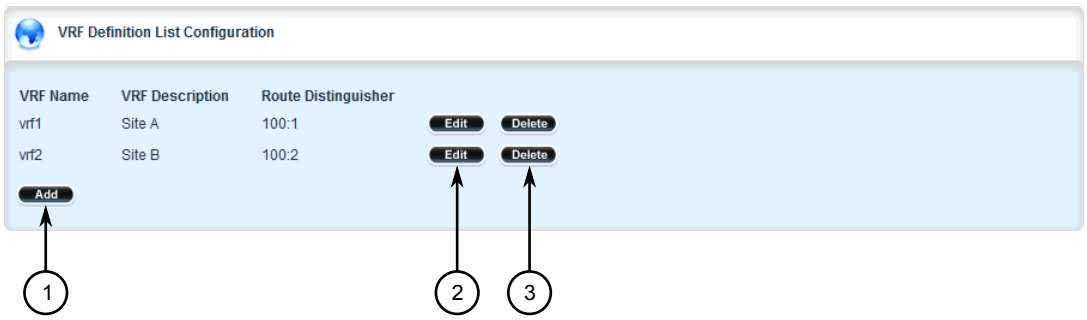


Figure 105: VRF Definition List Configuration Table

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

4. Click **Edit** next to the desired VRF definition. The **Remote Admin Sessions Through VRF** form appears.

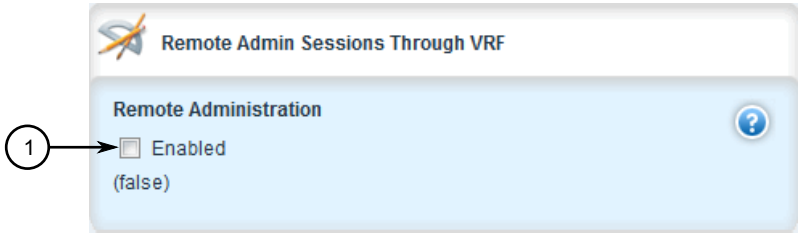


Figure 106: Remote Admin Sessions Through VRF Form

1. Remote Administration Check Box

5. Select **Remote Administration** to enable the feature, or clear the check box to disable the feature.

   If the feature is enabled, additional options are available.

> **NOTE**
> *The parameters* `SNMP Administration` *and* `SNMP Listen Port` *are only available when SNMP sessions are enabled. For information about how to enable SNMP sessions, refer to Section 15.2.2, "Enabling and Configuring SNMP Sessions".*

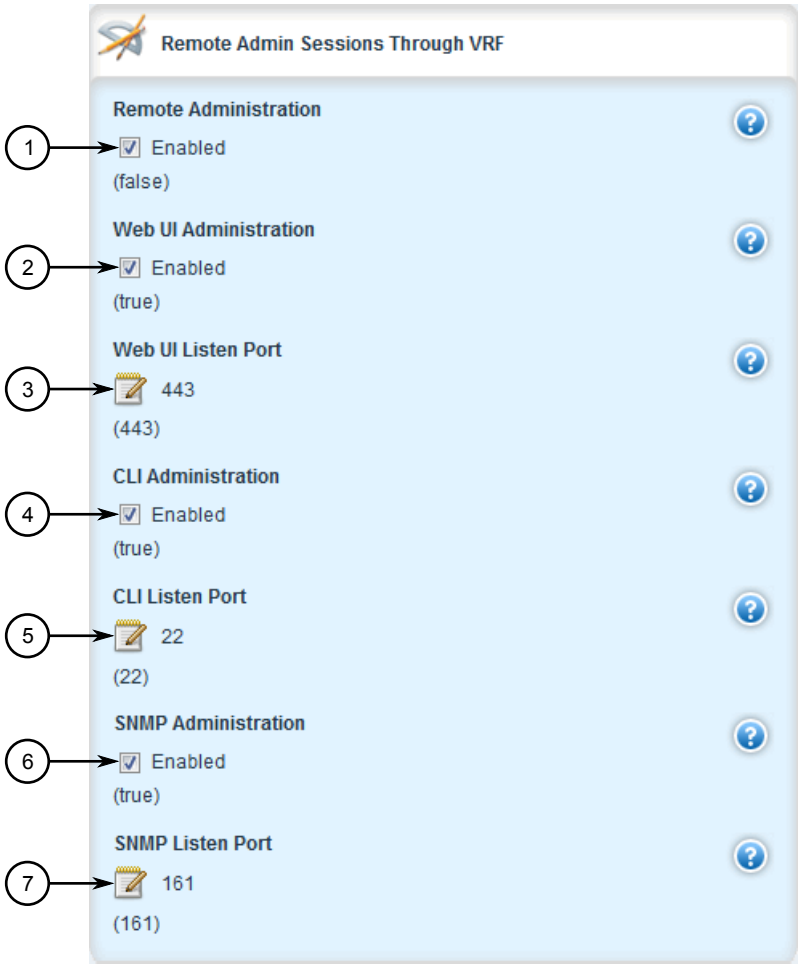


Figure 107: Remote Admin Sessions Through VRF Form

1. Remote Administration Check Box **2.** Web UI Administration Port Box **3.** Web UI Listen Port Box **4.** CLI Administration Box **5.** CLI Listen Port Box **6.** SNMP Administration Box **7.** SNMP Listen Port Box

6. Configure the following parameters:

Parameter	Description
Web UI Administration	**Synopsis:** { true, false } **Default:** true Enables access to the Web user interface over the VRF interface.
Web UI Listen Port	**Synopsis:** A 32-bit signed integer between 1 and 65535 **Default:** 443 The port the Web user interface will listen on for incoming connections over a VRF interface.
CLI Administration	**Synopsis:** { true, false } **Default:** true Enables access to the CLI over the VRF interface.
CLI Listen Port	**Synopsis:** A 32-bit signed integer between 1 and 65535 **Default:** 22

Parameter	Description
	The port the CLI will listen on for incoming connections over a VRF interface.
SNMP Administration	**Synopsis:** { true, false } **Default:** true Enables SNMP access over the VRF interface.
SNMP Listen Port	**Synopsis:** A 32-bit signed integer between 1 and 65535 **Default:** 161 The port SNMP will listen on for incoming connections over a VRF interface.

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.

> **NOTE**
> *Remote access through a VRF interface relies on Network Address Translation (NAT) rules to send frames through the VRF interface to the intended service running in the global namespace. In the case of SNMP, NAT rules are unaware of any listen IP address. As such, the listen IP address for SNMP sessions must be set to* `0.0.0.0` *to allow the session to connect to services in the global namespace.*

9. If the VRF instance is to be used as a listen IP address for SNMP, make sure the *`Listen IP`* parameter for SNMP sessions is set to `0.0.0.0`. For more information, refer to Section 15.2.2, "Enabling and Configuring SNMP Sessions".

Section 5.7
Managing Alarms

The alarm system in RUGGEDCOM ROX II notifies users when events of interest occur. The system is highly configurable, allowing users to:

- Enable/disable most alarms, with the exception of mandatory alarms
- Configure whether or not an alarm triggers the failsafe relay and illuminates the alarm indicator LED on the device
- Configure the severity of most alarms (i.e. emergency, alert, critical, error, etc.), with the exception of some where the severity is fixed

Each alarm is categorized by its type (or subsystem):

Alarm Type	Description
Admin	Admin alarms are for administrative aspects of the device, such as feature-key problems.
Chassis	Chassis alarms are for physical or electrical problems, or similar events of interest. This includes irregular voltages at the power supply or the insertion or removal of a module.
Switch	Switch alarms are for link up/down events on switch interfaces.
Eth	Eth alarms are for fe-cm port related events, such as link up/down events.
WAN	WAN alarms are for T1/E1 and DDS interface related events, such as link up/down events.
Cellmodem	Cellular alarms are for cellular interface related events, such as link up/down events.

Alarm Type	Description
Security	Security alarms are for certificate expiry events. This includes warnings 30 days before a certificate is set to expire and when an expired certificate is installed.
Services	Service alarms are for events related to RUGGEDCOM ROX II services, such as time services, link failover, Dynamic Domain Name Server (DNS) etc.

CONTENTS

Section 5.7.1

Pre-Configured Alarms

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.
Admin	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.
Chassis	PM2 bad supply (For RX1500 and RX1510 Only)	Input power to the power module is outside nominal operating range.	Make sure the input power operating range meets the device requirements.
Chassis	PM1 MOV protection bad	The Metal Oxide Varistor (MOV) protection component within the PM1 power module is damaged.	Contact Siemens Customer Support to return the power module.
Chassis	PM2 MOV protection bad (For RX1500 and RX1510 Only)	The Metal Oxide Varistor (MOV) protection component within the PM2 power module is damaged.	Contact Siemens Customer Support to return the power module.
Chassis	Real-time clock battery low	The Real-Time Clock (RTC) battery in the control module is depleted.	Contact Siemens Customer Support to return the device for repair.
Chassis	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.
Chassis	Module Type Mismatch	The configured module type does not match the detected module type.	Updated the chassis configuration or install the correct module type.
Chassis	Line Module Removed	The specified line module has either been removed or lost contact with the chassis.	Inspect the line module.

Alarm Type	Alarm	Description	Suggested Resolution
Chassis	Line Module Inserted	A new line module has been inserted in the specified slot.	
Security	Firmware Integrity Check Failed	The firmware has failed the binary integrity check, indicating that one or more operating system files have been modified or tampered with.	Contact Siemens Customer Support.

Section 5.7.2
Viewing a List of Active Alarms

To view a list of active alarms, navigate to ***admin » alarms***. If any alarms are currently active, the **Active Alarms** table appears.

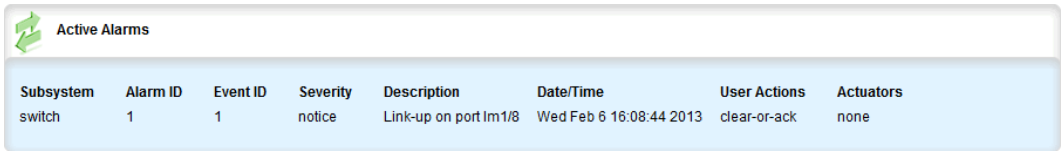


Figure 108: Active Alarms Table

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

Section 5.7.3
Clearing and Acknowledging Alarms

There are two types of alarms: conditional and non-conditional. Conditional alarms are generated when the condition is true and cleared when the condition is resolved and the incident is acknowledged by the user. Non-conditional alarms, however, are simply generated when the event occurs (a notification) and it is the responsibility of the user to clear the alarm.

An example of a conditional alarm is a *link down* alarm. When the condition is resolved (i.e. the link comes up), the LED and alarm relay are both disabled, if the **Auto Clear** option is enabled.

Examples of non-conditional alarms are *link up* and internal configuration errors.

CONTENTS

Section 5.7.3.1
Clearing Alarms

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.

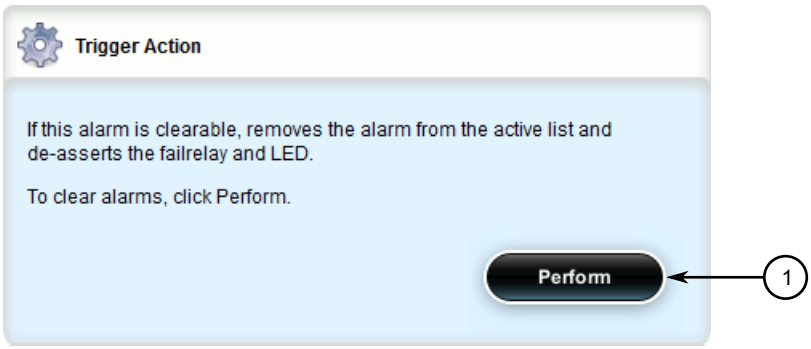


Figure 109: Trigger Action Form

1. Perform Button

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.

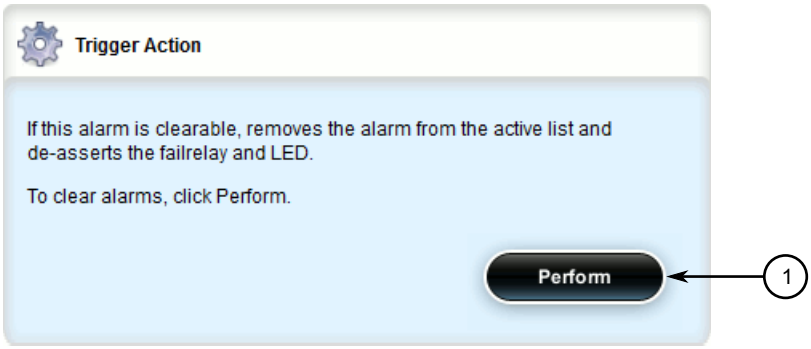


Figure 110: Trigger Action Form

1. Perform Button

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

Section 5.7.3.2

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.

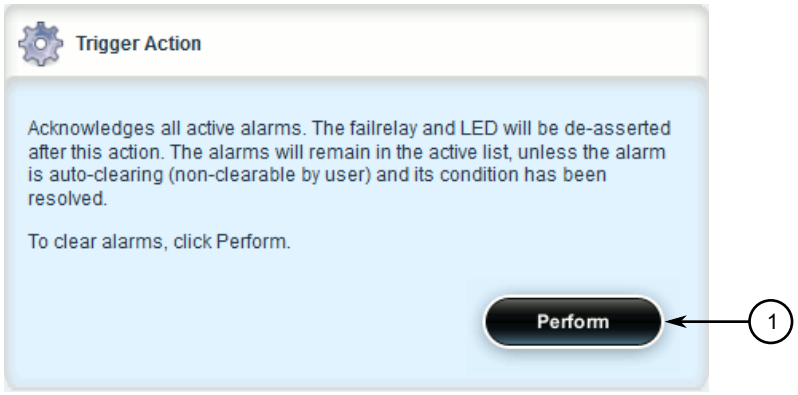


Figure 111: Trigger Action Form

1. Perform Button

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.

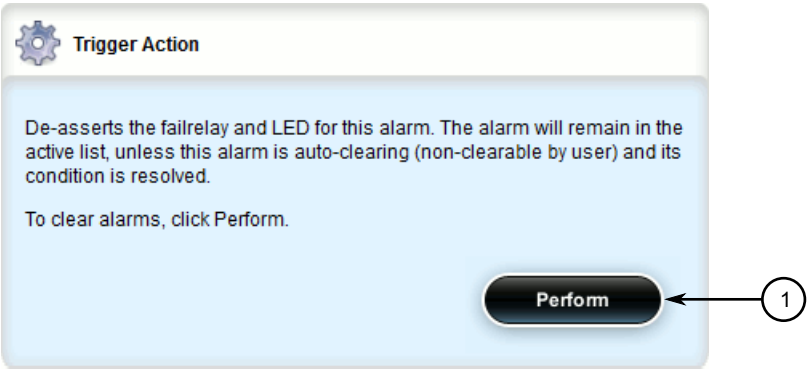


Figure 112: Trigger Action Form

1. Perform Button

3. Click **Perform** to acknowledge the alarm.

Section 5.7.4

Configuring an Alarm

While all alarms are pre-configured on the device, some alarms can be modified to suit the application. This includes changing the severity and enabling/disabling certain features.

NOTE
*The **Failrelay Enable** and **LED Enable** parameters are non-configurable for **link up** alarms.*

To configure an alarm, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to ***admin » 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.

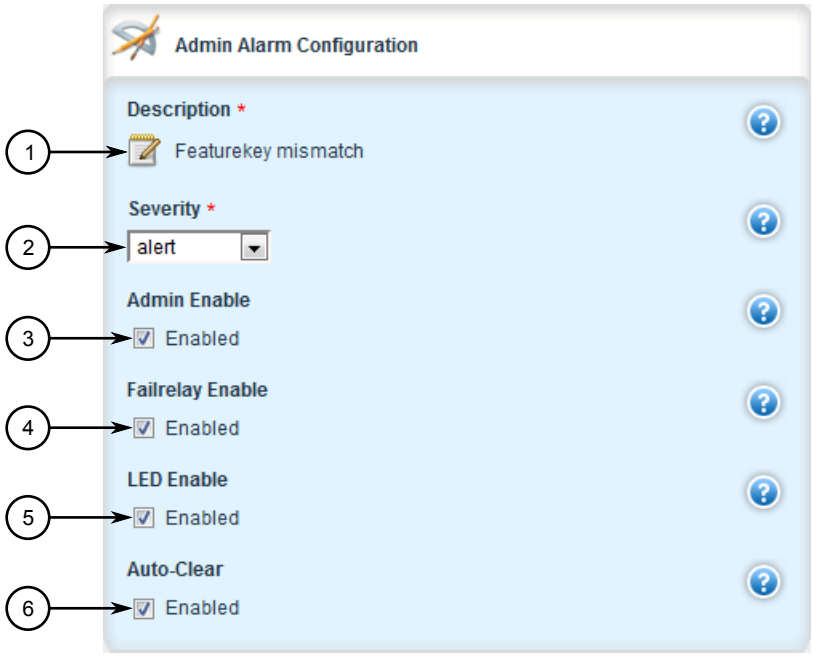


Figure 113: Alarm Configuration Form

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:

NOTE
Alarm descriptions are not configurable.

Parameter	Description
severity	**Synopsis:** { emergency, alert, critical, error, warning, notice, info, debug } The severity level can be one of emergency, alert, critical, error, warning, notice, info, and debug. This cannot be changed for some alarms. This parameter is mandatory.

Parameter	Description
Admin Enable	If disabled, the alarm is not reported in the active list and does not actuate LED/failrelay.
Failrelay Enable	If enabled, this alarm will assert the failrelay.
LED Enable	If enabled, the main 'Alarm' LED light will be red when this alarm is asserted. If disabled, the main 'Alarm' LED light is not affected by this alarm.
Auto-Clear	If enabled, the LED and failrelay will be cleared automatically when condition is met.

4. 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 5.8

Managing Users

RUGGEDCOM ROX II allows for up to three user profiles to be configured locally on the device. Each profile corresponds to one of the following access levels:

- Guest
- Operator
- Admin

The access levels provide or restrict the user's ability to change settings and execute various commands.

Rights	User Type		
	Guest	Operator	Admin
View Settings	✓	✓	✓
Clear Logs	✓	✓	✓
Reset Alarms	×	✓	✓
Clear Statistics	×	✓	✓
Change Basic Settings	×	✓	✓
Change Advanced Settings	×	×	✓
Run Commands	×	×	✓

CAUTION!
Security hazard – risk of unauthorized access and/or exploitation. To prevent unauthorized access to the device, make sure to change the default passwords for all users before commissioning the device. For more information, refer to Section 5.9.2, "Setting a User Password/Passphrase".

CONTENTS

- Section 5.8.4, "Monitoring Users"

Section 5.8.1
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.

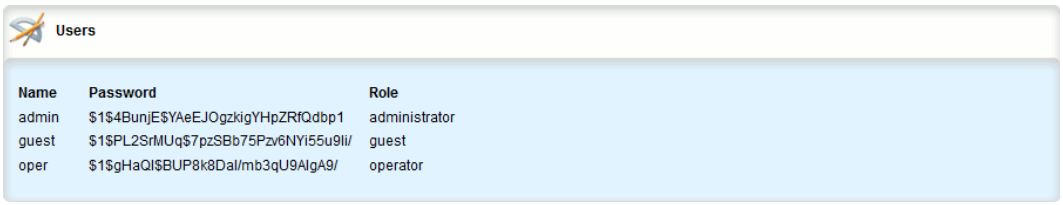


Figure 114: Users Table

If no user accounts have been configured, add user accounts as needed. For more information, refer to Section 5.8.2, "Adding a User".

Section 5.8.2
Adding a User

To add a new user account, do the following:

1. 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.

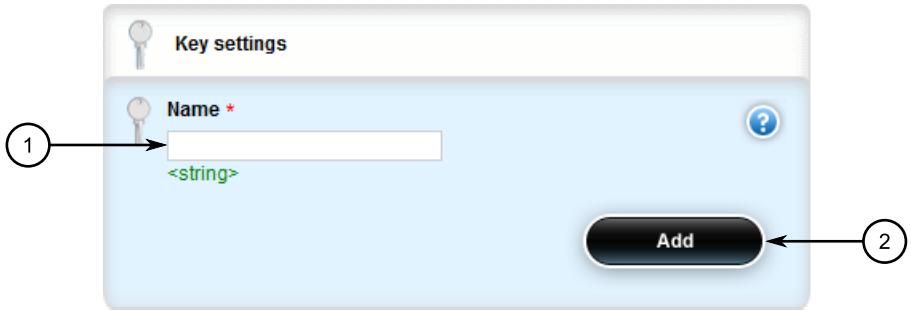


Figure 115: Key Settings Form

1. Name Box **2.** Add Button

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

Parameter	Description
name	**Synopsis:** A string 1 to 128 characters long

Parameter	Description
	The name of the user.

4. Click **Add** to create the new user account. The **Users** form appears.

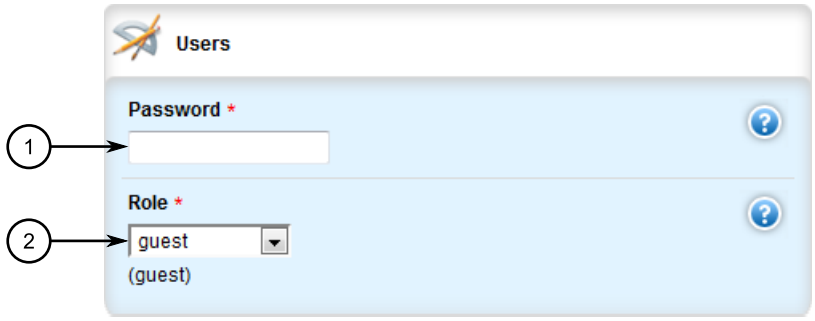


Figure 116: Users Form

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 5.9.2, "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.
9. [Optional] Assign a user authentication key to the user account, allowing the user to access the device via SSH without having to provide a password/passphrase. For more information, refer to Section 6.6.2, "Managing User Authentication Keys".

Section 5.8.3

Deleting a User

To delete a user account, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to ***admin » users***. The **Users** table appears.

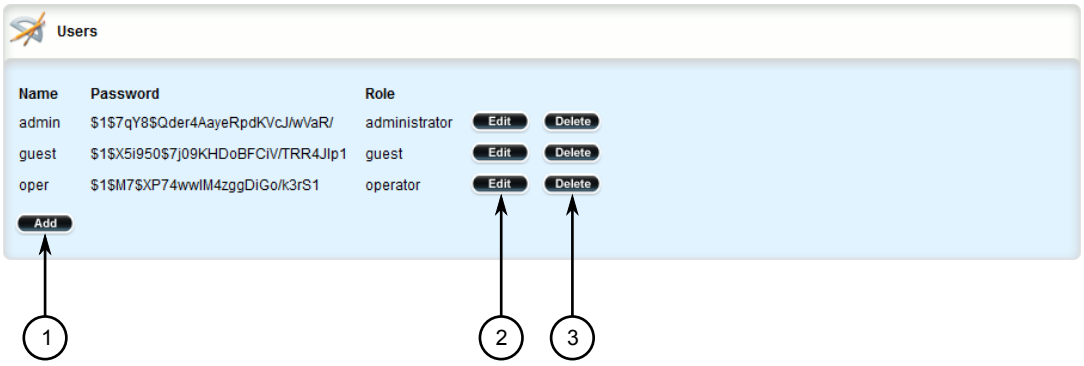


Figure 117: Users Table

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

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 5.8.4

Monitoring Users

Users currently logged in to the device are monitored by RUGGEDCOM ROX II and can be viewed on the **Users** screen. RUGGEDCOM ROX II allows administrators to monitor users, log users out, and broadcast 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.

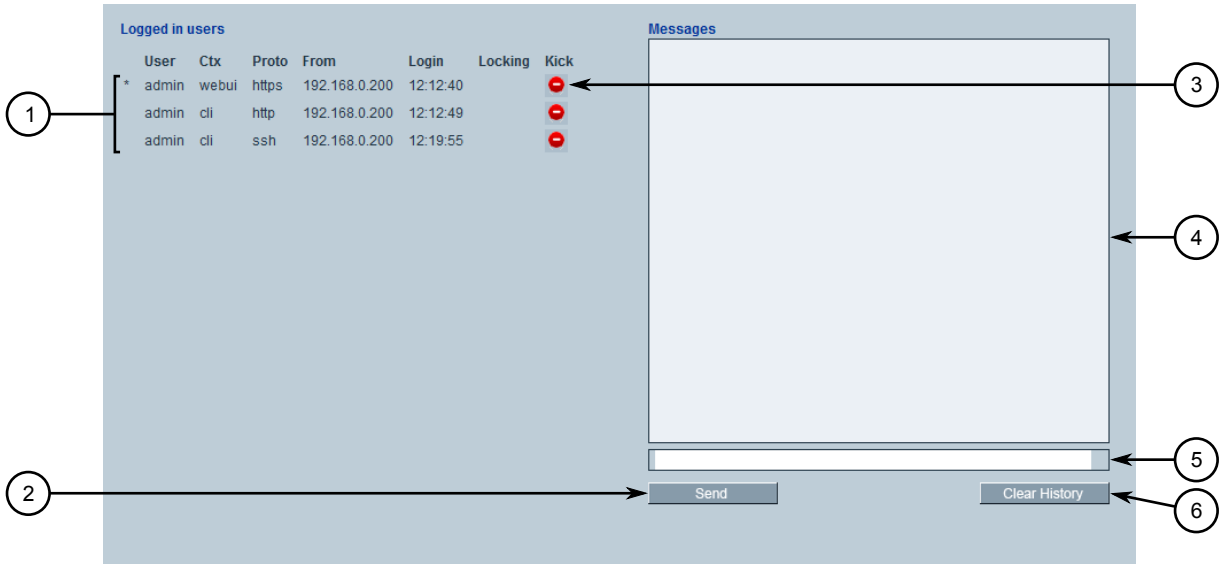


Figure 118: Users Screen

1. List of Users **2.** Send Button **3.** Kick Icon **4.** Messages Window **5.** Message Box **6.** Clear History Button

CONTENTS

Section 5.8.4.1

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.

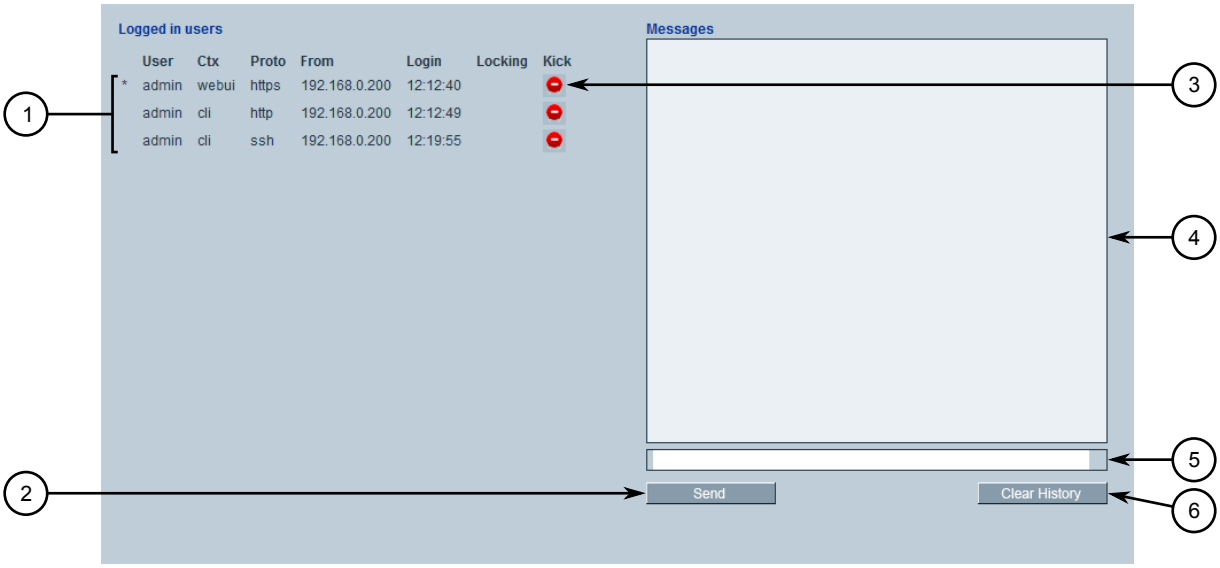


Figure 119: Users Screen

1. List of Users **2.** Send Button **3.** Kick Icon **4.** Messages Window **5.** Message Box **6.** Clear History Button

2. Click the **Kick** icon next to the user profile.

Section 5.8.4.2

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.

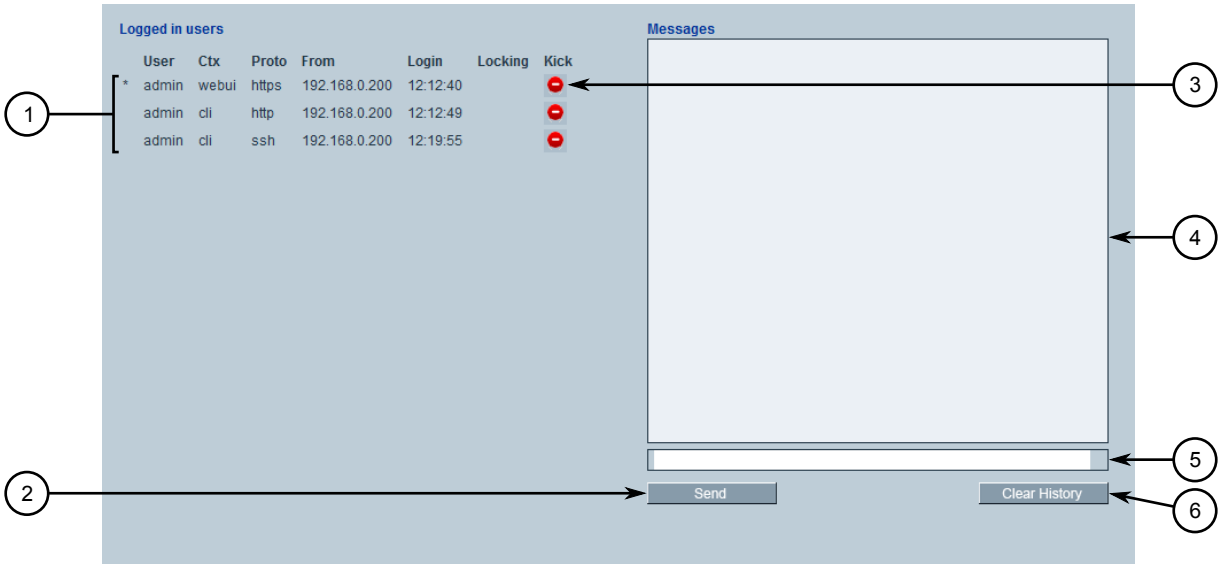


Figure 120: Users Screen

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 5.9

Managing Passwords and Passphrases

RUGGEDCOM ROX II requires separate passwords or passphrases for logging into the various device modes, such as normal, boot, service and maintenance modes. Default passwords are configured for each user type initially. It is strongly recommended that these be changed before the device is commissioned.

NOTE
For a list of default passwords, refer to Section 2.1, "Default User Names and Passwords".

The complexity of each password/passphrase can be chosen by the user or enforced through the device by an administrator. If a user's password/passphrase does not meet the password requirements, an alarm is generated. For example:

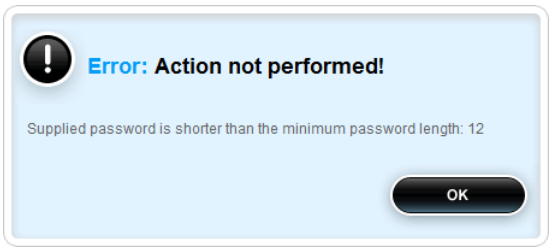


Figure 121: Example – Password Too Short Alarm

In general, passwords/passphrases should consist of:

- One lower case character
- One upper case character
- One number
- One special character (i.e. !@#$%^&*()_+-={}[];:',<.>/?\|`~)

NOTE
User authentication can also be verified through a RADIUS or TACACS+ server. When enabled for authentication and authorization, the RADIUS or TACACS+ server will be used. For more information about configuring a RADIUS or TACACS+ server, refer to Section 6.6.3, "Managing RADIUS Authentication" and Section 6.6.4, "Configuring TACACS+ Authentication".

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

CAUTION!
Accessibility hazard – risk of data loss. Do not forget the passwords for the device. If both the maintenance and boot passwords are forgotten, the device must be returned to Siemens Canada Ltd for repair. This service is not covered under warranty. Depending on the action that must be taken to regain access to the device, data may be lost.

CONTENTS

Section 5.9.1

Configuring Password/Passphrase Complexity Rules

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.

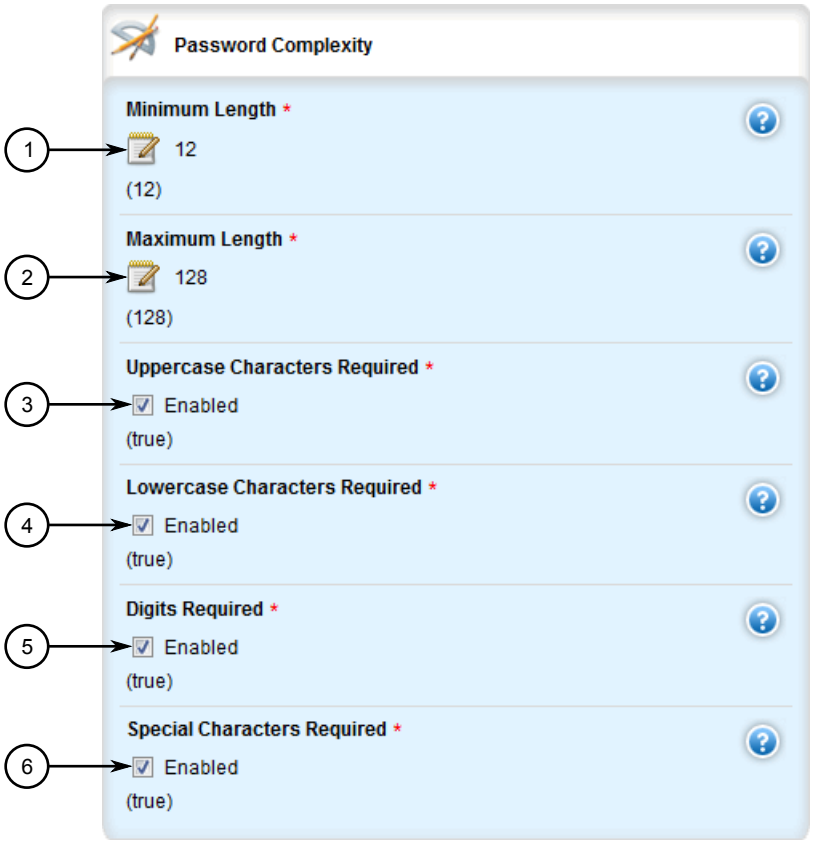


Figure 122: Password Complexity Form

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	**Synopsis:** A 32-bit unsigned integer between 1 and 128 **Default:** 12 Minimum password length.
Maximum Length	**Synopsis:** A 32-bit unsigned integer between 1 and 128 **Default:** 128 Maximum password length.
Uppercase Characters Required	**Synopsis:** { true, false } **Default:** true Requires the password to have at least one uppercase letter.
Lowercase Characters Required	**Synopsis:** { true, false } **Default:** true Requires the password to have at least one lowercase letter.
Digits Required	**Synopsis:** { true, false } **Default:** true Requires the password to have at least one numerical digit.

Parameter	Description
Special Characters Required	**Synopsis:** { true, false } **Default:** true Requires the password to have at least one non-alphanumeric character. Allowed characters include "!@#$%^&*()_+-={}[];:',<.>/?|`~".

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 5.9.2
Setting a User Password/Passphrase

To set the password/passphrase for a user profile, do the following:

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

1. Navigate to ***admin » users » {user} » set-password***, where *{user}* is the user ID. The **Set User Password** and **Trigger Action** forms appear.

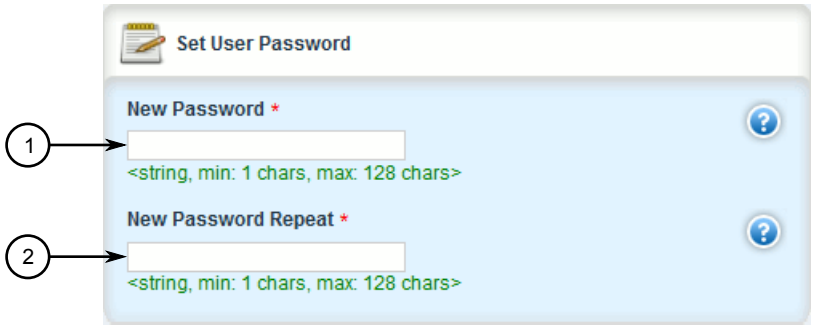


Figure 123: Set User Password Form

1. New Password Box **2.** New Password Repeat Box

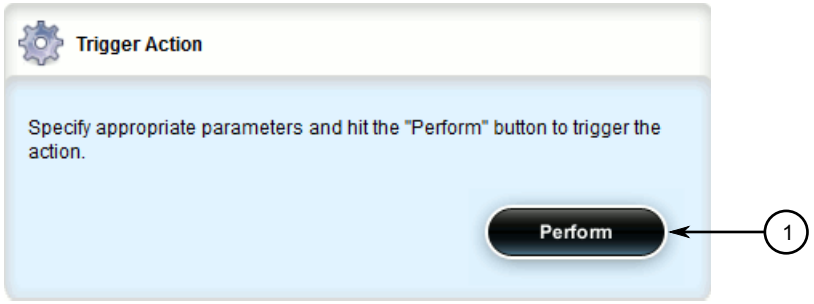


Figure 124: Trigger Action Form

1. Perform Button

2. On the **Set User Password** form, configure the following parameters:

Parameter	Description
New Password	**Synopsis:** 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. This parameter is mandatory.
New Password Repeat	**Synopsis:** 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. This parameter is mandatory.

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

Section 5.9.3

Setting the Boot Password/Passphrase

The boot password/passphrase grants access to BIST mode and service mode, which are only accessible through the Command Line Interface (CLI). For more information about these modes, refer to the *RUGGEDCOM ROX II v2.12 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 U-Boot binary. For information about determining and/or upgrading the U-Boot version installed on the device, refer to How to Upgrade the U-Boot Binary [https://support.industry.siemens.com/cs/ww/en/view/109738243] available on https://www.siemens.com/ruggedcom.

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

1. Navigate to ***admin » authentication » set-boot-password***. The **Set Boot Password** and **Trigger Action** forms appear.

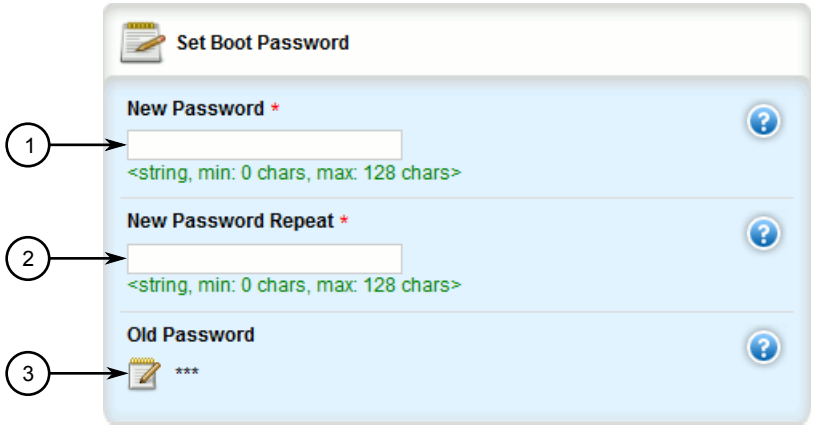


Figure 125: Set Boot Password Form

1. New Password Box **2.** New Password Repeat Box **3.** Old Password Box

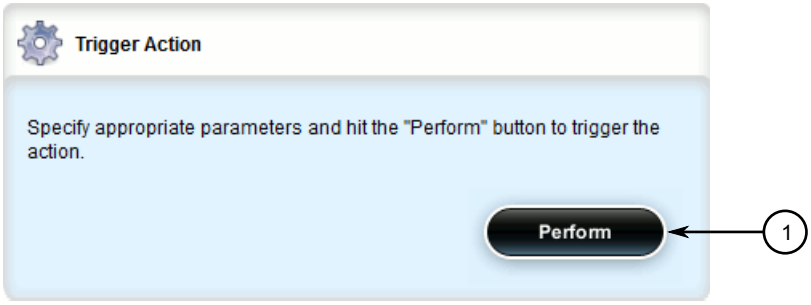


Figure 126: Trigger Action Form

1. Perform Button

2. On the **Set Boot Password** form, configure the following parameters:

Parameter	Description
New Password	**Synopsis:** 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. This parameter is mandatory.
New Password Repeat	**Synopsis:** 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. This parameter is mandatory.
Old Password	**Synopsis:** A string 0 to 128 characters long Specify the old password if there is currently a boot password set, otherwise leave it empty. This parameter is mandatory.

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

Section 5.9.4

Setting the Maintenance Password/Passphrase

The maintenance password/passphrase grants access to the maintenance mode, which is only accessible through the Command Line Interface (CLI). For more information about this mode, refer to the *RUGGEDCOM ROX II v2.12 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:

1. Navigate to ***admin » authentication » set-maint-password***. The **Set Maint Password** and **Trigger Action** forms appear.

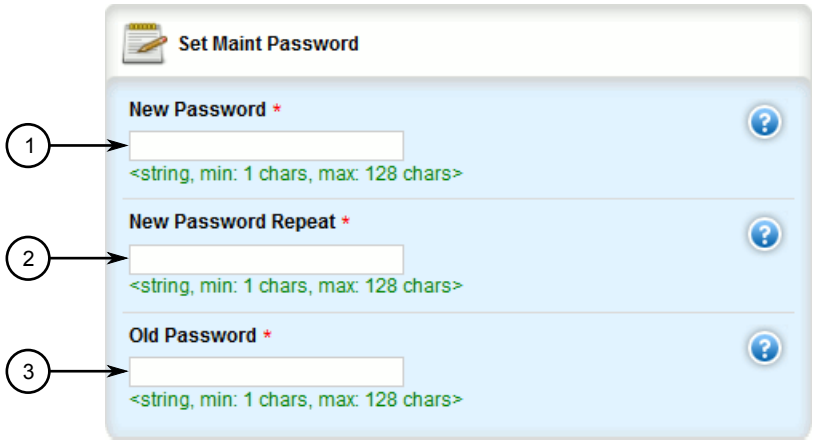


Figure 127: Set Maint Password Form

1. New Password Box **2.** New Password Repeat Box **3.** Old Password Box

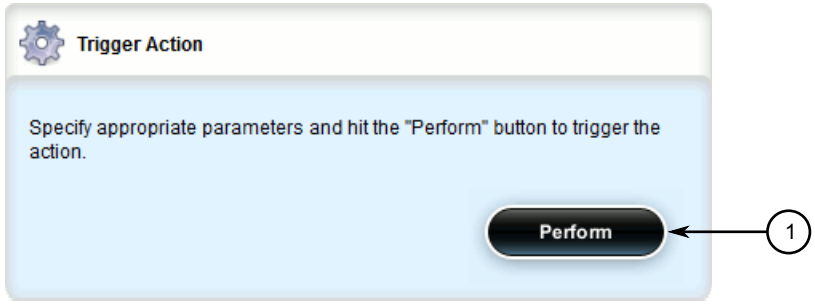


Figure 128: Trigger Action Form

1. Perform Button

2. On the **Set Maint Password** form, configure the following parameters:

Parameter	Description
New Password	**Synopsis:** 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. This parameter is mandatory.
New Password Repeat	**Synopsis:** 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. This parameter is mandatory.
Old Password	**Synopsis:** A string 1 to 128 characters long Specify the old password. This parameter is mandatory.

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

Section 5.9.5
Resetting Passwords and Passphrases

If either the admin, boot or maintenance password/passphrase is lost, the only method for resetting the password/passphrase is to physically connect to the device and reset the password/passphrase through the Command Line Interface (CLI). For information about resetting passwords/passphrases, refer to the *RUGGEDCOM ROX II v2.12 CLI User Guide*.

Section 5.10
Scheduling Jobs

The RUGGEDCOM ROX II scheduler allows users to create jobs that execute command line interface (CLI) commands at a specific date and time, or in response to specific configuration changes. Typical applications include scheduling the regular clearing of system logs, or performing periodic file transfers to remote servers.

There are two types of scheduled jobs:

- **Periodic jobs** are executed at a specified date and time.
- **Config change jobs** are executed only when a specific.

CONTENTS

Section 5.10.1
Viewing a List of Scheduled Jobs

To view a list of scheduled jobs, navigate to ***admin » scheduler***. If jobs have been configured, the **Scheduled Jobs** table appears.

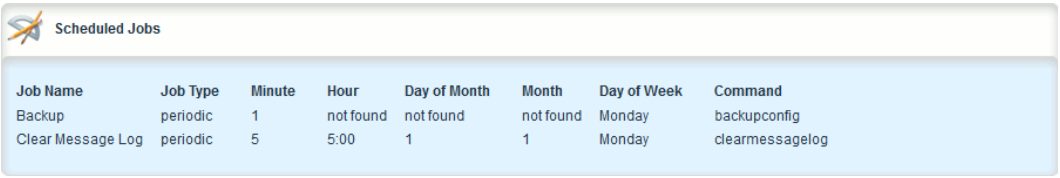


Figure 129: Scheduled Jobs Table

If no jobs have been configured, add jobs as needed. For more information, refer to Section 5.10.2, "Adding a Scheduled Job".

Section 5.10.2
Adding a Scheduled Job

To add a scheduled job, do the following:

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

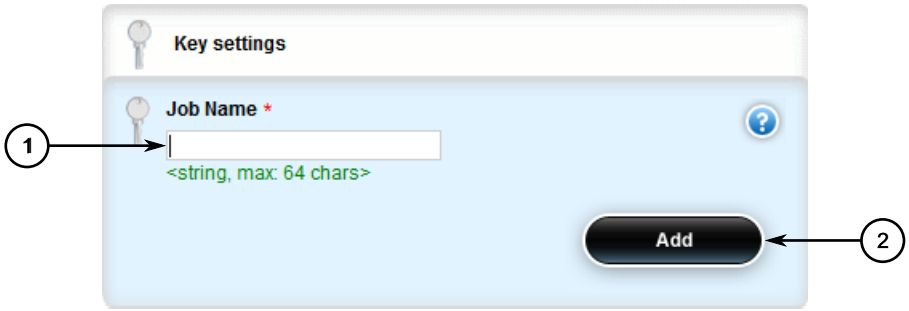


Figure 130: Key Settings Form

1. Job Name Box **2.** Add Button

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

Parameter	Description
Job Name	**Synopsis:** A string 1 to 64 characters long The name of the scheduled job. The name can be up to 64 characters in length.

4. Click **Add**. The **Scheduled Jobs** form appears.

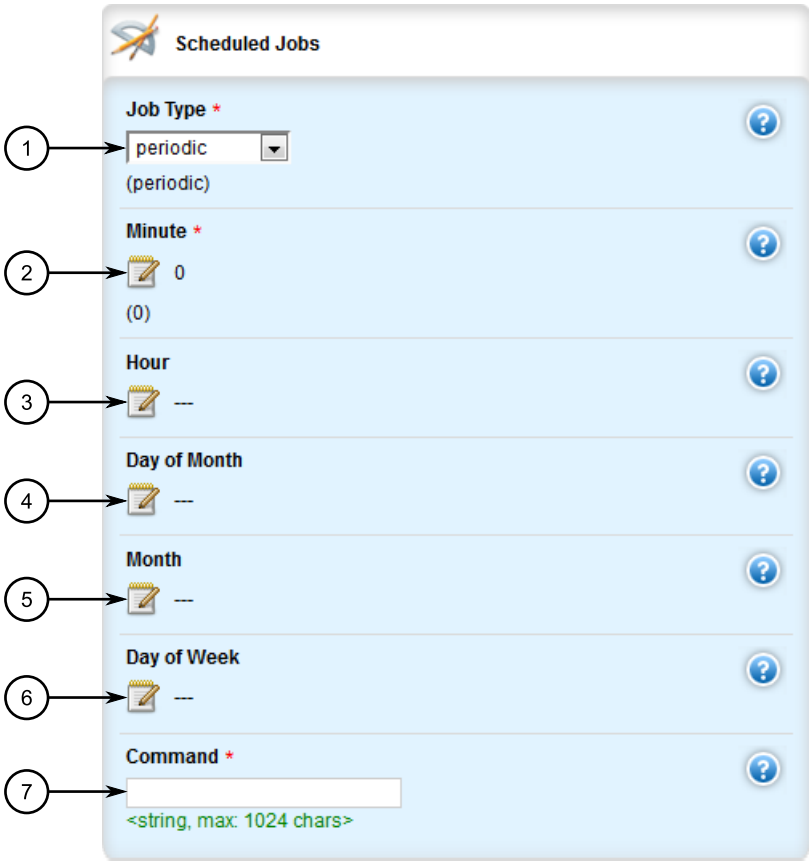


Figure 131: Key Settings Form

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	**Synopsis:** { configchange, periodic } **Default:** periodic Determines when to launch the scheduled job: • periodic: The job launches at a set date and time. • configchange: The job launches when the configuration changes.
Minute	**Synopsis:** A string 1 to 128 characters long **Default:** 0 For periodic jobs, sets the minutes portion of the job launch time. Valid values are in the range of 0 to 59. If no value is set, the scheduler uses the default value of 0 and launches the job every hour on the the hour. • To specify a single value, enter the value in the field. For example, to launch the job 10 minutes past the hour, enter 10. • To specify a list of values, enter the values as a comma-separated list. For example, to launch the job at 15, 30, and 45 minutes past the hour, enter 15,30,45. • To specify a range of values, enter the range as comma-separated values. For example, to launch the job every minute between 30 and 45 minutes past the hour, enter 30-45.

Parameter	Description
	This parameter is not required for configchange jobs.
Hour	**Synopsis:** A string 1 to 64 characters long For periodic jobs, sets the hour portion of the job launch time, in the 24-hour clock format. Valid values are in the range of 0 to 23. If no value is set, the job launches every hour at the time set in the Minute field. • To specify a single value, enter the value in the field. For example, to launch the job at 5:00 pm, enter 17. • To specify a list of values, enter the values as a comma-separated list. For example, to launch the job at 9:00 am, 12:00 pm, and 5:00 pm, enter 9,12,17. • To specify a range of values, enter the range as comma-separated values. For example, to launch the job every hour between 9:00 am and 5:00 pm, enter 9-17. This parameter is not required for configchange jobs.
Day of Month	**Synopsis:** A string 1 to 64 characters long For periodic jobs, sets the day of the month on which to run the scheduled job. Valid values are in the range of 1 to 31. If no value is set, the job launches every day. • To specify a single value, enter the value in the field. For example, to launch the job on the tenth day of the month, enter 10. • To specify a list of values, enter the values as a comma-separated list. For example, to launch the job on the first, fifteenth, and thirtieth days of the month, enter 10,15,30. • To specify a range of values, enter the range as comma-separated values. For example, to launch the job on days one through fifteen, enter 1-15. This parameter is not required for configchange jobs.
Month	**Synopsis:** A string 1 to 32 characters long For periodic jobs, sets the month in which to run the scheduled job. Valid values are in the rage of 1 to 12. If no value is set, the job launches every day. • To specify a single value, enter the value in the field. For example, to set the month to February, enter 2. • To specify a list of values, enter the values as a comma-separated list. For example, to set the months to January, June, and December, enter 1,6,12. • To specify a range of values, enter the range as comma-separated values. For example, to set the months to January through June, enter 1-6. This parameter is not required for configchange jobs.
Day of Week	**Synopsis:** A string 1 to 16 characters long For periodic jobs, sets the day of the week on which to run the scheduled job. Valid entries are in the range of 0 to 6, where 0 represents Sunday, 1 represents Monday, and so on. If no value is set, the job launches every day. • To specify a single value, enter the value in the field. For example, to set the day to Monday, enter 1. • To specify a list of values, enter the values as a comma-separated list. For example, to set the days to Friday, Saturday, and Sunday, enter 5,6,0. • To specify a range of values, enter the range as comma-separated values. For example, to set the days to Monday through Friday, enter 1-5. This parameter is not required for configchange jobs.
Command	**Synopsis:** A string 1 to 1024 characters long One or more commands to execute at the scheduled time. For example, this command saves the running configuration to a file name 'myconfig': show running-config | save myconfig. Do not use interactive commands or commands that require a manual response or confirmation. When entered in the CLI, the command string must be enclosed in quotation marks. When entered in the WebUI, the command string must not be enclosed in quotation marks.

Parameter	Description
	This parameter is mandatory.

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 5.10.3
Deleting a Scheduled Job

To delete a scheduled Job, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to ***admin » scheduler***. The **Scheduled Jobs** table appears.

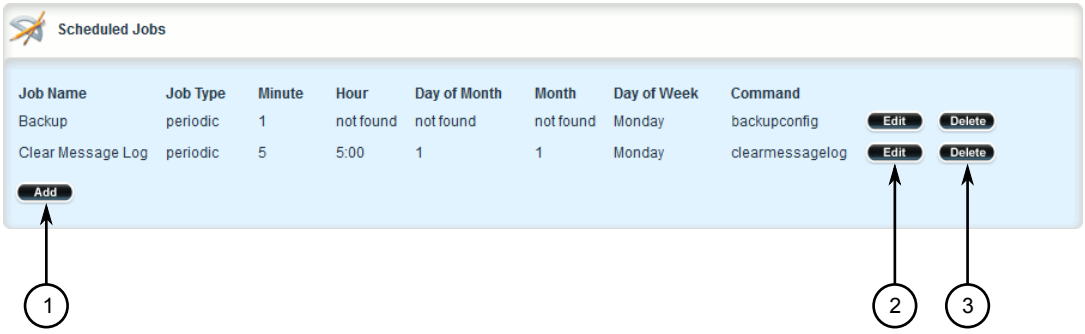


Figure 132: Scheduled Jobs Table

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

3. Click **Delete** next to the chosen job.
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 Security

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

CONTENTS

Section 6.1

Enabling and Configuring CLI Sessions

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.

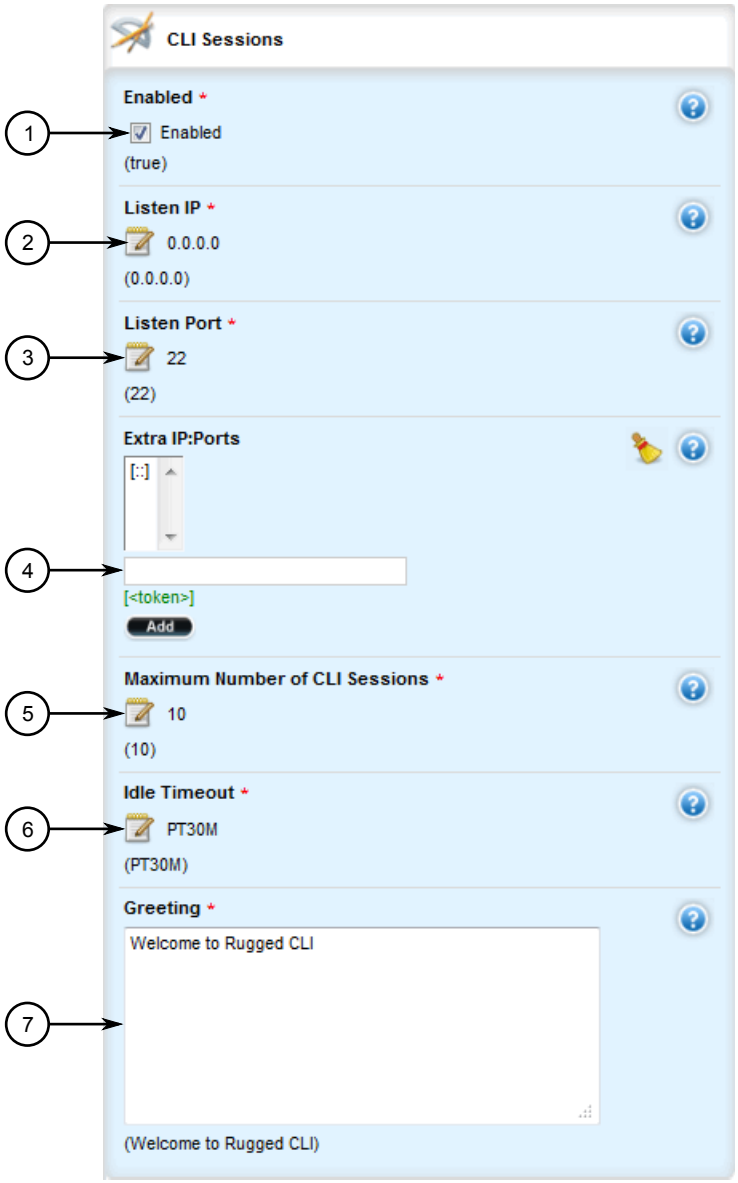


Figure 133: CLI Sessions

1. Enabled Check Box **2.** Listen IP Box **3.** Listen Port Box **4.** Extra IP Ports Box **5.** Maximum Number of CLI Sessions Box **6.** Idle Timeout Box **7.** Greeting Box

3. Configure the following parameter(s):

Parameter	Description
enabled	**Synopsis:** { true, false } **Default:** true When enabled, a command line interface (CLI) may be used to configure the device. A secure shell (SSH) client or serial console may be used to access the CLI.
Listen IP	**Synopsis:** A string **Default:** 0.0.0.0

Parameter	Description
	The IPv4 or IPv6 address on which the CLI will listen for requests from the device. The default value (i.e. 0.0.0.0) enables the CLI to receive requests via any IP address with which it is associated.
Listen Port	**Synopsis:** A 16-bit unsigned integer between 0 and 65535 **Default:** 22 The default port on which the CLI will listen for requests from the device. The port corresponds with the IP address specified by the Listen IP (listen-ip) parameter.
Extra IP:Ports	**Synopsis:** A string Additional IPv4 or IPv6 addresses and their associated ports on which the CLI will listen for requests from the device. IPv4 addresses and port numbers must be separated by a colon (e.g. 192.168.0.2: 19343). IPv6 addresses and port numbers must be separated by square brackets and a colon (e.g. [2001:db8:2728::2200]:[19343]). If the Listen IP (listen-ip) parameter is set to a value other than 0.0.0.0, the port specified by the Listen Port (port) parameter must not be associated with any additional addresses.
Maximum Number of CLI Sessions	**Synopsis:** a 32-bit unsigned integer **Default:** 10 The maximum number of concurrent CLI sessions.
Idle Timeout	**Synopsis:** A string **Default:** PT30M The maximum period of time that a CLI session may remain idle. After this period of time, the session is terminated. Values are expressed in durations of years, months, weeks, days, hours, minutes, and/or seconds in ISO 8601 format (e.g. P1Y1M2W3DT2H3M30S corresponds with 1 year, 1 month, 2 weeks, 3 days, 2 hours, 3 minutes, and 30 seconds). A session is not considered idle if the CLI is waiting for notifications or if commits are pending. If the value of this parameter is changed during a session, the change will not take effect until the next session.
Greeting	**Synopsis:** A string 1 to 8192 characters long A greeting message presented to users when they log in to the CLI.

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 6.2
Enabling and Configuring SFTP Sessions

To enable and configure SFTP sessions, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to ***admin***. The **SFTP Sessions** form appears.

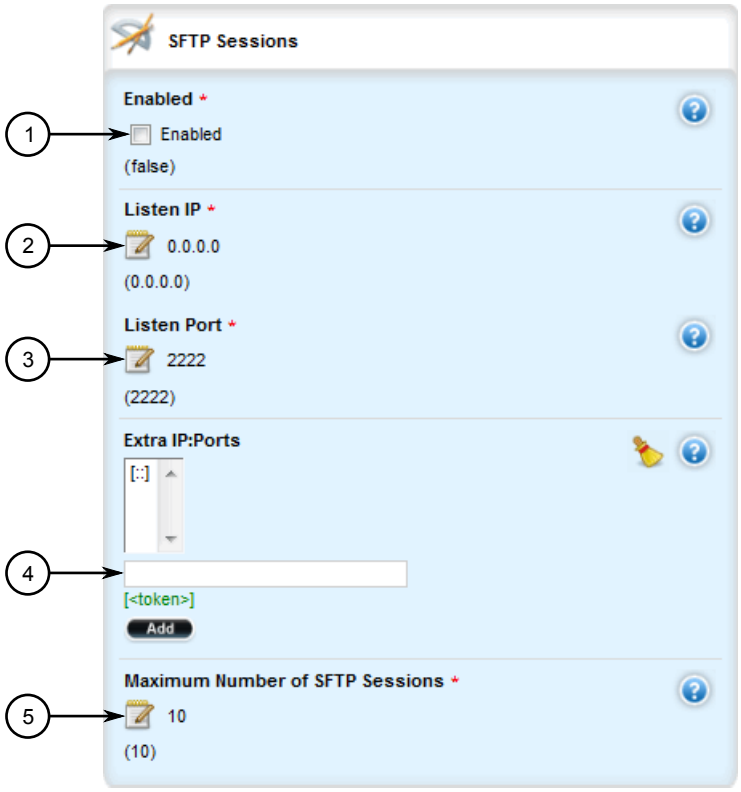


Figure 134: SFTP Sessions

1. Enabled Check Box **2.** Listen IP Box **3.** Listen Port Box **4.** Extra IP Ports Box **5.** Maximum Number of SFTP Sessions Box

3. Configure the following parameter(s):

Parameter	Description
enabled	**Synopsis:** { true, false } **Default:** false Enables/Disables the SFTP user interface.
Listen IP	**Synopsis:** A string **Default:** 0.0.0.0 The IP Address the SFTP will listen on for SFTP requests.
Listen Port	**Synopsis:** A 16-bit unsigned integer between 0 and 65535 **Default:** 2222 The port the SFTP will listen on for SFTP requests.
Extra IP:Ports	**Synopsis:** 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	**Synopsis:** a 32-bit unsigned integer **Default:** 10 This parameter is not supported and any value is ignored by the system.

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 6.3

Enabling/Disabling Brute Force Attack Protection

RUGGEDCOM ROX II features a Brute Force Attack (BFA) protection mechanism to prevent attacks via the CLI, Web interface and NETCONF. This mechanism analyzes the behavior of external hosts trying to access the SSH port, specifically the number of failed logins. After 15 failed login attempts, the IP address of the host will be blocked for 720 seconds or 12 minutes. The range of 15 failed login attempts exists to take into account various methods of accessing the device, notably when the same or different ports are used across a series of failed logins.

IMPORTANT!
The BFA protection system is not applicable to SNMP. Follow proper security practices for configuring SNMP. For example:

- *Do not use SNMP over the Internet*
- *Use a firewall to limit access to SNMP*
- *Do not use SNMPv1*

NOTE
Failed logins must happen within 10 minutes of each other to be considered malicious behavior.

Once the time has expired, the host will be allowed to access the device again. If the malicious behavior continues from the same IP address (e.g. another 15 failed login attempts), then the IP address will be blocked again, but the time blocked will increase by a factor of 1.5. This will continue as long as the host repeats the same behavior.

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

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

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

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

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

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

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

NOTE
For information about how to view `auth.log`*, refer to* *Section 4.10.1, "Viewing Logs"*.

When the default alarm for brute force attacks is enabled, a host that exceeds the maximum number of failed login attempts will trigger an alarm. The alarm will be listed on the list of active alarms until the alarm is resolved and acknowledged.

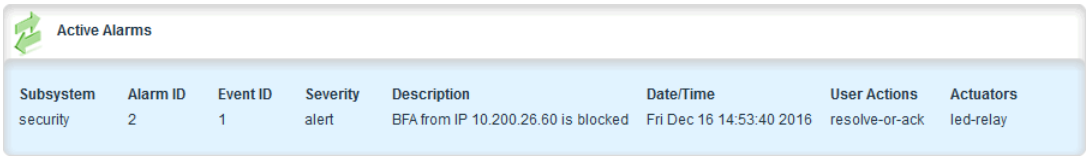


Figure 135: Active Alarms Table – BFA Alarm (Example)

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.

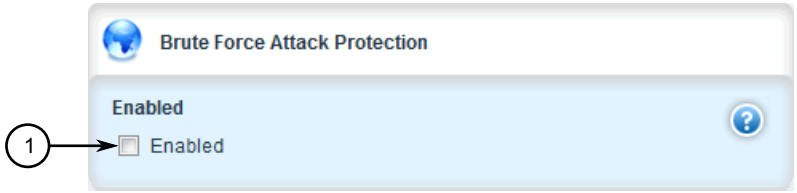


Figure 136: Brute Force Attack Protection Form

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.
6. [Optional] Enable or disable the default alarm for brute force attacks. For more information, refer to Section 5.7.4, "Configuring an Alarm".

Section 6.4

Enabling/Disabling SYN Cookies

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

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

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to ***admin***. The **System Control** form appears.

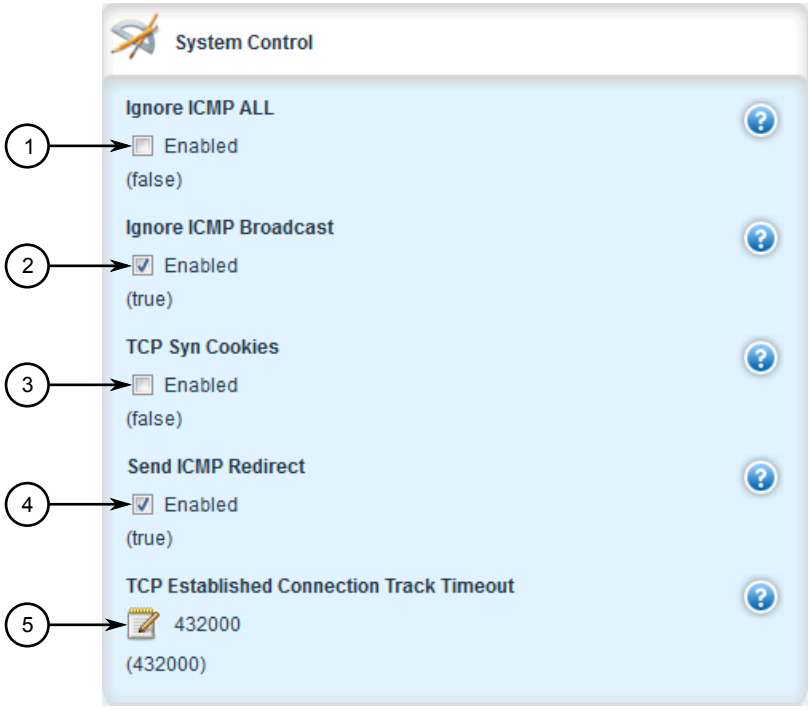


Figure 137: System Control Form

1. Ignore ICMP ALL Check Box **2.** Ignore ICMP Broadcast Check Box **3.** TCP Syn Cookies Check Box **4.** Send ICMP Redirect Check Box **5.** TCP Established Connection Track Timeout Box

3. Select **TCP Syn Cookies** to enable SYN cookies, or clear the checkbox to disable SYN cookies
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 6.5

Managing Port Security

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

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

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

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

NOTE
RUGGEDCOM ROX II supports 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.

CONTENTS

Section 6.5.1

Port Security Concepts

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

CONTENTS

Section 6.5.1.1

Static MAC Address-Based Authentication

In this method, the device validates the source MAC addresses of received frames against the contents in the Static MAC Address Table. RUGGEDCOM ROX II also supports a highly flexible Port Security configuration that provides a convenient means for network administrators to use the feature in various network scenarios.

A Static MAC address can be configured without a port number being explicitly specified. In this case, the configured MAC address will be automatically authorized on the port where it is detected. This allows devices to be connected to any secure port on the switch without requiring any reconfiguration.

The device can also be programmed to learn (and, thus, authorize) a pre-configured number of the first source MAC addresses encountered on a secure port. This enables the capture of the appropriate secure addresses when first configuring MAC address-based authorization on a port. Those MAC addresses are automatically inserted into the Static MAC Address Table and remain there until explicitly removed by the user.

Section 6.5.1.2
IEEE 802.1x Authentication

The IEEE 802.1x standard defines a mechanism for port-based network access control and provides a means of authenticating and authorizing devices attached to LAN ports.

Although IEEE 802.1x is mostly used in wireless networks, this method is also implemented in wired switches.

The IEEE 802.1x standard defines three major components of the authentication method: Supplicant, Authenticator and Authentication server. RUGGEDCOM ROX II supports the Authenticator component.

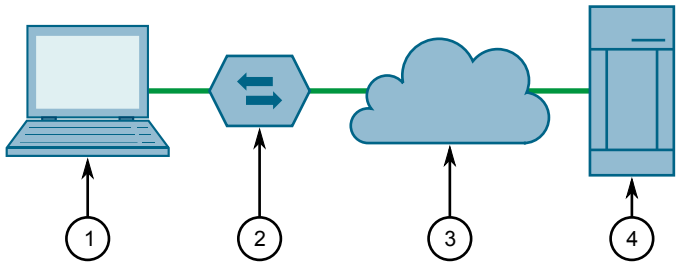


Figure 138: IEEE 802.1x General Topology

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

IMPORTANT!
RUGGEDCOM ROX II supports both Protected Extensible Authentication Protocol (PEAP) and EAP-MD5. PEAP is more secure and is recommended if available in the supplicant.

IEEE 802.1x makes use of the Extensible Authentication Protocol (EAP), which is a generic PPP authentication protocol that supports various authentication methods. IEEE 802.1x defines a protocol for communication between the Supplicant and the Authenticator, referred to as EAP over LAN (EAPOL).

RUGGEDCOM ROX II communicates with the Authentication Server using EAP over RADIUS.

NOTE
The device supports authentication of one host per port.

NOTE
If the host's MAC address is configured in the Static MAC Address Table, it will be authorized, even if the host authentication is rejected by the authentication server.

Section 6.5.1.3
IEEE 802.1X Authentication with MAC Address-Based Authentication

This method, also referred to as MAB (MAC-Authentication Bypass), is commonly used for devices, such as VoIP phones and Ethernet printers, that do not support the IEEE 802.1x protocol. This method allows such devices to be authenticated using the same database infrastructure as that used in IEEE 802.1x.

IEEE 802.1x with MAC-Authentication Bypass works as follows:

1. The device connects to a switch port.

2. The switch learns the device MAC address upon receiving the first frame from the device (the device usually sends out a DHCP request message when first connected).
3. The switch sends an EAP Request message to the device, attempting to start IEEE 802.1X authentication.
4. The switch times out while waiting for the EAP reply, because the device does not support IEEE 802.1x.
5. The switch sends an authentication message to the authentication server, using the device MAC address as the username and password.
6. The switch authenticates or rejects the device based on the reply from the authentication server.

Section 6.5.1.4
Assigning VLANS with Tunnel Attributes

RUGGEDCOM ROX II supports assigning a VLAN to an authorized port using tunnel attributes, as defined in RFC 3580 [http://tools.ietf.org/html/rfc3580], when the Port Security mode is set to `802.1x` or `802.1x/MAC-Auth`.

In some cases, it may be desirable to allow a port to be placed into a particular VLAN, based on the authentication result. For example:

- To allow a particular device, based on its MAC address, to remain on the same VLAN as it moves within a network, configure the switches for 802.1X/MAC-Auth mode
- To allow a particular user, based on the user's login credentials, to remain on the same VLAN when the user logs in from different locations, configure the switches for 802.1X mode

If the RADIUS server wants to use this feature, it indicates the desired VLAN by including tunnel attributes in the Access-Accept message. The RADIUS server uses the following tunnel attributes for VLAN assignment:

- Tunnel-Type=VLAN (13)
- Tunnel-Medium-Type=802
- Tunnel-Private-Group-ID=VLANID

Note that VLANID is 12-bits and takes a value between 1 and 4094, inclusive. The Tunnel-Private-Group-ID is a string as defined in RFC 2868 [http://tools.ietf.org/html/rfc2868], so the VLANID integer value is encoded as a string.

If the tunnel attributes are not returned by the authentication server, the VLAN assigned to the switch port remains unchanged.

Section 6.5.2
Configuring Port Security

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

1. 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.

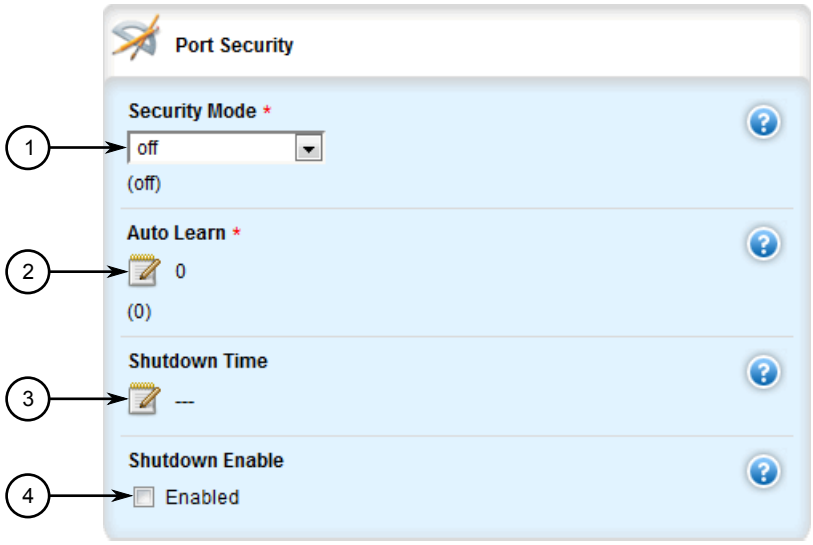


Figure 139: Port Security Form

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

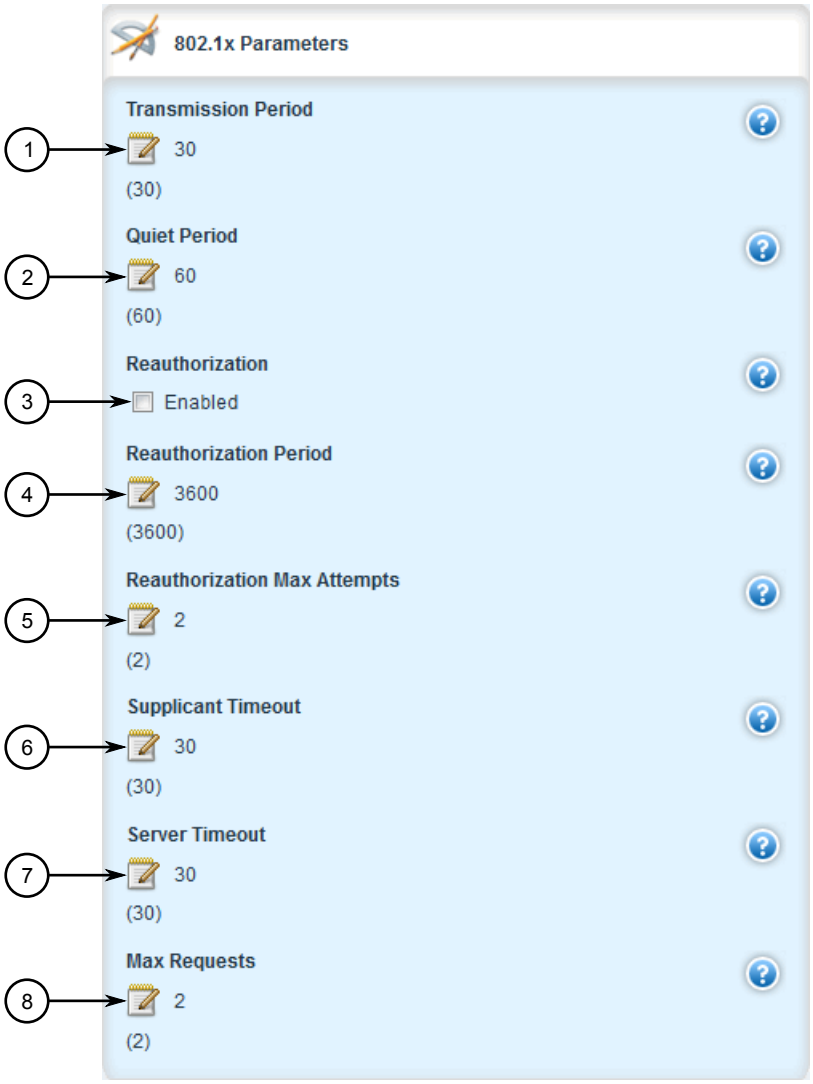


Figure 140: 802.1x Parameters

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:

NOTE
If `Shutdown Enable` is enabled and `Shutdown Time` is not defined, the port will remain disabled following a security violation until manually reset.

Parameter	Description
Security Mode	**Synopsis:** { dot1x_mac_auth, dot1x, per_macaddress, off } **Default:** off The security mode for the port. Options include: • `dot1x_mac_auth` - IEEE 802.1X with MAC authentication protocols are applied to the port. Until the client is authenticated by an IEEE 802.1X server, only EAPoL packets

Parameter	Description
	or packets from other network control protocols are forwarded. If the client does not support IEEE 802.1X supplicant functionality, the router sends the client's MAC address to server as the username and password for authentication. • `dot1x` - IEEE 802.1X authentication protocols are applied to the port. Until the client is authenticated by an IEEE 802.1X server, only EAPoL packets or packets from other network control protocols are forwarded. • `per_macaddress` - Only packets from authorized MAC addresses are forwarded. Authorized MAC addresses are either preconfigured in the static MAC address table or learned dynamically. • `off` - Disables security on the port
Auto Learn	**Synopsis:** A 32-bit signed integer between 0 and 16 **Default:** 0 The maximum number of MAC addresses that can be learned dynamically by the port. This includes static MAC addresses defined in the Static MAC Address table. Therefore, the actual number of learned MAC addresses is this number minus the number of addresses defined in the Static MAC Address table. Security Mode must be set to either `per_macaddress` or `dot1x_mac_auth`.
Shutdown Time	**Synopsis:** A 32-bit signed integer between 1 and 86400 The time in seconds (s) the port will be disabled if a security violation occurs. Shutdown Enable must be enabled.
Shutdown Enable	When enabled, the port is automatically shut down if a security violation occurs. The port is enabled automatically after the period of time specified by Shutdown Time.

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

Parameter	Description
Transmission Period	**Synopsis:** A 32-bit signed integer between 1 and 65535 **Default:** 30 The maximum time in seconds (s) allowed for one full set of packets to be transferred between the port and its client.
Quiet Period	**Synopsis:** A 32-bit signed integer between 0 and 65535 **Default:** 60 The time in seconds (s) to wait before retransmitting EAPoL packets to the client after a failed authentication session.
Reauthorization	When enabled, the port will attempt to reauthenticate the client periodically. The period of time between each reauthentication attempt is specified by Reauthentication Period. The port is considered unauthorized when the maximum number of reauthentication attempts (as defined by Reauthentication Max Attempts) is exceeded.
Reauthorization Period	**Synopsis:** A 32-bit signed integer between 60 and 86400 **Default:** 3600 The period of time in seconds (s) the port will wait before attempting to reauthenticate the client. Reauthentication must be enabled.
Reauthorization Max Attempts	**Synopsis:** A 32-bit signed integer between 1 and 10 **Default:** 2 The maximum number of unsuccessful reauthentication attempts allowed, after which the client is considered unauthorized. Reauthentication must be enabled.
Supplicant Timeout	**Synopsis:** A 32-bit signed integer between 1 and 300 **Default:** 30

Parameter	Description
	The period of time in seconds (s) the port will wait to receive the client's response to the authentication server's request. If no response is received by the end of this period, the authentication session fails.
Server Timeout	**Synopsis:** A 32-bit signed integer between 1 and 300 **Default:** 30 The period of time in seconds (s) the port will wait to receive the authentication server's response to the client's request. If no response is received by the end of this period, the authentication session fails.
Max Requests	**Synopsis:** A 32-bit signed integer between 1 and 10 **Default:** 2 The maximum number of times the port will attempt to forward the authentication server's request to the client. If none of these attempts are successful, the authentication session fails.

5. If IEEE 802.1x standard authentication or IEEE 802.1x with MAC authentication is selected, configure a primary and secondary RADIUS server. For more information, refer to Section 6.6.3.3, "Configuring RADIUS Authentication for Switched Ethernet Ports".
6. 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 6.5.3

Viewing the Security Status of Switched Ethernet Ports

To view the current security status of a 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 security status of the port is displayed on the **Port Security Status** form.

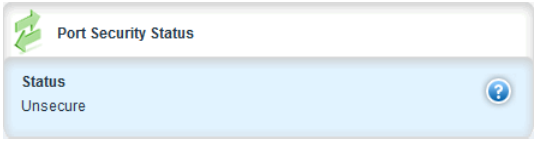


Figure 141: Port Security Status Form

Section 6.6

Managing User Authentication

This section describes the various methods for authenticating users.

CONTENTS

Section 6.6.1

Setting the User Authentication Mode

The user authentication mode controls whether user log in attempts are authenticated locally, by a RADIUS server, or by a TACACS+ server.

To set the authentication mode, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to ***admin » authentication***. The **Authentication** form appears.

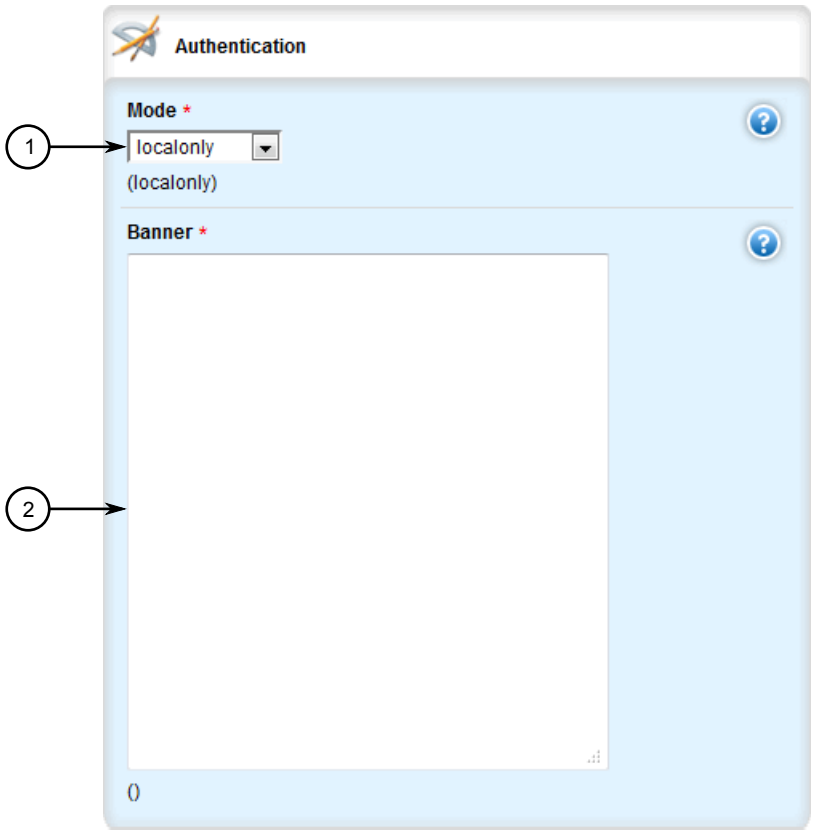


Figure 142: Authentication Form

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.
- If **tacacsplus_local** is selected, users will be authenticated against the configured TACACS+ server. If the user cannot be authenticated, they will then be authenticated locally.
- If **tacacsplus_only** is selected, users will be authenticated against the configured TACACS+ server. If the user cannot be authenticated, authentication is considered failed and no further authentication is attempted.

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 6.6.2

Managing User Authentication Keys

A user authentication key is the public key in an SSH key pair. When using a RUGGEDCOM ROX II user account associated with an authentication key, users can access the device via Secure Shell (SSH) without having to provide a password/passphrase, as long as their workstation holds the matching private key.

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

CONTENTS

Section 6.6.2.1

Determining Which Keys are Associated to a User

To list the user authentication keys associated with a user account, Navigate to ***admin » users » {profile} » authorized-keys***, where *{profile}* is the desired user profile (i.e. admin, guest or oper). The **Authorized Keys** table appears.

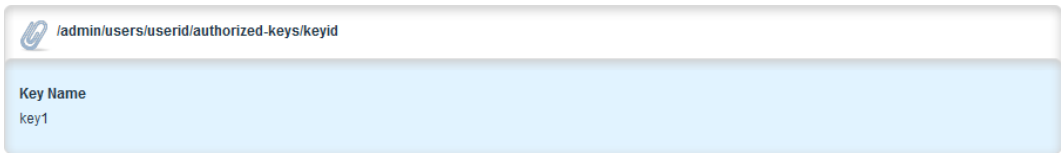


Figure 143: Authorized Keys Table

For information about associating keys with user accounts, refer to Section 6.6.2.4, "Associating/Disassociating a User Authentication Key".

Section 6.6.2.2
Adding a User Authentication Key

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

CAUTION!
Security hazard – risk of unauthorized access and/or exploitation. Do not share the private key outside the organization or with untrusted personnel. The private key is used to decrypt all encrypted correspondences with the associated public key.

IMPORTANT!
It is strongly recommended to apply an encryption passphrase during the key creation process. The passphrase will be applied to the private key and prevent malicious users from accessing its contents.

NOTE
Only SSH-2 RSA keys are supported.

1. On the workstation that will access the device, create a pair of RSA-based public and private SSH keys.
2. Open the public key and copy its contents.
3. Log in to RUGGEDCOM ROX II. For more information, refer to Section 2.2, "Logging In".
4. Navigate to ***security » crypto » authorized keys*** and click **<Add authorized keys>**. The **Key Settings** form appears.

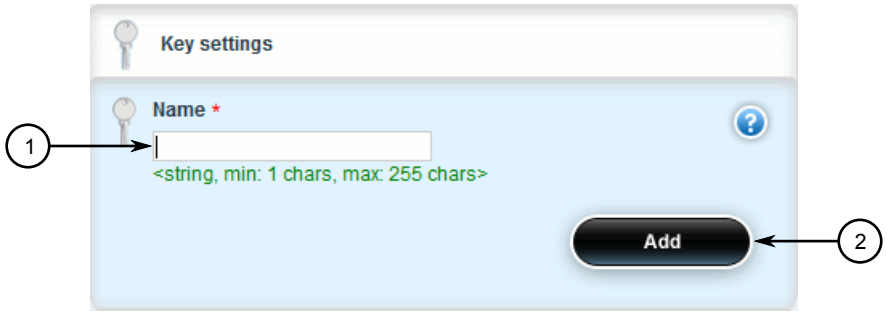


Figure 144: Key Settings Form

1. Name Box **2.** Add Button

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

Parameter	Description
Name	**Synopsis:** A string 1 to 255 characters long The name of the key.

6. Click **Add**. The **Authorized Key Settings** form appears.

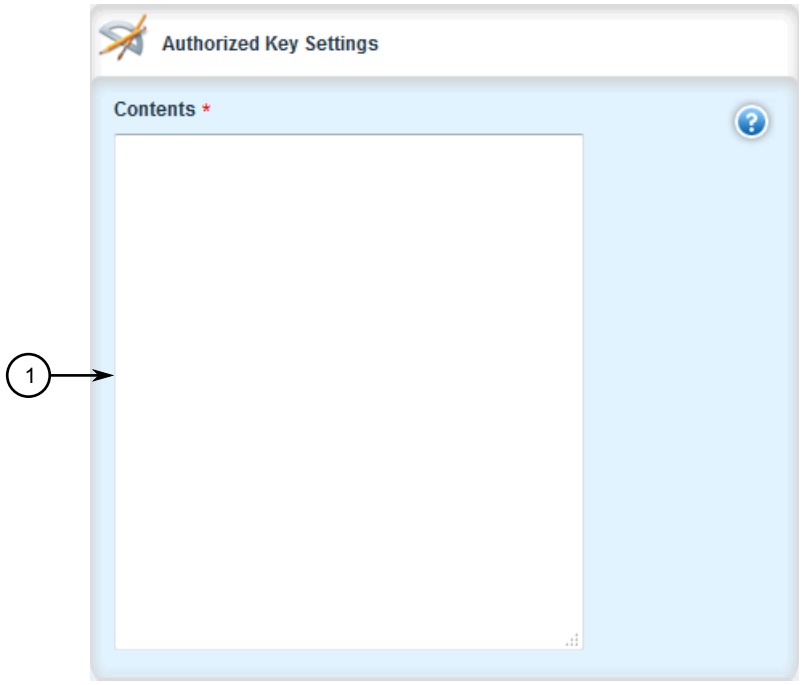


Figure 145: Authorized Key Settings Form

1. Contents Box

7. Paste the contents of the public key into the **Contents** box.
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.
10. Associate the new authentication key with one or more user accounts. For more information, refer to Section 6.6.2.4, "Associating/Disassociating a User Authentication Key".

Section 6.6.2.3
Deleting a User Authentication Key

To delete a user authentication key from the device, do the following::

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to ***security » crypto » authorized keys***. The **Authorized Keys** table appears.

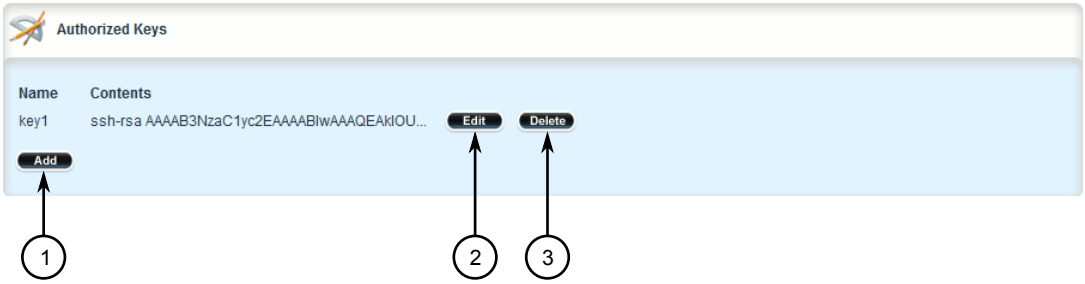


Figure 146: Authorized Keys Table

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

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 6.6.2.4

Associating/Disassociating a User Authentication Key

One or more user authentication keys can be associated with a single user account, allowing users to access the device from different workstations when needed.

IMPORTANT!
The matching public key must reside on the user's workstation for them to log in to the device without a password/passphrase.

» Associating an Authentication Key

To associate one of the authentication keys available on the device with a user account, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to ***admin » users » {profile} » authorized-keys***, where *{profile}* is the desired user profile (i.e. admin, guest or oper).
3. Click **<Add keyid>**. The **Key Settings** form appears.

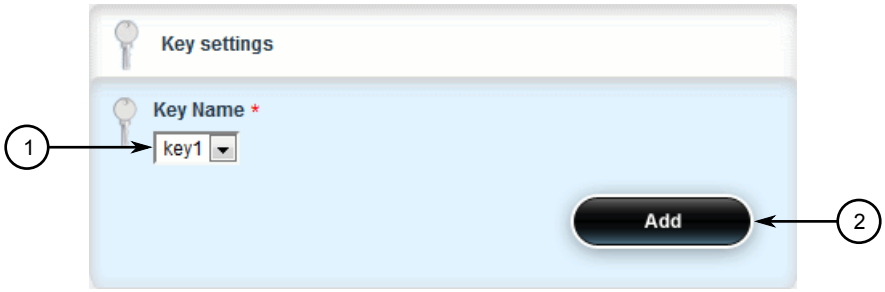


Figure 147: Key Settings Form

1. Key Name Box **2.** Add Button

4. Under **Key Name** select the desired authentication key and then click **Add**. If the desired authentication key is not present, add the key. For more information, refer to Section 6.6.2.2, "Adding a User Authentication Key".
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.

» Disassociating an Authentication Key

To disassociate one of the authentication keys from a user account, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to ***admin » users » {profile} » authorized-keys***, where *{profile}* is the desired user profile (i.e. admin, guest or oper). The **Authorized Keys** table appears.

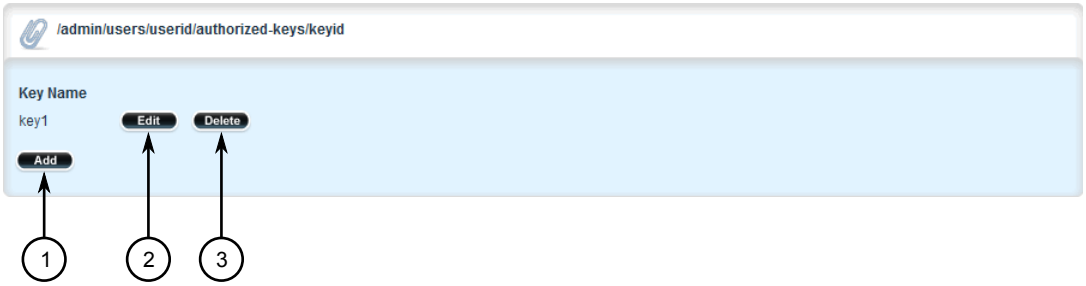


Figure 148: Authorized Keys Form

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

3. Click **Delete** next to the desired authentication 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 6.6.3

Managing RADIUS Authentication

RADIUS is a UDP-based protocol used for carrying authentication, authorization and configuration information between a Network Access Server (NAS) that desires to authenticate its links and a shared authentication server. It provides centralized authentication and authorization for network access.

RADIUS is also widely used in conjunction with the IEEE 802.1x standard for port security using the Extensible Authentication Protocol (EAP).

NOTE
For more information about the RADIUS protocol, refer to RFC 2865 [http://tools.ietf.org/html/rfc2865].

For more information about the Extensible Authentication Protocol (EAP), refer to RFC 3748 [http://tools.ietf.org/html/rfc3748].

IMPORTANT!
*The user authentication mode must be set to **radius_local** for users to be authenticated against the RADIUS server. For more information about setting the authentication mode, refer to Section 6.6.1, "Setting the User Authentication Mode".*

IMPORTANT!
RADIUS messages are sent as UDP messages. The switch and the RADIUS server must use the same authentication and encryption key.

In a RADIUS access request, the following attributes and values are typically sent by the RADIUS client to the RADIUS server:

Attribute	Value
User-Name	{ Guest, Operator, Admin }
User-Password	{ password }
Service-Type	1
Vendor-Specific	Vendor-ID: 15004 Type: 1 Length: 11 String: RuggedCom

A RADIUS server may also be used to authenticate access on ports with IEEE 802.1x security enabled. When this is required, the following attributes are sent by the RADIUS client to the RADIUS server:

Attribute	Value
User-Name	{ The user name as derived from the client's EAP identity response }
NAS-IP-Address	{ The Network Access Server IP address }
Service-Type	2
Frame-MTU	1500
EAP-Message[a]	{ A message(s) received from the authenticating peer }

[a] *EAP-Message is an extension attribute for RADIUS, as defined by RFC 2869 [http://freeradius.org/rfc/rfc2869.html#EAP-Message].*

Primary and secondary RADIUS servers, typically operating from a common database, can be configured for redundancy. If the first server does not respond to an authentication request, the request will be forwarded to the second server until a positive/negate acknowledgment is received.

NOTE
RADIUS authentication activity is logged to the authentication log file `var/log/auth.log`. *Details of each authentication including the time of occurrence, source and result are included. For more information about the authentication log file, refer to Section 4.10.1, "Viewing Logs".*

RUGGEDCOM ROX II supports RADIUS authentication for the LOGIN and PPP services. Different RADIUS servers can be configured to authenticate both services separately or in combination.

The LOGIN services consist of the following access types:

- Local console logins via the serial port
- Remote shell logins via SSH and HTTPS
- Secure file transfers using HTTPS, SCP and SFTP (based on SSH)

Authentication requests for LOGIN services will attempt to use RADIUS first and any local authentication settings will be ignored. Only when there is no response (positive/negative) from any of the configured RADIUS servers will RUGGEDCOM ROX II authenticate users locally.

The PPP service represents incoming PPP connections via a modem. Authentication requests to the PPP service use RADIUS only. In the event that no response is received from any configured RADIUS server, RUGGEDCOM ROX II will not complete the authentication request.

CONTENTS

Section 6.6.3.1
Configuring RADIUS Authentication for LOGIN Services

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 **RADIUS NAS Settings**, **Primary Radius Server** and **Secondary Radius Server** forms appear.

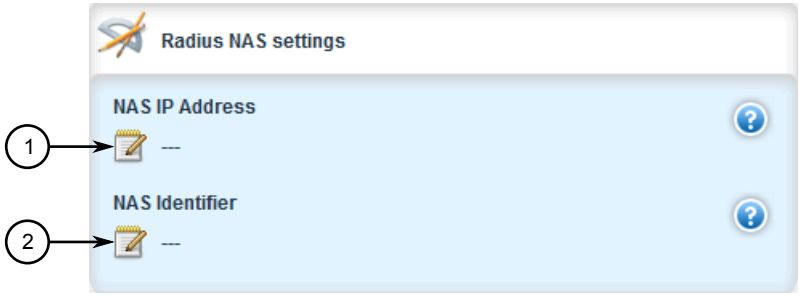


Figure 149: RADIUS NAS Settings Form

1. NAS IP Address Box **2.** NAS Identifier Box

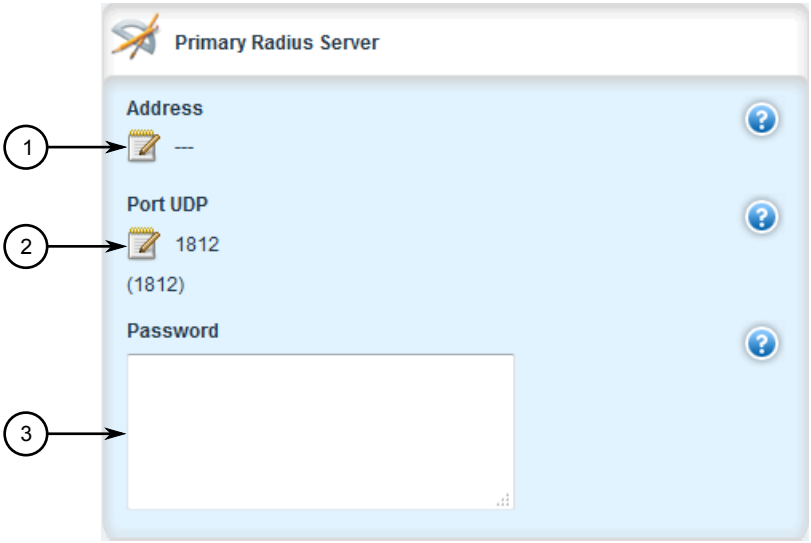


Figure 150: Primary Radius Server Form

1. Address Box **2.** Port UDP Box **3.** Password Box

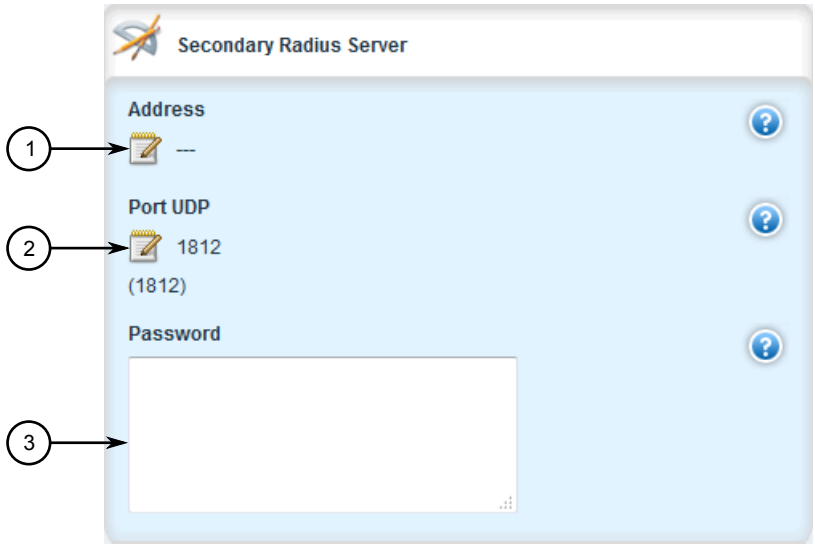


Figure 151: Secondary Radius Server Form

1. Address Box **2.** Port UDP Box **3.** Password Box

3. [Optional] If port security is enabled on any ports, on the **RADIUS NAS Settings** form, configure the following parameters as required to avoid conflicts with firewall rules/policies:

Parameter	Description
NAS IP Address	**Synopsis:** A string 7 to 15 characters long or a string 6 to 40 characters long The NAS-IP-Address. Set this to the primary IP address of the unit.
NAS Identifier	**Synopsis:** A string 1 to 64 characters long The NAS-Identifier. If not set, the hostname will be used as the NAS-Identifier.

4. On the **Primary Radius Server** and **Secondary Radius Server** forms, configure the following parameters as required:

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

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 6.6.3.2
Configuring RADIUS Authentication for PPP Services

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

IMPORTANT!
Passwords are case-sensitive.

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to ***global » ppp » radius***. The **Primary Radius Server** and **Secondary Radius Server** forms appear.

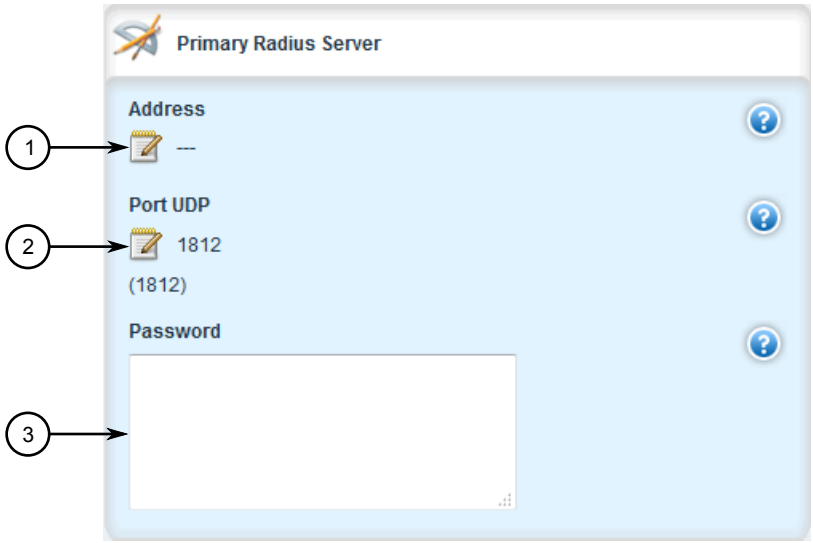


Figure 152: Primary Radius Server Form

1. Address Box **2.** Port UDP Box **3.** Password Box

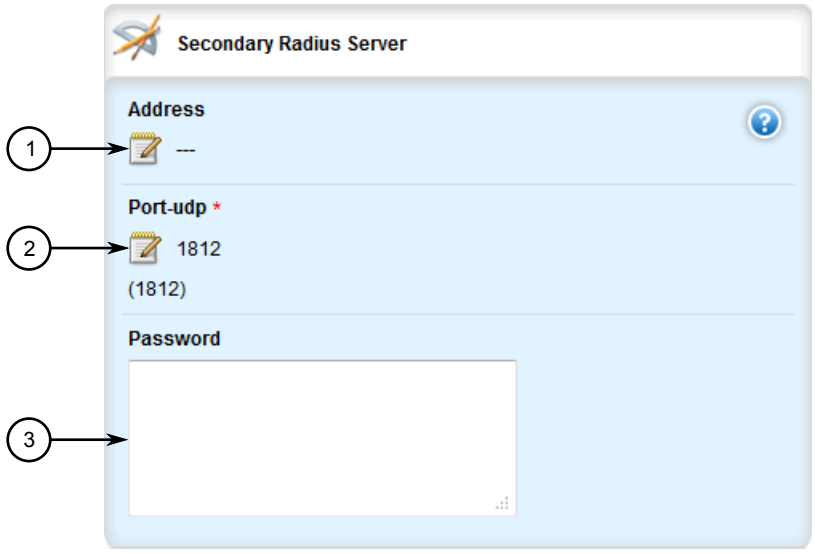


Figure 153: Secondary Radius Server Form

1. Address Box **2.** Port UDP Box **3.** Password Box

3. In both forms, configure the following parameters as required:

Parameter	Description
address	**Synopsis:** A string 7 to 15 characters long The IPv4 address of the server.
UDP Port	**Synopsis:** A 32-bit signed integer between 1 and 65535 **Default:** 1812
password	**Synopsis:** 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 6.6.3.3

Configuring RADIUS Authentication for Switched Ethernet Ports

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

IMPORTANT!
Passwords are case-sensitive.

1. 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.

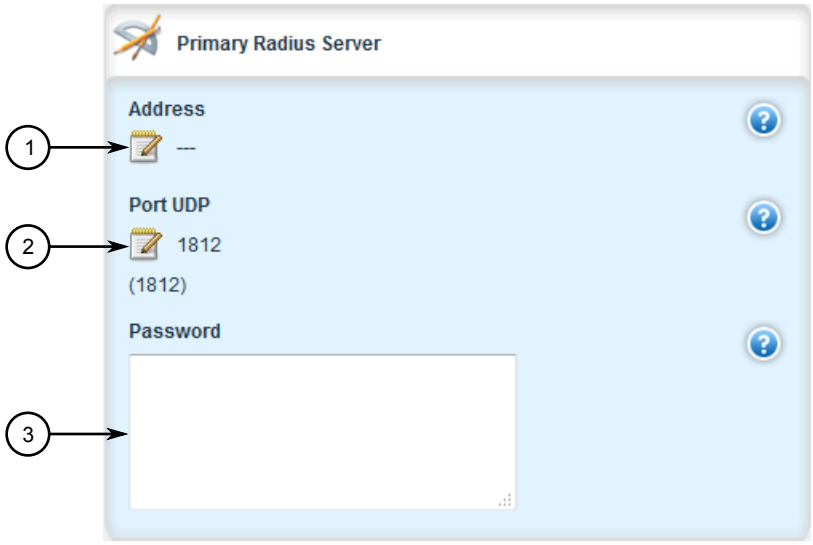


Figure 154: Primary Radius Server Form

1. Address Box **2.** Port UDP Box **3.** Password Box

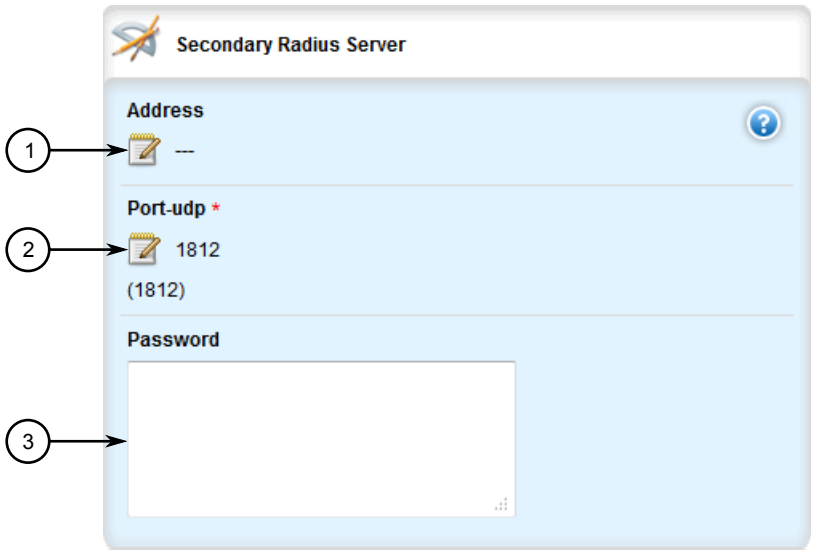


Figure 155: Secondary Radius Server Form

1. Address Box **2.** Port UDP Box **3.** Password Box

3. In both forms, configure the following parameters as required:

Parameter	Description
address	**Synopsis:** A string 7 to 15 characters long The IPv4 address of the server.
UDP Port	**Synopsis:** A 32-bit signed integer between 1 and 65535

Parameter	Description
	Default: 1812 The IPv4 port of the server.
password	**Synopsis:** A string The password of the 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 6.6.4

Configuring TACACS+ Authentication

TACACS+ (Terminal Access Controller Access-Control System Plus) is a TCP-based protocol which provides access control for routers, network access servers and other networked computing devices via one or more centralized servers. TACACS+ provides separate authentication, authorization and accounting services.

Primary and secondary TACACS+ servers, typically operating from a common database, can be configured for redundancy. If the first server does not respond to an authentication request, the request will be forwarded to the second server until a positive/negate acknowledgment is received.

IMPORTANT!
*The user authentication mode must be set to **tacacsplus_local** or **tacacsplus_only** for users to be authenticated against the TACACS+ server. For more information about setting the authentication mode, refer to Section 6.6.1, "Setting the User Authentication Mode".*

To configure TACACS+ authentication, do the following:

IMPORTANT!
Passwords are case-sensitive.

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to ***admin » authentication » tacacsplus***. The **Tacacsplus Server Privilege Settings**, **Primary Tacacsplus Server** and **Secondary Tacacsplus Server** forms appear.

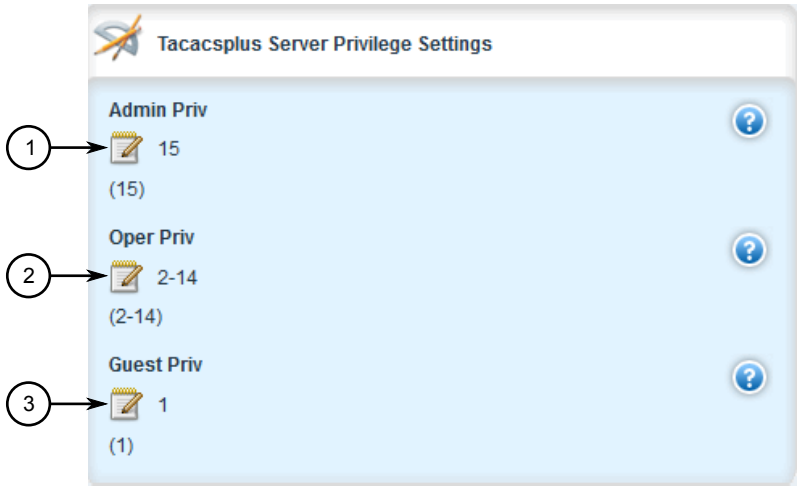


Figure 156: Tacacsplus Server Privilege Settings Form

1. Admin Priv Box **2.** Oper Priv Box **3.** Guest Priv Box

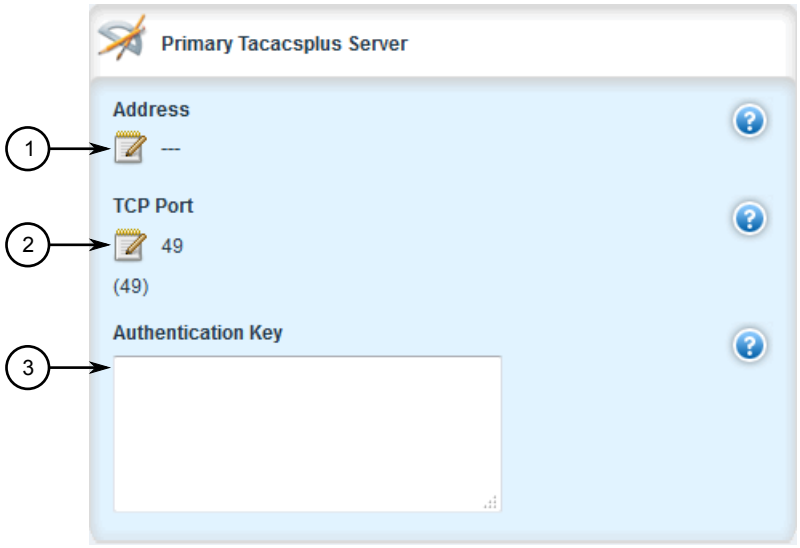


Figure 157: Primary Tacacsplus Server Form

1. Address Box **2.** TCP Port Box **3.** Authentication Key Box

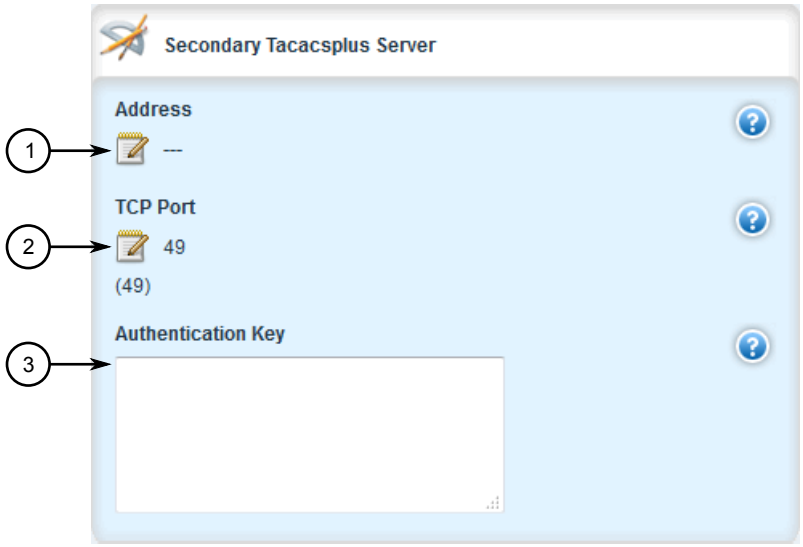


Figure 158: Secondary Tacacsplus Server Form

1. Address Box **2.** TCP Port Box **3.** Authentication Key Box

3. On the **Tacacsplus Server Privilege Settings** form, configure the following parameters as required:

Parameter	Description
Admin Privilege Levels	**Synopsis:** A string 1 to 5 characters long **Default:** 15 The privilege level(s) for administrator (admin) users. Options include any number between 0 and 15, or a range (e.g. 4-12).
Oper Privilege Levels	**Synopsis:** A string 1 to 5 characters long **Default:** 2-14 The privilege level(s) for operator (oper) users. Options include any number between 0 and 15, or a range (e.g. 4-12).
Guest Privilege Levels	**Synopsis:** A string 1 to 5 characters long **Default:** 1 The privilege level(s) for guest users. Options include any number between 0 and 15, or a range (e.g. 4-12).

4. On the **Primary Tacacsplus Server** form, configure the following parameters as required:

Parameter	Description
address	**Synopsis:** A string 7 to 15 characters long or a string 6 to 40 characters long The IP address of the TACACS+ server.
TCP Port	**Synopsis:** A 32-bit signed integer between 1 and 65535 **Default:** 49 The TCP port to use when connecting the TACACS+ server. The default port is 49.
Authentication Key	**Synopsis:** A string The authentication key to use for encrypting and decrypting TACACS+ traffic. Use only ASCII characters.

5. On the **Secondary Tacacsplus Server** form, configure the following parameters as required:

Parameter	Description
address	**Synopsis:** A string 7 to 15 characters long or a string 6 to 40 characters long The IP address of the TACACS+ server.
TCP Port	**Synopsis:** A 32-bit signed integer between 1 and 65535 **Default:** 49 The TCP port to use when connecting the TACACS+ server. The default port is 49.
Authentication Key	**Synopsis:** A string The authentication key to use for encrypting and decrypting TACACS+ traffic. Use only ASCII characters.

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 6.7

Managing Certificates and Keys

RUGGEDCOM ROX II uses X.509v3 certificates and keys to establish secure connections for remote logins (SSH) and Web access (SSL).

To allow for initial configuration, all RUGGEDCOM ROX II devices are shipped from the factory with a pair of pre-installed default certificates and keys. Certificates and keys for TLS and SSH are also auto-generated during initial boot-up and can be replaced by user-defined certificates and keys. Auto-generated certificates are self-signed.

Siemens recommends that all certificates be replaced by ones signed by a trusted Certificate Authority (CA).

NOTE
Only admin users can read/write certificates and keys on the device.

CONTENTS

Section 6.7.1

Viewing the Local Host SSH/RSA Public Key

To view the local host SSH/RSA public key, navigate to ***security » cyrypto***. The **Localhost SSH RSA Public Key** form appears.

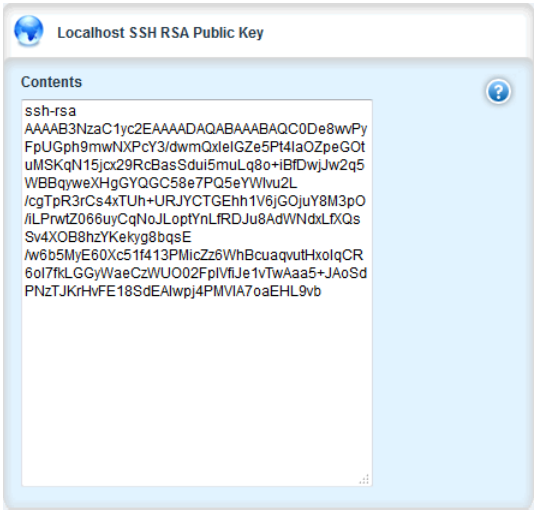


Figure 159: Localhost SSH RSA Public Key Form

Section 6.7.2

Managing the Trusted Certificate Store

The Trusted Certificate Store includes an extensive collection of publically available X.509 v3 root certificates. Once enabled and associated with one or more Certified Authorities (CAs), these certificates are available for all HTTPS or FTPS operations.

For a list of root certificates included in the Trusted Certificate Store, refer to Section 6.7.2.3, "List of Root Certificates in the Trusted Certificate Store".

NOTE
The Trusted Certificate Store is disabled by default.

NOTE
Custom certificates may be required for select features, such as IPsec tunnels. For more information about adding, a custom certificate, refer to Section 6.7.7.3, "Adding a Certificate".

CONTENTS

Section 6.7.2.1
Configuring the Trusted Certificate Store

To configure the Trusted Certificate Store, do the following:

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

Section 6.7.2.2
Enabling/Disabling the Trusted Certificate Store

To enable or disable the Trusted Certificate Store, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to ***admin » system-ca-certificates***. The **System CA Certificates** form appears.

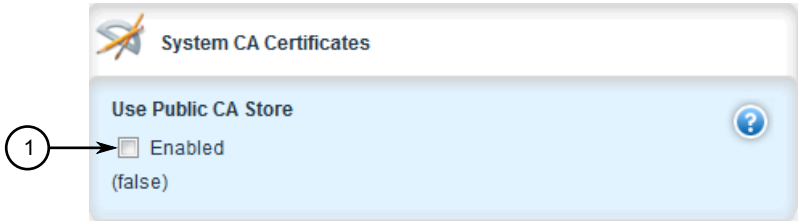


Figure 160: System CA Certificates Form

1. Use Public CA Store Check Box

3. Under **Use Public CA Store**, click **Enabled** to enable the Trusted Certificate Store, or clear **Enabled** to disable the Store.
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 6.7.2.3
List of Root Certificates in the Trusted Certificate Store

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

- **spi-cacert-2008.crt**
  Subject Name: /C=US/ST=Indiana/L=Indianapolis/O=Software in the Public Interest/OU=hostmaster/CN=Certificate Authority/emailAddress=hostmaster@spi-inc.org
  Fingerprint: AF:70:88:43:83:82:02:15:CD:61:C6:BC:EC:FD:37:24:A9:90:43:1C
  Issued: May 13 08:07:56 2008 GMT

Expires: May 11 08:07:56 2018 GMT

- **Go_Daddy_Class_2_CA.crt**
  Subject Name: /C=US/O=The Go Daddy Group, Inc./OU=Go Daddy Class 2 Certification Authority

  Fingerprint: 27:96:BA:E6:3F:18:01:E2:77:26:1B:A0:D7:77:70:02:8F:20:EE:E4

  Issued: Jun 29 17:06:20 2004 GMT

  Expires: Jun 29 17:06:20 2034 GMT
- **Staat_der_Nederlanden_EV_Root_CA**
  Subject Name: /C=NL/O=Staat der Nederlanden/CN=Staat der Nederlanden EV Root CA

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

  Issued: Dec 8 11:19:29 2010 GMT

  Expires: Dec 8 11:10:28 2022 GMT
- **Certinomis_-_Root_CA**
  Subject Name: /C=FR/O=Certinomis/OU=0002 433998903/CN=Certinomis - Root CA

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

  Issued: Oct 21 09:17:18 2013 GMT

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

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

  Issued: Dec 1 15:00:32 2014 GMT

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

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

  Issued: Mar 19 18:33:33 2001 GMT

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

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

  Issued: Aug 1 12:00:00 2013 GMT

  Expires: Jan 15 12:00:00 2038 GMT
- **Entrust.net_Premium_2048_Secure_Server_CA**
  Subject Name: /O=Entrust.net/OU=www.entrust.net/CPS_2048 incorp. by ref. (limits liab.)/OU=(c) 1999 Entrust.net Limited/CN=Entrust.net Certification Authority (2048)

  Fingerprint: 50:30:06:09:1D:97:D4:F5:AE:39:F7:CB:E7:92:7D:7D:65:2D:34:31

  Issued: Dec 24 17:50:51 1999 GMT

Expires: Jul 24 14:15:12 2029 GMT

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

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

  Issued: Apr 30 08:07:01 2013 GMT

  Expires: Apr 28 08:07:01 2023 GMT

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

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

  Issued: May 18 00:00:00 1998 GMT

  Expires: Aug 1 23:59:59 2028 GMT

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

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

  Issued: Jul 9 17:28:50 1999 GMT

  Expires: Jul 9 17:36:58 2019 GMT

- **AC_RaÃz_CerticÃ¡mara_S.A.**
  Subject Name: /C=CO/O=Sociedad Cameral de CertificacixC3xB3n Digital - CerticxC3xA1mara S.A./CN=AC RaxC3xADz CerticxC3xA1mara S.A.

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

  Issued: Nov 27 20:46:29 2006 GMT

  Expires: Apr 2 21:42:02 2030 GMT

- **IGC_A**
  Subject Name: /C=FR/ST=France/L=Paris/O=PM/SGDN/OU=DCSSI/CN=IGC/A/emailAddress=igca@sgdn.pm.gouv.fr

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

  Issued: Dec 13 14:29:23 2002 GMT

  Expires: Oct 17 14:29:22 2020 GMT

- **Verisign_Class_1_Public_Primary_Certification_Authority**
  Subject Name: /C=US/O=VeriSign, Inc./OU=Class 1 Public Primary Certification Authority

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

  Issued: Jan 29 00:00:00 1996 GMT

  Expires: Aug 2 23:59:59 2028 GMT

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

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

  Issued: Jan 29 14:20:24 2010 GMT

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

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

  Issued: Nov 14 11:28:42 2013 GMT

  Expires: Nov 13 23:00:00 2028 GMT
- **Swisscom_Root_CA_1**
  Subject Name: /C=ch/O=Swisscom/OU=Digital Certificate Services/CN=Swisscom Root CA 1

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

  Issued: Aug 18 12:06:20 2005 GMT

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

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

  Issued: Mar 24 11:32:18 2004 GMT

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

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

  Issued: Apr 6 07:29:40 2001 GMT

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

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

  Issued: Apr 2 00:00:00 2008 GMT

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

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

  Issued: Jan 1 00:00:00 2004 GMT

  Expires: Dec 31 23:59:59 2028 GMT

- **DigiCert_Global_Root_G3**
  Subject Name: /C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert Global Root G3

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

  Issued: Aug 1 12:00:00 2013 GMT

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

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

  Issued: Nov 20 21:19:58 2003 GMT

  Expires: Nov 20 21:19:58 2017 GMT
- **Deutsche_Telekom_Root_CA_2**
  Subject Name: /C=DE/O=Deutsche Telekom AG/OU=T-TeleSec Trust Center/CN=Deutsche Telekom Root CA 2

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

  Issued: Jul 9 12:11:00 1999 GMT

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

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

  Issued: Oct 18 12:00:50 2007 GMT

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

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

  Issued: Sep 30 21:12:19 2000 GMT

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

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

  Issued: Jan 1 00:00:00 2004 GMT

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

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

Issued: Dec 25 18:37:19 2007 GMT

Expires: Dec 22 18:37:19 2017 GMT

- **Certplus_Class_2_Primary_CA**
  Subject Name: /C=FR/O=Certplus/CN=Class 2 Primary CA

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

  Issued: Jul 7 17:05:00 1999 GMT

  Expires: Jul 6 23:59:59 2019 GMT
- **IdenTrust_Public_Sector_Root_CA_1**
  Subject Name: /C=US/O=IdenTrust/CN=IdenTrust Public Sector Root CA 1

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

  Issued: Jan 16 17:53:32 2014 GMT

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

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

  Issued: Oct 30 10:10:30 2010 GMT

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

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

  Issued: Dec 17 09:23:49 2002 GMT

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

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

  Issued: Oct 22 00:00:00 2013 GMT

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

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

  Issued: Nov 10 00:00:00 2006 GMT

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

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

Issued: Nov 10 00:00:00 2006 GMT

Expires: Nov 10 00:00:00 2031 GMT

- **GlobalSign_ECC_Root_CA_-_R4**
  Subject Name: /OU=GlobalSign ECC Root CA - R4/O=GlobalSign/CN=GlobalSign

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

  Issued: Nov 13 00:00:00 2012 GMT

  Expires: Jan 19 03:14:07 2038 GMT
- **AffirmTrust_Premium**
  Subject Name: /C=US/O=AffirmTrust/CN=AffirmTrust Premium

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

  Issued: Jan 29 14:10:36 2010 GMT

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

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

  Issued: Feb 1 00:00:00 2010 GMT

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

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

  Issued: Jul 4 17:20:04 2006 GMT

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

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

  Issued: May 5 09:37:37 2011 GMT

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

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

  Issued: Aug 24 11:37:07 2007 GMT

  Expires: Aug 21 11:37:07 2017 GMT

- **AddTrust_Qualified_Certificates_Root**
  Subject Name: /C=SE/O=AddTrust AB/OU=AddTrust TTP Network/CN=AddTrust Qualified CA Root

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

  Issued: May 30 10:44:50 2000 GMT

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

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

  Issued: Jan 29 14:06:06 2010 GMT

  Expires: Dec 31 14:06:06 2030 GMT
- **UTN_USERFirst_Hardware_Root_CA**
  Subject Name: /C=US/ST=UT/L=Salt Lake City/O=The USERTRUST Network/OU=http://www.usertrust.com/CN=UTN-USERFirst-Hardware

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

  Issued: Jul 9 18:10:42 1999 GMT

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

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

  Issued: Jun 26 02:18:36 2002 GMT

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

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

  Issued: May 30 10:41:50 2000 GMT

  Expires: May 30 10:41:50 2020 GMT
- **thawte_Primary_Root_CA**
  Subject Name: /C=US/O=thawte, Inc./OU=Certification Services Division/OU=(c) 2006 thawte, Inc. - For authorized use only/CN=thawte Primary Root CA

  Fingerprint: 91:C6:D6:EE:3E:8A:C8:63:84:E5:48:C2:99:29:5C:75:6C:81:7B:81

  Issued: Nov 17 00:00:00 2006 GMT

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

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

  Issued: Sep 17 19:46:36 2006 GMT

Expires: Sep 17 19:46:36 2036 GMT

- **StartCom_Certification_Authority_2**
  Subject Name: /C=IL/O=StartCom Ltd./OU=Secure Digital Certificate Signing/CN=StartCom Certification Authority

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

  Issued: Sep 17 19:46:37 2006 GMT

  Expires: Sep 17 19:46:36 2036 GMT
- **Go_Daddy_Root_Certificate_Authority_-_G2**
  Subject Name: /C=US/ST=Arizona/L=Scottsdale/O=GoDaddy.com, Inc./CN=Go Daddy Root Certificate Authority - G2

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

  Issued: Sep 1 00:00:00 2009 GMT

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

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

  Issued: Aug 1 12:00:00 2013 GMT

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

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

  Issued: Jun 21 04:00:00 1999 GMT

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

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

  Issued: Aug 31 07:11:25 2010 GMT

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

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

  Issued: Mar 4 05:00:00 2004 GMT

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

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

Issued: Sep 17 08:28:59 2008 GMT

Expires: Sep 17 08:28:59 2028 GMT

- **NetLock_Notary_=Class_A=_Root**
  Subject Name: /C=HU/ST=Hungary/L=Budapest/O=NetLock Halozatbiztonsagi Kft./OU=Tanusitvanykiadok/CN=NetLock Kozjegyzoi (Class A) Tanusitvanykiado

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

  Issued: Feb 24 23:14:47 1999 GMT

  Expires: Feb 19 23:14:47 2019 GMT
- **WoSign_China**
  Subject Name: /C=CN/O=WoSign CA Limited/CN=CA xE6xB2x83xE9x80x9AxE6xA0xB9xE8xAFx81xE4xB9xA6

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

  Issued: Aug 8 01:00:01 2009 GMT

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

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

  Issued: Jan 29 14:08:24 2010 GMT

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

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

  Issued: Nov 5 08:35:58 2009 GMT

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

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

  Issued: Dec 1 00:00:00 2006 GMT

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

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

  Issued: Jul 19 09:06:56 2012 GMT

  Expires: Jul 19 09:06:56 2042 GMT

- **thawte_Primary_Root_CA_-_G3**
  Subject Name: /C=US/O=thawte, Inc./OU=Certification Services Division/OU=(c) 2008 thawte, Inc. - For authorized use only/CN=thawte Primary Root CA - G3

  Fingerprint: F1:8B:53:8D:1B:E9:03:B6:A6:F0:56:43:5B:17:15:89:CA:F3:6B:F2

  Issued: Apr 2 00:00:00 2008 GMT

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

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

  Issued: May 30 10:48:38 2000 GMT

  Expires: May 30 10:48:38 2020 GMT
- **ACEDICOM_Root**
  Subject Name: /CN=ACEDICOM Root/OU=PKI/O=EDICOM/C=ES

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

  Issued: Apr 18 16:24:22 2008 GMT

  Expires: Apr 13 16:24:22 2028 GMT
- **VeriSign_Class_3_Public_Primary_Certification_Authority_-_G5**
  Subject Name: /C=US/O=VeriSign, Inc./OU=VeriSign Trust Network/OU=(c) 2006 VeriSign, Inc. - For authorized use only/CN=VeriSign Class 3 Public Primary Certification Authority - G5

  Fingerprint: 4E:B6:D5:78:49:9B:1C:CF:5F:58:1E:AD:56:BE:3D:9B:67:44:A5:E5

  Issued: Nov 8 00:00:00 2006 GMT

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

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

  Issued: Jan 16 18:12:23 2014 GMT

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

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

  Issued: Aug 30 14:23:01 2001 GMT

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

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

  Issued: Mar 18 10:00:00 2009 GMT

  Expires: Mar 18 10:00:00 2029 GMT

- **Security_Communication_EV_RootCA1**
  Subject Name: /C=JP/O=SECOM Trust Systems CO.,LTD./OU=Security Communication EV RootCA1

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

  Issued: Jun 6 02:12:32 2007 GMT

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

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

  Issued: Jun 16 11:30:18 2009 GMT

  Expires: Dec 30 11:30:18 2029 GMT
- **QuoVadis_Root_CA_3**
  Subject Name: /C=BM/O=QuoVadis Limited/CN=QuoVadis Root CA 3

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

  Issued: Nov 24 19:11:23 2006 GMT

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

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

  Issued: Jan 19 00:00:00 2010 GMT

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

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

  Issued: Jan 12 14:41:57 2006 GMT

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

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

  Issued: Oct 1 10:40:14 2008 GMT

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

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

Issued: Apr 16 07:09:14 2007 GMT

Expires: Apr 16 07:09:14 2027 GMT

- **COMODO_ECC_Certification_Authority**
  Subject Name: /C=GB/ST=Greater Manchester/L=Salford/O=COMODO CA Limited/CN=COMODO ECC Certification Authority

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

  Issued: Mar 6 00:00:00 2008 GMT

  Expires: Jan 18 23:59:59 2038 GMT
- **Trustis_FPS_Root_CA**
  Subject Name: /C=GB/O=Trustis Limited/OU=Trustis FPS Root CA

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

  Issued: Dec 23 12:14:06 2003 GMT

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

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

  Issued: Sep 1 00:00:00 2009 GMT

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

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

  Issued: Dec 6 13:49:52 2011 GMT

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

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

  Issued: Feb 22 20:39:23 2001 GMT

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

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

  Issued: Aug 1 12:00:00 2013 GMT

  Expires: Jan 15 12:00:00 2038 GMT

- **NetLock_Arany_=Class_Gold=_FÅ‘tanÃ°sÃtvÃ¡ny**
  Subject Name: /C=HU/L=Budapest/O=NetLock Kft./OU=TanxC3xBAsxC3xADtvxC3xA1nykiadxC3xB3k (Certification Services)/CN=NetLock Arany (Class Gold) FxC5x91tanxC3xBAsxC3xADtvxC3xA1ny

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

  Issued: Dec 11 15:08:21 2008 GMT

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

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

  Issued: Apr 6 10:49:13 2001 GMT

  Expires: Apr 6 10:49:13 2021 GMT
- **GeoTrust_Primary_Certification_Authority_-_G2**
  Subject Name: /C=US/O=GeoTrust Inc./OU=(c) 2007 GeoTrust Inc. - For authorized use only/CN=GeoTrust Primary Certification Authority - G2

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

  Issued: Nov 5 00:00:00 2007 GMT

  Expires: Jan 18 23:59:59 2038 GMT
- **Entrust_Root_Certification_Authority_-_EC1**
  Subject Name: /C=US/O=Entrust, Inc./OU=See www.entrust.net/legal-terms/OU=(c) 2012 Entrust, Inc. - for authorized use only/CN=Entrust Root Certification Authority - EC1

  Fingerprint: 20:D8:06:40:DF:9B:25:F5:12:25:3A:11:EA:F7:59:8A:EB:14:B5:47

  Issued: Dec 18 15:25:36 2012 GMT

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

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

  Issued: Jun 29 17:39:16 2004 GMT

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

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

  Issued: Mar 26 11:18:17 2008 GMT

  Expires: Mar 25 11:03:10 2020 GMT
- **Entrust_Root_Certification_Authority_-_G2**
  Subject Name: /C=US/O=Entrust, Inc./OU=See www.entrust.net/legal-terms/OU=(c) 2009 Entrust, Inc. - for authorized use only/CN=Entrust Root Certification Authority - G2

  Fingerprint: 8C:F4:27:FD:79:0C:3A:D1:66:06:8D:E8:1E:57:EF:BB:93:22:72:D4

Issued: Jul 7 17:25:54 2009 GMT

Expires: Dec 7 17:55:54 2030 GMT

- **Camerfirma_Global_Chambersign_Root**
  Subject Name: /C=EU/O=AC Camerfirma SA CIF A82743287/OU=http://www.chambersign.org/CN=Global Chambersign Root

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

  Issued: Sep 30 16:14:18 2003 GMT

  Expires: Sep 30 16:14:18 2037 GMT
- **S-TRUST_Authentication_and_Encryption_Root_CA_2005_PN**
  Subject Name: /C=DE/ST=Baden-Wuerttemberg (BW)/L=Stuttgart/O=Deutscher Sparkassen Verlag GmbH/CN=S-TRUST Authentication and Encryption Root CA 2005:PN

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

  Issued: Jun 22 00:00:00 2005 GMT

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

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

  Issued: Feb 25 14:10:22 1999 GMT

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

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

  Issued: May 12 18:46:00 2000 GMT

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

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

  Issued: Oct 1 00:00:00 1999 GMT

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

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

  Issued: Dec 12 15:00:00 2007 GMT

  Expires: Dec 12 15:00:00 2017 GMT

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

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

  Issued: Dec 18 09:04:10 2013 GMT

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

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

  Issued: Jul 19 09:15:30 2012 GMT

  Expires: Jul 19 09:15:30 2042 GMT
- **Chambers_of_Commerce_Root_-_2008**
  Subject Name: /C=EU/L=Madrid (see current address at www.camerfirma.com/address)/serialNumber=A82743287/O=AC Camerfirma S.A./CN=Chambers of Commerce Root - 2008

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

  Issued: Aug 1 12:29:50 2008 GMT

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

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

  Issued: Aug 1 12:00:00 2013 GMT

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

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

  Issued: Mar 5 12:09:48 2013 GMT

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

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

  Issued: Nov 5 00:00:00 2007 GMT

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

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

Issued: Aug 8 01:00:01 2009 GMT

Expires: Aug 8 01:00:01 2039 GMT

- **Equifax_Secure_Global_eBusiness_CA**
  Subject Name: /C=US/O=Equifax Secure Inc./CN=Equifax Secure Global eBusiness CA-1

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

  Issued: Jun 21 04:00:00 1999 GMT

  Expires: Jun 21 04:00:00 2020 GMT
- **Actalis_Authentication_Root_CA**
  Subject Name: /C=IT/L=Milan/O=Actalis S.p.A./03358520967/CN=Actalis Authentication Root CA

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

  Issued: Sep 22 11:22:02 2011 GMT

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

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

  Issued: Sep 30 16:13:43 2003 GMT

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

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

  Issued: Jan 12 17:27:44 2012 GMT

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

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

  Issued: Oct 22 12:07:37 2008 GMT

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

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

  Issued: Nov 5 08:50:46 2009 GMT

  Expires: Nov 5 08:50:46 2029 GMT

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

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

  Issued: Mar 30 01:47:11 2003 GMT

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

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

  Issued: Jan 1 01:00:01 2010 GMT

  Expires: Dec 31 23:59:01 2039 GMT
- **Buypass_Class_2_CA_1**
  Subject Name: /C=NO/O=Buypass AS-983163327/CN=Buypass Class 2 CA 1

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

  Issued: Oct 13 10:25:09 2006 GMT

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

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

  Issued: Nov 8 00:58:58 2014 GMT

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

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

  Issued: Nov 1 17:14:04 2004 GMT

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

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

  Issued: Jun 24 08:38:14 2011 GMT

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

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

  Issued: Jan 29 00:00:00 1996 GMT

  Expires: Aug 2 23:59:59 2028 GMT

- **TWCA_Root_Certification_Authority**
  Subject Name: /C=TW/O=TAIWAN-CA/OU=Root CA/CN=TWCA Root Certification Authority

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

  Issued: Aug 28 07:24:33 2008 GMT

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

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

  Issued: Mar 4 05:00:00 2004 GMT

  Expires: Mar 4 05:00:00 2029 GMT
- **VeriSign_Universal_Root_Certification_Authority**
  Subject Name: /C=US/O=VeriSign, Inc./OU=VeriSign Trust Network/OU=(c) 2008 VeriSign, Inc. - For authorized use only/CN=VeriSign Universal Root Certification Authority

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

  Issued: Apr 2 00:00:00 2008 GMT

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

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

  Issued: May 18 00:00:00 1998 GMT

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

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

  Issued: Oct 26 08:28:58 2010 GMT

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

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

  Issued: Sep 1 12:00:00 1998 GMT

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

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

  Issued: Oct 1 00:00:00 1999 GMT

Expires: Jul 16 23:59:59 2036 GMT

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

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

  Issued: Dec 28 16:51:00 2010 GMT

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

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

  Issued: Nov 24 18:27:00 2006 GMT

  Expires: Nov 24 18:23:33 2031 GMT
- **T-TeleSec_GlobalRoot_Class_3**
  Subject Name: /C=DE/O=T-Systems Enterprise Services GmbH/OU=T-Systems Trust Center/CN=T-TeleSec GlobalRoot Class 3

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

  Issued: Oct 1 10:29:56 2008 GMT

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

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

  Issued: Oct 25 08:36:00 2006 GMT

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

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

  Issued: Jun 11 10:46:39 2002 GMT

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

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

  Issued: Aug 17 00:21:09 2006 GMT

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

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

Issued: Jun 29 15:13:05 2007 GMT

Expires: Jun 29 15:13:05 2027 GMT

- **SecureTrust_CA**
  Subject Name: /C=US/O=SecureTrust Corporation/CN=SecureTrust CA

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

  Issued: Nov 7 19:31:18 2006 GMT

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

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

  Issued: Oct 25 08:32:46 2006 GMT

  Expires: Oct 25 08:32:46 2036 GMT
- **Taiwan_GRCA**
  Subject Name: /C=TW/O=Government Root Certification Authority

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

  Issued: Dec 5 13:23:33 2002 GMT

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

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

  Issued: Dec 13 17:07:54 2007 GMT

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

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

  Issued: May 30 10:38:31 2000 GMT

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

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

  Issued: Nov 10 00:00:00 2006 GMT

  Expires: Nov 10 00:00:00 2031 GMT
- **VeriSign_Class_3_Public_Primary_Certification_Authority_-_G4**
  Subject Name: /C=US/O=VeriSign, Inc./OU=VeriSign Trust Network/OU=(c) 2007 VeriSign, Inc. - For authorized use only/CN=VeriSign Class 3 Public Primary Certification Authority - G4

Fingerprint: 22:D5:D8:DF:8F:02:31:D1:8D:F7:9D:B7:CF:8A:2D:64:C9:3F:6C:3A

Issued: Nov 5 00:00:00 2007 GMT

Expires: Jan 18 23:59:59 2038 GMT

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

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

  Issued: May 18 00:00:00 1998 GMT

  Expires: Aug 1 23:59:59 2028 GMT
- **CFCA_EV_ROOT**
  Subject Name: /C=CN/O=China Financial Certification Authority/CN=CFCA EV ROOT

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

  Issued: Aug 8 03:07:01 2012 GMT

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

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

  Issued: Jun 27 06:28:33 2012 GMT

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

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

  Issued: Apr 8 04:56:47 2009 GMT

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

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

  Issued: Nov 27 00:00:00 2006 GMT

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

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

  Issued: Aug 22 16:41:51 1998 GMT

  Expires: Aug 22 16:41:51 2018 GMT
- **Entrust_Root_Certification_Authority**
  Subject Name: /C=US/O=Entrust, Inc./OU=www.entrust.net/CPS is incorporated by reference/OU=(c) 2006 Entrust, Inc./CN=Entrust Root Certification Authority

Fingerprint: B3:1E:B1:B7:40:E3:6C:84:02:DA:DC:37:D4:4D:F5:D4:67:49:52:F9

Issued: Nov 27 20:23:42 2006 GMT

Expires: Nov 27 20:53:42 2026 GMT

- **Network_Solutions_Certificate_Authority**
  Subject Name: /C=US/O=Network Solutions L.L.C./CN=Network Solutions Certificate Authority

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

  Issued: Dec 1 00:00:00 2006 GMT

  Expires: Dec 31 23:59:59 2029 GMT
- **QuoVadis_Root_CA_3_G3**
  Subject Name: /C=BM/O=QuoVadis Limited/CN=QuoVadis Root CA 3 G3

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

  Expires: Jan 12 20:26:32 2012 GMT

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

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

  Issued: Sep 30 04:20:49 2003 GMT

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

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

  Issued: Sep 1 00:00:00 2009 GMT

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

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

  Issued: Dec 15 08:00:00 2006 GMT

  Expires: Dec 15 08:00:00 2021 GMT
- **Global_Chambersign_Root_-_2008**
  Subject Name: /C=EU/L=Madrid (see current address at www.camerfirma.com/address)/serialNumber=A82743287/O=AC Camerfirma S.A./CN=Global Chambersign Root - 2008

  Fingerprint: 4A:BD:EE:EC:95:0D:35:9C:89:AE:C7:52:A1:2C:5B:29:F6:D6:AA:0C

  Issued: Aug 1 12:31:40 2008 GMT

  Expires: Jul 31 12:31:40 2038 GMT

- **Comodo_Trusted_Services_root**
  Subject Name: /C=GB/ST=Greater Manchester/L=Salford/O=Comodo CA Limited/CN=Trusted Certificate Services

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

  Issued: Jan 1 00:00:00 2004 GMT

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

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

  Issued: Nov 7 19:42:28 2006 GMT

  Expires: Dec 31 19:52:06 2029 GMT
- **SwissSign_Gold_CA_-_G2**
  Subject Name: /C=CH/O=SwissSign AG/CN=SwissSign Gold CA - G2

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

  Issued: Oct 25 08:30:35 2006 GMT

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

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

  Issued: Feb 25 14:08:11 1999 GMT

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

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

  Issued: Nov 13 00:00:00 2012 GMT

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

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

  Issued: Jul 7 14:58:30 2011 GMT

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

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

  Issued: Jul 6 16:22:47 2001 GMT

  Expires: Jul 1 15:22:47 2021 GMT

- **Hongkong_Post_Root_CA_1**
  Subject Name: /C=HK/O=Hongkong Post/CN=Hongkong Post Root CA 1

  Fingerprint: D6:DA:A8:20:8D:09:D2:15:4D:24:B5:2F:CB:34:6E:B2:58:B2:8A:58

  Issued: May 15 05:13:14 2003 GMT

  Expires: May 15 04:52:29 2023 GMT
- **Security_Communication_RootCA2**
  Subject Name: /C=JP/O=SECOM Trust Systems CO.,LTD./OU=Security Communication RootCA2

  Fingerprint: 5F:3B:8C:F2:F8:10:B3:7D:78:B4:CE:EC:19:19:C3:73:34:B9:C7:74

  Issued: May 29 05:00:39 2009 GMT

  Expires: May 29 05:00:39 2029 GMT
- **QuoVadis_Root_CA_2_G3**
  Subject Name: /C=BM/O=QuoVadis Limited/CN=QuoVadis Root CA 2 G3

  Fingerprint: 09:3C:61:F3:8B:8B:DC:7D:55:DF:75:38:02:05:00:E1:25:F5:C8:36

  Issued: Jan 12 18:59:32 2012 GMT

  Expires: Jan 12 18:59:32 2042 GMT
- **OISTE_WISeKey_Global_Root_GA_CA**
  Subject Name: /C=CH/O=WISeKey/OU=Copyright (c) 2005/OU=OISTE Foundation Endorsed/CN=OISTE WISeKey Global Root GA CA

  Fingerprint: 59:22:A1:E1:5A:EA:16:35:21:F8:98:39:6A:46:46:B0:44:1B:0F:A9

  Issued: Dec 11 16:03:44 2005 GMT

  Expires: Dec 11 16:09:51 2037 GMT
- **Verisign_Class_3_Public_Primary_Certification_Authority**
  Subject Name: /C=US/O=VeriSign, Inc./OU=Class 3 Public Primary Certification Authority

  Fingerprint: 74:2C:31:92:E6:07:E4:24:EB:45:49:54:2B:E1:BB:C5:3E:61:74:E2

  Issued: Jan 29 00:00:00 1996 GMT

  Expires: Aug 1 23:59:59 2028 GMT
- **Microsec_e-Szigno_Root_CA**
  Subject Name: /C=HU/L=Budapest/O=Microsec Ltd./OU=e-Szigno CA/CN=Microsec e-Szigno Root CA

  Fingerprint: 23:88:C9:D3:71:CC:9E:96:3D:FF:7D:3C:A7:CE:FC:D6:25:EC:19:0D

  Issued: Apr 6 12:28:44 2005 GMT

  Expires: Apr 6 12:28:44 2017 GMT
- **Izenpe.com**
  Subject Name: /C=ES/O=IZENPE S.A./CN=Izenpe.com

  Fingerprint: 2F:78:3D:25:52:18:A7:4A:65:39:71:B5:2C:A2:9C:45:15:6F:E9:19

  Issued: Dec 13 13:08:28 2007 GMT

  Expires: Dec 13 08:27:25 2037 GMT

- **Buypass_Class_2_Root_CA**
  Subject Name: /C=NO/O=Buypass AS-983163327/CN=Buypass Class 2 Root CA

  Fingerprint: 49:0A:75:74:DE:87:0A:47:FE:58:EE:F6:C7:6B:EB:C6:0B:12:40:99

  Issued: Oct 26 08:38:03 2010 GMT

  Expires: Oct 26 08:38:03 2040 GMT
- **GeoTrust_Global_CA**
  Subject Name: /C=US/O=GeoTrust Inc./CN=GeoTrust Global CA

  Fingerprint: DE:28:F4:A4:FF:E5:B9:2F:A3:C5:03:D1:A3:49:A7:F9:96:2A:82:12

  Issued: May 21 04:00:00 2002 GMT

  Expires: May 21 04:00:00 2022 GMT
- **GlobalSign_Root_CA_-_R2**
  Subject Name: /OU=GlobalSign Root CA - R2/O=GlobalSign/CN=GlobalSign

  Fingerprint: 75:E0:AB:B6:13:85:12:27:1C:04:F8:5F:DD:DE:38:E4:B7:24:2E:FE

  Issued: Dec 15 08:00:00 2006 GMT

  Expires: Dec 15 08:00:00 2021 GMT
- **Certification_Authority_of_WoSign_G2**
  Subject Name: /C=CN/O=WoSign CA Limited/CN=Certification Authority of WoSign G2

  Fingerprint: FB:ED:DC:90:65:B7:27:20:37:BC:55:0C:9C:56:DE:BB:F2:78:94:E1

  Issued: Nov 8 00:58:58 2014 GMT

  Expires: Nov 8 00:58:58 2044 GMT
- **Autoridad_de_Certificacion_Firmaprofesional_CIF_A62634068**
  Subject Name: /C=ES/CN=Autoridad de Certificacion Firmaprofesional CIF A62634068

  Fingerprint: AE:C5:FB:3F:C8:E1:BF:C4:E5:4F:03:07:5A:9A:E8:00:B7:F7:B6:FA

  Issued: May 20 08:38:15 2009 GMT

  Expires: Dec 31 08:38:15 2030 GMT
- **EC-ACC**
  Subject Name: /C=ES/O=Agencia Catalana de Certificacio (NIF Q-0801176-I)/OU=Serveis Publics de Certificacio/OU=Vegeu https://www.catcert.net/verarrel (c)03/OU=Jerarquia Entitats de Certificacio Catalanes/CN=EC-ACC

  Fingerprint: 28:90:3A:63:5B:52:80:FA:E6:77:4C:0B:6D:A7:D6:BA:A6:4A:F2:E8

  Issued: Jan 7 23:00:00 2003 GMT

  Expires: Jan 7 22:59:59 2031 GMT
- **USERTrust_ECC_Certification_Authority**
  Subject Name: /C=US/ST=New Jersey/L=Jersey City/O=The USERTRUST Network/CN=USERTrust ECC Certification Authority

  Fingerprint: D1:CB:CA:5D:B2:D5:2A:7F:69:3B:67:4D:E5:F0:5A:1D:0C:95:7D:F0

  Issued: Feb 1 00:00:00 2010 GMT

Expires: Jan 18 23:59:59 2038 GMT

- **Swisscom_Root_EV_CA_2**
  Subject Name: /C=ch/O=Swisscom/OU=Digital Certificate Services/CN=Swisscom Root EV CA 2
  Fingerprint: E7:A1:90:29:D3:D5:52:DC:0D:0F:C6:92:D3:EA:88:0D:15:2E:1A:6B
  Issued: Jun 24 09:45:08 2011 GMT
  Expires: Jun 25 08:45:08 2031 GMT
- **CA_Disig**
  Subject Name: /C=SK/L=Bratislava/O=Disig a.s./CN=CA Disig
  Fingerprint: 2A:C8:D5:8B:57:CE:BF:2F:49:AF:F2:FC:76:8F:51:14:62:90:7A:41
  Issued: Mar 22 01:39:34 2006 GMT
  Expires: Mar 22 01:39:34 2016 GMT
- **ePKI_Root_Certification_Authority**
  Subject Name: /C=TW/O=Chunghwa Telecom Co., Ltd./OU=ePKI Root Certification Authority
  Fingerprint: 67:65:0D:F1:7E:8E:7E:5B:82:40:A4:F4:56:4B:CF:E2:3D:69:C6:F0
  Issued: Dec 20 02:31:27 2004 GMT
  Expires: Dec 20 02:31:27 2034 GMT
- **GeoTrust_Global_CA_2**
  Subject Name: /C=US/O=GeoTrust Inc./CN=GeoTrust Global CA 2
  Fingerprint: A9:E9:78:08:14:37:58:88:F2:05:19:B0:6D:2B:0D:2B:60:16:90:7D
  Issued: Mar 4 05:00:00 2004 GMT
  Expires: Mar 4 05:00:00 2019 GMT
- **Verisign_Class_3_Public_Primary_Certification_Authority_-_G3**
  Subject Name: /C=US/O=VeriSign, Inc./OU=VeriSign Trust Network/OU=(c) 1999 VeriSign, Inc. - For authorized use only/CN=VeriSign Class 3 Public Primary Certification Authority - G3
  Fingerprint: 13:2D:0D:45:53:4B:69:97:CD:B2:D5:C3:39:E2:55:76:60:9B:5C:C6
  Issued: Oct 1 00:00:00 1999 GMT
  Expires: Jul 16 23:59:59 2036 GMT

Section 6.7.3

Managing CA Certificates for the Trusted Certificate Store

To establish trust between the device and an endpoint (e.g. server, portal, etc.), add the necessary CA certificates to the Trusted Certificate Store.

CONTENTS

- Section 6.7.3.3, "Deleting a CA Certificate from the Trusted Certificate Store"

Section 6.7.3.1
Viewing a List of CA Certificates Added to the Trusted Certificate Store

To view a list of CA certificates added to the Trusted Certificate Store, navigate to ***admin » system-ca-certificates » configured-cas***. If CA certificates have been associated with the Store, the **Configured CAs** table appears.

Figure 161: Configured CAs Table

If no CA certificates have been added to the Store, add certificates as needed. For more information, refer to Section 6.7.3.2, "Adding a CA Certificate to the Trusted Certificate Store".

Section 6.7.3.2
Adding a CA Certificate to the Trusted Certificate Store

To add a CA certificate to the Trusted Certificate Store, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to ***admin » system-ca-certificates » configured-cas*** and click **<Add configured-cas>**. The **Key Settings** form appears.

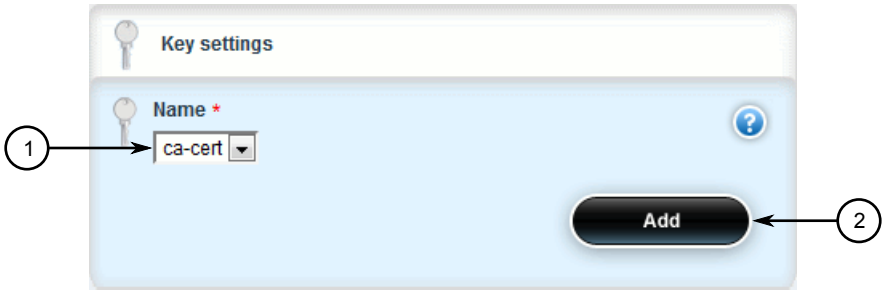


Figure 162: Key Settings Form

1. Name List **2.** Add Button

3. Under **Name**, select one of the available CA certificates configured on the device, and then click **Add**.
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 6.7.3.3
Deleting a CA Certificate from the Trusted Certificate Store

To delete a CA certificate from the Trusted Certificate Store, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to ***admin » system-ca-certificates » configured-cas***. The **Configured CAs** table appears.

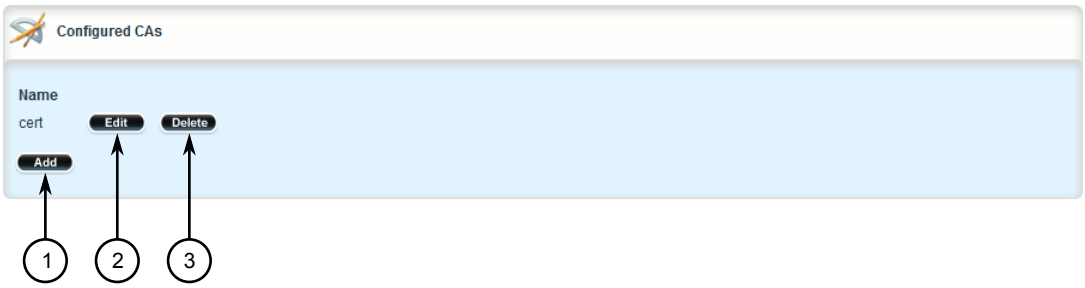


Figure 163: Configured CAs Table

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

3. Click **Delete** next to the chosen CA 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 6.7.4
Managing CA Certificates and CRLs

This section describes how to view, add and delete Certified Authority (CA) certificates and Certificate Revocation Lists (CRLs) on the device.

CONTENTS

Section 6.7.4.1
Viewing a List of CA Certificates and CRLs

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.

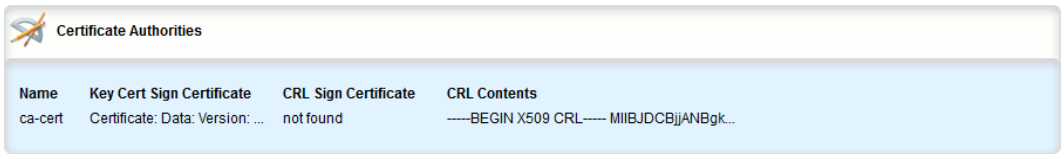


Figure 164: Certificate Authorities Table

If no certificates have been configured, add certificates as needed. For more information, refer to Section 6.7.4.3, "Adding a CA Certificate and CRL".

Section 6.7.4.2

Viewing the Status of a CA Certificate and CRL

To view the status of a CA certificate 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.

Figure 165: Key Cert Sign Certificate Status Form

1. Issuer **2.** Subject **3.** Not Before **4.** Not After

Figure 166: CRL Sign Certificate Status Form

1. Issuer **2.** Subject **3.** Not Before **4.** Not After

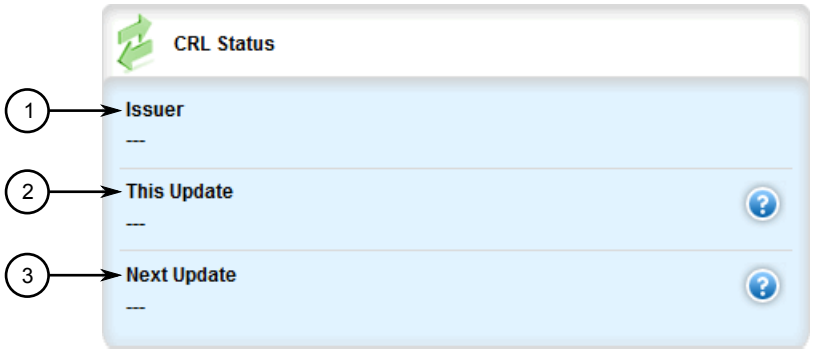


Figure 167: CRL Status Form

1. Issuer **2.** This Update **3.** Next Update

The **Key Cert Sign Certificate Status** form provides the following information:

Parameter	Description
issuer	**Synopsis:** A string
subject	**Synopsis:** A string
Not Before	**Synopsis:** A string This certificate is not valid before this date.
Not After	**Synopsis:** A string This certificate is not valid after this date.

The **CRL Sign Certificate Status** form provides the following information:

Parameter	Description
issuer	**Synopsis:** A string
subject	**Synopsis:** A string

Parameter	Description
Not Before	**Synopsis:** A string This certificate is not valid before this date.
Not After	**Synopsis:** A string This certificate is not valid after this date.

The **CRL Status** form provides the following information:

Parameter	Description
issuer	**Synopsis:** A string
This Update	**Synopsis:** A string This CRL was updated at this date and time.
Next Update	**Synopsis:** A string This certificate must be updated by this date and time.

Section 6.7.4.3
Adding a CA Certificate and CRL

To add a certificate issued by a Certified Authority (CA) and its associated Certificate Revocation List (CRL), do the following:

NOTE
Only admin users can read/write certificates and keys on the device.

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

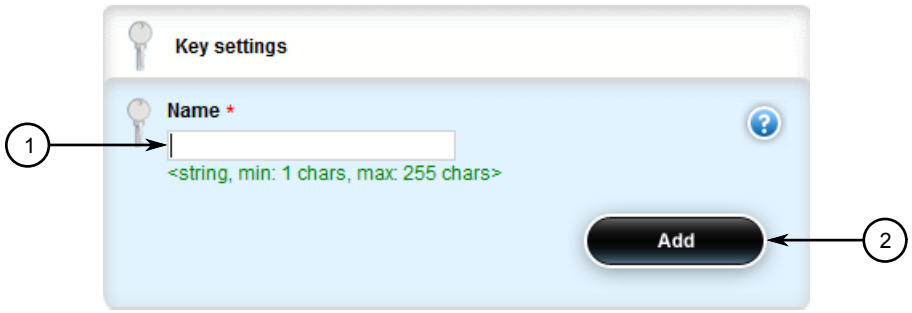


Figure 168: Key Settings Form

1. Name Box **2.** Add Button

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

Parameter	Description
Name	**Synopsis:** A string 1 to 255 characters long The name of the CA certificate.

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

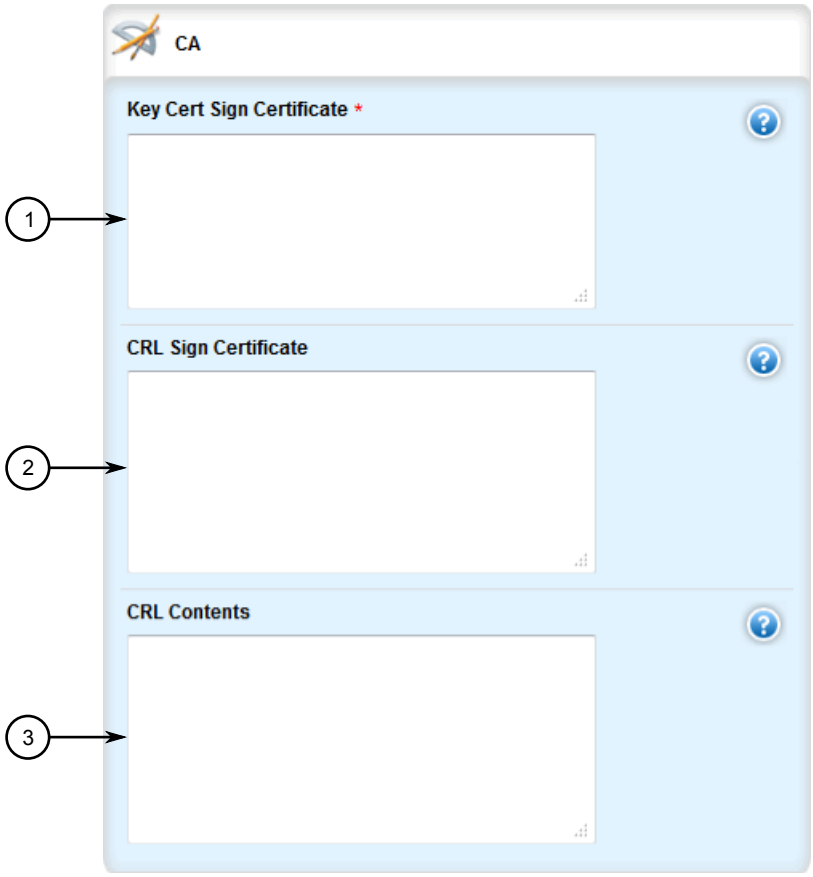


Figure 169: CA Form

1. Key Cert Sign Certificate Box **2.** CRL Sign Certificate Box **3.** CRL Contents Box

5. Copy the contents of the CA certificate into the **Key Cert Sign Certificate** box.

> **NOTE**
> *Large CRLs (bigger than 100KB) are not currently supported and may be difficult to add/view in the configuration.*

6. Add the associated Certificate Revocation List (CRL).
   - If the CRL is signed by a separate certificate, copy the contents of the CRL into the **CRL Sign Certificate** box
   - If the CRL is not signed, copy the contents of the CRL into the **CRL Contents** box
7. 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 6.7.4.4

Deleting a CA Certificate and CRL

To delete a certificate issued by a Certified Authority (CA) and its associated Certificate Revocation List (CRL), do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to ***security » crypto » ca***. The **Certificate Authorities** table appears.

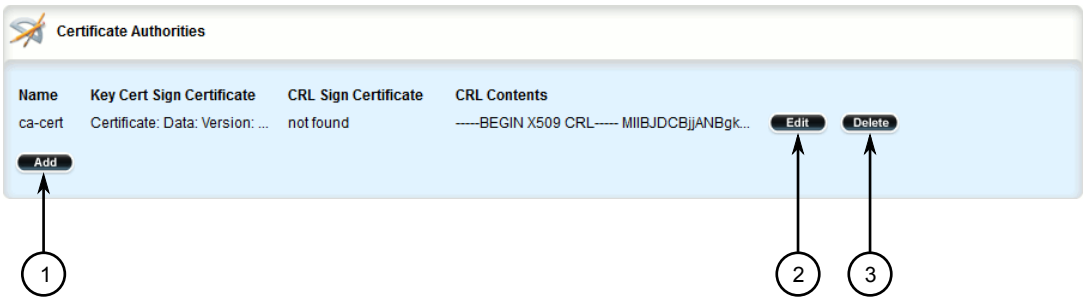


Figure 170: Certificate Authorities Table

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

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 6.7.5

Managing Private Keys

This section describes how to view, add and delete private keys on the device.

NOTE
Private keys are automatically encrypted using an AES-CFB-128 cipher to protect them from being viewed by unauthorized users.

CONTENTS

Section 6.7.5.1
Viewing a List of Private Keys

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.

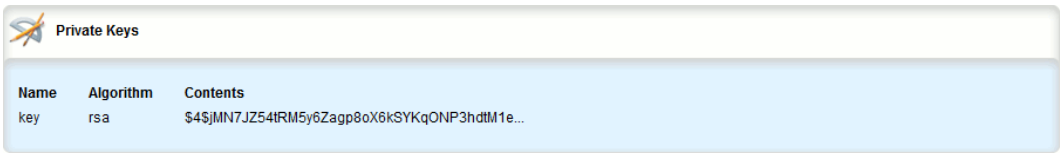


Figure 171: Private Key Table

If no private keys have been configured, add keys as needed. For more information, refer to Section 6.7.5.2, "Adding a Private Key".

Section 6.7.5.2
Adding a Private Key

To add an unsigned private key, do the following:

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.

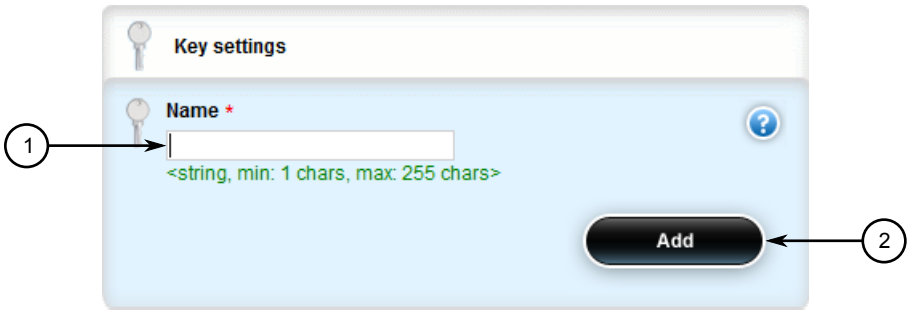


Figure 172: Key Settings Form

1. Name Box **2.** Add Button

3. In the **Key Settings** form, configure the following parameters as required:

Parameter	Description
Name	**Synopsis:** 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.

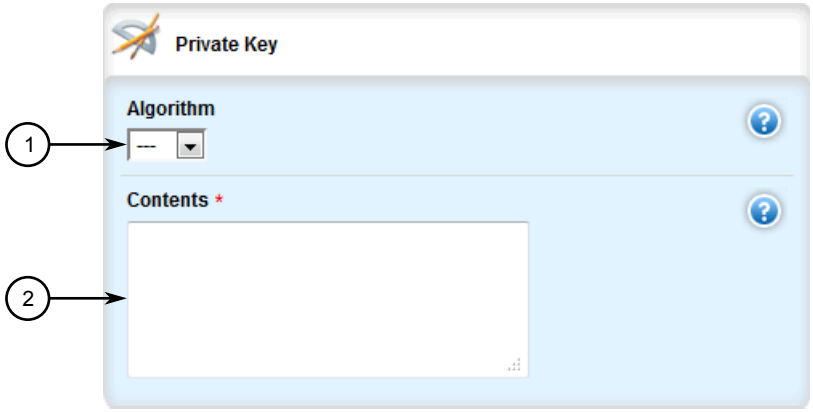


Figure 173: Private Key Form

1. Algorithm List **2.** Contents Box

5. In the **Private Key** form, configure the following parameters as required:

Parameter	Description
Algorithm	**Synopsis:** { rsa, dsa, ssh-rsa } The type of key. This parameter is mandatory.
Contents	**Synopsis:** A string 1 to 8192 characters long The contents of the unsigned private key. This parameter is mandatory.

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 6.7.5.3
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.

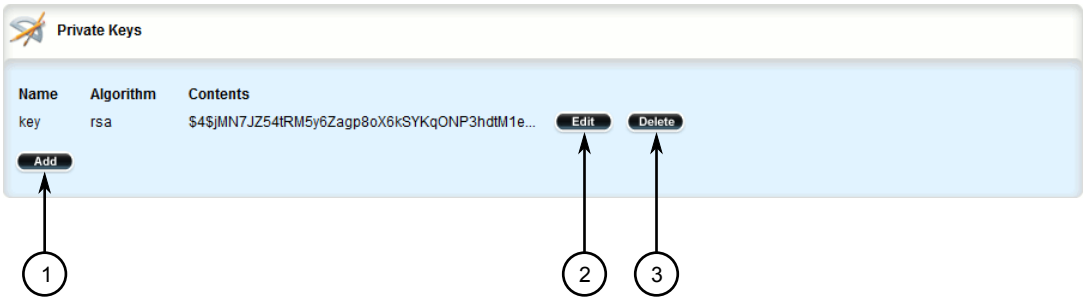


Figure 174: Private Key Table

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 6.7.6

Managing Public Keys

This section describes how to manage public keys on the device.

CONTENTS

Section 6.7.6.1

Viewing a List of Public Keys

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.

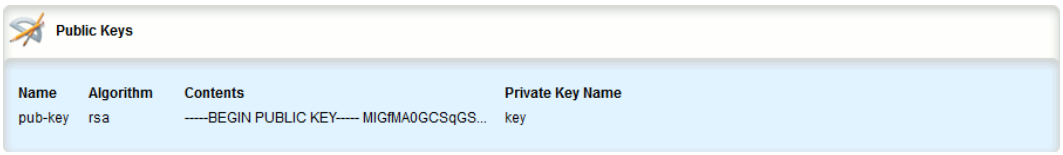


Figure 175: Public Key Table

If no public keys have been configured, add keys as needed. For more information, refer to Section 6.7.6.2, "Adding a Public Key".

Section 6.7.6.2
Adding a Public Key

To add an unsigned public key, do the following:

NOTE
Do not associate the public key with the private key if the public key belongs to another device.

1. Make sure the private key associated with the public key has been added. For more information, refer to Section 6.7.5.2, "Adding a Private Key".
2. Change the mode to **Edit Private** or **Edit Exclusive**.
3. Navigate to ***security » crypto » public-key*** and click **<Add public-key>**. The **Key Settings** form appears.

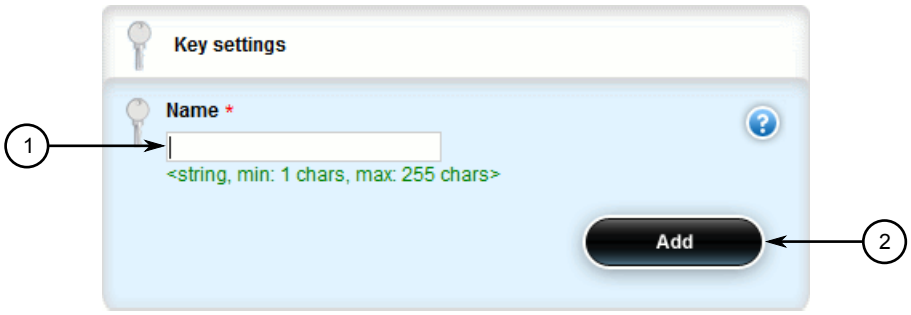


Figure 176: Key Settings Form

1. Name Box **2.** Add Button

4. In the **Key Settings** form, configure the following parameters as required:

Parameter	Description
Name	**Synopsis:** 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.

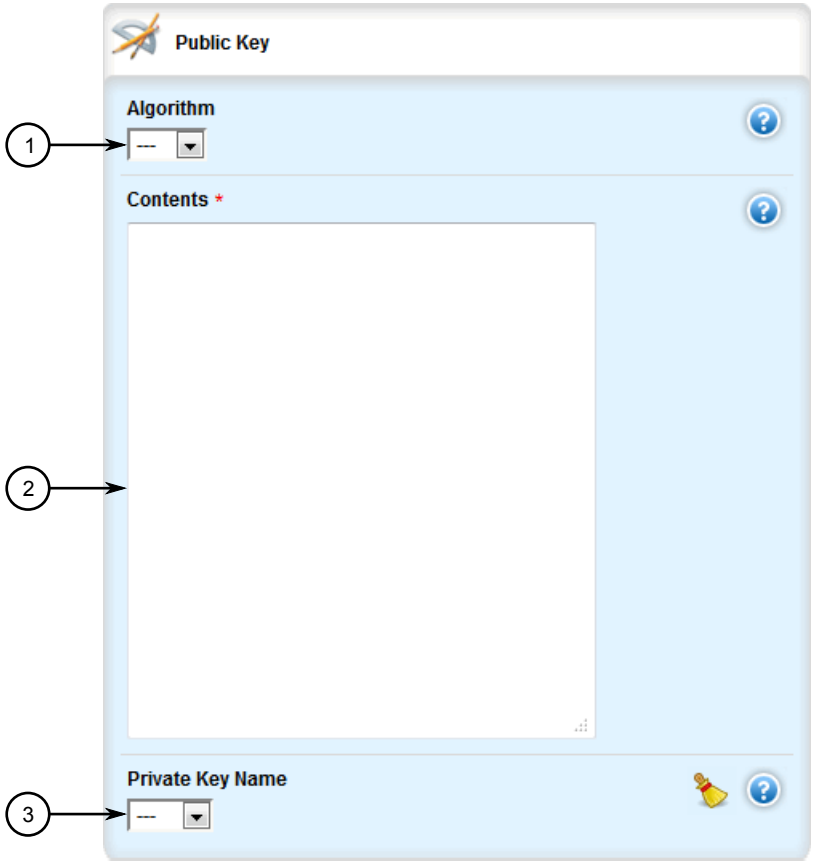


Figure 177: Public Key Form

1. Algorithm List **2.** Contents Box **3.** Private Key Name Box

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 6.7.6.3, "Adding an IPSec-Formatted Public Key".*

Parameter	Description
Algorithm	**Synopsis:** { rsa, dsa, ssh-rsa } The algorithm of the key. This parameter is mandatory.
Contents	**Synopsis:** A string 1 to 8192 characters long The contents of the key. This parameter is mandatory.
Private Key Name	**Synopsis:** A string 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 6.7.6.3
Adding an IPSec-Formatted Public Key

IPSec-formatted public keys from systems that do not support the Privacy-Enhanced Mail (PEM) format, such as RUGGEDCOM ROX devices, can be imported into RUGGEDCOM ROX II and automatically converted.

Once added to the RUGGEDCOM ROX II database, the IPSec-formatted public key is visible via the **System Public Key** form under ***tunnel » ipsec » connection » {name} » {end}***, where *{name}* is the name of the connection and *{end}* is the either the left (local router) or right (remote router) connection end. **Type** must be set to `rsasig` to display the public key.

The public key can be copied from the **System Public Key** form and added to another RUGGEDCOM ROX II device, as described in the following procedure, or to a RUGGEDCOM ROX device.

To add an IPSec-formatted public key and have it converted into PEM format, do the following:

1. Change the mode to **Edit Private** 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 6.7.6.2, "Adding a Public Key".
3. Click **add-ipsec-formatted-public-key** in the menu. The **Add IPSec-Formatted Public Key** and **Trigger Action** forms appears:

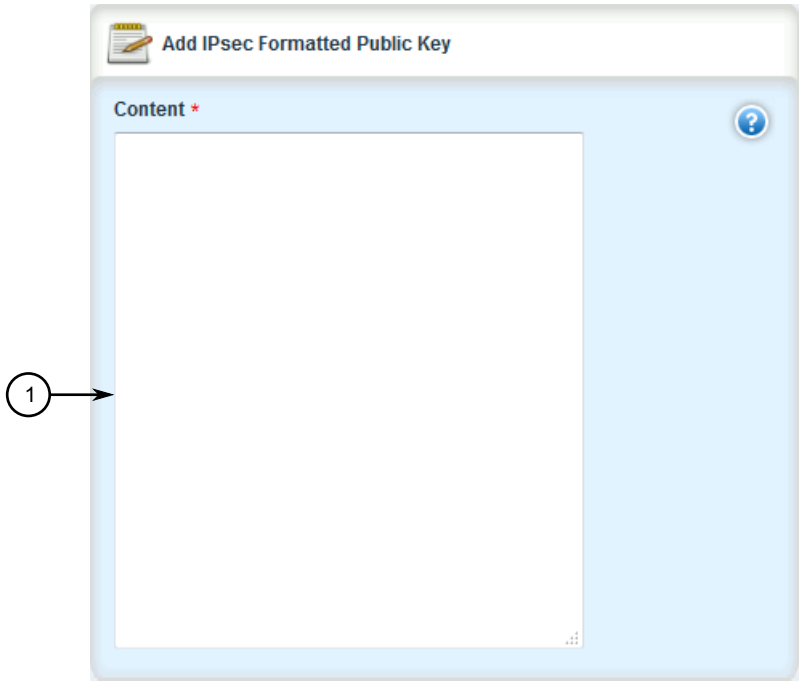


Figure 178: Add IPSec-Formatted Public Key Form

1. Content Box

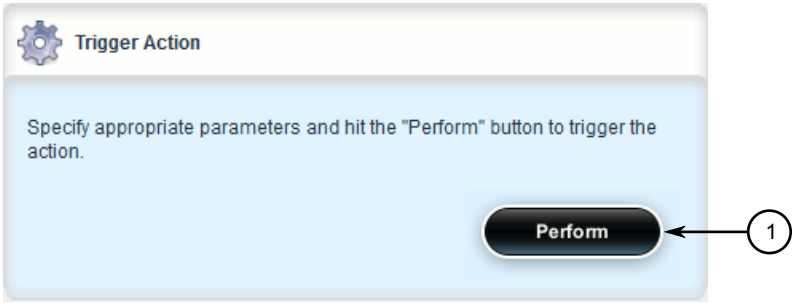


Figure 179: Trigger Action Form

1. Perform Button

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 6.7.6.4

Deleting a Public Key

To delete an unsigned public key, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to ***security » crpto » public-key***. The **Public Key** table appears.

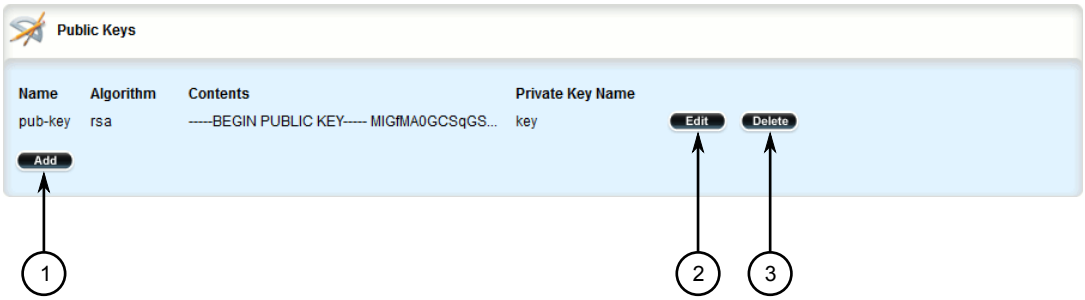


Figure 180: Public Key Table

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

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 6.7.7
Managing Certificates

This section describes how to manage certificates on the device.

CONTENTS

Section 6.7.7.1
Viewing a List of Certificates

To view a list of certificates, navigate to ***security » crypto » certificate***. If certificates have been configured, the **Certificates** table appears.

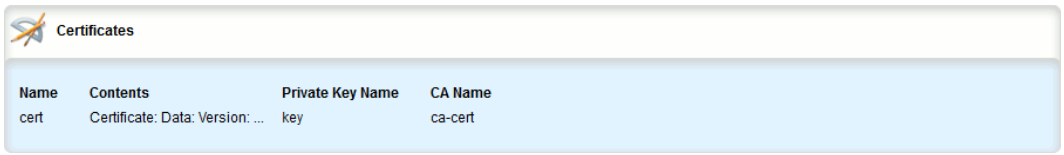


Figure 181: Certificates Table

If no certificates have been configured, add certificates as needed. For more information, refer to Section 6.7.7.3, "Adding a Certificate".

Section 6.7.7.2
Viewing the Status of a Certificate

To view the status of a certificate, navigate to ***security » crypto » certificate » {name}***, where *{name}* is the name of the certificate. The **Certificate Status** form appears.

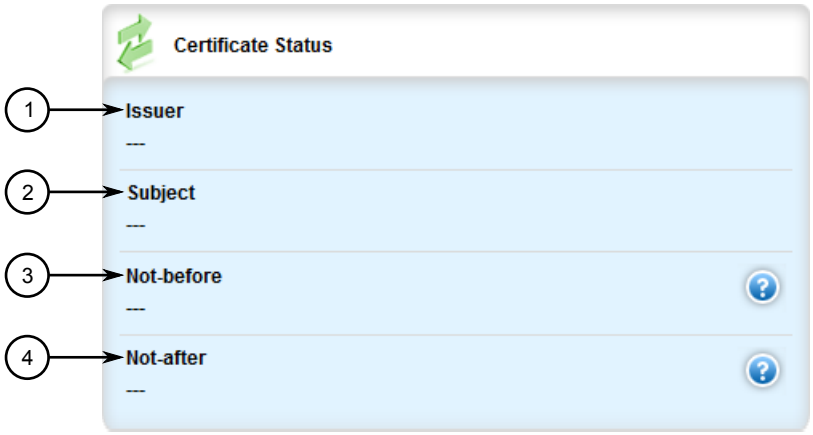


Figure 182: Certificate Status Form

1. Issuer **2.** Subject **3.** Not Before **4.** Not After

This table provides the following information:

Parameter	Description
Issuer	**Synopsis:** A string
Subject	**Synopsis:** A string
Not Before	**Synopsis:** A string This certificate is not valid before this date.
Not After	**Synopsis:** A string This certificate is not valid after this date.

Section 6.7.7.3
Adding a Certificate

To add a certificate, do the following:

NOTE
Only admin users can read/write certificates and keys on the device.

1. Make sure the required CA certificates and/or private keys have been added to the device.
   - For more information about adding CA Certificates, refer to Section 6.7.4.3, "Adding a CA Certificate and CRL"
   - For more information about adding private keys, refer to Section 6.7.5.2, "Adding a Private Key"
2. Change the mode to **Edit Private** or **Edit Exclusive**.
3. Navigate to ***security » crypto » certificate*** and click **<Add certificate>**. The **Key Settings** form appears.

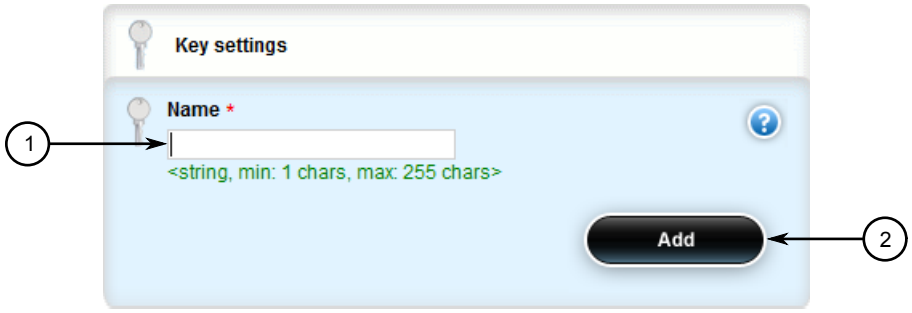


Figure 183: Key Settings Form

1. Name Box **2.** Add Button

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

Parameter	Description
Name	**Synopsis:** A string 1 to 255 characters long The name of the certificate.

5. Click **Add**. The **Certificate** form appears.

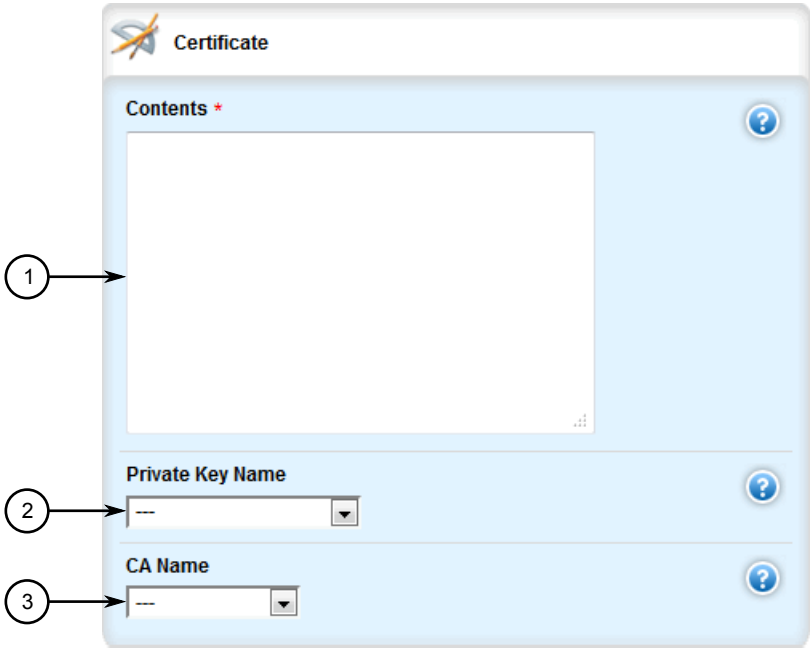


Figure 184: Certificate Form

1. Contents Box **2.** Private Key Name List **3.** CA Certificate Name List

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

Parameter	Description
Contents	**Synopsis:** A string 1 to 8192 characters long The contents of the certificate. This parameter is mandatory.
Private Key Name	**Synopsis:** A string The private key associated with this certificate.
CA Name	**Synopsis:** A string The optional CA certificate for this certificate.

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 6.7.7.4
Deleting a Certificate

To delete a certificate, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to ***security » crypto » certificate***. The **Certificate** table appears.

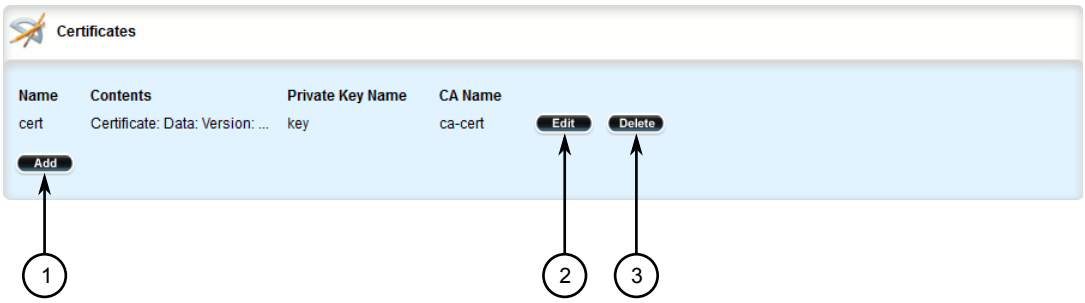


Figure 185: Certificate Table

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

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 6.7.8
Managing Known Hosts

RUGGEDCOM ROX II maintains a Known Hosts list for defining each SSH (SCP) server the device pulls updates or files from. Servers are identified by their host name or IP address. Users can further define a specific port on the server designated for SSH communications and/or an SSH/RSA public key.

Servers can also be enabled or disabled.

CONTENTS

Section 6.7.8.1
Viewing a List of Known Hosts

To view a list of servers defined in the Known Hosts list, navigate to ***admin » known-hosts***. The **Known Hosts** table appears.

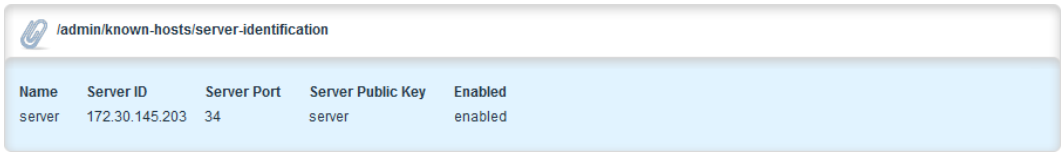


Figure 186: Known Hosts Table

If no servers have been configured, add servers as needed. For more information, refer to Section 6.7.8.2, "Adding a Known Host".

Section 6.7.8.2
Adding a Known Host

To add a server to the Known Hosts list, do the following:

1. Make sure the server's public key has been added to the device. For more information, refer to Section 6.7.6, "Managing Public Keys".
2. Change the mode to **Edit Private** or **Edit Exclusive**.
3. Navigate to ***admin » known-hosts*** and then click **<Add server-identification**. The **Key Settings** form appears.

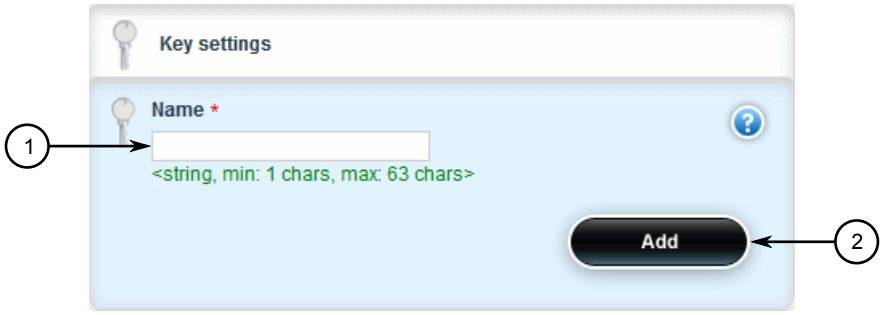


Figure 187: Key Settings Form

1. Name Box **2.** Add Button

4. Under **Name**, enter a unique name for the server and then click **Add**. The **Server Identification** form appears.

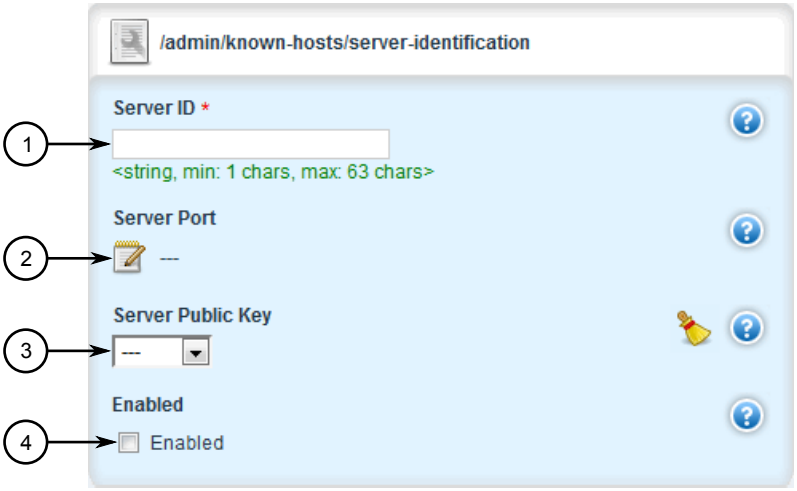


Figure 188: Server Identification Form

1. Server ID Box **2.** Server Port Box **3.** Server Public Key **4.** Enabled Check Box

5. Configure the following parameters as required:

Parameter	Description
name	**Synopsis:** A string 1 to 63 characters long The user's name to identify the remote server. This parameter is mandatory.
Server ID	**Synopsis:** A string 1 to 63 characters long The name to identify the remote server. This may be the ASCII hostname of the server or the IPv4 address (xxx.xxx.xxx.xxx) of the server. This parameter is mandatory.
Server Port	**Synopsis:** A 32-bit signed integer between 0 and 65535

Parameter	Description
	The port number (optional) uniquely identifies the remote SSH server. If no port is specified, then you will be able to access SSH servers on the remote server that are running on different ports.
Server Public Key	**Synopsis:** A string The name of the authorized ssh-rsa key for the server. The acceptable keys are taken from the list of authorized keys in /security/crypto.
enabled	Enables remote login to the server when using ssh, scp or sftp. If enabled, the server id and public key are saved in the known_hosts file.

6. 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 6.7.8.3
Deleting a Known Host

To delete a server from the Known Hosts list, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to ***admin » known-hosts***. The **Known Hosts** table appears.

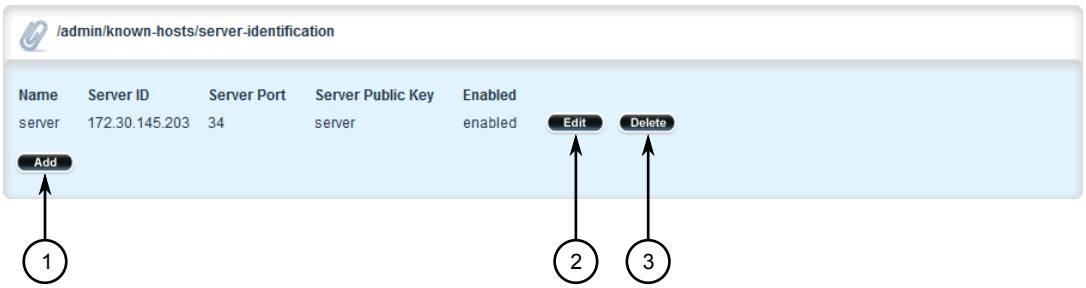


Figure 189: Known Hosts Table

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

3. Click **Delete** next to the desired 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 6.8
Managing Firewalls

Firewalls are software systems designed to prevent unauthorized access to or from private networks. Firewalls are most often used to prevent unauthorized Internet users from accessing private networks (Intranets) connected to the Internet.

When the RUGGEDCOM ROX II firewall is enabled, the router serves as a gateway machine through which all messages entering or leaving the Intranet pass. The router examines each message and blocks those that do not meet the specified security criteria. The router also acts as a proxy, preventing direct communication between computers on the Internet and Intranet. Proxy servers can filter the kinds of communication that are allowed between two computers and perform address translation.

NOTE

In general, the RUGGEDCOM ROX II firewall implementation will maintain established connections. This applies when adding, deleting, or changing rules, and also when adding, deleting, or changing policies. When applying new, or modified, rules or policies, previous traffic seen by the router might still be considered as having valid connections by the connection tracking table. For instance:

a. A rule for the TCP and UDP protocols is applied.

b. The router sees both TCP and UDP traffic that qualifies for NAT.

c. The rule is then modified to allow only UDP.

d. The router will still see TCP packets (i.e. retransmission packets).

If required, reboot the router to flush all existing connection streams.

RUGGEDCOM ROX II employs a stateful firewall system known as netfilter, a subsystem of the Linux kernel that provides the ability to examine IP packets on a per-session basis.

For more information about firewalls, refer to Section 6.8.1, "Firewall Concepts".

CONTENTS

Section 6.8.1

Firewall Concepts

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

CONTENTS

Section 6.8.1.1

Stateless vs. Stateful Firewalls

There are two types of firewalls: stateless and stateful.

Stateless or static firewalls make decisions about traffic without regard to traffic history. They simply open a path for the traffic type based on a TCP or UDP port number. Stateless firewalls are relatively simple, easily handling Web and e-mail traffic. However, stateless firewalls have some disadvantages. All paths opened in the firewall are always open, and connections are not opened or closed based on outside criteria. Static IP filters offer no form of authentication.

Stateful or session-based firewalls add considerably more complexity to the firewalling process. They track the state of each connection, look at and test each packet (connection tracking), and recognize and manage as a whole traffic from a particular protocol that is on connected sets of TCP/UDP ports.

Section 6.8.1.2

Linux netfilter

Netfilter, a subsystem of the Linux kernel, is a stateful firewall that provides the ability to examine IP packets on a per-session basis.

Netfilter uses rulesets, which are collections of packet classification rules that determine the outcome of the examination of a specific packet. The rules are defined by iptables, a generic table structure syntax and utility program for the configuration and control of netfilter.

RUGGEDCOM ROX II implements an IP firewall using a structured user interface to configure iptables rules and netfilter rulesets.

Section 6.8.1.3

Network Address Translation

Network Address Translation (NAT) enables a LAN to use one set of IP addresses for internal traffic and a second set for external traffic. The netfilter NAT function makes all necessary IP address translations as traffic passes between the Intranet and the Internet. NAT is often referred to in Linux as IP Masquerading.

NAT itself provides a type of firewall by hiding internal IP addresses. More importantly, NAT enables a network to use more internal IP addresses. Since they are only used internally, there is no possibility of conflict with IP addresses used by other organizations. Typically, an internal network is configured to use one or more of the reserved address blocks described in RFC1918.

Table: RFC1918 Reserved IP Address Blocks

IP Network/Mask	Address Range
10.0.0.0/8	10.0.0.0 – 10.255.255.255
172.16.0.0/12	172.16.0.0 – 172.31.255.255
192.168.0.0/16	192.168.0.0 – 192.168.255.255

When a packet from a host on the internal network reaches the NAT gateway, its source address and source TCP/UDP port number are recorded. The address and port number is translated to the public IP address and an unused port number on the public interface. When the Internet host replies to the internal host's packet, it is addressed to the NAT gateway's external IP address at the translation port number. The NAT gateway searches its tables and makes the opposite changes it made to the outgoing packet. NAT then forwards the reply packet to the internal host.

Translation of ICMP packets happens in a similar fashion, but without the source port modification.

NAT can be used in static and dynamic modes. Static NAT (SNAT) masks the private IP addresses by translating each internal address to a unique external address. Dynamic NAT translates all internal addresses to one or more external addresses.

Section 6.8.1.4

Port Forwarding

Port forwarding, also known as redirection, allows traffic coming from the Internet to be sent to a host behind the NAT gateway.

Previous examples have described the NAT process when connections are made from the Intranet to the Internet. In those examples, addresses and ports were unambiguous.

When connections are attempted from the Internet to the Intranet, the NAT gateway will have multiple hosts on the Intranet that could accept the connection. It needs additional information to identify the specific host to accept the connection.

Suppose that two hosts, 192.168.1.10 and 192.168.1.20 are located behind a NAT gateway having a public interface of 213.18.101.62. When a connection request for http port 80 arrives at 213.18.101.62, the NAT gateway could forward the request to either of the hosts (or could accept it itself). Port forwarding configuration could be used to redirect the requests to port 80 to the first host.

Port forwarding can also remap port numbers. The second host may also need to answer http requests. As connections to port 80 are directed to the first host, another port number (such as 8080) can be dedicated to the second host. As requests arrive at the gateway for port 8080, the gateway remaps the port number to 80 and forwards the request to the second host.

Port forwarding also takes the source address into account. Another way to solve the above problem could be to dedicate two hosts 200.0.0.1 and 200.0.0.2 and have the NAT gateway forward requests on port 80 from 200.0.0.1 to 192.168.1.10 and from 200.0.0.2 to 192.168.1.20.

Section 6.8.1.5
Protecting Against a SYN Flood Attack

RUGGEDCOM ROX II responds to SYN packets according to the TCP standard by replying with a SYN-ACK packet for open ports and an RST packet for closed ports. If the device is flooded by a high frequency of SYN packets, the port being flooded may become unresponsive.

To prevent SYN flood attacks on closed ports, set the firewall to block all traffic to closed ports. This prevents SYN packets from reaching the kernel.

Siemens also recommends setting the listen ports to include IP addresses on separate interfaces. For example, set the device to listen to an IP address on switch.0001 and fe-cm-1. This will make sure that one port is accessible if the other is flooded.

Section 6.8.1.6
Protecting Against IP Spoofing

IP spoofing is a technique where IP packets are created with a false source IP address, with the intent of concealing the identity of the sender or impersonating a trusted host. As a result, unauthorized users can gain access to a network.

In RUGGEDCOM ROX II, IP spoofing can be prevented by enabling the *Route Filter* and *Log Martians* for the firewall interface.

For information about enabling *Route Filter* and *Log Martians*, refer to Section 6.8.10.2, "Adding an Interface".

Section 6.8.2
Viewing a List of Firewalls

To view a list of firewalls, navigate to ***security » firewall » fwconfig***. If firewalls have been configured, the **Firewall Configurations** table appears.

Figure 190: Firewall Configurations Table

If no firewalls have been configured, add firewalls as needed. For more information, refer to Section 6.8.3, "Adding a Firewall".

Section 6.8.3
Adding a Firewall

To add a new firewall, do the following:

1. 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.

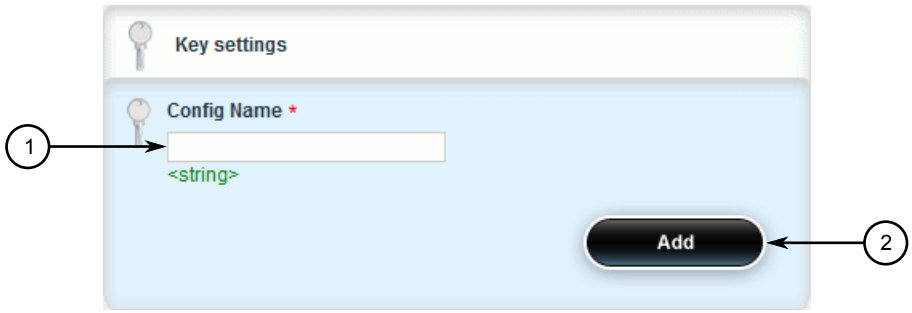


Figure 191: Key Settings Form

1. Config Name Box **2.** Add Button

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

Parameter	Description
Config Name	**Synopsis:** A string

4. Click **Add**. The **Firewall Settings** form appears.

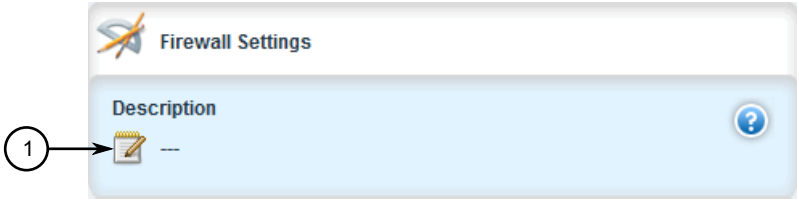


Figure 192: Firewall Settings Form

1. Description Box

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

Parameter	Description
Description	**Synopsis:** A string An optional description string.

6. Add interfaces associated with the firewall. For more information about adding interfaces, refer to Section 6.8.10.2, "Adding an Interface".
7. Add network zones for the firewall. Make sure a zone with the type **firewall** exists. For more information about adding network zones, refer to Section 6.8.9.2, "Adding a Zone".
8. Associate an interface with each zone. For more information about associating interfaces with zones, refer to Section 6.8.10.3, "Associating an Interface with a Zone".

9. Set the default policies for traffic control between zones. Make sure the policies are as restrictive as possible. For more information about configuring policies, refer to Section 6.8.12, "Managing Policies".
10. Configure the network address translation (NAT), masquerading or static network address translation (SNAT) settings. For more information about configuring NAT settings, refer to Section 6.8.13, "Managing Network Address Translation Settings". For more information about configuring masquerading and/or SNAT settings, refer to Section 6.8.14, "Managing Masquerade and SNAT Settings".
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 6.8.11, "Managing Hosts".
12. If required, configure rules that override the default policies. For more information about configuring rules, refer to Section 6.8.15, "Managing Rules".
13. If required, configure support for a VPN. For more information, refer to:
    - Section 6.8.6, "Configuring the Firewall for a VPN"
    - Section 6.8.7, "Configuring the Firewall for a VPN in a DMZ"
14. Validate the configuration. For more information about validating a firewall configuration, refer to Section 6.8.16, "Validating a Firewall Configuration".
15. Enable the firewall. For more information, refer to Section 6.8.17, "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 6.8.4

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 Configurations** table appears.

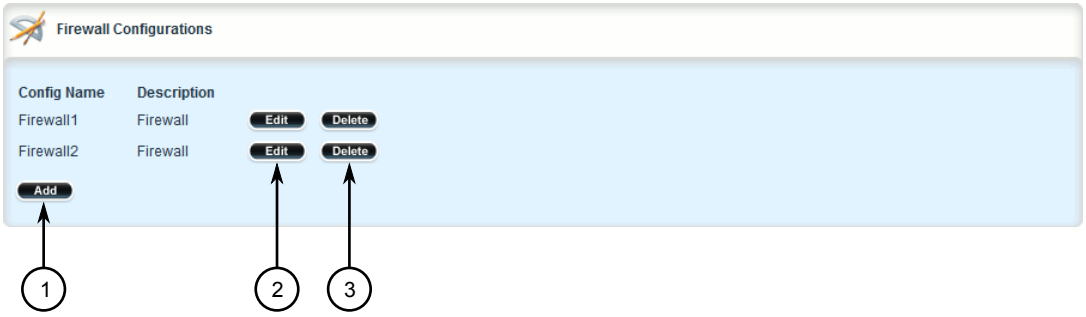


Figure 193: Firewall Configurations Table

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

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 6.8.5
Working with Multiple Firewall Configurations

RUGGEDCOM ROX II allows users to create multiple firewall configurations and work with one configuration while another is active.

To set one configuration as the working configuration and another as the active configuration, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to ***security » firewall***. The **Firewall Configuration** form appears.

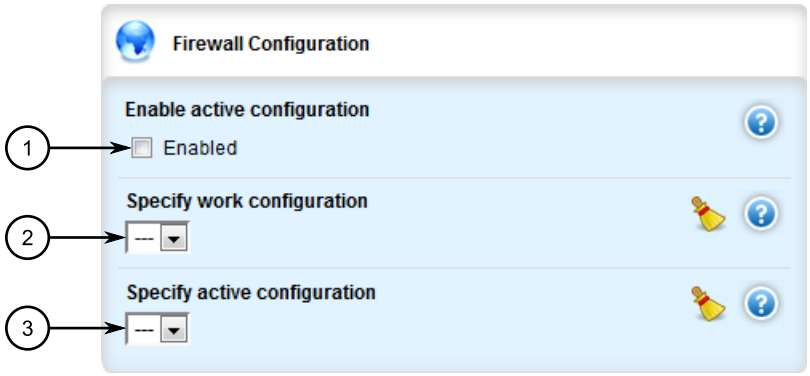


Figure 194: Firewall Configuration Form

1. Enable Active Configuration Check Box **2.** Specify Work Configuration List **3.** Specify Active Configuration List

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 6.8.6
Configuring the Firewall for a VPN

To configure the firewall for a policy-based VPN, do the following:

1. Make sure a basic firewall has been configured. For more information about configuring a firewall, refer to Section 6.8.3, "Adding a Firewall".
2. 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 6.8.9, "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 6.8.9, "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 6.8.10.3, "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 6.8.11, "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 6.8.11, "Managing Hosts".

   NOTE
   The VPN host must be specified before the network host so the more specific VPN zone subnet can be inspected first.

   The following are examples of possible host configurations:

Host	Interface	Subnet	IPsec Zone
vpn	W1ppp	192.168.1.0/24	Yes
net	W1ppp	0.0.0.0/0	No

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.

Action	Source-Zone	Destination-Zone	Protocol	Dest-Port
Accept	net	fw	ah	—
Accept	net	fw	esp	—
Accept	net	fw	udp	500

   For more information about configuring rules, refer to Section 6.8.15, "Managing Rules".
10. Configure the following rule to allow traffic from Libreswan, the IPsec daemon, to enter the firewall:

    NOTE
    IPsec traffic arriving at the firewall is directed to Libreswan, the IPsec daemon. Libreswan decrypts the traffic and then forwards it back to the firewall on the same interface that originally received it. A rule is required to allow traffic to enter the firewall from this interface.

Action	Source-Zone	Destination-Zone	Protocol	Dest-Port
Accept	vpn	loc	—	—

    For more information about configuring rules, refer to Section 6.8.15, "Managing Rules".

Section 6.8.7

Configuring the Firewall for a VPN in a DMZ

When the firewall needs to pass VPN traffic through to another device, such as a VPN device in a Demilitarized Zone (DMZ), then a DMZ zone and special rules are required.

To configure the firewall for a VPN in a DMZ, do the following:

1. Make sure a basic firewall has been configured. For more information about configuring a firewall, refer to Section 6.8.3, "Adding a Firewall".
2. 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 6.8.9, "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.

Action	Source-Zone	Destination-Zone	Protocol	Dest-Port
Accept	Net	dmz	Ah	—
Accept	Net	dmz	Esp	—
Accept	Net	dmz	UDP	500
Accept	dmz	Net	Ah	—
Accept	dmz	Net	Esp	—
Accept	dmz	Net	Udp	500

   For more information about configuring rules, refer to Section 6.8.15, "Managing Rules".

Section 6.8.8

Configuring Netfilter

To configure Netfilter, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to **admin**. The **System Control** form appears.

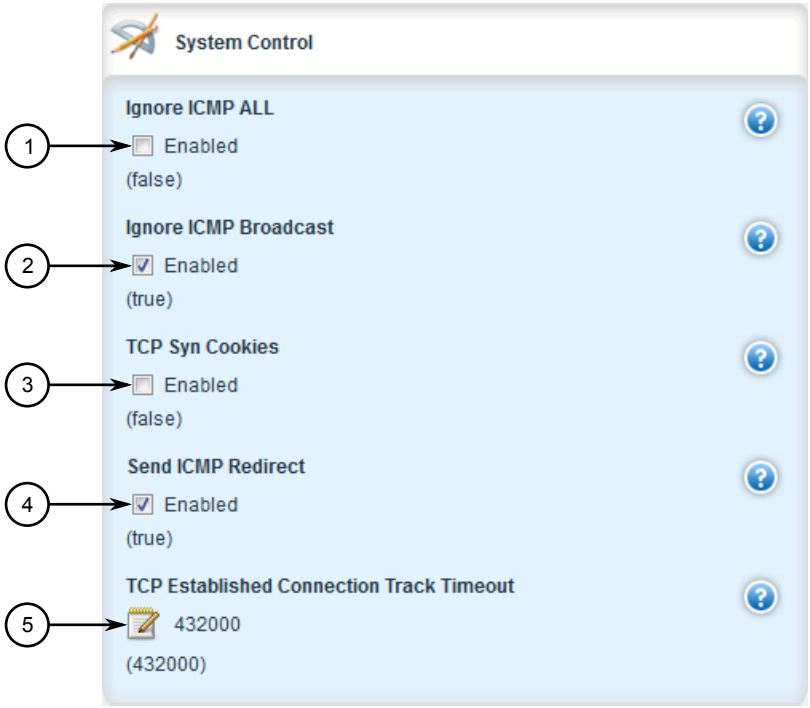


Figure 195: System Control Form

1. Ignore ICMP ALL Check Box **2.** Ignore ICMP Broadcast Check Box **3.** TCP Syn Cookies Check Box **4.** Send ICMP Redirect Check Box **5.** TCP Established Connection Track Timeout Box

3. Under **TCP Established Connection Track Timeout**, set the time in seconds (s) a stale TCP connection can reside in the connection tracking table. The value can between 300 and 432000 s. The default value is 432000 s, or five days.
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 6.8.9

Managing Zones

A network zone is a collection of interfaces for which forwarding decisions are made. Common zones include:

Zone	Description
Net	The Internet
Loc	The local network
DMZ	Demilitarized zone
Fw	The firewall itself
Vpn1	IPsec connections on w1ppp

Zone	Description
Vpn2	IPsec connections on w2ppp

New zones may be defined as needed. For example, if each Ethernet interface is part of the local network zone, disabling traffic from the Internet zone to the local network zone would disable traffic to all Ethernet interfaces. If access to the Internet is required for some Ethernet interfaces, but not others, a new zone may be required for those interfaces.

CONTENTS

Section 6.8.9.1
Viewing a List of Zones

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 **Zones** table appears.

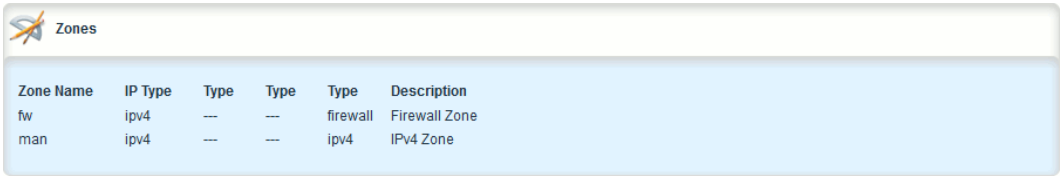


Figure 196: Zones Table

If no zones have been configured, add zones as needed. For more information, refer to Section 6.8.9.2, "Adding a Zone".

Section 6.8.9.2
Adding a Zone

To add a new zone for a firewall, do the following:

1. 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.

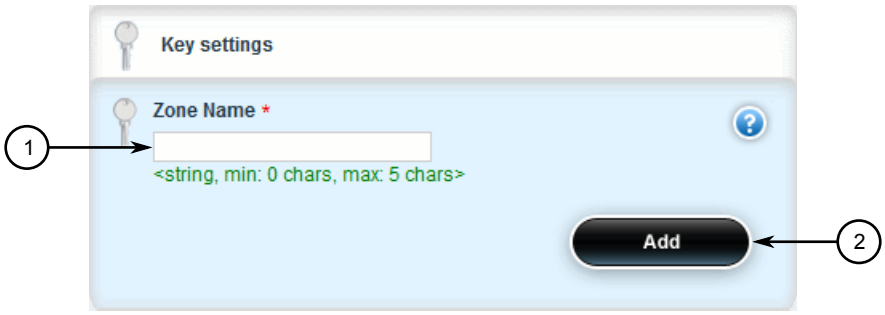


Figure 197: Key Settings Form

1. Zone Name Box **2.** Add Button

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

Parameter	Description
Zone Name	**Synopsis:** A string 0 to 5 characters long A unique name to assign to this zone. Be sure to *also create* a zone called **fw** that is of the zone type *firewall*. This parameter is mandatory.

5. Click **Add**. The **Zone Settings** form appears.

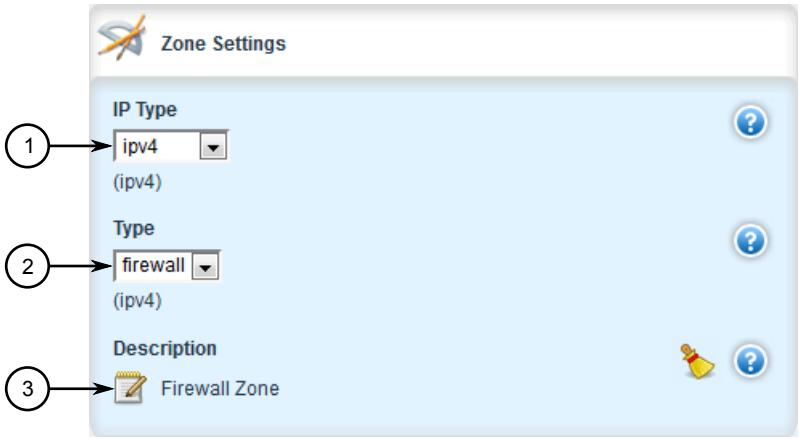


Figure 198: Zone Settings Form

1. Type List **2.** Description Box

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

Parameter	Description
IP Type	**Synopsis:** { ipv4, ipv6, ipv4ipv6 } **Default:** ipv4 Internet protocol type - use both when no addresses are used, otherwise define IPv4 and IPv6 rules for each type of addresses used.
Type	**Synopsis:** { ip, ipsec, firewall }

Parameter	Description
	Default: ip Zone types applying to both IPv4 and IPv6: plain IP, firewall, or IPSec
Type	**Synopsis:** { ipv6, ipsec, firewall } **Default:** ipv6 Zone types are plain IPv6, firewall, or IPSec
Type	**Synopsis:** { ipv4, ipsec, firewall } **Default:** ipv4 Zone types are plain IPv4, firewall, or IPSec
Description	**Synopsis:** A string (Optional) The description string for this zone

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 6.8.9.3
Deleting a Zone

To delete a zone, 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. The **Zones** table appears.

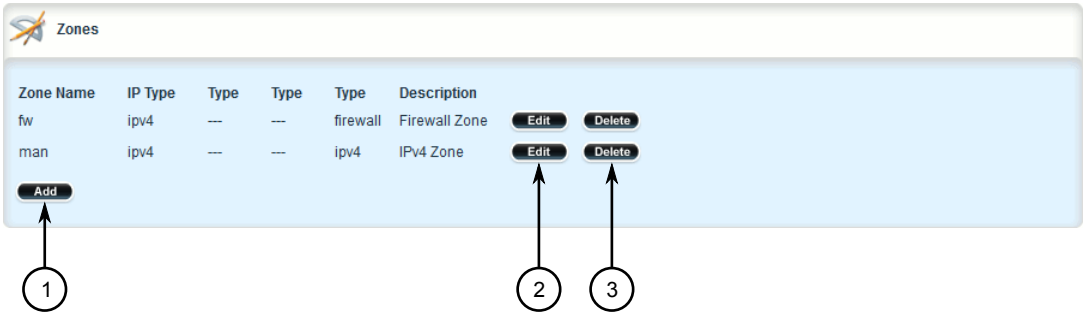


Figure 199: Zones Table

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

3. Click **Delete** next to the chosen zone.
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 6.8.10

Managing Interfaces

Firewall interfaces are the LAN and WAN interfaces available to the router. Each interface must be placed in a network zone. If an interface supports more than one zone, its zone must be marked as *undefined* and the interface must use the zone host's setup to define a zone for each subnet on the interface.

Table: Example

Interface	Zone
Switch.0001	Loc
Switch.0002	Loc
Switch.0003	Any
Switch.0004	DMZ
W1ppp	net

CONTENTS

Section 6.8.10.1

Viewing a List of Interfaces

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 **Interfaces** table appears.

Figure 200: Interfaces Table

If no interfaces have been configured, add interfaces as needed. For more information, refer to Section 6.8.10.2, "Adding an Interface".

Section 6.8.10.2

Adding an Interface

To configure an interface for a firewall, do the following:

1. 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.

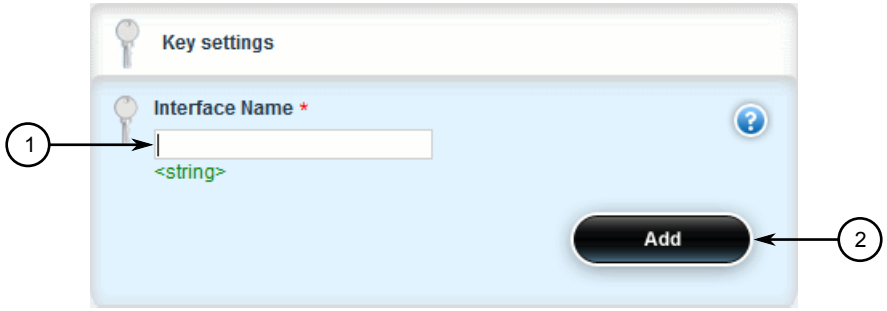


Figure 201: Key Settings Form

1. Interface Name Box **2.** Add Button

5. Configure the following parameter as required:

Parameter	Description
Interface Name	**Synopsis:** A string Currently active or not - add '+' for the same interfaces: ppp+. This parameter is mandatory.

6. Click **Add**. The **Interface Settings** and **Interface Options** forms appear.

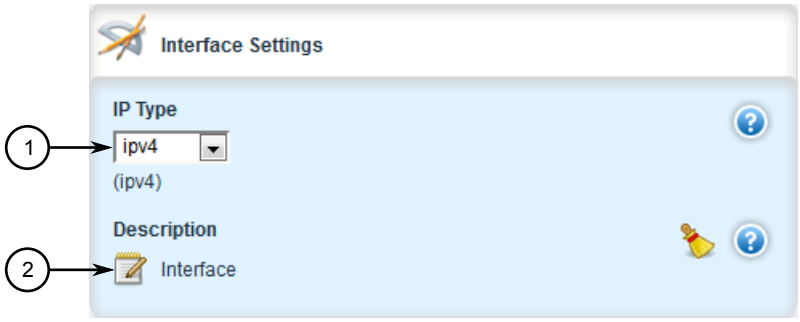


Figure 202: Interface Settings Form

1. Description Box

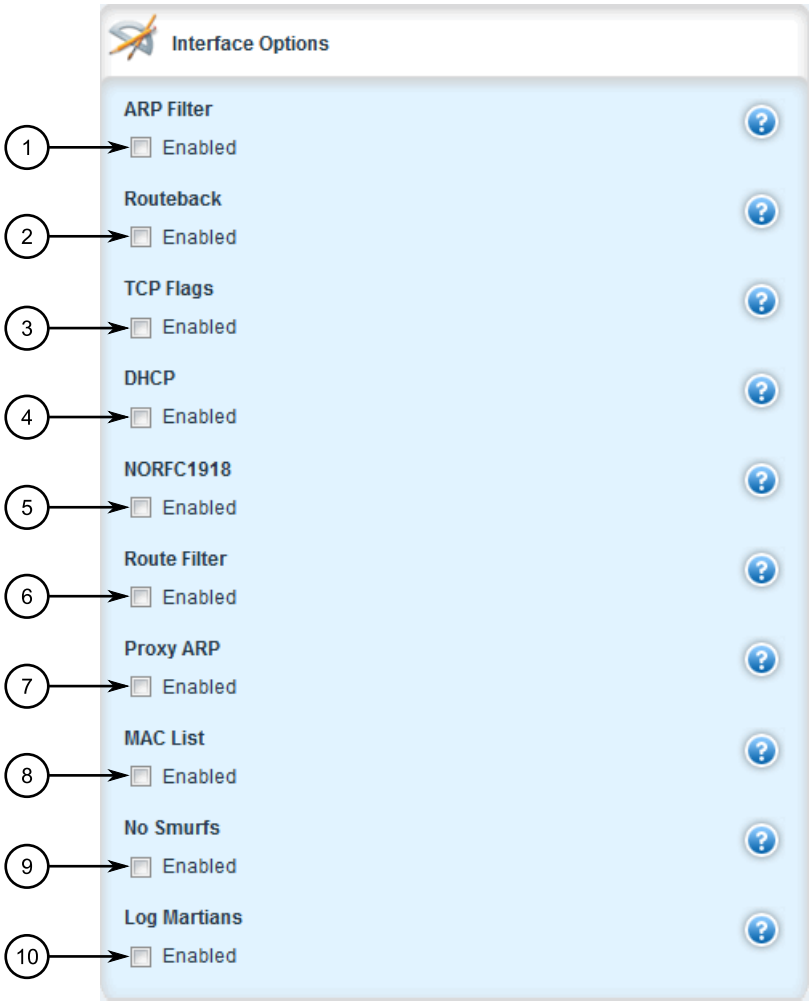


Figure 203: Interface Options Form

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 **Interface Settings**, configure the following parameter(s) as required:

Parameter	Description
IP Type	**Synopsis:** { ipv4, ipv6, ipv4ipv6 } **Default:** ipv4 Internet protocol type - use both when no addresses are used, otherwise define IPv4 and IPv6 rules for each type of addresses used.
Description	**Synopsis:** 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	IPv4 ONLY- See additional info. Responds only to ARP requests for configured IP addresses (This is permanently enabled system wide since ROX 2.3.0, and this option no longer has any effect).
Routeback	IPv4 and IPv6 - Interface traffic routed back out that same interface.
TCP Flags	IPv4 and IPv6. Illegal combinations of TCP flags dropped and logged at info level.
DHCP	IPv4 and IPv6 - Allows DHCP datagrams to enter and leave the interface.
NORFC1918	Not currently implemented
Route Filter	IPv4 and IPv6 - Enables /rpfilter/ spoofing protection
Proxy ARP	IPv4 ONLY - Enables proxy ARP.
MAC List	Not currently implemented
No Smurfs	IPv4 ONLY - Packets with broadcast address as source dropped and logged at info level.
Log Martians	IPv4 ONLY - Logging of packets with impossible source addresses.

9. Associate the interface with a pre-defined zone or mark the associated zone as undefined. For more information about associating the interface with a zone, refer to Section 6.8.10.3, "Associating an Interface with a Zone".
10. Configure a broadcast address for the interface. For more information configuring a broadcast address, refer to Section 6.8.10.4, "Configuring a Broadcast Address".
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 6.8.10.3
Associating an Interface with a Zone

To associate an interface with a pre-defined zone or mark the associated zone as undefined, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to ***security » firewall » fwconfig » {firewall} » fwinterface{interface} » zone***, where *{firewall}* is the name of the firewall and *{interface}* is the name of the interface. The **Zone** form appears.

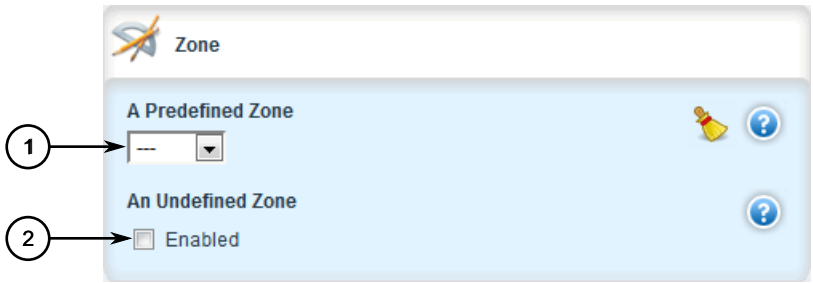


Figure 204: Zone Form

1. Predefined Zone List **2.** Undefined Zone Check Box

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

Parameter	Description
A Predefined Zone	**Synopsis:** A string A pre-defined zone
An 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 6.8.10.4
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 » {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.

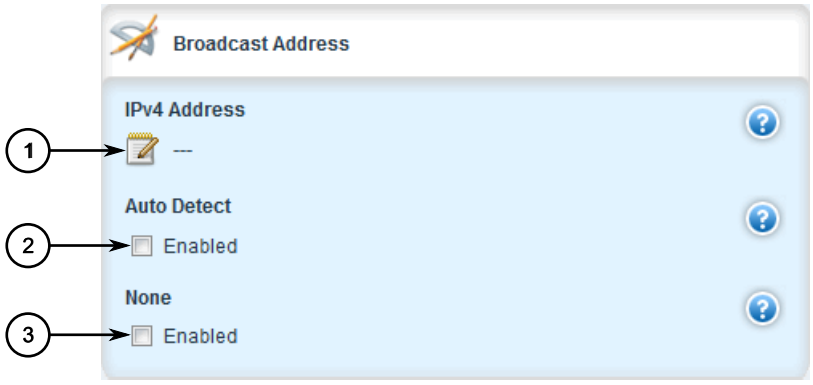


Figure 205: Broadcast Address Form

1. IPv4 Address Box **2.** Auto Detect Check Box **3.** None Check Box

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

Parameter	Description
IPv4 Address	**Synopsis:** A string An IPv4 address for a broadcast address.
Auto Detect	Automatic detection of the broadcast address(es).
None	The default.

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 6.8.10.5
Deleting an Interface

To delete an interface, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to ***security » firewall » fwconfig » {firewall} » fwinterface***, where *{firewall}* is the name of the firewall. The **Interfaces** table appears.

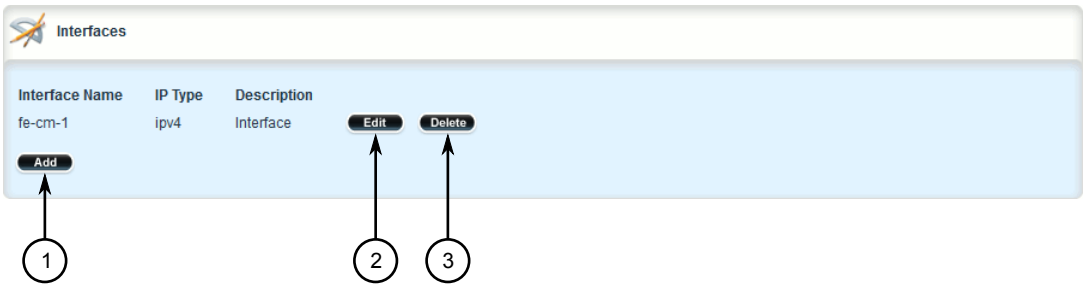


Figure 206: Interfaces Table

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 6.8.11
Managing Hosts

Hosts are used to assign zones to individual hosts or subnets (if the interface supports multiple subnets). This allows the firewall to receive a packet and then redirect it to the same device that received it. This functionality is useful for VPN setups to handle the VPN traffic separately from the other traffic on the interface which carries the VPN traffic.

Table: Example

Zone	Interface	IP Address or Network
Local	Switch.0003	10.0.0.0/8
Guests	Switch.0003	192.168.0.0/24

CONTENTS

Section 6.8.11.1
Viewing a List of Hosts

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 **Hosts** table appears.

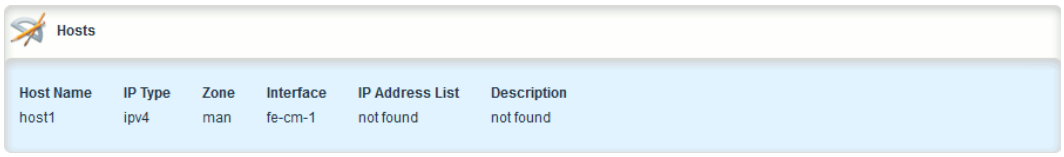


Figure 207: Hosts Table

If no hosts have been configured, add hosts as needed. For more information, refer to Section 6.8.11.2, "Adding a Host".

Section 6.8.11.2
Adding a Host

To add a new host for a firewall, do the following:

1. 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.

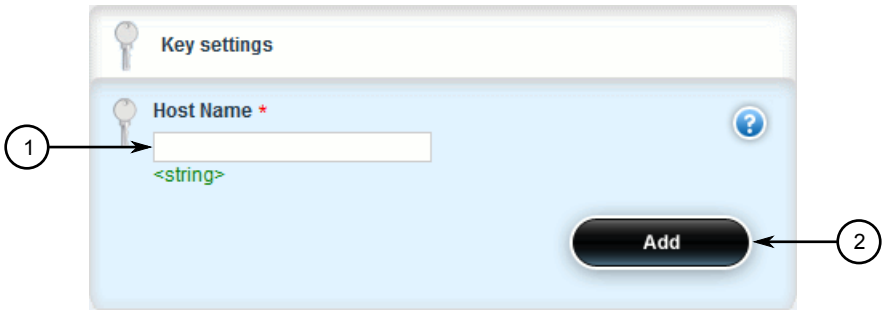


Figure 208: Key Settings Form

1. Host Name Box **2.** Add Button

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

Parameter	Description
Host Name	**Synopsis:** A string The name of a host configuration entry.

5. Click **Add**. The **Host Options** and **Host Settings** forms appear.

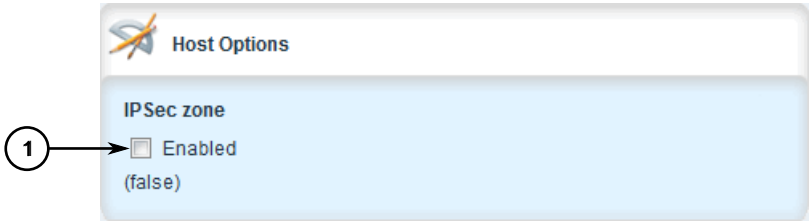


Figure 209: Host Options Form

1. IPsec Zone Check Box

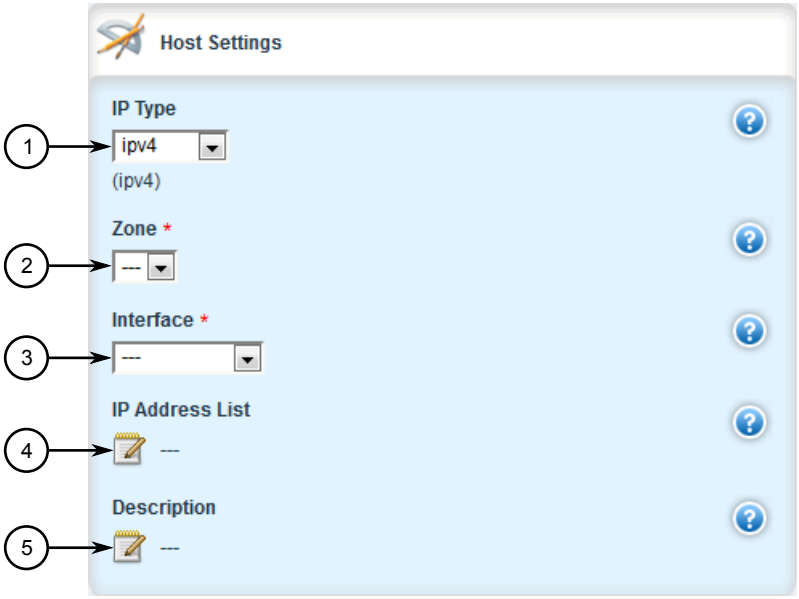


Figure 210: Host Settings Form

1. IP Type List **2.** Zone List **3.** Interface List **4.** IP Address Box **5.** Description Box

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

Parameter	Description
IPSec zone	**Synopsis:** { true, false } **Default:** false

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

Parameter	Description
IP Type	**Synopsis:** { ipv4, ipv6, ipv4ipv6 } **Default:** ipv4 Internet protocol type - use both when no addresses are used, otherwise define IPv4 and IPv6 rules for each type of addresses used.
Zone	**Synopsis:** A string A pre-defined zone

Parameter	Description
	This parameter is mandatory.
Interface	**Synopsis:** A string A pre-defined interface to which optional IPs and/or networks can be added. This parameter is mandatory.
IP Address List	**Synopsis:** A string Additional IP addresses or networks - comma separated, or a range in the form of low.address-high.address
Description	**Synopsis:** A string (Optional) The description string for this host.

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 6.8.11.3
Deleting a Host

To delete a host, 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. The **Hosts** table appears.

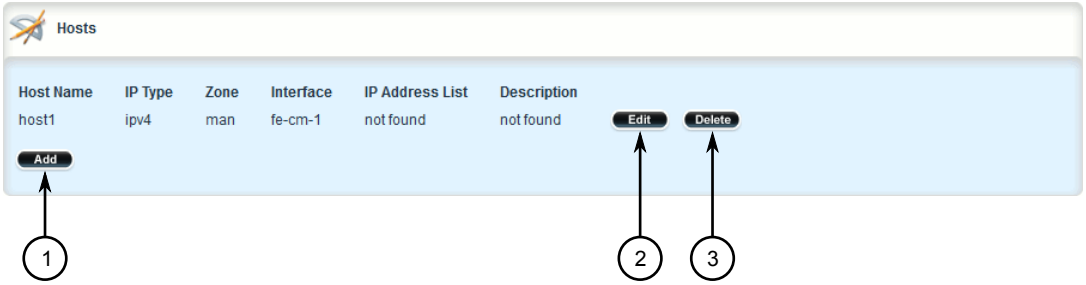


Figure 211: Hosts Table

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

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 6.8.12
Managing Policies

Policies define the default actions for establishing a connection between different firewall zones. Each policy consists of a source zone, a destination zone and an action to be performed when a connection request is received.

The following example illustrates the policies for establishing connections between a local network and the Internet.

Policy	Source Zone	Destination Zone	Action
1	Loc	Net	ACCEPT
2	Net	All	DROP
3	All	All	REJECT

Each policy controls the connection between the source and destination zones. The first policy accepts all connection requests from the local network to the Internet. The second policy drops or ignores all connection requests from the Internet to any device on the network. The third policy rejects all other connection requests and sends a TCP RST or an ICMP destination-unreachable packet to the client.

The order of the policies is important. If the last policy in the example above were to be the first policy, the firewall would reject all connection requests.

NOTE
The source and destination zones must be configured before a policy can be created. For more information about zones, refer to Section 6.8.9, "Managing Zones".

NOTE
Policies for specific hosts or types of traffic can be overridden by rules. For more information about rules, refer to Section 6.8.15, "Managing Rules".

CONTENTS

Section 6.8.12.1
Viewing a List of Policies

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 **Policies** table appears.

Figure 212: Policies Table

If no policies have been configured, add policies as needed. For more information, refer to Section 6.8.12.2, "Adding a Policy".

Section 6.8.12.2
Adding a Policy

To configure a policy for the firewall, do the following:

1. 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.

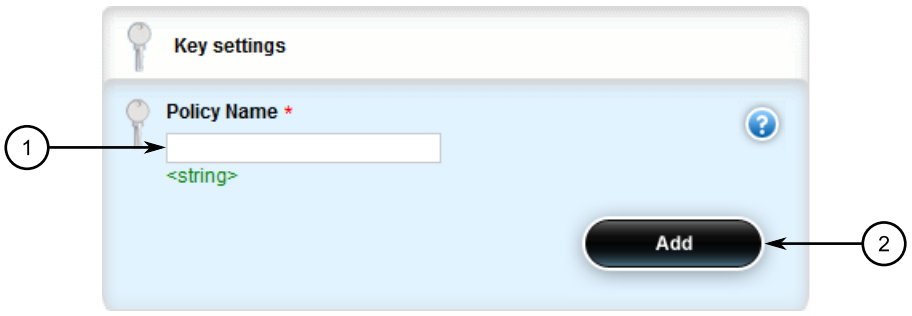


Figure 213: Key Settings Form

1. Policy Name Box **2.** Add Button

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

Parameter	Description
Policy Name	**Synopsis:** A string Enter a name tag for this policy.

5. Click **Add**. The **Policy Settings** form appears.

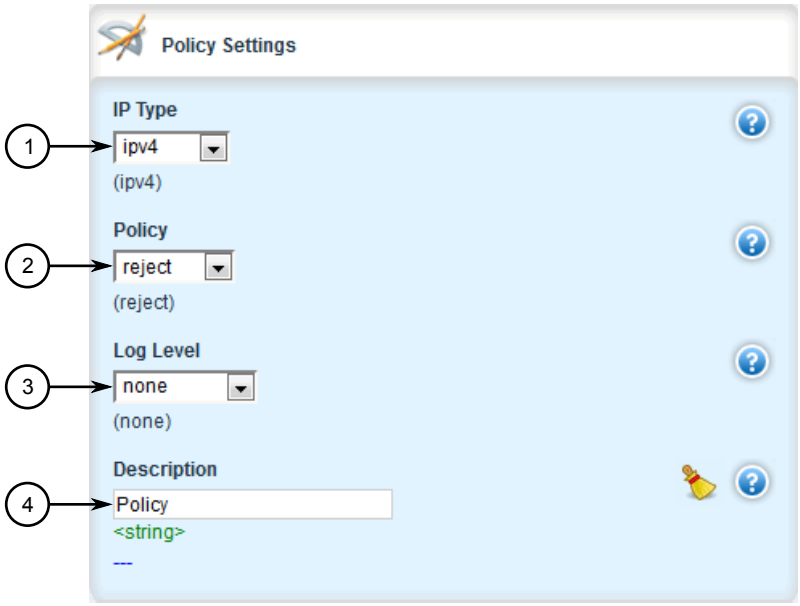


Figure 214: Policy Settings Form

1. IP Type List **2.** Policy List **3.** Log Level List **4.** Description Box

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

Parameter	Description
IP Type	**Synopsis:** { ipv4, ipv6, ipv4ipv6 } **Default:** ipv4 Internet protocol type - use both when no addresses are used, otherwise define IPv4 and IPv6 rules for each type of addresses used.
Policy	**Synopsis:** { accept, drop, reject, continue } **Default:** reject A default action for connection establishment between different zones.
Log Level	**Synopsis:** { none, debug, info, notice, warning, error, critical, alert, emergency } **Default:** none (Optional) Determines whether or not logging will take place and at which logging level.
Description	**Synopsis:** A string (Optional) The description string for this policy.

7. Configure the source zone for the policy. For more information, refer to Section 6.8.12.3, "Configuring the Source Zone".
8. Configure the destination zone for the policy. For more information, refer to Section 6.8.12.4, "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 6.8.12.3
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.

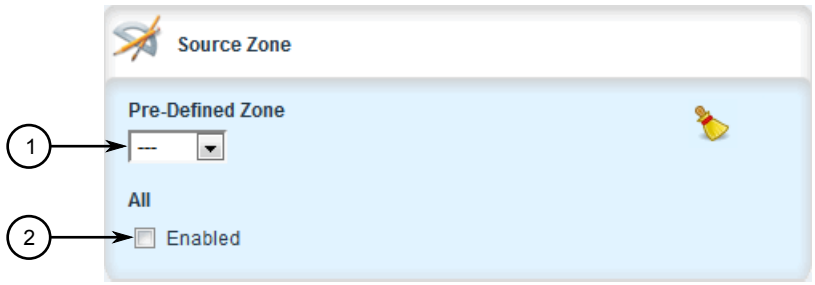


Figure 215: Source Zone Form

1. Pre-Defined Zone List **2.** All Check Box

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

Parameter	Description
Pre-Defined Zone	**Synopsis:** A string
All	

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 6.8.12.4
Configuring the Destination Zone

To configure the destination 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} » destination-zone***, where *{firewall}* is the name of the firewall and *{policy}* is the name of the policy. The **Destination Zone** form appears.

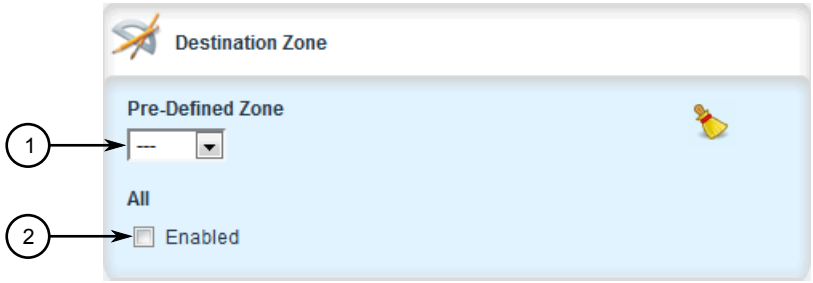


Figure 216: Destination Zone Form

1. Pre-Defined Zone List **2.** All Check Box

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

Parameter	Description
Pre-Defined Zone	**Synopsis:** A string
All	

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 6.8.12.5
Deleting a Policy

To delete a policy, 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. The **Policies** table appears.

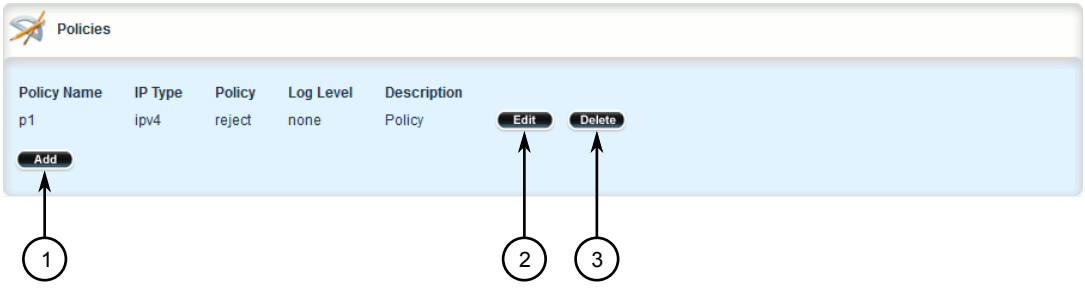


Figure 217: Policies Table

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

3. Click **Delete** next to the chosen policy.

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 6.8.13
Managing Network Address Translation Settings

Network address translation entries can be used to set up a one-to-one correspondence between an external address on the firewall and the RFC1918 address of a host behind the firewall. This is often set up to allow connections to an internal server from outside the network.

NOTE
Destination Network Address Translation (DNAT) can be setup by configuring the destination zone in a rule. For more information on rules, refer to Section 6.8.15, "Managing Rules".

CONTENTS

Section 6.8.13.1
Viewing a List of NAT Settings

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** table appears.

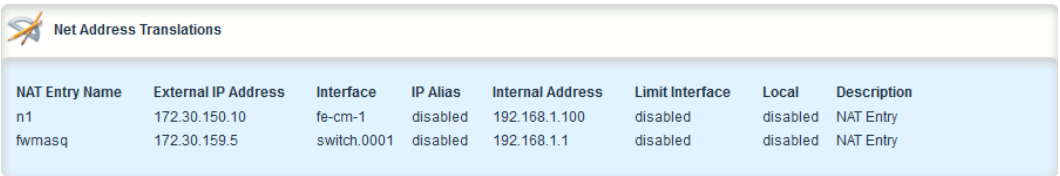


Figure 218: Net Address Translations Table

If no NAT settings have been configured, add NAT settings as needed. For more information, refer to Section 6.8.13.2, "Adding a NAT Setting".

Section 6.8.13.2
Adding a NAT Setting

To configure a Network Address Translation (NAT) entry, do the following:

1. 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.

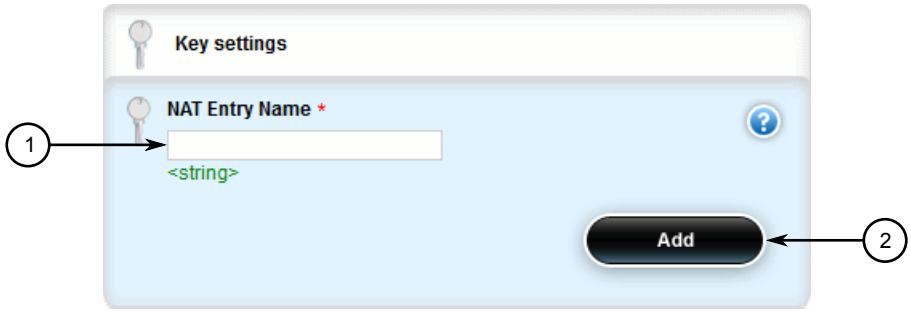


Figure 219: Key Settings Form

1. NAT Entry Name Box **2.** Add Button

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

Parameter	Description
NAT Entry Name	**Synopsis:** A string Enter a name for this NAT entry

5. Click **Add**. The **Net Address Translation Settings** forms appear.

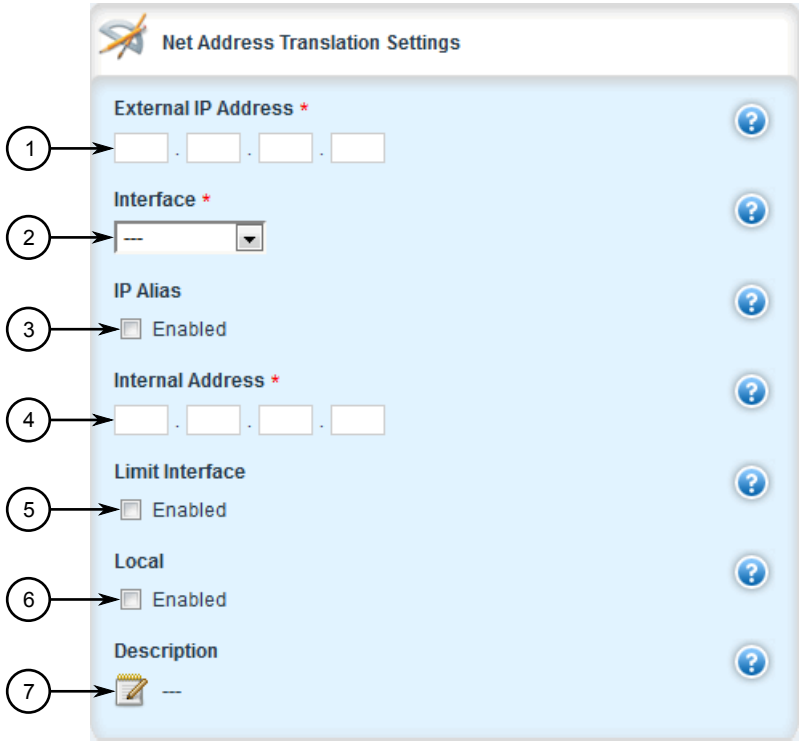


Figure 220: Net Address Translation Settings Form

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 7.1, "Managing IP Addresses for Routable Interfaces".

Parameter	Description
External IP Address	**Synopsis:** A string The external IP Address. The address must not be a DNS name. External IP addresses must be manually added to the interface. This parameter is mandatory.
Interface	**Synopsis:** A string An interface that has an external IP address. This parameter is mandatory.
IP Alias	Create IP Alias for NAT rule.
Internal Address	**Synopsis:** A string The internal IP address. The address must not be a DNS Name. This parameter is mandatory.

Parameter	Description
Limit Interface	Translation only effective from the defined interface.
Local	Translation effective from the firewall system.
Description	**Synopsis:** A string (Optional) The description string for this NAT 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 6.8.13.3
Deleting a NAT Setting

To delete a network address translation 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. The **Net Address Translation** table appears.

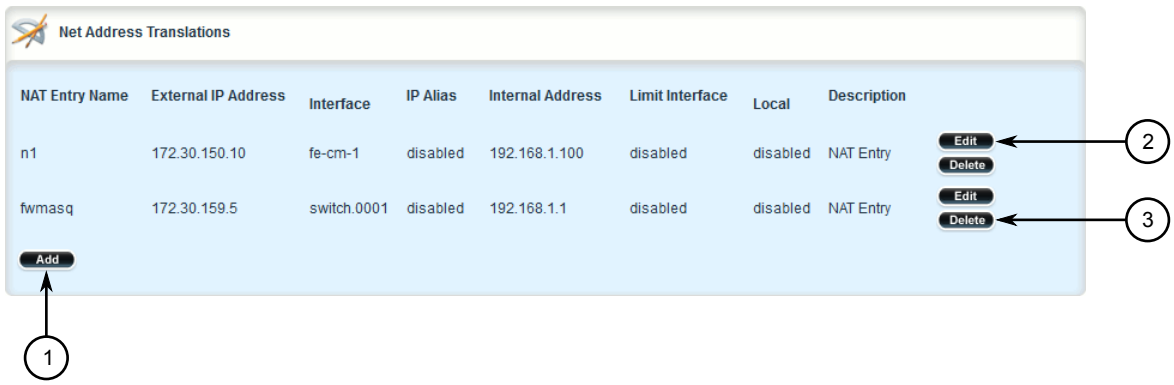


Figure 221: Net Address Translations Table

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

3. Click **Delete** next to the chosen NAT 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 6.8.14
Managing Masquerade and SNAT Settings

Masquerading and Source Network Address Translation (SNAT) are forms of dynamic Network Address Translation (NAT). Both hide a subnetwork behind a single public IP address.

Masquerading is used when the ISP provides a dynamic IP address. SNAT is used when the ISP provides a static IP address.

CONTENTS

Section 6.8.14.1

Viewing a List of Masquerade and SNAT Settings

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 **Masqueradings** table appears.

Figure 222: Masqueradings Table

If no masquerade or SNAT settings have been configured, add masquerade or SNAT settings as needed. For more information, refer to Section 6.8.14.2, "Adding Masquerade or SNAT Settings".

Section 6.8.14.2

Adding Masquerade or SNAT Settings

To add rules for masquerading or SNAT, do the following:

NOTE
Masquerading requires that the IP address being used to masquerade must belong to the router. When configuring the SNAT address under masquerading, the SNAT address must be one of the IP addresses on the outbound interface.

1. 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.

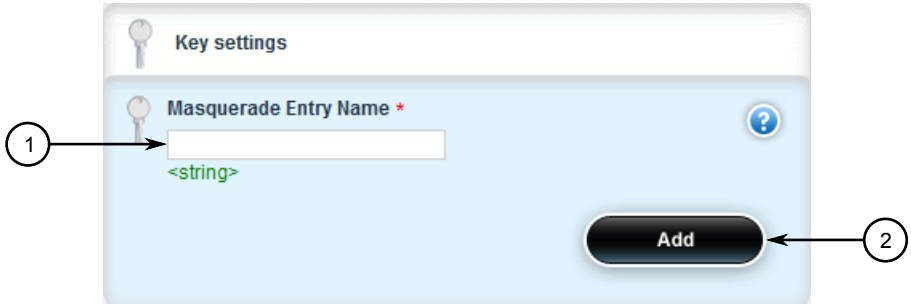


Figure 223: Key Settings Form

1. Masquerade Entry Name Box **2.** Add Button

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

Parameter	Description
Masquerade Entry Name	**Synopsis:** A string A name for this masquerading configuration entry.

5. Click **Add**. The **Masquerade Settings** form appears.

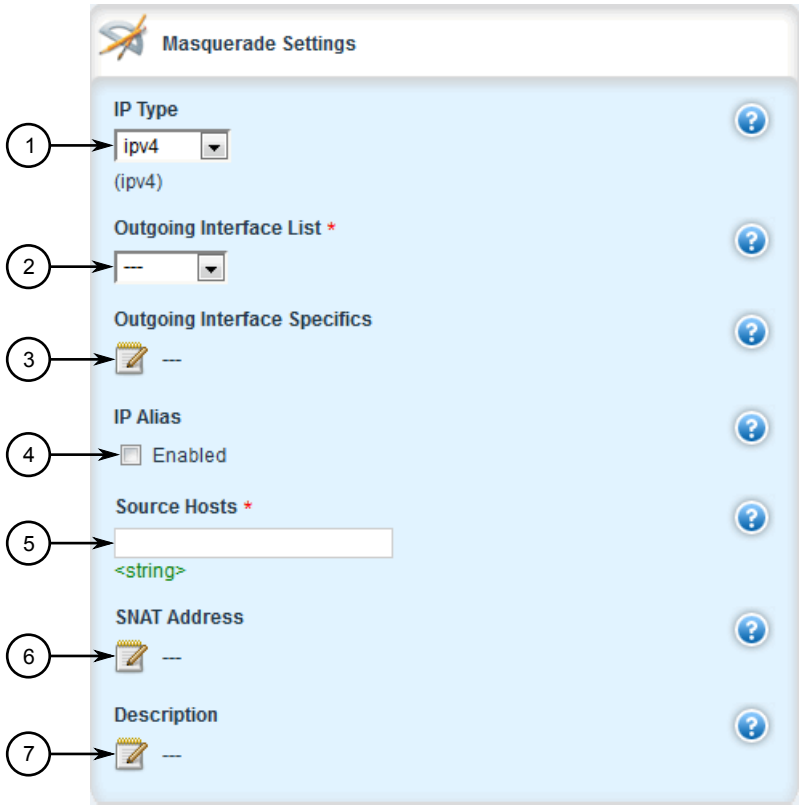


Figure 224: Masquerade Settings Form

1. IP Type List **2.** Outgoing Interface List **3.** Outgoing Interface Specifics Box **4.** IP Alias Check Box **5.** Source Hosts Box **6.** SNAT Address Box **7.** Description Box

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

Parameter	Description
IP Type	**Synopsis:** { ipv4, ipv6, ipv4ipv6 } **Default:** ipv4 Internet protocol type - use both when no addresses are used, otherwise define IPv4 and IPv6 rules for each type of addresses used.
Outgoing Interface List	**Synopsis:** A string An outgoing interface list - usually the internet interface. This parameter is mandatory.
Outgoing Interface Specifics	**Synopsis:** A string (Optional) An outgoing interface list - specific IP destinations for the out-interface.
IP Alias	Create IP Alias for NAT rule.
Source Hosts	**Synopsis:** A string Subnet range or comma-separated list of hosts (IPs) This parameter is mandatory.
SNAT Address	**Synopsis:** A string

Parameter	Description
	(Optional) By specifying an address here, SNAT will be used and this will be the source address.
Description	**Synopsis:** A string (Optional) The description string for this masq 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 6.8.14.3
Deleting a Masquerade or SNAT Setting

To delete a masquerade or SNAT setting, do the following:

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. The **Masqueradings** table appears.

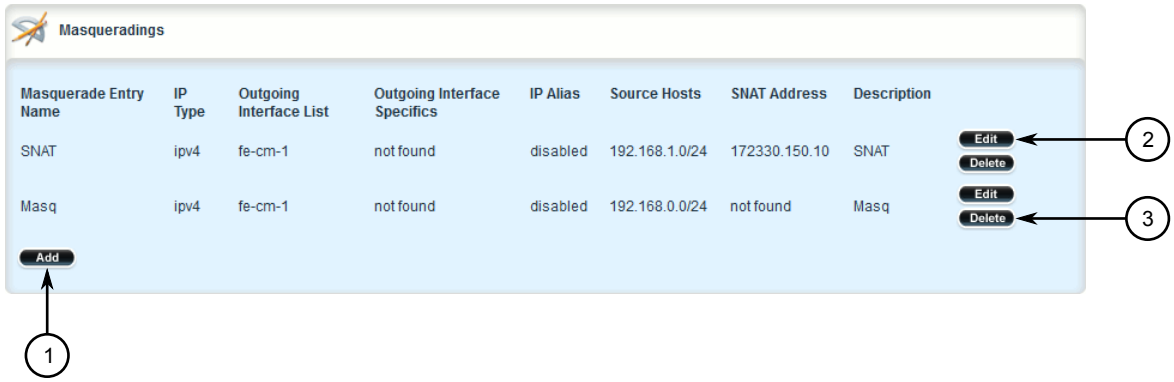


Figure 225: Masqueradings Table

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

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 6.8.15

Managing Rules

Rules establish exceptions to the default firewall policies for certain types of traffic, sources or destinations. Each rule defines specific criteria. If an incoming packet matches that criteria, the default policy is overridden and the action defined by the rule is applied.

CONTENTS

Section 6.8.15.1

Viewing a List of Rules

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 **Rules** table appears.

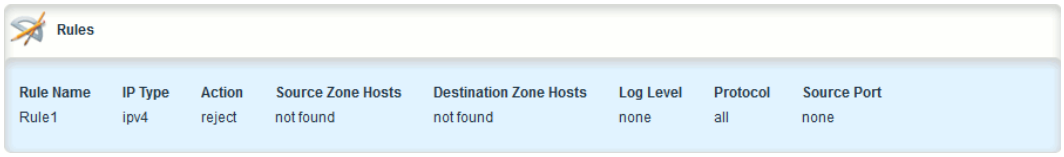


Figure 226: Rules Table

If no rules have been configured, add rules as needed. For more information, refer to Section 6.8.15.2, "Adding a Rule".

Section 6.8.15.2

Adding a Rule

To configure a rule for a firewall, do the following:

1. 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.

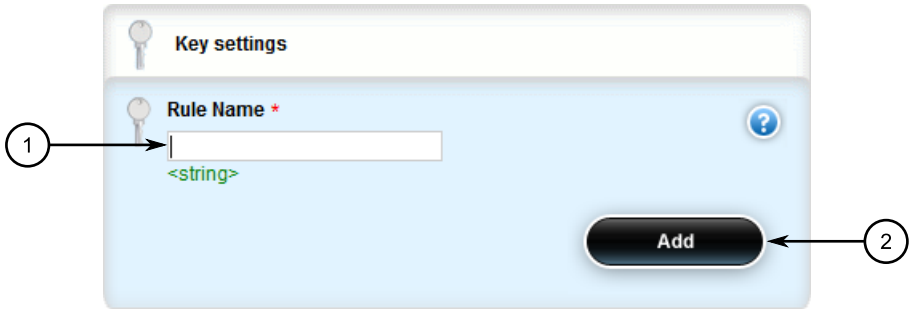


Figure 227: Key Settings Form

1. Rule Name Box **2.** Add Button

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

Parameter	Description
Rule Name	**Synopsis:** A string Enter a unique name that identifies this rule.

5. Click **Add**. The **Rule Settings** form appears.

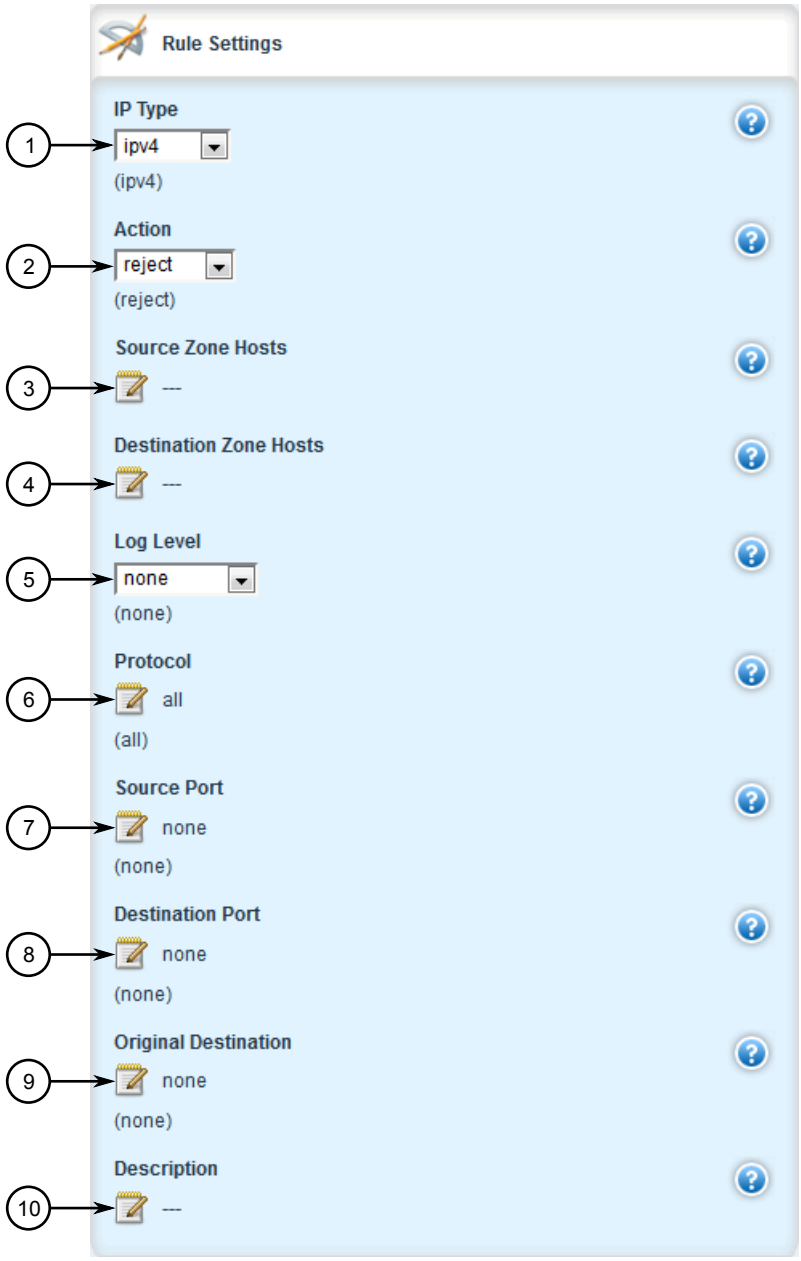


Figure 228: Rule Settings Form

1. IP type List **2.** Action List **3.** Source Zone Hosts Box **4.** Destination Zone Hosts Box **5.** Log Level List **6.** Protocol Box **7.** Source Port Box **8.** Destination Port Box **9.** Original Destination Box **10.** 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. A rule for the TCP and UDP protocols is applied.

b. The router sees both TCP and UDP traffic that qualifies for NAT.

c. The rule is then modified to allow only UDP.

d. The router will still see TCP packets (i.e. retransmission packets).

If required, reboot the router to flush all existing connection streams.

Parameter	Description
IP Type	**Synopsis:** { ipv4, ipv6, ipv4ipv6 } **Default:** ipv4 Internet protocol type - use both when no addresses are used, otherwise define IPv4 and IPv6 rules for each type of addresses used.
Action	**Synopsis:** { accept, drop, reject, continue, redirect, dnat-, dnat, copy-dnat } **Default:** reject The final action to take on incoming packets matching this rule. Options include: • accept: Allows the connection request to proceed. • continue: Passes the connection request past any other rules. • copy-dnat: Sends a copy to a second system using a DNAT rule. Protocol must be set to 'udp', and Original Destination must be defined. • dnat: Forwards the request to another system and (optionally) another port. • dnat-: Only generates the DNAT IPtables rule and not the companion ACCEPT rule. • drop: The connection request is ignored. No notification is sent. • redirect: Redirects the request to a local TCP port number on the local firewall. • reject: Rejects the connection with an RST (TCP) or ICMP destination-unreachable.
Source Zone Hosts	**Synopsis:** A string (Optional) Add comma-separated host IPs to a predefined source-zone.
Destination Zone Hosts	**Synopsis:** A string (Optional) Add comma-separated host IPs to the destination-zone - may include :port for DNAT or REDIRECT.
Log Level	**Synopsis:** { none, debug, info, notice, warning, error, critical, alert, emergency } **Default:** none (Optional) Determines whether or not logging will take place and at which logging level.
Protocol	**Synopsis:** { tcp, udp, icmp, all } or a string **Default:** all The protocol to match for this rule - must be 'udp' for rules using copy-dnat actions.
Source Port	**Synopsis:** A string **Default:** none (Optional) The TCP/UDP port(s) the connection originated from. Default: all ports. Add a single port or a list of comma-separated ports
Destination Port	**Synopsis:** A string **Default:** none (Optional) The TCP/UDP port(s) the connection is destined for. Default: all ports. Add a single port or a list of comma-separated ports
Original Destination	**Synopsis:** { None } or a string **Default:** none (Optional) The destination IP address in the connection request as it was received by the firewall - (mandatory) for rules using copy-dnat actions.
Description	**Synopsis:** A string

Parameter	Description
	(Optional) The description string for this rule.

7. Configure the source zone for the rule. For more information, refer to Section 6.8.15.3, "Configuring the Source Zone".
8. Configure the destination zone for the rule. For more information, refer to Section 6.8.15.4, "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 6.8.15.3
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.

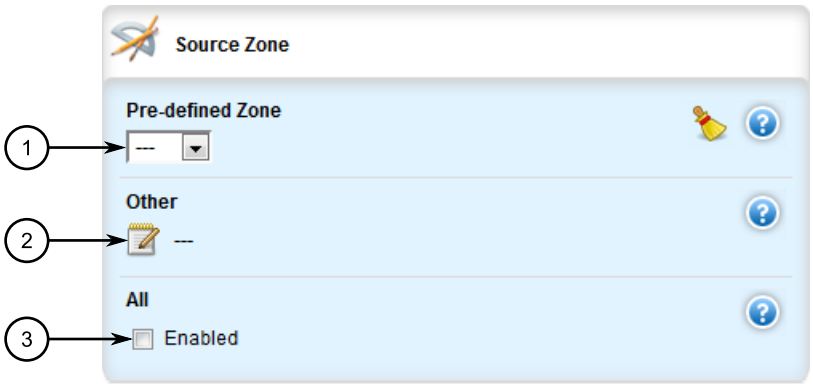


Figure 229: Source Zone Form

1. Pre-Defined Zone List **2.** Other Box **3.** All Check Box

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

Parameter	Description
Pre-Defined Zone	**Synopsis:** A string A predefined zone
Other	**Synopsis:** 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 6.8.15.4
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.

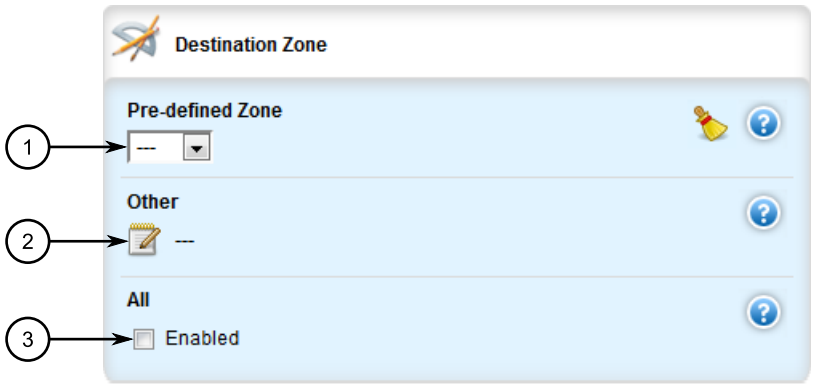


Figure 230: Destination Zone Form

1. Pre-Defined Zone List **2.** Other Box **3.** All Check Box

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

Parameter	Description
Pre-Defined Zone	**Synopsis:** A string A pre-defined zone
Other	**Synopsis:** 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 6.8.15.5
Deleting a Rule

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 **Rules** table appears.

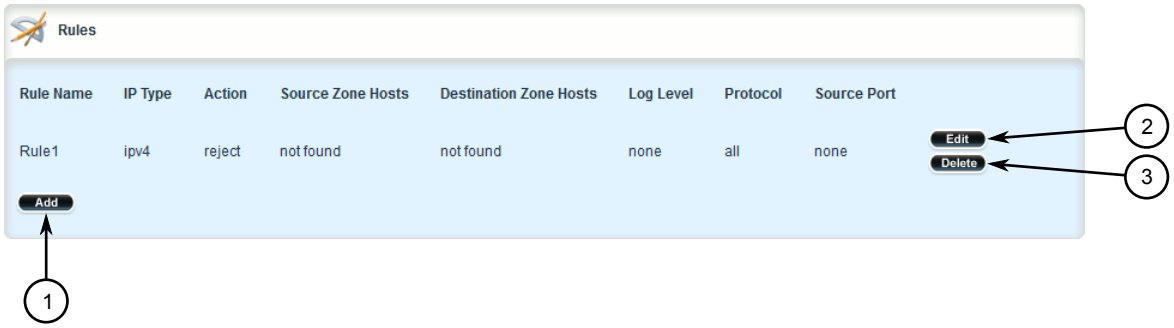


Figure 231: Rules Table

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

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 6.8.16

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.

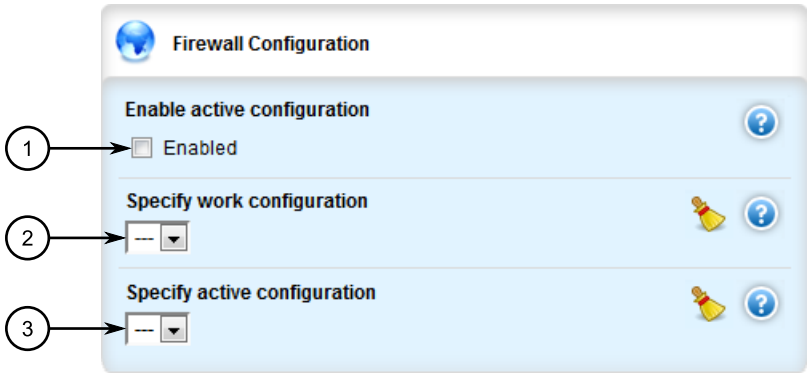


Figure 232: Firewall Configuration Form

1. Enable Active Configuration Check Box **2.** Specify Work Configuration List **3.** Specify Active Configuration List

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 6.8.17

Enabling/Disabling a Firewall

To enable or disable the firewall, do the following:

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

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to ***security » firewall***. The **Firewall Configuration** form appears.

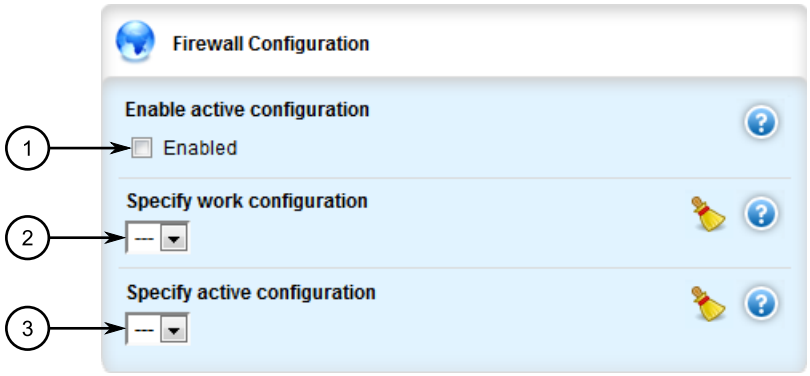


Figure 233: Firewall Configuration Form

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.

7 IP Address Assignment

This chapter describes features related to the assignment of IP addresses, such as DHCP and DNS.

CONTENTS

Section 7.1

Managing IP Addresses for Routable Interfaces

This section describes how to manage IP address for routable interfaces.

CONTENTS

Section 7.1.1

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.*

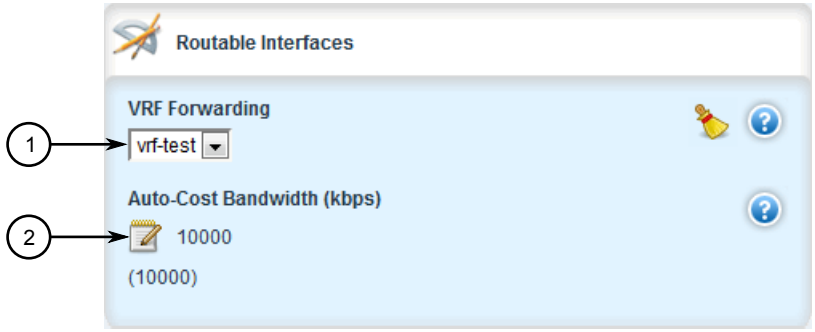


Figure 234: Routable Interfaces Form

1. VRF Forwarding List **2.** Auto-Cost Bandwidth Box

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

Parameter	Description
Auto-Cost Bandwidth (kbps)	**Synopsis:** A 64-bit unsigned integer between 1 and 10000000000 **Default:** 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 7.1.2

Viewing Statistics for Routable Interfaces

To view basic statistics for all routable interfaces, navigate to ***interfaces » ip***. The **Routeable Interface Statistics** form appears.

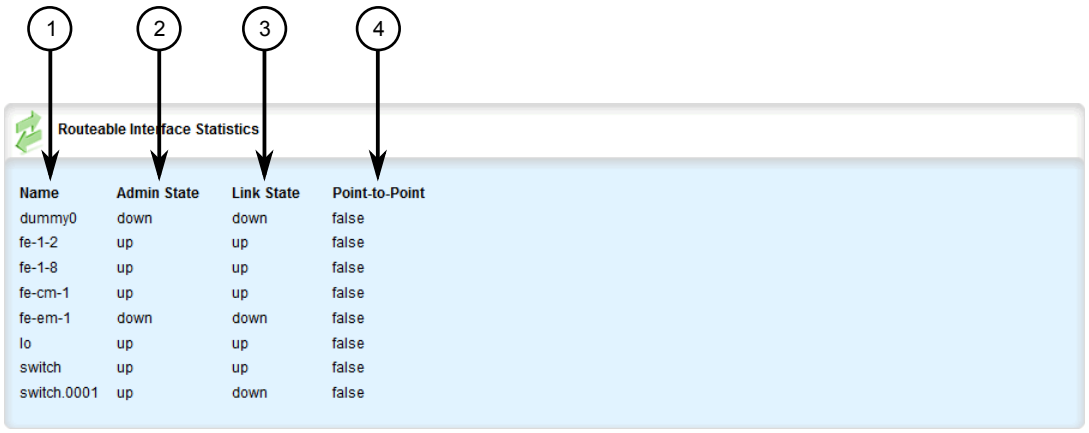


Figure 235: Routeable Interface Statistics Form

1. Name **2.** Admin State **3.** Link State **4.** Point-to-Point

This table displays the following information:

Parameter	Description
Name	**Synopsis:** A string 1 to 15 characters long The name of the interface.
Admin State	**Synopsis:** { not set, up, down, testing, unknown, dormant, notPresent, lowerLayerDown } The port's administrative status. This parameter is mandatory.
State	**Synopsis:** { not set, up, down, testing, unknown, dormant, notPresent, lowerLayerDown } Shows whether the link is up or down. This parameter is mandatory.
Point-to-Point	**Synopsis:** { true, false } The point-to-point link. This parameter is mandatory.

To view statistics for specific routable interfaces, navigate to ***interfaces » ip » {interfaces}***, where *{interfaces}* is the name of the routable interface. The **Key Settings**, **Routable Interface Statistics**, **Receive Statistics** and **Transmit Statistics** forms appear.

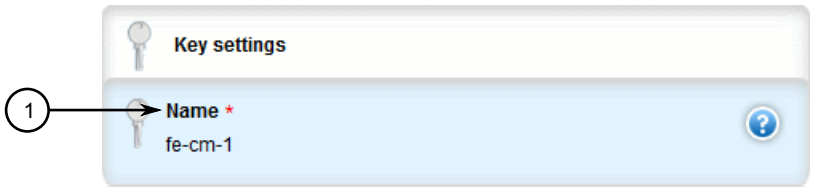


Figure 236: Key Settings Form

1. Name

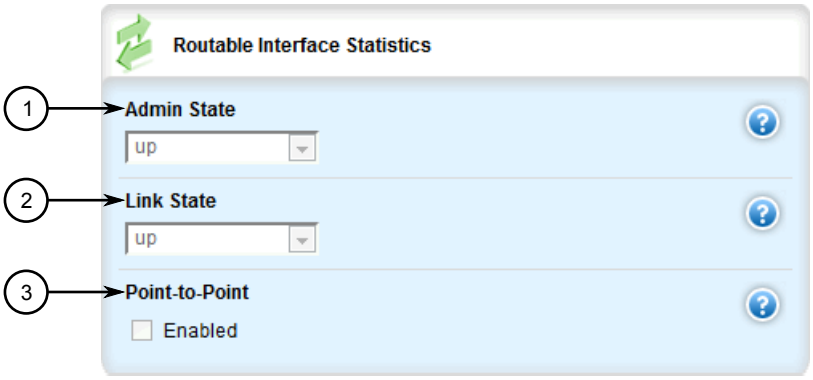


Figure 237: Routeable Interface Statistics Form

1. Admin State List **2.** Link State List **3.** Point-to-Point Check Box

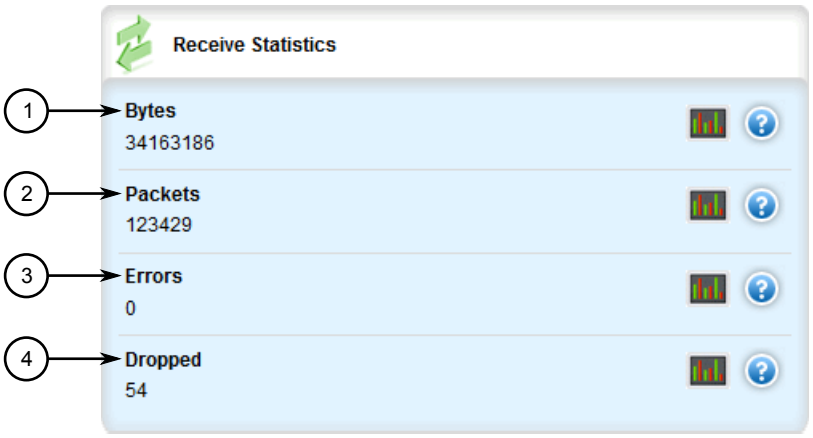


Figure 238: Receive Statistics Form

1. Bytes **2.** Packets **3.** Errors **4.** Dropped

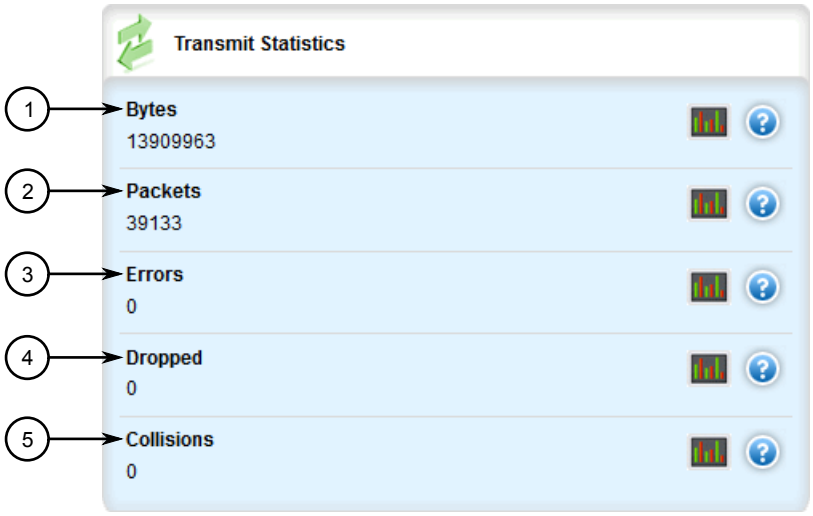


Figure 239: Transmit Statistics Form

1. Bytes **2.** Packets **3.** Errors **4.** Dropped **5.** Collisions

These forms display the following information:

Parameter	Description
Name	**Synopsis:** A string 1 to 15 characters long The name of the interface.
Admin State	**Synopsis:** { not set, up, down, testing, unknown, dormant, notPresent, lowerLayerDown } The port's administrative status. This parameter is mandatory.
State	**Synopsis:** { not set, up, down, testing, unknown, dormant, notPresent, lowerLayerDown } Shows whether the link is up or down. This parameter is mandatory.
Point-to-Point	**Synopsis:** { true, false } The point-to-point link. This parameter is mandatory.
Bytes	**Synopsis:** A 64-bit unsigned integer The number of bytes received. This parameter is mandatory.
Packets	**Synopsis:** A 64-bit unsigned integer The number of packets received. This parameter is mandatory.
Errors	**Synopsis:** A 32-bit unsigned integer The number of error packets received. This parameter is mandatory.
Dropped	**Synopsis:** A 32-bit unsigned integer The number of packets dropped by the receiving device. This parameter is mandatory.

Parameter	Description
Bytes	**Synopsis:** A 64-bit unsigned integer The number of bytes transmitted. This parameter is mandatory.
Packets	**Synopsis:** A 64-bit unsigned integer The number of packets transmitted. This parameter is mandatory.
Errors	**Synopsis:** A 32-bit unsigned integer The number of error packets transmitted. This parameter is mandatory.
Dropped	**Synopsis:** A 32-bit unsigned integer The number of packets dropped by the transmitting device. This parameter is mandatory.
Collisions	**Synopsis:** A 32-bit unsigned integer The number of collisions detected on the port. This parameter is mandatory.

Section 7.1.3
Managing IPv4 Addresses

This section describes how to manage IPv4 addresses for a routable interface.

CONTENTS

Section 7.1.3.1
Viewing a List of IPv4 Addresses

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.

Figure 240: Addresses Table

If no addresses have been configured, add addresses as needed. For more information, refer to Section 7.1.3.2, "Adding an IPv4 Address".

Section 7.1.3.2
Adding an IPv4 Address

To add an IPv4 address to a routable interface, do the following:

1. 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 241: Key Settings Form

1. Address Box **2.** Add Button

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

Parameter	Description
IP Address	**Synopsis:** 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.

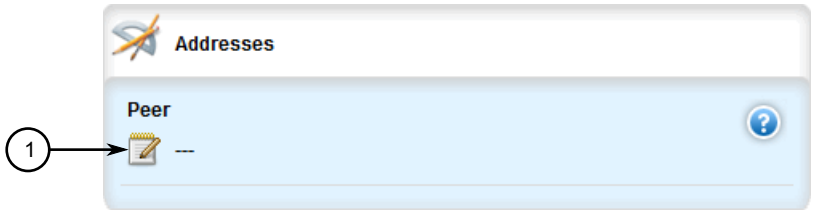


Figure 242: Addresses Form

1. Peer Box

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

Parameter	Description
peer	**Synopsis:** 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 7.1.3.3
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.

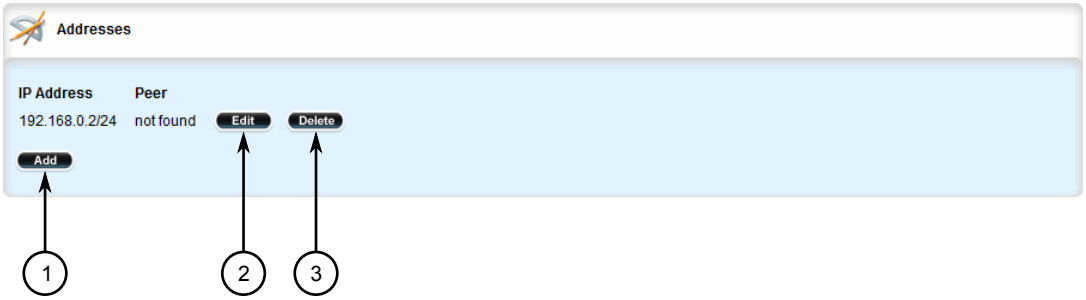


Figure 243: Addresses Table

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 7.1.4
Managing IPv6 Addresses

This section describes how to manage IPv6 addresses for a routable interface.

CONTENTS

Section 7.1.4.1
Viewing a List of IPv6 Addresses

To view a list of IPv6 address for a specific 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.

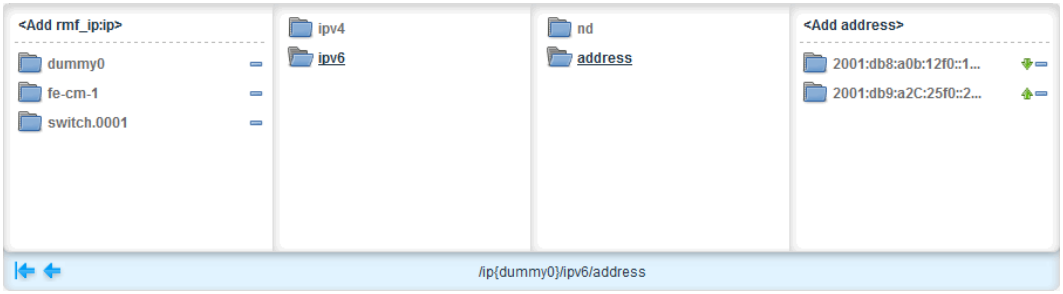


Figure 244: IPv6 Address Menu

If no addresses have been configured, add addresses as needed. For more information, refer to Section 7.1.4.2, "Adding an IPv6 Address".

Section 7.1.4.2

Adding an IPv6 Address

To add an IPv6 address to a routable interface, do the following:

1. 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.

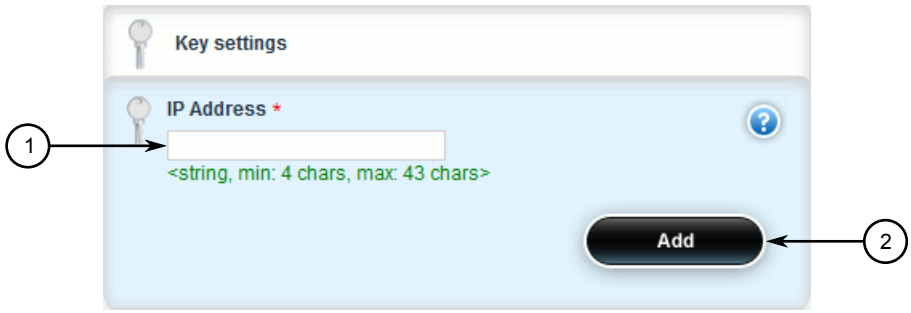


Figure 245: Key Settings Form

1. Address Box **2.** Add Button

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

Parameter	Description
IP Address	**Synopsis:** 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 7.1.4.3
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 7.1.5
Configuring IPv6 Neighbor Discovery

The Neighbor Discovery (ND) protocol in IPv6 is a replacement for IPv4 ARP messages. The protocol uses ICMPv6 messages with for various purposes including:

- Find a link-layer address of a neighbor
- Discover neighbor routers
- Determine any change in the link-layer address
- Determine when a neighbor is down
- Send network information from routers to hosts, which includes hop limit, MTU size, determining the network prefix used on a link, address auto configuration, and the default route information

The Neighbor Discovery protocol uses five types of ICMPv6 messages:

- **Router Solicitation (ICMPv6 type 133)**

  This message is sent by hosts to routers as a request to router advertisement message. It uses a destination multicast address (i.e. FF02:2).

- **Router Advertisement Messages (ICMPv6 type 134)**

  This message is used by routers to announce its presence in a network. The message includes network information related to IPv6 prefixes, default route, MTU size, hop limit and auto configuration flag. It uses a destination multicast address (i.e. FF02:1).

- **Neighbor Solicitation Messages (ICMPv6 type 135)**

  This message is sent by hosts to determine the existence of another host on the same link. The goal is to find the link-layer of neighboring nodes.

- **Neighbor Advertisement Messages (ICMPv6 type 136)**

  This message is sent by hosts to indicate the existence of the host and it provides information about its own link-layer address.

- **Redirect Messages (ICMPv6 type 137)**

  This message is sent by a router to inform a host about a better router to reach a particular destination address.

Neighbor Discovery should be configured on all Ethernet interfaces enabled for IPv6.

To enable and configure settings for IPv6 Neighbor Discovery, do the following:

1. 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.

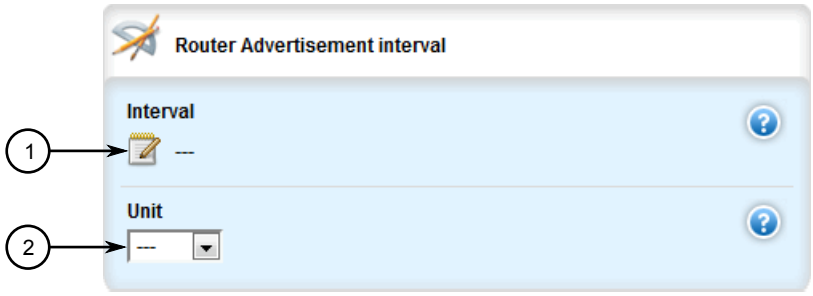


Figure 246: Router Advertisement Interval Form

1. Interval Box **2.** Unit List

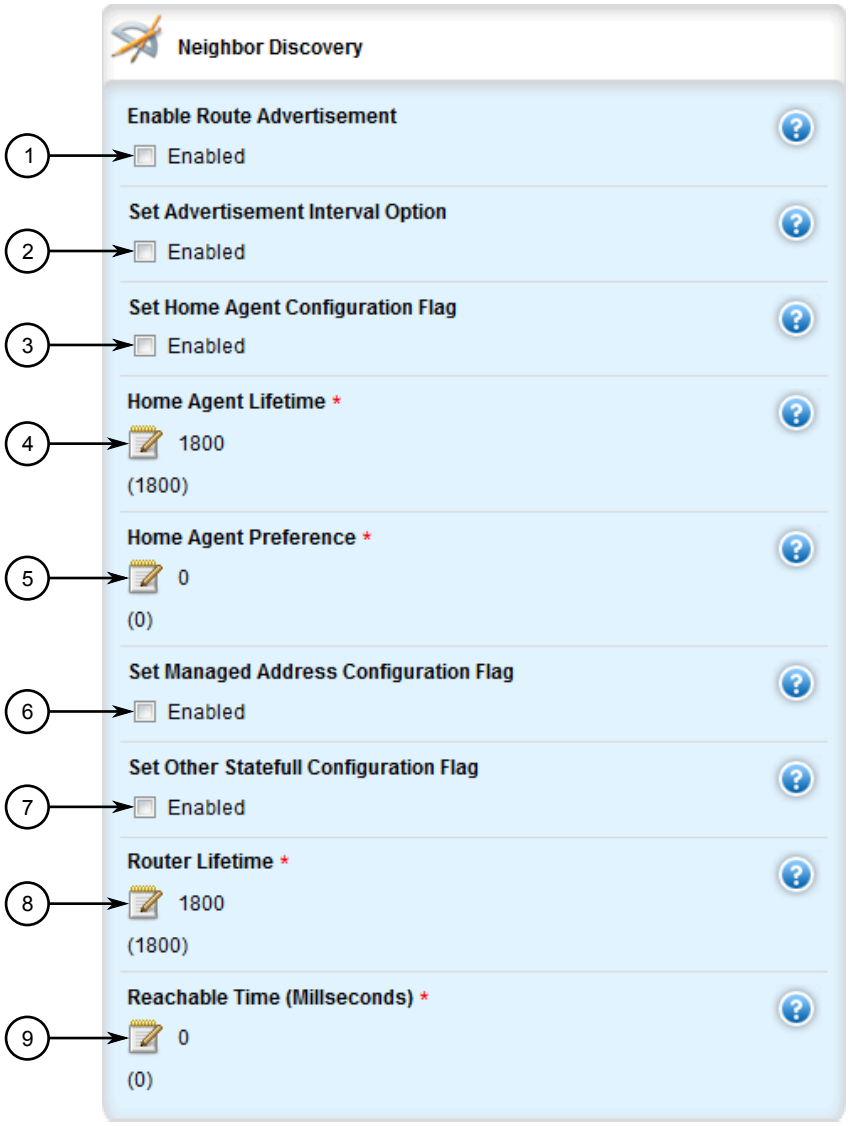


Figure 247: Neighbor Discovery Form

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	**Synopsis:** A 32-bit unsigned integer between 3 and 1800 The interval value.
Unit	**Synopsis:** { sec, msec } The interval unit.

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

Parameter	Description
Enable Route Advertisement	Enable to send router advertisement messages.
Set Advertisement Interval Option	Includes an Advertisement Interval option which indicates to hosts the maximum time in milliseconds, between successive unsolicited router advertisements.
Set Home Agent Configuration Flag	Sets/unsets the flag in IPv6 router advertisements which indicates to hosts that the router acts as a home agent and includes a home agent option.
Home Agent Lifetime	**Synopsis:** A 32-bit unsigned integer between 0 and 65520 **Default:** 1800 The value to be placed in the home agent option, when the home agent configuration flag is set, which indicates the home agent lifetime to hosts. A value of 0 means to place a router lifetime value.
Home Agent Preference	**Synopsis:** A 32-bit unsigned integer between 0 and 65535 **Default:** 0 The value to be placed in the home agent option, when the home agent configuration flag is set, which indicates the home agent preference to hosts.
Set Managed Address Configuration Flag	The flag in IPv6 router advertisements, which indicates to hosts that they should use the managed (stateful) protocol for addresses autoconfiguraiton in addition to any addresses autoconfigured using stateless address autoconfiguration.
Set Other Statefull Configuration Flag	The flag in IPv6 router advertisements, which indicates to hosts that they should use the administered (stateful) protocol to obtain autoconfiguration information other than addresses.
Router Lifetime	**Synopsis:** A 32-bit unsigned integer between 0 and 9000 **Default:** 1800 The value (in seconds) to be placed in the Router Lifetime field of router advertisements sent from the interface. Indicates the usefulness of the router as a default router on this interface. Setting the value to zero indicates that the router should not be considered a default router on this interface. It must be either zero or between the value specified with the IPv6 nd ra-interval (or default) and 9000 seconds.
Reachable Time (Millseconds)	**Synopsis:** A 32-bit unsigned integer between 0 and 3600000 **Default:** 0 The value (in milliseconds) to be placed in the Reachable Time field in the router advertisement messages sent by the router. The configured time enables the router to detect unavailable neightbors. The value zero means unspecified (by this router).

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 7.1.6, "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 7.1.6

Managing IPv6 Network Prefixes

An IPv6-capable interface can use Neighbor Discovery to advertise IPv6 network prefixes to its neighbor on the same link.

CONTENTS

- Section 7.1.6.2, "Deleting an IPv6 Network Prefix"

Section 7.1.6.1
Adding an IPv6 Network Prefix

To add a network prefix to the neighbor discovery configuration for an IPv6 address, do the following:

1. 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.

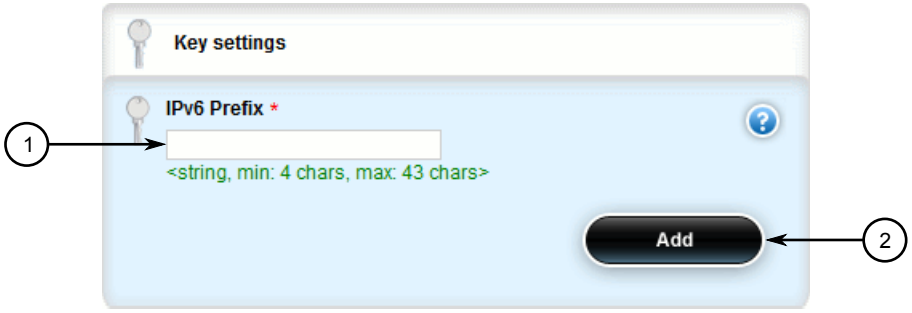


Figure 248: Key Settings Form

1. IPv6 Prefix Box **2.** Add Button

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

Parameter	Description
IPv6 Prefix	**Synopsis:** 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.

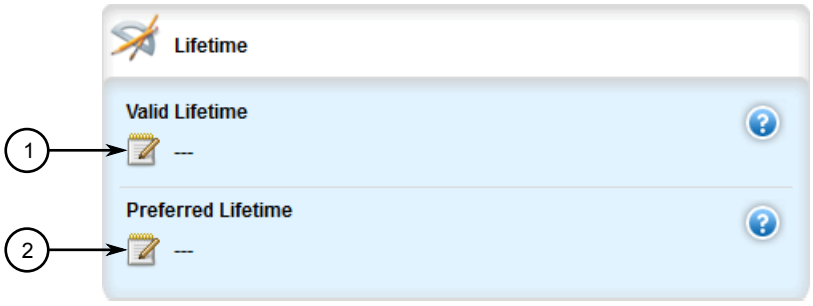


Figure 249: Lifetime Form

1. Valid Lifetime Box **2.** Preferred Lifetime Box

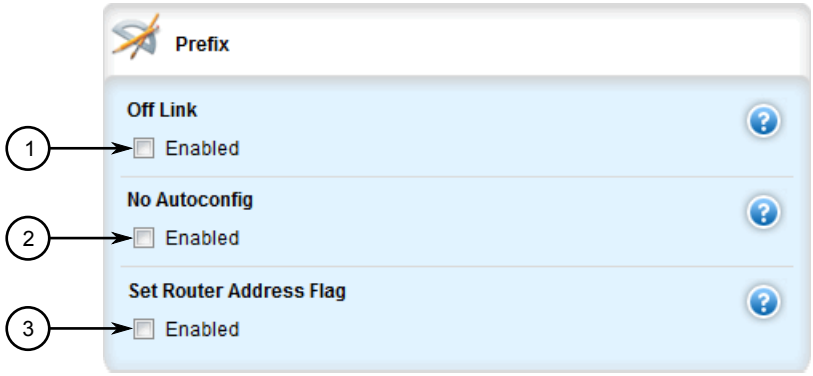


Figure 250: Prefix Form

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	**Synopsis:** { infinite } or a 32-bit unsigned integer between 0 and 4294967295 The length of time in seconds during which time the prefix is valid for the purpose of on-link determination.
Preferred Lifetime	**Synopsis:** { infinite } or a 32-bit unsigned integer between 0 and 4294967295 The length of time in seconds during which addresses generated from the prefix remain preferred.

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

Parameter	Description
Off Link	Indicates that advertisement makes no statement about on-link or off-link properties of the prefix.
No Autoconfig	Indicates to hosts on the local link that the specified prefix cannot be used for IPv6 autoconfiguration.
Set Router Address Flag	Indicates to hosts on the local link that the specified prefix contains a complete IP address by setting the R flag.

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 7.1.6.2

Deleting an IPv6 Network Prefix

To delete a network prefix to the neighbor discovery configuration for an IPv6 address, do the following:

1. 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. In the menu, click the **-** symbol next to chosen network prefix to delete it.

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 7.2

Managing the DHCP Relay Agent

A DHCP Relay Agent is a device that forwards DHCP packets between clients and servers when they are not on the same physical LAN segment or IP subnet. The feature is enabled if the DHCP server IP address and a set of access ports are configured.

DHCP Option 82 provides a mechanism for assigning an IP Address based on the location of the client device in the network. Information about the client's location can be sent along with the DHCP request to the server. Based on this information, the DHCP server makes a decision about an IP Address to be assigned.

DHCP Relay Agent takes the broadcast DHCP requests from clients received on the configured access port and inserts the relay agent information option (Option 82) into the packet. Option 82 contains the VLAN ID (2 bytes) and the port number of the access port (2 bytes: the circuit ID sub-option) and the switch's MAC address (the remote ID sub-option). This information uniquely defines the access port's position in the network. For example, in RUGGEDCOM ROX II, the Circuit ID for VLAN 2 on Line Module (LM) 4 Port 15 is `00:00:00:02:04:0F`.

The DHCP Server supporting DHCP Option 82 sends a unicast reply and echoes Option 82. The DHCP Relay Agent removes the Option 82 field and broadcasts the packet to the port from which the original request was received.

The DHCP Relay Agent communicates to the server on a management interface. The agent's IP address is the address configured for the management interface.

RUGGEDCOM ROX II can be configured to act as a DHCP Relay Agent that forwards DHCP and BOOTP requests from clients on one Layer 2 network to one or more configured DHCP servers on other networks. This allows the implementation of some measure of isolation between DHCP clients and servers.

The DHCP Relay Agent is configured to listen for DHCP and BOOTP requests on particular Ethernet and VLAN network interfaces, and to relay to a list of one or more DHCP servers. When a request is received from a client, RUGGEDCOM ROX II forwards the request to each of the configured DHCP servers. When a reply is received from a server, RUGGEDCOM ROX II forwards the reply back to the originating client.

NOTE
While DHCP Relay and DHCP Server may both be configured to run concurrently, they may not be configured to run on the same network interface.

CONTENTS

Section 7.2.1
Configuring the DHCP Relay Agent

To configure the DHCP relay agent, do the following:

1. Assign an IP address to the DHCP Server where DHCP queries are to be forwarded. For more information, refer to Section 7.2.2, "Assigning a DHCP Server Address".

   NOTE
   If client ports do not reside on the same subnet, make sure to assign the client ports to different VLANs.

2. Add client ports. For more information, refer to Section 7.2.4, "Adding a DHCP Client Port".
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 7.2.2
Assigning a DHCP Server Address

To assign a DHCP server address to 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.

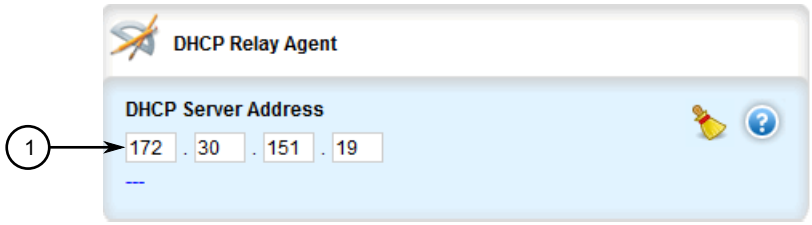


Figure 251: DHCP Relay Agent Form

1. DHCP Server Address Box

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

Parameter	Description
DHCP Server Address	**Synopsis:** A string The IP address of the DHCP server to which DHCP queries will be forwarded from this relay agent.

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 7.2.3
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.

Figure 252: DHCP Relay Agent Client Ports Table

If no client ports have been configured, add client ports as needed. For more information, refer to Section 7.2.4, "Adding a DHCP Client Port".

Section 7.2.4
Adding a DHCP Client Port

To add a client port for the DHCP relay agent, do the following:

1. 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.

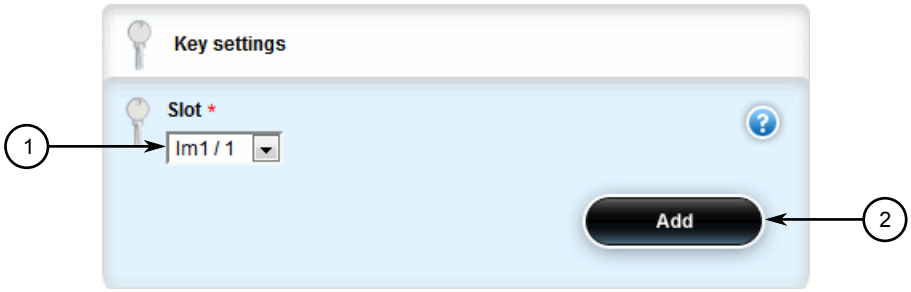


Figure 253: Key Settings Form

1. Slot List **2.** Add Button

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

Parameter	Description
Slot	**Synopsis:** A string The name of the module location provided on the silkscreen across the top of the device.
Port	**Synopsis:** A string The selected ports on the module installed in the indicated slot.

4. Click **Add** to add the client 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 7.2.5
Deleting a DHCP Client Port

To delete 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***. The **DHCP Relay Agent Client Ports** table appears.

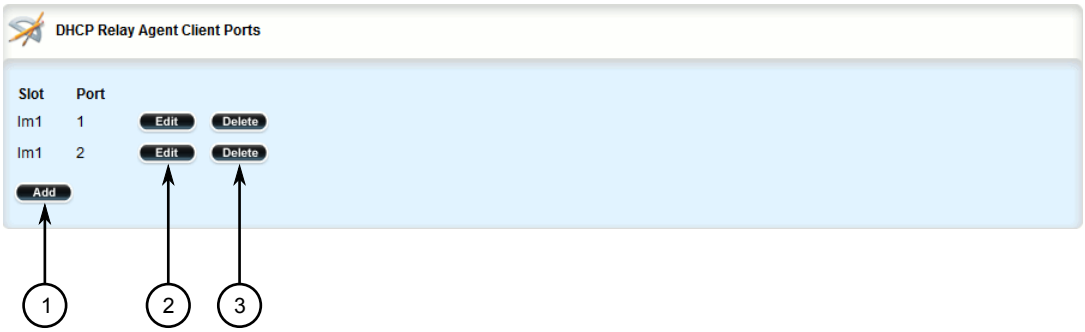


Figure 254: DHCP Relay Agent Client Ports Table

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

3. Click **Delete** next to the chosen client 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 7.2.6
Example: Configuring the Device as a Relay Agent

This example demonstrates how to configure the device as a DHCP relay agent.

The following topology depicts a scenario where two clients on separate LANs require IP addresses on different subnets from a DHCP server. Each client connects to the DHCP relay agent using different VLANs. The DHCP relay agent manages the requests and responses between the clients and the DHCP server.

IMPORTANT!
The values shown are specific to the provided topology. Actual values can vary based on the user's configuration.

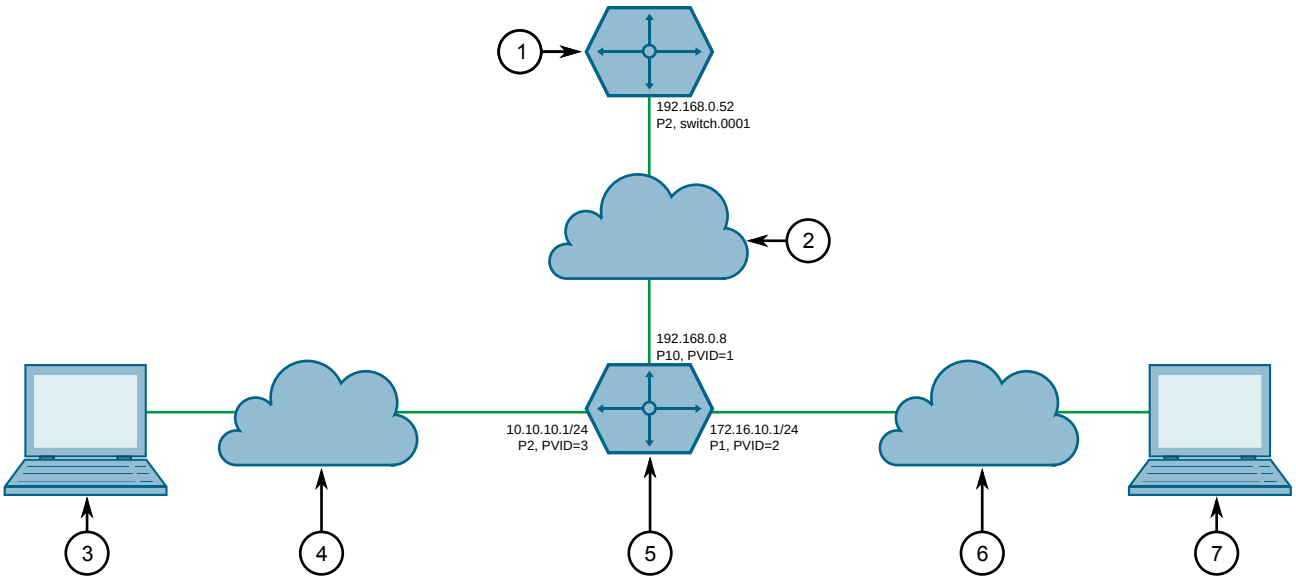


Figure 255: Topology – Device as a Relay Agent

1. DHCP Server **2.** LAN A **3.** Client 2 **4.** LAN B **5.** DHCP Relay Agent (RUGGEDCOM ROX II Device) **6.** LAN C **7.** Client 1

To configure the device as a DHCP relay agent per the topology, do the following:

1. Configure the device as a DHCP relay agent:
   a. Add VLAN 2 and VLAN 3. For more information, refer to Section 8.5.5.2, "Adding a Static VLAN".
   b. Assign IP address *192.168.0.8* to VLAN 1. For more information, refer to Section 7.1.3.2, "Adding an IPv4 Address" or Section 7.1.4.2, "Adding an IPv6 Address".
   c. Change the PVID of port 1 to PVID 2, and change the PVID of port 2 to PVID 3. Refer to Section 8.1.2, "Configuring a Switched Ethernet Port" for more information.
2. Configure a separate device as the DHCP Server. If the DHCP server being used is a RUGGEDCOM ROX II device, refer to Section 7.3.19, "Example: Configuring the Device as a DHCP Server to Support a Relay Agent" for more information.

» Final Configuration Example

The following configuration reflects the topology:

```
# show running-config switch dhcp-relay-agent
 dhcp-server-address 192.168.0.52
 dhcp-client-ports lm4 1
 !
 dhcp-client-ports lm4 2
 !
```

Section 7.3
Managing the DHCP Server

Dynamic Host Configuration Protocol (DHCP) is a method for centrally and consistently managing IP addresses and settings for clients, offering a variety of assignment methods. IP addresses can be assigned based on the Ethernet MAC address of a client either sequentially or by using port identification provided by a DHCP relay agent device.

The information that is assigned to addresses in DHCP is organized to deal with clients at the interface, subnet, pool, shared network, host-group and host levels.

RUGGEDCOM ROX II supports both IPv4 and IPv6 address assignments.

CONTENTS

Section 7.3.1
Viewing a List of Active Leases

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:
   - **For IPv4**
     services » dhcpserver

- **For IPv6**
  services » dhcpserver6

2. Click **show-active-leases** in the menu. The **Trigger Action** form appears.

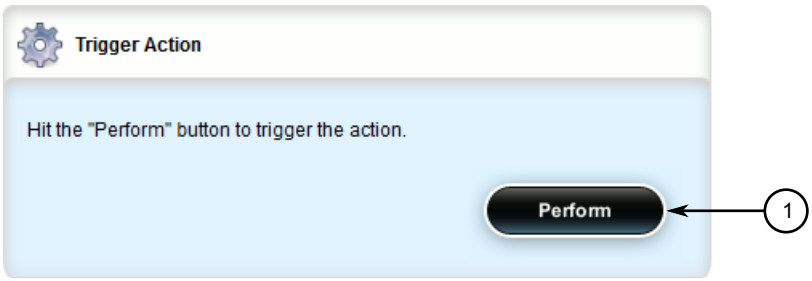


Figure 256: Trigger Action Form

1. Perform Button

3. Click **Perform**. The **Show Active Leases** table appears listing the active DHCP leases.

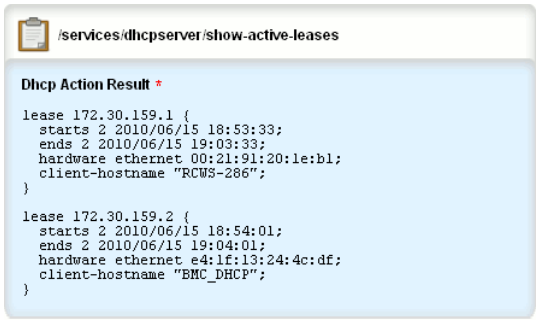


Figure 257: Show Active Leases

Section 7.3.2

Configuring the DHCP Server

To configure the DHCP server, do the following:

NOTE
This procedure outlines the basic steps required to configure the device as a DHCP server. For a configuration example that includes a DHCP relay agent, refer to Section 7.3.19, "Example: Configuring the Device as a DHCP Server to Support a Relay Agent".

1. [Optional] Configure a separate device as a DHCP relay agent. The relay agent may be a RUGGEDCOM ROX II device, a RUGGEDCOM ROS device, or a third party device with relay agent capabilities.

   If the relay agent being used is a RUGGEDCOM ROX II device, refer to Section 7.2.6, "Example: Configuring the Device as a Relay Agent" for more information.

2. Enable the DHCP server. For more information, refer to Section 7.3.3, "Enabling/Disabling the DHCP Server".

3. Add a DHCP listen interface. For more information, refer to Section 7.3.6.2, "Adding a DHCP Listen Interface".
4. Assign an IP address to the listen interface. For more information, refer to Section 7.3.8.2, "Adding a Subnet".
5. Create a shared network and enable Option82. For more information, refer to Section 7.3.7.2, "Adding a Shared Network" and Section 7.3.7.3, "Configuring Shared Network Options".
6. Create a subnet for each LAN that has DHCP clients. For more information about creating subnets, refer to Section 7.3.8.2, "Adding a Subnet".
7. [Optional] If a dynamic IP address is needed for the relay agent, create a subnet for the DHCP relay agent. For more information about creating subnets, refer to Section 7.3.8.2, "Adding a Subnet".
8. For each client subnet (excluding the subnet for the DHCP relay agent, if used), do the following:
   a. Create one or more IP address pools to define a range of IP addresses for each client.

      For more information about IP address pools, refer to Section 7.3.11.2, "Adding an Address Pool (IPv4)" or Section 7.3.12.2, "Adding an Address Pool (IPv6)".

      For more information about IP ranges, refer to Section 7.3.13.2, "Adding an IP Range (IPv4)" or Section 7.3.14.2, "Adding an IP Range (IPv6)".

   b. [Optional] Configure the option82 class on the relay agent, if used. For more information, refer to Section 7.3.18.2, "Adding an Option 82 Class to an Address Pool".
9. [Optional] Add and configure hosts and host-groups. For more information, refer to Section 7.3.10.2, "Adding a Host".

Section 7.3.3

Enabling/Disabling the DHCP Server

To enable or disable the DHCP server, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to:
   - **For IPv4**
     services » dhcpserver
   - **For IPv6**
     services » dhcpserver6
3. The **Dynamic Host Control Protocol (DHCP) Server** form appears.

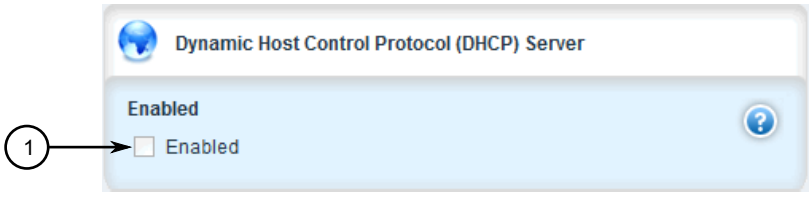


Figure 258: Dynamic Host Control Protocol (DHCP) Server Form (IPv4)

1. Enabled Check Box

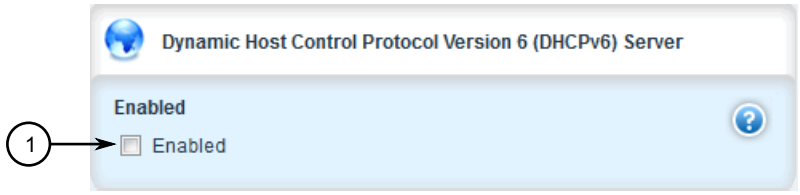


Figure 259: Dynamic Host Control Protocol (DHCP) Server Form (IPv6)

1. Enabled Check Box

4. Configure the following parameter(s) as required:
   - **For IPv4**

Parameter	Description
enabled	Enables and disables the the DHCP server.

   - **For IPv6**

Parameter	Description
enabled	Enables and disables the DHCPv6 server.

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 7.3.4
Configuring DHCP Server Options

To configure options for the DHCP server, do the following:

NOTE
Options set at the subnet level override options set at the DHCP server level.

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to:
   - **For IPv4**
     services » dhcpserver » options
   - **For IPv6**
     services » dhcpserver6 » options
3. The **Leased Configuration** and **Client Options** forms appear.

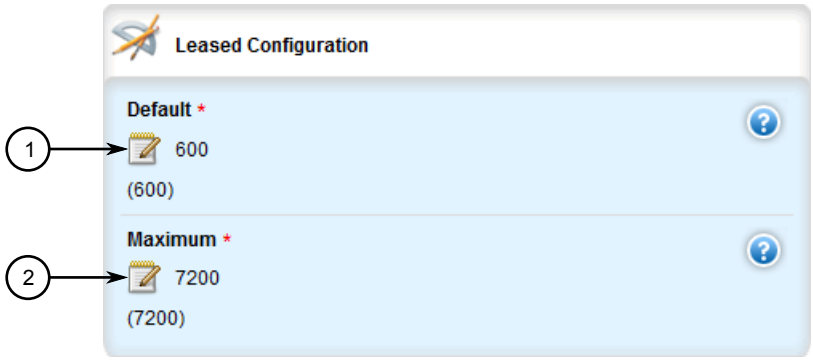


Figure 260: Leased Configuration Form

1. Default Box **2.** Maximum Box

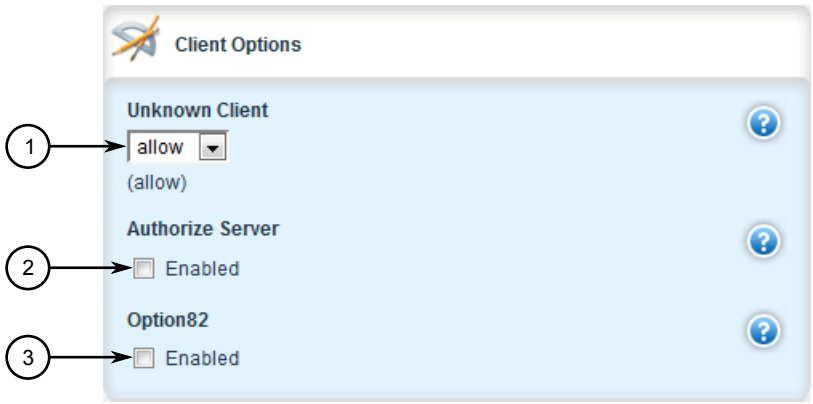


Figure 261: Client Options Form (IPv4)

1. Unknown Client Box **2.** Authorize Server Box **3.** Option 82 Box

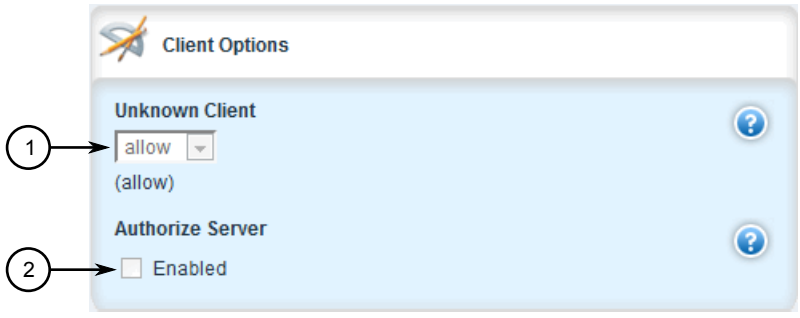


Figure 262: Client Options Form (IPv6)

1. Unknown Client Box **2.** Authorize Server Box

4. In the **Leased Configuration** form, configure the following parameters as required:

Parameter	Description
default	**Synopsis:** A 32-bit unsigned integer **Default:** 600 The minimum leased time in seconds that the server offers to the clients.
maximum	**Synopsis:** A 32-bit unsigned integer **Default:** 7200 The maximum leased time in seconds that the server offers to the clients.

5. In the **Client Options** form, configure the following parameters as required:

IMPORTANT!
For IPv4 only:

If DHCP relay (or Option 82) clients are used on the same subnet as the DHCP server, some clients will try to renew a lease immediately after receiving it by requesting a renewal directly from the DHCP server. Because the DHCP server is configured by default to only provide the lease through a relay agent configured with the current Option 82 fields, the server sends the client a NAK (negative acknowledgment or not acknowledged) message to disallow the lease. Enabling Option 82 disables the NAK message so the renewal request sent from the DHCP relay agent (which the DHCP server accepts, since it has the correct Option 82 fields added) is the only message for which the client receives a reply.

Option 82 support should only be enabled If the DHCP server and clients are on the same subnet.

The meaning of most Option 82 fields is determined by the DHCP relay client. To determine which values are required by the client for special options, refer to the client documentation.

DHCP relay support can also be enabled on individual subnets. For more information, refer to Section 7.3.8.3, "Configuring Subnet Options".

Parameter	Description
Unknown Client	**Synopsis:** { allow, deny, ignore } The action to take for previously unregistered clients
Authorize Server	Enables/disables the server's authorization on this client. If enabled, the server will send deny messages to the client that is trying to renew the lease, which the server knows the client shouldn't have.
option82	Enables/disables the NAK of option 82 clients for this subnet.

6. [Optional] Configure additional client configuration options. For more information, refer to Section 7.3.5.1, "Configuring Standard DHCP Client Configuration Options (IPv4)" or Section 7.3.5.2, "Configuring Standard DHCP Client Configuration Options (IPv6)".
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 7.3.5

Managing DHCP Client Configuration Options

Standard and custom options can be configured globally at the DHCP server level, or for specific shared networks, subnets, host groups or hosts. Options set at an individual level override options set at the global level.

CONTENTS

Section 7.3.5.1

Configuring Standard DHCP Client Configuration Options (IPv4)

Configuration options for DHCP clients can be configured globally or for an individual shared network, subnet, host group or host.

NOTE
Options set for individual shared networks, subnets, host groups or hosts override the options set at the global level.

To configure client options, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to ***services » dhcpserver » {path} » options***, where *path* is the path to and name of the desired shared network, subnet, host group or host. For example, to access the options for a shared network named *Shared*, navigate to:

   services » dhcpserver » shared-network » Shared » options

   To access options at the global level, navigate to:

   services » dhcpserver » options

   In all cases, the **Client Options**, **NIS Configuration** and **NetBios Configuration** forms appear.

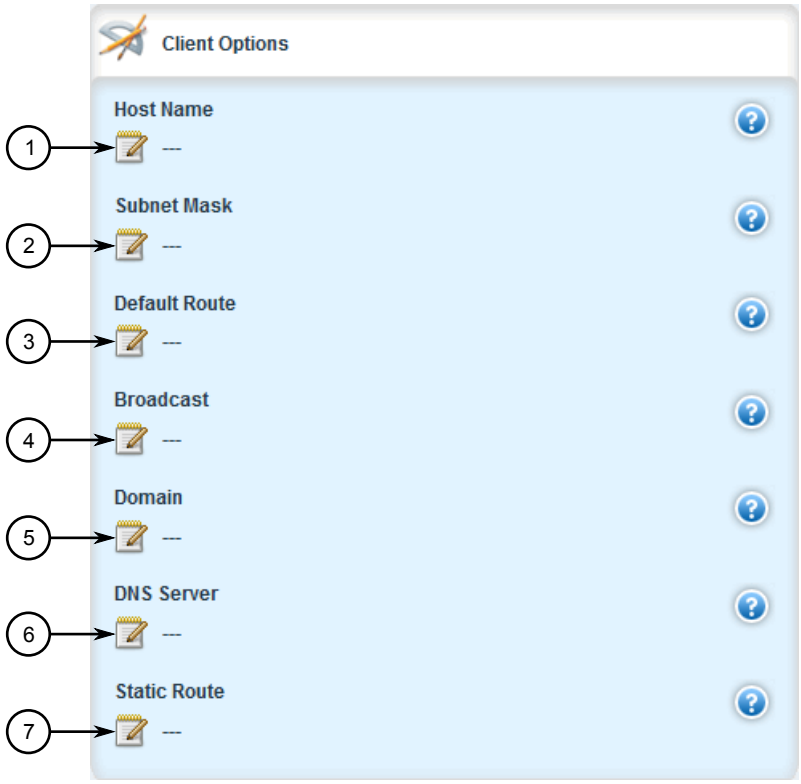


Figure 263: Client Options Form

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

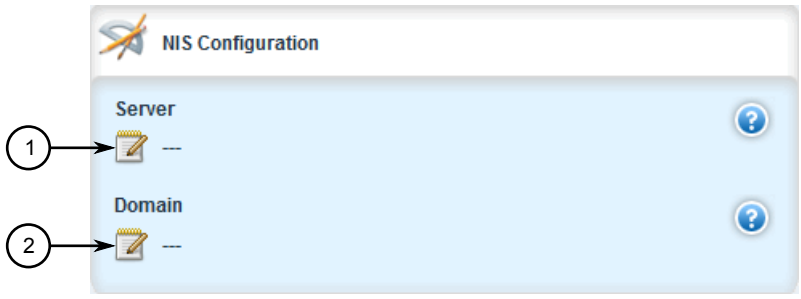


Figure 264: NIS Configuration Form

1. Server Box **2.** Domain Box

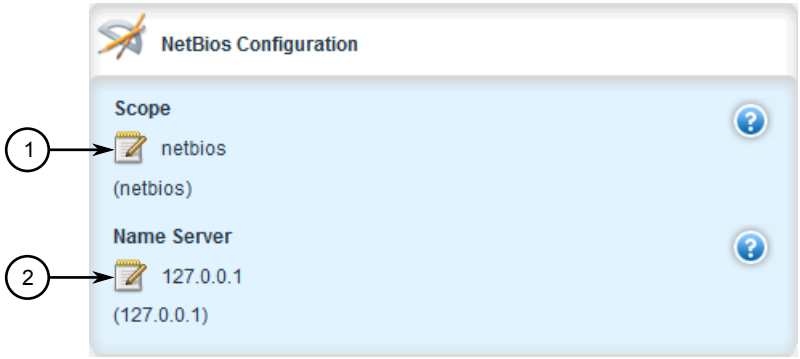


Figure 265: NetBios Configuration Form

1. Scope Box **2.** Name Server Box

3. In the **Client Options** form, configure the following parameters as required:

Parameter	Description
Host Name	**Synopsis:** A string 1 to 32 characters long The unique name to refer to the host within a DHCP configuration.
Subnet Mask	**Synopsis:** A string 7 to 15 characters long Subnet mask
Default Route	**Synopsis:** A string 7 to 15 characters long The default route that the server offers to the client when it issues the lease to the client.
broadcast	**Synopsis:** A string 7 to 15 characters long The broadcast address that the server offers to the client when it issues the lease to the client.
domain	**Synopsis:** A string 1 to 253 characters long The domain name that the server offers to the client when it issues the lease to the client.
DNS Server	**Synopsis:** A string 7 to 31 characters long The domain name server that the server offers to the client when it issues the lease to the client.
Static Route	**Synopsis:** A string 7 to 15 characters long The static route that the DHCP server offers to the client when it issues the lease to the client.

4. In the **NIS Configuration** form, configure the following parameters as required:

Parameter	Description
server	**Synopsis:** A string 7 to 15 characters long The NIS server address that the DHCP server offers to the client when it issues the lease to the client.
domain	**Synopsis:** A string 1 to 253 characters long The NIS domain name that the DHCP server offers to the client when it issues the lease to the client.

5. In the **NetBios Configuration** form, configure the following parameters as required:

Parameter	Description
scope	**Synopsis:** A string 1 to 256 characters long **Default:** netbios The NetBIOS scope that the DHCP server offers to the client when it issues the lease to the client.
Name Server	**Synopsis:** A string 1 to 256 characters long **Default:** 127.0.0.1 The NetBIOS name server that the DHCP server offers to the client when it issues the lease to the client.

6. [Optional] Add custom options. For more information, refer to Section 7.3.5.4, "Adding a Custom DHCP Client Configuration Option".
7. 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 7.3.5.2
Configuring Standard DHCP Client Configuration Options (IPv6)

Configuration options for DHCP clients can be configured globally or for an individual shared network, subnet, host group or host.

NOTE
Options set for individual shared networks, subnets, host groups or hosts override the options set at the global level.

To configure client options, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to ***services » dhcpserver6 » {path} » {name} » options***, where *path* is the path to and name of the desired shared network, subnet, host group or host and *name* is the user-added name.

   For example, to access the options for a shared network named *Shared*, navigate to:

   services » dhcpserver6 » shared-network » Shared » options

   To access options at the global level, navigate to:

   services » dhcpserver6 » options

   In all cases, the **Client Options** and **NIS Configuration** forms appear.

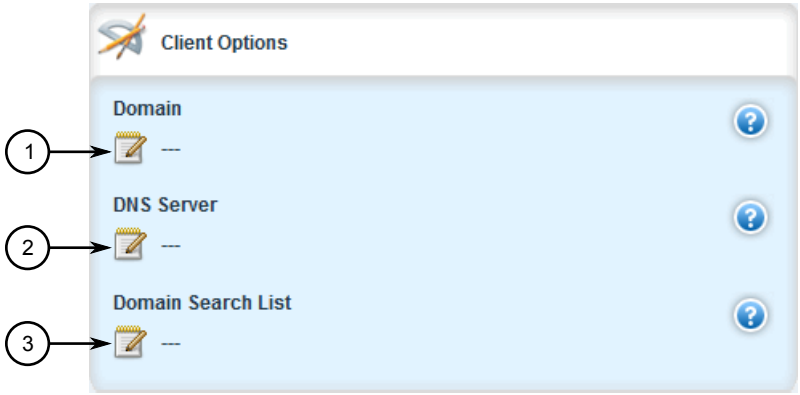


Figure 266: Client Options Form

1. Domain Box **2.** DNS Server Box **3.** Domain Search List Box

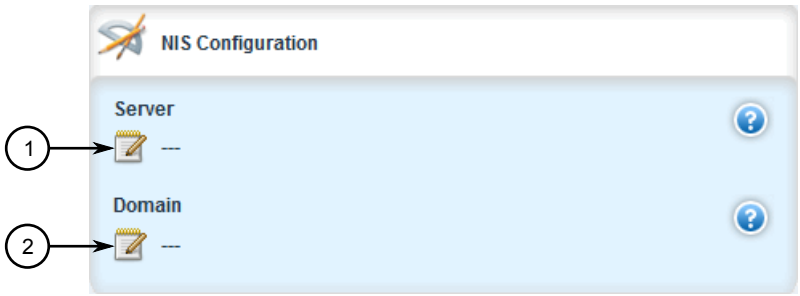


Figure 267: NIS Configuration Form

1. Server Box **2.** Domain Box

3. In the **Client Options** form, configure the following parameters as required:

Parameter	Description
domain	**Synopsis:** A string 1 to 253 characters long The domain name that the server offers to the client when it issues the lease to the client.
DNS Server	**Synopsis:** A string 6 to 87 characters long The domain name server that the server offers to the client when it issues the lease to the client.
Domain Search List	**Synopsis:** A string 1 to 773 characters long The domain search list that the server offers to the client when it issues the lease to the client.

4. In the **NIS Configuration** form, configure the following parameters as required:

Parameter	Description
server	**Synopsis:** A string 6 to 40 characters long

Parameter	Description
	The NIS server address that the DHCPv6 server offers to the client when it issues the lease to the client.
domain	**Synopsis:** A string 1 to 253 characters long The NIS domain name that the DHCPv6 server offers to the client when it issues the lease to the client.

5. [Optional] Add custom options. For more information, refer to Section 7.3.5.4, "Adding a Custom DHCP Client Configuration Option".
6. 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 7.3.5.3
Viewing a List of Custom DHCP Client Configuration Options

To view a list of custom DHCP client configuration options set at the global level or for a specific shared network, subnet, host group or host, navigate to:

- **For IPv4**
  services » dhcpserver » {path} » options » client » custom
- **For IPv6**
  services » dhcpserver6 » options » client » custom

where *path* is the path to and name of the desired shared network, subnet, host group or host.

NOTE
*Custom options at the **{path}** level are only available for IPv4.*

For example, to view the custom IPv4 options for a shared network named *Shared*, navigate to:

services » dhcpserver » shared-network » Shared » options » client » custom

To view custom IPv4 options at the global level, navigate to:

services » dhcpserver » options » client » custom

In all cases, the **Custom Configuration** table appears.

Figure 268: Custom Configuration Form

If custom configurations have not been configured, add custom configurations as needed. For more information, refer to Section 7.3.5.4, "Adding a Custom DHCP Client Configuration Option".

Section 7.3.5.4

Adding a Custom DHCP Client Configuration Option

To add a custom client option, do the following:

NOTE
The number of the option (defined by the Internet Assigned Numbers Authority or IANA) and its allowed value must be known before a custom option can be configured. For more information about available DHCP options, refer to RFC 2132 [http://tools.ietf.org/html/rfc2132].

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to:
   - **For IPv4**
     services » dhcpserver » {path} » options » client » custom
   - **For IPv6**
     services » dhcpserver6 » {path} » options » client » custom

   where *path* is the path to and name of the desired shared network, subnet, host group or host.

   NOTE
   *Custom options at the **{path}** level are only available for IPv4.*

   For example, to access the custom IPv4 options for a shared network named *Shared*, navigate to:

   services » dhcpserver » shared-network » Shared » options » client » custom

   To access custom IPv4 options at the global level, navigate to:

   services » dhcpserver » options » client » custom
3. Click **<Add custom>**. The **Key Settings** form appears.

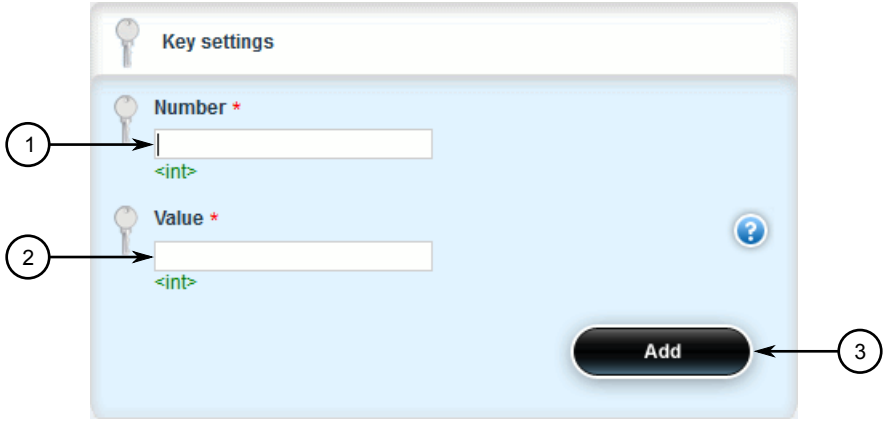


Figure 269: Key Settings Form

1. Number Box **2.** Value Box **3.** Add Button

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

Parameter	Description
number	**Synopsis:** A 32-bit signed integer

Parameter	Description
value	**Synopsis:** A 32-bit signed integer The value of the custom option.

5. Click **Add** to add the custom 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 7.3.5.5
Deleting a Custom DHCP Client Configuration Option

To delete a custom client option, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to:
   - **For IPv4**
     services » dhcpserver » {path} » options » client » custom
   - **For IPv6**
     services » dhcpserver6 » options » client » custom

   where *path* is the path to and name of the desired shared network, subnet, host group or host.

> **NOTE**
> *Custom options at the **{path}** level are only available for IPv4.*

For example, to access the custom IPv4 options for a shared network named *Shared*, navigate to:

services » dhcpserver » shared-network » Shared » options » client » custom

To access custom IPv4 options at the global level, navigate to:

services » dhcpserver » options » client » custom

In all cases, the **Custom Configuration** table appears.

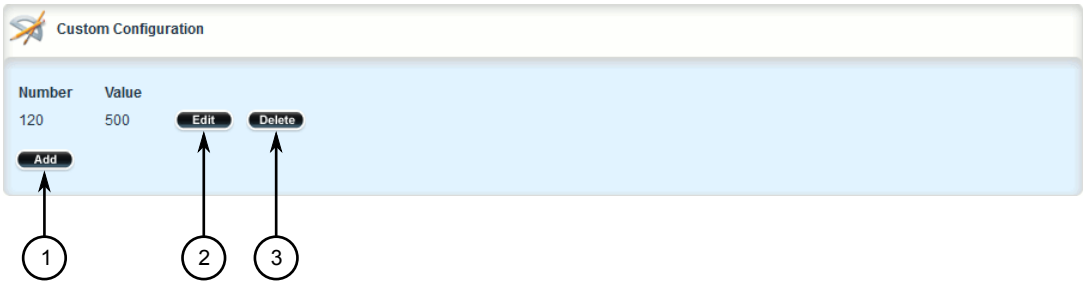


Figure 270: Custom Configuration Form

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

3. Click **Delete** next to the desired custom 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 7.3.6
Managing DHCP Listen Interfaces

DHCP listen interfaces specify the IP interface to which the client sends a request.

CONTENTS

Section 7.3.6.1
Viewing a List of DHCP Listen Interfaces

To view a list of DHCP listen interfaces, navigate to:

- **For IPv4**
  services » dhcpserver » interface
- **For IPv6**
  services » dhcpserver6 » interface

If DHCP listen interfaces have been configured, the **Listen Interfaces** table appears.

Figure 271: Listen Interfaces Table

If no DHCP listen interfaces have been configured, add interfaces as needed. For more information, refer to Section 7.3.6.2, "Adding a DHCP Listen Interface".

Section 7.3.6.2
Adding a DHCP Listen Interface

To add a DHCP listen interface, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to:
   - **For IPv4**
     services » dhcpserver » interface

- **For IPv6**
  services » dhcpserver6 » interface

3. Click **<Add interface>**. The **Key Settings** form appears.

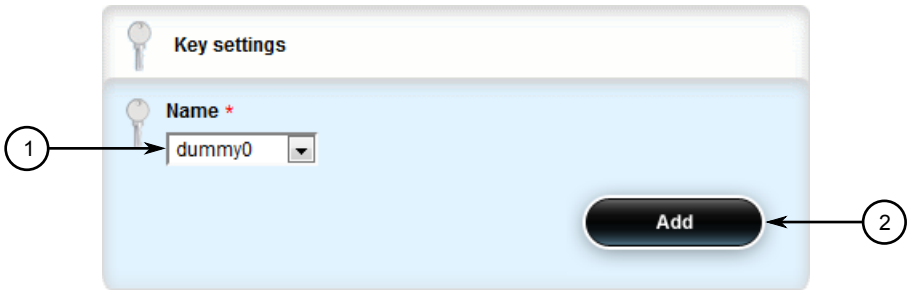


Figure 272: Key Settings Form

1. Name Box **2.** Add Button

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

Parameter	Description
name	**Synopsis:** A string

5. Click **Add** to create the new DHCP listen 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 7.3.6.3
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:
   - **For IPv4**
     services » dhcpserver » interface
   - **For IPv6**
     services » dhcpserver6 » interface

   The **Listen Interfaces** table appears.

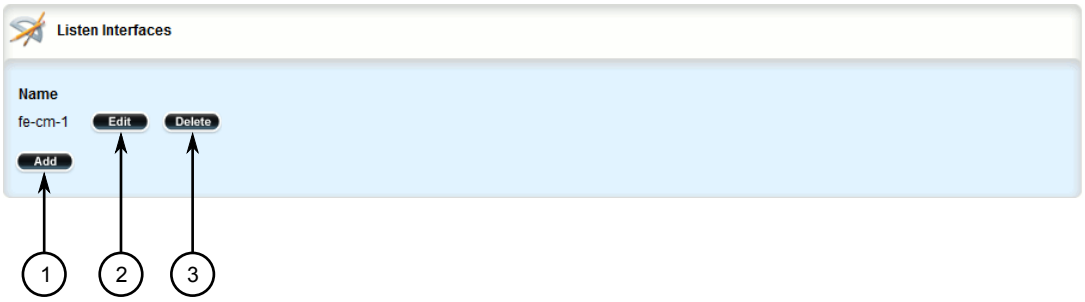


Figure 273: Listen Interfaces Table

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

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 7.3.7

Managing Shared Networks

Shared networks are used when multiple subnets should be served by a single physical port. This applies both when using a DHCP relay agent connected to the port with additional subnets behind the relay agent, or when multiple virtual networks exist on one physical interface. Each subnet then gets its own subnet definition inside the shared network rather than at the top level. Shared networks contain subnets, groups and hosts.

CONTENTS

Section 7.3.7.1

Viewing a List of Shared Networks

To view a list of shared networks, navigate to:

- **For IPv4**
  services » dhcpserver » shared-network
- **For IPv6**
  services » dhcpserver6 » shared-network

If shared networks have been configured, the **Shared network Configuration** table appears.

Figure 274: Shared Network Configuration Table

If no shared networks have been configured, add shared networks as needed. For more information, refer to Section 7.3.7.2, "Adding a Shared Network".

Section 7.3.7.2
Adding a Shared Network

To add a shared network to the DHCP server, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to:
   - **For IPv4**
     services » dhcpserver » shared-network
   - **For IPv6**
     services » dhcpserver6 » shared-network
3. Click **<Add shared-network>**. The **Key Settings** form appears.

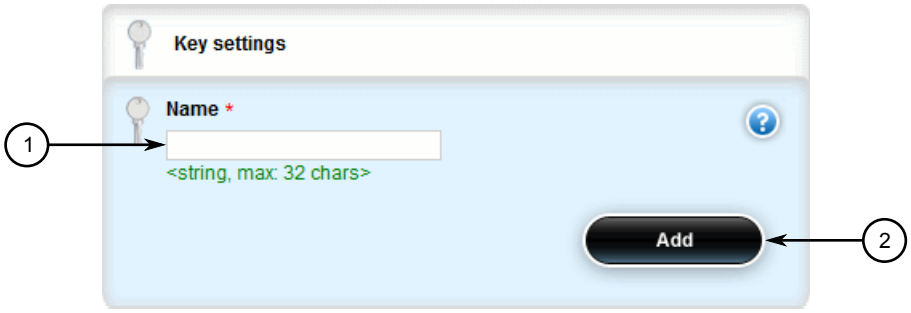


Figure 275: Key Settings Form

1. Name Box **2.** Add Button

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

Parameter	Description
name	**Synopsis:** A string 1 to 32 characters long The unique name to refer to the host within a DHCP configuration.

5. Click **Add** to create the new shared network.
6. Configure options for the shared network. For more information, refer to Section 7.3.7.3, "Configuring Shared Network Options".

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 7.3.7.3
Configuring Shared Network Options

To configure options for a shared network on the DHCP server, do the following:

> **NOTE**
> *Options set at the shared network level override options set at the DHCP server level.*

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to:
   - **For IPv4**
     services » dhcpserver » shared-network{shared network} » options
   - **For IPv6**
     services » dhcpserver6 » shared-network{shared network} » options

   Where *{shared network}* is the name of the shared network. The **Leased Configuration** and **Client Configuration** forms appear.

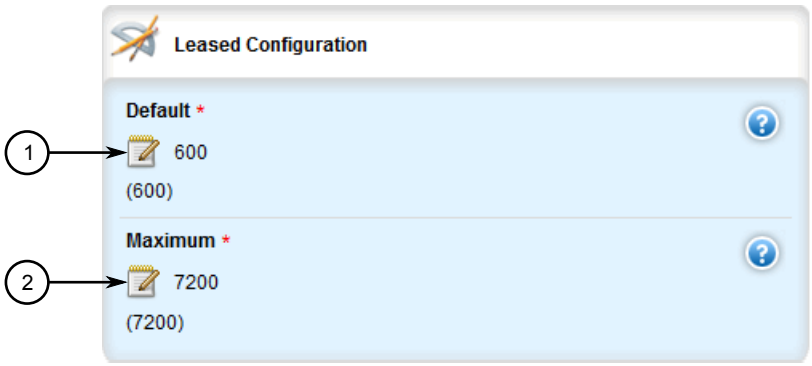


Figure 276: Leased Configuration Form

1. Default Box **2.** Maximum Box

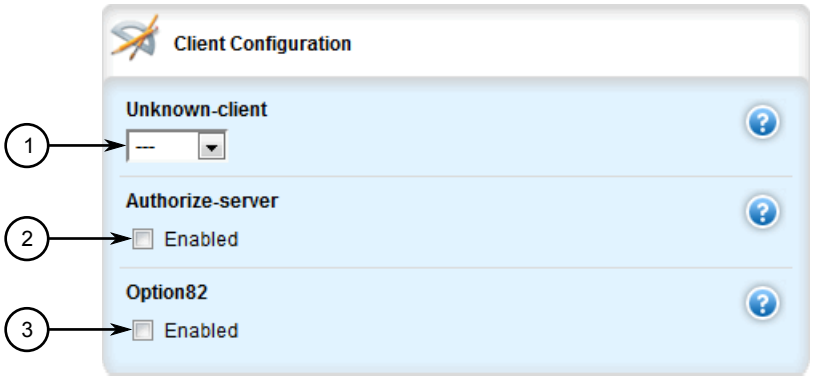


Figure 277: Client Configuration Form (IPv4)

1. Unknown Client List **2.** Authorize Server Check Box **3.** Option 82 Check Box

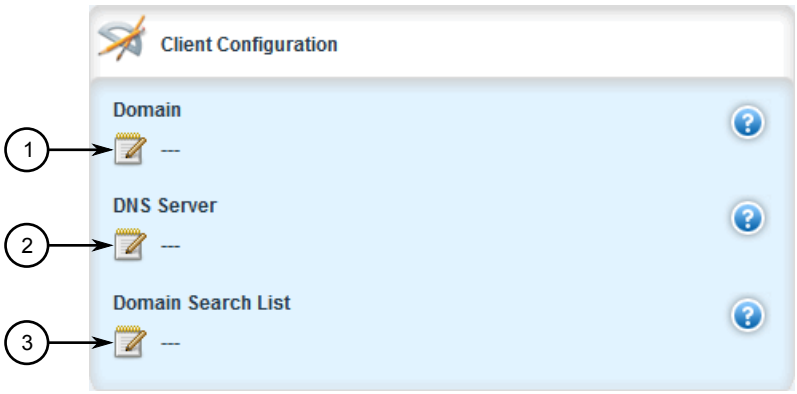


Figure 278: Client Configuration Form (IPv6)

1. Unknown Client List **2.** Authorize Server Check Box

3. On the **Leased Configuration** form, configure the following parameters as required:

Parameter	Description
default	**Synopsis:** A 32-bit unsigned integer **Default:** 600 The minimum leased time in seconds that the server offers to the clients.
maximum	**Synopsis:** A 32-bit unsigned integer **Default:** 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:

IMPORTANT!
For IPv4 only:

If DHCP relay (or Option 82) clients are used on the same subnet as the DHCP server, some clients will try to renew a lease immediately after receiving it by requesting a renewal directly from the

DHCP server. Because the DHCP server is configured by default to only provide the lease through a relay agent configured with the current Option 82 fields, the server sends the client a NAK (negative acknowledgment or not acknowledged) message to disallow the lease. Enabling Option 82 disables the NAK message so the renewal request sent from the DHCP relay agent (which the DHCP server accepts, since it has the correct Option 82 fields added) is the only message for which the client receives a reply.

Option 82 support should only be enabled If the DHCP server and clients are on the same subnet.

The meaning of most Option 82 fields is determined by the DHCP relay client. To determine which values are required by the client for special options, refer to the client documentation.

DHCP relay support can also be enabled on individual subnets. For more information, refer to Section 7.3.8.3, "Configuring Subnet Options".

Parameter	Description
Unknown Client	**Synopsis:** { allow, deny, ignore } The action to take for previously unregistered clients
Authorize Server	Enables/disables the server's authorization on this client. If enabled, the server will send deny messages to the client that is trying to renew the lease, which the server knows the client shouldn't have.
option82	Enables/disables the NAK of option 82 clients for this subnet.

5. [Optional] Configure configuration options for DHCP clients at the shared network level. For more information, refer to Section 7.3.5.1, "Configuring Standard DHCP Client Configuration Options (IPv4)" or Section 7.3.5.2, "Configuring Standard DHCP Client Configuration Options (IPv6)".
6. 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 7.3.7.4
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:
   - **For IPv4**
     services » dhcpserver » shared-network
   - **For IPv6**
     services » dhcpserver6 » shared-network

   The **Shared network Configuration** table appears.

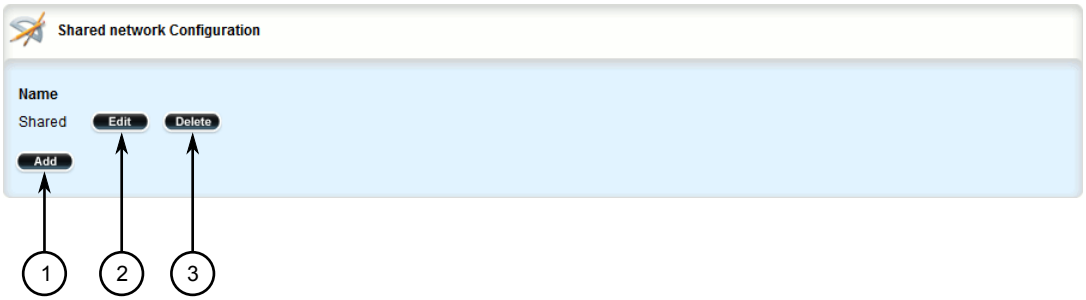


Figure 279: Shared Network Configuration Table

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

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 7.3.8

Managing Subnets

Subnets control settings for each subnet that DHCP serves. A subnet can include a range of IP addresses to give clients. Subnets contain groups, pools and hosts. Only one subnet can contain dynamic IP address ranges without any access restrictions on any given physical port, since DHCP doesn't know which subnet a client should belong to when the request is received.

CONTENTS

Section 7.3.8.1

Viewing a List of Subnets

To view a list of subnets, navigate to:

- **For IPv4**
  services » dhcpserver » subnet-name
- **For IPv6**
  services » dhcpserver6 » subnet6-name

If subnets have been configured, the **Subnet Configuration** table appears.

Figure 280: Subnet Configuration Table

If no subnets have been configured, add subnets as needed. For more information, refer to Section 7.3.8.2, "Adding a Subnet".

Section 7.3.8.2
Adding a Subnet

To add a subnet to the DHCP server, do the following:

NOTE
At least one shared network must be available if two or more subnets are configured for the same interface. For information about configuring a shared network, refer to Section 7.3.7.2, "Adding a Shared Network".

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to:
   - **For IPv4**
     services » dhcpserver » subnet-name
   - **For IPv6**
     services » dhcpserver6 » subnet6-name
3. Click **<Add subnet-name>** in the menu. The **Key Settings** form appears.

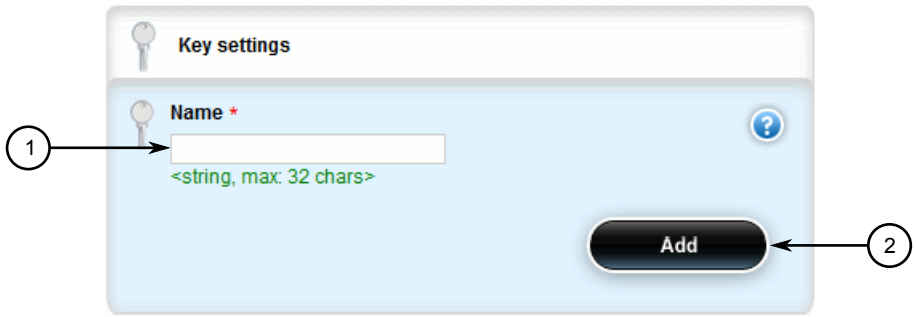


Figure 281: Key Settings Form

1. Name Box **2.** Add Button

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

Parameter	Description
name	**Synopsis:** A string 1 to 32 characters long

Parameter	Description
	The unique name to refer to the host within a DHCP configuration.

5. Click **Add** to create the new subnet. The **Subnet Configuration** form appears.

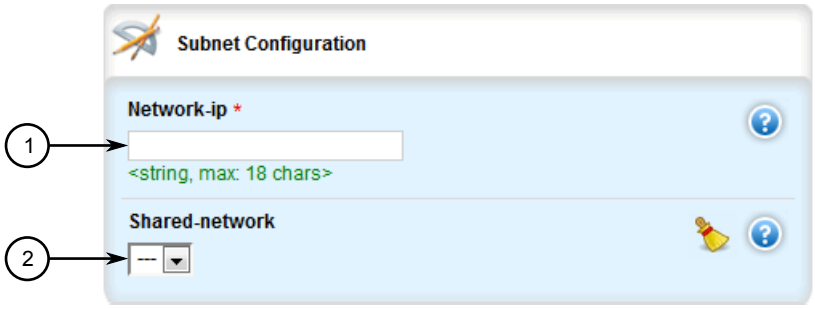


Figure 282: Subnet Configuration Form (IPv4)

1. Network IP Box **2.** Shared Network List

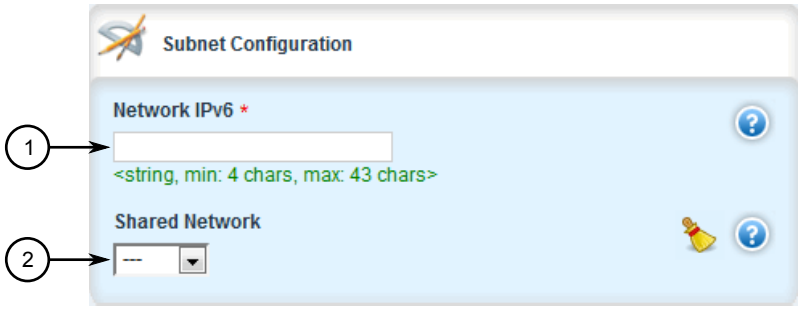


Figure 283: Subnet Configuration Form (IPv6)

1. Network IPv6 Box **2.** Shared Network List

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

Parameter	Description
Network IP	**Synopsis:** A string 9 to 18 characters long The network IP address for this subnet. This parameter is mandatory.
Shared Network	**Synopsis:** A string The shared-network that this host belongs to.

Parameter	Description
Network IPv6	**Synopsis:** A string 4 to 43 characters long The network IPv6 address for this subnet. This parameter is mandatory.
Shared Network	**Synopsis:** A string

Parameter	Description
	The shared-network that this host belongs to.

7. Configure the options for the subnet. For more information, refer to Section 7.3.8.3, "Configuring Subnet Options".
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 7.3.8.3
Configuring Subnet Options

To configure options for a subnet, do the following:

NOTE
Options set at the subnet level override options set at the DHCP server level.

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to:
   - **For IPv4**
     services » dhcpserver » subnet-name » {name} » options
   - **For IPv6**
     services » dhcpserver6 » subnet6-name » {name} » options

   Where *{name}* is the name of the subnet. The **Leased Configuration** and **Client Configuration** forms appear.

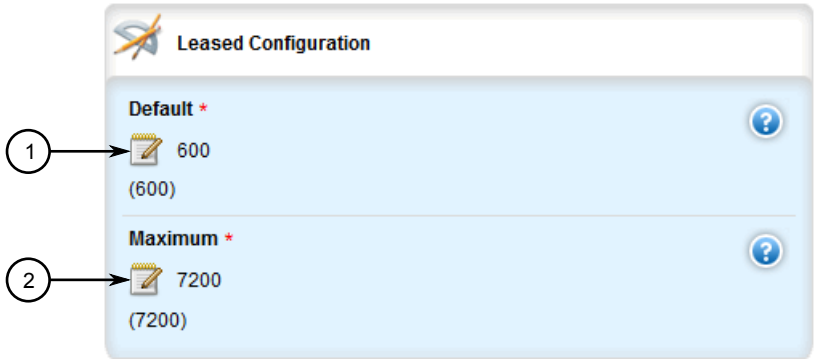


Figure 284: Leased Configuration Form

1. Default Box **2.** Maximum Box

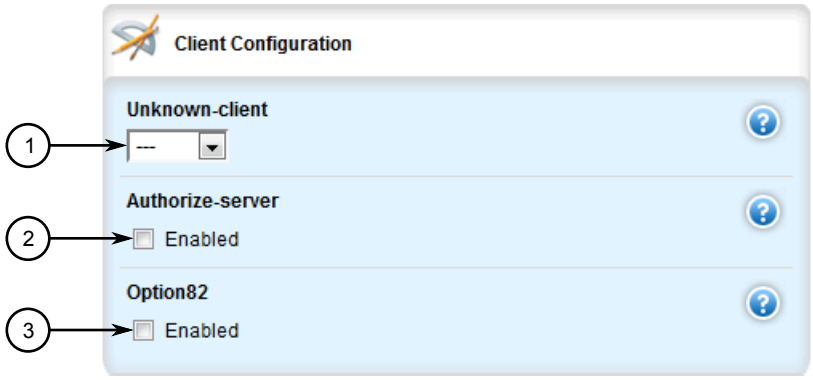


Figure 285: Client Configuration Form (IPv4)

1. Unknown Client Box **2.** Authorize Server Box **3.** Option 82 Box

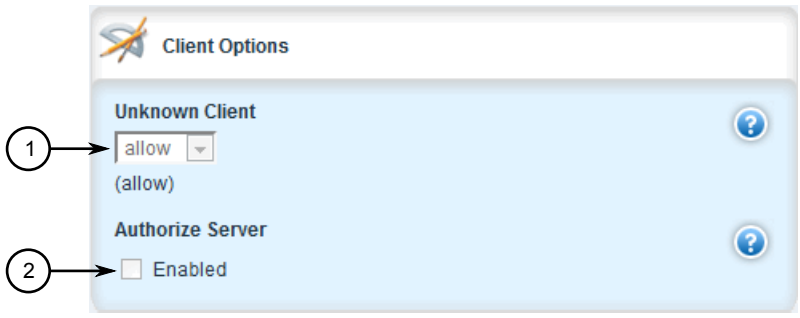


Figure 286: Client Configuration Form (IPv6)

1. Unknown Client Box **2.** Authorize Server Box

3. In the **Leased Configuration** form, configure the following parameters as required:

Parameter	Description
default	**Synopsis:** A 32-bit unsigned integer **Default:** 600 The minimum leased time in seconds that the server offers to the clients.
maximum	**Synopsis:** A 32-bit unsigned integer **Default:** 7200 The maximum leased time in seconds that the server offers to the clients.

4. In the **Client Configuration** form, configure the following parameters as required:

IMPORTANT!
For IPv4 only:

If DHCP relay (or Option 82) clients are used on the same subnet as the DHCP server, some clients will try to renew a lease immediately after receiving it by requesting a renewal directly from the DHCP server. Because the DHCP server is configured by default to only provide the lease through a relay agent configured with the current Option 82 fields, the server sends the client a NAK (negative acknowledgment or not acknowledged) message to disallow the lease. Enabling Option

82 disables the NAK message so the renewal request sent from the DHCP relay agent (which the DHCP server accepts, since it has the correct Option 82 fields added) is the only message for which the client receives a reply.

Option 82 support should only be enabled If the DHCP server and clients are on the same subnet.

The meaning of most Option 82 fields is determined by the DHCP relay client. To determine which values are required by the client for special options, refer to the client documentation.

DHCP relay support can also be enabled on individual subnets.

Parameter	Description
Unknown Client	**Synopsis:** { allow, deny, ignore } The action to take for previously unregistered clients
option82	Enables/disables the NAK of option 82 clients for this subnet.
Authorize Server	Enables/disables the server's authorization on this client. If enabled, the server will send deny messages to the client that is trying to renew the lease, which the server knows the client shouldn't have.

5. [Optional] Configure configuration options for DHCP clients at the subnet level. For more information, refer to Section 7.3.5.1, "Configuring Standard DHCP Client Configuration Options (IPv4)" or Section 7.3.5.2, "Configuring Standard DHCP Client Configuration Options (IPv6)".
6. Configure one or more address pools to the subnet. For more information, refer to Section 7.3.11.2, "Adding an Address Pool (IPv4)" or Section 7.3.12.2, "Adding an Address Pool (IPv6)".
7. Configure one or more IP ranges to the subnet. For more information, refer to Section 7.3.13.2, "Adding an IP Range (IPv4)" or Section 7.3.14.2, "Adding an IP Range (IPv6)".
8. 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 7.3.8.4

Deleting a Subnet

To delete a subnet, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to:
   - **For IPv4**
     services » dhcpserver » subnet-name
   - **For IPv6**
     services » dhcpserver6 » subnet6-name

   The **Subnet Configuration** table appears.

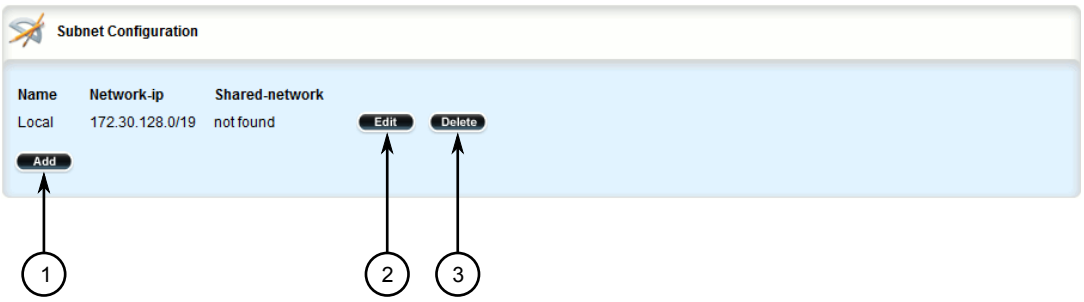


Figure 287: Subnet Configuration Table

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

3. Click **Delete** next to the chosen subnet.
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 7.3.9

Managing Host Groups

Host-groups allow identical settings to be created for a group of hosts, making it easier to manage changes to the settings for all the hosts contained within the group. Host-groups contain hosts.

CONTENTS

Section 7.3.9.1

Viewing a List of Host Groups

To view a list of host groups, navigate to:

- **For IPv4**
  services » dhcpserver » host-groups
- **For IPv6**
  services » dhcpserver6 » host-groups

If host groups have been configured, the **Host Group Configuration** table appears.

Figure 288: Host Group Configuration Table

If no host groups have been configured, add host groups as needed. For more information, refer to Section 7.3.9.2, "Adding a Host Group".

Section 7.3.9.2

Adding a Host Group

To add a host group to the DHCP server, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to:
   - **For IPv4**
     services » dhcpserver » host-groups
   - **For IPv6**
     services » dhcpserver6 » host-groups
3. Click **<Add host-groups>**. The **Key Settings** form appears.

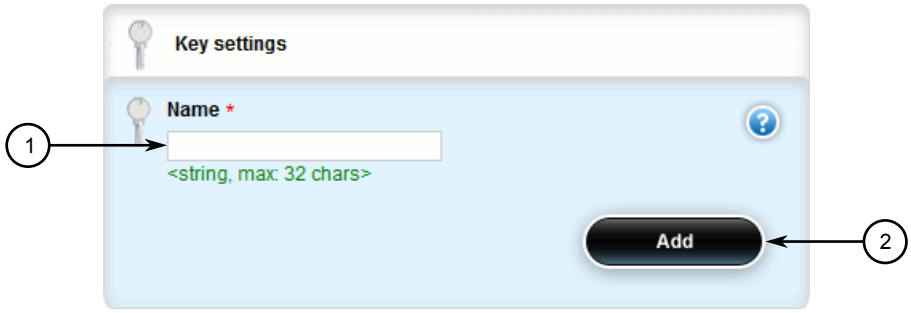


Figure 289: Key Settings Form

1. Name Box **2.** Add Button

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

Parameter	Description
name	**Synopsis:** A string 1 to 32 characters long The description of the host groups.

5. Click **Add** to create the new host group.
6. Configure the options for the host group. For more information, refer to Section 7.3.9.3, "Configuring Host Group Options".

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 7.3.9.3
Configuring Host Group Options

To configure options for a host group on the DHCP server, do the following:

NOTE
Options set at the host group level override options set at the DHCP server level.

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to:
   - **For IPv4**
     services » dhcpserver » host-groups » {host} » options
   - **For IPv6**
     services » dhcpserver6 » host-groups » {host} » options

   Where *{host}* is the name of the host group. The **Leased Configuration** and **Client Configuration** forms appear.

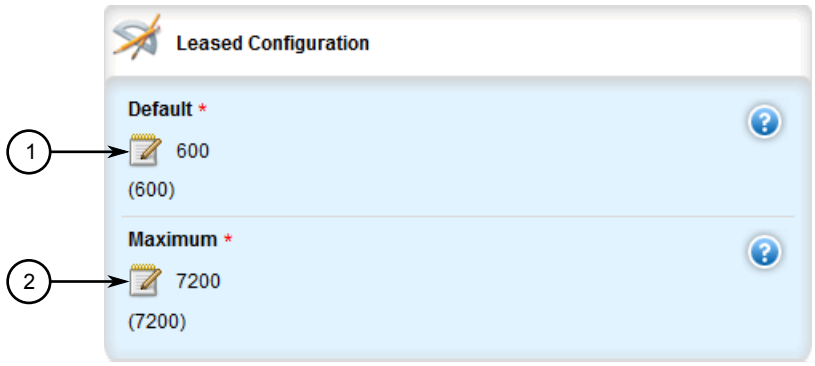


Figure 290: Leased Configuration Form

1. Default Box **2.** Maximum Box

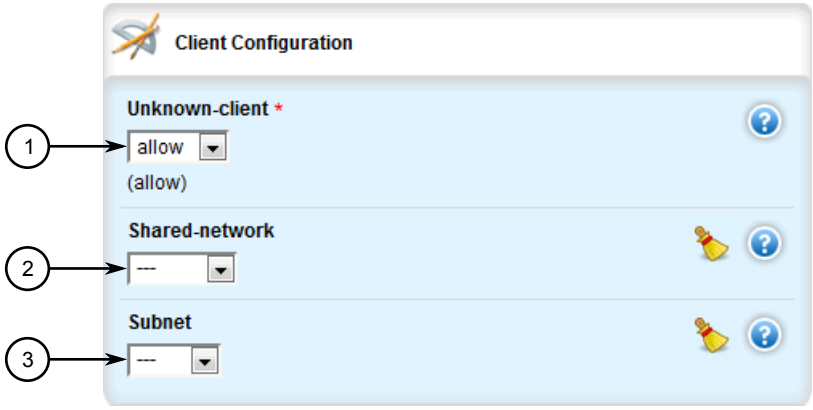


Figure 291: Client Configuration Form (IPv4)

1. Unknown Client List **2.** Shared Network List **3.** Subnet List

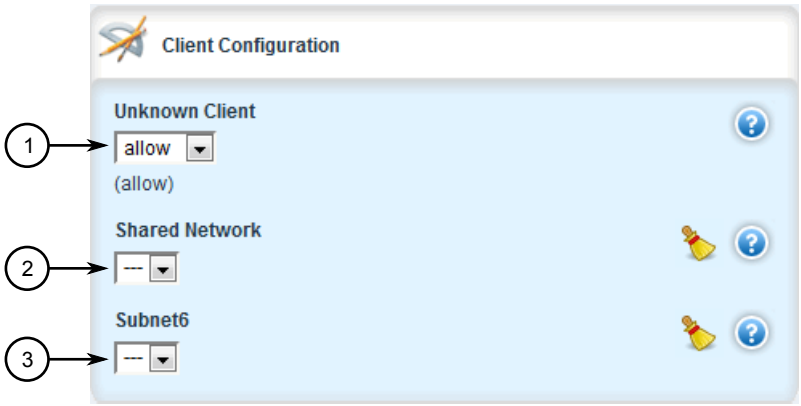


Figure 292: Client Configuration Form IPv6

1. Unknown Client List **2.** Shared Network List **3.** Subnet6 List

3. On the **Leased Configuration** form, configure the following parameters as required:

- **For IPv4**

Parameter	Description
default	**Synopsis:** A 32-bit unsigned integer **Default:** 600 The minimum leased time in seconds that the server offers to the clients.
maximum	**Synopsis:** A 32-bit unsigned integer **Default:** 7200 The maximum leased time in seconds that the server offers to the clients.

- **For IPv6**

Parameter	Description
default	**Synopsis:** A 32-bit unsigned integer **Default:** 600

Parameter	Description
	The minimum leased time in seconds that the server offers to the clients.
maximum	**Synopsis:** A 32-bit unsigned integer **Default:** 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:
   - **For IPv4**

Parameter	Description
Unknown Client	**Synopsis:** { allow, deny, ignore } The action to take for previously unregistered clients
Shared Network	**Synopsis:** A string The shared-network that this host belongs to.
subnet	**Synopsis:** A string The subnet that this host belongs to.

   - **For IPv6**

Parameter	Description
Unknown Client	**Synopsis:** { allow, deny, ignore } The action to take for previously unregistered clients
Shared Network	**Synopsis:** A string The shared-network that this host belongs to.
subnet6	**Synopsis:** A string The subnet that this host belongs to.

5. [Optional] Configure configuration options for DHCP clients at the host group level. For more information, refer to refer to Section 7.3.5.1, "Configuring Standard DHCP Client Configuration Options (IPv4)" or Section 7.3.5.2, "Configuring Standard DHCP Client Configuration Options (IPv6)".
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 7.3.9.4
Deleting a Host Group

To delete a host group, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to:
   - **For IPv4**
     services » dhcpserver » host-groups
   - **For IPv6**
     services » dhcpserver6 » host-groups

   The **Host Group Configuration** table appears.

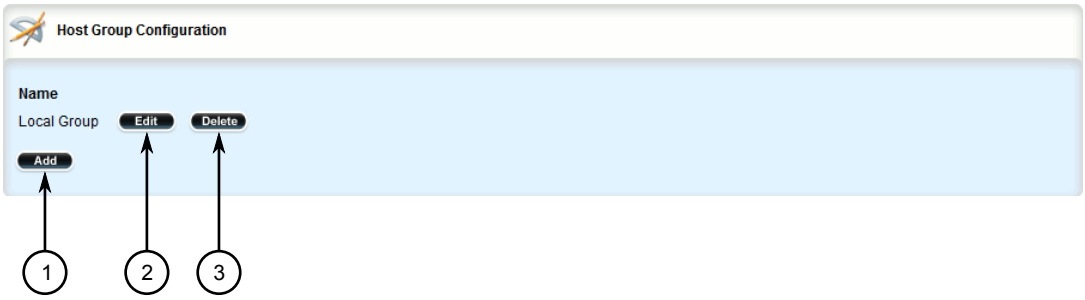


Figure 293: Host Group Configuration Table

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

3. Click **Delete** next to the chosen host 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 7.3.10

Managing DHCP Hosts

Host entries assign settings to a specific client based on its Ethernet MAC address.

CONTENTS

Section 7.3.10.1

Viewing a List of Hosts

To view a list of hosts on the DHCP server, navigate to:

- **For IPv4**
  services » dhcpserver » hosts
- **For IPv6**
  services » dhcpserver6 » hosts

If hosts have been configured, the **Host Configuration** table appears.

Figure 294: Host Configuration Table

If no hosts have been configured, add hosts as needed. For more information, refer to Section 7.3.10.2, "Adding a Host".

Section 7.3.10.2
Adding a Host

To add a host to the DHCP server, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to:
   - **For IPv4**
     services » dhcpserver » hosts
   - **For IPv6**
     services » dhcpserver6 » hosts
3. Click **<Add host>**. The **Key Settings** form appears.

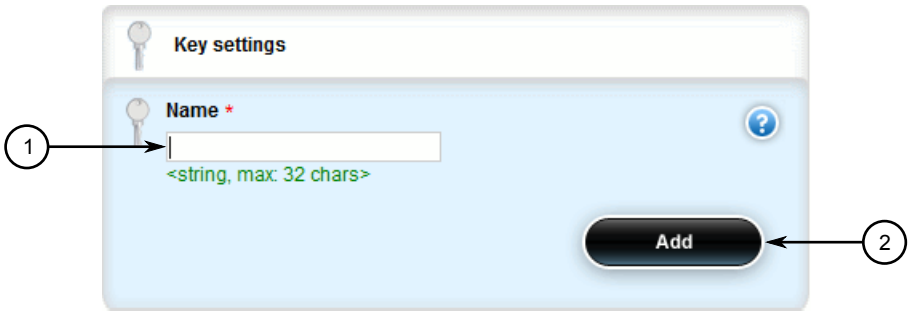


Figure 295: Key Settings Form

1. Name Box **2.** Add Button

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

Parameter	Description
name	**Synopsis:** A string 1 to 32 characters long The unique name to refer to the host within a DHCP configuration.

5. Click **Add** to create the new host.
6. Configure options for the host. For more information, refer to Section 7.3.10.3, "Configuring Host Options".

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 7.3.10.3
Configuring Host Options

To configure options for a host on the DHCP server, do the following:

> **NOTE**
> *Options set at the host level override options set at the DHCP server level.*

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to:
   - **For IPv4**
     services » dhcpserver » hosts » {host} » options
   - **For IPv6**
     services » dhcpserver6 » hosts » {host} » options

   Where *{host}* is the name of the host. The **Hardware Configuration**, **Leased Configuration** and **Client Configuration** forms appear.

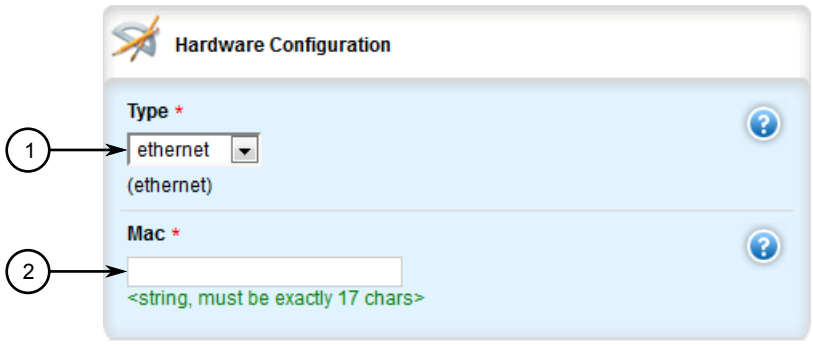


Figure 296: Hardware Configuration Form

1. Type List **2.** MAC Box

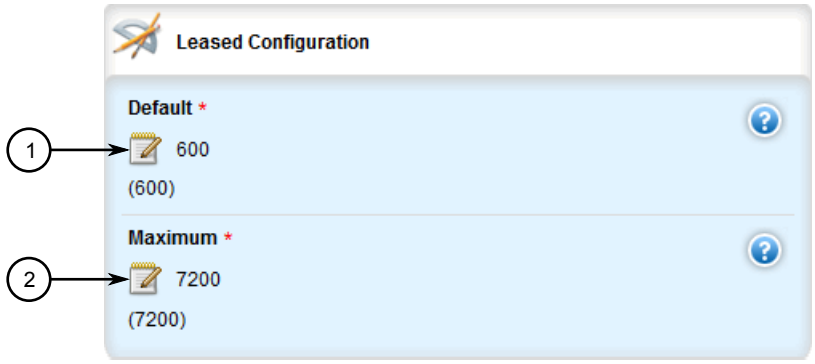


Figure 297: Leased Configuration Form

1. Default Box **2.** Maximum Box

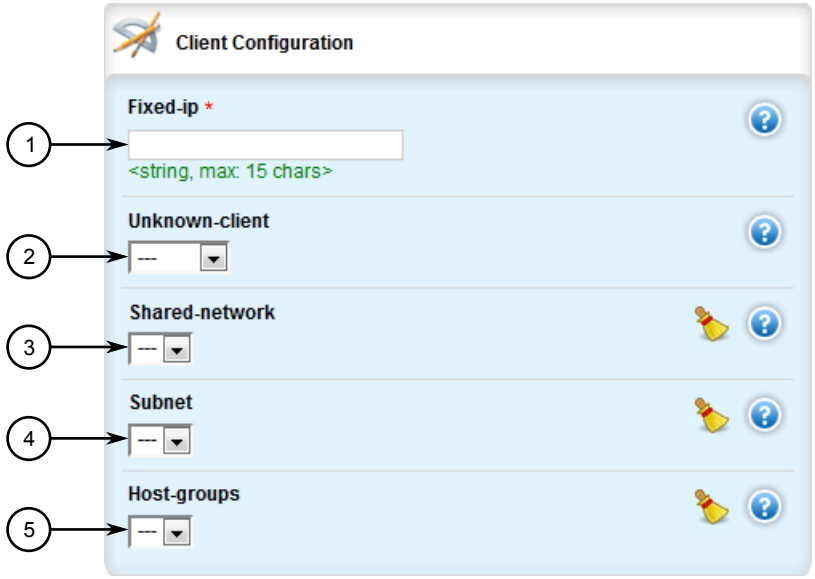


Figure 298: Client Configuration Form (IPv4)

1. Fixed IP Box **2.** Unknown Client LIst **3.** Shared Network LIst **4.** Subnet LIst **5.** Host Groups LIst

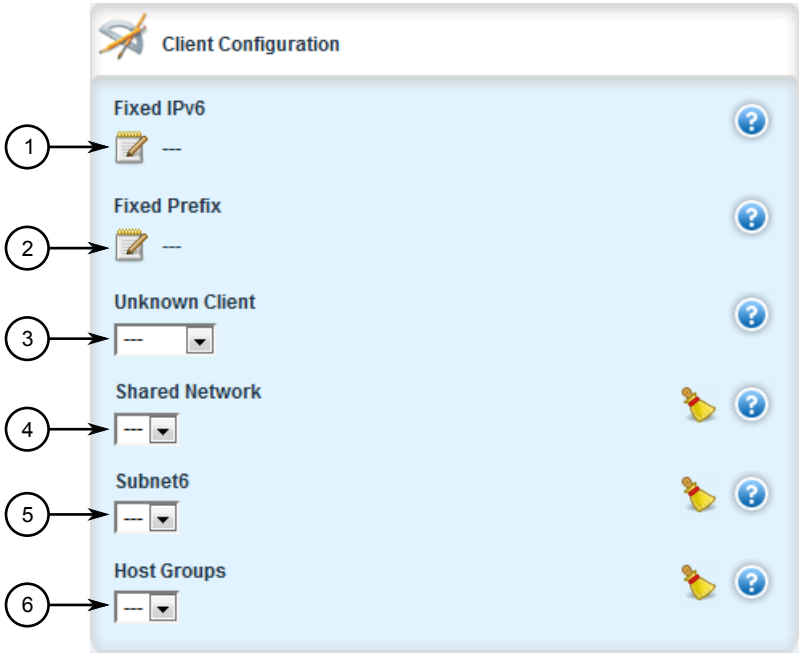


Figure 299: Client Configuration Form (IPv6)

1. Fixed IP Box **2.** Unknown Client LIst **3.** Shared Network LIst **4.** Subnet LIst **5.** Host Groups LIst

3. On the **Hardware Configuration** form, configure the following parameters as required:

Parameter	Description
type	**Synopsis:** { fddi, token-ring, ethernet } **Default:** ethernet The type of network hardware used by the client, associated with the host entry.
mac	**Synopsis:** A string 17 characters long The physical network address of the client. Note that this corresponds to the hardware type; for example, the MAC address for the ethernet. This parameter is mandatory.

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

Parameter	Description
default	**Synopsis:** A 32-bit unsigned integer **Default:** 600 The minimum leased time in seconds that the server offers to the clients.
maximum	**Synopsis:** A 32-bit unsigned integer **Default:** 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:

- **For IPv4**

Parameter	Description
Fixed IP	**Synopsis:** A string 7 to 15 characters long The IP address that the server assigns to the matching client. This parameter is mandatory.
Unknown Client	**Synopsis:** { allow, deny, ignore } The action to take for previously unregistered clients
Shared Network	**Synopsis:** A string The shared-network that this host belongs to.
subnet	**Synopsis:** A string The subnet that this host belongs to.
Host Groups	**Synopsis:** A string The host groups that this host belongs to.

- **For IPv6**

Parameter	Description
Fixed IPv6	**Synopsis:** A string 6 to 40 characters long The IPv6 address that the server assigns to the matching client.
Fixed Prefix	**Synopsis:** A string 4 to 43 characters long The IPv6 prefix delegation that the server assigns to the matching client.
Unknown Client	**Synopsis:** { allow, deny, ignore } The action to take for previously unregistered clients
Shared Network	**Synopsis:** A string The shared-network that this host belongs to.
subnet6	**Synopsis:** A string The subnet that this host belongs to.
Host Groups	**Synopsis:** A string The host groups that this host belongs to.

6. [Optional] Configure configuration options for DHCP clients at the host level. For more information, refer to refer to Section 7.3.5.1, "Configuring Standard DHCP Client Configuration Options (IPv4)" or Section 7.3.5.2, "Configuring Standard DHCP Client Configuration Options (IPv6)".
7. 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 7.3.10.4
Deleting Hosts

To delete a host, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to:

- **For IPv4**
  services » dhcpserver » hosts
- **For IPv6**
  services » dhcpserver6 » hosts

The **Host Configuration** table appears.

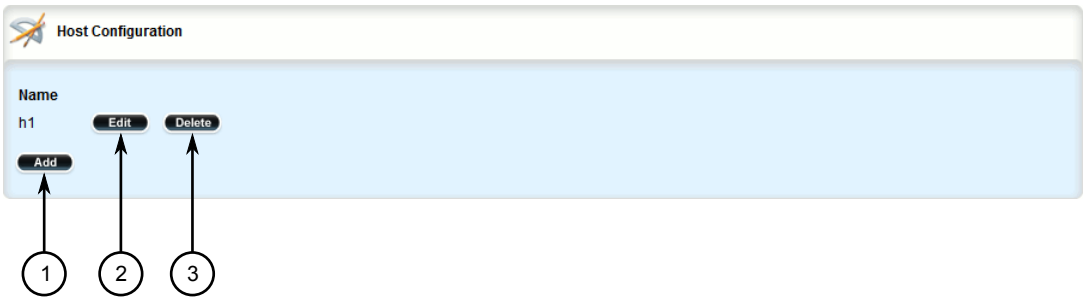


Figure 300: Host Configuration Table

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

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 7.3.11

Managing Address Pools (IPv4)

Address pools define a range of IP addresses that can be assigned to DHCP clients belonging to the same subnet.

CONTENTS

Section 7.3.11.1

Viewing a List of Address Pools (IPv4)

To view a list of address pools configured for a DHCP subnet, navigate to ***services » dhcpserver » subnet-name » {name} » options » ippool***, where *{name}* is the name of the subnet. If pools have been configured, the **IP Pool Configuration** table appears.

Figure 301: IP Pool Configuration Table

If no IP pools have been configured, add pools as needed. For more information, refer to Section 7.3.11.2, "Adding an Address Pool (IPv4)".

Section 7.3.11.2
Adding an Address Pool (IPv4)

To add an address pool to a DHCP subnet, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to ***services » dhcpserver » subnet-name » {name} » options » ippool***, where *{name}* is the name of the subnet.
3. Click **<Add ippool>**. The **Key Settings** form appears.

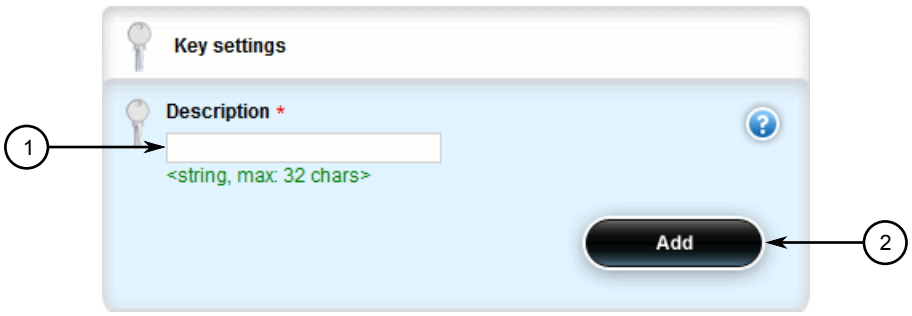


Figure 302: Key Settings Form

1. Description Box **2.** Add Button

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

Parameter	Description
description	**Synopsis:** 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.

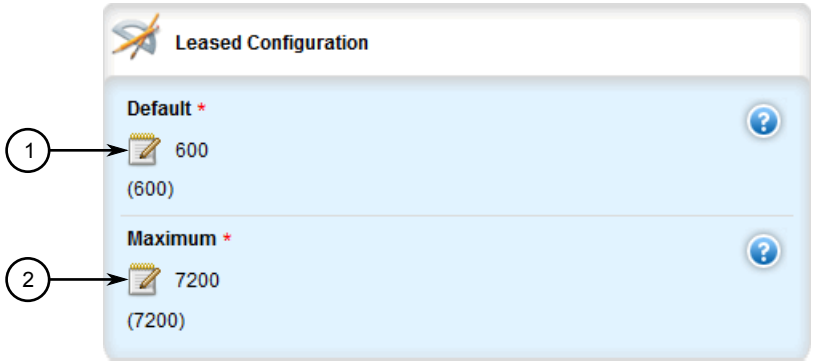


Figure 303: Leased Configuration Form

1. Default Box **2.** Maximum Box

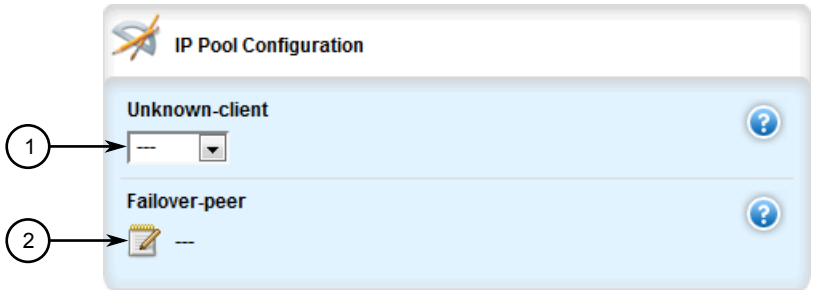


Figure 304: IP Pool Configuration Form

1. Unknown Client Box **2.** Failover Peer Box

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

Parameter	Description
default	**Synopsis:** A 32-bit unsigned integer **Default:** 600 The minimum leased time in seconds that the server offers to the clients.
maximum	**Synopsis:** A 32-bit unsigned integer **Default:** 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	**Synopsis:** { allow, deny, ignore } The action to take for previously unregistered clients
Failover Peer	**Synopsis:** 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 to the pool. For more information, refer to Section 7.3.13.2, "Adding an IP Range (IPv4)".
9. Add one or more Option82 classes to the pool. For more information, refer to Section 7.3.18.2, "Adding an Option 82 Class to an Address Pool".
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 7.3.11.3
Deleting an Address Pool (IPv4)

To delete an address pool, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to ***services » dhcpserver » subnet-name » {name} » options » ippool***, where *{name}* is the name of the subnet. The **IP Pool Configuration** table appears.

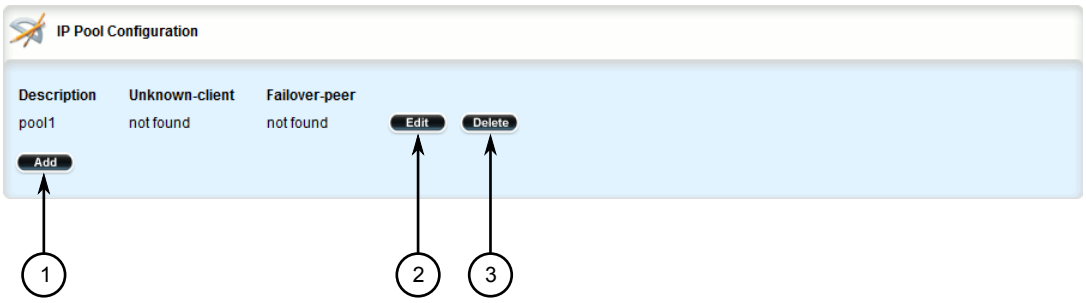


Figure 305: IP Pool Configuration Table

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

3. Click **Delete** next to the chosen pool.
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 7.3.12
Managing Address Pools (IPv6)

Address pools define a range of IP addresses that can be assigned to DHCP clients belonging to the same subnet.

CONTENTS

Section 7.3.12.1
Viewing a List of Address Pools (IPv6)

To view a list of address pools configured for a DHCP subnet, navigate to ***services » dhcpserver6 » subnet6-name » {name} » options » ippool6***, where *{name}* is the name of the subnet. If pools have been configured, the **IP Pool Configuration** table appears.

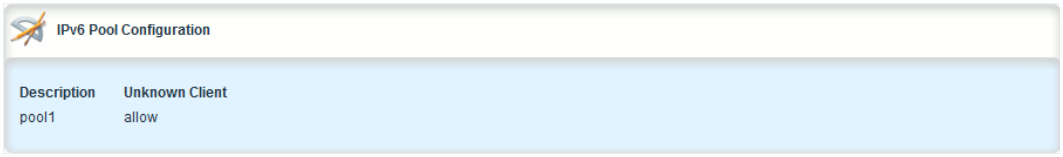


Figure 306: IP Pool Configuration Table

If no IP pools have been configured, add pools as needed. For more information, refer to Section 7.3.12.2, "Adding an Address Pool (IPv6)".

Section 7.3.12.2
Adding an Address Pool (IPv6)

To add an address pool to a DHCP subnet, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to ***services » dhcpserver6 » subnet6-name » {name} » options » ippool6***, where *{name}* is the name of the subnet.
3. Click **<Add ippool6>**. The **Key Settings** form appears.

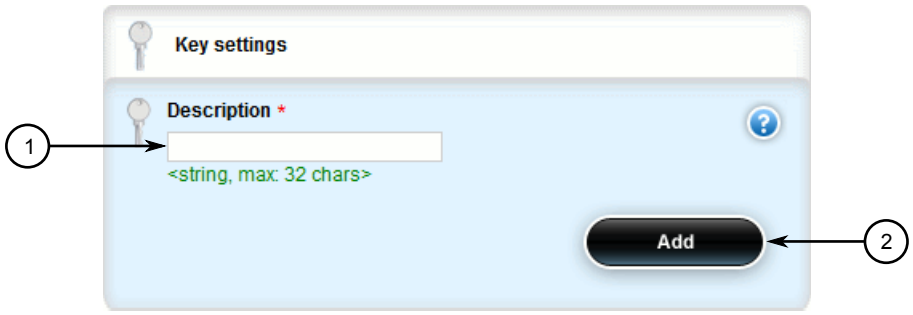


Figure 307: Key Settings Form

1. Description Box **2.** Add Button

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

Parameter	Description
description	**Synopsis:** A string 1 to 32 characters long Describes the IPv6 pool.

5. Click **Add** to create the IP pool. The **Leased Configuration** and **IPv6 Pool Configuration** forms appear.

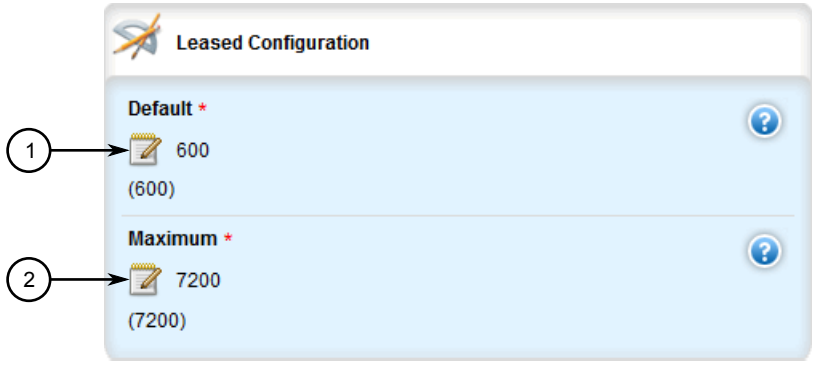


Figure 308: Leased Configuration Form

1. Default Box **2.** Maximum Box

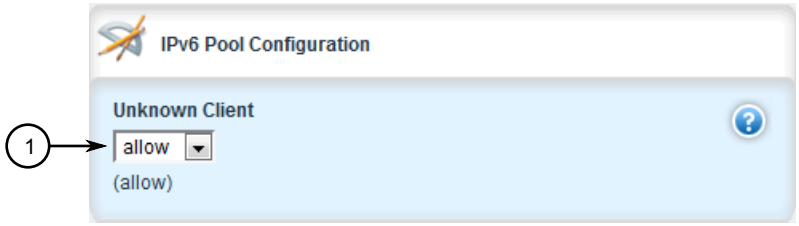


Figure 309: IP Pool Configuration Form

1. Unknown Client Box **2.** Failover Peer Box

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

Parameter	Description
default	**Synopsis:** A 32-bit unsigned integer **Default:** 600 The minimum leased time in seconds that the server offers to the clients.
maximum	**Synopsis:** A 32-bit unsigned integer **Default:** 7200 The maximum leased time in seconds that the server offers to the clients.

7. On the **IPv6 Pool Configuration** form, configure the following parameter(s) as required:

Parameter	Description
Unknown Client	**Synopsis:** { allow, deny, ignore } The action to take for previously unregistered clients

8. [Optional] Add one or more IP ranges to the pool. For more information, refer to Section 7.3.14.2, "Adding an IP Range (IPv6)".
9. [Optional] Add one or more subnets to the pool. For more information, refer to Section 7.3.17.2, "Adding a IPv6 Subnet".

10. [Optional] Add one or more temporary subnets to the pool. For more information, refer to Section 7.3.16.2, "Adding a Temporary Subnet".
11. [Optional] Add one or more prefixes to the pool. For more information, refer to Section 7.3.15.2, "Adding an IPv6 Prefix".
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 7.3.12.3
Deleting an Address Pool (IPv6)

To delete an address pool, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to ***services » dhcpserver6 » subnet6-name » {name} » options » ippool6***, where *{name}* is the name of the subnet. The **IP Pool Configuration** table appears.

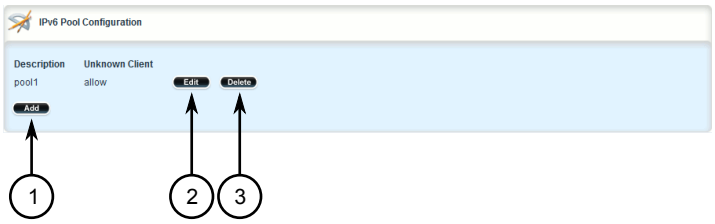


Figure 310: IP Pool Configuration Table

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

3. Click **Delete** next to the chosen pool.
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 7.3.13
Managing IP Ranges (IPv4)

An IP range represents the range of IP addresses the DHCP server can assign to clients. IP addresses outside the set range are reserved for statically addressed clients.

An IP range can be configured for a DHCP subnet and/or its associated address pool(s).

CONTENTS

Section 7.3.13.1
Viewing a List of IP Ranges (IPv4)

To view a list of IP ranges configured for a DHCP subnet or one of its associated address pools, navigate to:

- **For a DHCP subnet**
  services » dhcpserver » subnet-name » {name} » options » iprange
- **For an address pool**
  services » dhcpserver » subnet-name » {name} » options » ippool » {description} » iprange

Where *{name}* is the name of the subnet and *{description}* (if applicable) is the name of the address pool. If ranges have been configured, the **IP Range Configuration** table appears.

Figure 311: IP Range Configuration Table

If no IP ranges have been configured, add ranges as needed. For more information, refer to Section 7.3.13.2, "Adding an IP Range (IPv4)" or Section 7.3.14.2, "Adding an IP Range (IPv6)".

Section 7.3.13.2
Adding an IP Range (IPv4)

To add an IP range to a DHCP subnet or one of its associated address pools, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to:
   - **For a DHCP subnet**
     services » dhcpserver » subnet-name » {name} » options » iprange
   - **For an address pool**
     services » dhcpserver » subnet-name » {name} » options » ippool » {description} » iprange

   Where *{name}* is the name of the subnet and *{description}* (if applicable) is the name of the address pool.
3. Click **<Add iprange>**. The **Key Settings** form appears.

Figure 312: Key Settings Form

1. Start Box **2.** Add Button

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

Parameter	Description
start	**Synopsis:** A string 7 to 15 characters long The starting IP address pool that the server uses to offer to the client. This parameter is mandatory.

5. Click **Add** to create the IP range. The **IP Range Configuration** form appears.

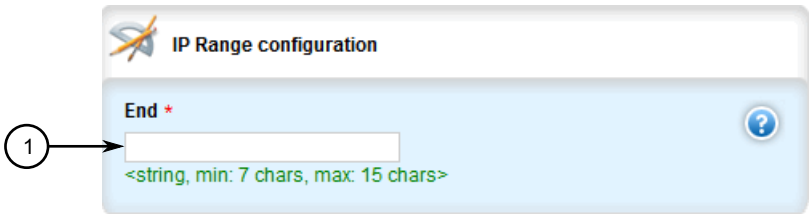


Figure 313: IP Range Configuration Form

1. End Box

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

Parameter	Description
end	**Synopsis:** A string 7 to 15 characters long The ending IP address pool that the server uses to offer to the client. This parameter is mandatory.

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 7.3.13.3
Deleting an IP Range (IPv4)

To delete an IP range from a DHCP subnet or one of its associated address pools, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to:
   - **For a DHCP subnet**
     services » dhcpserver » subnet-name » {name} » options » iprange
   - **For an address pool**
     services » dhcpserver » subnet-name » {name} » options » ippool » {description} » iprange

   Where *{name}* is the name of the subnet and *{description}* (if applicable) is the name of the address pool. The **IP Range Configuration** table appears.

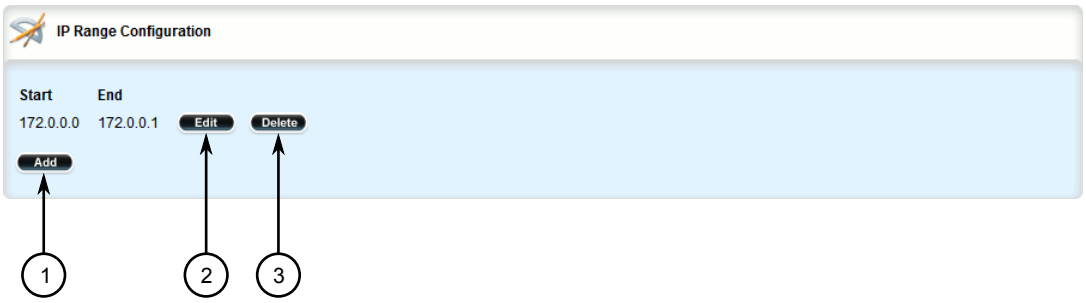


Figure 314: IP Range Configuration Table

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

3. Click **Delete** next to the chosen IP range.
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 7.3.14
Managing IP Ranges (IPv6)

An IP range represents the range of IP addresses the DHCP server can assign to clients. IP addresses outside the set range are reserved for statically addressed clients.

An IP range can be configured for a DHCP subnet and/or its associated address pool(s).

CONTENTS

Section 7.3.14.1
Viewing a List of IP Ranges (IPv6)

To view a list of IP ranges configured for a DHCP subnet or one of its associated address pools, navigate to:

- **For a DHCP IPv6 subnet**
  services » dhcpserver6 » subnet6-name » {name} » options » iprange6
- **For an IPv6 address pool**
  services » dhcpserver6 » subnet6-name » {name} » options » ippool6 » {description} » iprange6

Where *{name}* is the name of the subnet and *{description}* (if applicable) is the name of the address pool. If ranges have been configured, the **IPv6 Range Configuration** table appears.

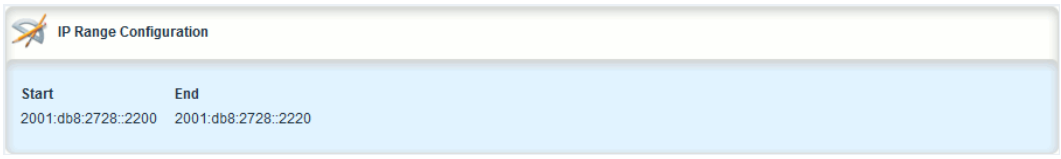


Figure 315: IPv6 Range Configuration Table

If no IP ranges have been configured, add ranges as needed. For more information, refer to Section 7.3.14.2, "Adding an IP Range (IPv6)".

Section 7.3.14.2
Adding an IP Range (IPv6)

To add an IP range to a DHCP subnet or one of its associated address pools, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to:
   - **For a DHCP IPv6 subnet**
     services » dhcpserver6 » subnet6-name » {name} » options » iprange6
   - **For an IPv6 address pool**
     services » dhcpserver6 » subnet6-name » {name} » options » ippool6 » {description} » iprange6

   Where *{name}* is the name of the subnet and *{description}* (if applicable) is the name of the address pool.
3. Click **<Add iprange>**. The **Key Settings** form appears.

Figure 316: Key Settings Form

1. Start Box **2.** Add Button

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

Parameter	Description
start	**Synopsis:** A string 6 to 40 characters long The starting IPv6 address pool that the server uses to offer to the client. This parameter is mandatory.

5. Click **Add** to create the IP range. The **IPv6 Range Configuration** form appears.

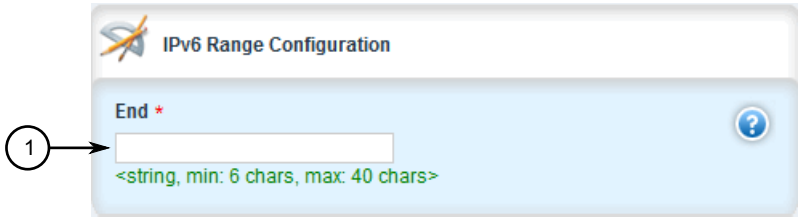


Figure 317: IP Range Configuration Form

1. End Box

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

Parameter	Description
end	**Synopsis:** A string 6 to 40 characters long The ending IPv6 address pool that the server uses to offer to the client. This parameter is mandatory.

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 7.3.14.3
Deleting an IP Range (IPv6)

To delete an IP range from a DHCP subnet or one of its associated address pools, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to:
   - **For a DHCP IPv6 subnet**
     services » dhcpserver6 » subnet6-name » {name} » options » iprange6
   - **For an IPv6 address pool**
     services » dhcpserver6 » subnet6-name » {name} » options » ippool6 » {description} » iprange6

   Where *{name}* is the name of the subnet and *{description}* (if applicable) is the name of the address pool. The **IP Range Configuration** table appears.

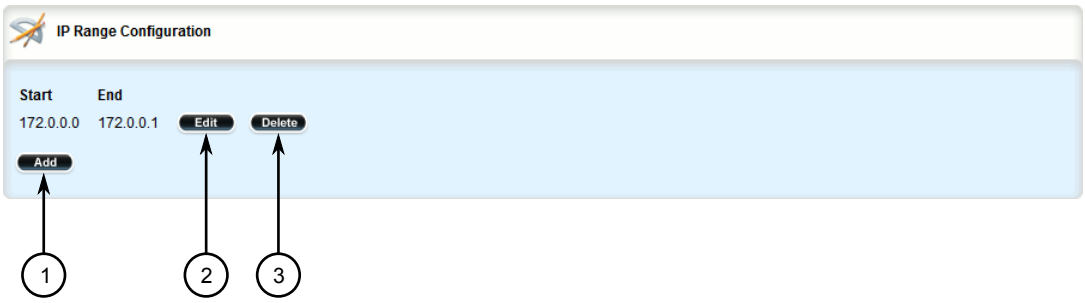


Figure 318: IP Range Configuration Table

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

3. Click **Delete** next to the chosen IP range.
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 7.3.15
Managing IPv6 Prefixes

One or more optional IPv6 prefix can be defined for the server to offer to the client.

A *prefix6* delegation includes the IPv6 subnetwork, along with the prefix length in bits. The subnetwork value used should be within the subnetwork value of the enclosing subnet6 declaration.

CONTENTS

Section 7.3.15.1
Viewing a List of IPv6 Prefixes

To view a list of prefixes, navigate to ***services » dhcpserver6 » subnet6-name » {name} » options » prefix6***, where *{name}* is the name of the subnet. If prefixes have been configured, the **IPv6 Prefix Delegation Configuration** table appears.

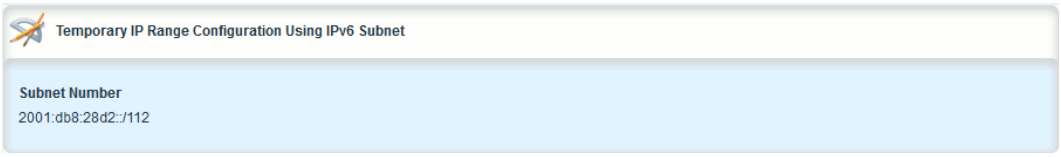


Figure 319: IPv6 Range Configuration Table

If no prefixes have been configured, add ranges as needed. For more information, refer to Section 7.3.15.2, "Adding an IPv6 Prefix".

Section 7.3.15.2
Adding an IPv6 Prefix

To add a prefix, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to ***services » dhcpserver6 » subnet6-name » {name} » options » prefix6***, Where *{name}* is the name of the subnet.
3. Click **<Add prefix6>**. The **Key Settings** form appears.

Figure 320: Key Settings Form

1. Start Box **2.** Add Button

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

Parameter	Description
start	**Synopsis:** A string 6 to 40 characters long The starting IPv6 prefix delegation that the server uses to offer to the client. This parameter is mandatory.

5. Click **Add** to create the IP range. The **IPv6 Prefix Delegation Configuration** form appears.

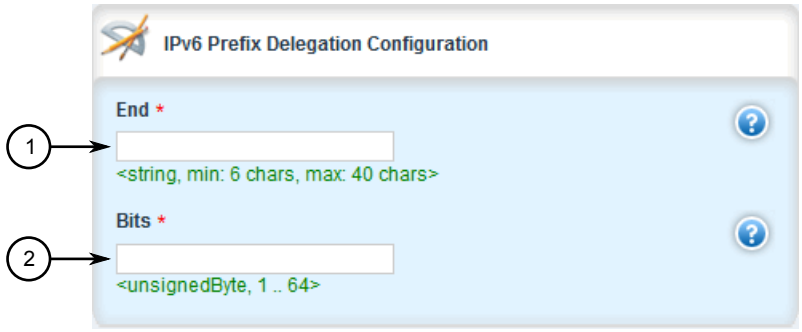


Figure 321: IPv6 Prefix Delegation Configuration Form

1. End Box **2.** Bits Box

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

Parameter	Description
end	**Synopsis:** A string 6 to 40 characters long The ending IPv6 prefix delegation that the server uses to offer to the client. This parameter is mandatory.
bits	**Synopsis:** An 8-bit unsigned integer between 1 and 64 Prefix delegations of bits length that are offered to the client. This parameter is mandatory.

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 7.3.15.3

Deleting an IPv6 Prefix

To delete a prefix, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to ***services » dhcpserver6 » subnet6-name » {name} » options » prefix6***

   Where *{name}* is the name of the subnet. The **IPv6 Prefix Delegation Configuration** table appears.

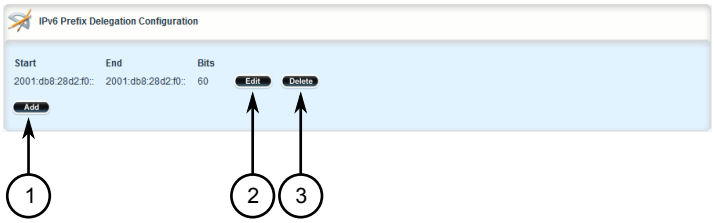


Figure 322: IP Range Configuration Table

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

3. Click **Delete** next to the chosen prefix.
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 7.3.16

Managing Temporary Subnets

One or more optional IPv6 subnets with temporary addresses can be defined for the server to offer to the client.

CONTENTS

Section 7.3.16.1

Viewing a List of Temporary Subnets

To view a list of temporary subnets, navigate to ***services » dhcpserver6 » subnet6-name » {name} » options » temporarysubnet6***, where *{name}* is the name of the subnet. If temporary subnets have been configured, the **Temporary IP Range Configuration Using IPv6 Subnet** table appears.

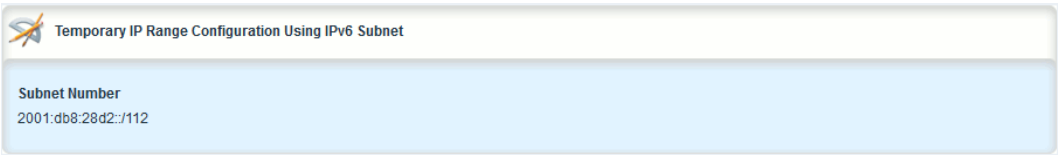


Figure 323: IPv6 Temporary Subnet Delegation Configuration

If no prefixes have been configured, add ranges as needed. For more information, refer to Section 7.3.15.2, "Adding an IPv6 Prefix".

Section 7.3.16.2
Adding a Temporary Subnet

To add a temporary subnet, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to ***services » dhcpserver6 » subnet6-name » {name} » options » temporarysubnet6***, where *{name}* is the name of the subnet.
3. Click **<Add temporarysubnet6>**. The **Key Settings** form appears.

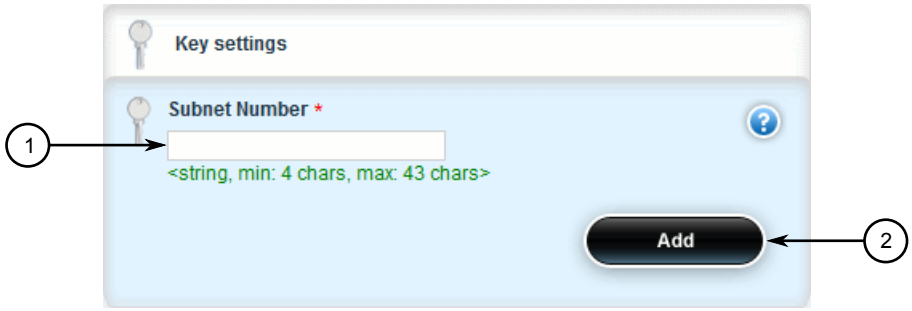


Figure 324: Key Settings Form

1. Subnet Number Box **2.** Add Button

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

Parameter	Description
Subnet Number	**Synopsis:** A string 4 to 43 characters long The IPv6 subnet with temporary addresses that the server uses to offer to the client. This parameter is mandatory.

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 7.3.16.3
Deleting a Temporary Subnet

To delete a prefix, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to ***services » dhcpserver6 » subnet6-name » {name} » options » temporarysubnet6***, where *{name}* is the name of the subnet. The **Temporary IP Range Configuration Using IPv6 Subnet** table appears.

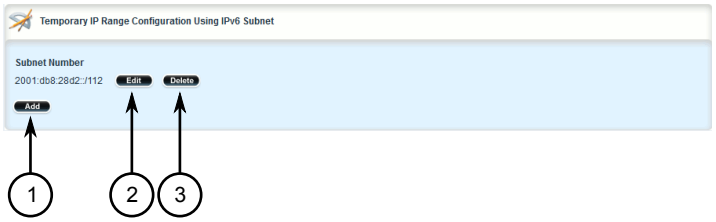


Figure 325: Temporary IP Range Configuration Using IPv6 Subnet Table

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

3. Click **Delete** next to the chosen prefix.
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 7.3.17

Managing IPv6 Subnets

One or more optional IPv6 subnets can be defined for the server to offer to the client.

CONTENTS

Section 7.3.17.1

Viewing a List of IPv6 Subnets

To view a list of IPv6 subnets, navigate to ***services » dhcpserver6 » subnet6-name » {name} » options » subnet6***, where *{name}* is the name of the subnet. If IPv6 subnets have been configured, the **IP Range Configuration Using IPv6 Subnet** table appears.

Figure 326: IP Range Configuration Using IPv6 Subnet

If no prefixes have been configured, add ranges as needed. For more information, refer to Section 7.3.15.2, "Adding an IPv6 Prefix".

Section 7.3.17.2
Adding a IPv6 Subnet

To add a IPv6 subnet, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to ***services » dhcpserver6 » subnet6-name » {name} » options » subnet6***, where *{name}* is the name of the subnet.
3. Click **<Add prefix6>**. The **Key Settings** form appears.

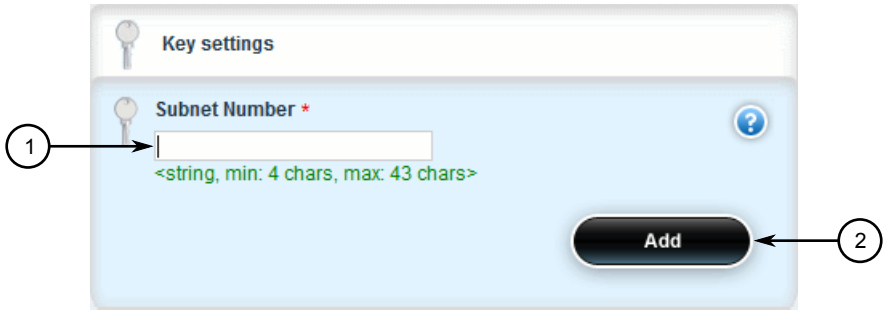


Figure 327: Key Settings Form

1. Start Box **2.** Add Button

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

Parameter	Description
Subnet Number	**Synopsis:** A string 4 to 43 characters long The IPv6 subnet that the server uses to offer to the client. This parameter is mandatory.

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 7.3.17.3
Deleting an IPv6 Subnet

To delete an IPv6 subnet, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to ***services » dhcpserver6 » subnet6-name » {name} » options » subnet6***, where *{name}* is the name of the subnet. The **IP Range Configuration Using IPv6 Subnet** table appears.

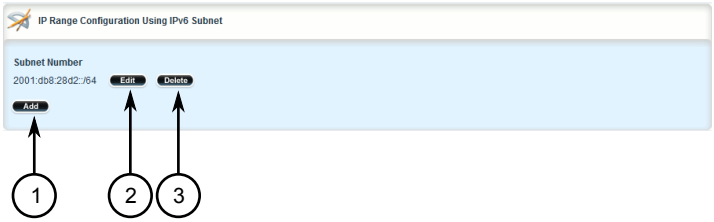


Figure 328: IP Range Configuration Using IPv6 Subnet Table

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

3. Click **Delete** next to the chosen prefix.
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 7.3.18

Managing Option 82 Classes for Address Pools

Option 82, or the DHCP relay agent information option, helps protect the DHCP server from IP address spoofing and DHCP IP starvation attacks by providing information about the network source of IP address requests. When a DHCP client issues an IP address request, a DHCP relay agent adds Option 82 information to the packet header for the request. The relay agent then forwards the request to the DHCP server for consideration. If the DHCP server determines the request came from an untrusted source, the request is rejected.

The DHCP server must be configured to accept Option 82 information if it is to determine the trustworthiness of the network interface used by a DHCP client. This can be done at the global level or for individual subnets.

IMPORTANT!
For more information about enabling the DHCP server to accept Option 82 information, refer to either Section 7.3.4, "Configuring DHCP Server Options" or Section 7.3.8.3, "Configuring Subnet Options".

Once Option 82 is enabled, sub-option components (or classes) must be defined for each address pool that includes DHCP clients that will send Option 82 information. This section describes how to manage the sub-option components for address pools.

CONTENTS

Section 7.3.18.1

Viewing a List of Option 82 Classes for Address Pools

To view a list of Option 82 classes configured for an address pool, navigate to ***services » dhcpserver » subnet-name » {name} » options » ippool » {description} » option82***, where *{name}* is the name of the subnet and

{description} is the name of the address pool. If classes have been configured, the **Option 82 Configuration** table appears.

Figure 329: Option 82 Configuration Table

If no Option 82 classes have been configured, add classes as needed. For more information, refer to Section 7.3.18.2, "Adding an Option 82 Class to an Address Pool".

Section 7.3.18.2
Adding an Option 82 Class to an Address Pool

To add an Option 82 class to an address pool, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to ***services » dhcpserver » subnet-name » {name} » options » ippool » {description} » option82***, where *{name}* is the name of the subnet and *{description}* is the name of the address pool.
3. Click **<Add option82>**. The **Key Settings** form appears.

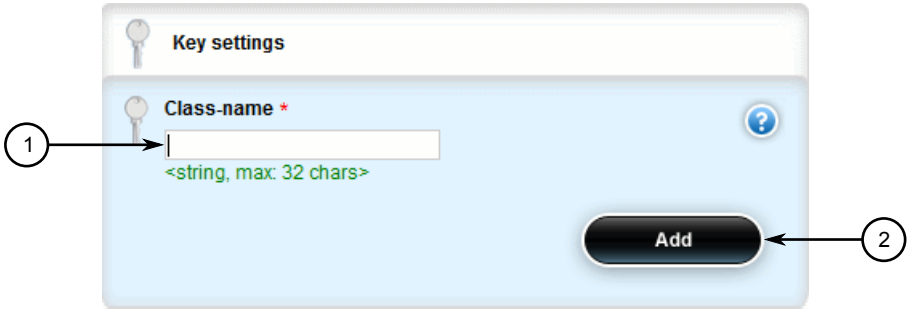


Figure 330: Key Settings Form

1. Class Name Box **2.** Add Button

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

Parameter	Description
Class Name	**Synopsis:** 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.

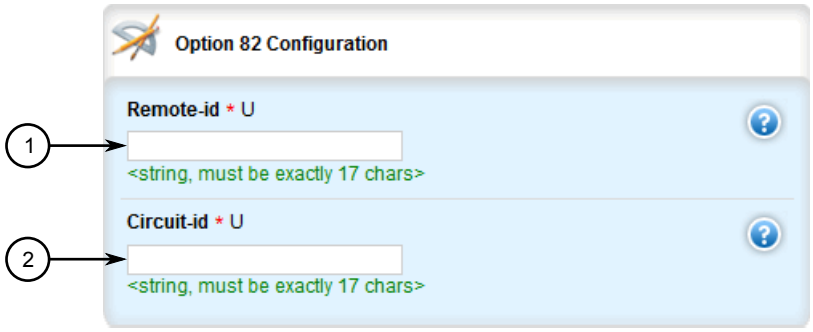


Figure 331: Option 82 Configuration Form

1. Remote ID Box **2.** Circuit ID Box

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

> **NOTE**
> *The format for the **Circuit ID** value is **00:00:00:{vlan}:{slot}:{port}**. If the remote host is connected to LM3/1 on VLAN 1, the ID would be 00:00:00:01:03:01. The Circuit ID uses hexadecimal values.*

Parameter	Description
Remote ID	**Synopsis:** A string 17 characters long Specifies the information relating to the remote host end of the circuit. This parameter is mandatory.
Circuit ID	**Synopsis:** A string 1 to 17 characters long Specifies the local information to which circuit the request came in on (ie. 00:02:03:02) This parameter is mandatory.

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 7.3.18.3
Deleting an Option 82 Class From an Address Pool

To delete an Option 82 class from an address pool, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to ***services » dhcpserver » subnet-name » {name} » options » ippool » {description} » option82***, where *{name}* is the name of the subnet and *{description}* is the name of the address pool. The **Option 82 Configuration** table appears.

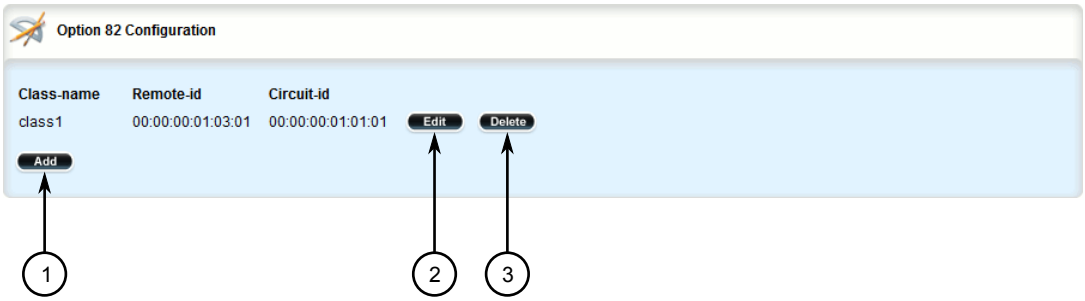


Figure 332: Option 82 Configuration Table

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

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 7.3.19

Example: Configuring the Device as a DHCP Server to Support a Relay Agent

This example demonstrates how to configure the device as a DHCP server, with a relay agent, without hosts or host groups.

The following topology depicts a scenario where two clients on separate LANs require IP addresses on different subnets from a DHCP server. Each client connects to the DHCP relay agent using different VLANs. The DHCP relay agent manages the requests and responses between the clients and the DHCP server.

IMPORTANT!
The values shown are specific to the provided topology. Actual values can vary based on the user's configuration.

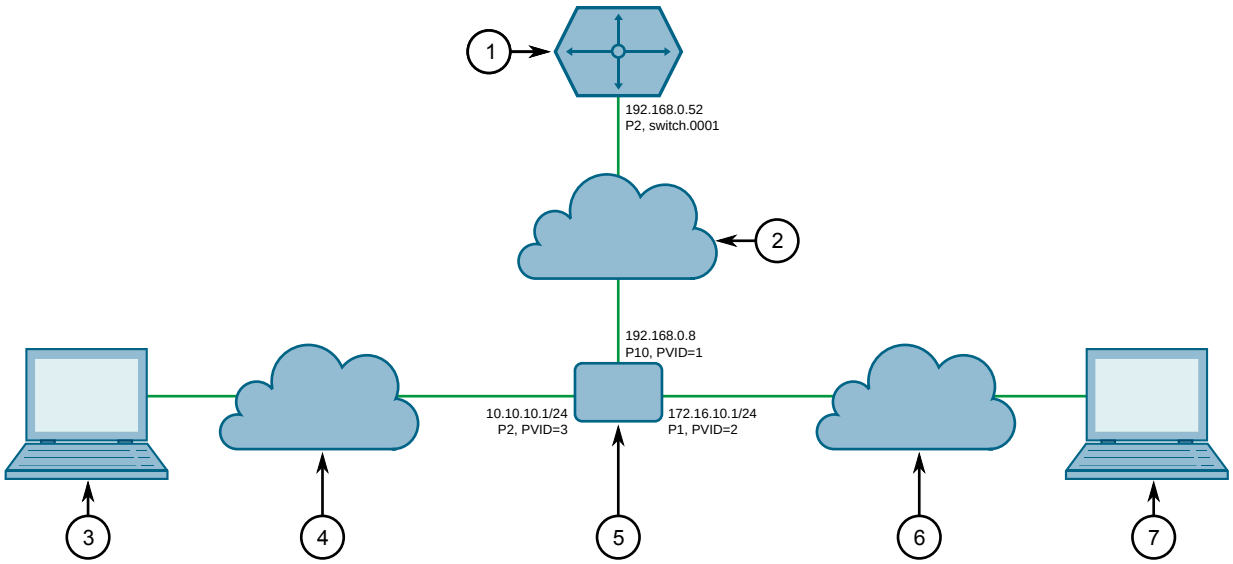


Figure 333: Topology – Device as a DHCP Server

1. DHCP Server (RUGGEDCOM ROX II Device) **2.** LAN A **3.** Client 2 **4.** LAN B **5.** DHCP Relay Agent **6.** LAN C **7.** Client 1

To configure the device per the topology, do the following:

1. Configure a separate device as the DHCP relay agent:

   NOTE
   The relay agent may be a RUGGEDCOM ROX II device, a RUGGEDCOM ROS device, or a third party device with relay agent capabilities.

   a. Add and configure VLAN 2 and VLAN 3.
   b. Assign IP address *192.168.0.8* to VLAN 1.
   c. Change the PVID of port 1 to PVID 2.
   d. Change the PVID of port 2 to PVID 3.

   If the relay agent being used is a RUGGEDCOM ROX II device, refer to Section 7.2.6, "Example: Configuring the Device as a Relay Agent" for more information.
2. Enable the DHCP server. For more information, refer to Section 7.3.3, "Enabling/Disabling the DHCP Server".
3. Add the management interface (switch.0001) as a DHCP listen interface. For more information, refer to Section 7.3.6.2, "Adding a DHCP Listen Interface".
4. Assign IP address *192.168.0.52* to switch.0001 on the DHCP server. For more information, refer to Section 7.1.3.2, "Adding an IPv4 Address" or Section 7.1.4.2, "Adding an IPv6 Address".
5. Create a shared network named *LAN.10-LAN.172* and enable Option82. For more information, refer to Section 7.3.7.3, "Configuring Shared Network Options".
6. Under the subnet for the DHCP Client, create the following 3 subnets:

Name	Network IP	Shared Network
MainSub	192.168.0.0/24	LAN.10-LAN.172
LAN_A-172	172.16.10.0/24	LAN.10-LAN.172

Name	Network IP	Shared Network
LAN_B-10	10.10.10.0/24	LAN.10-LAN.172

For more information about creating subnets, refer to Section 7.3.8.2, "Adding a Subnet".

7. [Optional] For the LAN A-172 subnet, configure *172.16.10.1* as a default route for clients. For more information, refer to Section 7.3.5.1, "Configuring Standard DHCP Client Configuration Options (IPv4)".
8. Create an address pool for the LAN A-172 subnet and configure the IP range for the address pool with the following parameters:

Pool Name	Starting Address	Ending Address
LAN-A_VLAN2	172.16.10.10	172.16.10.200

For more information, refer to Section 7.3.11.2, "Adding an Address Pool (IPv4)" or Section 7.3.12.2, "Adding an Address Pool (IPv6)".

9. Configure the following option82 class for the LAN-A_VLAN2 pool:

Class Name	Remote ID	Circuit ID
LAN-A_Option	00:0a:dc:00:00:00	00:02:00:01

The Remote ID represents the MAC address of the DHCP relay agent. In the Circuit ID, *00:02* denotes the VLAN ID and *00:01* represents the line module (if applicable) and the port number of the DHCP relay agent where Client 1 is connected.

For more information, refer to Section 7.3.18.2, "Adding an Option 82 Class to an Address Pool".

10. [Optional] For the LAN B-10 subnet, configure *10.10.10.1* as a default route for clients. For more information, refer to Section 7.3.5.1, "Configuring Standard DHCP Client Configuration Options (IPv4)".
11. Create an address pool for the LAN B-10 subnet and configure the IP range for the address pool with the following parameters:

Pool Name	Starting Address	Ending Address
LAN-B_VLAN3	10.10.10.10	10.10.10.200

For more information, refer to Section 7.3.11.2, "Adding an Address Pool (IPv4)" or Section 7.3.12.2, "Adding an Address Pool (IPv6)".

12. Configure the following option82 class for LAN-B_VLAN3 pool:

Class Name	Remote ID	Circuit ID
LAN-B_Option	00:0a:dc:00:00:00	00:03:00:02

The Remote ID represents the MAC address of the DHCP relay agent, *00:03* denotes the VLAN ID and *00:02* represents the line module (if applicable) and the port number of the DHCP relay agent where Client 2 is connected.

For more information, refer to Section 7.3.18.2, "Adding an Option 82 Class to an Address Pool".

Final Configuration Example

The following configuration reflects the topology:

```
#show running-config services dhcpserver
  enabled
```

```
  interface switch.0001
  !
  options
   client
    no hostname
    no subnetmask
 no default-route
    no broadcast
    no domain
    no dns-server
    no static-route
    no nis server
    no nis domain
   !
  !
  shared-network LAN.10-LAN.172
   options option82
   options client
    no hostname
    no subnetmask
    no default-route
    no broadcast
    no domain
    no dns-server
    no static-route
    no nis server
    no nis domain
   !
  !
  subnet-name "LAN A-172"
   network-ip     172.16.10.0/24
   shared-network LAN.10-LAN.172
   options
    no unknown-client
    ippool LAN-A_VLAN2
     no unknown-client
     iprange 172.16.10.10
      end 172.16.10.200
     !
     option82 LAN-A_Option
      remote-id  00:0a:dc:00:00:00
      circuit-id 00:02:00:01
     !
    !
    client
     no hostname`
     no subnetmask
     default-route 172.16.10.1
     no broadcast
no domain
     no dns-server
     no static-route
     no nis server
     no nis domain
    !
   !
  !
  subnet-name "LAN B-10"
   network-ip     10.10.10.0/24
   shared-network LAN.10-LAN.172
   options
    no unknown-client
    ippool LAN-B_VLAN3
     no unknown-client
     iprange 10.10.10.10
      end 10.10.10.200
     !
```

```
     option82 LAN-B_Option
      remote-id  00:0a:dc:00:00:00
      circuit-id 00:03:00:02
     !
    !
    client
     no hostname
     no subnetmask
     default-route 10.10.10.1
     no broadcast
     no domain
     no dns-server
     no static-route
     no nis server
     no nis domain
    !
   !
  !
  subnet-name mainSub
   network-ip     192.168.0.0/24
   shared-network LAN.10-LAN.172
   options
    no unknown-client
    client
     no hostname
no subnetmask
     no default-route
     no broadcast
     no domain
     no dns-server
     no static-route
     no nis server
     no nis domain
```

Section 7.4

Managing Static DNS

This section describes how to reserve a static or fixed IP address for the device. While it is more common to obtain a random address from a *dynamic* DNS server, obtaining a fixed address from a static DNS server may be required to connect to Virtual Private Networks (VPNs) or other remote access services that only trust specific IP addresses.

CONTENTS

Section 7.4.1

Managing Domain Names

The DNS service can be configured to use one or more domain names when querying a domain name server. The list of domain names can include the domain in which the router is a member of, and other domains that may be used to search for an unqualified host name (i.e. as though it were local).

CONTENTS

Section 7.4.1.1

Viewing a List of Domain Names

To view a list of domain names, navigate to ***admin » dns » search***. If domain names have been configured, the **Domain Name Searches** table appears.

Figure 334: Domain Name Searches Table

If no domain names have been configured, add names as needed. For more information, refer to Section 7.4.1.2, "Adding a Domain Name".

Section 7.4.1.2

Adding a Domain Name

To add a domain name, do the following:

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

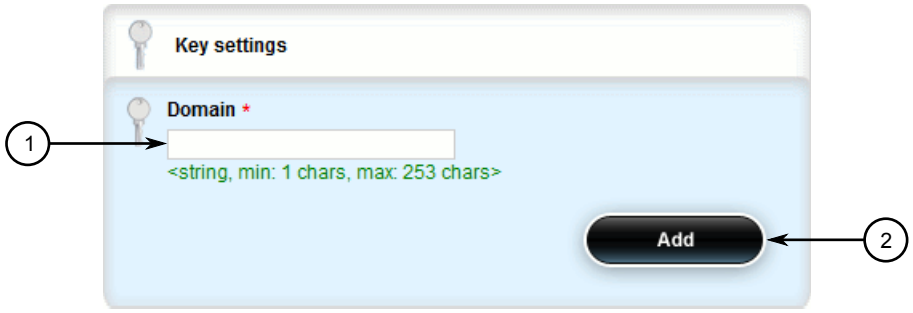


Figure 335: Key Settings Form

1. Domain Box **2.** Add Button

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

Parameter	Description
domain	**Synopsis:** A string 1 to 253 characters long

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 7.4.1.3

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.

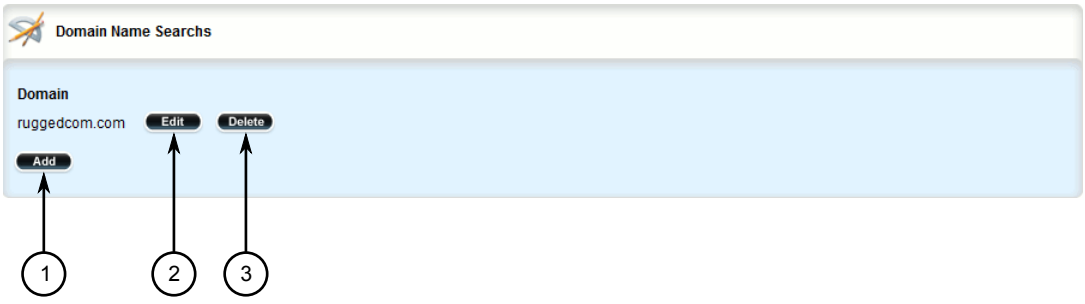


Figure 336: Domain Name Searches Table

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

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 7.4.2
Managing Domain Name Servers

A hierarchical list of domain name servers can be configured for the DNS service. RUGGEDCOM ROX II will contact each server in the order they are listed when domain names require resolution.

CONTENTS

Section 7.4.2.1
Viewing a List of Domain Name Servers

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.

Figure 337: Domain Name Servers Table

If no domain name servers have been configured, add servers as needed. For more information, refer to Section 7.4.2.2, "Adding a Domain Name Server".

Section 7.4.2.2
Adding a Domain Name Server

To add a domain name server, do the following:

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

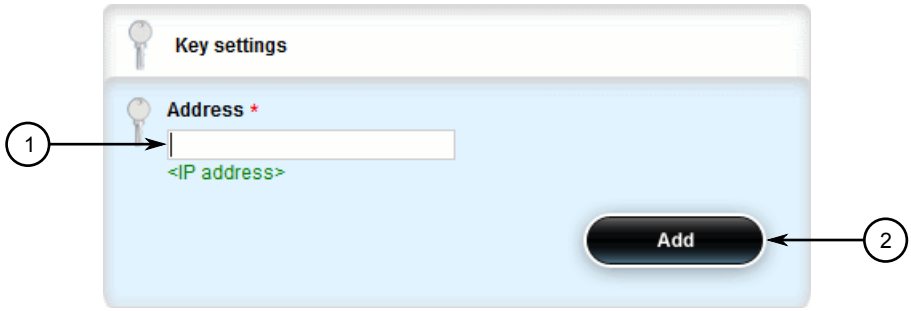


Figure 338: Key Settings Form

1. Address Box **2.** Add Button

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

Parameter	Description
address	**Synopsis:** 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 7.4.2.3

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.

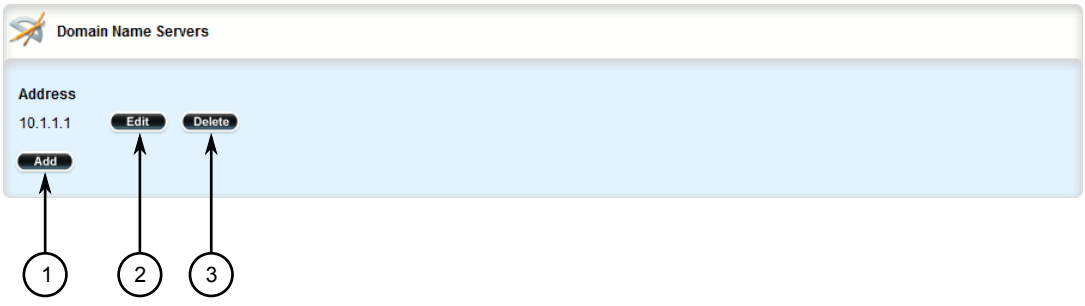


Figure 339: Domain Name Servers Table

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

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.

Section 7.5
Managing Dynamic DNS

Enable the Dynamic Domain Name Server (DNS) service in RUGGEDCOM ROX II to allow remote hosts to connect with the device's default interface via a fixed host name. The Dynamic DNS service uses a DNS client to log into a DNS service provider and register the assigned host name(s) that can be used to access the device via the Internet.

An account is required with one of the supported dynamic DNS service providers:

- noip.com [http://www.noip.com]
- dyn.com [http://www.dyn.com]

Responses from each Dynamic DNS service provider are validated by the Dynamic DNS client. If a response is determined to be invalid, a *DDNS Bad Response* alarm is raised and the service is temporarily disabled. Service can only be restored once the alarm has been cleared. For information about how to configure this alarm, refer to Section 5.7.4, "Configuring an Alarm".

CONTENTS

Section 7.5.1
Enabling and Configuring Dynamic DNS

To enable and configure dynamic DNS, do the following:

IMPORTANT!
Update requests are sent to the selected service provider via HTTPS. As such, before enabling Dynamic DNS, the Trusted Certificate Store must be enabled. For more information, refer to Section 6.7.2.2, "Enabling/Disabling the Trusted Certificate Store".

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to ***services » ddns***. The **Dynamic DNS** and **Dynamic DNS Configuration** forms appear.

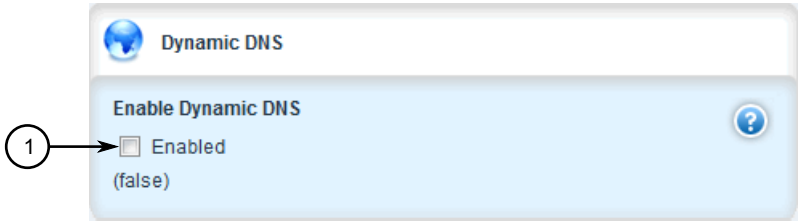


Figure 340: Dynamic DNS Form

1. Enable Dynamic DNS Check Box

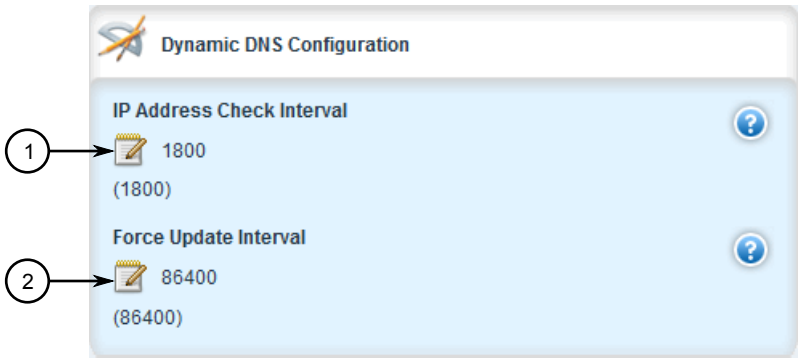


Figure 341: Dynamic DNS Configuration Form

1. IP Address Check Interval Box **2.** Force Update Interval Box

3. On the **Dynamic DNS** form, select **Enable Dynamic DNS**.
4. On the **Dynamic DNS Configuration** form, configure the following parameter(s) as required:

IMPORTANT!
Make sure the `IP Check Interval` setting does not exceed the service provider's requirements, if any, regarding the frequency of update requests. Requests made too frequently may be considered an abuse of the service, potentially resulting in the device's IP address being blocked.

Parameter	Description
IP Address Check Interval	**Synopsis:** A 32-bit unsigned integer between 600 and 864000 **Default:** 1800 Interval (in seconds) to check change of the IP address
Force Update Interval	**Synopsis:** A 32-bit unsigned integer between 600 and 2592000 **Default:** 86400 Interval (in seconds) to send update to DDNS server even it has not changed

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 7.5.2

Managing Dynamic DNS Servers

This section describes how to configure a connection with one or more of the supported dynamic DNS service providers.

CONTENTS

Section 7.5.2.1

Viewing a List of Dynamic DNS Servers

To view a list of dynamic DNS servers, navigate to ***services » ddns » servers***. If dynamic DNS servers have been configured, the **Dynamic DNS Servers** table appears.

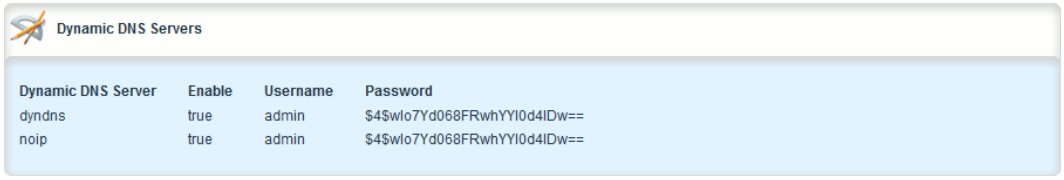


Figure 342: Dynamic DNS Servers Table

If no dynamic DNS servers have been configured, add servers as needed. For more information, refer to Section 7.5.2.3, "Adding a Dynamic DNS Server".

Section 7.5.2.2

Viewing the Status of a Dynamic DNS Server

To view the status of a dynamic DNS server, navigate to ***services » ddns » servers » {server} » status***, where *{server}* is the selected dynamic DNS server. If the selected dynamic DNS server is enabled, the **Dynamic DNS Status** and **Dynamic DNS Status Details** forms appear.

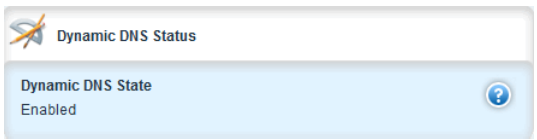


Figure 343: Dynamic DNS Status Form

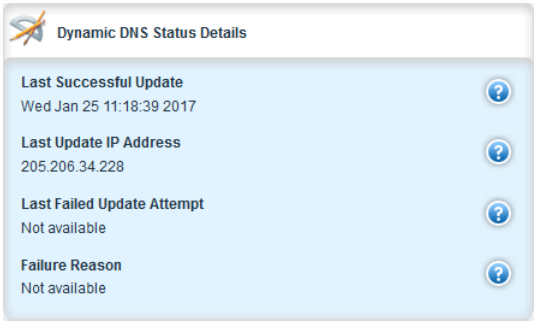


Figure 344: Dynamic DNS Status Details Form

These forms provide the following information:

To view the status of a dynamic DNS server, type:

```
show services ddns servers [ noip | dyndns ] status
```

If the selected dynamic DNS server is enabled, a table or list similar to the following example appears:

```
ruggedcom# show services ddns servers dyndns status
status
 ddns state Enabled
 details
  ddns last success        "Wed Jan 25 11:18:39 2017"
  ddns last ip address     205.206.34.228
  ddns last failure        "Not available"
  ddns last failure reason "Not available"
```

The table/list provides the following information:

Parameter	Description
Dynamic DNS State	**Synopsis:** A string Displays DDNS state

Section 7.5.2.3

Adding a Dynamic DNS Server

To add a dynamic DNS server, do the following:

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

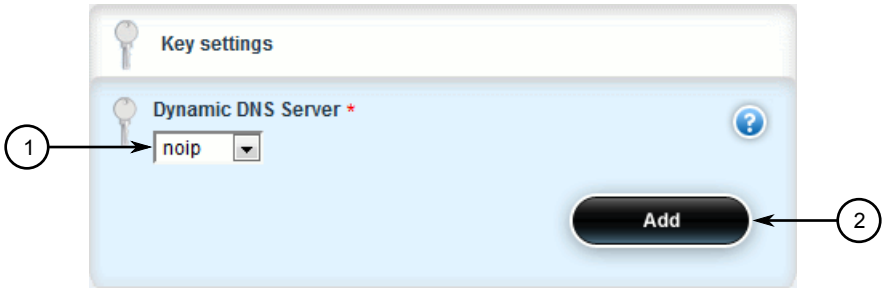


Figure 345: Key Settings Form

1. Dynamic DNS Server List **2.** Add Button

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

Parameter	Description
Dynamic DNS Server	**Synopsis:** { dyndns, noip } Name of the DDNS server

4. Click **Add** to create the server. The **Dynamic DNS Servers** form appears.

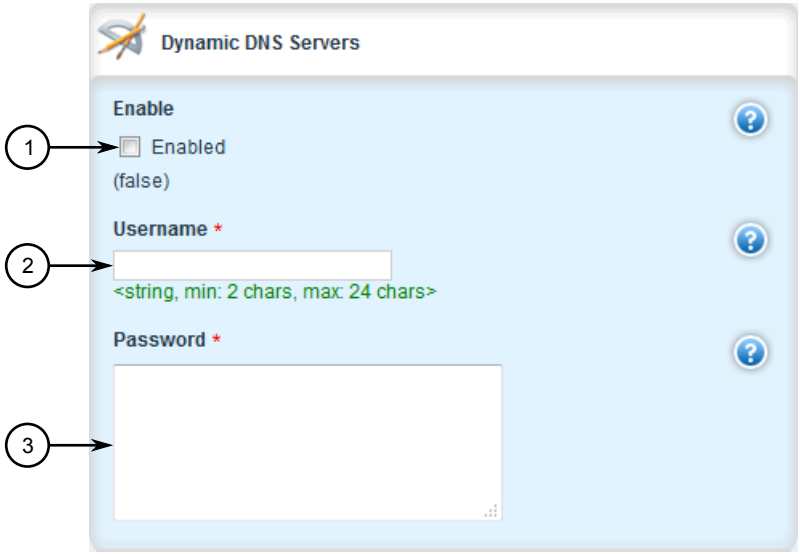


Figure 346: Dynamic DNS Servers Form

1. Enable Check Box **2.** Username Box **3.** Password Box

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

Parameter	Description
Enable	**Synopsis:** { true, false } **Default:** false Enables / disables DDNS updates for the server

Parameter	Description
Username	**Synopsis:** A string 2 to 24 characters long The username of the DDNS server This parameter is mandatory.
Password	**Synopsis:** A string The password of the DDNS server This parameter is mandatory.

6. Define one or more host names for the server. For more information, refer to Section 7.5.3.2, "Adding a Host 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 7.5.2.4
Deleting a Dynamic DNS Server

To delete a dynamic DNS server, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to ***services » ddns » servers***. The **Dynamic DNS Servers** table appears.

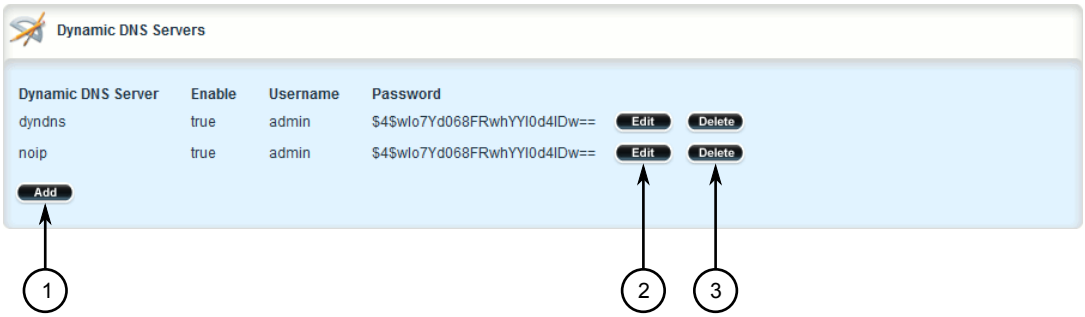


Figure 347: Dynamic DNS Servers Table

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

3. Click **Delete** next to the desired 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 7.5.3
Managing Dynamic DNS Server Host Names

This section describes how to manage host names for the configured dynamic DNS servers.

IMPORTANT!
At least one host name is required for each configured dynamic DNS server.

CONTENTS

Section 7.5.3.1
Viewing a List of Host Names

To view a list of host names configured for a dynamic DNS server, navigate to ***services » ddns » servers » {server} » hostnames***, where *{server}* is the selected dynamic DNS server. If host names have been configured, the **Dynamic DNS Servers** table appears.

Figure 348: Dynamic DNS Servers Table

If no host names have been configured, add host names as needed. For more information, refer to Section 7.5.3.2, "Adding a Host Name".

Section 7.5.3.2
Adding a Host Name

To add a host name for a dynamic DNS server, do the following:

IMPORTANT!
At least one host name is required for each configured dynamic DNS server.

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to ***services » ddns » servers » {server} » hostnames***, where *{server}* is the selected dynamic DNS server.
3. Click **<Add hostname>**. The **Key Settings** form appears.

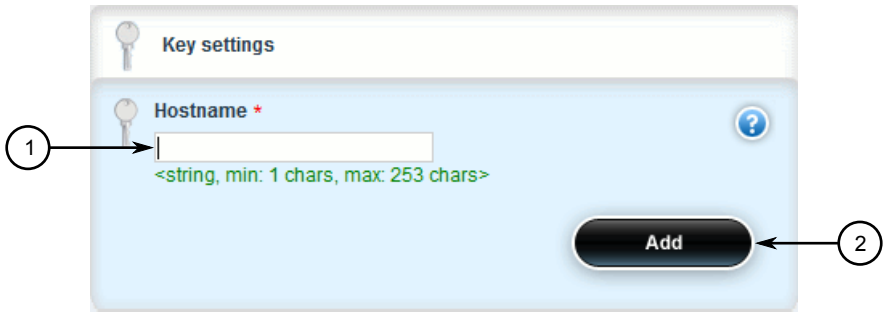


Figure 349: Key Settings Form

1. Hostname Box **2.** Add Button

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

Parameter	Description
Hostname	**Synopsis:** A string 1 to 253 characters long Hostname to be updated

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 7.5.3.3

Deleting a Host Name

To delete a host name, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to ***services » ddns » servers » {server} » hostnames***, where *{server}* is the selected dynamic DNS server. The **Dynamic DNS Hostnames** table appears.

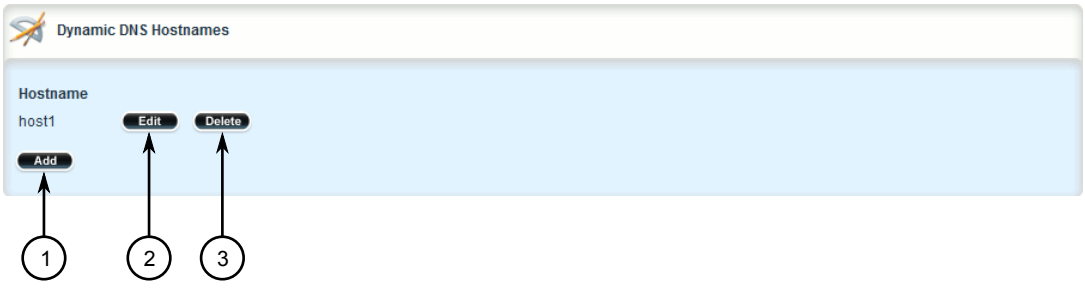


Figure 350: Dynamic DNS Hostnames Table

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

3. Click **Delete** next to the desired host 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.

8 Layer 2

This chapter describes the Layer 2, or Data Link Layer (DLL), features of RUGGEDCOM ROX II.

CONTENTS

Section 8.1

Managing Switched Ethernet Ports

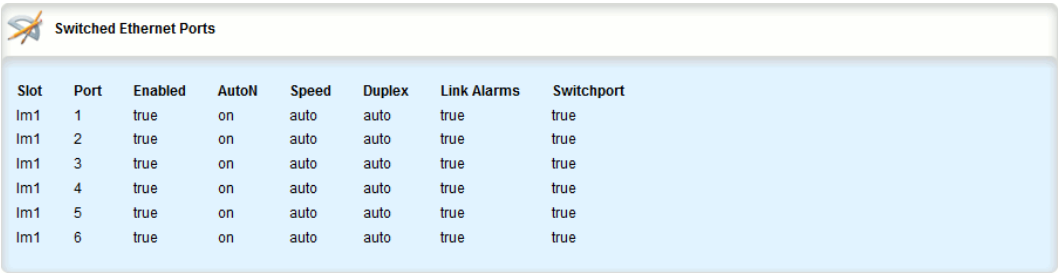
This section describes how to configure and manage switched Ethernet ports.

CONTENTS

Section 8.1.1

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.



Switched Ethernet Ports

Slot	Port	Enabled	AutoN	Speed	Duplex	Link Alarms	Switchport
lm1	1	true	on	auto	auto	true	true
lm1	2	true	on	auto	auto	true	true
lm1	3	true	on	auto	auto	true	true
lm1	4	true	on	auto	auto	true	true
lm1	5	true	on	auto	auto	true	true
lm1	6	true	on	auto	auto	true	true

Figure 351: Switched Ethernet Ports Table

Section 8.1.2

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.

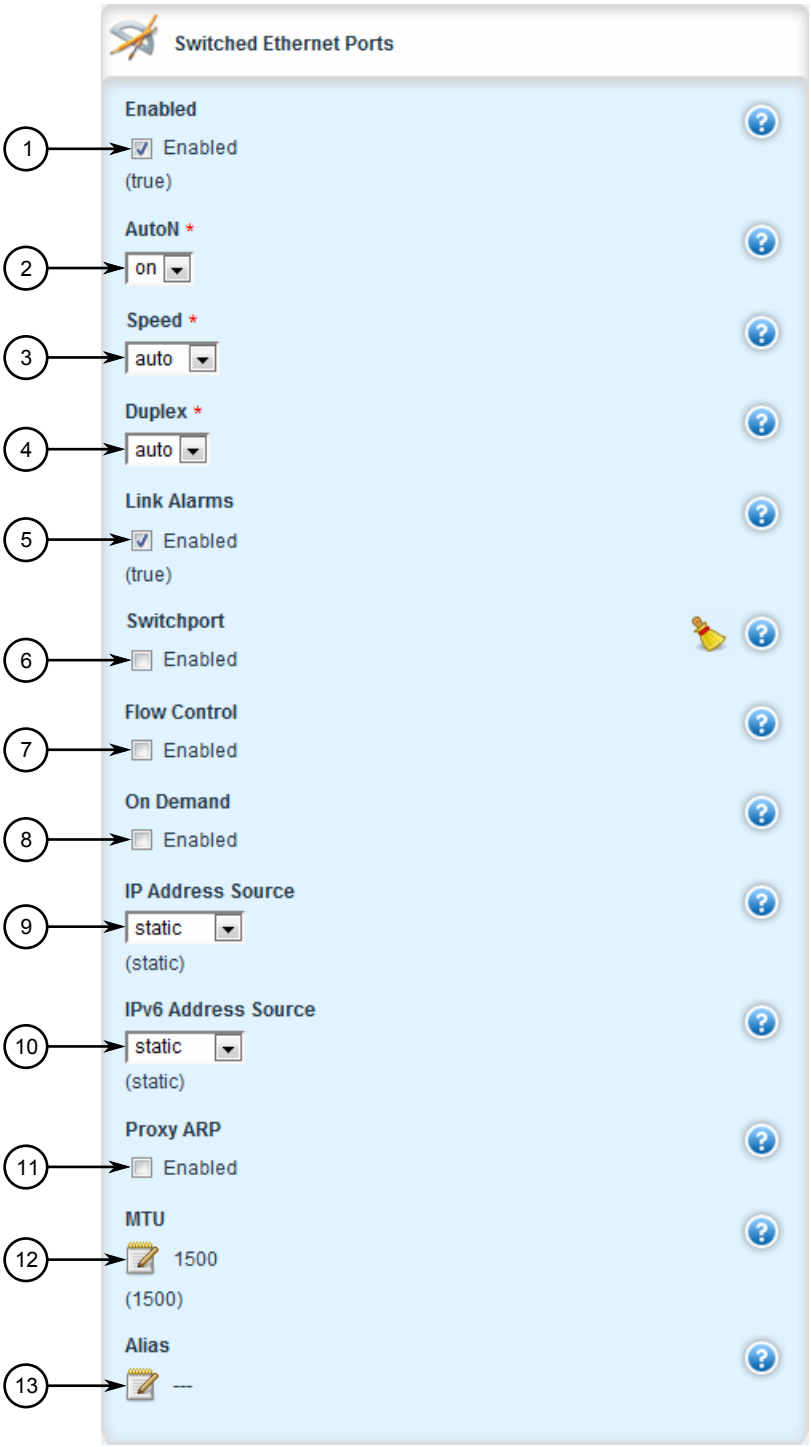


Figure 352: Switched Ethernet Ports Form

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 Source List **10.** IPv6 Address Source List **11.** Proxyarp Check Box **12.** MTU Box **13.** Alias Box

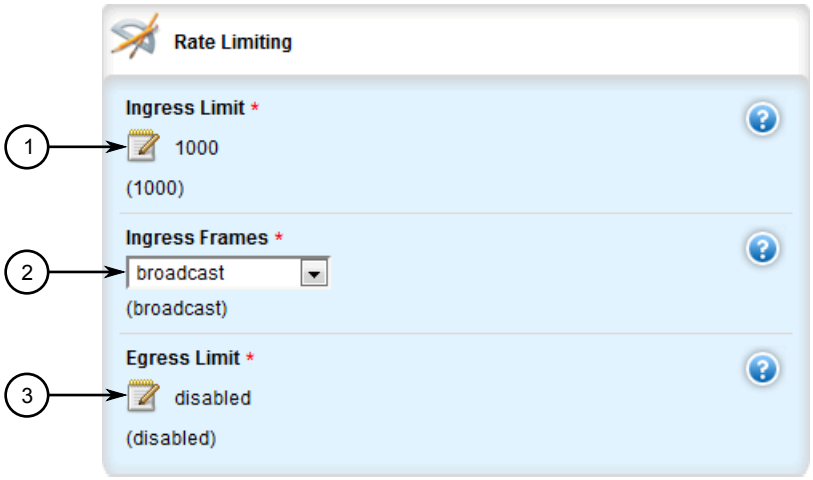


Figure 353: Rate Limiting Form

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

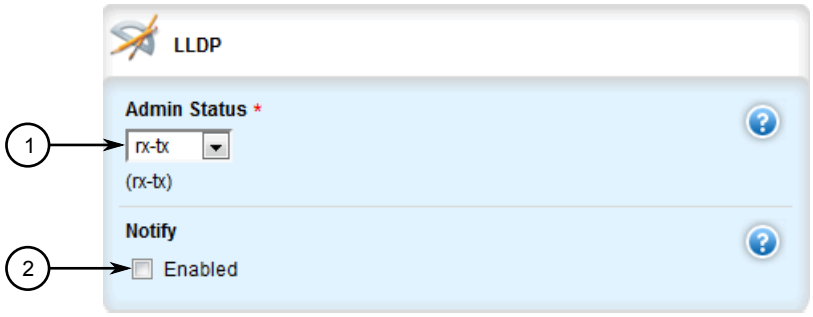


Figure 354: LLDP Form

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.*

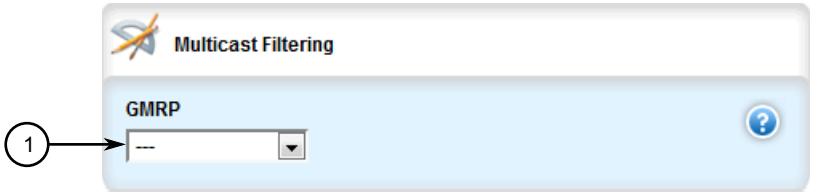


Figure 355: Multicast Filtering Form

1. GMRP List

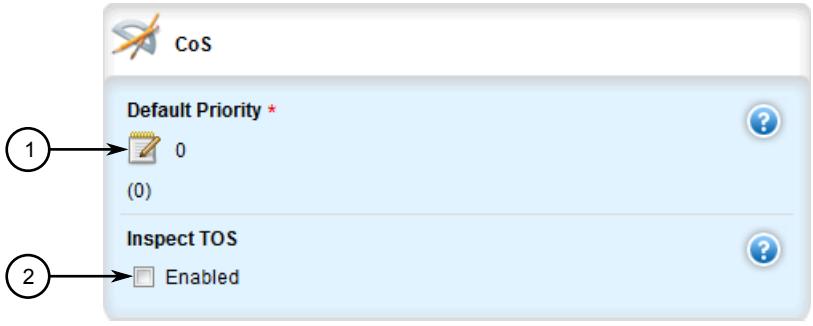


Figure 356: CoS Form

1. Default Priority Box **2.** Inspect TOS Check Box

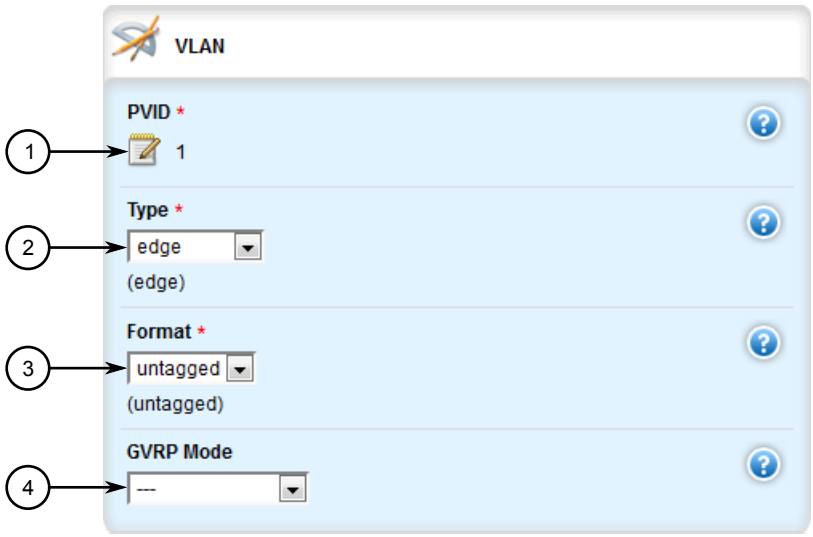


Figure 357: VLAN Form

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	**Synopsis:** { true, false } **Default:** true Provides the option to enable or disable this interface. When unchecked(i.e disabled), the interface will prevent all frames from being sent and received on that interface.
AutoN	**Synopsis:** A string Enables or disables IEEE 802.3 auto-negotiation. Enabling auto-negotiation results in speed and duplex being negotiated upon link detection; both end devices must be auto-negotiation compliant for the best possible results. This parameter is mandatory.
Speed	**Synopsis:** A string Speed (in megabits-per-second or gigabits-per-second). If auto-negotiation is enabled, this is the speed capability advertised by the auto-negotiation process. If auto-negotiation is disabled, the port is explicitly forced to this speed mode. AUTO means advertise all supported speed modes. This parameter is mandatory.
Duplex	**Synopsis:** A string If auto-negotiation is enabled, this is the duplex capability advertised by the auto-negotiation process. If auto-negotiation is disabled, the port is explicitly forced to this duplex mode. AUTO means advertise all supported duplex modes. This parameter is mandatory.
Link Alarms	**Synopsis:** { true, false } **Default:** true Disabling link-alarms will prevent alarms and LinkUp and LinkDown SNMP traps from being sent for that interface. Link alarms may also be controlled for the whole system under admin / alarm-cfg.
Switchport	**Synopsis:** { true, false } Sets the physical port into either switched mode or a dedicated routing mode.
Flow Control	Flow control is useful for preventing frame loss during times of severe network traffic
On Demand	Bring up this interface on-demand only
IP Address Source	**Synopsis:** { static, dynamic } **Default:** static Whether the IP address is static or dynamically assigned via DHCP or BOOTP. Option DYNAMIC is a common case of a dynamically assigned IP address. It switches between BOOTP and DHCP until it gets the response from the relevant server. This must be static for non-management interfaces.
IPv6 Address Source	**Synopsis:** { static, dynamic } **Default:** static

Parameter	Description
	Whether the IPv6 address is static or dynamically assigned via DHCPv6. Option DYNAMIC is a common case of a dynamically assigned IPv6 address. This must be static for non-management interfaces.
Proxy ARP	Enables/Disables whether the VLAN will respond to ARP requests for hosts other than itself
MTU	**Synopsis:** A 32-bit signed integer between 68 and 9216 **Default:** 1500 Maximum transmission unit (largest packet size allowed for this interface).
Alias	**Synopsis:** 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	**Synopsis:** { disabled } or a 32-bit signed integer between 62 and 256000 **Default:** 1000 The data rate in kbps at which received frames (of the type described by the ingress frames parameter) will start to be discarded by the switch. The valid range is 62 to 256000 kbps. The default value is 1000 kbps. If not set(cleared), this feature is disabled.
Ingress Frames	**Synopsis:** { broadcast, multicast, mcast-flood-ucast, all } **Default:** broadcast This parameter specifies the types of frames to rate-limit on this port. It applies only to received frames: • BROADCAST : only broadcast frames will be limited. • MULTICAST : all multicast frames (including broadcast) will be limited. • MCAST-FLOOD-UCAST : all multicast frames (including broadcast) will be limited. Unicast will not be limited. • ALL : all frames (both multicast and unicast) will be limited.
Egress Limit	**Synopsis:** { disabled } or a 32-bit signed integer between 62 and 256000 **Default:** disabled The maximum data rate in kbps at which the switch will transmit (multicast, broadcast and unicast) frames on this port. The switch will discard frames in order to meet this rate if required. The valid range is 62 to 256000 Kbps. If not set, this feature is disabled.

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

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

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

Parameter	Description
GMRP	**Synopsis:** { advertise_only, learn_advertise }

Parameter	Description
	GMRP (GARP Multicast Registration Protocol) operation on the port. There are several GMRP operation modes: • DISABLED : the port is not capable of any GMRP processing. • ADVERTISE ONLY : the port will declare all MCAST addresses existing in the switch (configured or learned) but will not learn any MCAST addresses. • ADVERTISE and LEARN : the port will declare all MCAST Addresses existing in the switch (configured or learned) and can dynamically learn MCAST addresses.

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

Parameter	Description
Default Priority	**Synopsis:** A 32-bit signed integer between 0 and 7 **Default:** 0 The priority of frames received on this port that are not prioritized based on the frame's contents (e.g. the priority field in the VLAN tag, DiffServ field in the IP header, prioritized MAC address).
Inspect ToS	Enables or disables parsing of the Type-of-Service (ToS) field in the IP header of the received frames to determine what Class of Service (CoS) they should be assigned. When ToS parsing is enabled the switch will use the differentiated services bits in the TOS field.

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

Parameter	Description
PVID	**Synopsis:** A 32-bit signed integer between 1 and 4094 The Port VLAN Identifier specifies the VLAN ID associated with untagged (and 802.1p priority tagged) frames received on this port. Frames tagged with a non-zero VLAN ID will always be associated with the VLAN ID retrieved from the frame tag.
Type	**Synopsis:** { edge, trunk, pvlanedge } **Default:** edge How the port determines its membership in VLANs. There are a few types of ports: • EDGE : the port is only a member of one VLAN (its native VLAN specified by the 'PVID' parameter). • PVLAN Edge : the port does not forward traffic to other PVLAN edge ports within the same VLAN. • TRUNK : the port is automatically a member of all configured VLANs. Frames transmitted out of the port on all VLANs except the port's native VLAN will be always tagged. It can also be configured to use GVRP for automatic VLAN configuration.
Format	**Synopsis:** { untagged, tagged } **Default:** untagged Whether frames transmitted out of the port on its native VLAN (specified by the 'PVID' parameter) will be tagged or untagged.
GVRP Mode	**Synopsis:** { advertise_only, learn_advertise } GVRP (Generic VLAN Registration Protocol) operation on the port. There are several GVRP operation modes: • DISABLED : the port is not capable of any GVRP processing. • ADVERTISE ONLY : the port will declare all VLANs existing in the switch (configured or learned) but will not learn any VLANs. • ADVERTISE and LEARN : the port will declare all VLANs existing in the switch (configured or learned) and can dynamically learn VLANs.

NOTE
*Once a VLAN ID has been assigned to a switched Ethernet port, a VLAN is created and can be configured in **switch » vlans » all-vlans**.*

9. If the port is in switchport mode, configure the VLAN for the port. For more information, refer to Section 8.5.4.2, "Configuring VLANs for Switched Ethernet Ports".
10. Configure the port security settings. For more information, refer to Section 6.5.2, "Configuring Port Security".
11. Configure the spanning tree settings. For more information, refer to Section 14.3.5, "Configuring STP for Switched Ethernet Ports and Ethernet Trunk Interfaces".
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 8.1.3
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.

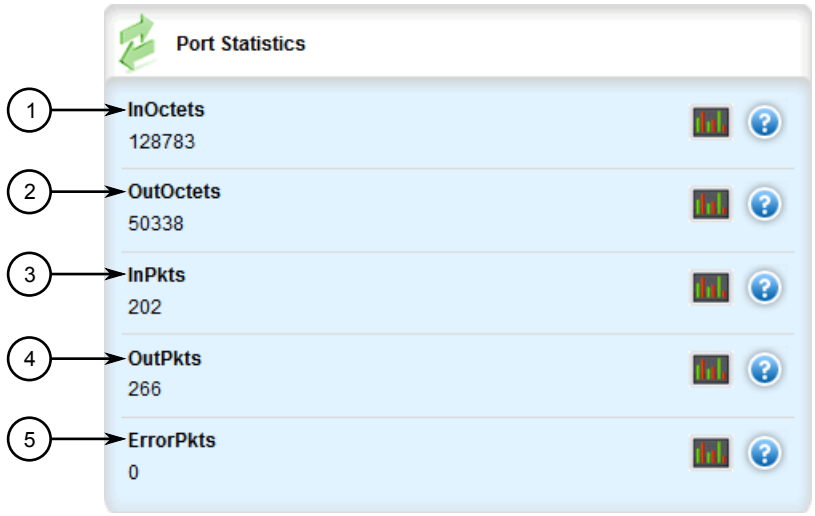


Figure 358: Port Statistics Form

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

This form provides the following information:

Parameter	Description
InOctets	**Synopsis:** A 32-bit unsigned integer The number of octets in received good packets. (Unicast+Multicast+Broadcast) and dropped packets. This parameter is mandatory.

Parameter	Description
OutOctets	**Synopsis:** A 32-bit unsigned integer The number of octets in transmitted good packets. This parameter is mandatory.
InPkts	**Synopsis:** A 32-bit unsigned integer The number of received good packets (Unicast+Multicast+Broadcast) and dropped packets. This parameter is mandatory.
OutPkts	**Synopsis:** A 32-bit unsigned integer The number of transmitted good packets. This parameter is mandatory.
ErrorPkts	**Synopsis:** A 32-bit unsigned integer The number of any type of erroneous packets. This parameter is mandatory.

Section 8.1.4

Viewing the Status of a Switched Ethernet Port

To view the current status of a switched Ethernet port, navigate to ***interfaces » switch » {slot} » {port}***, where *{slot}* is the slot number (e.g. lm1) and *{port}* is the port number of the switched Ethernet port. The **Switched Ethernet Port Status** form appears.

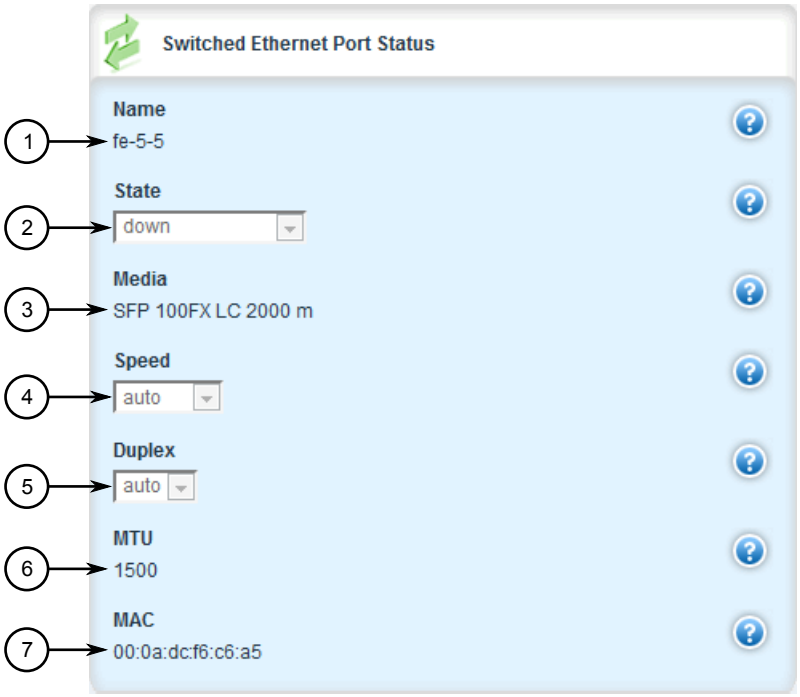


Figure 359: Switched Ethernet Port Status Form

1. Name **2.** State **3.** Media **4.** Speed **5.** Duplex **6.** MTU **7.** MAC

This form provides the following information:

Parameter	Description
Name	**Synopsis:** A string 1 to 10 characters long A descriptive name that may be used to identify the device connected on that port. This parameter is mandatory.
State	**Synopsis:** { not set, up, down, testing, unknown, dormant, notPresent, lowerLayerDown } The port's link status. This parameter is mandatory.
Media	**Synopsis:** A string 1 to 31 characters long The type of port media { 100TX, 10FL, 100FX, 1000X, 1000T, 802.11g, EoVDSL, 100TX }. It provides the user with a description of the installed media type on the port for modular products. Please note that fiber media may be either Single Mode(SM), Multi Mode(MM), and may be Short Distance, Long Distance or Very Long Distance with connectors like LC, SC, ST, MTRJ etc. For the modules with SFP/GBICs, the media description is displayed per the SFF-8472 specification, if the transceiver is plugged into the module. E.g. 10/100/1000TX RJ45, 100FX SM SC, 10FX MM ST,1000SX SFP LC S SL M5. This parameter is mandatory.
Speed	**Synopsis:** { auto, 1.5M, 2.4M, 10M, 100M, 1G, 10G, 1.776M, 3.072M, 7.2M, 1.2K, 2.4K, 9.6K, 19.2K, 38.4K, 57.6K, 115.2K, 230.4K, 4.8K, 76.8K } Speed (in Megabits-per-second or Gigabits-per-second) This parameter is mandatory.
Duplex	**Synopsis:** { auto, half, full } Duplex Setting: { Auto, Half, Full } This parameter is mandatory.
MTU	**Synopsis:** A 32-bit signed integer The Maximum Transmission Unit of frame (in bytes) permitted on the interface. This parameter is mandatory.
MAC	**Synopsis:** A string 17 characters long The MAC Address of this specific port. This parameter is mandatory.

Section 8.1.5

Viewing RMON Port Statistics

To view Remote Network Monitoring (RMON) statistics collected for a specific switched Ethernet port, 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.

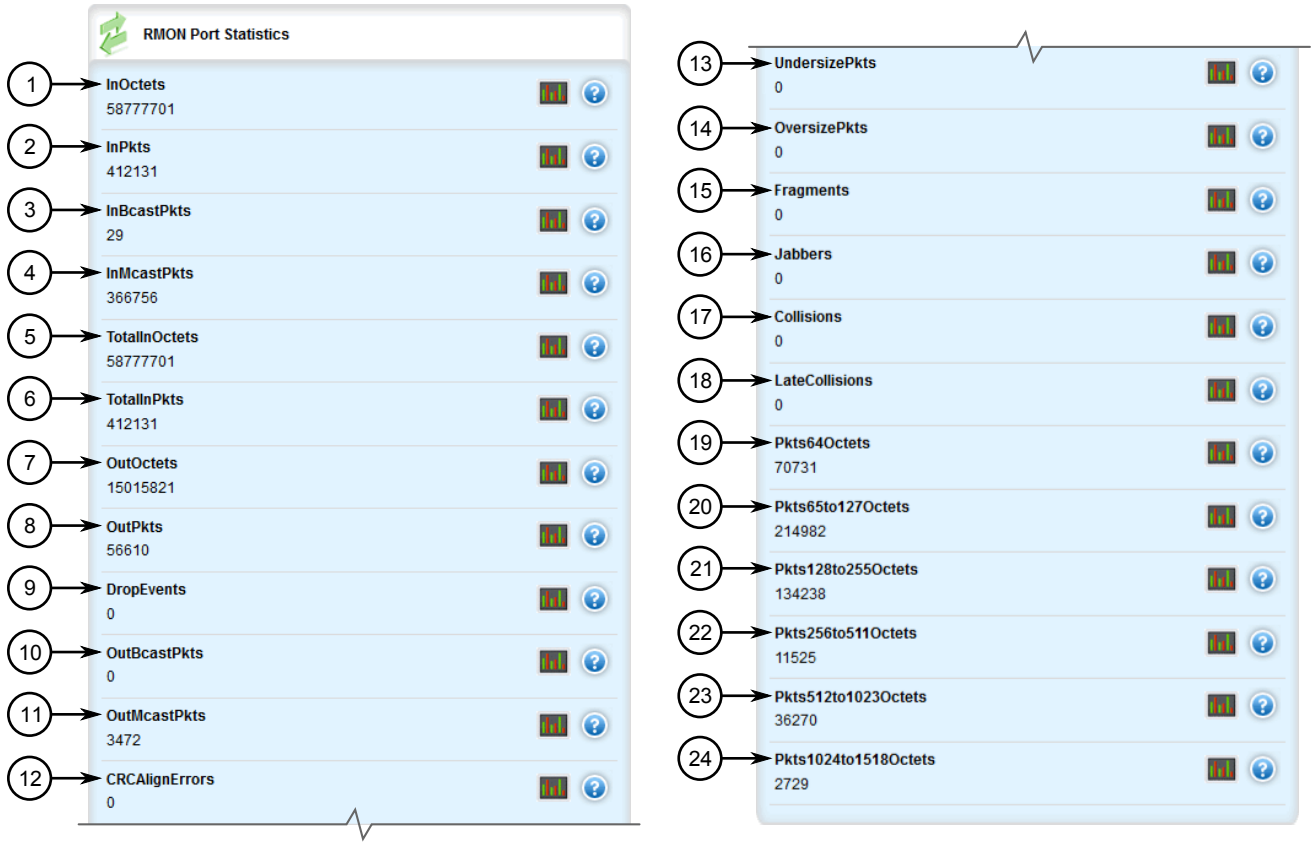


Figure 360: RMON Port Statistics Form

1. InOctets **2.** InPkts **3.** InBcastPkts **4.** InMcastPkts **5.** TotalInOctets **6.** TotalInPkts **7.** OutOctets **8.** OutPkts **9.** DropEvents **10.** OutBcastPkts **11.** OutMcastPkts **12.** CRCAlignErrors **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	**Synopsis:** A 64-bit unsigned integer The number of octets in received good packets (Unicast+Multicast+Broadcast) and dropped packets. This parameter is mandatory.
InPkts	**Synopsis:** A 64-bit unsigned integer The number of received good packets (Unicast+Multicast+Broadcast) and dropped packets. This parameter is mandatory.
InBcastPkts	**Synopsis:** A 64-bit unsigned integer The number of good broadcast packets received. This parameter is mandatory.
InMcastPkts	**Synopsis:** A 64-bit unsigned integer The number of good multicast packets received. This parameter is mandatory.

Parameter	Description
TotalInOctets	**Synopsis:** A 64-bit unsigned integer The total number of octets of all received packets. This includes data octets of rejected and local packets which are not forwarded to the switching core for transmission. It should reflect all the data octets received on the line. This parameter is mandatory.
TotalInPkts	**Synopsis:** A 64-bit unsigned integer The number of received packets. This includes rejected, dropped and local packets, as well as packets which are not forwarded to the switching core for transmission. It should reflect all packets received on the line. This parameter is mandatory.
OutOctets	**Synopsis:** A 64-bit unsigned integer The number of octets in transmitted good packets. This parameter is mandatory.
OutPkts	**Synopsis:** A 64-bit unsigned integer The number of transmitted good packets. This parameter is mandatory.
DropEvents	**Synopsis:** A 32-bit unsigned integer The number of received packets that are dropped due to lack of receive buffers. This parameter is mandatory.
OutBcastPkts	**Synopsis:** A 64-bit unsigned integer The number of transmitted broadcast packets. This parameter is mandatory.
OutMcastPkts	**Synopsis:** A 64-bit unsigned integer The number of transmitted multicast packets. This does not include broadcast packets. This parameter is mandatory.
CRCAlignErrors	**Synopsis:** A 32-bit unsigned integer The number of packets received which meet all the following conditions: 1. The packet data length is between 64 and 1536 octets inclusive. 2. The packet has invalid CRC. 3. A Collision Event has not been detected. 4. A Late Collision Event has not been detected. This parameter is mandatory.
UndersizePkts	**Synopsis:** A 64-bit unsigned integer The number of received packets which meet all the following conditions: 1. The packet data length is less than 64 octets. 2. A Collision Event has not been detected. 3. A Late Collision Event has not been detected. 4. The packet has valid CRC. This parameter is mandatory.
OversizePkts	**Synopsis:** A 32-bit unsigned integer The number of packets received with data length greater than 1536 octets and valid CRC. This parameter is mandatory.
Fragments	**Synopsis:** A 32-bit unsigned integer The number of packets received which meet all the following conditions: 1. The packet data length is less than 64 octets, or it is a packet without SFD and is less than 64 octets in length. 2. A Collision Event has not been detected. 3. A Late Collision Event has not been detected. 4. The packet has invalid CRC. This parameter is mandatory.
Jabbers	**Synopsis:** A 32-bit unsigned integer

Parameter	Description
	The number of packets which meet all the following conditions: 1. The packet data length is greater that 1536 octets. 2. The packet has invalid CRC. This parameter is mandatory.
Collisions	**Synopsis:** A 32-bit unsigned integer The number of received packets for which a Collision Event has been detected. This parameter is mandatory.
LateCollisions	**Synopsis:** A 32-bit unsigned integer The number of received packets for which a Late Collision Event has been detected. This parameter is mandatory.
Pkts64Octets	**Synopsis:** A 32-bit unsigned integer The number of received and transmitted packets with a size of 64 octets. This includes received and transmitted packets as well as dropped and local received packets. This does not include rejected received packets. This parameter is mandatory.
Pkts65to127Octets	**Synopsis:** A 32-bit unsigned integer The number of received and transmitted packets with a size of 65 to 127 octets. This includes received and transmitted packets as well as dropped and local received packets. This does not include rejected received packets This parameter is mandatory.
Pkts128to255Octets	**Synopsis:** A 32-bit unsigned integer The number of received and transmitted packets with a size of 128 to 257 octets. This includes received and transmitted packets as well as dropped and local received packets. This does not include rejected received packets This parameter is mandatory.
Pkts256to511Octets	**Synopsis:** A 32-bit unsigned integer The number of received and transmitted packets with size of 256 to 511 octets. This includes received and transmitted packets as well as dropped and local received packets. This does not include rejected received packets. This parameter is mandatory.
Pkts512to1023Octets	**Synopsis:** A 32-bit unsigned integer The number of received and transmitted packets with size of 512 to 1023 octets. This includes received and transmitted packets as well as dropped and local received packets. This does not include rejected received packets This parameter is mandatory.
Pkts1024to1518Octets	**Synopsis:** A 32-bit unsigned integer The number of received and transmitted packets with a size of 1024 to 1536 octets. This includes received and transmitted packets as well as dropped and local received packets. This does not include rejected received packets. This parameter is mandatory.

Section 8.1.6

Clearing Switched Ethernet Port Statistics

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.

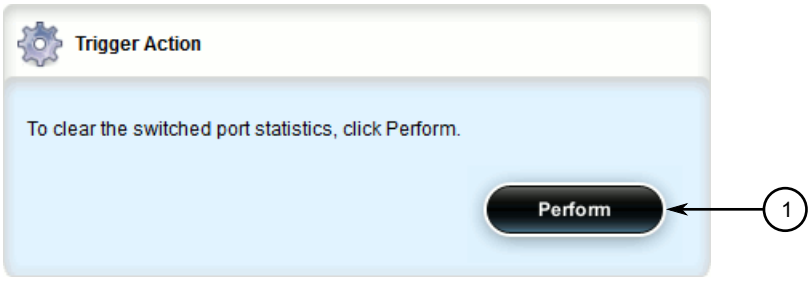


Figure 361: Trigger Action Form

1. Perform Button

3. Click **Perform**.

Section 8.1.7

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.

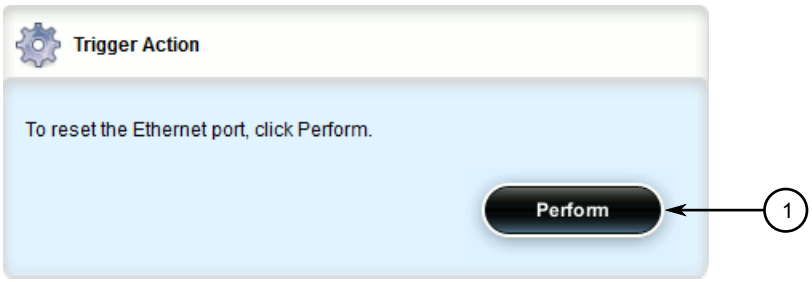


Figure 362: Trigger Action Form

1. Perform Button

3. Click **Perform**.

Section 8.1.8
Testing Switched Ethernet Port Cables

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

CONTENTS

Section 8.1.8.1
Running a Cable Diagnostic Test

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.

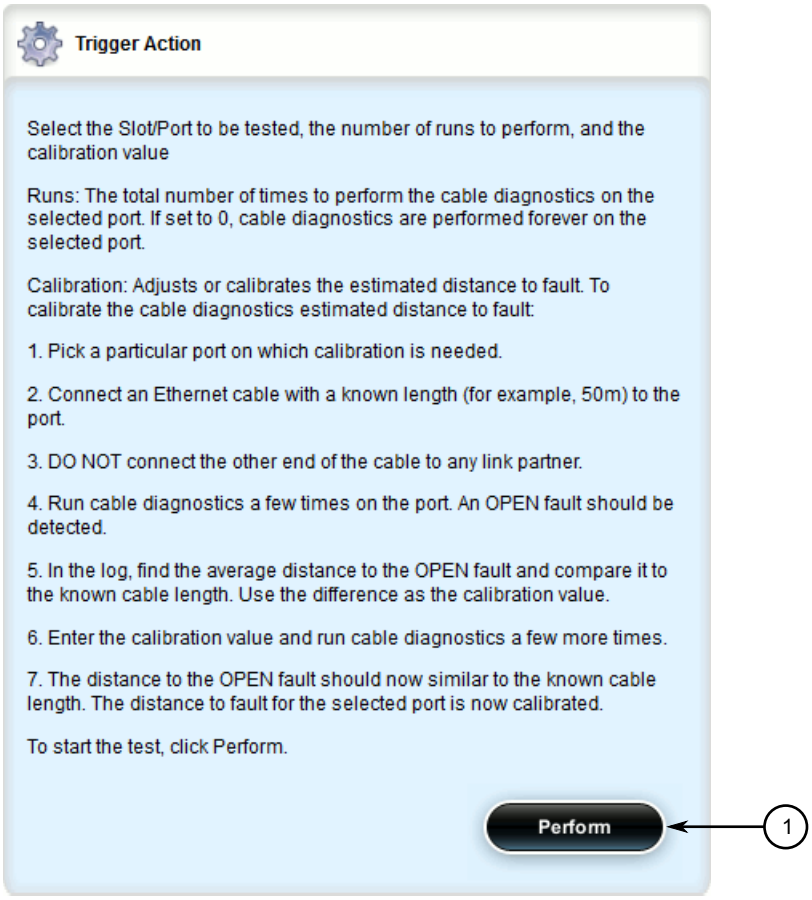


Figure 363: Trigger Action Form

1. Perform Button

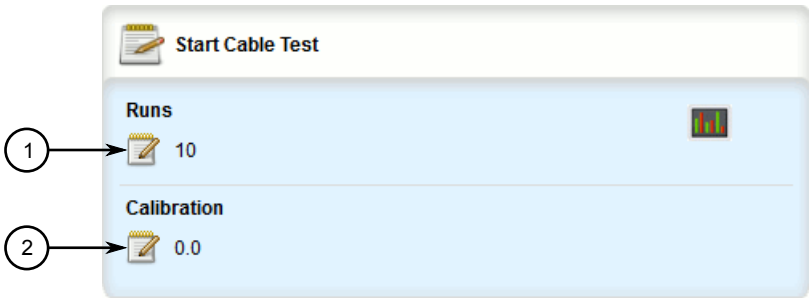


Figure 364: Start Cable Test Form

1. Runs Box **2.** Calibration Box

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

Parameter	Description
Runs	**Synopsis:** A 32-bit unsigned integer between 0 and 65535

Parameter	Description
	Default: 10
Calibration	**Synopsis:** A string **Default:** 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 8.1.8.2, "Viewing Cable Diagnostic Statistics".

Section 8.1.8.2
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.

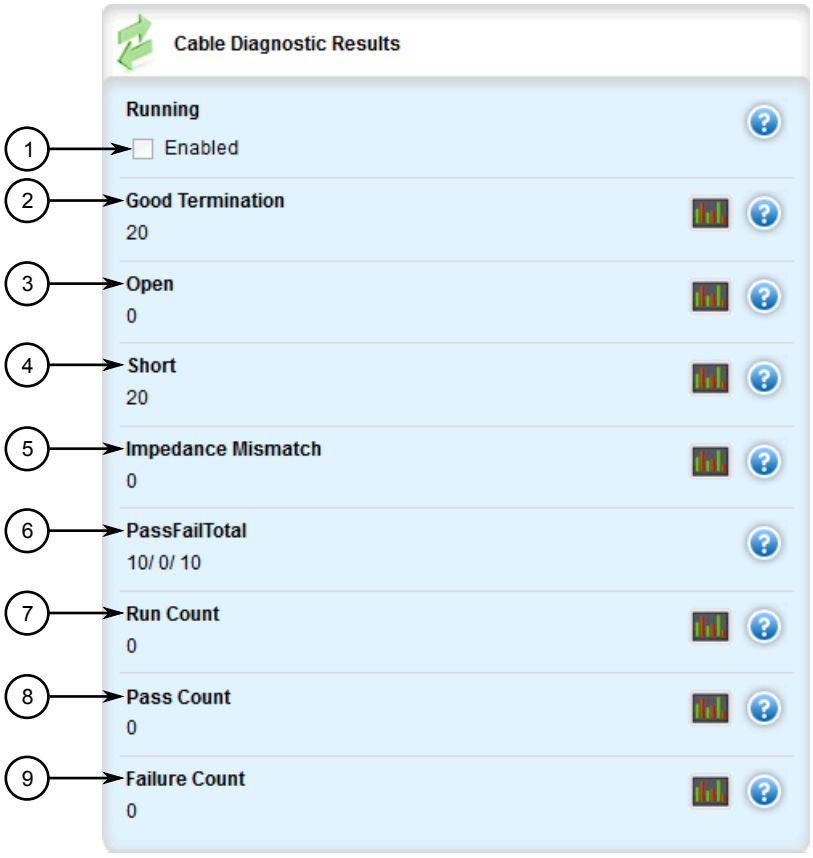


Figure 365: Cable Diagnostic Results Form

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	**Synopsis:** { true, false } Whether or not a cable test is currently running on this port This parameter is mandatory.
Good Termination	**Synopsis:** A 16-bit unsigned integer The number of times GOOD TERMINATION (no fault) is detected on the cable pairs of the selected port. This parameter is mandatory.
Open	**Synopsis:** A 16-bit unsigned integer The number of times OPEN is detected on the cable pairs of the selected port. This parameter is mandatory.
Short	**Synopsis:** A 16-bit unsigned integer The number of times SHORT is detected on the cable pairs of the selected port. This parameter is mandatory.
Impedance Mismatch	**Synopsis:** A 16-bit unsigned integer The number of times IMPEDANCE MISMATCH is detected on the cable pairs of the selected port. This parameter is mandatory.
PassFailTotal	**Synopsis:** A string 1 to 19 characters long This field summarizes the results of the cable diagnostics performed so far. • Pass : the number of times cable diagnostics were successfully completed on the selected port. • Fail : the number of times cable diagnostics failed to complete on the selected port. • Total : the total number of times cable diagnostics have been attempted on the selected port. This parameter is mandatory.
Run Count	**Synopsis:** A 16-bit unsigned integer Run Count : The total number of iterations This parameter is mandatory.
Pass Count	**Synopsis:** A 16-bit unsigned integer Pass Count This parameter is mandatory.
Failure Count	**Synopsis:** A 16-bit unsigned integer Failure Count This parameter is mandatory.

Section 8.1.8.3
Clearing Cable Diagnostic Statistics

The following describes how to clear the statistics collected when cable diagnostic tests are performed. All of the statistics or only those for a specific switchport can be cleared.

» Clearing All Cable Diagnostic Statistics

To clear the statistics, 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.

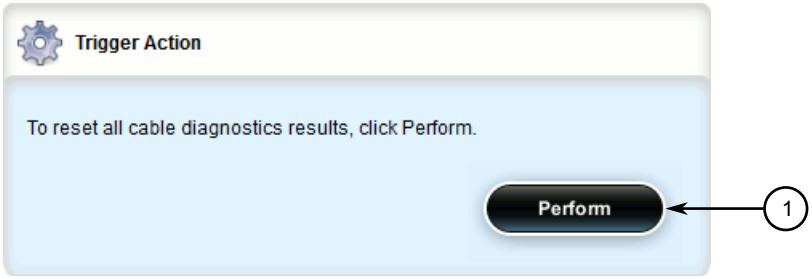


Figure 366: Trigger Action Form

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.

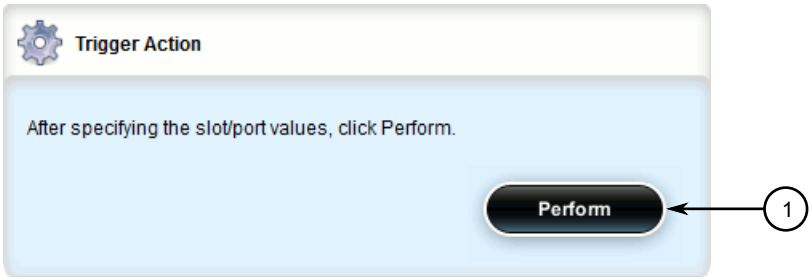


Figure 367: Trigger Action Form

1. Perform Button

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

Section 8.2
Managing Ethernet Trunk Interfaces

This section describes how to configure and manage Ethernet trunk interfaces.

CONTENTS

Section 8.2.1
Viewing a List of Ethernet Trunk Interfaces

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

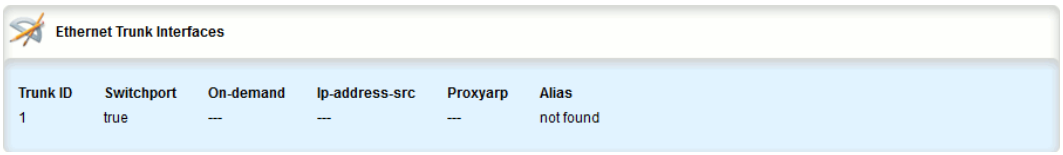


Figure 368: Ethernet Trunk Interfaces Table

If no Ethernet trunk interfaces have been configured, add trunks as needed. For more information, refer to Section 8.2.2, "Adding an Ethernet Trunk Interface".

Section 8.2.2
Adding an Ethernet Trunk Interface

To add an Ethernet trunk interface, do the following:

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

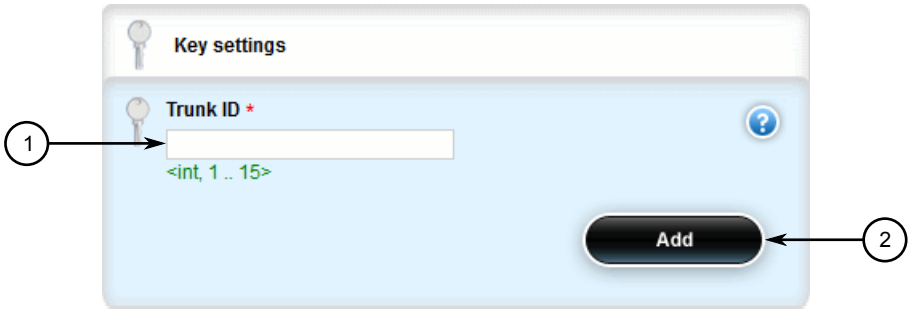


Figure 369: Key Settings Form

1. Trunk ID Box **2.** Add Button

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

Parameter	Description
Trunk ID	**Synopsis:** A 32-bit signed integer between 1 and 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.

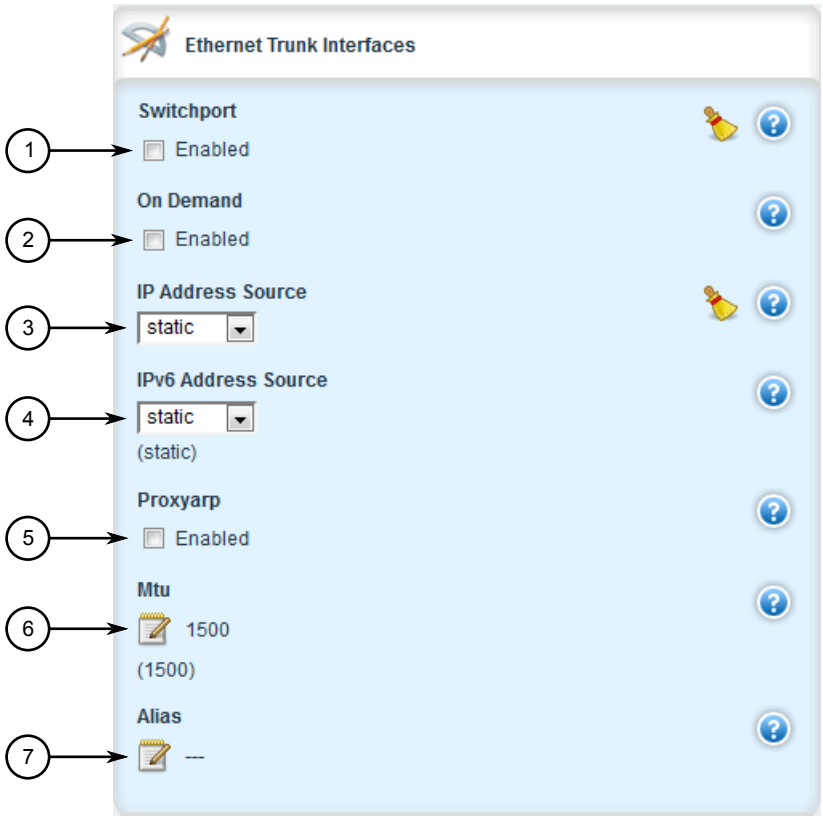


Figure 370: Ethernet Trunk Interfaces Form

1. Switchport Check Box **2.** On-Demand Check Box **3.** IP Address Source List **4.** IPv6 Address Source List **5.** Proxyarp Box **6.** Mtu Box **7.** Alias Box

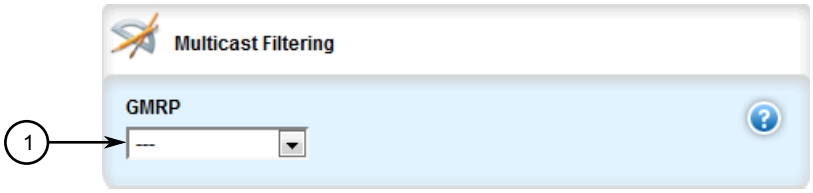


Figure 371: Multicast Filtering Form

1. GMRP List

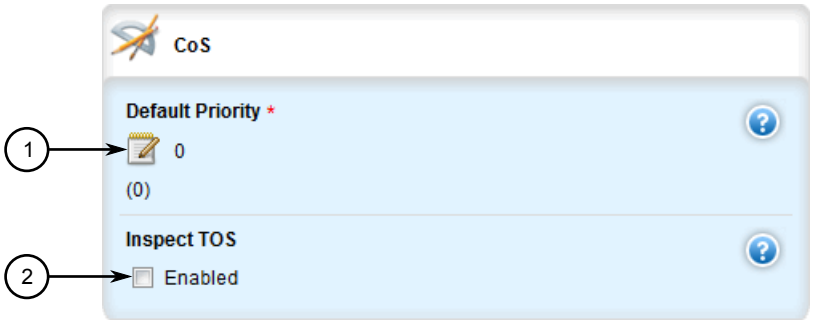


Figure 372: CoS Form

1. Default Priority Box **2.** Inspect TOS Check Box

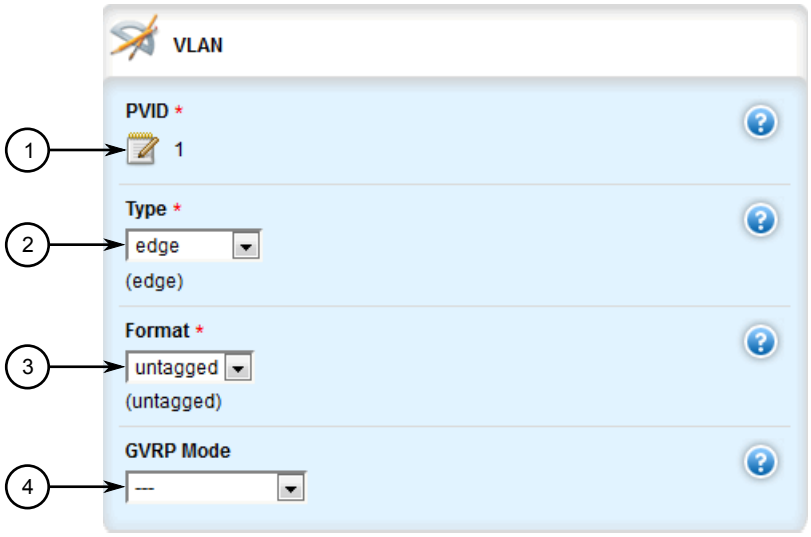


Figure 373: VLAN Form

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	**Synopsis:** { true, false } The physical port into either Switched mode or a dedicated Routing mode.
On Demand	Bring up this interface on-demand only
IP Address Source	**Synopsis:** { static, dynamic } Whether the IP address is static or dynamically assigned via DHCP or BOOTP. Option DYNAMIC is a common case of a dynamically assigned IP address. It switches between BOOTP and DHCP until it gets the response from the relevant server. This must be static for non-management interfaces.
IPv6 Address Source	**Synopsis:** { static, dynamic } **Default:** static

Parameter	Description
	Whether the IP address is static or dynamically assigned via DHCP. Option DYNAMIC is a common case of a dynamically assigned IP address. This must be static for non-management interfaces.
proxyarp	Enables/Disables whether the VLAN will respond to ARP requests for hosts other than itself
mtu	**Synopsis:** A 32-bit signed integer between 68 and 9216 **Default:** 1500 Maximum transmission unit (largest packet size allowed for this interface).
alias	**Synopsis:** 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	**Synopsis:** { advertise_only, learn_advertise } GMRP (GARP Multicast Registration Protocol) operation on the port. There are several GMRP operation modes: • DISABLED : the port is not capable of any GMRP processing. • ADVERTISE ONLY : the port will declare all MCAST addresses existing in the switch (configured or learned) but will not learn any MCAST addresses. • ADVERTISE and LEARN : the port will declare all MCAST Addresses existing in the switch (configured or learned) and can dynamically learn MCAST addresses.

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

Parameter	Description
Default Priority	**Synopsis:** A 32-bit signed integer between 0 and 7 **Default:** 0 The priority of frames received on this port that are not prioritized based on the frame's contents (e.g. priority field in the VLAN tag, DiffServ field in the IP header, prioritized MAC address).
Inspect ToS	Enables or disables parsing of the Type-Of-Service (TOS) field in the IP header of the received frames to determine what Class of Service they should be assigned. When TOS parsing is enabled the switch will use the Differentiated Services bits in the TOS field.

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

Parameter	Description
PVID	**Synopsis:** A 32-bit signed integer between 1 and 4094 The Port VLAN Identifier specifies the VLAN ID associated with untagged (and 802.1p priority tagged) frames received on this port. Frames tagged with a non-zero VLAN ID will always be associated with the VLAN ID retrieved from the frame tag.
Type	**Synopsis:** { edge, trunk, pvlanedge } **Default:** edge How the port determines its membership in VLANs. There are the following port types: • EDGE : the port is only a member of one VLAN (its native VLAN specified by the'PVID' parameter). • PVLAN Edge : the port does not forward traffic to other PVLAN edge ports within the same VLAN.

Parameter	Description
	• TRUNK : the port is automatically a member of all configured VLANs. Frames transmitted out of the port on all VLANs except the port's native VLAN will be always tagged. It can also be configured to use GVRP for automatic VLANconfiguration.
Format	**Synopsis:** { untagged, tagged } **Default:** untagged Whether frames transmitted out of the port on its native VLAN(specified by the 'PVID' parameter) will be tagged or untagged.
GVRP Mode	**Synopsis:** { advertise_only, learn_advertise } GVRP (Generic VLAN Registration Protocol) operation on the port. There are several GVRP operation modes: • DISABLED : the port is not capable of any GVRP processing. • ADVERTISE ONLY : the port will declare all VLANs existing in the switch (configured or learned) but will not learn any VLANs. • ADVERTISE and LEARN : the port will declare all VLANs existing in the switch (configured or learned) and can dynamically learn VLANs.

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 8.2.3

Deleting an Ethernet Trunk Interface

To delete an Ethernet trunk interface, do the following:

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

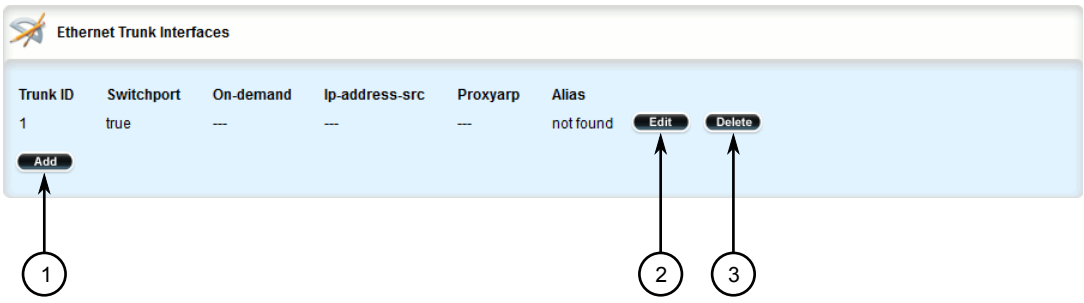


Figure 374: Ethernet Trunk Interfaces Table

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

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 8.2.4

Managing Ethernet Trunk Ports

This section describes how to manage Ethernet trunk port assignments.

CONTENTS

Section 8.2.4.1

Viewing a List of Ethernet Trunk Ports

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.

Figure 375: Trunk Ports Table

If no Ethernet trunk ports have been configured, add ports as needed. For more information, refer to Section 8.2.4.2, “Adding an Ethernet Trunk Port”.

Section 8.2.4.2

Adding an Ethernet Trunk Port

To add an Ethernet trunk port, do the following:

1. 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.

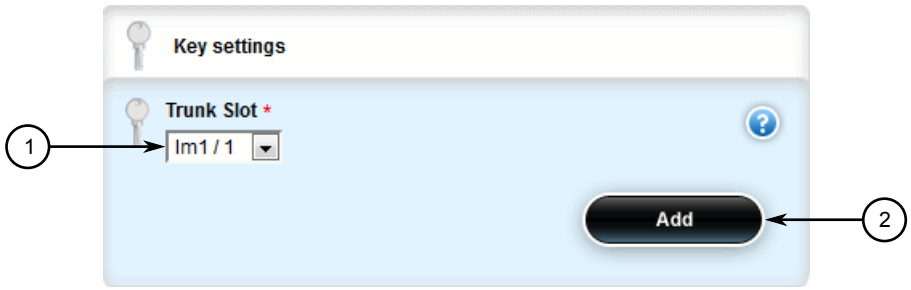


Figure 376: Key Settings Form

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	**Synopsis:** A string The name of the module location provided on the silkscreen across the top of the device.
Trunk Port	**Synopsis:** A string 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 8.2.4.3
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.

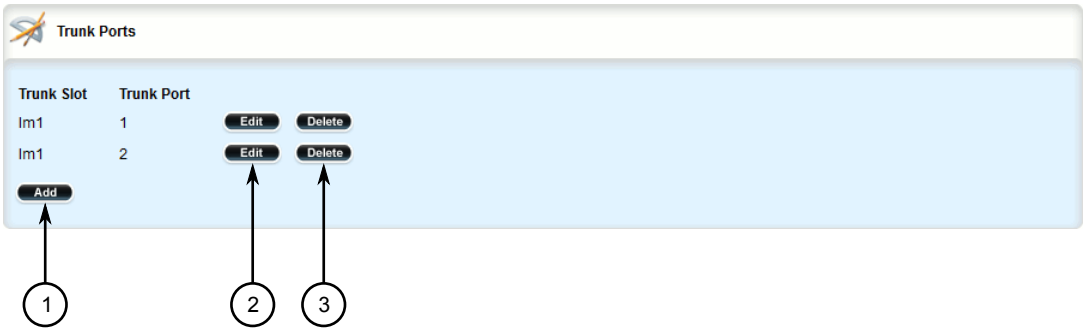


Figure 377: Trunk Ports Table

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 8.3

Managing MAC Addresses

As part of the Layer 2 functionality, RUGGEDCOM ROX II maintains a Media Access Control (MAC) address table, a list of unique MAC addresses for network interfaces that can communicate with the device at the data link layer. The MAC address table can be populated manually by defining specific MAC addresses and/or dynamically. When populated dynamically, RUGGEDCOM ROX II automatically adds the MAC addresses of network interfaces it detects on the network. It will also remove those addresses if the address ages out or there is a link failure.

CONTENTS

Section 8.3.1

Viewing a Dynamic List of MAC Addresses

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.

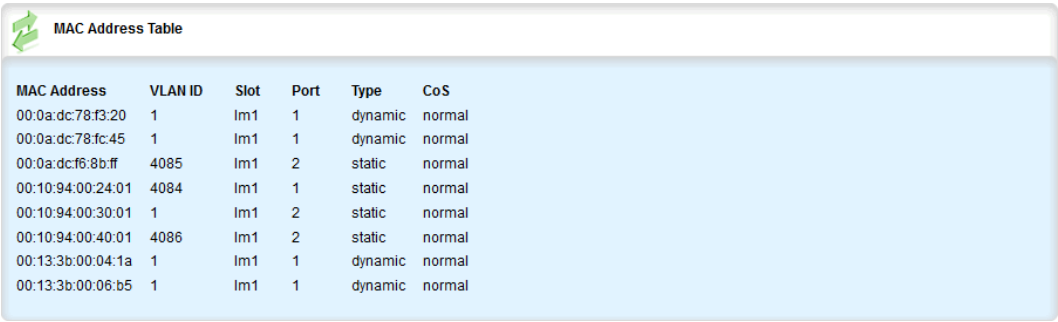


Figure 378: MAC Address Table

This table provides the following information:

Parameter	Description
MAC Address	**Synopsis:** A string 17 characters long The MAC address learned by the switch.
VLAN ID	**Synopsis:** A 32-bit signed integer The VLAN identifier of the VLAN upon which the MAC address operates. This parameter is mandatory.
Slot	**Synopsis:** { sm, lm1, lm2, lm3, lm4, lm5, lm6, swport, eth, serport, celport, wlanport } The slot containing the module including the port. This parameter is mandatory.
Port	**Synopsis:** A 32-bit signed integer between 1 and 16 The port on which the MAC address has been learned. This parameter is mandatory.
Type	**Synopsis:** { static, dynamic } How the MAC address has been learned by the switch: • STATIC: The address has been learned as a result of static MAC address table configuration or some other management activity and cannot be automatically unlearned or relearned by the switch. • DYNAMIC: The address has been automatically learned by the switch and can be automatically unlearned. This parameter is mandatory.
CoS	**Synopsis:** { N/A, normal, medium, high, crit } The Class Of Service (CoS) that is assigned to frames carrying this address as a source or destination address. This parameter is mandatory.

If a MAC address is not listed, do the following:

- Configure the MAC address learning options to dynamically detect the MAC addresses of other devices on the network. For more information, refer to Section 8.3.3, "Configuring MAC Address Learning Options".
- Configure the address on the device as a static MAC address. For more information, refer to Section 8.3.4.2, "Adding a Static MAC Address".

Section 8.3.2

Purging the Dynamic MAC Address List

To purge the dynamic MAC address list of all entries, do the following:

1. Navigate to ***switch » mac-tables*** and click **purge-mac-table** in the menu. The **Trigger Action** form appears.

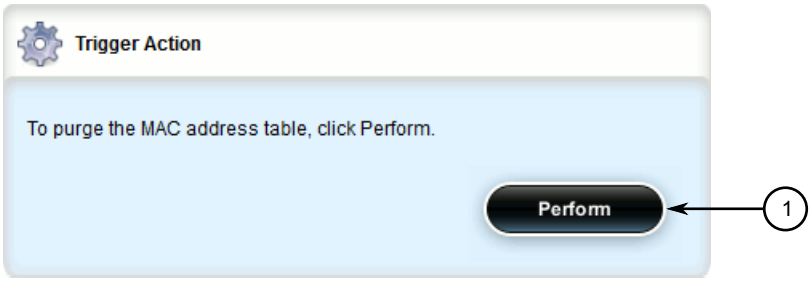


Figure 379: Trigger Action Form

1. Perform Button

2. Click the **Perform** button. Once the table is purged, the **Success!** and **Purge MAC Table Results** forms appear.

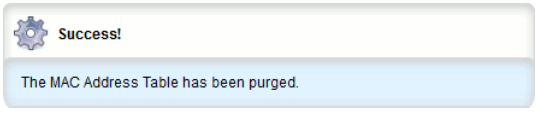


Figure 380: Success! Form

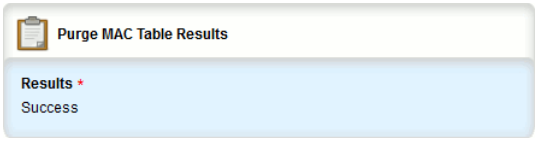


Figure 381: Purge MAC Table Results Form

Section 8.3.3

Configuring MAC Address Learning Options

The MAC address learning options control how and when MAC addresses are removed automatically from the MAC address table. Individual addresses are removed when the aging timer is exceeded. Addresses can also be removed when a link failure or topology change occurs.

To configure the MAC address learning options, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to ***switch » mac-tables***. The **MAC Tables** form appears.

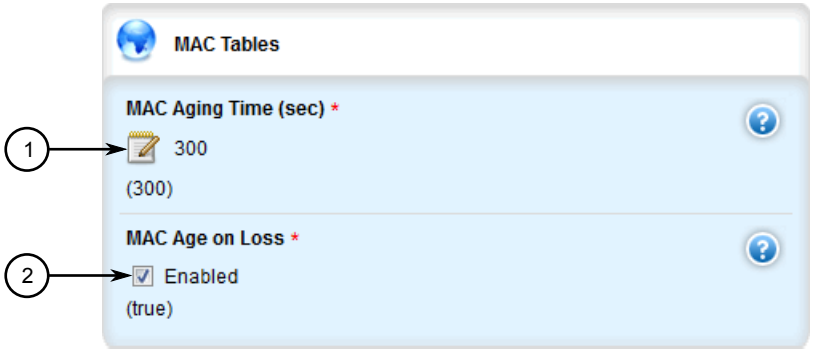


Figure 382: MAC Tables

1. MAC Aging Time Box **2.** MAC Age on Loss Box

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

Parameter	Description
MAC Aging Time (sec)	**Synopsis:** A 32-bit signed integer between 15 and 800 **Default:** 300 The time a learned MAC address is held before being aged out.
MAC Age on Loss	**Synopsis:** { true, false } **Default:** true When link failure (and potentially a topology change) occurs, the switch may have some MAC addresses previously learned on the failed port. As long as those addresses are not aged-out, the switch will still be forwarding traffic to that port, thus preventing that traffic from reaching its destination via the new network topology. This parameter allows the aging-out of all MAC addresses learned on a failed port immediately upon link failure detection.

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 8.3.4

Managing Static MAC Addresses

Static MAC addresses must be configured when destination devices are only able to receive frames, not transmit them. They may also need to be configured if port security (if supported) must be enforced.

Prioritized MAC addresses are configured when traffic to or from a specific device on a LAN segment is to be assigned a higher CoS priority than other devices on that LAN segment.

CONTENTS

Section 8.3.4.1
Viewing a List of Static MAC Addresses

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.

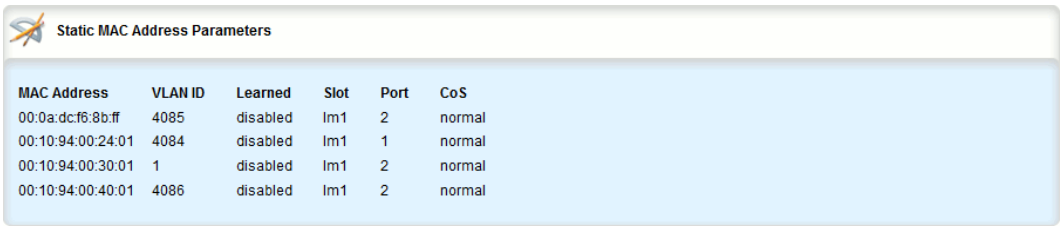


Figure 383: Static MAC Address Parameters Table

If no static MAC addresses have been configured, add addreses as needed. For more information, refer to Section 8.3.4.2, "Adding a Static MAC Address".

Section 8.3.4.2
Adding a Static MAC Address

To add a static MAC address, do the following:

1. 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.

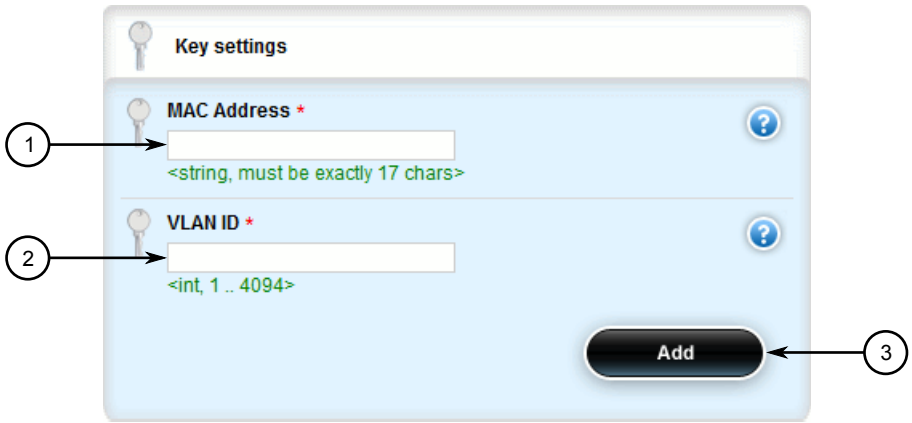


Figure 384: Key Settings Form

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	**Synopsis:** A string 17 characters long A unicast MAC address that is to be statically configured. It can have up to 6 '*' wildcard characters continuously applied from the right.
VLAN ID	**Synopsis:** A 32-bit signed 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.

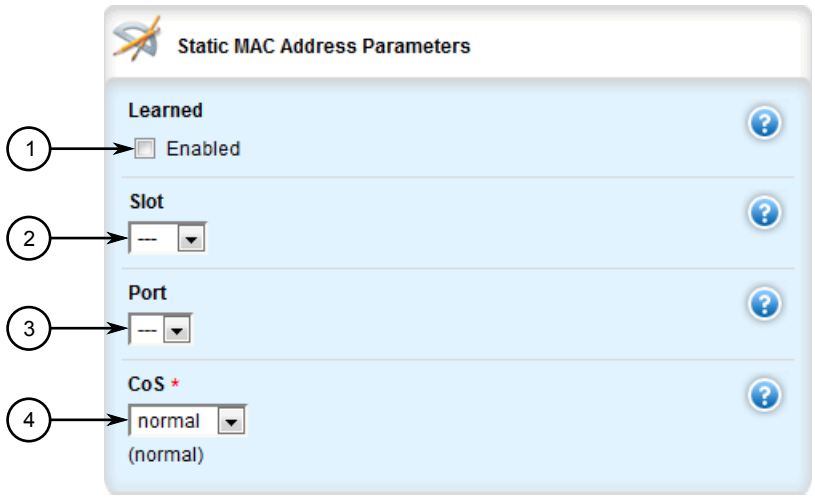


Figure 385: Static MAC Address Parameters Form

1. Learned Check Box **2.** Slot List **3.** Port List **4.** CoS List

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

Parameter	Description
learned	If set, the system will auto-learn the port upon which the device with this address is located.
Slot	**Synopsis:** A string The name of the module location provided on the silkscreen across the top of the device.
Port	**Synopsis:** A string The selected ports on the module installed in the indicated slot.
CoS	**Synopsis:** { N/A, normal, medium, high, crit } **Default:** normal The priority of traffic for a specified 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 8.3.4.3
Deleting a Static MAC Address

To delete 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***. The **Static MAC Address Parameters** table appears.

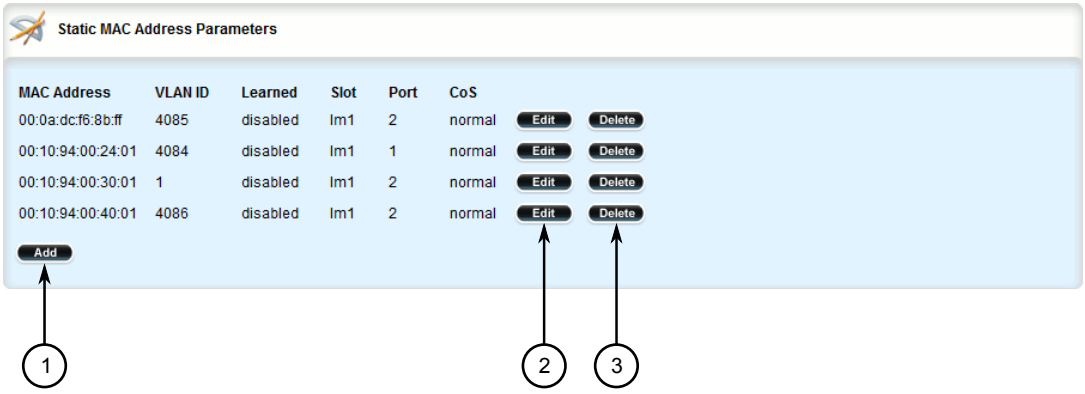


Figure 386: Static MAC Address Parameters Table

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

3. Click **Delete** next to the chosen static MAC 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 8.4
Managing Multicast Filtering

Multicast traffic can be filtered using either static multicast groups, IGMP (Internet Group Management Protocol) snooping, or GMRP (GARP Multicast Registration Protocol).

CONTENTS

Section 8.4.1

Multicast Filtering Concepts

This section describes some of the concepts important to the implementation of multicast filtering in RUGGEDCOM ROX II.

CONTENTS

Section 8.4.1.1

IGMP

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.

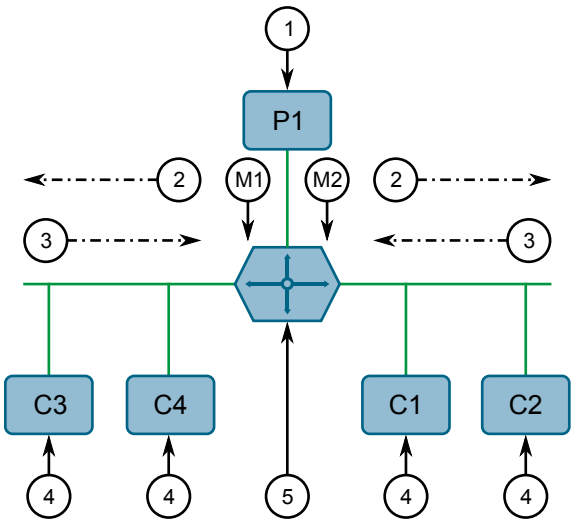


Figure 387: Example – IGMP In Operation

1. Producer **2.** Membership Queries **3.** Membership Reports **4.** Host **5.** Mulicast Router

One *producer* IP host (P1) is generating two IP multicast streams, M1 and M2. There are four potential *consumers* of these streams, C1 through C4. The multicast router discovers which host wishes to subscribe to which stream by sending general membership queries to each segment.

In this example, the general membership query sent to the C1-C2 segment is answered by a membership report (or *join*) indicating the desire to subscribe to stream M2. The router will forward the M2 stream to the C1-C2 segment. In a similar fashion, the router discovers that it must forward stream M1 to segment C3-C4.

A *consumer* may join any number of multicast groups, issuing a membership report for each group. When a host issues a membership report, other hosts on the same network segment that also require membership to the same group suppress their own requests, since they would be redundant. In this way, the IGMP protocol guarantees the segment will issue only one membership report for each group.

The router periodically queries each of its segments in order to determine whether at least one consumer still subscribes to a given stream. If it receives no responses within a given time period (usually two query intervals), the router will prune the multicast stream from the given segment.

A more common method of pruning occurs when consumers wishing to unsubscribe issue an IGMP *leave group* message. The router will immediately issue a group-specific membership query to determine whether there are any remaining subscribers of that group on the segment. After the last consumer of a group has unsubscribed, the router will prune the multicast stream from the given segment.

Switch IGMP Operation

The IGMP Snooping feature provides a means for switches to snoop (i.e. watch) the operation of routers, respond with joins/leaves on the behalf of consumer ports, and prune multicast streams accordingly. There are two modes of IGMP the switch can be configured to assume: active and passive.

- **Active Mode**
  IGMP supports a *routerless* mode of operation.

  When such a switch is used without a multicast router, it is able to function as if it is a multicast router sending IGMP general queries.
- **Passive Mode**
  When such a switch is used in a network with a multicast router, it can be configured to run Passive IGMP. This mode prevents the switch from sending the queries that can confuse the router causing it to stop issuing IGMP queries.

NOTE
A switch running in passive mode requires the presence of a multicast router or it will be unable to forward multicast streams at all if no multicast routers are present.

NOTE
Without a multicast router, at least one IGMP Snooping switch must be in active mode to make IGMP functional.

IGMP Snooping Rules

IGMP Snooping adheres to the following rules:

- When a multicast source starts multicasting, the traffic stream will be immediately blocked on segments from which joins have not been received.
- Unless configured otherwise, the switch will forward all multicast traffic to the ports where multicast routers are attached.

- Packets with a destination IP multicast address in the 224.0.0.X range that are not IGMP are always forwarded to all ports. This behavior is based on the fact that many systems do not send membership reports for IP multicast addresses in this range while still listening to such packets.
- The switch implements *proxy-reporting* (i.e. membership reports received from downstream are summarized and used by the switch to issue its own reports).
- The switch will only send IGMP membership reports out of those ports where multicast routers are attached, as sending membership reports to hosts could result in unintentionally preventing a host from joining a specific group.
- Multicast routers use IGMP to elect a master router known as the *querier*. The *querier* is the router with the lowest IP address. All other routers become non-queriers, participating only in forwarding multicast traffic. Switches running in active mode participate in the querier election the same as multicast routers.
- When the querier election process is complete, the switch simply relays IGMP queries received from the querier.
- When sending IGMP packets, the switch uses its own IP address, if it has one, for the VLAN on which packets are sent, or an address of 0.0.0.0, if it does not have an assigned IP address.

NOTE
IGMP Snooping switches perform multicast pruning using a multicast frame's destination MAC multicast address, which depends on the group IP multicast address. IP address W.X.Y.Z corresponds to MAC address 01-00-5E-XX-YY-ZZ where XX is the lower 7 bits of X, and YY and ZZ are simply Y and Z coded in hexadecimal.

One can note that IP multicast addresses, such as 224.1.1.1 and 225.1.1.1, will both map onto the same MAC address 01-00-5E-01-01-01. This is a problem for which the IETF Network Working Group currently has offered no solution. Users are advised to be aware of and avoid this problem.

IGMP and RSTP

An RSTP change of topology can render the routes selected to carry multicast traffic as incorrect. This results in lost multicast traffic.

If RSTP detects a change in the network topology, IGMP will take some actions to avoid the loss of multicast connectivity and reduce network convergence time:

- The switch will immediately issue IGMP queries (if in IGMP Active mode) to obtain potential new group membership information.
- The switch can be configured to flood multicast streams temporarily out of all ports that are not RSTP Edge Ports.

Combined Router and Switch IGMP Operation

The following example illustrates the challenges faced with multiple routers, VLAN support and switching.

Producer P1 resides on VLAN 2 while P2 resides on VLAN 3. Consumer C1 resides on both VLANs whereas C2 and C3 reside on VLANs 3 and 2, respectively. Router 2 resides on VLAN 2, presumably to forward multicast traffic to a remote network or act as a source of multicast traffic itself.

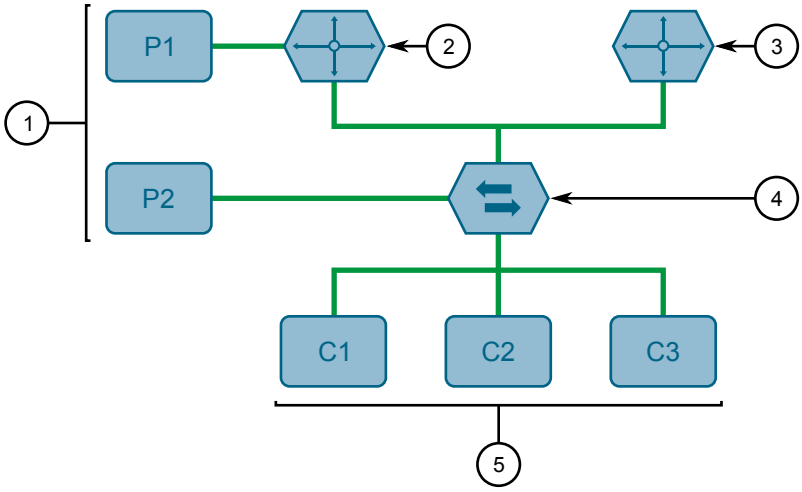


Figure 388: Example – Combined Router and Switch IGMP In Operation

1. Producer **2.** Multicast Router 1 **3.** Multicast Router 2 **4.** Switch **5.** Host

In this example:

- P1, Router 1, Router 2 and C3 are on VLAN 2
- P2 and C2 are on VLAN 3
- C1 is on both VLAN 2 and 3

Assuming that router 1 is the querier for VLAN 2 and router 2 is simply a non-querier, the switch will periodically receive queries from router 1 and maintain the information concerning which port links to the multicast router. However, the switch port that links to router 2 must be manually configured as a *router port*. Otherwise, the switch will send neither multicast streams nor joins/leaves to router 2.

Note that VLAN 3 does not have an external multicast router. The switch should be configured to operate in its *routerless* mode and issue general membership queries as if it is the router.

- **Processing Joins**
  If host C1 wants to subscribe to the multicast streams for both P1 and P2, it will generate two membership reports. The membership report from C1 on VLAN 2 will cause the switch to immediately initiate its own membership report to multicast router 1 (and to issue its own membership report as a response to queries).

  The membership report from host C1 for VLAN 3 will cause the switch to immediately begin forwarding multicast traffic from producer P2 to host C2.
- **Processing Leaves**
  When host C1 decides to leave a multicast group, it will issue a leave request to the switch. The switch will poll the port to determine if host C1 is the last member of the group on that port. If host C1 is the last (or only) member, the group will immediately be pruned from the port.

  Should host C1 leave the multicast group without issuing a leave group message and then fail to respond to a general membership query, the switch will stop forwarding traffic after two queries.

  When the last port in a multicast group leaves the group (or is aged-out), the switch will issue an IGMP leave report to the router.

Section 8.4.1.2

GMRP (GARP Multicast Registration Protocol)

The GARP Multicast Registration Protocol (GMRP) is an application of the Generic Attribute Registration Protocol (GARP) that provides a Layer 2 mechanism for managing multicast group memberships in a bridged Layer 2 network. It allows Ethernet switches and end stations to register and unregister membership in multicast groups with other switches on a LAN, and for that information to be disseminated to all switches in the LAN that support Extended Filtering Services.

GMRP is an industry-standard protocol first defined in IEEE 802.1D-1998 and extended in IEEE 802.1Q-2005. GARP was defined in IEEE 802.1D-1998 and updated in 802.1D-2004.

NOTE
GMRP provides similar functionality at Layer 2 to what IGMP provides at Layer 3.

Joining a Multicast Group

In order to join a multicast group, an end station transmits a GMRP *join* message. The switch that receives the *join* message adds the port through which the message was received to the multicast group specified in the message. It then propagates the *join* message to all other hosts in the VLAN, one of which is expected to be the multicast source.

When a switch transmits GMRP updates (from GMRP-enabled ports), all of the multicast groups known to the switch, whether configured manually or learned dynamically through GMRP, are advertised to the rest of network.

As long as one host on the Layer 2 network has registered for a given multicast group, traffic from the corresponding multicast source will be carried on the network. Traffic multicast by the source is only forwarded by each switch in the network to those ports from which it has received join messages for the multicast group.

Leaving a Multicast Group

Periodically, the switch sends GMRP queries in the form of a *leave all* message. If a host (either a switch or an end station) wishes to remain in a multicast group, it reasserts its group membership by responding with an appropriate *join* request. Otherwise, it can either respond with a *leave* message or simply not respond at all. If the switch receives a *leave* message or receives no response from the host for a timeout period, the switch removes the host from the multicast group.

Notes About GMRP

Since GMRP is an application of GARP, transactions take place using the GARP protocol. GMRP defines the following two Attribute Types:

- The Group Attribute Type, used to identify the values of group MAC addresses
- The Service Requirement Attribute Type, used to identify service requirements for the group

Service Requirement Attributes are used to change the receiving port's multicast filtering behavior to one of the following:

- Forward All Multicast group traffic in the VLAN, or
- Forward All Unknown Traffic (Multicast Groups) for which there are no members registered in the device in a VLAN

If GMRP is disabled on the RUGGEDCOM RX1500, GMRP packets received will be forwarded like any other traffic. Otherwise, GMRP packets will be processed by the RUGGEDCOM RX1500, and not forwarded.

Example: Establishing Membership with GMRP

The following example illustrates how a network of hosts and switches can dynamically join two multicast groups using GMRP.

In this scenario, there are two multicast sources, S1 and S2, multicasting to Multicast Groups 1 and 2, respectively. A network of five switches, including one core switch (B), connects the sources to two hosts, H1 and H2, which receive the multicast streams from S1 and S2, respectively.

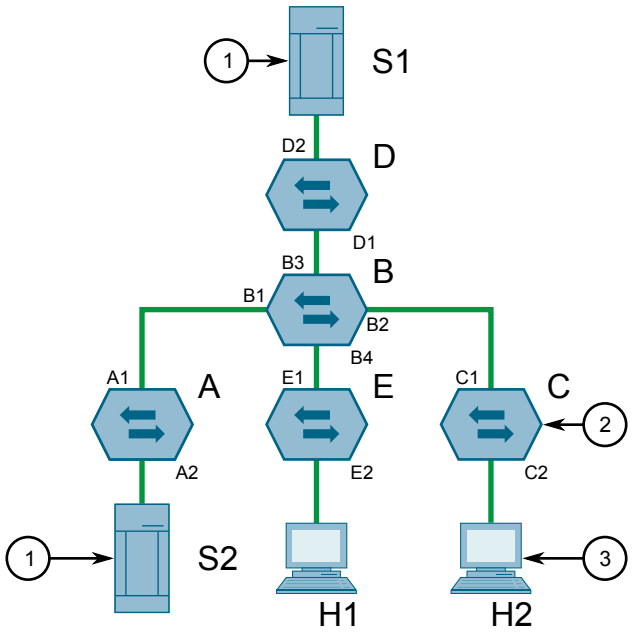


Figure 389: Example – Establishing Membership with GMRP

1. Multicast Source **2.** Switch **3.** Multicast Host

The hosts and switches establish membership with the Multicast Group 1 and 2 as follows:

1. Host H1 is GMRP unaware, but needs to see traffic for Multicast Group 1. Therefore, Port E2 on Switch E is statically configured to forward traffic for Multicast Group 1.
2. Switch E advertises membership in Multicast Group 1 to the network through Port E1, making Port B4 on Switch B a member of Multicast Group 1.
3. Switch B propagates the *join* message, causing Ports A1, C1 and D1 to become members of Multicast Group 1.
4. Host H2 is GMRP-aware and sends a *join* request for Multicast Group 2 to Port C2, which thereby becomes a member of Multicast Group 2.
5. Switch C propagates the *join* message, causing Ports A1, B2, D1 and E1 to become members of Multicast Group 2.

Once GMRP-based registration has propagated through the network, multicast traffic from S1 and S2 can reach its destination as follows:

- Source S1 transmits multicast traffic to Port D2 which is forwarded via Port D1, which has previously become a member of Multicast Group 1.
- Switch B forwards the Group 1 multicast via Port B4 towards Switch E.
- Switch E forwards the Group 1 multicast via Port E2, which has been statically configured for membership in Multicast Group 1.

- Host H1, connected to Port E2, thus receives the Group 1 multicast.
- Source S2 transmits multicast traffic to Port A2, which is then forwarded via port A1, which has previously become a member of Multicast Group 2.
- Switch B forwards the Group 2 multicast via Port B2 towards Switch C.
- Switch C forwards the Group 2 multicast via Port C2, which has previously become a member of Group 2.
- Ultimately, Host H2, connected to Port C2, receives the Group 2 multicast.

Section 8.4.2
Enabling and Configuring GMRP

To enable and configure GMRP (GARP Multicast Registration Protocol), do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to ***switch » mcast-filtering***. The **GMRP** form appears.

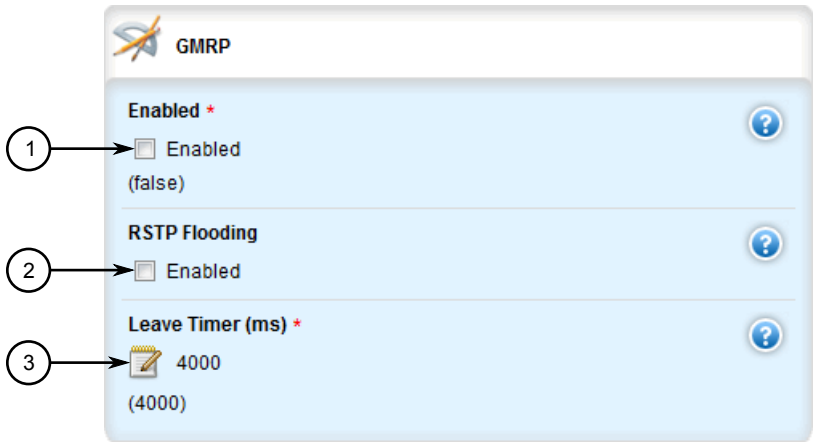


Figure 390: GMRP Form

1. Enabled Check Box **2.** RSTP Flooding Check Box **3.** Leave Timer Box

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

Parameter	Description
Enabled	**Synopsis:** { true, false } **Default:** false GMRP Enable
RSTP Flooding	Determines whether or not multicast streams will be flooded out of all Rapid Spanning Tree Protocol (RSTP) non-edge ports upon detection of a topology change. Such flooding is desirable, if multicast stream delivery must be guaranteed without interruption.
Leave Timer (ms)	**Synopsis:** A 32-bit signed integer between 600 and 300000 **Default:** 4000 The time in milliseconds to wait after issuing Leave or LeaveAll before removing registered multicast groups. If Join messages for specific addresses are received before this timer expires, the addresses will be kept registered.

4. Enable GMRP on one or more switched Ethernet ports. For more information, refer to Section 8.1.2, "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 8.4.3
Managing IGMP Snooping

This sections describes how to configure IGMP snooping and manage ports monitored by the service.

CONTENTS

Section 8.4.3.1
Configuring IGMP Snooping

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.

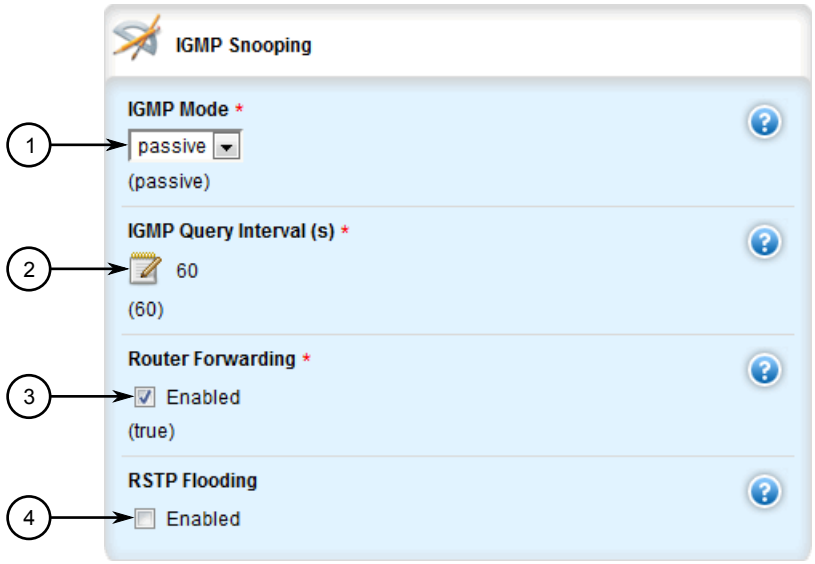


Figure 391: IGMP Snooping Form

1. IGMP Mode List **2.** IGMP Query Interval Box **3.** Router Forwarding Check Box **4.** RSTP Flooding Check Box

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

Parameter	Description
IGMP Mode	**Synopsis:** { active, passive } **Default:** passive Specifies the IGMP mode: • PASSIVE : The switch passively snoops IGMP traffic and never sends IGMP queries. • ACTIVE : The switch generates IGMP queries, if no queries from a better candidate for the querier are detected for a while.
IGMP Query Interval (s)	**Synopsis:** A 32-bit signed integer between 10 and 3600 **Default:** 60 The time interval between IGMP queries generated by the switch. NOTE: This parameter also affects the Group Membership Interval (i.e. the group subscriber aging time), therefore, it takes effect even in PASSIVE mode.
Router Forwarding	**Synopsis:** { true, false } **Default:** true Whether or not multicast streams will always be forwarded to multicast routers.
RSTP Flooding	Whether or not multicast streams will be flooded out of all Rapid Spanning Tree Protocol (RSTP) non-edge ports upon detection of a topology change. Such flooding is desirable, if multicast stream delivery must be guaranteed without interruption.

4. Assign one or more ports for IGMP to use when sending Membership Reports. For more information, refer to Section 8.4.3.3, "Adding a Router Port".
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 8.4.3.2
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.

Figure 392: Router Ports Table

If no router ports have been configured, add ports as needed. For more information, refer to Section 8.4.3.3, "Adding a Router Port".

Section 8.4.3.3
Adding a Router Port

To add a router port for IGMP snooping, do the following:

1. 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.

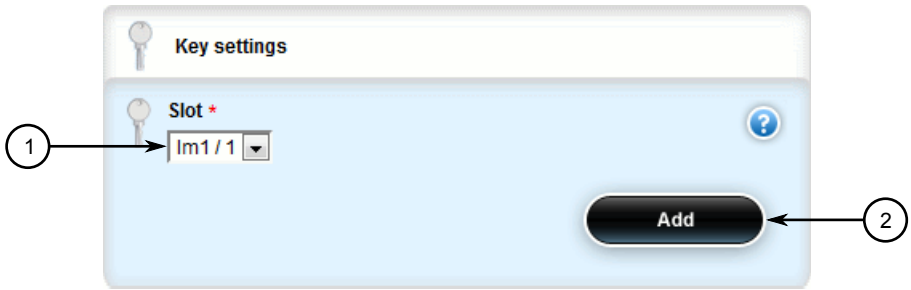


Figure 393: Key Settings Form

1. Slot Box **2.** Add Button

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

Parameter	Description
Slot	**Synopsis:** A string The name of the module location provided on the silkscreen across the top of the device.
Port	**Synopsis:** A string The selected ports on the module installed in the indicated slot.

4. Click **Add** to add the 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 8.4.3.4
Deleting a Router Port

To delete 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***. The **Router Ports** table appears.

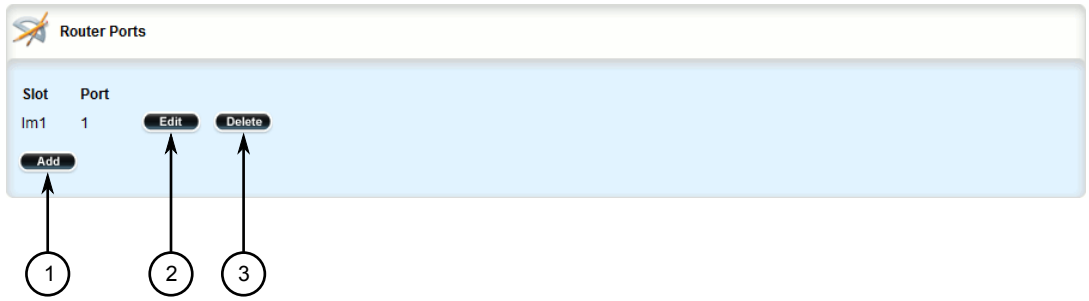


Figure 394: Router Ports Table

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

3. Click **Delete** next to the chosen router 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 8.4.4
Managing the Static Multicast Group Table

This section describes how to manage entries in the Static Multicast Group table.

CONTENTS

Section 8.4.4.1
Viewing a List of Static Multicast Group Entries

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.

Figure 395: Static Multicast Summary Table

If no entries have been configured, add entries as needed. For more information, refer to Section 8.4.4.2, "Adding a Static Multicast Group Entry".

Section 8.4.4.2
Adding a Static Multicast Group Entry

To list a static multicast group from another device in the Static Multicast Summary table, do the following:

1. 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.

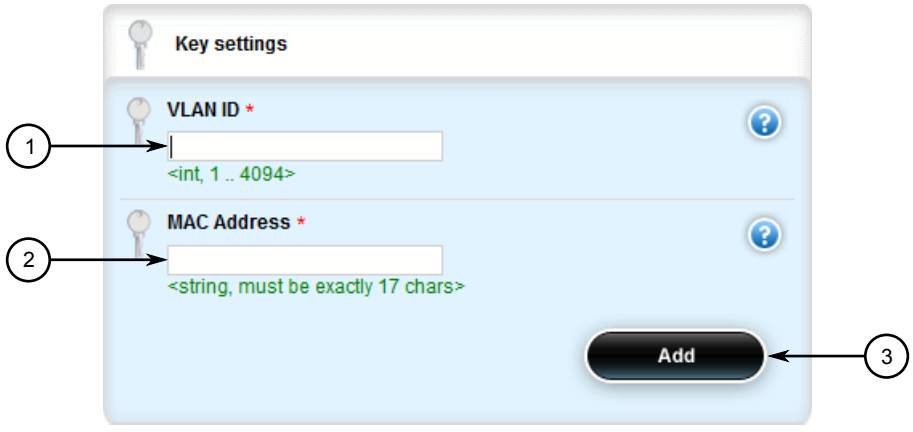


Figure 396: Key Settings Form

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	**Synopsis:** A 32-bit signed integer between 1 and 4094 The VLAN Identifier of the VLAN upon which the multicast group operates.
MAC Address	**Synopsis:** A string 17 characters long The multicast group MAC address in the form 01:xx:xx:xx:xx:xx.
CoS	**Synopsis:** { N/A, normal, medium, high, crit } **Default:** normal The Class Of Service that is assigned to the multicast group frames.

4. Add one or more egress ports. For more information, refer to Section 8.4.5.2, "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 8.4.4.3
Deleting a Static Multicast Group Entry

To delete a static multicast group from the Static Multicast Summary table, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to ***switch » mcast-filtering » static-mcast-table***. The **Static Multicast Summary** table appears.

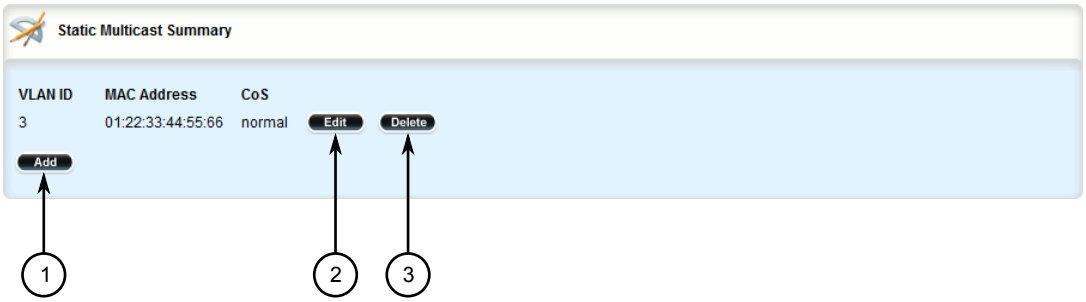


Figure 397: Static Multicast Summary Table

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

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 8.4.5

Managing Egress Ports for Multicast Groups

This section describes how to configure and manage egress ports for a multicast group.

CONTENTS

Section 8.4.5.1

Viewing a List of Egress Ports

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.

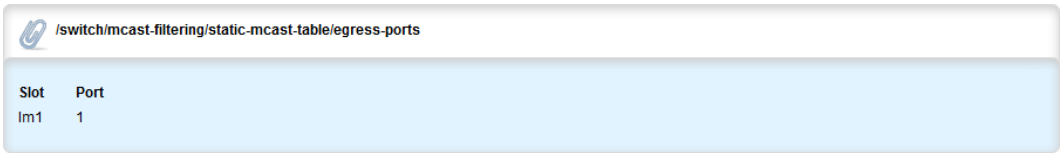


Figure 398: Egress Ports Table

If no egress ports have been configured, add egress ports as needed. For more information, refer to Section 8.4.5.2, "Adding an Egress Port".

Section 8.4.5.2

Adding an Egress Port

To add an egress port to a static multicast group defined in the Static Multicast Group Summary table, do the following:

1. 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.

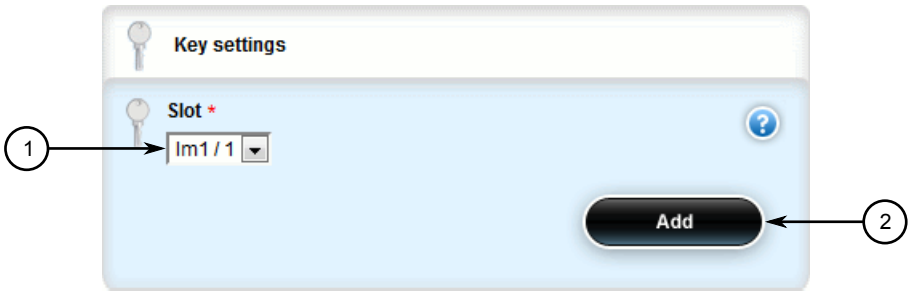


Figure 399: Key Settings Form

1. Slot List **2.** Add Button

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

Parameter	Description
Slot	**Synopsis:** A string The name of the module location provided on the silkscreen across the top of the device.
Port	**Synopsis:** A string 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 8.4.5.3

Deleting an Egress Port

To delete an egress port for a static multicast group defined in the Static Multicast Group Summary table, do the following:

1. 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.

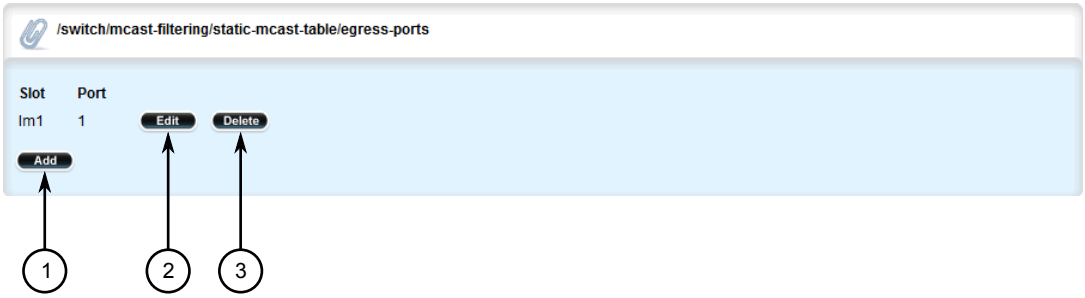


Figure 400: Egress Ports Table

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 8.4.6

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.

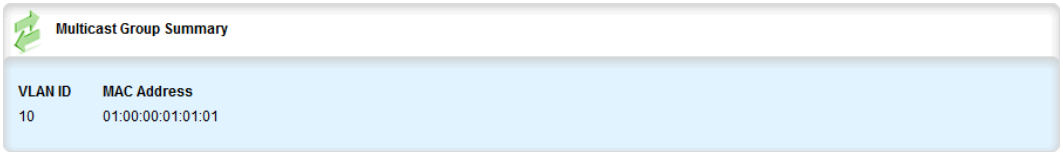


Figure 401: Multicast Group Summary Table

This table provides the following information:

Parameter	Description
VLAN ID	**Synopsis:** A 32-bit signed integer The VLAN Identifier of the VLAN upon which the multicast group operates.
MAC Address	**Synopsis:** A string 17 characters long The multicast group MAC address.

Section 8.4.7

Viewing a List of IP Multicast Groups

To view a list of all IP multicast groups, navigate to ***switch » mcast-filtering » ip-mcast-groups***. If IP multicast groups have been configured, the **IP Multicast Groups** table appears.

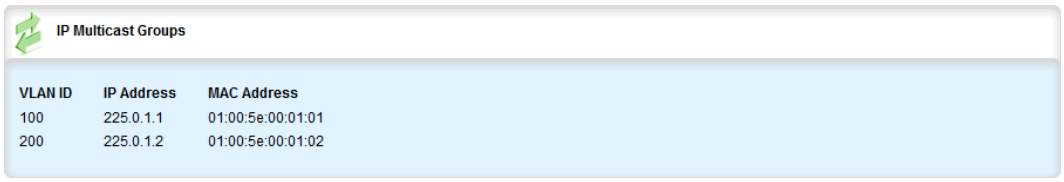


Figure 402: IP Multicast Groups Table

This table provides the following information:

Section 8.5

Managing VLANs

A Virtual Local Area Network (VLAN) is a group of devices on one or more LAN segments that communicate as if they were attached to the same physical LAN segment. VLANs are extremely flexible because they are based on logical connections, rather than physical connections.

When VLANs are introduced, all traffic in the network must belong to one VLAN or another. Traffic on one VLAN cannot pass to another, except through an inter-network router or Layer 3 switch.

VLANs are created in three ways:

- **Explicitly**
  Static VLANs can be created in the switch. For more information about static VLANs, refer to Section 8.5.5, "Managing Static VLANs".
- **Implicitly**
  When a VLAN ID (VID) is set for a Port VLAN (PVLAN), static MAC address or IP interface, an appropriate VLAN is automatically created if it does not yet exist.
- **Dynamically**
  VLANs can be learned through GVRP. For more information about GVRP, refer to Section 8.5.1.7, "GARP VLAN Registration Protocol (GVRP)"

CONTENTS

Section 8.5.1
VLAN Concepts

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

CONTENTS

Section 8.5.1.1
Tagged vs. Untagged Frames

VLAN tags identify frames as part of a VLAN network. When a switch receives a frame with a VLAN (or 802.1Q) tag, the VLAN identifier (VID) is extracted and the frame is forwarded to other ports on the same VLAN.

When a frame does not contain a VLAN tag, or contains an 802.1p (prioritization) tag that only has prioritization information and a VID of 0, it is considered an untagged frame.

Section 8.5.1.2
Native VLAN

Each port is assigned a native VLAN number, the Port VLAN ID (PVID). When an untagged frame ingresses a port, it is associated with the port's native VLAN.

By default, when a switch transmits a frame on the native VLAN, it sends the frame untagged. The switch can be configured to transmit tagged frames on the native VLAN.

Section 8.5.1.3
Edge and Trunk Port Types

Each port can be configured as an edge or trunk port.

An edge port attaches to a single end device, such as a PC or Intelligent Electronic Device (IED). An edge port carries traffic on the native VLAN.

Trunk ports are part of the network and carry traffic for all VLANs between switches. Trunk ports are automatically members of all VLANs configured in the switch.

The switch can 'pass through' traffic, forwarding frames received on one trunk port out of another trunk port. The trunk ports must be members of all VLANs that the 'pass through' traffic is part of, even if none of those VLANs are used on edge ports.

Frames transmitted out of the port on all VLANs other than the port's native VLAN are always sent tagged.

NOTE
It may be desirable to manually restrict the traffic on the trunk to a specific group of VLANs. For example, when the trunk connects to a device, such as a Layer 3 router, that supports a subset of the available LANs. To prevent the trunk port from being a member of the VLAN, include it in the VLAN's Forbidden Ports list.

For more information about the Forbidden Ports list, refer to Section 8.5.1.5, "Forbidden Ports List".

Port Type	VLANs Supported	PVID Format	Usage
Edge	1 (Native) Configured	Untagged	*VLAN Unaware Networks*: All frames are sent and received without the need for VLAN tags.
		Tagged	*VLAN Aware Networks*: VLAN traffic domains are enforced on a single VLAN.
Trunk	All Configured	Tagged or Untagged	*switch-to-Switch Connections*: VLANs must be manually created and administered, or can be dynamically learned through GVRP. *Multiple-VLAN End Devices*: Implement connections to end devices that support multiple VLANs at the same time.

Section 8.5.1.4
Ingress Filtering

Ingress filtering is a method of verifying that inbound packets arriving at a network originate from the source they are expected to be from, before entry (or ingress) is granted.

When ingress filtering is enabled, the switch verifies any tagged frame arriving at a port. When the port is not a member of the VLAN with which the frame is associated, the frame is dropped. When ingress filtering is disabled, frames from VLANs configured to the switch are not dropped. For more information about enabling or disabling ingress filtering, refer to Section 8.5.3, "Enabling/Disabling Ingress Filtering".

Section 8.5.1.5
Forbidden Ports List

Each VLAN can be configured to exclude ports from membership in the VLAN using the forbidden ports list. For more about configuring a list of forbidden ports, refer to Section 8.5.6, "Managing Forbidden Ports".

Section 8.5.1.6
VLAN-Aware Mode of Operation

The native operation mode for an IEEE 802.1Q compliant switch is VLAN-aware. Even if a specific network architecture does not use VLANs, RUGGEDCOM ROX II's default VLAN settings allow the switch to still operate in a VLAN-aware mode, while providing functionality required for almost any network application. However, the IEEE 802.1Q standard defines a set of rules that must be followed by all VLAN-aware switches:

- Valid VIDs are within the range of 1 to 4094. VIDs equal to 0 or 4095 are invalid.

- Each frame ingressing a VLAN-aware switch is associated with a valid VID.
- Each frame egressing a VLAN-aware switch is either untagged or tagged with a valid VID. Priority-tagged frames with an invalid VID will never sent out by a VLAN-aware switch.

NOTE
Some applications have requirements conflicting with IEEE 802.Q native mode of operation. For example, some applications explicitly require priority-tagged frames to be received by end devices.

Section 8.5.1.7
GARP VLAN Registration Protocol (GVRP)

GARP VLAN Registration Protocol (GVRP) is a standard protocol built on GARP (Generic Attribute Registration Protocol) to automatically distribute VLAN configuration information in a network. Each switch in a network needs only to be configured with VLANs it requires locally. VLANs configured elsewhere in the network are learned through GVRP. A GVRP-aware end station (i.e. PC or Intelligent Electronic Device) configured for a particular VID can be connected to a trunk on a GVRP-aware switch and automatically become part of the desired VLAN.

When a switch sends GVRP bridge protocol data units (BPDUs) out of all GVRP-enabled ports, GVRP BPDUs advertise all the VLANs known to that switch (configured manually or learned dynamically through GVRP) to the rest of the network.

When a GVRP-enabled switch receives a GVRP BPDU advertising a set of VLANs, the receiving port becomes a member of those advertised VLANs and the switch begins advertising those VLANs through all the GVRP-enabled ports (other than the port on which the VLANs were learned).

To improve network security using VLANs, GVRP-enabled ports may be configured to prohibit the learning of any new dynamic VLANs but at the same time be allowed to advertise the VLANs configured on the switch.

The following is an example of how to use GVRP:

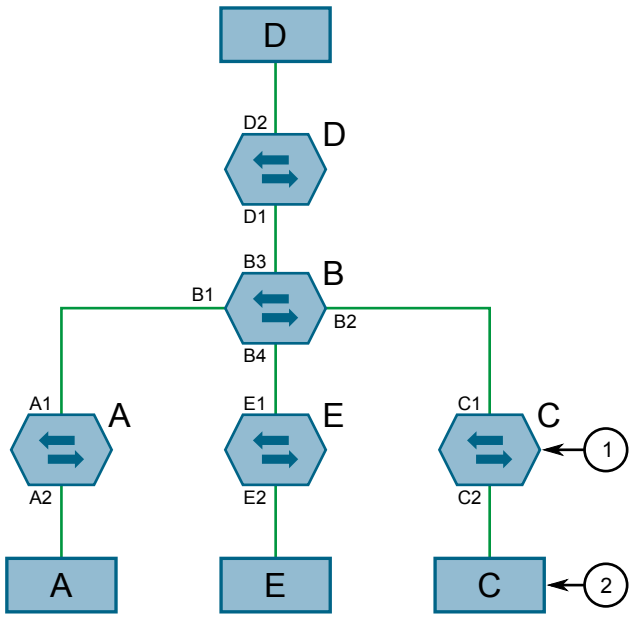


Figure 403: Using GVRP

1. Switch **2.** End Node

- Switch B is the core switch, all others are edge switches
- Ports A1, B1 to B4, C1, D1, D2 and E1 are GVRP aware
- Ports B1 to B4, D1 and D2 are set to advertise and learn
- Ports A1, C1 and E1 are set to advertise only
- Ports A2, C2 and E2 are edge ports
- End node D is GVRP aware
- End nodes A, E and C are GVRP unaware
- Ports A2 and C2 are configured with PVID 7
- Port E2 is configured with PVID 20
- End node D is interested in VLAN 20, hence VLAN 20 is advertised by it towards switch D
- D2 becomes a member of VLAN 20
- Ports A1 and C1 advertise VID 7
- Ports B1 and B2 become members of VLAN 7
- Ports D1 and B1 advertise VID 20
- Ports B3, B4 and D1 become members of VLAN 20

Section 8.5.1.8
PVLAN Edge

Protected VLAN (PVLAN) Edge refers to a feature of the switch that isolates multiple VLAN Edge ports from each other on a single device. All VLAN Edge ports in a switch that are configured as *protected* in this way are prohibited from sending frames to one another, but are still permitted to send frames to other, non-protected ports within the same VLAN. This protection extends to all traffic on the VLAN, including unicast, multicast and broadcast traffic.

NOTE
This feature is strictly local to the switch. PVLAN Edge ports are not prevented from communicating with ports outside of the switch, whether protected (remotely) or not.

Ports belonging to a specific PVID and a VLAN type of PVLAN Edge are part of one PVLAN Edge group. A PVLAN Edge group should include a minimum of two ports. There can be multiple PVLAN Edge groups on a switch.

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 8.5.1.9
VLAN Advantages

The following are a few of the advantages offered by VLANs.

Traffic Domain Isolation

VLANs are most often used for their ability to restrict traffic flows between groups of devices.

Unnecessary broadcast traffic can be restricted to the VLAN that requires it. Broadcast storms in one VLAN need not affect users in other VLANs.

Hosts on one VLAN can be prevented from accidentally or deliberately assuming the IP address of a host on another VLAN.

The use of creative bridge filtering and multiple VLANs can carve seemingly unified IP subnets into multiple regions policed by different security/access policies.

Multi-VLAN hosts can assign different traffic types to different VLANs.

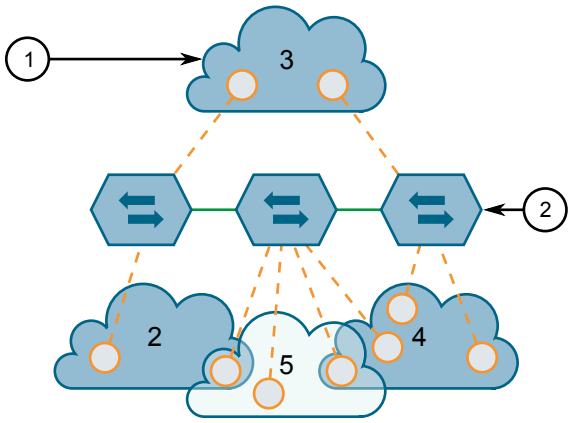


Figure 404: Multiple Overlapping VLANs

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.

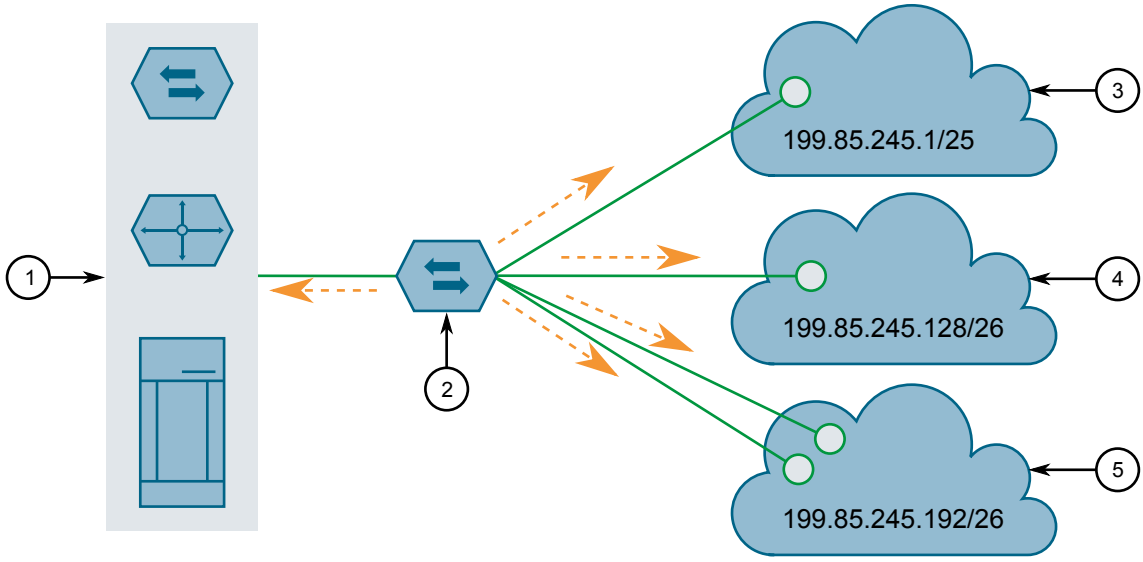


Figure 405: Inter-VLAN Communications

1. Server, Router or Layer 3 Switch **2.** Switch **3.** VLAN 2 **4.** VLAN 3 **5.** VLAN 4

Section 8.5.2

Configuring the Internal VLAN Range

RUGGEDCOM ROX II creates and utilizes internal VLANs for internal functions. To provide RUGGEDCOM ROX II with a pool of VLAN IDs to pull from when creating internal VLANs, a range of VLAN IDs must be reserved.

CAUTION!
Configuration hazard – risk of data loss. If the range-start or range-end values are changed in a way that invalidates any configured internal VLANs, the configurations defined for the affected VLANs will be lost upon repositioning.

IMPORTANT!
VLAN IDs reserved for internal VLANs should not be used by the network.

NOTE
*Changing the **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.

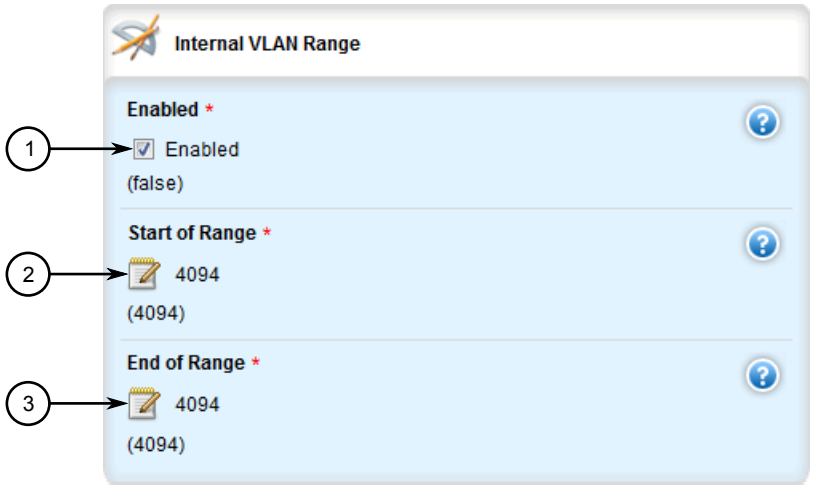


Figure 406: Internal VLAN Range Form

1. Enabled Check Box **2.** Start of Range Box **3.** End of Range Box

3. Configure the following parameters:

NOTE
By default, internal VLAN ranges are enabled whenever a serial module is detected, and are disabled otherwise.

Parameter	Description
enabled	**Synopsis:** { true, false } **Default:** false Enables/disables the Internal VLAN Range settings.
Start of Range	**Synopsis:** A 32-bit signed integer between 2 and 4094 **Default:** 4094 Defines the lower end of a range of VLANs used for the device only. VLAN ID 1 is not permitted.
End of Range	**Synopsis:** A 32-bit signed integer between 2 and 4094 **Default:** 4094 Defines the higher end of a range of VLANs used for the device only.VLAN ID 1 is not permitted.

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 8.5.3
Enabling/Disabling Ingress Filtering

When ingress filtering is enabled, any tagged packet arriving at a port, which is not a member of a VLAN with which that packet is associated, is dropped. When disabled, packets are not dropped.

To enable or disable ingress filtering, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to ***switch » vlans***. The **ingress-filtering** form appears.

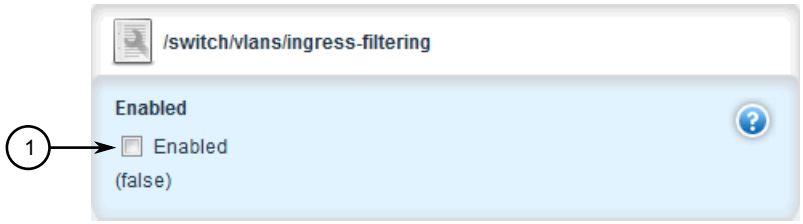


Figure 407: Ingress Filtering Form

1. Enabled Check Box

3. Click **Enabled** to enable ingress filtering, or clear **Enabled** to disable ingress filtering.
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 8.5.4
Managing VLANs for Switched Ethernet Ports

This section describes how to configure and manage VLANs assigned to switched Ethernet ports.

CONTENTS

Section 8.5.4.1
Viewing VLAN Assignments for Switched Ethernet Ports

To determine which VLANs are assigned to each switched Ethernet port, navigate to ***switch » vlans » vlan-summary***. The **VLAN Summary** table appears.

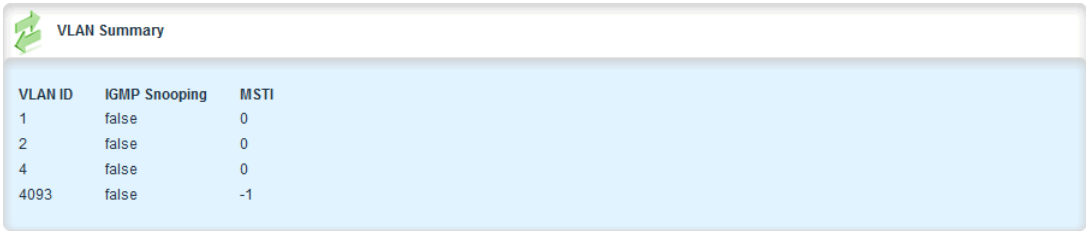


Figure 408: VLAN Summary Table

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 8.1.2, "Configuring a Switched Ethernet Port".

Section 8.5.4.2

Configuring VLANs for Switched Ethernet Ports

When a VLAN ID is assigned to a switched Ethernet port, the VLAN appears in the All-VLANs Table where it can be further configured.

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

1. 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.

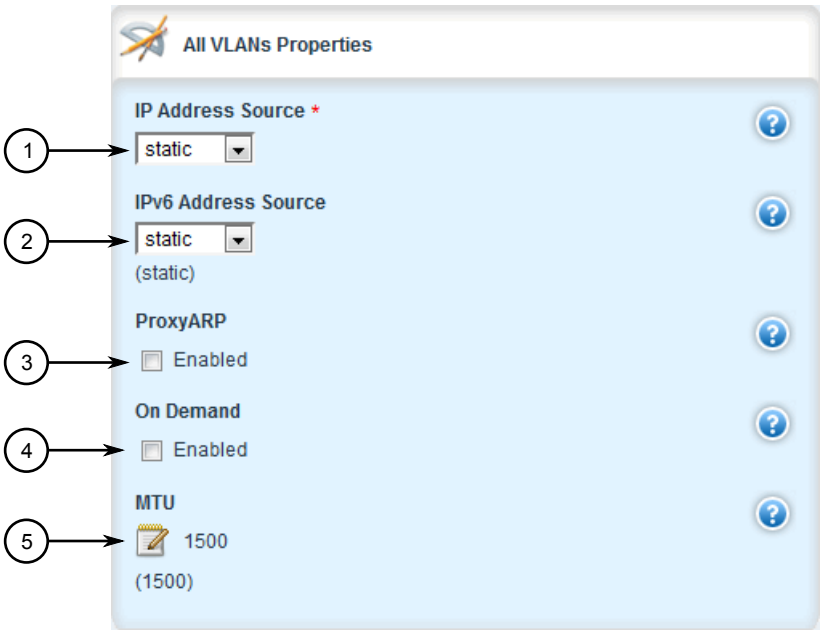


Figure 409: All VLANs Properties Form

1. IP Address Source List **2.** IPv6 Address Source List **3.** ProxyARP Check Box **4.** On-Demand Check Box **5.** MTU Box

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

Parameter	Description
VLAN ID	**Synopsis:** A 32-bit signed integer between 1 and 4094 The VLAN ID for this routable logical interface.
IP Address Source	**Synopsis:** { static, dynamic } Whether the IP address is static or dynamically assigned via Dynamic Host Configuration Protocol (DHCP) or Bootstrap Protocol (BOOTP). The DYNAMIC option is a common case of a dynamically assigned IP address. It switches between BOOTP and DHCP until it gets the response from the relevant server. This must be static for non-management interfaces. This parameter is mandatory.
IPv6 Address Source	**Synopsis:** { static, dynamic } **Default:** static Whether the IPv6 address is static or dynamically assigned via Dynamic Host Configuration Protocol (DHCP). This must be static for non-management interfaces.
ProxyARP	Enables/Disables whether the VLAN will respond to ARP requests for hosts other than itself.
On Demand	Brings up this interface on demand only.
MTU	**Synopsis:** A 32-bit signed integer between 68 and 9216 **Default:** 1500 The maximum transmission unit (the largest packet size allowed for this interface).

4. Add Quality of Service (QoS) maps to the VLAN. For more information, refer to Section 16.2.7.2, "Adding a QoS Map".
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 8.5.5
Managing Static VLANs

This section describes how to configure and manage static VLANs.

CONTENTS

Section 8.5.5.1
Viewing a List of Static VLANs

To view a list of static VLANs, navigate to ***switch » vlans » static-vlan***. If static VLANs have been configured, the **Static VLANs** table appears.

Figure 410: Static VLANs Table

If no static VLANs have been configured, add static VLANs as needed. For more information, refer to Section 8.5.5.2, "Adding a Static VLAN".

Section 8.5.5.2

Adding a Static VLAN

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

1. 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.

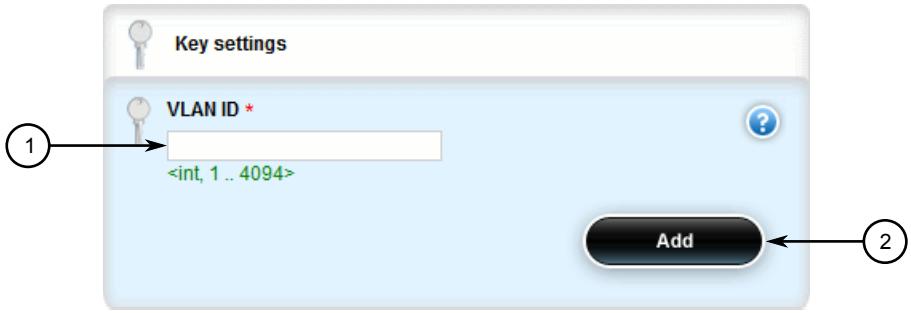


Figure 411: Key Settings Form

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 8.5.2, "Configuring the Internal VLAN Range".

Parameter	Description
VLAN ID	**Synopsis:** A 32-bit signed integer between 1 and 4094 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.

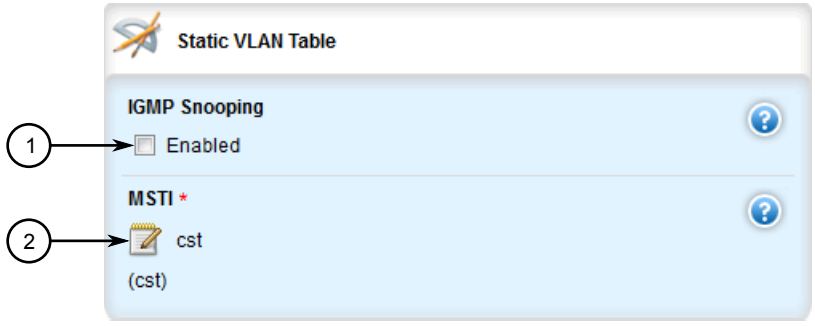


Figure 412: Static VLAN Table Form

1. IGMP Snooping Check Box **2.** MSTI Box

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	Enables or disables IGMP Snooping on the VLAN.
MSTI	**Synopsis:** { cst } or a 32-bit signed integer between 1 and 16 **Default:** cst Only valid for Multiple Spanning Tree Protocol (MSTP) and has no effect, if MSTP is not used. The parameter specifies the Multiple Spanning Tree Instance (MSTI) the VLAN should be mapped to.

6. If needed, configure a forbidden ports list. For more information, refer to Section 8.5.6.2, "Adding a Forbidden Port".
7. Configure the VLAN. For more information, refer to Section 8.5.4.2, "Configuring VLANs for Switched 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 8.5.5.3

Deleting a Static VLAN

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

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to ***switch » vlans » static-vlan***. The **Static VLANs** table appears.

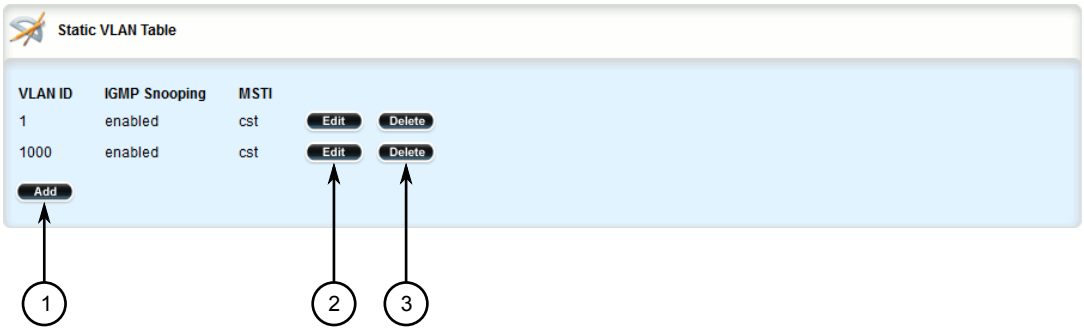


Figure 413: Static VLANs Table

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

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 8.5.6

Managing Forbidden Ports

Static VLANs can be configured to exclude ports from membership in the VLAN using the forbidden ports list.

CONTENTS

Section 8.5.6.1

Viewing a List of Forbidden Ports

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.

Figure 414: Forbidden Ports Table

If no ports have been forbidden, add forbidden ports as needed. For more information, refer to Section 8.5.6.2, "Adding a Forbidden Port".

Section 8.5.6.2
Adding a Forbidden Port

To add a forbidden port, do the following:

1. 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.

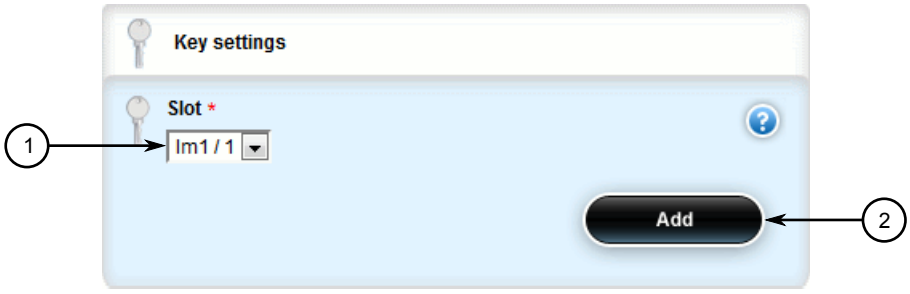


Figure 415: Key Settings Form

1. Slot Box **2.** Add Button

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

Parameter	Description
Slot	**Synopsis:** A string The name of the module location provided on the silkscreen across the top of the device.
Port	**Synopsis:** A string 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 8.5.6.3
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.

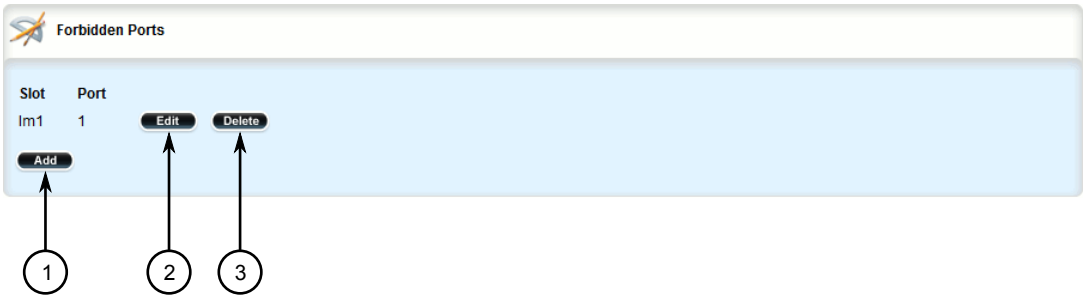


Figure 416: Forbidden Ports Table

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

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 8.5.7

Managing VLANs for Interfaces and Tunnels

This section describes how to view, add and delete tunnels for specific interfaces and tunnels.

- Section 11.1.15, “Managing VLANs for HDLC-ETH Connections”
- Section 12.2.8, “Managing VLANs for Virtual Switches”
- Section 12.4.6, “Managing VLANs for L2TPv3 Tunnels”
- Section 4.17.3, “Managing VLANs for Routable Ethernet Ports”

9 Layer 3

This chapter describes the Layer 3, or Network layer, features of RUGGEDCOM ROX II. For information about specific protocols that operate on this network layer, such as RIP, refer to Chapter 13, *Unicast and Multicast Routing*.

CONTENTS

Section 9.1

Layer 3 Switching Concepts

This section describes some of the concepts important to the implementation of Layer 3 switching in RUGGEDCOM ROX II.

CONTENTS

Section 9.1.1

Layer 3 Switch Forwarding Table

To route a packet with a specific destination IP address, a router needs the following information:

- **Egress interface (subnet):** this information is stored in the router's Routing Table.

NOTE
In a Layer 2 switched network segment, a VLAN constitutes an IP subnet.

- **Next-hop gateway Media Access Control (MAC) address:** this information is stored in the router's ARP Table.

NOTE
If the next hop is the destination subnet itself, then the destination host MAC address is required.

A Layer 3 Switch uses the routing information listed above and translates it into Layer 3 switching rules. These rules are known as the *Layer 3 Switch Forwarding Information Base (FIB)* or the *Layer 3 Switch Forwarding Table*. A Layer 3 switching rule is actually a set of parameters identifying a traffic flow to be switched and determining how to perform the switching.

Layer 3 switching Application-Specific Integrated Circuits (ASICs) store Layer 3 switching rules in a Ternary Content Addressable Memory (TCAM) table. Layer 3 switching rules can be statically configured or dynamically learned (also known as *auto-learned*).

Section 9.1.2
Static Layer 3 Switching Rules

When creating a static route through switch management, hardware acceleration can be explicitly configured. If hardware acceleration is selected, an appropriate Layer 3 switching rule is installed in the ASIC's TCAM and never ages out.

NOTE
Only TCP and UDP traffic flows will be accelerated by the IP/Layer 3 switch fabric.

Section 9.1.3
Dynamic Learning of Layer 3 Switching Rules

For static routes without hardware acceleration or for dynamic routes, Layer 3 switching rules can be dynamically learned based on software-based router and firewall decisions. For example, the Layer 3 switch can automatically decide to offload some flows from the router into the Layer 3 Forwarding Table.

After a certain amount of traffic for the same flow is successfully routed, the Layer 3 switching ASIC begins switching the rest of the packets belonging to the same flow. A flow is unidirectional traffic between two hosts. For example, traffic flowing between ports from one host to another is considered a flow. Traffic flowing in the opposite direction between the same ports is considered a different flow.

NOTE
For 8G SM, the maximum number of Layer 3 switching rules is 1000.

Different auto-learning methods may be used:

- **Flow-oriented learning** is when the switch uses the following information to identify a traffic flow:
  - Source IP address
  - Destination IP address

- Protocol
- Source TCP/UDP port
- Destination TCP/UDP port

This learning method is more granular and requires more ASIC resources, but it provides more flexibility in firewall configuration as the rule takes the protocol and TCP/UDP port into consideration to make forwarding decisions.

- **Host-oriented learning** is when the switch uses the following information to identify a traffic flow:
  - Source IP address
  - Destination IP address

  This learning method provides less flexibility in firewall configuration, as the user can allow or disallow traffic between two hosts.

For unicast traffic, each flow constitutes one rule. For multicast routing, one multicast route may constitute several rules.

The Layer 3 switch continuously monitors activity (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 9.1.4
Layer 3 Switch ARP Table

A router needs to know the destination host or next-hop gateway MAC address for it to forward a packet on the other subnet. Therefore, software maintains an Address Resolution Protocol (ARP) table that maps IP addresses to MAC addresses. The same information is also needed by the Layer 3 switching ASIC when it switches IP packets between subnets.

The destination or gateway MAC address is usually obtained through ARP. However, ARP entries can also be statically configured in the Layer 3 Switch so that they do not time out. When configuring a static ARP entry, if no value is entered for the MAC Address parameter, the address is automatically resolved through ARP and then saved statically. This is preserved across reboots of the device.

For a static Layer 3 switching rule, the destination MAC address for the rule is always resolved, and is also saved statically.

Section 9.1.5
Multicast Cross-VLAN Layer 2 Switching

Some RUGGEDCOM Layer 3 Switch models do not have full multicast Layer 3 switching capability and only support multicast cross-VLAN Layer 2 switching. Multicast cross-VLAN Layer 2 switching differs from the normal multicast Layer 3 switching in the following ways:

- Packet modification is not done. Specifically, the source MAC address and Time-To-Live (TTL) values in forwarded packets do not change.
- Separate TCAM table entries are required for each VLAN in the multicast switching rule. For example, a multicast stream ingressing VLAN 1 and egressing VLAN 2 and VLAN 3 requires three TCAM table entries.
- Supported bandwidth depends on the rule. Multicast traffic potentially has multiple egress VLANs, and the total utilized ASIC bandwidth is the ingress bandwidth multiplied by the number of ingress and egress VLANs. For

example, a 256 Mbps multicast stream ingressing VLAN 1 and egressing VLANs 2 and 3 requires 768 Mbps (256 Mbps × 3) of ASIC bandwidth.

- If a multicast packet should be forwarded to multiple egress VLANs, it egresses those VLANs sequentially rather than concurrently. This means the packet will experience different latency for each egress VLAN.

Section 9.1.6
Size of the Layer 3 Switch Forwarding Table

The routing table in a software router is limited only by the amount of available memory; its size can be virtually unlimited. However, the size of the TCAM in Layer 3 switching ASICs is significantly limited and may not be sufficient to accommodate all Layer 3 switching rules. If the TCAM is full and a new static rule is created, the new rule replaces some dynamically learned rule. If all of the rules in the TCAM are static, then the new static rule is rejected.

Section 9.1.7
Interaction with the Firewall

If security is a concern and you use a firewall in a Layer 3 Switch, it is important to understand how the Layer 3 switch interacts with the firewall.

A software router always works in agreement with a firewall so that firewall rules are always applied. However, in a Layer 3 Switch, if a switching rule is set in the switching ASIC (for example, due to a statically configured route), the ASIC switches all the traffic matching the rule before the firewall inspects the traffic.

Layer 3 switch ASICs are somewhat limited in how switching rules can be defined. These limitations do not allow configuring arbitrary firewall rules directly in the Layer 3 switch hardware. For sophisticated firewall rules, the firewall has to be implemented in software and the Layer 3 Switch must not switch traffic that is subject to firewall processing.

Whenever a change is made to the firewall configuration, some of the dynamically learned Layer 3 switching rules might conflict with the new firewall configuration. To resolve potential conflicts, dynamically learned Layer 3 switching rules are flushed upon any changes to the firewall configuration. The dynamically learned Layer 3 switching rules then have to be re-learned while the new firewall rules are applied.

For statically configured Layer 3 switching rules, take care to avoid conflicts between Layer 3 switching and the firewall. It should be understood that static Layer 3 switching rules always take precedence. Therefore, you must thoroughly examine the switch configuration for potential conflicts with the firewall. For more information about firewalls, refer to Section 6.8, “Managing Firewalls”

Section 9.2
Configuring Layer 3 Switching

To configure Layer 3 switching, do the following:

NOTE
*When hardware acceleration is used, and learning mode is set to **flow-oriented**, 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.

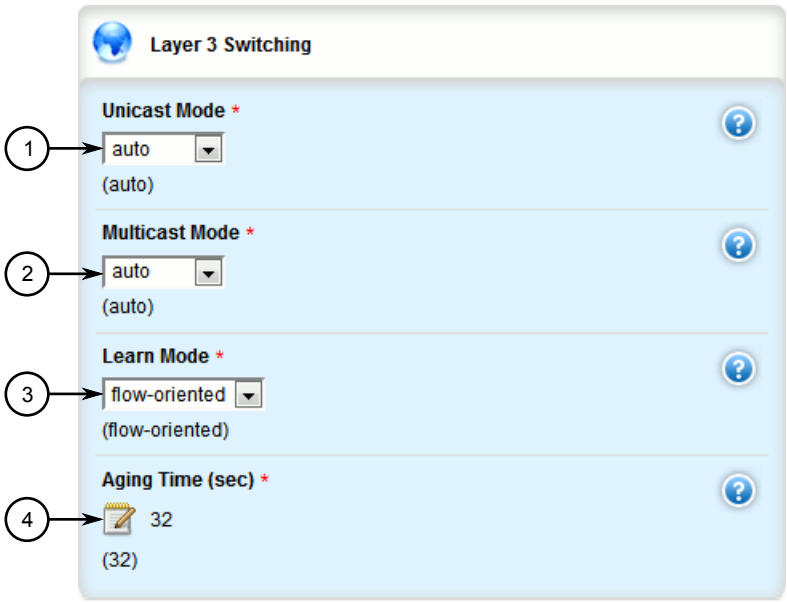


Figure 417: Layer 3 Switching Form

1. Unicast Mode List **2.** Multicast Mode List **3.** Learn Mode List **4.** Aging Time (sec) Box

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

Parameter	Description
Unicast Mode	**Synopsis:** { disabled, auto, static } **Default:** auto • Disabled: Layer 3 switching is disabled. The ability to disable routing hardware acceleration may be desired, for example, in a system with sophisticated firewall rules, which could not be supported by the Layer 3 switching ASIC and would require software processing. • Static: Only statically configured Layer 3 switching rules will be used. This mode may be useful, for example, in a system with complex configuration where static routes do not conflict with a firewall, while traffic flows following dynamic routes have to be subject to sophisticated firewall filtering. • Auto: Both statically configured and dynamically learned Layer 3 switching rules will be used. In this mode, maximum routing hardware acceleration is utilized.
Multicast Mode	**Synopsis:** { disabled, auto, static } **Default:** auto • Disabled: Layer 3 switching is disabled. The ability to disable routing hardware acceleration may be desired, for example, in a system with sophisticated firewall rules, which could not be supported by the Layer 3 switching ASIC and would require software processing. • Static: Only statically configured Layer 3 switching rules will be used. This mode may be useful, for example, in a system with complex configuration where static routes do not conflict with a firewall, while traffic flows following dynamic routes have to be subject to sophisticated firewall filtering. • Auto: Both statically configured and dynamically learned Layer 3 switching rules will be used. In this mode, maximum routing hardware acceleration is utilized.
Learn Mode	**Synopsis:** { flow-oriented, host-oriented }

Parameter	Description

	Default: flow-oriented
	Defines how dynamically learned traffic flows are identified:
	• Flow-oriented: Traffic flows are identified by a 5-tuple signature:
	`Src IP address Dst IP address Protocol Src TCP/UDP port Dst TCP/UDP port`
	This mode should be used, if fine-granularity firewall filtering is configured in the device (i.e. some flows between two hosts should be forwarded, while other flows between the same two hosts should be filtered). However, this mode utilizes more Layer 3 switching ASIC resources and is not recommended if fine-granularity firewall filtering is not required.
	• Host-oriented: Traffic flows are identified by a 2-tuple signature:
	`Src IP address Dst IP address`
	All traffic between two IP hosts is hardware-accelerated regardless of the protocol and TCP/UDP ports. This mode potentially controls multiple flows with a single rule and hence is more efficient in utilizing Layer3 switching ASIC resources.

Aging Time (sec)	**Synopsis:** A 32-bit signed integer between 16 and 600 **Default:** 32 This parameter configures the time a dynamically learned rule for a traffic flow, which has become inactive, is held before being removed from the Layer 3 switch forwarding table.

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 9.3
Managing Static ARP Table Entries

This section describes how to configure and manage static ARP table entries.

CONTENTS

Section 9.3.1
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.

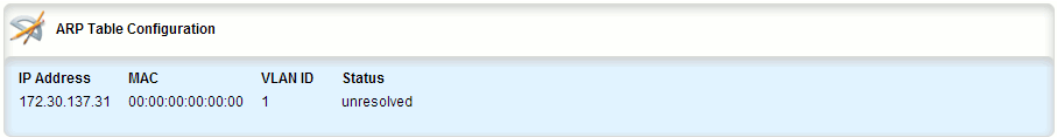


Figure 418: ARP Table Configuration Table

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 9.3.2, "Adding a Static ARP Table Entry".

Section 9.3.2

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.

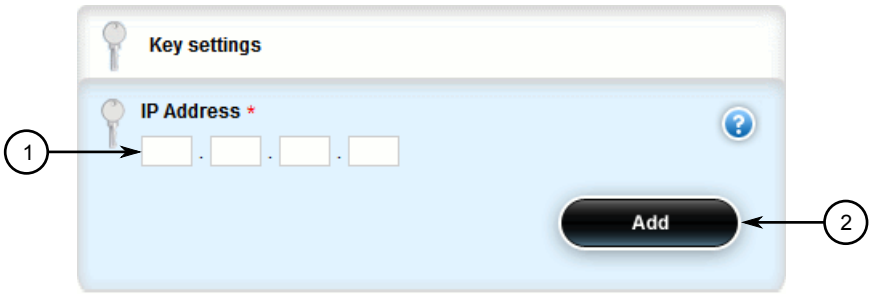


Figure 419: Key Settings Form

1. IP Address Box **2.** Add Button

3. Configure the following parameters as required:

Parameter	Description
IP Address	**Synopsis:** A string The IP address of the network device the entry describes.

4. Click **Add**. The **ARP Table Configuration** form appears.

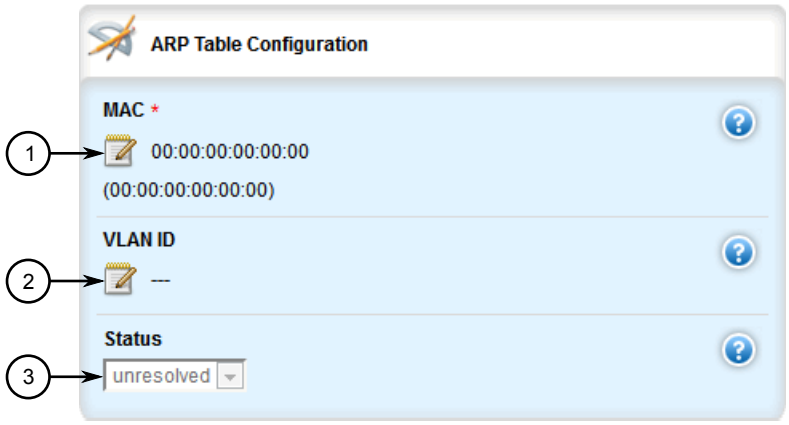


Figure 420: ARP Table Configuration Form

1. MAC Box **2.** VLAN ID Box **3.** Status List

5. Configure the following parameters as required:

NOTE
Letters in MAC addresses must be lowercase.

Parameter	Description
MAC	**Synopsis:** A string 17 characters long **Default:** 00:00:00:00:00:00 The MAC address of the network device specified by the IP address.
VLAN ID	**Synopsis:** A 32-bit signed integer between 1 and 4094 The VLAN Identifier of the VLAN upon which the MAC address operates.

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 9.3.3
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.

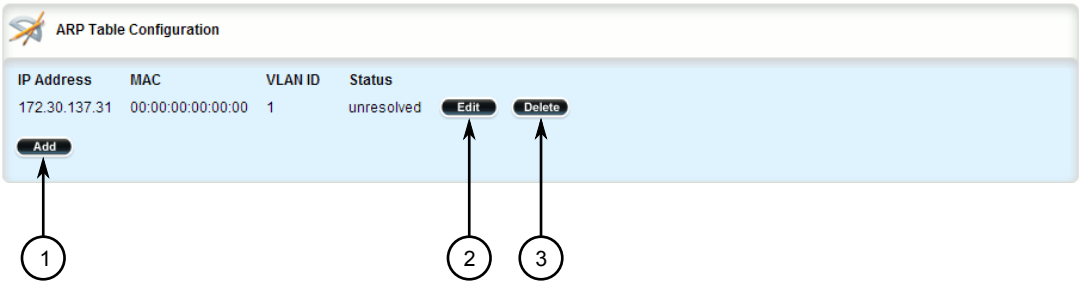


Figure 421: ARP Table Configuration Table

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

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 9.4

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.

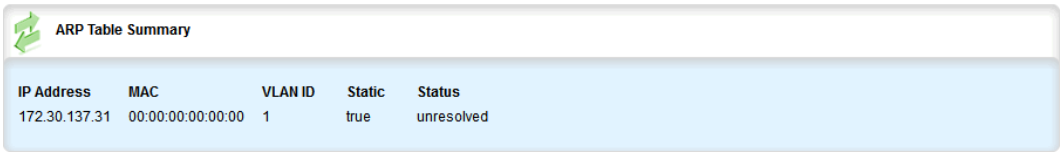


Figure 422: ARP Table Summary

This table provides the following information:

Parameter	Description
IP Address	**Synopsis:** A string The IP address of the network device the entry describes.
MAC	**Synopsis:** A string 17 characters long **Default:** 00:00:00:00:00:00 The MAC address of the network device specified by the IP address.
VLAN ID	**Synopsis:** A 32-bit signed integer The VLAN Identifier of the VLAN upon which the MAC address operates.
static	**Synopsis:** { true, false } **Default:** 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	**Synopsis:** { resolved, unresolved } **Default:** unresolved The Address Resolution Protocol (ARP) entry resolution status: • Resolved: MAC-IP address pair is resolved and operational. • Unresolved: the device hasn't resolved the MAC-IP address pair and keeps sending ARP requests periodically.

If no ARP table entries have been configured, add static ARP table entries as needed. For more information, refer to Section 9.3.2, "Adding a Static ARP Table Entry".

Section 9.5
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.

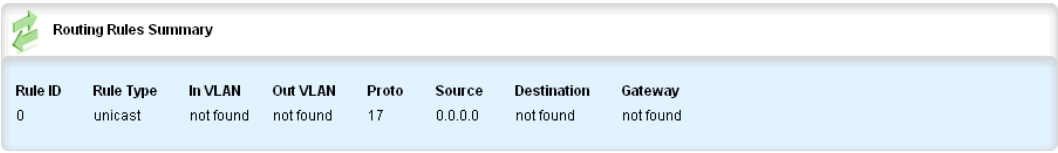


Figure 423: Routing Rules Summary Table

This table provides the following information:

Parameter	Description
Rule ID	**Synopsis:** A 32-bit unsigned integer between 0 and 2999 Defines the order in which rules are matched on each ingress packet. The first matched rule is applied on the packet.
Rule Type	**Synopsis:** { multicast, unicast, invalid, hidden } Identifies the type of the rule: unicast,multicast,invalid.
In VLAN	**Synopsis:** A 32-bit signed integer Identifies the ingress VLAN. To match the rule, the packet's ingress VLAN must match the number.
Out VLAN(s)	**Synopsis:** A 32-bit signed integer Identifies the egress VLAN. The matched multicast packet is sent to the identified VLAN.
Protocol	**Synopsis:** An 8-bit unsigned integer The IP Encapsulated Protocol number. Unless zero is specified, the incoming packet's IP protocol must match this number.
source	**Synopsis:** { 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.

Parameter	Description
Source Port	**Synopsis:** A 32-bit signed integer between 0 and 65535 The port associated with the source flow. A value of 0 means Not Applicable.
destination	**Synopsis:** { 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	**Synopsis:** A 32-bit signed integer between 0 and 65535 The port associated with the destination flow. A value of 0 means Not Applicable.
gateway	**Synopsis:** A string Defines the nexthop IP address. The matched unicast packet is sent to the identified gateway.
Pkts/sec	**Synopsis:** A 32-bit unsigned integer Displays the statistical throughput of all packets matching the rule, in packets per second.
static	**Synopsis:** { true, false } Whether the rule is static or dynamic. Static rules are configured as a result of management activity. Dynamic rules are automatically learned by the device and can be unlearned subject to aging time.
Routing Action	**Synopsis:** { forward, exclude } The action applied to packets matching the rule: • Forward: Perform a hardware acceleration. • Exclude: Exclude from hardware acceleration and always pass matching packets to the CPU for software routing.
status	**Synopsis:** { active, resolving, pending, excluding } Whether the rule is currently operational or not: • Active: The rule is fully operational and can be applied, so hardware acceleration is performed. • Resolving: The rule is not operational yet due to some unresolved information, like the Address Resolution Protocol (ARP) or gateway's MAC address in the MAC Address Table. Hardware acceleration is not performed. • Pending: there are not enough hardware resources to setup the rule and all its dependencies. Hardware acceleration is not performed.

Section 9.6
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 9.1, "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.

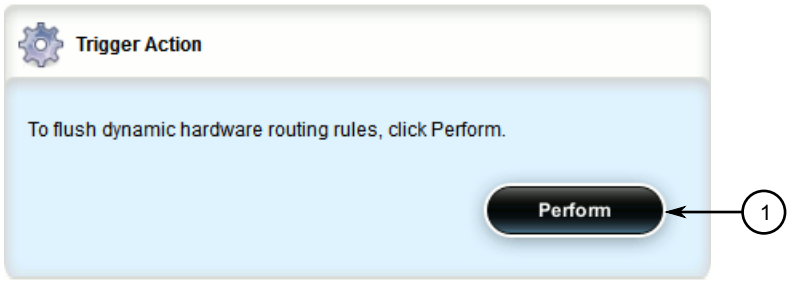


Figure 424: Trigger Action Form

1. Perform Button

2. Click **Perform**.

10 Serial Server

This chapter describes how to manage and configure the serial server, including serial ports, protocols, remote hosts and the Device Address Tables.

NOTE
Serial server functions are dependent on the installation of a serial line module. For more information about available serial line modules, refer to the RUGGEDCOM Modules Catalog [https://support.industry.siemens.com/cs/ww/en/view/109747072] for the RUGGEDCOM RX1500 series.

CONTENTS

Section 10.1

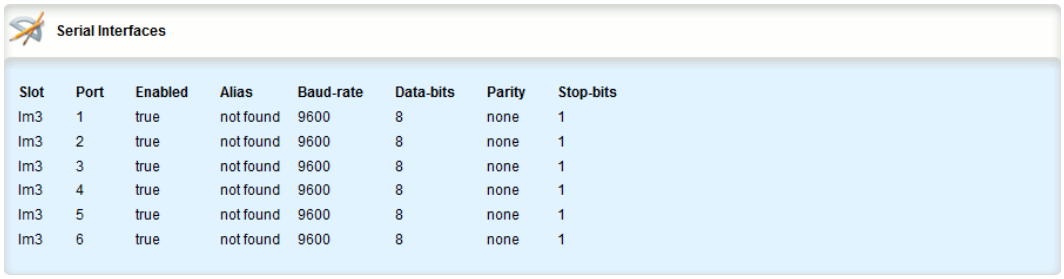
Managing Serial Ports

This section describes how to configure, monitor and manage serial ports on the device.

CONTENTS

Section 10.1.1
Viewing a List of Serial Ports

To view a list of serial ports configured on the device, navigate to ***interface » serial***. The **Serial Interfaces** table appears.

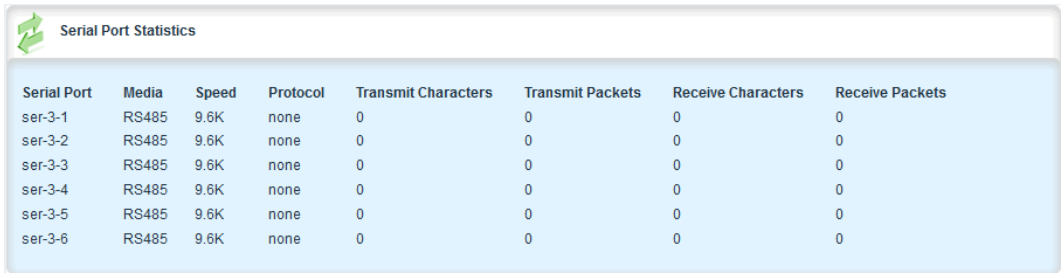

Serial Interfaces

Slot	Port	Enabled	Alias	Baud-rate	Data-bits	Parity	Stop-bits
Im3	1	true	not found	9600	8	none	1
Im3	2	true	not found	9600	8	none	1
Im3	3	true	not found	9600	8	none	1
Im3	4	true	not found	9600	8	none	1
Im3	5	true	not found	9600	8	none	1
Im3	6	true	not found	9600	8	none	1

Figure 425: Serial Interfaces Table

Section 10.1.2
Viewing Serial Port Statistics

To view statistics collected on the serial ports, navigate to ***interfaces » serial » port***. The **Serial Port Statistics** form appears.


Serial Port Statistics

Serial Port	Media	Speed	Protocol	Transmit Characters	Transmit Packets	Receive Characters	Receive Packets
ser-3-1	RS485	9.6K	none	0	0	0	0
ser-3-2	RS485	9.6K	none	0	0	0	0
ser-3-3	RS485	9.6K	none	0	0	0	0
ser-3-4	RS485	9.6K	none	0	0	0	0
ser-3-5	RS485	9.6K	none	0	0	0	0
ser-3-6	RS485	9.6K	none	0	0	0	0

Figure 426: Serial Port Statistics Form

This form provides the following information:

Parameter	Description
Serial Port	**Synopsis:** A string 1 to 10 characters long The name of the serial interface.
media	**Synopsis:** A string 1 to 31 characters long The type of port media { RS232 RS422 RS485 }. This parameter is mandatory.
speed	**Synopsis:** { auto, 1.5M, 2.4M, 10M, 100M, 1G, 10G, 1.776M, 3.072M, 7.2M, 1.2K, 2.4K, 9.6K, 19.2K, 38.4K, 57.6K, 115.2K, 230.4K, 4.8K, 76.8K } The speed (in Kilobits-per-second). This parameter is mandatory.

Parameter	Description
protocol	**Synopsis:** A string 1 to 31 characters long The serial protocol assigned to this port. This parameter is mandatory.
Transmit Characters	**Synopsis:** A 32-bit unsigned integer The number of bytes transmitted over the serial port. This parameter is mandatory.
Transmit Packets	**Synopsis:** A 32-bit unsigned integer The number of packets transmitted over the serial port. This parameter is mandatory.
Receive Characters	**Synopsis:** A 32-bit unsigned integer The number of bytes received by the serial port. This parameter is mandatory.
Receive Packets	**Synopsis:** A 32-bit unsigned integer The number of packets received by the serial port. This parameter is mandatory.
Packet Errors	**Synopsis:** A 32-bit unsigned integer The number of packet errors on this serial port. This parameter is mandatory.
Parity Errors	**Synopsis:** A 32-bit unsigned integer The number of parity errors on this serial port. This parameter is mandatory.
Framing Errors	**Synopsis:** A 32-bit unsigned integer The number of framing errors on this serial port. This parameter is mandatory.
Overrun Errors	**Synopsis:** A 32-bit unsigned integer The number of overrun errors on this serial port. This parameter is mandatory.

Section 10.1.3

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.

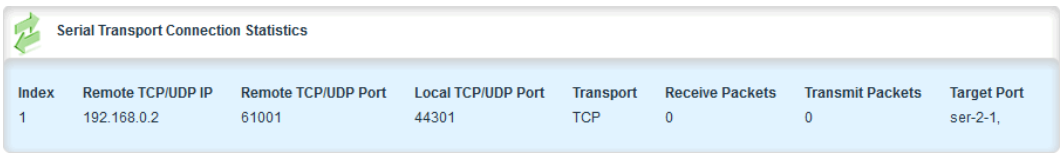


Figure 427: Transport Connection Statistics Table

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.

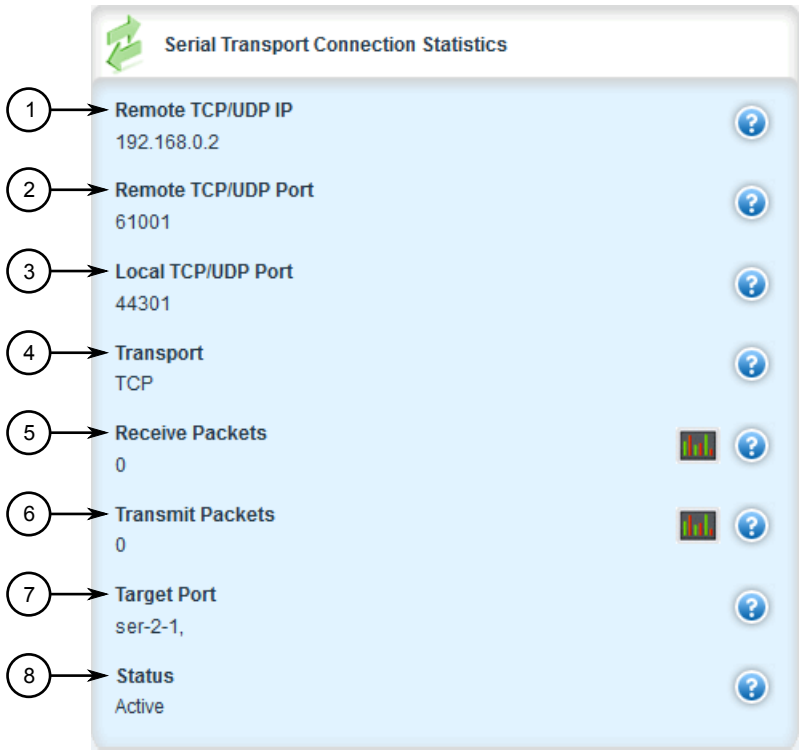


Figure 428: TCP/UDP Connection Statistics Form

1. Remote TCP/UDP IP **2.** Remote TCP/UDP Port **3.** Local TCP/UDP Port **4.** Transport **5.** Receive Packets **6.** Transmit Packets **7.** Target Port **8.** Status

These tables and forms provide the following information:

Parameter	Description
index	**Synopsis:** A string 1 to 32 characters long The transport connection index.
Remote TCP/UDP IP	**Synopsis:** A string 1 to 32 characters long The IP address of the remote serial server. This parameter is mandatory.
Remote TCP/UDP Port	**Synopsis:** A 32-bit signed integer The port of the remote serial server. This parameter is mandatory.
Local TCP/UDP Port	**Synopsis:** A 32-bit signed integer The local port for the incoming connection. This parameter is mandatory.
transport	**Synopsis:** A string 1 to 8 characters long The transport protocol (UDP or TCP) for this serial port.

Parameter	Description
	This parameter is mandatory.
Receive Packets	**Synopsis:** A 32-bit unsigned integer The number of packets received from TCP/UDP. This parameter is mandatory.
Transmit Packets	**Synopsis:** A 32-bit unsigned integer The number of packets transmitted to TCP/UDP. This parameter is mandatory.
Target Port	**Synopsis:** A string 1 to 1024 characters long The target serial port. This parameter is mandatory.
status	**Synopsis:** A string 1 to 31 characters long The connection status of the serial port. This parameter is mandatory.

Section 10.1.4
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.

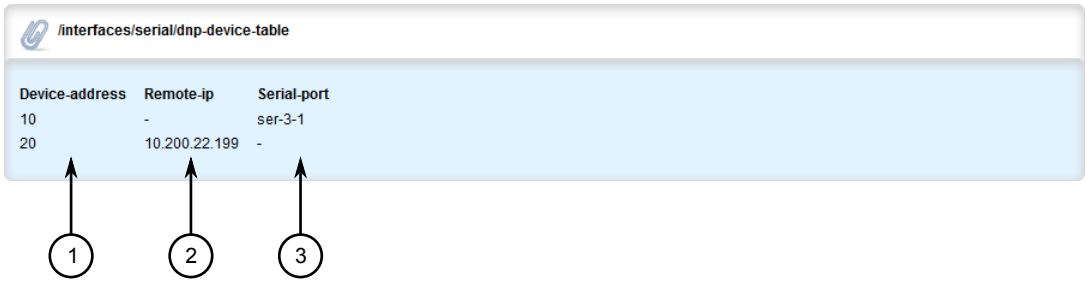


Figure 429: DNP Device Table

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

This table provides the following information:

Parameter	Description
Device Address	**Synopsis:** A string 1 to 32 characters long The DNP device address.
Remote IP	**Synopsis:** A string 1 to 32 characters long The IP address of the remote host that provides a connection to the this DNP device address. This parameter is mandatory.
Serial Port	**Synopsis:** A string 1 to 128 characters long The target serial port.

Parameter	Description
	This parameter is mandatory.

Section 10.1.5
Clearing Serial Port Statistics

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

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

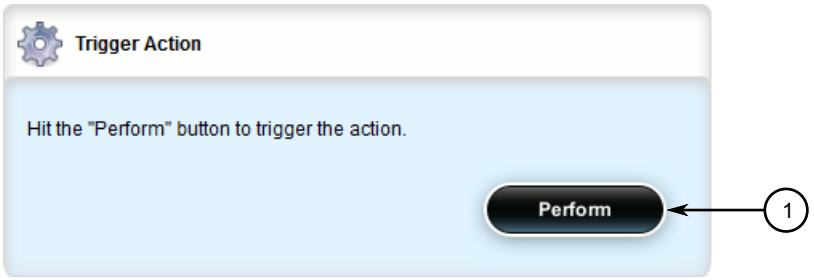


Figure 430: Trigger Action Form

1. Perform Button

3. Click **Perform**.

Section 10.1.6
Configuring a Serial Port

To configure a serial port, do the following:

IMPORTANT!
Do not enable flow control when Modbus TCP protocol is enabled.

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to ***interface » serial » {port}***, where *{port}* is the serial port. The **Serial Interfaces** form appears.

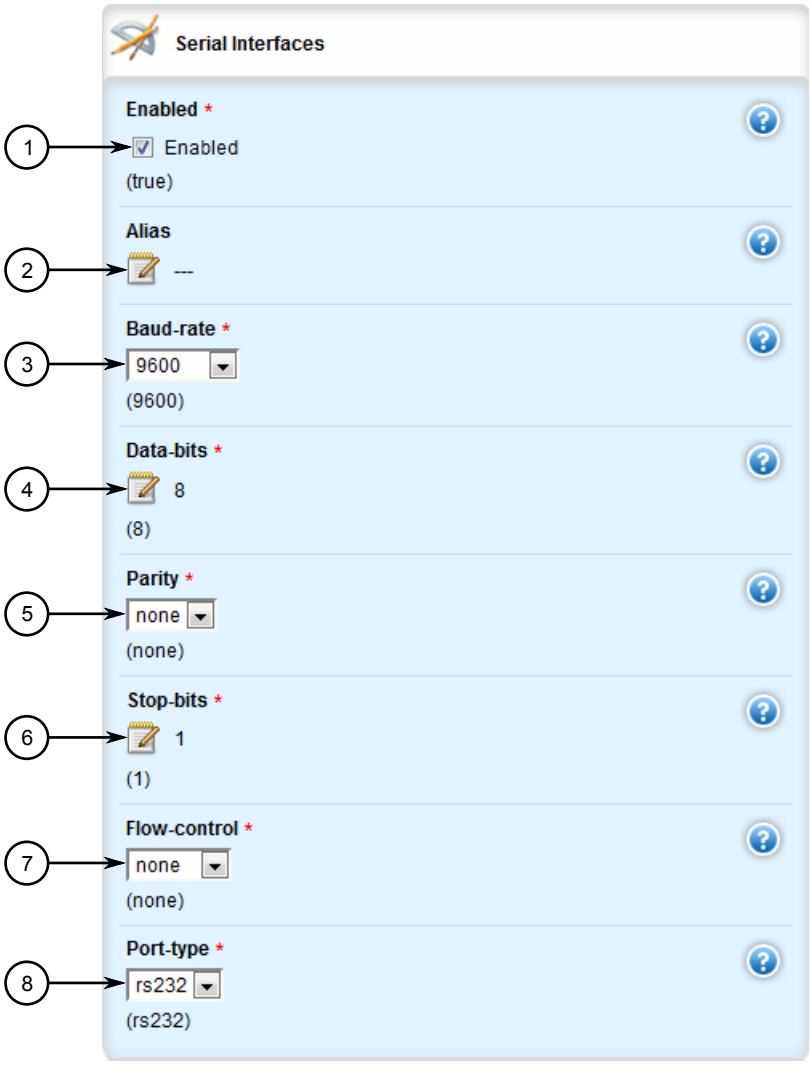


Figure 431: Serial Interfaces Form

1. Enabled Check Box **2.** Alias Box **3.** Baud-Rate List **4.** Data Bits Box **5.** Parity List **6.** Stop Bits Box **7.** Flow Control List **8.** Port Type List

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

Parameter	Description
slot	**Synopsis:** { sm, lm1, lm2, lm3, lm4, lm5, lm6, swport, eth, serport, celport, wlanport } The name of the module location provided on the silkscreen across the top of the device.
port	**Synopsis:** A 32-bit signed integer between 1 and 16 The port number as seen on the front plate silkscreen of the switch (or a list of ports, if aggregated in a port trunk).
enabled	**Synopsis:** { true, false } **Default:** true Provides the option to enable or disable this interface. When unchecked (i.e disabled), the interface will prevent all frames from being sent and received on that interface.

Parameter	Description
alias	**Synopsis:** A string 1 to 64 characters long The SNMP alias name of the interface.
Baud Rate	**Synopsis:** { 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200, 230400, 76800 } **Default:** 9600 The baud rate selection of the serial port.
Data Bits	**Synopsis:** A 32-bit signed integer between 7 and 8 **Default:** 8 The number of data bits.
parity	**Synopsis:** { none, even, odd } **Default:** none The parity of the serial port.
Stop Bits	**Synopsis:** A 32-bit signed integer between 1 and 2 **Default:** 1 The number of stop bits of the serial port.
Flow Control	**Synopsis:** { none, xonxoff } **Default:** none The flow control of the serial port.
Port Type	**Synopsis:** { rs232, rs422, rs485 } **Default:** rs485 The type of serial port.

4. Configure one or more serial protocols. For more information, refer to Section 10.2.3, "Adding a Serial Port Protocol".
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 10.1.7
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.

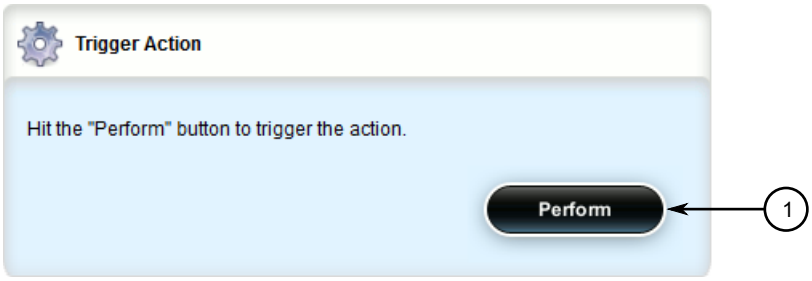


Figure 432: Trigger Action Form

1. Perform Button

2. Click **Perform**.

Section 10.1.8

Resetting a Serial Port

To reset a serial port, do the following:

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

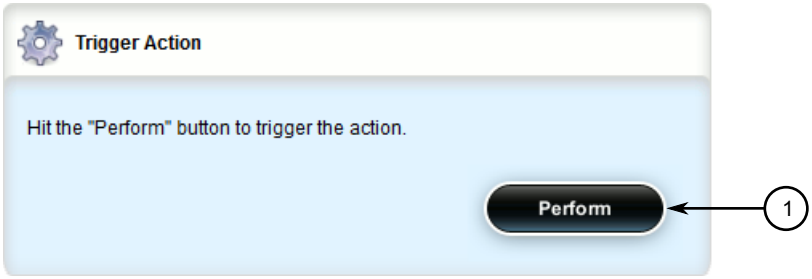


Figure 433: Trigger Action Form

1. Perform Button

3. Click **Perform**.

Section 10.2

Managing Serial Port Protocols

This section describes how to configure and manage serial protocols for serial ports.

CONTENTS

Section 10.2.1

Serial Port Protocol Concepts

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

CONTENTS

Section 10.2.1.1

Raw Socket Applications

The raw socket protocol transports streams of characters from one serial port on the device to a specified remote IP address and port. The raw socket protocol supports TCP and UDP transport.

Broadcast RTU Polling

Broadcast polling allows a single host connected to the device to broadcast a polling stream to a number of remote RTUs.

The host connects through a serial port to the device. Up to 32 TCP remote RTUs may connect to the device's host-end via the network. For UDP transport, the device can send a polling stream to up to 64 remote hosts (RTUs).

Initially, the remote hosts place TCP connections to the device's host-end. The host-end in turn is configured to accept the required number of incoming TCP connections. The host connected to the device then sequentially polls each remote host. When a poll is received, the device forwards (i.e. broadcasts) it to all the remote hosts. All

remote hosts will receive the request and the appropriate remote host will issue a reply. The reply is returned to the device, where it is forwarded to the host.

Host And Remote Roles

The raw socket protocol can either initiate or accept a TCP connection for serial encapsulation. It can establish a connection initiated from a remote host, vice versa, or bidirectionally.

Configure the device at the host-end to establish a connection with the remote host when:

- The host-end uses a port redirector that must make the connection
- The host-end is only occasionally activated and will make the connection when it becomes active
- A host-end firewall requires the connection to be made outbound

If the host-end wants to open multiple connections with the remote-ends in order to implement broadcast polling, configure the device to accept connections with the remote-ends.

Configure the device to connect from each side (host or remote) to the other if both sides support this functionality.

Message Packetization

The serial server buffers receive characters into packets in order to improve network efficiency and demarcate messages.

The serial server uses three methods to decide when to packetize and forward the buffered characters to the network:

- packetize on a specific character
- packetize on timeout
- packetize on a full packet

If configured to packetize on a specific character, the serial server will examine each received character, packetize and forward it upon receiving the specific character. The character is usually a <CR> or an <LF> character but may be any ASCII character.

If configured to packetize on a timeout, the serial server will wait for a configurable time after receiving a character before packetizing and forwarding it. If another character arrives during the waiting interval, the timer is restarted. This method allows characters transmitted as part of an entire message to be forwarded to the network in a single packet, when the timer expires after receiving the very last character of the message. This is usually the only packetizer selected when supporting Modbus TCP communications.

Finally, the serial server will always packetize and forward on a full packet, specifically when the number of characters fills its communications buffer (1024 bytes).

Section 10.2.1.2
Modbus TCP Applications

The Modbus TCP Server application is used to transport Modbus requests and responses across IP networks. The source of the polls is a Modbus *master*, a host computer that issues the polls to a remote host (RTU) connected to the serial port of the device running the Modbus TCP Server application. The Modbus polls encapsulated in TCP packets received by the device will be forwarded to the remote host via the serial port based on the host's address defined in the RTU list. The responses from remote host are TCP encapsulated and returned to the *master* that originated the polls.

Port Numbers

The TCP port number dedicated to Modbus use is port 502. The Modbus TCP Server application can also be configured to accept a connection on a configurable port number. This auxiliary port can be used by masters that do not support port 502.

Retransmissions

The Server Gateway offers the ability to resend a request to a remote host should the remote host receive the request in error or the Server Gateway receives the remote host response in error.

The decision to use retransmissions, and the number to use, depends upon factors such as:

- The probability of a line failure.
- The number of remote hosts and the amount of traffic on the port.
- The cost of retransmitting the request from the server versus timing-out and retransmitting at the master. This cost is affected by the speed of the ports and of the network.

ModBus Exception Handling

If the Server Gateway receives a request for an un-configured remote host, it will respond to the originator with a special message called an exception (type 10). A type 11 exception is returned by the server if the remote host fails to respond to requests.

Native Modbus TCP polling packages will want to receive these messages. Immediate indication of a failure can accelerate recovery sequences and reduce the need for long timeouts.

Section 10.2.1.3

DNP Applications

RUGGEDCOM ROX II supports Distributed Network Protocol (DNP) version 3.0, commonly used by utilities in process automation systems. DNP3 protocol messages specify source and destination addresses. A destination address specifies which device should process the data, and the source address specifies which device sent the message. Having both destination and source addresses satisfies at least one requirement for peer-to-peer communication since the receiver knows where to direct a response.

Each device supporting DNP must have a unique address within the collection of devices sending and receiving DNP messages.

Address Learning for DNP

RUGGEDCOM ROX II implements both local and remote address learning for DNP. A local Device Address Table is populated with DNP Addresses learned for local and remote DNP devices. Each DNP address is associated with either a local serial port or a remote IP address.

When a message with an unknown DNP source address is received on a local serial port, the DNP source address and serial port number are entered into the Device Address Table. When a message with an unknown DNP source address is received from the IP network, on the IP interface that is configured as the DNP learning interface, the DNP source address and the IP address of the sender are entered into the Device Address Table.

When a message with an unknown DNP destination address is received on a local serial port, the message is sent in a UDP broadcast to the network interface configured as the DNP learning interface. When a message with an unknown DNP destination address is received from the IP network, it is sent to all local serial ports configured as DNP ports.

NOTE
Learned addresses are not recorded in the Device Address Table.

UDP transport is used during the DNP address learning phase.

An aging timer is maintained for each DNP address in the table, and is reset whenever a DNP message is sent to or received for the specified address.

This learning facility makes it possible to configure the DNP3 protocol with a minimum number of parameters: a TCP/UDP port number, a learning network interface and an aging timer.

» DNP Broadcast Messages

DNP addresses 65521 through 65535 are reserved as DNP3 broadcast addresses. RUGGEDCOM ROX II supports DNP3 broadcast messages. DNP broadcast messages received on local serial ports are transmitted to all IP Addresses in the Device Address Table (whether learned or statically configured).

When a DNP broadcast message is received from the IP network, it is transmitted on all local serial ports configured as DNP ports.

Section 10.2.1.4
Incoming/Outgoing Serial Connections

The RUGGEDCOM RX1500/RX1501/RX1510/RX1511/RX1512 supports up to 32 TCP/UDP connections per serial port, up to a total of 128 TCP/UDP connections to the serial server.

Section 10.2.2
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.

Figure 434: Serial Protocols Table

If no serial port protocols have been configured, add protocols as needed. For more information, refer to Section 10.2.3, “Adding a Serial Port Protocol”.

Section 10.2.3
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.

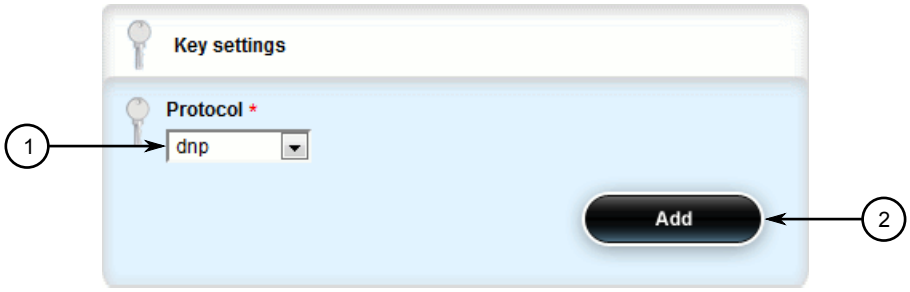


Figure 435: Key Settings Form

1. Protocol Box **2.** Add Button

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

Parameter	Description
protocol	**Synopsis:** { rawsocket, tcpmodbus, dnp, vmserial } The protocol of the serial port.

5. Click **Add** to create the protocol.
6. If `dnp`, `tcpmodbus`, or `rawsocket` was selected, configure the protocol.
   - For information about configuring a DNP protocol, refer to Section 10.2.4, "Configuring the DNP Protocol".
   - For information about configuring a Modbus TCP protocol, refer to Section 10.2.5, "Configuring the Modbus TCP Protocol".
   - For information about configuring a raw socket protocol, refer to Section 10.2.6, "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 10.2.4

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

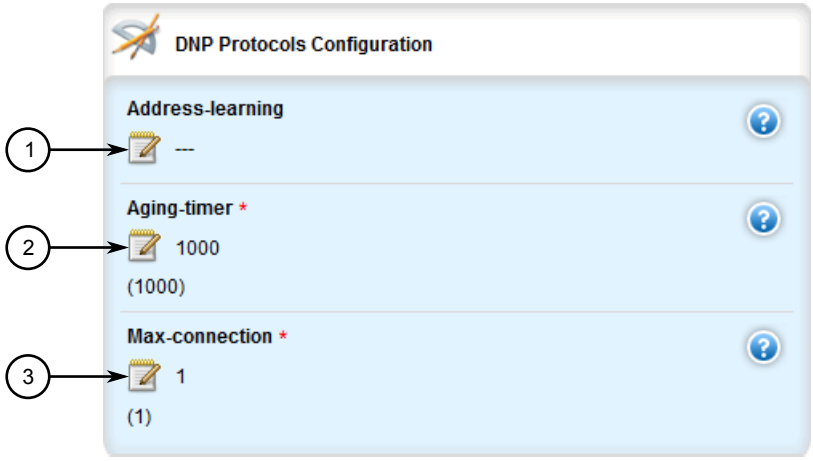


Figure 436: DNP Protocols Configuration Form

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

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

Parameter	Description
Address Learning	**Synopsis:** A string 1 to 15 characters long The interface to learn the RTU address from.
Aging Timer	**Synopsis:** A 32-bit signed integer between 60 and 10800 **Default:** 1000 The length of time a learned DNP device in the Device Address Table may go without any DNP communication before it is removed from the table.
Max Connection	**Synopsis:** A 32-bit signed integer between 1 and 32 **Default:** 1 The maximum number of incoming DNP connections.

5. Add a Device Address table. For more information about adding Device Address tables, refer to Section 10.3.2, "Adding a Device Address Table".
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 10.2.5

Configuring the Modbus TCP Protocol

To configure the modbus TCP 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 » tcpmodbus » settcpmodbus***, where *{interface}* is the serial port. The **TCP Modbus Configuration** form appears.

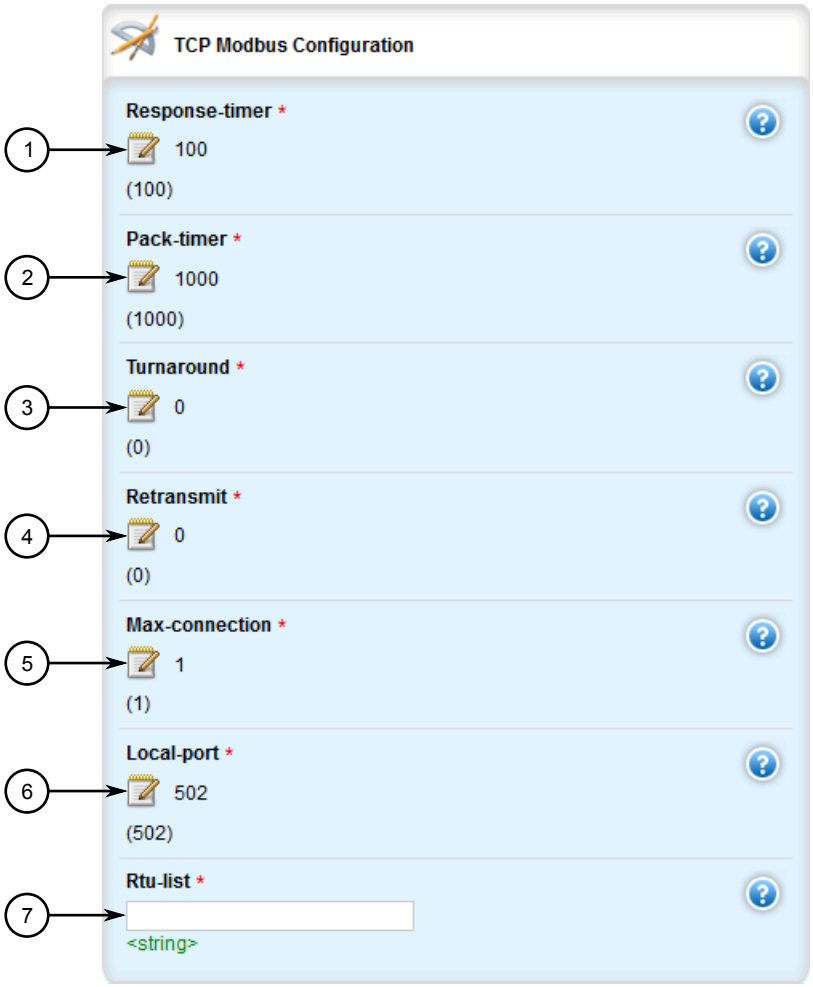


Figure 437: TCP Modbus Configuration Form

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	**Synopsis:** A 32-bit signed integer between 50 and 10000 **Default:** 100 The maximum time from the last transmitted character of the outgoing poll until the first character of the response. If the RTU does not respond in this time, the poll will have been considered failed.
Pack Timer	**Synopsis:** A 32-bit signed integer between 5 and 1000 **Default:** 1000 The maximum allowable time to wait for a response to a Modbus request to complete once it has started.
Turn Around	**Synopsis:** A 32-bit signed integer between 0 and 1000 **Default:** 0

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

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 10.2.6
Configuring the Raw Socket Protocol

To configure the raw socket 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 » rawsocket***, where *{interface}* is the serial port.
3. Click the **+** symbol in the menu next to **setrawsocket**. The **Raw Socket Configuration** form appears.

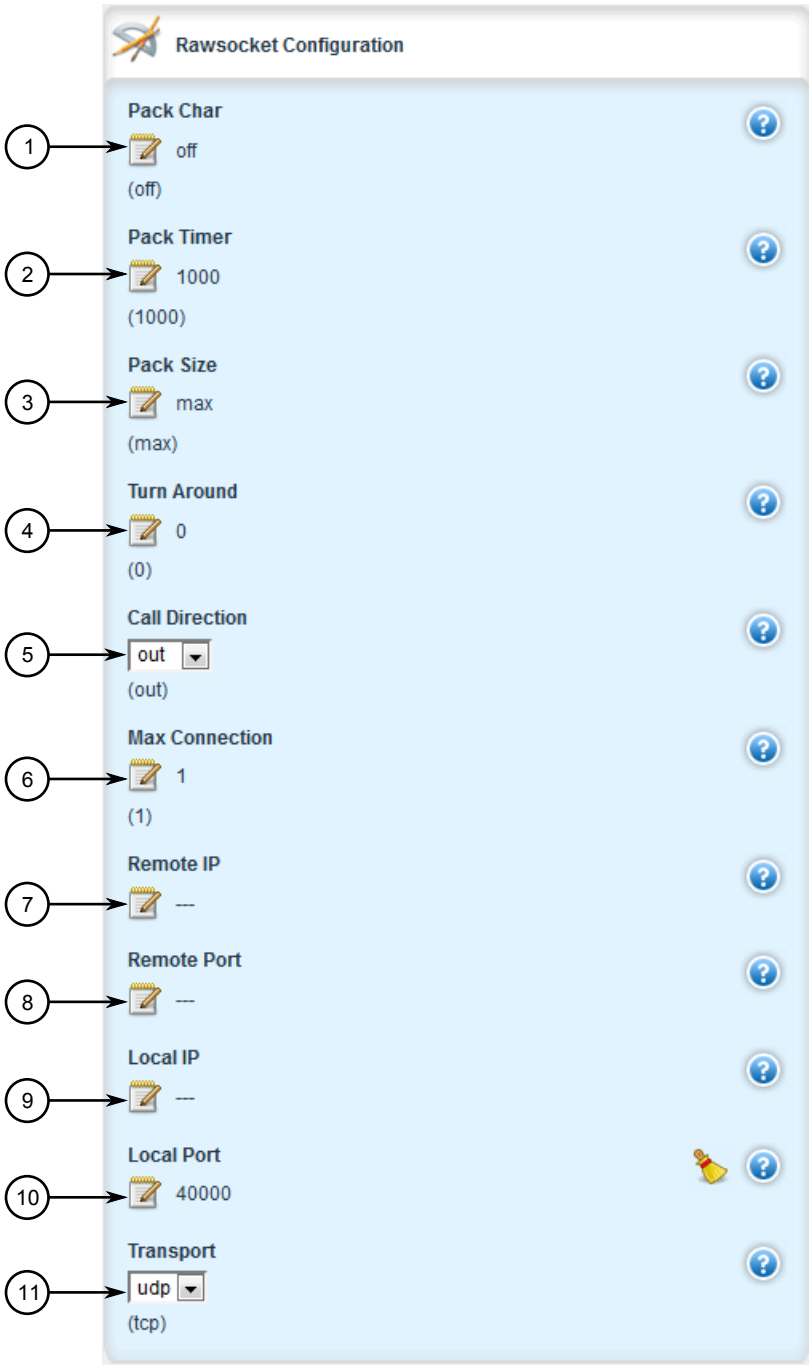


Figure 438: Raw Socket Configuration Form

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	**Synopsis:** { off } or a 32-bit signed integer between 0 and 255 **Default:** off The numeric value of the ASCII character which will force forwarding of accumulated data to the network.
Pack Timer	**Synopsis:** A 32-bit signed integer between 5 and 1000 **Default:** 1000 The delay from the last received character until when data is forwarded.
Pack Size	**Synopsis:** { max } or a 32-bit signed integer between 16 and 1400 **Default:** max The maximum number of bytes received from the serial port to be forwarded.
Turn Around	**Synopsis:** A 32-bit signed integer between 0 and 1000 **Default:** 0 The amount of delay (if any) to insert between the transmissions of individual messages out the serial port.
Call Direction	**Synopsis:** { in, out, both } **Default:** out Whether to accept an incoming connection, place an outgoing connection or do both.
Max Connection	**Synopsis:** A 32-bit signed integer between 1 and 32 **Default:** 1 The maximum number of incoming connections to permit when the call direction is incoming.
Remote IP	**Synopsis:** A string 7 to 15 characters long or a string 6 to 40 characters long The IP address used when placing an outgoing connection.
Remote Port	**Synopsis:** A 32-bit signed integer between 1024 and 65535 The TCP destination port used in outgoing connections.
Local IP	**Synopsis:** A string 7 to 15 characters long or a string 6 to 40 characters long The IP address used to establish a connection. Leaving it blank allows an incoming connection to any interface.
Local Port	**Synopsis:** A 32-bit signed integer between 1024 and 65535 The local TCP/UDP port to use to accept incoming connections.
Transport	**Synopsis:** { tcp, udp } **Default:** 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 10.5.2, "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 10.2.7
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.

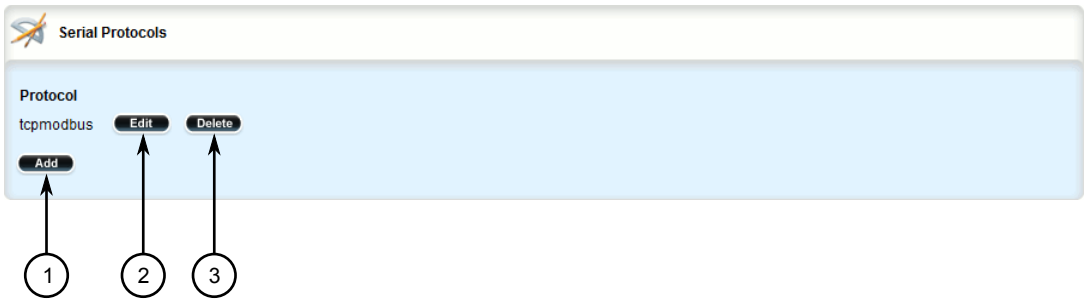


Figure 439: Serial Protocols Table

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

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 10.3

Managing Device Address Tables

This section describes how to manage DNP addresses in the local Device Address Table.

CONTENTS

Section 10.3.1

Viewing a List of Device Address Tables

To view a list of Device Address tables configured for a serial port using the DNP protocol, 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.

Figure 440: DNP Device Address Table Configuration Table

If no Device Address tables have been configured, add tables as needed. For more information, refer to Section 10.3.2, "Adding a Device Address Table".

Section 10.3.2

Adding a Device Address Table

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

1. 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.

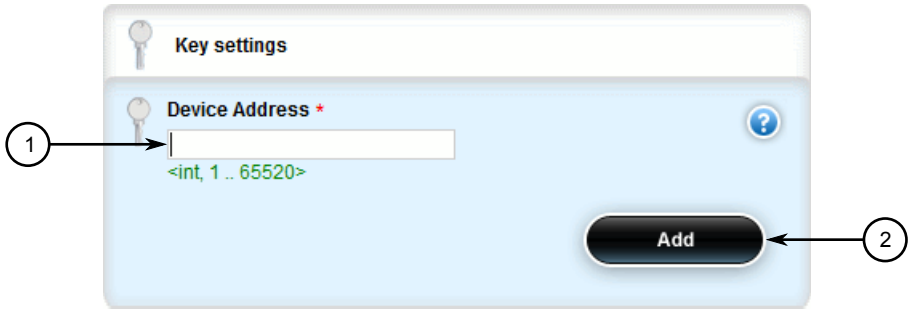


Figure 441: Key Settings Form

1. Device Address Box **2.** Add Button

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

Parameter	Description
Device Address	**Synopsis:** A 32-bit signed integer between 1 and 65520 The local or remote DNP device address. The address may be that of a DNP device connected to a local serial port or one available via the serial port of a remote IP host.

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

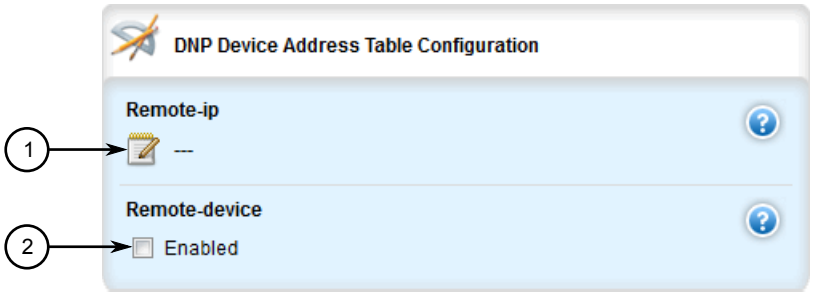


Figure 442: DNP Device Address Table Configuration Form

1. Remote IP Box **2.** Remote Device Check Box

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

Parameter	Description
Remote IP	**Synopsis:** A string 7 to 15 characters long or a string 6 to 40 characters long The IP address of the remote host that provides a connection to the DNP device with the configured address. Leave this field empty to forward DNP messages that match the configured address to the local serial port.
Remote Device	Enables forwarding of DNP messages that match the device address to the remote IP.

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 10.3.3

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.

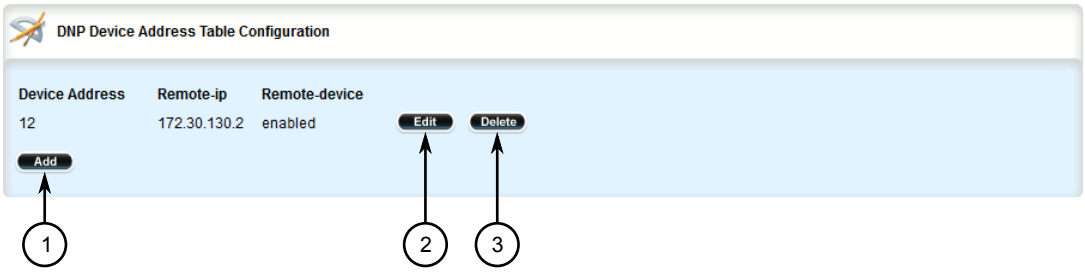


Figure 443: DNP Device Address Table Configuration Table

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 10.4

Managing Serial Multicast Streaming

RUGGEDCOM ROX II supports the ingress and egress of raw-socket UDP serial multicast streams.

This section describes how to configure and manage serial multicast streaming.

CONTENTS

Section 10.4.1

Understanding Serial Multicast Streaming

Serial multicast streaming allows the transport of serial data streams to individual or groups of remote hosts via the UDP protocol.

An Ethernet multicast stream consists of a multicast group IP address (e.g. 232.1.1.1), destination UDP port (e.g. 1 to 65535) and an interface.

A serial port can act as both:

- A *sink* for data coming from IP multicast streams

- A *source* of data to be transmitted to multiple IP multicast receivers

CONTENTS

Section 10.4.1.1
Sink vs. Source Ports

A serial port can act as either a *sink* and/or *source* port:

- **Sink Port**
  A sink port is a consumer of multicast packets. It registers itself to receive multicast traffic from a known multicast group IPv4 address and destination UDP port and then forwards the traffic along the serial link. The traffic is then received by a connected third-party serial device and processed.
- **Source Port**
  A source port is a producer of multicast packets. It receives serial traffic from a connected third-party serial device and packetizes it into multicast IPv4 packets. Each packet is assigned a specific multicast group IPv4 address, destination UDP port and source UDP port.

Section 10.4.1.2
Multicast Streaming Examples

Serial multicast streaming can be deployed in multiple ways:

» Serial Interfaces Configured as a Sink for Multicast Streams

In this configuration, the source of the multicast data comes from the Ethernet network interfaces and is transmitted to multiple sink serial devices. The advantage of this scenario is the ease of configuration on the Ethernet networking side. Instead of indicating which serial port to send to via unicast packets, the controller can send a single multicast stream to all or some connected serial devices.

» Serial Interfaces Configured as a Source for Multicast Streams

In this configuration, the source of the multicast data comes from the serial port and device side and is transmitted to multiple Ethernet interfaces over one multicast stream. The advantage of this scenario is the ease of configuration of listening devices. There will be a lesser need to keep track of IP addresses of interfaces, and listeners can be easily substituted without concern over maintaining the same IP address.

» Serial Interfaces Configured as a Source and Sink for Multicast Streams

In this configuration, the serial data is forwarded to other serial devices, with the ability to transmit to multiple Ethernet interfaces via a single multicast stream. This is an extension of the two previous examples. The advantage of this configuration is to allow one serial source device to send data to multiple receivers whether they are another serial port or a listener device over an Ethernet network.

Section 10.4.2

Configuring Serial Multicast Streaming

To configure serial multicast streaming, do the following:

1. Configure the raw socket protocol for one or more serial ports. For more information, refer to Section 10.2.3, "Adding a Serial Port Protocol".
2. Configure the remote host for the encapsulation of rawsocket serial over multicast with the destination multicast IP, UDP port, and interface(s). For more information, refer to Section 10.5.2, "Adding a Remote Host" and Section 10.7.2, "Adding a Remote Host Interface".
3. Configure the local port, local host multicast IP and local host interface(s) for the de-encapsulation of multicast stream(s) into raw socket serial. For more information, refer to Section 10.6.2, "Adding a Local Host" and Section 10.8.2, "Adding a Local Host Interface".
4. Verify that multicast traffic can be seen on the incoming and outgoing interface(s). For more information, refer to Section 10.1.2, "Viewing Serial Port Statistics".

Section 10.4.3

Example: Serial Interfaces Configured as a Sink for Multicast Streams

This configuration example shows multicast messages from group 232.1.1.1, directed to UDP port 5001, reaching ser-1-1 from the interface switch.0010 via raw socket connections. Ser-1-1, upon receiving these messages, passes on the data to serial device S1, to which it is directly connected.

IMPORTANT!
The values shown are specific to the provided topology. Actual values can vary based on the user's configuration.

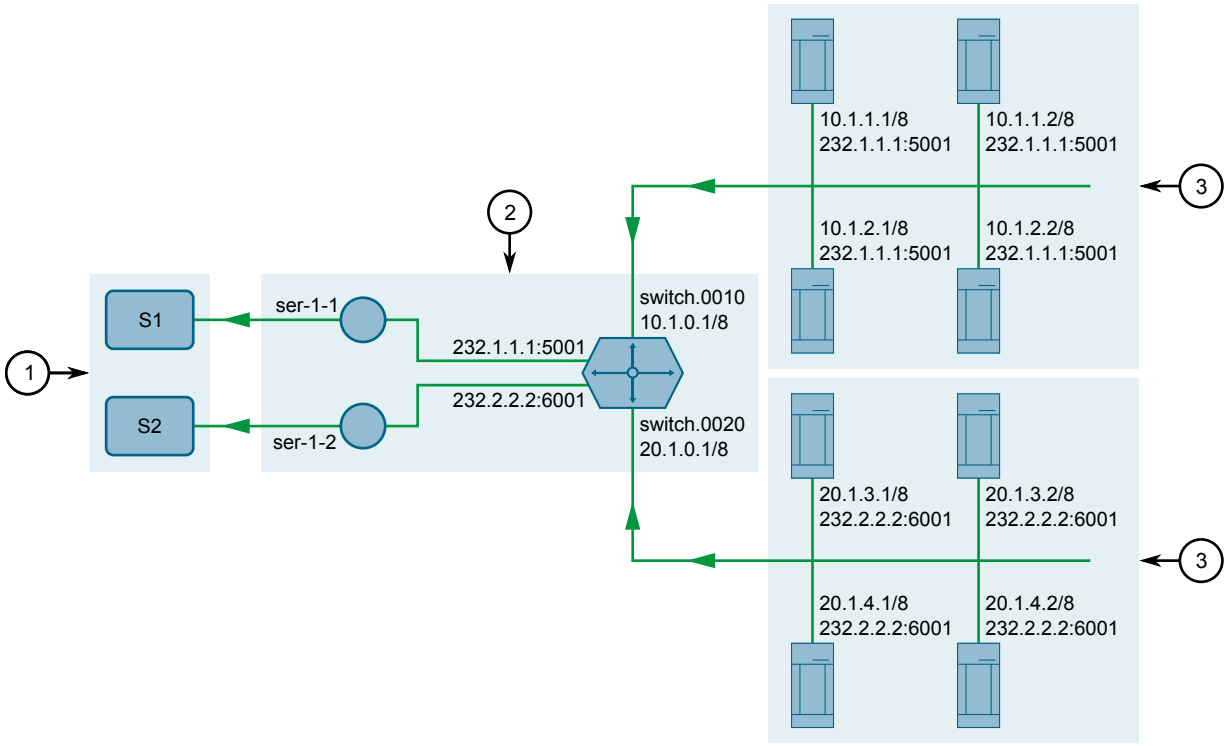


Figure 444: Topology – Serial Interfaces Configured as a Sink for Multicast Streams

1. Serial Devices **2.** Sink Device (RUGGEDCOM RX1500) **3.** Ethernet Network Interfaces

» Step 1: Configure ser-1-1

1. Configure IP addresses for the interfaces (switch.0010 and switch.0020). For more information, refer to Section 7.1.3.2, "Adding an IPv4 Address".
2. Create a raw socket connection for ser-1-1. For more information, refer to Section 10.2.3, "Adding a Serial Port Protocol".
3. Set the raw socket of the local port to 5001. For more information, refer to Section 10.2.6, "Configuring the Raw Socket Protocol".
4. Set the transport method to *UDP*. For more information, refer to Section 10.2.6, "Configuring the Raw Socket Protocol".
5. Set the multicast group for the local host to 232.1.1.1. For more information, refer to Section 10.6.2, "Adding a Local Host".
6. Set *switch.0010* as the interface for the local host. For more information, refer to Section 10.8.2, "Adding a Local Host Interface"
7. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.

» Step 2: Configure ser-1-2

1. Create a raw socket connection for ser-1-2. For more information, refer to Section 10.2.3, "Adding a Serial Port Protocol".
2. Set the raw socket of the local port to 6001. For more information, refer to Section 10.2.6, "Configuring the Raw Socket Protocol".
3. Set the transport method to *UDP*. For more information, refer to Section 10.2.6, "Configuring the Raw Socket Protocol".
4. Set the multicast group for the local host to 232.2.2.2. For more information, refer to Section 10.6.2, "Adding a Local Host".
5. Set *switch.0020* as the interface for the local host. For more information, refer to Section 10.8.2, "Adding a Local Host Interface"
6. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
7. Verify the configuration by viewing the statistics collected on the serial ports. For more information, refer to Section 10.1.2, "Viewing Serial Port Statistics".

» Final Configuration Example

ser-1-1 Configuration

```
serial lm1 1
  no alias
  protocols rawsocket
   setrawsocket local-port 5001
   setrawsocket transport udp
   setrawsocket local-host 232.1.1.1
    interface switch.0010
```

ser-1-2 Configuration

```
serial lm1 2
  no alias
  protocols rawsocket
   setrawsocket local-port 6001
   setrawsocket transport udp
   setrawsocket local-host 232.2.2.2
    interface switch.0020
```

Section 10.4.4

Example: Serial Interfaces Configured as a Source for Multicast Streams

This configuration example shows ser-1-1 receiving data on the wire from S1, then creating multiple raw socket remote host interfaces to send the data to both interfaces switch.0010 and switch.0020. This data is then packetized as multicast packets and sent to destination group 232.1.1.1 and destination UDP port 5001.

IMPORTANT!
The values shown are specific to the provided topology. Actual values can vary based on the user's configuration.

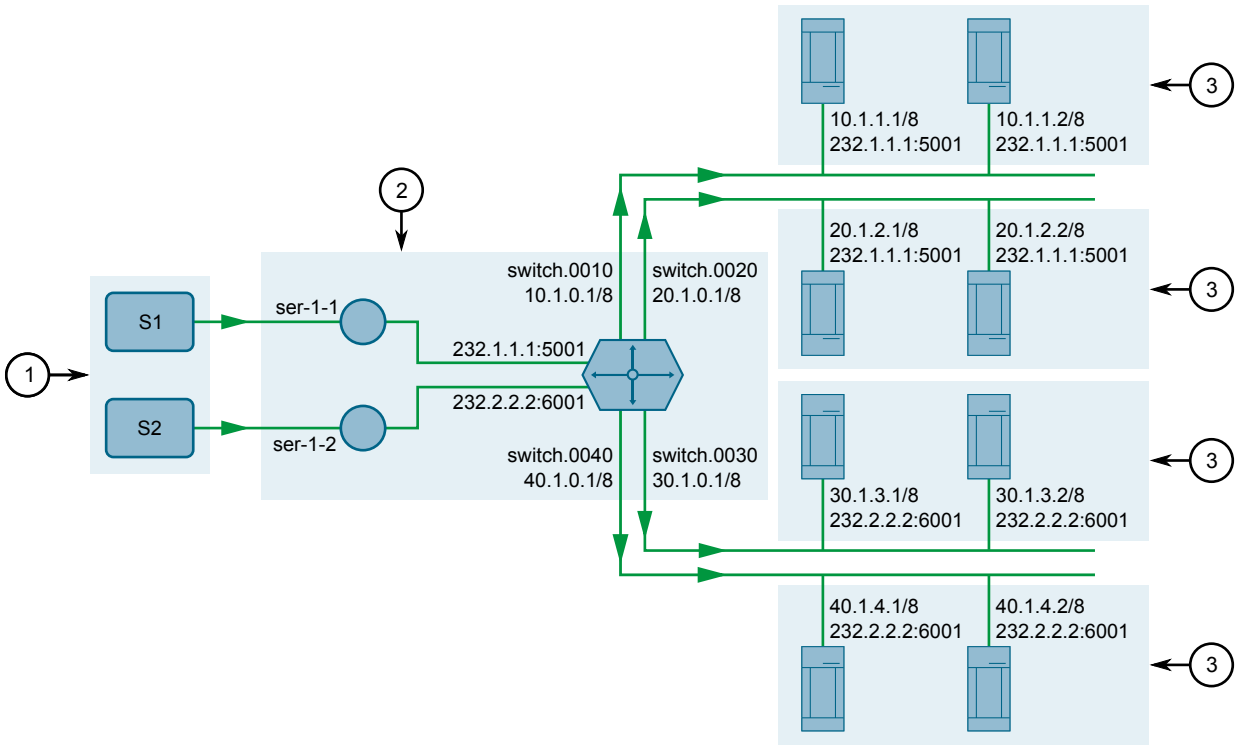


Figure 445: Topology - Serial Interfaces Configured as a Source for Multicast Streams

1. Serial Devices **2.** Source Device (RUGGEDCOM RX1500) **3.** Listeners

» Step 1: Configure ser-1-1

1. Configure IP addresses for the interfaces (switch.0010, switch.0020, switch.0030, and switch.0040). For more information, refer to Section 7.1.3.2, "Adding an IPv4 Address".
2. Create a raw socket connection for ser-1-1. For more information, refer to Section 10.2.3, "Adding a Serial Port Protocol".
3. Set the raw socket of the local port to 10001. For more information, refer to Section 10.2.6, "Configuring the Raw Socket Protocol".
4. Set the transport method to *UDP*. For more information, refer to Section 10.2.6, "Configuring the Raw Socket Protocol".
5. Set the multicast group for the remote host to 232.1.1.1 and the UDP destination port to 5001. For more information, refer to Section 10.5.2, "Adding a Remote Host".
6. Set *switch.0010* and *switch.0020* as the interfaces for the remote host. For more information, refer to Section 10.7.2, "Adding a Remote Host Interface"
7. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.

» Step 2: Configure ser-1-2

1. Create a raw socket connection for ser-1-2. For more information, refer to Section 10.2.3, "Adding a Serial Port Protocol".
2. Set the raw socket of the local port to 10002. For more information, refer to Section 10.2.6, "Configuring the Raw Socket Protocol".
3. Set the transport method to *UDP*. For more information, refer to Section 10.2.6, "Configuring the Raw Socket Protocol".
4. Set the multicast group for the remote host to 232.2.2.2 and the UDP destination port to 6001. For more information, refer to Section 10.5.2, "Adding a Remote Host".
5. Set *switch.0030* and *switch.0040* as the interfaces for the remote host. For more information, refer to Section 10.7.2, "Adding a Remote Host Interface"
6. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
7. Verify the configuration by viewing the statistics collected on the serial ports. For more information, refer to Section 10.1.2, "Viewing Serial Port Statistics".

» Final Configuration Example

Serial Port 1 Configuration

```
serial lm1 1
  no alias
  protocols rawsocket
   setrawsocket local-port 10001
   setrawsocket transport udp
   setrawsocket remote-host 232.1.1.1 5001
    interface switch.0010
    !
    interface switch.0020
```

Serial Port 2 Configuration

```
serial lm1 2
  no alias
  protocols rawsocket
   setrawsocket local-port 10002
   setrawsocket transport udp
   setrawsocket remote-host 232.2.2.2 6001
    interface switch.0030
    !
    interface switch.0040
```

Section 10.4.5

Example: Serial Interfaces Configured as a Source and Sink for Multicast Streams

This configuration example shows ser-1-1 receiving data on the wire from S1, then creating multiple raw socket connections to send the data to both interfaces switch.0010 and switch.0020. This data is then packetized as multicast packets and sent to destination group 232.1.1.1 and destination UDP port 5001. Additionally, ser-1-1 forwards the same data stream to ser-1-2, which then sends the data to S2.

IMPORTANT!
The values shown are specific to the provided topology. Actual values can vary based on the user's configuration.

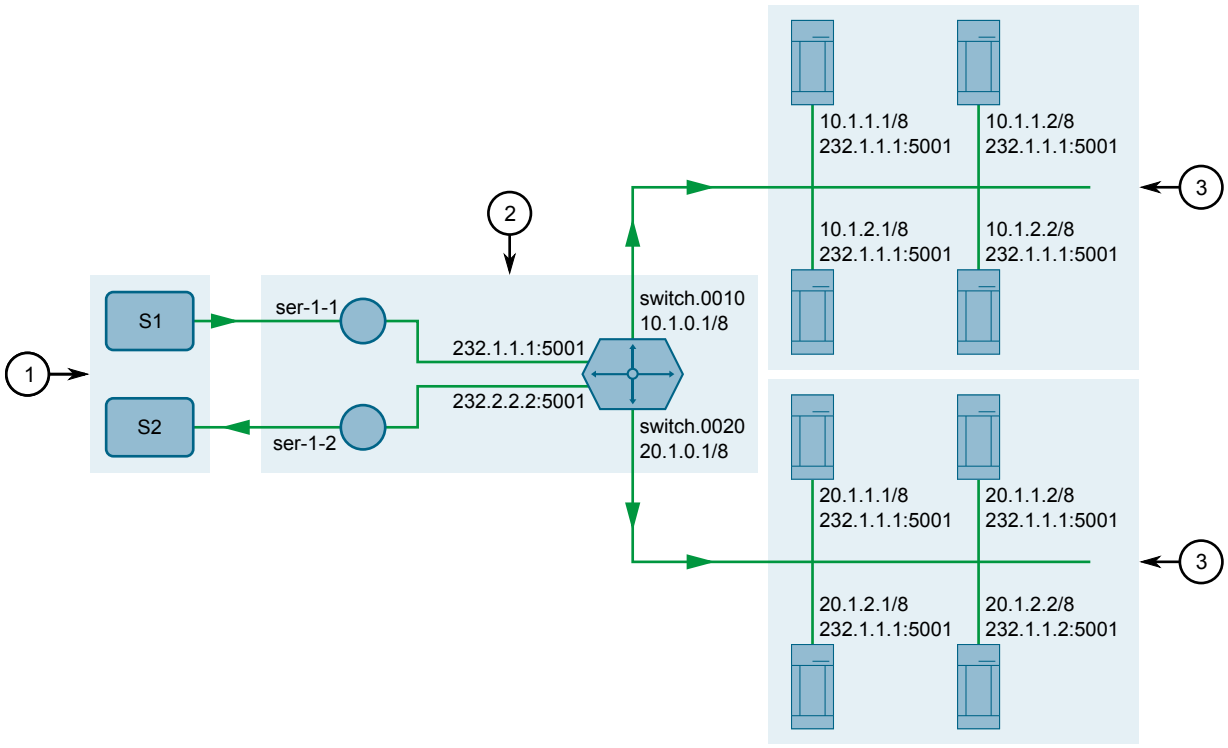


Figure 446: Topology - Serial Interfaces Configured as a Source and Sink for Multicast Streams

1. Serial Devices **2.** Source and Sink Device (RUGGEDCOM RX1500) **3.** Listeners **4.** Ethernet Network Interfaces

» Configure ser-1-1 and ser-1-2

1. Configure IP addresses for the interfaces (switch.0010 and switch.0020). For more information, refer to Section 7.1.3.2, "Adding an IPv4 Address".
2. Create a raw socket connection for ser-1-1. For more information, refer to Section 10.2.3, "Adding a Serial Port Protocol".
3. Set the raw socket of the local port to 10001. For more information, refer to Section 10.2.6, "Configuring the Raw Socket Protocol".
4. Set the transport method to *UDP*. For more information, refer to Section 10.2.6, "Configuring the Raw Socket Protocol".
5. Set the multicast group for the remote host to 232.1.1.1 and the UDP destination port to 5001. For more information, refer to Section 10.5.2, "Adding a Remote Host".
6. Set *switch.0010* and *switch.0020* as the interfaces for the remote host. For more information, refer to Section 10.7.2, "Adding a Remote Host Interface"
7. Enable remote host loopback. For more information, refer to Section 10.6.2, "Adding a Local Host"

8. Create a raw socket connection for ser-1-2. For more information, refer to Section 10.2.3, "Adding a Serial Port Protocol"
9. Set the raw socket of the local port to 5001. This must be the same as the UDP destination port of the multicast remote host configured for ser-1-1. For more information, refer to Section 10.6.2, "Adding a Local Host"
10. Set the transport method to *UDP*. For more information, refer to Section 10.2.6, "Configuring the Raw Socket Protocol".
11. Set the multicast group for the local host to 232.1.1.1. This must be the same as the destination multicast group configured for the multicast remote host configured for ser-1-1. For more information, refer to Section 10.6.2, "Adding a Local Host"
12. Enable local host loopback to indicate multicast messages are expected to arrive from another serial interface. For more information, refer to Section 10.6.2, "Adding a Local Host"
13. Click **Commit** to save the changes or click **Revert All** to abort. A confirmation dialog box appears. Click **OK** to proceed.
14. Verify the configuration by viewing the statistics collected on the serial ports. For more information, refer to Section 10.1.2, "Viewing Serial Port Statistics".

Final Configuration Example

Serial Port 1 Configuration

```
serial lm1 1
  no alias
  protocols rawsocket
   setrawsocket local-port 10001
   setrawsocket transport udp
   setrawsocket remote-host 232.1.1.1 5001
    loopback true
    interface switch.0010
    !
    interface switch.0020
```

Serial Port 2 Configuration

```
serial lm1 2
  no alias
  protocols rawsocket
   setrawsocket local-port 5001
   setrawsocket transport udp
   setrawsocket local-host 232.1.1.1
    loopback true
```

Section 10.5

Managing Remote Hosts

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

CONTENTS

- Section 10.5.3, “Deleting a Remote Host”

Section 10.5.1
Viewing a List of Remote Hosts

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

Figure 447: Remote Host Configuration Table

If no remote hosts have been configured, add hosts as needed. For more information, refer to Section 10.5.2, “Adding a Remote Host”.

Section 10.5.2
Adding a Remote Host

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

NOTE
A maximum of two multicast remote host entries are permitted per serial interface.

1. 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 local-host>**. The **Key Settings** form appears.

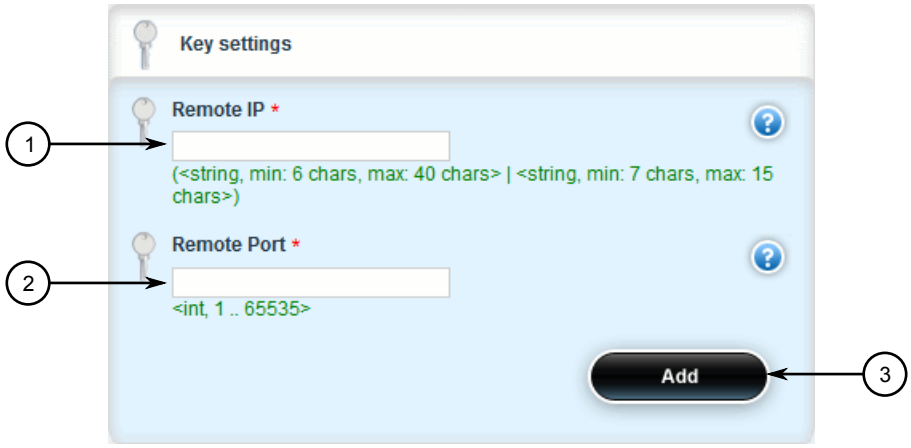


Figure 448: Key Settings Form

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

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

Parameter	Description
Remote IP	**Synopsis:** A string 7 to 15 characters long or a string 6 to 40 characters long The IP address of the remote host or destination multicast group.
Remote Port	**Synopsis:** A 32-bit signed integer between 1 and 65535 The transport port of the remote host or destination multicast group.

5. Click **Add** to create the remote host. The **Remote Host Configuration** form appears.

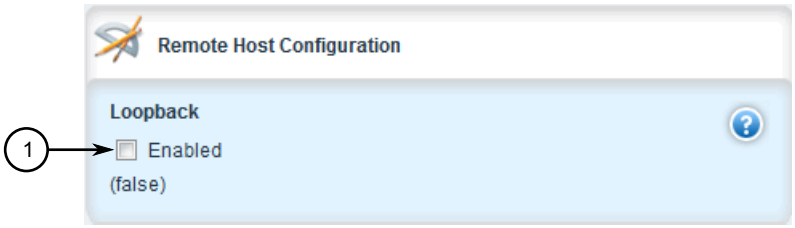


Figure 449: Remote Host Configuration

1. Loopback Check Box

6. [Optional] Add a remote host interface. For more information, refer to Section 10.7.2, "Adding a Remote Host 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 10.5.3
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.

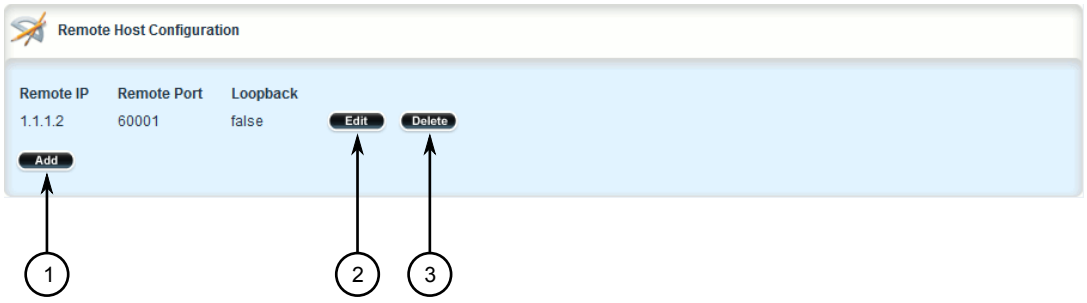


Figure 450: Remote Host Configuration Table

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

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 10.6
Managing Local Hosts

Local hosts are required when the UDP transport connection protocol is selected and multicast streams are to be received for the raw socket protocol.

CONTENTS

Section 10.6.1
Viewing a List of Local Hosts

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

Figure 451: Local Host Configuration Table

If no local hosts have been configured, add hosts as needed. For more information, refer to Section 10.6.2, "Adding a Local Host".

Section 10.6.2
Adding a Local Host

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

NOTE
A maximum of two multicast local host entries are permitted per serial interface.

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

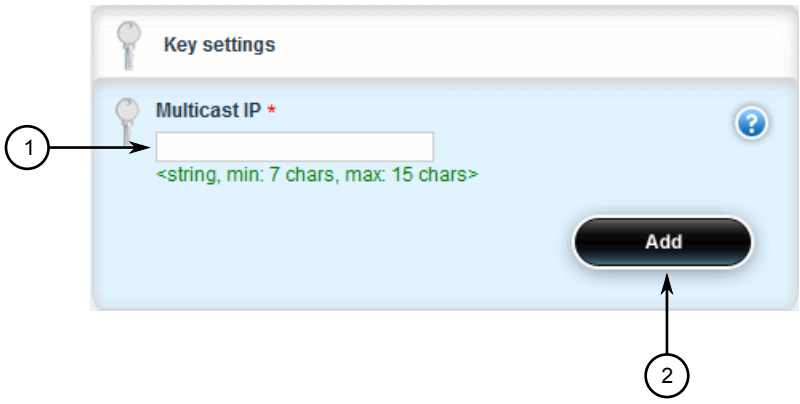


Figure 452: Key Settings Form

1. Multicast IP Box

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

Parameter	Description
Multicast IP	**Synopsis:** A string 7 to 15 characters long The source multicast group IP address (2xx.xxx.xxx.xxx) of the local host. The listening UDP port for the multicast group implicitly uses the local port number defined for the serial port.

5. Click **Add**. The **Local Host Configuration** form appears.

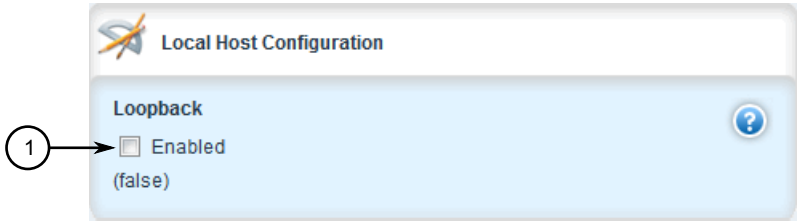


Figure 453: Local Host Configuration

1. Loopback Check Box

NOTE
When a local host is added, either loopback must be enabled or a local host interface must be added.

6. If a local host interface is required, proceed to Step 7. Otherwise, select **Loopback** to enable the local host to receive data from a loopback interface.

   The loopback interface must have the same source multicast group IP address and local port number as the serial port. A matching remote host with loopback enabled must also be configured.

7. [Optional] Add a local host interface. For more information, refer to Section 10.8.2, "Adding a Local Host 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 10.6.3
Deleting a Local Host

To delete a local host, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to ***interface » serial » {interface} » protocols » rawsocket » setrawsocket » local-host***, where *{interface}* is the slot name and port number of the serial port. The **Local Host Configuration** table appears.

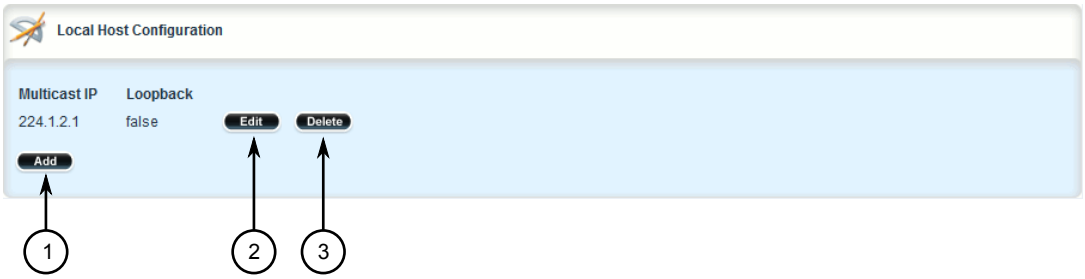


Figure 454: Local Host Configuration Table

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

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 10.7

Managing Remote Host Interfaces

Remote host interfaces are required when the UDP transport connection protocol is selected for the raw socket protocol and when the remote host is a multicast stream.

CONTENTS

Section 10.7.1

Viewing a List of Remote Host Interfaces

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

Figure 455: Interface Table

If no remote host interfaces have been configured, add interfaces as needed. For more information, refer to Section 10.7.2, "Adding a Remote Host Interface".

Section 10.7.2

Adding a Remote Host Interface

NOTE
A maximum of ten interfaces are permitted for each remote host.

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

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

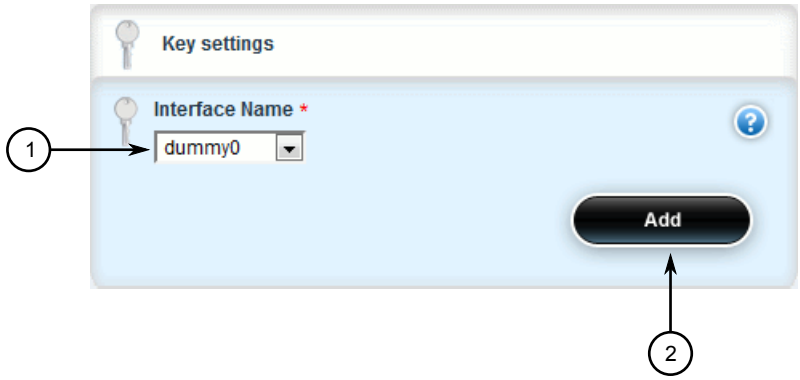


Figure 456: Key Settings Form

1. Interface Name Box **2.** Add Button

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

Parameter	Description
Interface Name	**Synopsis:** A string The transmitting interface's name for the destination multicast group IP address and remote port.

5. Click **Add** to add the interface to 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 10.7.3
Deleting a Remote Host Interface

To delete a remote host interface, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. ***interface » serial » {interface} » protocols » rawsocket » setrawsocket » remote-host » {remote-host} » interface***, where *{interface}* is the slot name and port number of the serial port and *{remote-host}* is the multicast streaming remote host. The **Interface** table appears.

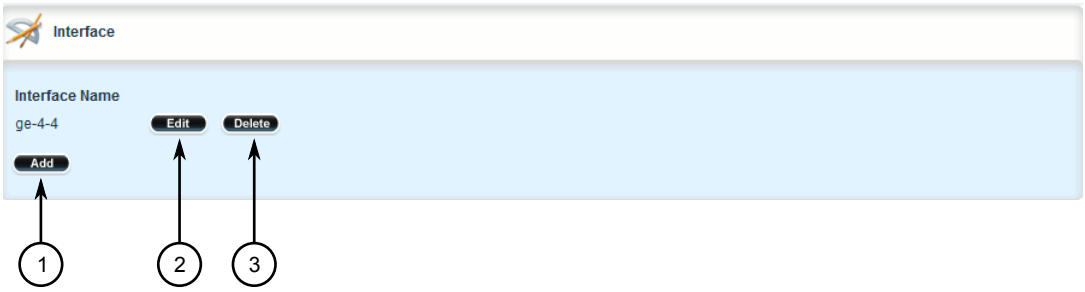


Figure 457: Interface Table

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 10.8
Managing Local Host Interfaces

Local host interfaces are required when the UDP transport connection protocol is selected for the raw socket protocol and when a local host is configured.

CONTENTS

Section 10.8.1
Viewing a List of Local Host Interfaces

To view a list of local host interfaces configured for a serial port using the raw socket protocol, navigate to ***interface » serial » {interface} » protocols » rawsocket » setrawsocket » local-host » {local-host} » interface***, where *{interface}* is the slot name and port number of the serial port and *{local-host}* is the multicast streaming local host. If interfaces have been configured, the **Interface** table appears.

Figure 458: Interface Table

If no local host interfaces have been configured, add interfaces as needed. For more information, refer to Section 10.8.2, "Adding a Local Host Interface".

Section 10.8.2
Adding a Local Host Interface

NOTE
A maximum of two interfaces are permitted for each local host.

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

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

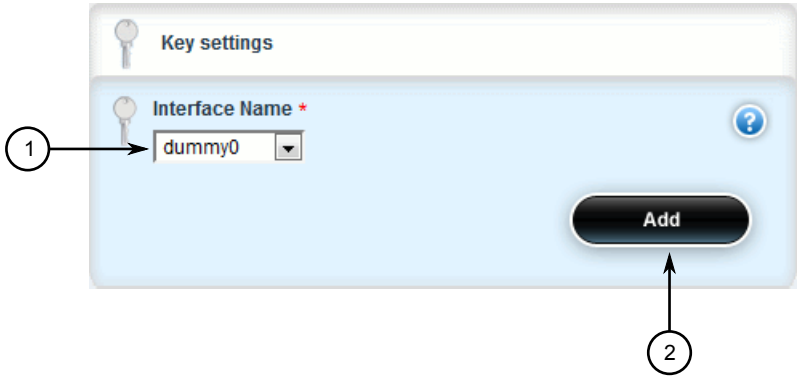


Figure 459: Key Settings Form

1. Interface Name Box **2.** Add Button

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

Parameter	Description
Interface Name	**Synopsis:** A string The receiving interface's name for the source multicast group IP address and the local port number defined for the serial port.

5. Click **Add** to add the interface to the local 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 10.8.3

Deleting a Local Host Interface

To delete a local host interface, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. ***interface » serial » {interface} » protocols » rawsocket » setrawsocket » local-host » {local-host} » interface***, where *{interface}* is the slot name and port number of the serial port and *{local-host}* is the multicast streaming local host. The **Interface** table appears.

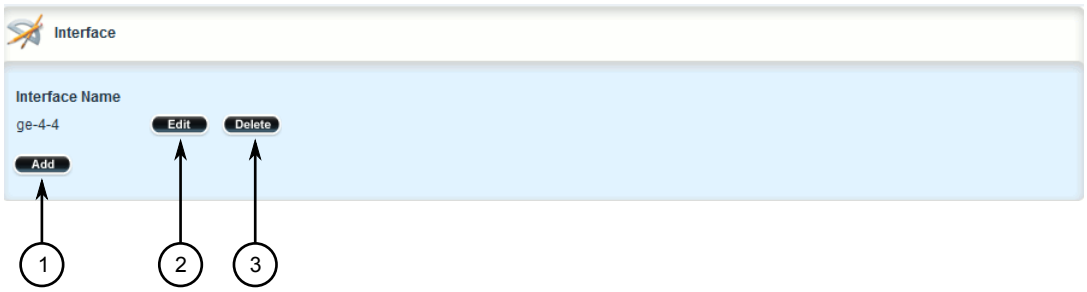


Figure 460: Interface Table

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.

11 Wireless

This chapter describes how to configure and manage the various wireless interfaces and utilities available in RUGGEDCOM ROX II.

NOTE
Some wireless features require the device to be equipped with a specific line module.

CONTENTS

Section 11.1

Managing WAN Interfaces

This section describes how to configure an interface to a Wide Area Network (WAN).

CONTENTS

Section 11.1.1
Viewing a List of WAN Interfaces

To view a list of WAN interfaces, navigate to ***interface » wan***. The **WAN Slot Port Settings** table appears.

Figure 461: WAN Slot Port Settings Table

Section 11.1.2
Configuring a WAN Interface

To configure a WAN interface, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to ***interface » wan » {interface}***, where *{interface}* is the WAN interface. The **Enable WAN Interface** form appears.

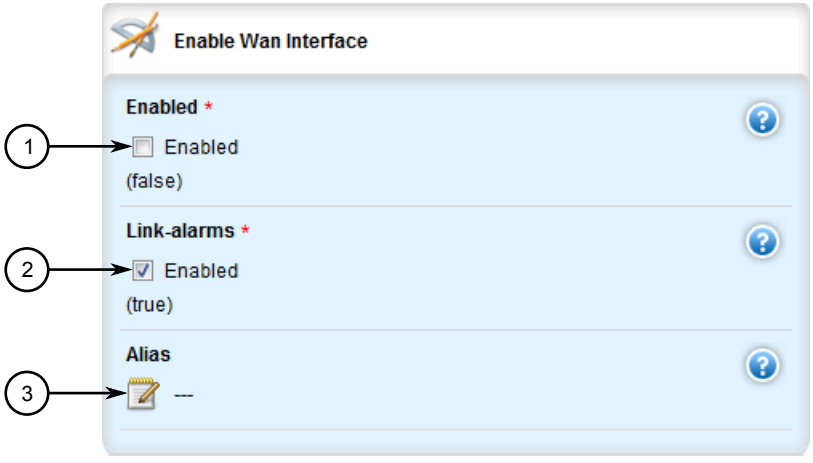


Figure 462: Enable WAN Interface Form

1. Enabled Check Box **2.** Link Alarms Check Box **3.** Alias Box

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

Parameter	Description
slot	**Synopsis:** { sm, lm1, lm2, lm3, lm4, lm5, lm6, swport, eth, serport, celport, wlanport } The name of the module location for the WAN card.
port	**Synopsis:** A 32-bit signed integer between 1 and 16 The port number on the WAN card.
enabled	**Synopsis:** { true, false } **Default:** false Enables this WAN port.
Link Alarms	**Synopsis:** { true, false } **Default:** true Disabling link-alarms will prevent alarms and LinkUp and LinkDown SNMP traps from being sent for that interface. Link alarms may also be controlled for the whole system under admin / alarm-cfg.
alias	**Synopsis:** A string 1 to 64 characters long The SNMP alias name of the interface

4. Configure a T1 or E1 line. For more information, refer to Section 11.1.6, “Configuring a T1 Line” or Section 11.1.7, “Configuring an E1 Line”.
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 11.1.3
Viewing WAN Statistics

To view statistics for the WAN network, navigate to ***interfaces » wan » t1e1***. The **T1/E1 Statistics** form appears.

NOTE
Some statistics are only available for physical or logical interfaces.

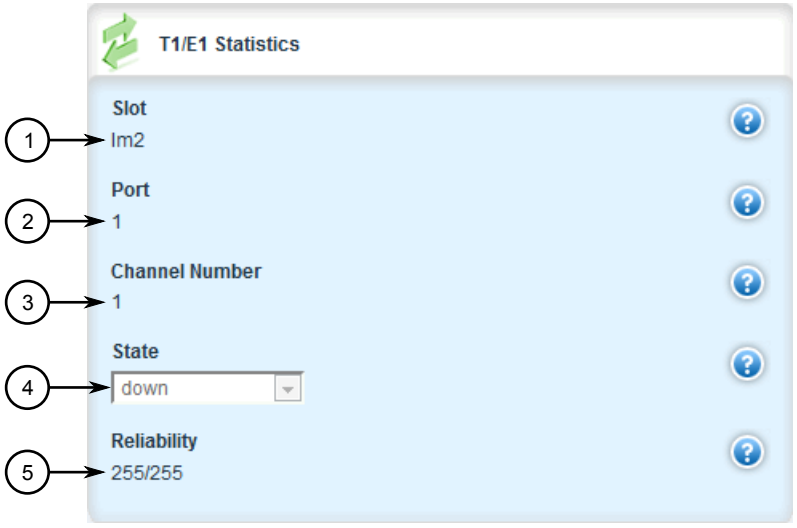


Figure 463: T1/E1 Statistics Form - Physical T1/E1 Interface

1. Slot **2.** Port **3.** Channel Number **4.** State **5.** Local **6.** Remote **7.** Mask **8.** Reliability

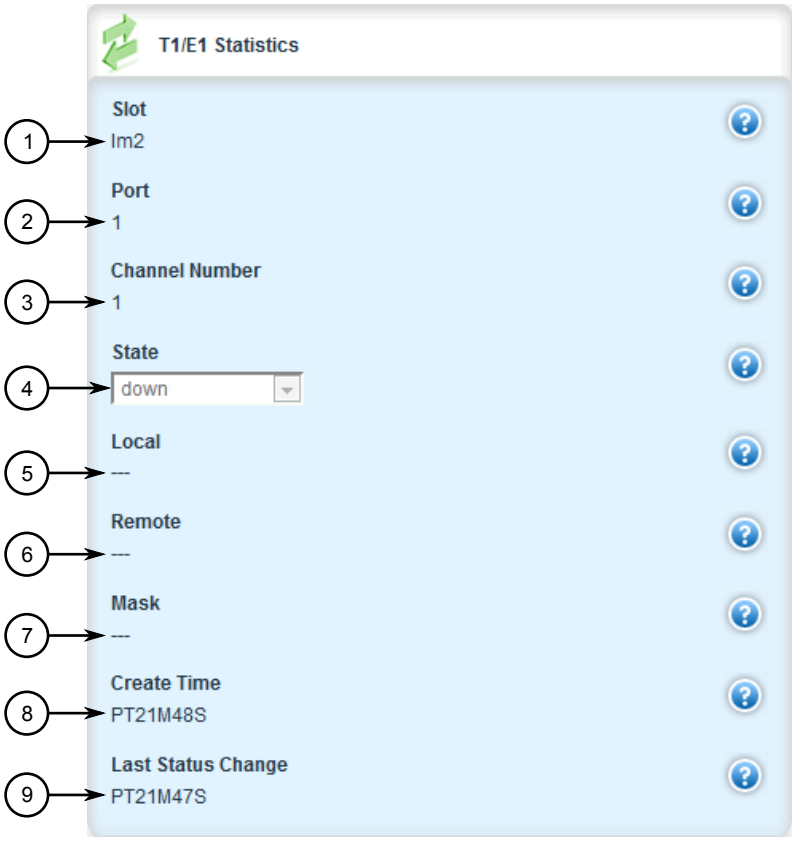


Figure 464: T1/E1 Statistics Form - Logical T1/E1 Interface

1. Slot **2.** Port **3.** Channel Number **4.** State **5.** Local **6.** Remote **7.** Mask **8.** Create Time **9.** Last Status Change

This form provides the following information:

Parameter	Description
name	**Synopsis:** A string 1 to 15 characters long Interface name.
slot	**Synopsis:** { sm, lm1, lm2, lm3, lm4, lm5, lm6, swport, eth, serport, celport, wlanport } or a string Line module name of the slot. This parameter is mandatory.
Port	**Synopsis:** a 32-bit signed integer between 1 and 16A string Port number on the slot. This parameter is mandatory.
Channel Number	**Synopsis:** a 32-bit signed integer between 1 and 32A string Channel number on the port. This parameter is mandatory.
state	**Synopsis:** { not set, up, down, testing, unknown, dormant, notPresent, lowerLayerDown } Status of the interface. This parameter is mandatory.
local	**Synopsis:** A string Loacal IP address of the interface.
remote	**Synopsis:** A string Peer IP address.
mask	**Synopsis:** A string Netmask.
Reliability	**Synopsis:** A string Reliability of the interface over 5 minutes. It is calculated as an exponential average of the fraction of the total received and transmitted errors and the total packets that are received and transmitted successfully. This parameter is mandatory.
Create Time	**Synopsis:** A string The duration of time since interface is created. This parameter is mandatory.
Last Status Change	**Synopsis:** A string The duration of time since last change of interface status. This parameter is mandatory.
Frames	**Synopsis:** A 32-bit unsigned integer The number of frames received. This parameter is mandatory.
Bytes	**Synopsis:** A 32-bit unsigned integer The number of bytes received. This parameter is mandatory.
Frames Discarded as Link Inactive	**Synopsis:** A 32-bit unsigned integer Received frames that were discarded (link inactive). This parameter is mandatory.

Parameter	Description
Load	**Synopsis:** A string Receive load over 5 minutes. It is calculated as an exponential average over 5 minutes of the fraction of the received bits per seconds and the interface bandwidth configured. This parameter is mandatory.
Frames	**Synopsis:** A 32-bit unsigned integer The number of frames transmitted. This parameter is mandatory.
Bytes	**Synopsis:** A 32-bit unsigned integer The number of bytes transmitted. This parameter is mandatory.
Realigned	**Synopsis:** A 32-bit unsigned integer Transmits frames that were realigned. This parameter is mandatory.
Load	**Synopsis:** A string Transmit load over 5 minutes. It is calculated as an exponential average over 5 minutes of the fraction of the transmitted bits per seconds and the interface bandwidth configured. This parameter is mandatory.
Overrun	**Synopsis:** A 32-bit unsigned integer The number of receiver overrun errors. This parameter is mandatory.
CRC Error	**Synopsis:** A 32-bit unsigned integer The number of receiver CRC errors. This parameter is mandatory.
Abort	**Synopsis:** A 32-bit unsigned integer The number of receiver abort errors. This parameter is mandatory.
Corruption	**Synopsis:** A 32-bit unsigned integer The number of receiver corruption errors. This parameter is mandatory.
PCI Error	**Synopsis:** A 32-bit unsigned integer The number of receiver PCI errors. This parameter is mandatory.
DMA Error	**Synopsis:** A 32-bit unsigned integer The number of receiver DMA descriptor errors. This parameter is mandatory.
length_errors	**Synopsis:** A 32-bit unsigned integer Length errors. This parameter is mandatory.
frame_errors	**Synopsis:** A 32-bit unsigned integer Frame errors. This parameter is mandatory.
PCI Error	**Synopsis:** A 32-bit unsigned integer

Parameter	Description
	The number of transmitter PCI errors. This parameter is mandatory.
PCI Latency Warning	**Synopsis:** A 32-bit unsigned integer The number of transmitter PCI latency warnings. This parameter is mandatory.
DMA Error	**Synopsis:** A 32-bit unsigned integer The number of transmitter DMA descriptor errors. This parameter is mandatory.
DMA Length Error	**Synopsis:** A 32-bit unsigned integer The number of transmitter DMA descriptor length errors. This parameter is mandatory.
Abort	**Synopsis:** A 32-bit unsigned integer Abort errors. This parameter is mandatory.
txcarrier_errors	**Synopsis:** A 32-bit unsigned integer Carrier errors. This parameter is mandatory.
alos	**Synopsis:** A string ALOS (Loss of Signal) alarm. This parameter is mandatory.
los	**Synopsis:** A string LOS (Loss Of Signal) alarm. This parameter is mandatory.
red	**Synopsis:** A string RED (red alarm is a combination of a LOS or an OOF failure) alarm. This parameter is mandatory.
ais	**Synopsis:** A string AIS (Alarm Indication Signal) alarm. This parameter is mandatory.
oof	**Synopsis:** A string OOF (Out Of Frame) alarm. This parameter is mandatory.
rai	**Synopsis:** A string RAI (Remote Alarm Indication) alarm. This parameter is mandatory.
Bytes	**Synopsis:** A 64-bit unsigned integer Number of bytes received. This parameter is mandatory.
Packets	**Synopsis:** A 64-bit unsigned integer Number of packets received. This parameter is mandatory.

Parameter	Description
Errors	**Synopsis:** A 32-bit unsigned integer Number of error packets received. This parameter is mandatory.
Dropped	**Synopsis:** A 32-bit unsigned integer Number of packets dropped. This parameter is mandatory.
Bit Rate	**Synopsis:** A 32-bit unsigned integer 5 minutes interval receiving bit rate (bits/sec). This parameter is mandatory.
Packet Rate	**Synopsis:** A string 5 minutes interval receiving packet rate (packets/sec). This parameter is mandatory.
Bytes	**Synopsis:** A 64-bit unsigned integer Number of bytes transmitted. This parameter is mandatory.
Packets	**Synopsis:** A 64-bit unsigned integer Number of packets transmitted. This parameter is mandatory.
Errors	**Synopsis:** A 32-bit unsigned integer Number of error packets. This parameter is mandatory.
Dropped	**Synopsis:** A 32-bit unsigned integer Number of packets dropped. This parameter is mandatory.
Collision	**Synopsis:** A 32-bit unsigned integer Number of collisions detected. This parameter is mandatory.
Bit Rate	**Synopsis:** A 32-bit unsigned integer 5 minutes interval transmitting bit rate (bits/sec). This parameter is mandatory.
Packet Rate	**Synopsis:** A string 5 minutes interval transmitting packet rate (packets/sec). This parameter is mandatory.

For information about clearing the WAN statistics, refer to Section 11.1.4, “Clearing WAN Statistics”.

Section 11.1.4
Clearing WAN Statistics

The following describes how to clear the statistics collected when WAN interfaces are enabled. All of the statistics or only those for a interface can be cleared.

To clear the statistics, do the following:

1. Navigate to ***interfaces » wan*** and click **clearstatistics** in the menu. The **Clear Interface Statistics** and **Trigger Action** forms appear.

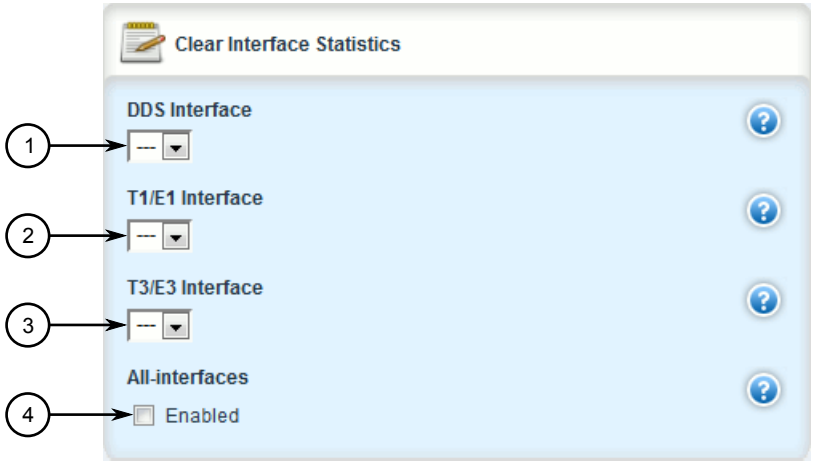


Figure 465: Clear Interface Statistics Form

1. DDS Interface List **2.** T1/E1 Interface List **3.** T3/E3 Interface List **4.** All Interfaces CheckBox

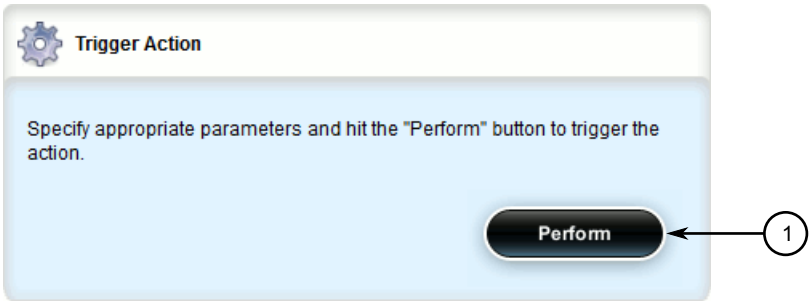


Figure 466: Trigger Action Form

1. Perform Button

2. On the **Clear Interface Statistics** form, configuring the following parameter(s):

Parameter	Description
DDS Interface	**Synopsis:** A string Select the DDS interface for which to clear statistics.
T1/E1 Interface	**Synopsis:** A string Select the T1E1 interface for which to clear statistics.
T3/E3 Interface	**Synopsis:** A string Select T3E3 interface for which to clear statistics.
All Interfaces	Clear statistics for all WAN interfaces.

3. On the **Trigger Action** form, click **Perform** to clear the statistics.

Section 11.1.5

Performing a Loopback Test

Loopback tests are a useful means of testing the T1/E1 hardware on the device and the T1/E1 connection with remote devices. Three types of tests are available:

- Digital Loopback – RUGGEDCOM ROX II digitally sends frames and immediately returns them to the device. This test is used to isolate problems within the T1/E1 circuit.
- Remote Loopback – RUGGEDCOM ROX II transmits frames to the Tx port and compares them with frames received on the Rx port. A loopback plug or cable must be installed on the T1/E1 port. This test is used to isolate problems within the WAN module.
- Line Loopback – RUGGEDCOM ROX II transmits frames across the T1/E1 line to a remote Channel Service Unit/ Data Service Unit (CSU/DSU). This test determines if a problem exists outside the device.

Regardless of the loopback type, a loopback test is successful if the frames received match those that were sent. Missing frames and frames that contain discrepancies indicate a potential problem in the T1/E1 hardware or line.

To perform a loopback test on a WAN interface, do the following:

IMPORTANT!
Performing a loopback test on an active interface will immediately cause it to go down. However, the trunk will be automatically initialized after the test is complete.

1. Make sure a WAN interface has been configured. For more information, refer to Section 11.1.2, "Configuring a WAN Interface".
2. Navigate to ***interfaces » wan*** and click **loopback** in the menu. The **Loopback Test** and **Trigger Action** forms appear.

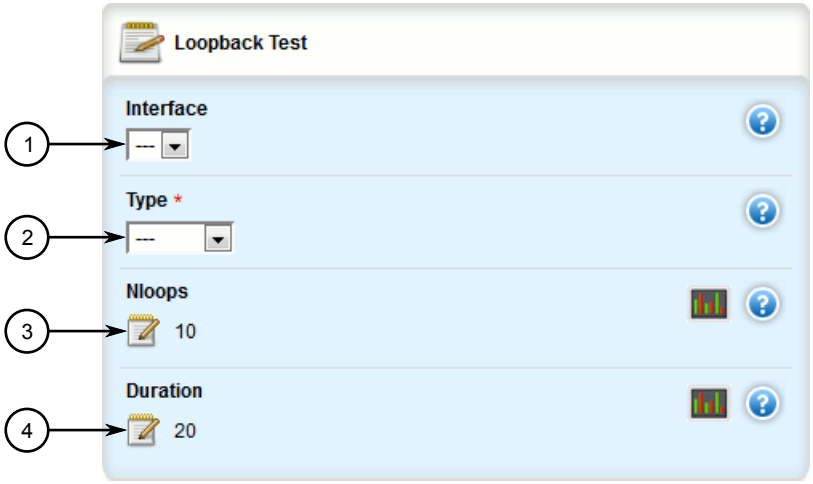


Figure 467: Loopback Test Form

1. Interface List **2.** Type List **3.** Nloops Box **4.** Duration Box

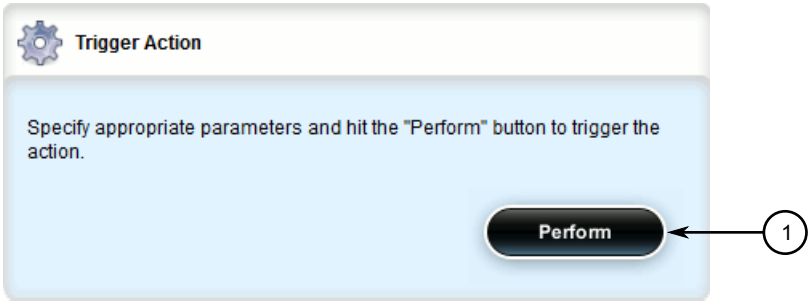


Figure 468: Trigger Action Form

1. Perform Button

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

Parameter	Description
Interface	**Synopsis:** A string Physical interface name.
Type	**Synopsis:** { digital, remote, line } The loopback type. This parameter is mandatory.
Number of Loops	**Synopsis:** A 32-bit signed integer between 1 and 200 **Default:** 10 The number of loops.
Duration	**Synopsis:** A 32-bit signed integer between 1 and 240 **Default:** 20 The number of seconds required to run the test.

4. On the **Trigger Action** form, click **Perform**. The results are displayed when the test is complete.

Section 11.1.6
Configuring a T1 Line

To configure a T1 line for a WAN interface, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to ***interface » wan » {interface}***, where *{interface}* is the WAN interface.
3. Click the **+** symbol in the menu next to **t1**. The **T1 Parameters** form appears.

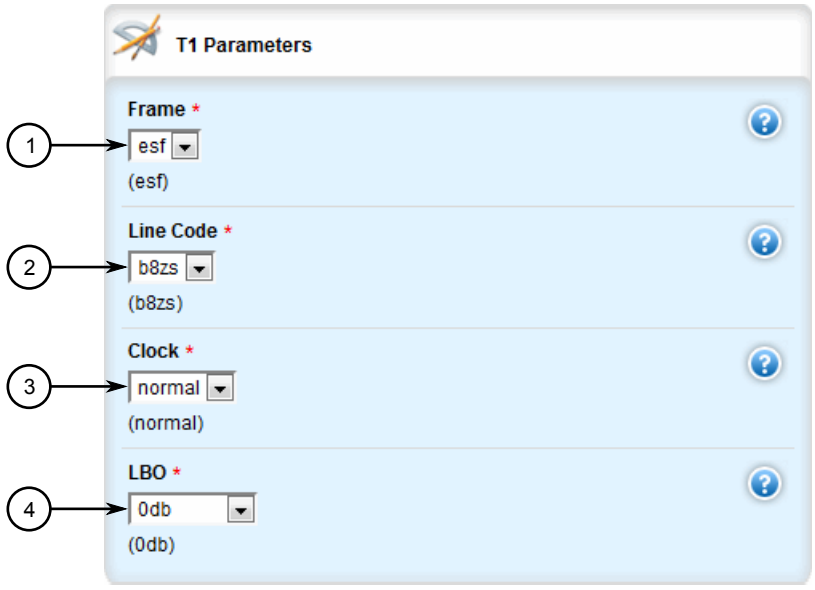


Figure 469: T1 Parameters Form

1. Frame List **2.** Line Code List **3.** Clock List **4.** LBO List

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

Parameter	Description
frame	**Synopsis:** { esf } **Default:** esf The frame format.
Line Code	**Synopsis:** { b8zs } **Default:** b8zs The line encoding/decoding scheme.
clock	**Synopsis:** { normal, master } **Default:** normal Serial clocking mode: master or normal. • master : provide serial clock signal. • normal : accept external clock signal.
LBO	**Synopsis:** { 0db, 7.5db, 15db, 22.5db, 0-110ft, 110-220ft, 220-330ft, 330-440ft, 440-550ft, 550-660ft } **Default:** 0db Line Build Out: tunes the shape of the T1 pulses and adjusts their amplitude depending upon distances and the desired attenuation.

5. Add and configure channels for the T1 line. For more information, refer to Section 11.1.9.2, "Adding a Channel".
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 11.1.7

Configuring an E1 Line

To configure E1 parameters for a WAN interface, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to ***interface » wan » {interface}***, where *{interface}* is the WAN interface.
3. Click the **+** symbol in the menu next to **e1**. The **E1 Parameters** form appears.

Figure 470: E1 Parameters Form

1. Frame List **2.** Line Code List **3.** Clock List

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

Parameter	Description
frame	**Synopsis:** { ncrc4, crc4 } **Default:** ncrc4 The frame format.
Line Code	**Synopsis:** { hdb3 } **Default:** hdb3 A line encoding/decoding scheme.
clock	**Synopsis:** { normal, master } **Default:** normal Serial clocking mode: master or normal. • master : provide serial clock signal. • normal : accept external clock signal.

5. Add and configure channels for the E1 line. For more information, refer to Section 11.1.9.2, "Adding a Channel".
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 11.1.8
Configuring DDS

To configure DDS for a WAN interface, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to ***interface » wan » {interface}***, where *{interface}* is the WAN interface.
3. Click the **+** symbol in the menu next to **DDS** to enable DDS.
4. Click the **+** symbol in the menu next to **ddsparams**. The **DDS Parameters** form appears.

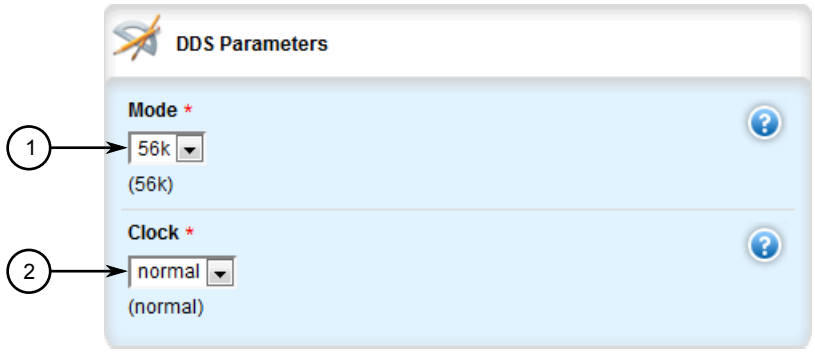


Figure 471: DDS Parameters Form

1. Mode List **2.** Clock List

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

Parameter	Description
mode	**Synopsis:** { 56k, 64k } **Default:** 56k DDS speed mode (kbps).
clock	**Synopsis:** { normal, master } **Default:** normal Serial clocking mode: master or normal. • master : provide serial clock signal. • normal : accept external clock signal.

6. Configure a PPP or frame relay connection. For more information, refer to Section 11.1.12, "Configuring a PPP Connection" or Section 11.1.13, "Configuring a Frame Relay Connection".
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 11.1.9
Managing Channels

This section describes how to create and manage channels for a T1/E1 WAN interface.

CONTENTS

Section 11.1.9.1
Viewing a List of Channels

To view a list of channels configured for a T1/E1 interface, navigate to ***interface » wan » {interface} » {protocol} » channel***, where *{interface}* is the WAN interface and *{protocol}* is either T1 or E1. If channels have been configured, the **Channels and Associated Time Slots** table appears.

Figure 472: T1 Channels and Associated Time Slots Table (Example)

If no channels have been configured, add channels as needed. For more information, refer to Section 11.1.9.2, "Adding a Channel".

Section 11.1.9.2
Adding a Channel

To configure a channel for a T1/E1 physical interface, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to ***interface » wan » {interface} » {protocol} » channel***, where *{interface}* is the WAN interface and *{protocol}* is either T1 or E1.
3. Click **<Add channel>**. The **Key Settings** form appears.

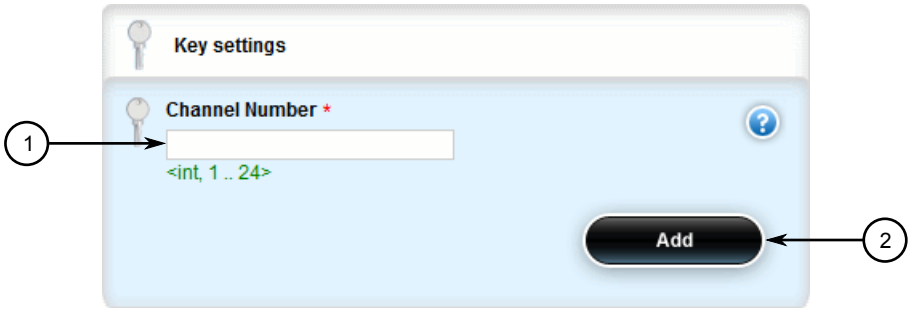


Figure 473: Key Settings Form

1. Channel Number Box **2.** Add Button

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

Parameter	Description
Channel Number	**Synopsis:** A 32-bit signed integer between 1 and 24 Channel Number.

5. Click **Add** to create the new channel. The **T1/E1 Time Slot Settings** form appears.

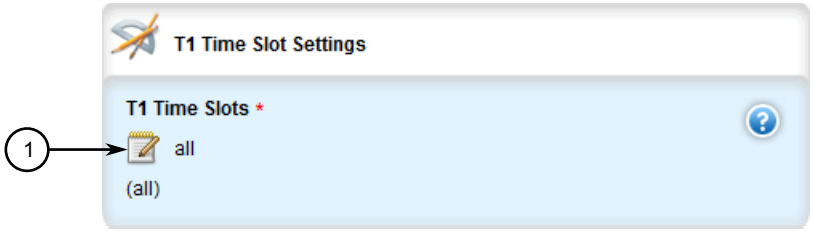


Figure 474: T1 Time Slot Settings Form

1. T1 Time Slots Box

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

Parameter	Description
T1 Time Slots	**Synopsis:** A string 0 to 128 characters long **Default:** all Time slots for this channel. Format: the string 'all', or a comma-separated list of numbers in the range of 1 to 24. To specify a range of numbers, separate the start and end of the range with '..' or with a hyphen '-' Example 1: 1,2,3 and 1..3 both represent time slots 1 through 3. Example 2: 1,2,5..10,11 represents time slots 1, 2, 5, 6, 7, 8, 9, 10, and 11.

7. If necessary, configure VLANs for an HDLC-ETH connection. For more information, refer to Section 11.1.15.2, "Adding an HDLC-ETH VLAN".
8. If necessary, configure an MLPPP connection. For more information, refer to Section 11.1.11, "Configuring a Multi Link PPP Connection".

9. If necessary, configure a PPP connection. For more information, refer to Section 11.1.12, "Configuring a PPP Connection".
10. If necessary, configure a frame relay connection. For more information, refer to Section 11.1.13, "Configuring a Frame Relay Connection".
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 11.1.9.3
Deleting a Channel

To delete a channel configured for a T1/E1 physical interface, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to ***interface » wan » {interface} » {protocol} » channel***, where *{interface}* is the WAN interface and *{protocol}* is either T1 or E1. The **T1/E1 Channels and Associated Time Slots** table appears.

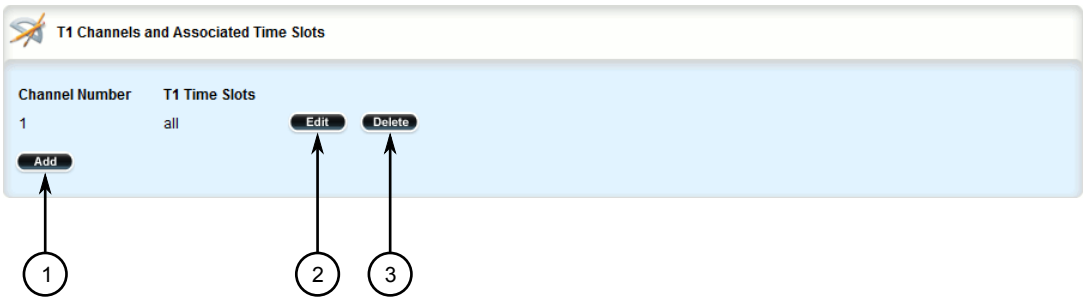


Figure 475: T1 Channels and Associated Time Slots Table

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

3. Click **Delete** next to the chosen serial 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 11.1.10
Configuring an HDLC-ETH Connection

HDLC-ETH refers to Ethernet over an HDLC (High-Level Data LInk Control) connection on a T1/E1 line. This connection passes Layer2 and Layer 3 packets from a LAN through a T1/E1 line by creating a virtual switch containing one or more Ethernet interfaces and an HDLC-ETH interface. For more information about configuring a virtual switch, refer to Section 12.2.2, "Adding a Virtual Switch".

A T1/E1 WAN interface configured for HDLC-ETH works like a routable Ethernet port, such as fe-cm-1 and switch.0001, which can be configured with an IP address and subnet mask. Since it acts the same as an Ethernet port, a peer IP address for an HDLC-ETH interface does not need to be configured.

Before adding an HDLC-ETH connection, a T1/E1 line must be in place. For more information, refer to:

- Section 11.1.6, "Configuring a T1 Line"
- Section 11.1.7, "Configuring an E1 Line"

To configure an HLDC-ETH connection for a T1 or E1 line, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to ***interface » wan » {interface} » {protocol} » channel » {number} » connection***, where *{interface}* is the WAN interface, *{parameter}* is either T1 or E1, and *{number}* is the channel number.
3. Click the **+** symbol in the menu next to **hdlc-eth**. The **Ethernet Over HDLC Settings** form appears.

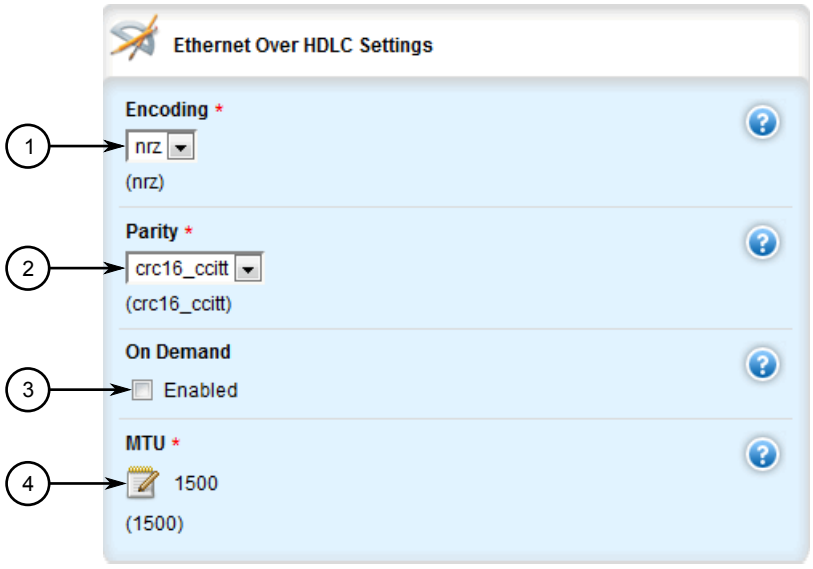


Figure 476: Ethernet Over HDLC Settings Form

1. Encoding List **2.** Parity List **3.** On Demand Check Box **4.** MTU Box

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

Parameter	Description
encoding	**Synopsis:** { nrz } **Default:** nrz HDLC encoding type
parity	**Synopsis:** { crc16_ccitt } **Default:** crc16_ccitt HDLC parity type
On Demand	This interface is up or down on demand of link fail over.
MTU	**Synopsis:** A 32-bit signed integer between 256 and 1500 **Default:** 1500 Maximum transmission unit (largest packet size allowed for this interface).

5. Add one or more VLANs for the HDLC-ETH connection. For more information, refer to Section 11.1.15.2, "Adding an HDLC-ETH VLAN".

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 11.1.11

Configuring a Multi Link PPP Connection

To configure a Multi Link Point-to-Point Protocol (MLPPP) connection for a T1 or E1 line, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to ***interface » wan » {interface} » {protocol} » channel » {number}*** , where *{interface}* is the WAN interface, *{protocol}* is either T1 or E1, and *{number}* is the channel number.
3. Click the **+** symbol in the menu next to **mlppp**. The **Multilink PPP** form appears.

Figure 477: Multilink PPP Form

1. Bundle Box **2.** On Demand Check Box **3.** MTU Box

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

Parameter	Description
bundle	**Synopsis:** A 32-bit signed integer between 1 and 50 **Default:** 1 The bundle number
On Demand	This interface is up or down on demand of link fail over.
MTU	**Synopsis:** A 32-bit signed integer between 256 and 1500 **Default:** 1500 Maximum transmission unit (largest packet size allowed for 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 11.1.12

Configuring a PPP Connection

To configure a Point-to-Point Protocol (PPP) connection, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Depending on the WAN module, navigate to either:
   - **For T1/E1 Lines**
     interface » wan » {interface} » {protocol} » channel » {number} » connection, where *{interface}* is the WAN interface, *{parameter}* is either T1 or E1, and *{number}* is the channel number.
   - **For DDS**
     interface » wan » {interface} » dds » connection, where *{interface}* is the WAN interface, *{parameter}* is either T1 or E1, and *{number}* is the channel number.
3. Click the **+** symbol in the menu next to **ppp**. The **PPP** form appears.

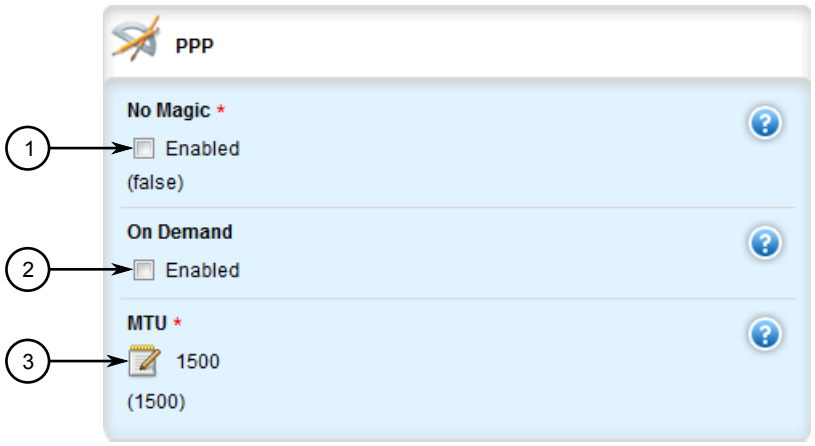


Figure 478: PPP Form

1. No Magic Check Box **2.** On Demand Check Box **3.** MTU Box

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

Parameter	Description
No Magic	**Synopsis:** { true, false } **Default:** false Disables the Magic Number. (Valid on RX1000 only)
On Demand	This interface is up or down on demand of link fail over.
MTU	**Synopsis:** A 32-bit signed integer between 256 and 1500 **Default:** 1500 Maximum transmission unit (largest packet size allowed for 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 11.1.13

Configuring a Frame Relay Connection

To configure a frame relay connection for a T1 or E1 line, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Depending on the WAN module, navigate to either:
   - **For T1/E1 Lines**
     interface » wan » {interface} » {protocol} » channel » {number} » connection, where *{interface}* is the WAN interface, *{parameter}* is either T1 or E1, and *{number}* is the channel number.
   - **For DDS**
     interface » wan » {interface} » dds » connection, where *{interface}* is the WAN interface, *{parameter}* is either T1 or E1, and *{number}* is the channel number.
3. Click the **+** symbol in the menu next to **framerelay**. The **Frame Relay Parameters** form appears.

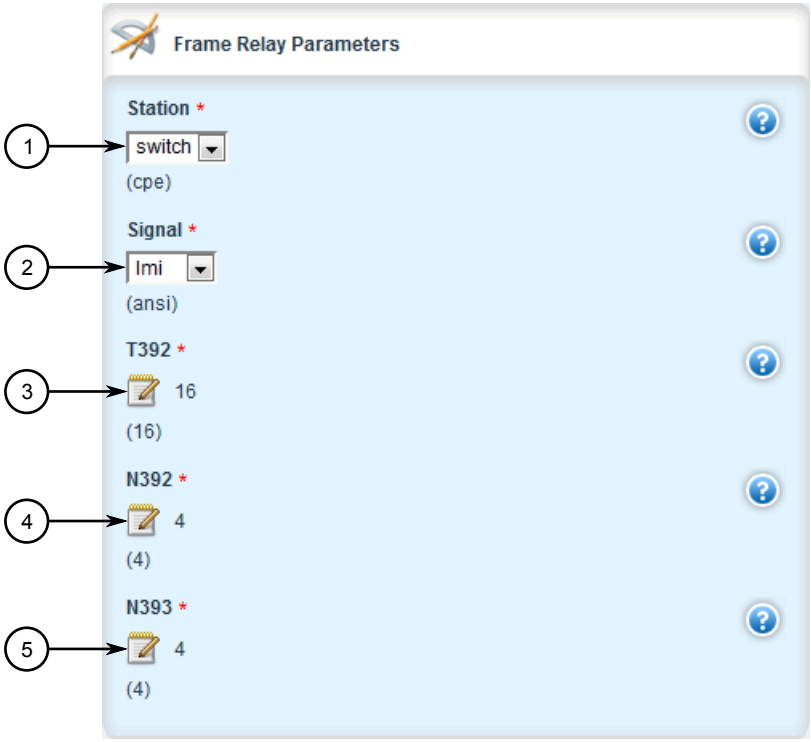


Figure 479: Frame Relay Parameters Form – Switch Selected

1. Station List **2.** Signal List **3.** T391 Box **4.** N391 Box **5.** N392 Box **6.** N393 Box

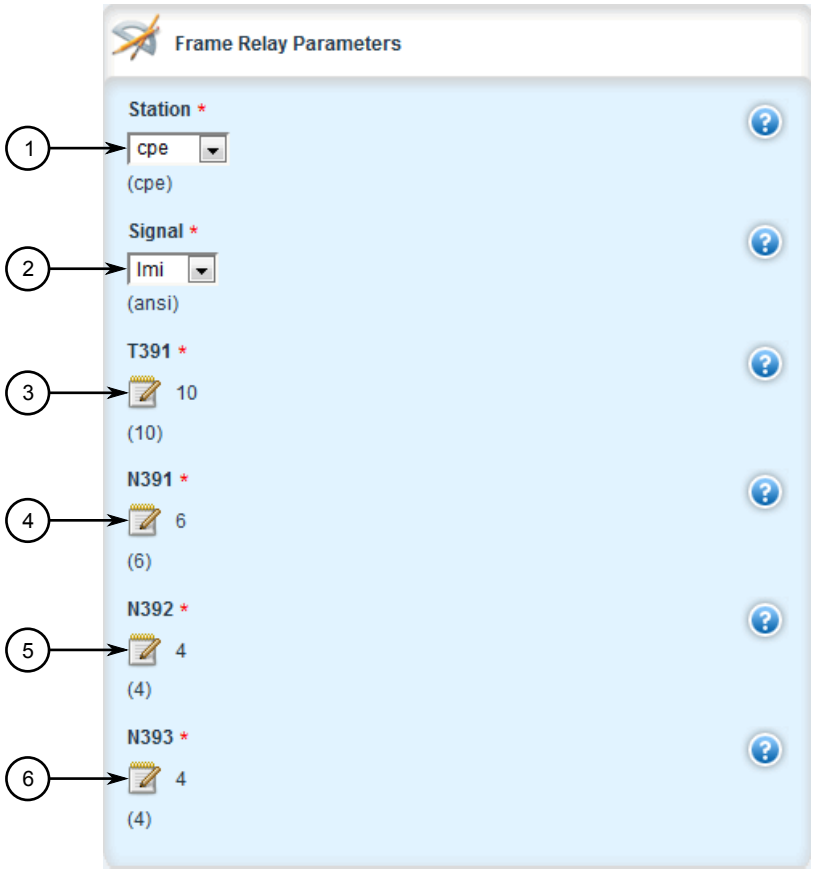


Figure 480: Frame Relay Parameters Form – CPE Selected

1. Station List **2.** Signal List **3.** T392 Box **4.** N392 Box **5.** N393 Box

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

Parameter	Description
station	**Synopsis:** { cpe, switch } **Default:** cpe The behavior of the frame relay connection, i.e. CPE (Customer Premises Equipment) or as a switch.
signal	**Synopsis:** { ansi, lmi, q933, none } **Default:** ansi The frame relay link management protocol used.
t391	**Synopsis:** A 32-bit signed integer between 5 and 30 **Default:** 10 (Link Integrity Verification polling) Indicates the number of seconds between transmission of in-channel signaling messages. Valid for cpe.
t392	**Synopsis:** A 32-bit signed integer between 5 and 30 **Default:** 16 (Verification of polling cycle) Indicates the expected number of seconds between reception of in-channel signaling messages transmitted by cpe. Valid for Switch.
n391	**Synopsis:** A 32-bit signed integer between 1 and 255

Parameter	Description
	Default: 6 Defines the frequency of transmission of full status enquiry messages. Valid for CPE.
n392	**Synopsis:** A 32-bit signed integer between 1 and 10 **Default:** 4 The number of error events (enumerated by n393) for which the channel is declared inactive; valid for either cpe or Switch.
n393	**Synopsis:** A 32-bit signed integer between 1 and 10 **Default:** 4 The number of error events on the frame relay channel; valid for either cpe or 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 11.1.14
Managing Data Links for Frame Relay Connections

Before data can be forwarded over a Frame Relay connection to a remote destination, links to link-local virtual circuits must be configured.

CONTENTS

Section 11.1.14.1
Viewing a List of Data Links

To view a list of data links configured for a frame relay connection, navigate to ***interface » wan » {interface} » {protocol} » channel » {number} » connection » framerelay » dlci***, where *{interface}* is the WAN interface, *{parameter}* is either T1 or E1, and *{number}* is the channel number. If data links have been configured, the **On Demand Settings** table appears.

Figure 481: On Demand Settings Table

If no data links have been configured, add data links as needed. For more information, refer to Section 11.1.14.2, "Adding a Data Link".

Section 11.1.14.2
Adding a Data Link

To add a data link for a frame relay connection, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Depending on the WAN module, navigate to either:
   - **For T1/E1 Lines**
     interface » wan » {interface} » {protocol} » channel » {number} » connection » framerelay » dlci, where *{interface}* is the WAN interface, *{parameter}* is either T1 or E1, and *{number}* is the channel number.
   - **For DDS**
     interface » wan » {interface} » dds » connection » framerelay » dlci, where *{interface}* is the WAN interface, *{parameter}* is either T1 or E1, and *{number}* is the channel number.
3. Navigate to ***interface » wan » {interface} » {protocol} » channel » {number} » connection » framerelay » dlci***, where *{interface}* is the WAN interface, *{parameter}* is either T1 or E1, and *{number}* is the channel number. The **Key Settings** form appears.

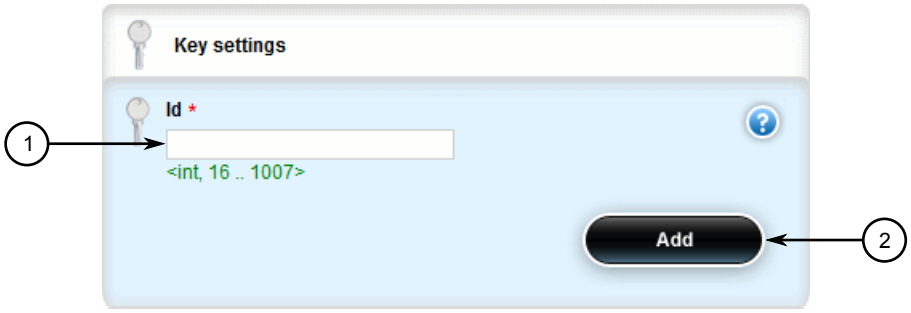


Figure 482: Key Settings Form

1. ID Box **2.** Add Button

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

Parameter	Description
id	**Synopsis:** A 32-bit signed integer between 16 and 1007 DLCI (data link connection identifier) Number.

5. Click **Add** to add the data link. The **On Demand** form appears.

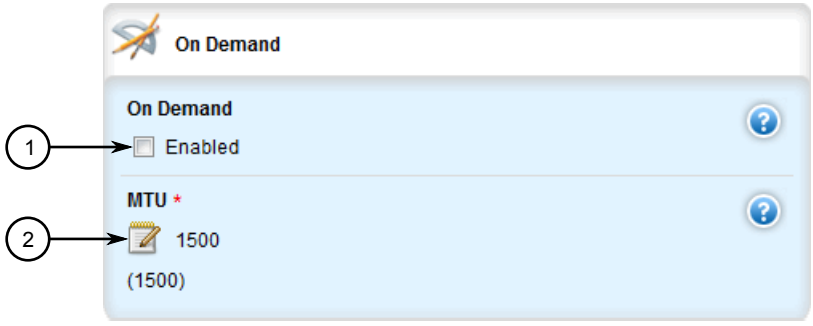


Figure 483: On Demand Form

1. On Demand Check Box **2.** MTU Box

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

Parameter	Description
On Demand	This interface is up or down on demand of link fail over.
MTU	**Synopsis:** A 32-bit signed integer between 256 and 1500 **Default:** 1500 Maximum transmission unit (largest packet size allowed for this 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 11.1.14.3

Deleting a Data Link

To delete a data link for a frame relay connection, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to ***interface » wan » {interface} » {protocol} » channel » {number} » connection » framerelay » dlci***, where *{interface}* is the WAN interface, *{parameter}* is either T1 or E1, and *{number}* is the channel number. The **On Demand Settings** table appears.

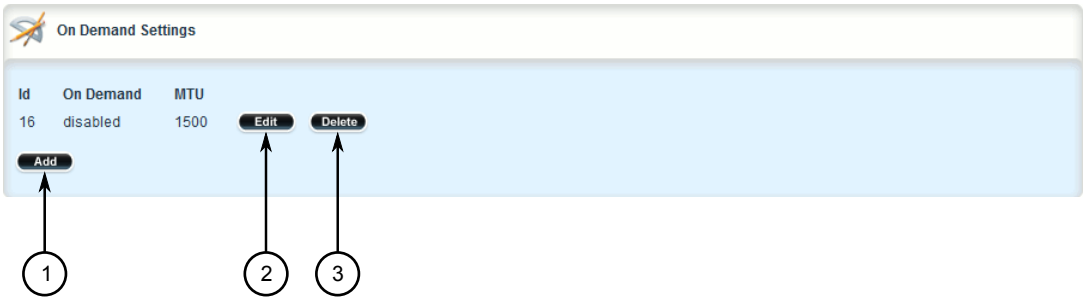


Figure 484: On Demand Settings Table

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

3. Click **Delete** next to the chosen data link.
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 11.1.15

Managing VLANs for HDLC-ETH Connections

VLANs can be used to create logical separations between multiple HDLC-ETH connections within a T1 or E1 channel.

NOTE
Frames egressed through this logical interface will not be tagged with the VLAN configured for the HDLC-ETH connection.

CONTENTS

Section 11.1.15.1

Viewing a List of HDLC-ETH VLANs

To view a list of VLANs configured for an HDLC-ETH connection, navigate to ***interface » wan » {interface} » {protocol} » channel » {number} » connection » hdlc-eth » vlan***, where *{interface}* is the WAN interface, *{protocol}* is either T1 or E1, and *{number}* is the channel number. If VLANs have been configured, the **Ethernet Over HDLC VLAN Settings** table appears.

Figure 485: Ethernet Over HDLC VLAN Settings Table

If no VLANs have been configured, add VLANs as needed. For more information, refer to Section 11.1.15.2, "Adding an HDLC-ETH VLAN".

Section 11.1.15.2
Adding an HDLC-ETH VLAN

To add a VLAN to an HDLC-ETH connection, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to ***interface » wan » {interface} » {protocol} » channel » {number} » connection » hdlc-eth » vlan***, where *{interface}* is the WAN interface, *{protocol}* is either T1 or E1, and *{number}* is the channel number.
3. Click **<Add vlan>**. The **Key Settings** form appears.

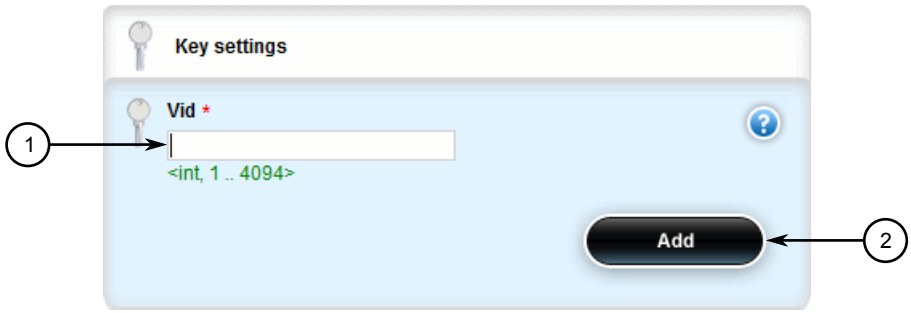


Figure 486: Key Settings Form

1. VID Box **2.** Add Button

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

Parameter	Description
vid	**Synopsis:** A 32-bit signed integer between 1 and 4094 VLAN ID for this routable logical interface

5. Click **Add** to create the new channel. The **Ethernet Over HDLC VLAN Settings** form appears.

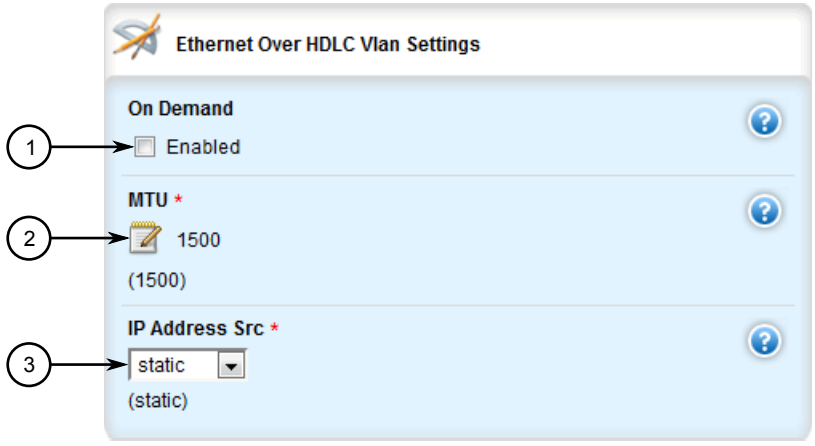


Figure 487: Ethernet Over HDLC VLAN Settings Form

1. On Demand Check Box **2.** MTU Box **3.** IP Address Source List

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

Parameter	Description
On Demand	This interface is up or down on demand of link fail over.
MTU	**Synopsis:** A 32-bit signed integer between 256 and 1500 **Default:** 1500 Maximum transmission unit (largest packet size allowed for this interface).
IP Address Src	**Synopsis:** { static, dynamic } **Default:** static Whether the IP address is static or dynamically assigned via DHCP or BOOTP. The DYNAMIC option is a common case of a dynamically assigned IP address. It switches between BOOTP and DHCP until it gets the response from the relevant server. It must be static for non-management interfaces

7. Add Quality of Service (QoS) maps to the VLAN. For more information, refer to Section 16.2.7.2, "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 11.1.15.3
Deleting an HDLC-ETH VLAN

To delete a VLAN for an HDLC-ETH connection, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to ***interface » wan » {interface} » {protocol} » channel » {number} » connection » hdlc-eth » vlan***, where *{interface}* is the WAN interface, *{protocol}* is either T1 or E1, and *{number}* is the channel number. The **Ethernet Over HDLC VLAN Settings** table appears.

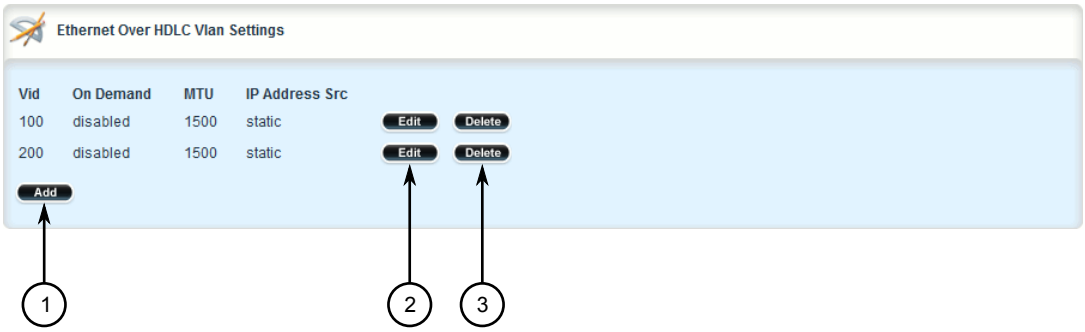


Figure 488: Ethernet Over HDLC VLAN Settings Table

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 11.2

Managing Cellular Modem Interfaces

This section describes how to configure an interface to a cellular network. Depending on the cellular modem module installed, the device can access a 3G or 4G LTE network. Some modules also feature GPS capabilities.

CONTENTS

Section 11.2.1

Enabling/Disabling Cellular Modem Interfaces

To enable or disable a cellular modem interface, do the following:

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

2. Navigate to ***interface » cellmodem » {interface}***, where *{interface}* is the cellular modem interface. The **Routable Cellular Modem Interfaces** form appears.

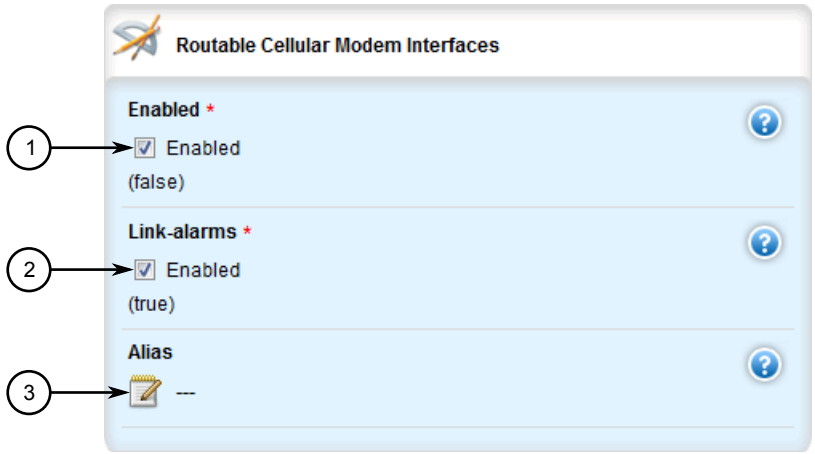


Figure 489: Routable Cellular Modem Interfaces Form

1. Enabled Check Box **2.** Link Alarms Check Box **3.** Alias Box

3. Select **Enabled** to enable the cellular modem interface, or clear the check box to disable the interface.
4. If the interface is enabled, further configure the interface as required. For more information, refer to Section 11.2.2, "Configuring a Cellular Modem 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 11.2.2

Configuring a Cellular Modem Interface

To configure a cellular modem interface, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to ***interface » wan » {interface}***, where *{interface}* is the cellular modem interface. The **Routable Cellular Modem Interfaces** form appears.

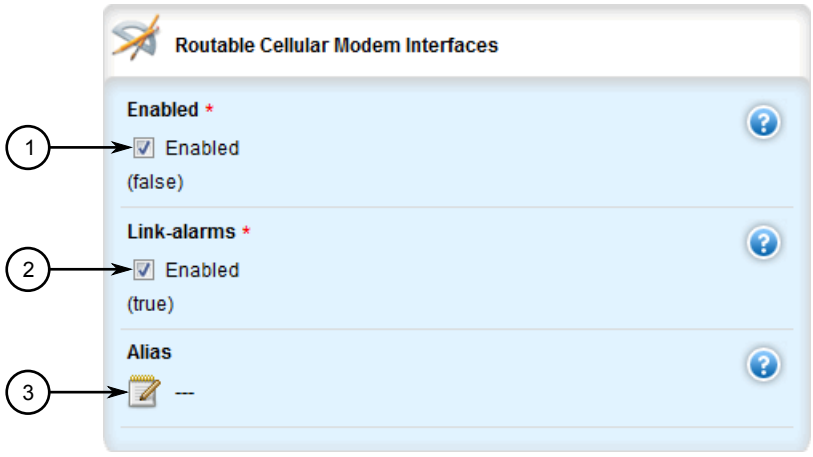


Figure 490: Routable Cellular Modem Interfaces Form

1. Enabled Check Box **2.** Link Alarms Check Box **3.** Alias Box

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

Parameter	Description
Link Alarms	**Synopsis:** { true, false } **Default:** true Disabling link-alarms will prevent alarms and LinkUp and LinkDown SNMP traps from being sent for that interface. Link alarms may also be controlled for the whole system under admin / alarm-cfg.
alias	**Synopsis:** A string 1 to 64 characters long The SNMP alias name of the interface

4. [Optional] Enable the interface. For more information, refer to Section 11.2.1, "Enabling/Disabling Cellular Modem Interfaces".
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 11.2.3

Activating Dual SIM Cards

The RUGGEDCOM RX1500 supports dual micro-SIM cards for the LTE modem to provide a fail-over mechanism should one of the SIM cards lose connectivity with the network.

To activate both micro-SIM cards, do the following:

1. Make sure both micro-SIM cards are installed. For more information, refer to the *Modules Catalog* for the RUGGEDCOM RX1500 series.
2. Configure a GSM profile for each micro-SIM card, making sure the fail-over profile for each is the other card. For more information, refer to Section 11.5.2.2, "Adding a GSM Profile".

3. Configure the cellular modem interface to connect to the cellular network via the primary profile. For more information, refer to Section 11.4, "Connecting as a PPP Client".

Section 11.2.4
Viewing a List of Cellular Modem Interfaces

To view a list of cellular modem interfaces, navigate to ***interface » cellmodem***. The **Routable Cellular Modem Interfaces** table appears.

Figure 491: Routable Cellular Modem Interfaces Table

Section 11.2.5
Viewing the Status of a Cellular Modem Interface

To view the status of a cellular modem interface, navigate to ***interfaces » cellmodem » {slot/port/profile}***, where *{slot/port/profile}* is the slot name, port number and profile configured for the cellular modem. The **Cellular Modem Interfaces** form appears.

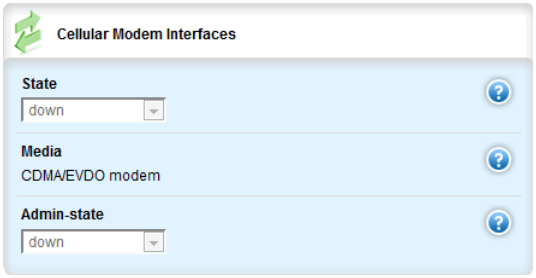


Figure 492: Cellular Modem Interfaces Form

This table provides the following information:

Parameter	Description
Name	**Synopsis:** A string 1 to 10 characters long Interface name
type	**Synopsis:** { edge, hspa, cdma, hspaplus, lte }
state	**Synopsis:** { not set, up, down, testing, unknown, dormant, notPresent, lowerLayerDown } The port's link status. This parameter is mandatory.
media	**Synopsis:** A string 1 to 31 characters long

Parameter	Description
	The wireless data communication technology that modem is compatible with{ GSM/HSPA, CDMA/EVDO, LTE }. This parameter is mandatory.
Admin State	**Synopsis:** { not set, up, down, testing, unknown, dormant, notPresent, lowerLayerDown } The port's administrative status. This parameter is mandatory.
Network Supported	**Synopsis:** A string 1 to 128 characters long Wireless technologies supported by the modem This parameter is mandatory.
IMEI	**Synopsis:** A string 1 to 128 characters long International Mobile Equipment Indentity This parameter is mandatory.
Radio	**Synopsis:** A string 1 to 128 characters long The current RF status of cellmodem This parameter is mandatory.
RSSI Indicator	**Synopsis:** A 32-bit signed integer The Received Signal Strength Indicator in dBm This parameter is mandatory.
Network Operator	**Synopsis:** A string 1 to 128 characters long The wireless network operator currently in use This parameter is mandatory.
Network In Use	**Synopsis:** A string 1 to 128 characters long The network technology currently in use by the modem This parameter is mandatory.
Network Status	**Synopsis:** A string 1 to 128 characters long The registration status of the modem with the wireless network This parameter is mandatory.
SIM	**Synopsis:** A string 1 to 128 characters long The Subscriber Indentity Module number This parameter is mandatory.
Active Profile	**Synopsis:** A string 1 to 128 characters long The active profile of cellular connection This parameter is mandatory.
Network Supported	**Synopsis:** A string 1 to 128 characters long Wireless technologies supported by the modem This parameter is mandatory.
IMEI	**Synopsis:** A string 1 to 128 characters long International Mobile Equipment Indentity This parameter is mandatory.
Radio	**Synopsis:** A string 1 to 128 characters long The current RF status of cellmodem This parameter is mandatory.

Parameter	Description
RSSI Indicator	**Synopsis:** A 32-bit signed integer The Received Signal Strength Indicator in dBm This parameter is mandatory.
Network Operator	**Synopsis:** A string 1 to 128 characters long The wireless network operator currently in use This parameter is mandatory.
Network In Use	**Synopsis:** A string 1 to 128 characters long The network technology currently in use by the modem This parameter is mandatory.
Network Status	**Synopsis:** A string 1 to 128 characters long The registration status of the modem with the wireless network This parameter is mandatory.
SIM	**Synopsis:** A string 1 to 128 characters long The Subscriber Indentity Module number This parameter is mandatory.
Active Profile	**Synopsis:** A string 1 to 128 characters long The active profile of cellular connection This parameter is mandatory.
Network Supported	**Synopsis:** A string 1 to 128 characters long Wireless technologies supported by the modem This parameter is mandatory.
IMEI	**Synopsis:** A string 1 to 128 characters long International Mobile Equipment Indentity This parameter is mandatory.
Radio	**Synopsis:** A string 1 to 128 characters long The current RF status of cellmodem This parameter is mandatory.
RSSI Indicator	**Synopsis:** A 32-bit signed integer The Received Signal Strength Indicator in dBm This parameter is mandatory.
Network Operator	**Synopsis:** A string 1 to 128 characters long The wireless network operator currently in use This parameter is mandatory.
Network In Use	**Synopsis:** A string 1 to 128 characters long The network technology currently in use by the modem This parameter is mandatory.
Network Status	**Synopsis:** A string 1 to 128 characters long The registration status of the modem with the wireless network This parameter is mandatory.
SIM	**Synopsis:** A string 1 to 128 characters long The Subscriber Indentity Module number

Parameter	Description
	This parameter is mandatory.
Active Profile	**Synopsis:** A string 1 to 128 characters long The active profile of cellular connection This parameter is mandatory.
Network Supported	**Synopsis:** A string 1 to 128 characters long Wireless technologies supported by the modem This parameter is mandatory.
ESN	**Synopsis:** A string 1 to 128 characters long The Electronic Serial Number of the modem. ESN is only avaible for the CDMA modem. This parameter is mandatory.
ECIO	**Synopsis:** A 32-bit signed integer The total energy per chip per power density value in dBm This parameter is mandatory.
RSSI Indicator	**Synopsis:** A 32-bit signed integer The Received Signal Strength Indicator in dBm This parameter is mandatory.
Network Operator	**Synopsis:** A string 1 to 128 characters long The wireless network operator currently in use This parameter is mandatory.
Network In Use	**Synopsis:** A string 1 to 128 characters long The network technology currently in use by the modem This parameter is mandatory.
Network Status	**Synopsis:** A string 1 to 128 characters long The registration status of the modem with the wireless network This parameter is mandatory.
Phone Number	**Synopsis:** A string 1 to 128 characters long The subscriber phone number of the CDMA modem This parameter is mandatory.
Status	**Synopsis:** A string 1 to 128 characters long PPP connection status This parameter is mandatory.
Local IP address	**Synopsis:** A string 1 to 32 characters long The IP address assigned to the modem by the remote server This parameter is mandatory.
Peer IP address	**Synopsis:** A string 1 to 32 characters long The IP address of the remote server This parameter is mandatory.
TX (bytes)	**Synopsis:** A 32-bit unsigned integer The bytes transmitted over the modem This parameter is mandatory.
RX (bytes)	**Synopsis:** A 32-bit unsigned integer

Parameter	Description
	The bytes received by the modem This parameter is mandatory.
mtu	**Synopsis:** A 32-bit unsigned integer MTU (Maximum Transmission Unit) value on the ppp interface This parameter is mandatory.

Section 11.2.6
Viewing PPP Interface Statistics

To view the statistics for the PPP interface, navigate to ***interfaces » cellmodem » {slot/port/profile}***, where *{slot/port/profile}* is the slot name, port number and profile configured for the cellular modem. The **PPP Interfaces Statistics** form appears.

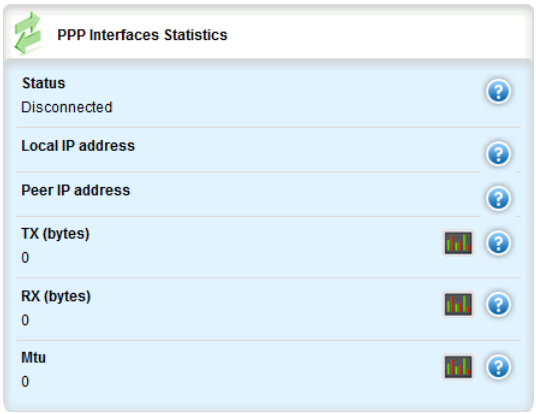


Figure 493: PPP Interfaces Statistics Form

This table provides the following information:

Parameter	Description
Status	**Synopsis:** A string 1 to 128 characters long PPP connection status This parameter is mandatory.
Local IP address	**Synopsis:** A string 1 to 32 characters long The IP address assigned to the modem by the remote server This parameter is mandatory.
Peer IP address	**Synopsis:** A string 1 to 32 characters long The IP address of the remote server This parameter is mandatory.
TX (bytes)	**Synopsis:** A 32-bit unsigned integer The bytes transmitted over the modem This parameter is mandatory.
RX (bytes)	**Synopsis:** A 32-bit unsigned integer

Parameter	Description
	The bytes received by the modem This parameter is mandatory.
mtu	**Synopsis:** A 32-bit unsigned integer MTU (Maximum Transmission Unit) value on the ppp interface This parameter is mandatory.

Section 11.2.7
Viewing the HSPA Network Status for Cellular Modems

To view the status of the HSPA GSM network for a cellular modem, navigate to ***interfaces » cellmodem » {slot/port} {profile} » {profile}***, where *{slot/port}* is the slot name and port number for the cellular modem, and *{profile}* is the profile (e.g. hspa or hspaplus). The **GSM/HSPA/HSPA+ Cellular Modem Information** form appears.

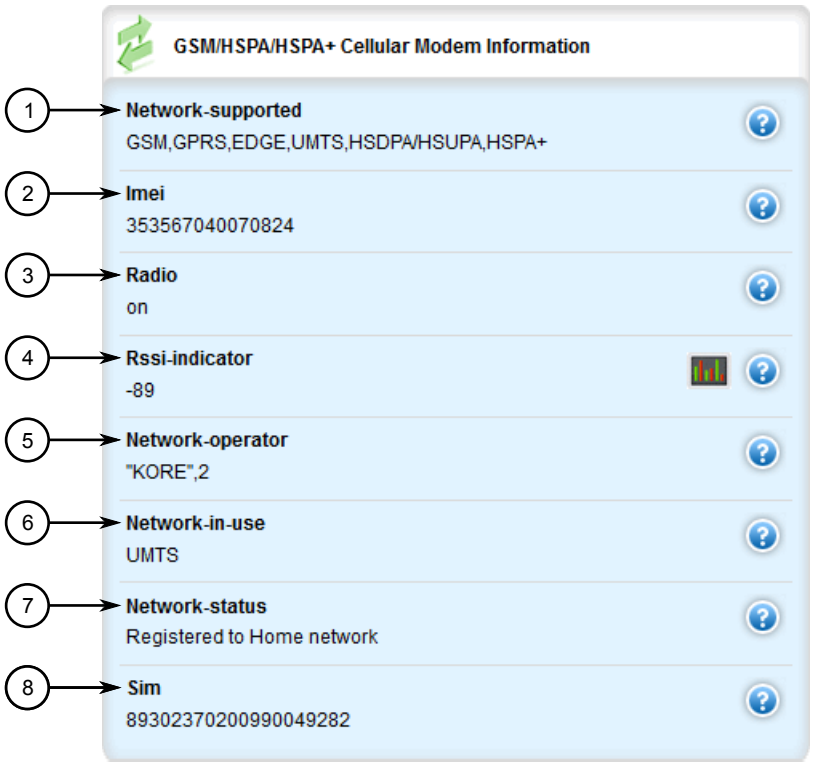


Figure 494: GSM/HSPA/HSPA+ Cellular Modem Information Form

1. Network Supported **2.** IMEI **3.** Radio **4.** RSSI Indicator **5.** Network Operator **6.** Network In Use **7.** Network Status **8.** SIM

This form provides the following information:

Parameter	Description
Network Supported	**Synopsis:** A string 1 to 128 characters long Wireless technologies supported by the modem This parameter is mandatory.

Parameter	Description
IMEI	**Synopsis:** A string 1 to 128 characters long International Mobile Equipment Indentity This parameter is mandatory.
Radio	**Synopsis:** A string 1 to 128 characters long The current RF status of cellmodem This parameter is mandatory.
RSSI Indicator	**Synopsis:** A 32-bit signed integer The Received Signal Strength Indicator in dBm This parameter is mandatory.
Network Operator	**Synopsis:** A string 1 to 128 characters long The wireless network operator currently in use This parameter is mandatory.
Network In Use	**Synopsis:** A string 1 to 128 characters long The network technology currently in use by the modem This parameter is mandatory.
Network Status	**Synopsis:** A string 1 to 128 characters long The registration status of the modem with the wireless network This parameter is mandatory.
SIM	**Synopsis:** A string 1 to 128 characters long The Subscriber Indentity Module number This parameter is mandatory.
Active Profile	**Synopsis:** A string 1 to 128 characters long The active profile of cellular connection This parameter is mandatory.

Section 11.2.8
Viewing the CDMA Network Status for Cellular Modems

To view the status of the CDMA network for a cellular modem, navigate to ***interfaces » cellmodem » {slot/port/profile} » cdma***, where *{slot/port/profile}* is the slot name, port number and profile configured for the cellular modem. The **3G CDMA/EVDO Cellular Modem Information** form appears.

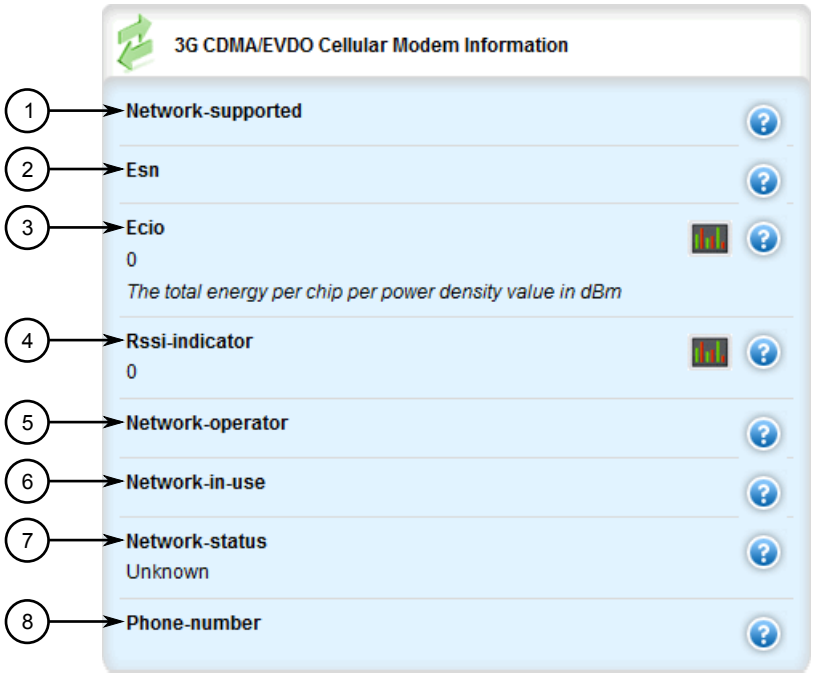


Figure 495: 3G CDMA/EVDO Cellular Modem Information Form

1. Network Supported **2.** ESN **3.** ECIO **4.** RSSI Indicator **5.** Network Operator **6.** Network In Use **7.** Network Status **8.** Phone Number

This form provides the following information:

Parameter	Description
Network Supported	**Synopsis:** A string 1 to 128 characters long Wireless technologies supported by the modem This parameter is mandatory.
ESN	**Synopsis:** A string 1 to 128 characters long The Electronic Serial Number of the modem. ESN is only avaible for the CDMA modem. This parameter is mandatory.
ECIO	**Synopsis:** A 32-bit signed integer The total energy per chip per power density value in dBm This parameter is mandatory.
RSSI Indicator	**Synopsis:** A 32-bit signed integer The Received Signal Strength Indicator in dBm This parameter is mandatory.
Network Operator	**Synopsis:** A string 1 to 128 characters long The wireless network operator currently in use This parameter is mandatory.
Network In Use	**Synopsis:** A string 1 to 128 characters long The network technology currently in use by the modem This parameter is mandatory.

Parameter	Description
Network Status	**Synopsis:** A string 1 to 128 characters long The registration status of the modem with the wireless network This parameter is mandatory.
Phone Number	**Synopsis:** A string 1 to 128 characters long The subscriber phone number of the CDMA modem This parameter is mandatory.

Section 11.2.9
Activating a Cellular Modem Account

Before using the cellular modem, a cellular account must be activated on a service provider's network. Once the account is activated, the modem will be able to connect to the cellular network without further intervention. There are two account activation methods used by RUGGEDCOM ROX II: OTA (Over-the-Air) and Manual.

CONTENTS

Section 11.2.9.1
Activating a Cellular Modem Account Over-the-Air

RUGGEDCOM ROX II supports the OTASP (Over-the-Air Service Provisioning) mechanism offered by most CDMA cellular service providers for provisioning cellular end stations for use on their networks. Using this method, the service provider (or carrier) supplies an OTASP dial string which RUGGEDCOM ROX II can use to activate the cellular account. During this OTASP call, the carrier authorizes and configures the modem for use on its network.

NOTE
The service provider may issue a second OTASP dial string for accessing the cellular network if a string other than the default is required. This string must be configured when adding a CDMA profile for the cellular modem interface. For more information about adding a CDMA profile, refer to Section 11.5.1.2, "Adding a CDMA Profile".

NOTE
*A typical OTASP dial string begins with ***228**.*

To configure the OTASP dial string, do the following:

1. Establish an account with a service provider and obtain the OTASP dial string.
2. Change the mode to **Edit Private** or **Edit Exclusive**.
3. Navigate to ***interfaces » cellmodem » {slot/port/profile} » activation***, where *{slot/port/profile}* is the slot name, port number and profile configured for the cellular modem.
4. Click **over-the-air-activation** in the menu. The **Over The Air Activation** and **Trigger Action** forms appears.

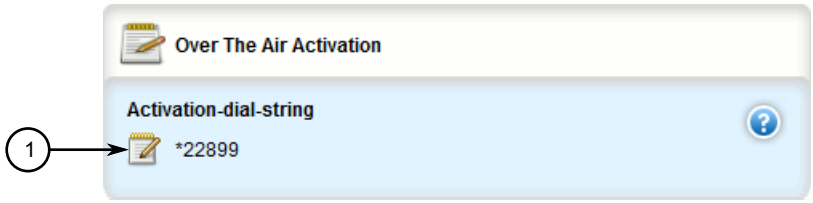


Figure 496: Over The Air Activation Form

1. Activation Dial String Box

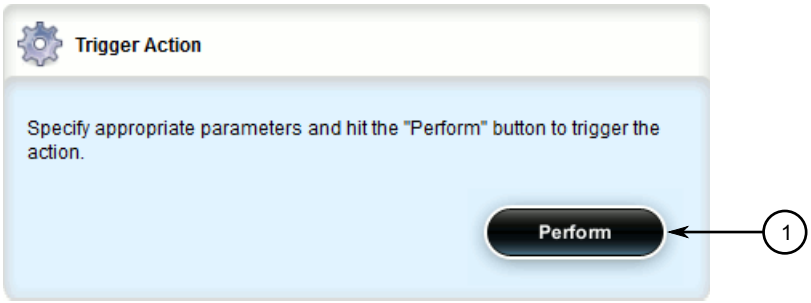


Figure 497: Trigger Action Form

1. Perform Button

5. On the **Over The Air Activation** form, configure the following parameter(s) as required:

Parameter	Description
Activation Dial String	**Synopsis:** A string 1 to 128 characters long **Default:** *22899 The dial string to activate the modem over the air

6. On the **Trigger Action** form, click **Perform** to activate the account.

Section 11.2.9.2

Activating a Cellular Modem Account Manually

If the service provider does not support Over the Air Service Provisioning (OTASP), the account must be activated manually.

To manually activate a cellular modem account, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to ***interfaces » cellmodem » {slot/port/profile} » activation***, where *{slot/port/profile}* is the slot name, port number and profile configured for the cellular modem.
3. Click **manual-activation** in the menu. The **Manual Activation** and **Trigger Action** forms appears.

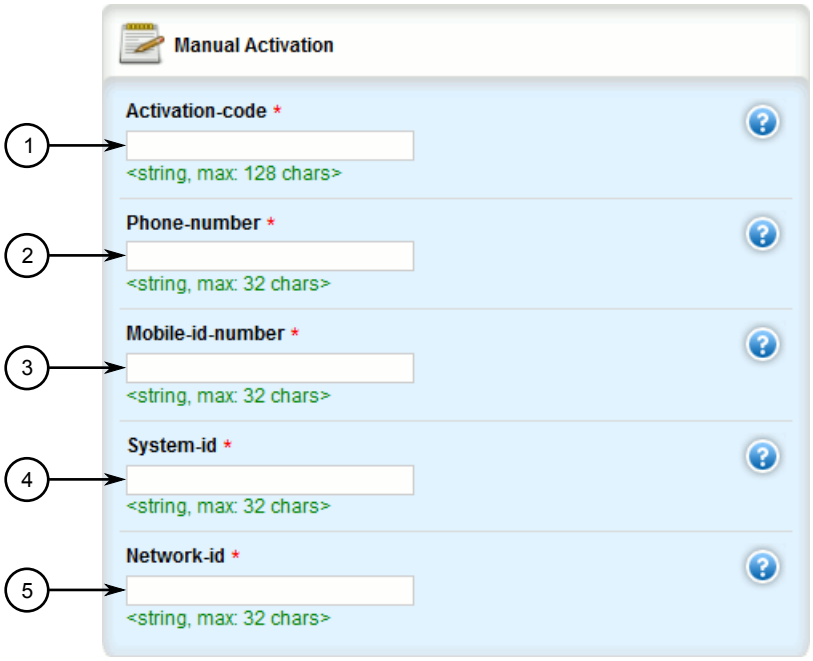


Figure 498: Manual Activation Form

1. Activation Code Box **2.** Phone Number Box **3.** Mobile ID Number Box **4.** System ID Box **5.** Network ID Box

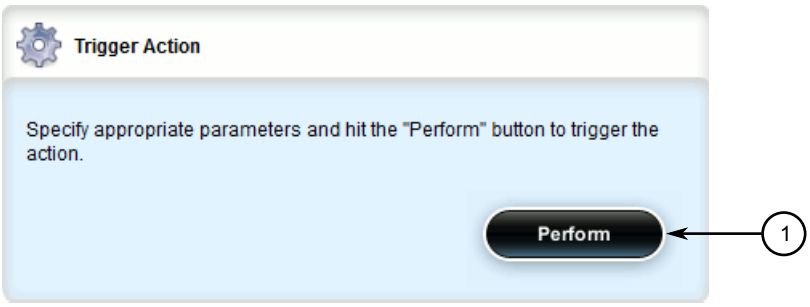


Figure 499: Trigger Action Form

1. Perform Button

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

Parameter	Description
Activation Code	**Synopsis:** A string 1 to 128 characters long The Master Subsidy Lock code provided by the wireless service carrier This parameter is mandatory.
Phone Number	**Synopsis:** A string 1 to 32 characters long The Mobile Directory Number provided by the wireless service carrier This parameter is mandatory.

Parameter	Description
Mobile ID Number	**Synopsis:** A string 1 to 32 characters long The Mobile Indentification Number provided by the wireless service carrier This parameter is mandatory.
System ID	**Synopsis:** A string 1 to 32 characters long System Identification Number provided by wireless service carrier This parameter is mandatory.
Network ID	**Synopsis:** A string 1 to 32 characters long The Wireless Network ID provided by the wireless service carrier This parameter is mandatory.

5. On the **Trigger Action** form, click **Perform** to activate the account.

Section 11.3
Running AT Commands

To issue AT (Hayes) commands to the cellular modem, do the following:

1. Navigate to ***interfaces » cellmodem » {interface}***, where *{interface}* is the cellular modem interface.
2. Click **at** in the menu. The **AT Command** and **Trigger Action** forms appears.

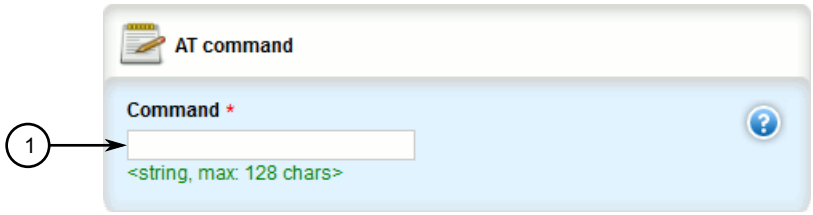


Figure 500: AT Command Form

1. Command Box

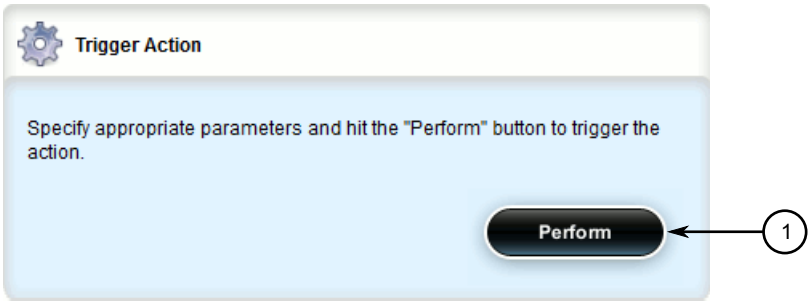


Figure 501: Trigger Action Form

1. Perform Button

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

Parameter	Description
command	**Synopsis:** A string 1 to 128 characters long The Modem AT command to be executed. Note: The command must begin with the prefix 'AT' This parameter is mandatory.

4. On the **Trigger Action** form, click **Perform** to run the command.

Section 11.4
Connecting as a PPP Client

To connect or disconnect from a cellular network as a PPP client, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Make sure the cellular modem interface has been configured. For more information, refer to Section 11.2.2, "Configuring a Cellular Modem Interface".
3. Make sure an appropriate cellular modem profile has been configured. For more information, refer to Section 11.5, "Managing Cellular Modem Profiles".
4. Make sure an account has been activated with a service provider for the modem type.
5. Make sure antennas are properly connected to the device before initiating the connection. For more information, refer to the *RUGGEDCOM RX1500 Installation Guide*.
6. For HSPA+ and Edge modems, insert a SIM card into the cellular modem module.
7. For CDMA modems, activate the modem either manually or over-the-air. For more information, refer to Section 11.2.9, "Activating a Cellular Modem Account".
8. Verify the network status. For more information, refer to:
   - Section 11.2.7, "Viewing the HSPA Network Status for Cellular Modems"
   - Section 11.2.8, "Viewing the CDMA Network Status for Cellular Modems"
9. Navigate to ***interface » cellmodem » {interface} » {hspa/edge/cdma}***, where *{interface}* is the cellular modem interface.
10. Click the **+** symbol in the menu next to *ppp-client*. The **CDMA Profile** form appears.

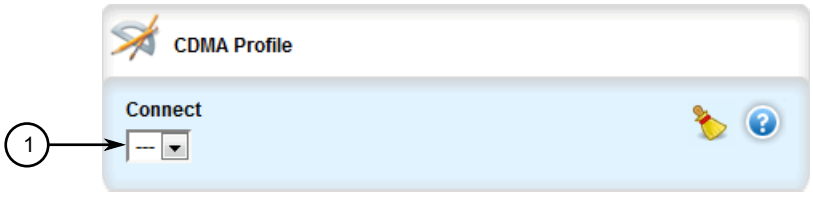


Figure 502: CDMA Profile Form (Example)

1. Connect List

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

Parameter	Description
Connect	**Synopsis:** A string Selects the gsm profile to connect to wireless network. The gsm profile is configured in /global/cellular/profiles/gsm

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 11.5
Managing Cellular Modem Profiles

CONTENTS

Section 11.5.1
Managing CDMA Profiles

CDMA (Code Division Multiple Access) profiles must be configured before 3G EVDO CDMA data is available. For more information about viewing 3G EVDO CDMA data, refer to Section 11.2.8, "Viewing the CDMA Network Status for Cellular Modems".

CONTENTS

Section 11.5.1.1
Viewing a List of CDMA Profiles

To view a list of CDMA profiles, navigate to ***global » cellular » profiles » cdma***. If profiles have been configured, the **Cellular Network Configuration** table appears.

Figure 503: Cellular Network Configuration Table

If no CDMA profiles have been configured, add profiles as needed. For more information, refer to Section 11.5.1.2, "Adding a CDMA Profile".

Section 11.5.1.2
Adding a CDMA Profile

To add a CDMA profile for the cellular modem interface, do the following:

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

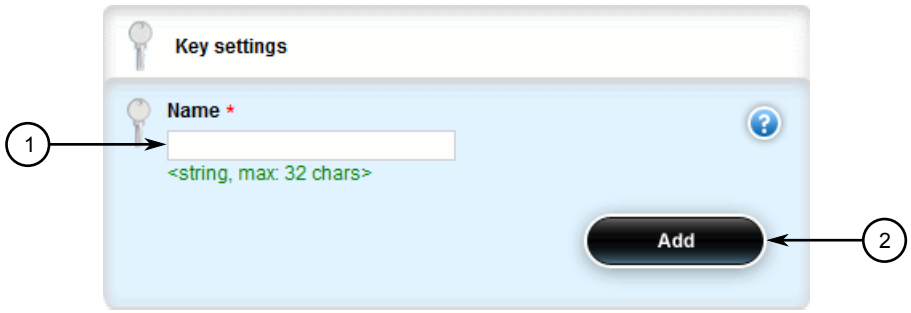


Figure 504: Key Settings Form

1. Name Box **2.** Add Button

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

Parameter	Description
name	**Synopsis:** A string 1 to 32 characters long Create a CDMA profile name

4. Click **Add** to create the new profile. The **Cellular Network Configuration** and **CDMA PPP Configuration** forms appear.

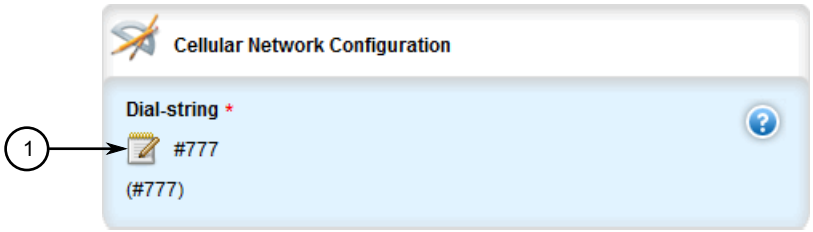


Figure 505: Cellular Network Configuration Form

1. Dial String Box

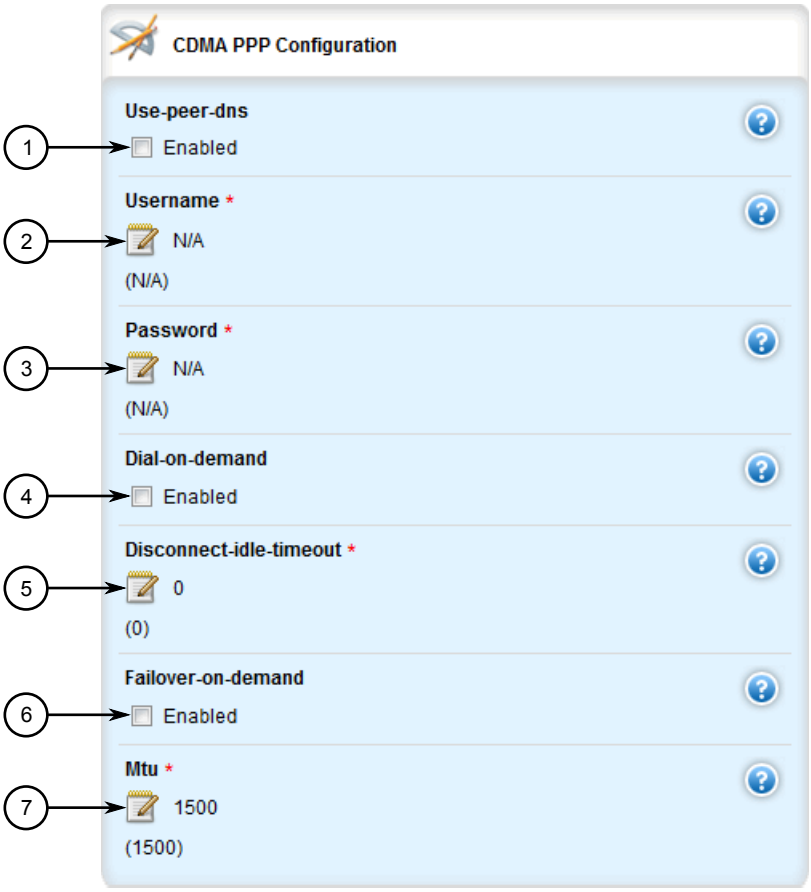


Figure 506: CDMA PPP Configuration Form

1. Use Peer DNS Check Box **2.** Username Box **3.** Password Box **4.** Dial On Demand Check Box **5.** Disconnect Idle Timeout Box **6.** Failover On Demand Check Box **7.** MTU Box

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

NOTE

RUGGEDCOM ROX II supports the OTASP (Over-the-Air Service Provisioning) mechanism offered by most CDMA cellular service providers for provisioning cellular end stations for use on their networks. Using this method, the service provider (or carrier) supplies an OTASP dial string which RUGGEDCOM ROX II can use to contact the cellular network via the modem. During this OTASP call, the carrier authorizes and configures the modem for use on its network.

A typical OTASP dial string begins with ****228****.*

Parameter	Description
Dial String	**Synopsis:** A string 1 to 32 characters long **Default:** #777 The dial string to connect to the wireless provider.

6. On the **CDMA PPP Configuration** form, configure the following parameter(s) as required:

Parameter	Description
Use Peer DNS	Enables the DNS server entries that the PPP server recommends. Enables this option unless you provide your own name servers.
username	**Synopsis:** A string **Default:** N/A The user ID to connect to the remote server.
password	**Synopsis:** A string **Default:** N/A The password to be authenticated by the remote server.
Dial-on-Demand	Activates dial-on-demand for this connection. The establishment of the PPP connection is postponed until there is data to be transmitted via the interface. If dial-on-demand is configured, Failover on Demand cannot be configured.
Disconnect Idle Timeout	**Synopsis:** A 32-bit signed integer **Default:** 0 The time in seconds to wait before disconnecting PPP when there is no traffic on the link. This option is only valid when dial-on-demand is enabled.
Failover On Demand	Activates link failover on-demand on this device. PPP link establishment on this device is controlled by link failover. If Failover on Demand is configured, Dial on Demand cannot be configured.
mtu	**Synopsis:** A 32-bit signed integer between 128 and 1500 **Default:** 1500 MTU (Maximum Transmission Unit) value on a PPP 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 11.5.1.3
Deleting a CDMA Profile

To delete a CDMA Profile, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to ***global » cellular » profiles » cdma***. The **Cellular Network Configuration** table appears.

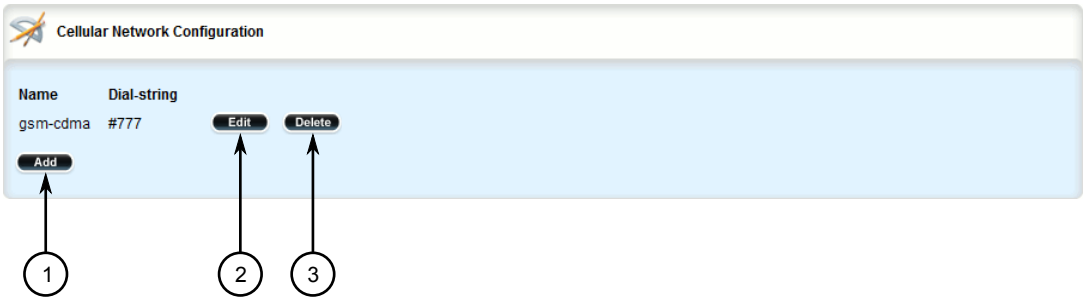


Figure 507: Cellular Network Configuration Table

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

3. Click **Delete** next to the chosen profile.
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 11.5.2
Managing GSM Profiles

GSM (Global System for Mobile Communications) profiles must be configured before HSPA data is available. For more information about viewing the status of the HSPA networks, refer to Section 11.2.7, "Viewing the HSPA Network Status for Cellular Modems".

CONTENTS

Section 11.5.2.1
Viewing a List of GSM Profiles

To view a list of GSM profiles, navigate to ***global » cellular » profiles » gsm***. If profiles have been configured, the **Cellular Network Configuration** table appears.

Figure 508: Cellular Network Configuration Table

If no GSM profiles have been configured, add profiles as needed. For more information, refer to Section 11.5.2.2, "Adding a GSM Profile".

Section 11.5.2.2
Adding a GSM Profile

To add a GSM profile for the cellular modem interface, do the following:

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

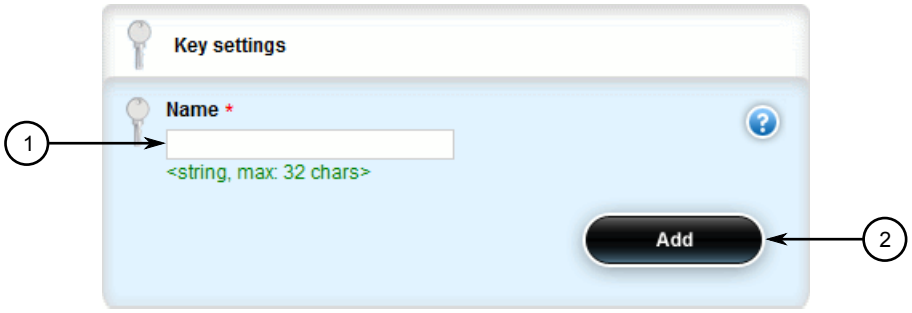


Figure 509: Key Settings Form

1. Name Box **2.** Add Button

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

Parameter	Description
name	**Synopsis:** A string 1 to 32 characters long Create a GSM profile name.

4. Click **Add** to create the new profile. The **Cellular Network Configuration** and **GSM PPP Configuration** forms appear.

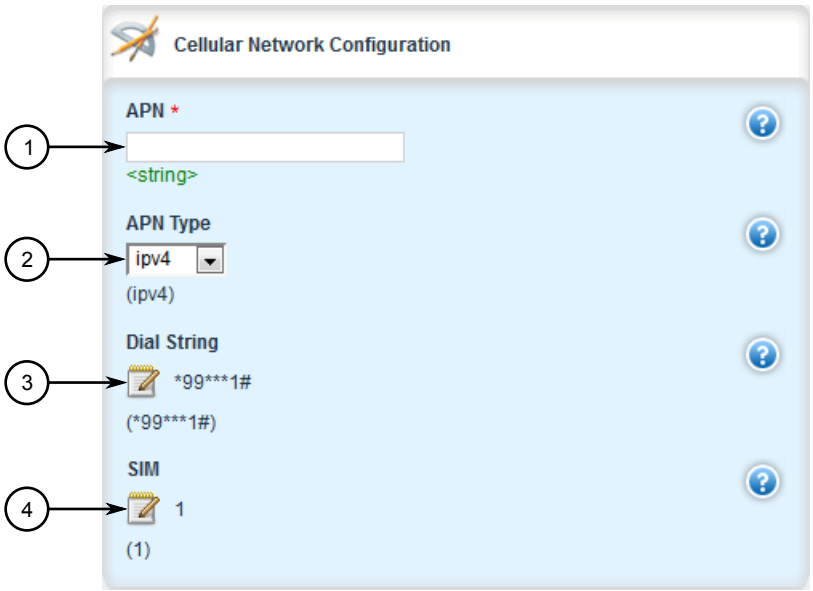


Figure 510: Cellular Network Configuration Form

1. APN Box **2.** APN Type List **3.** Dial String Box **4.** SIM Box

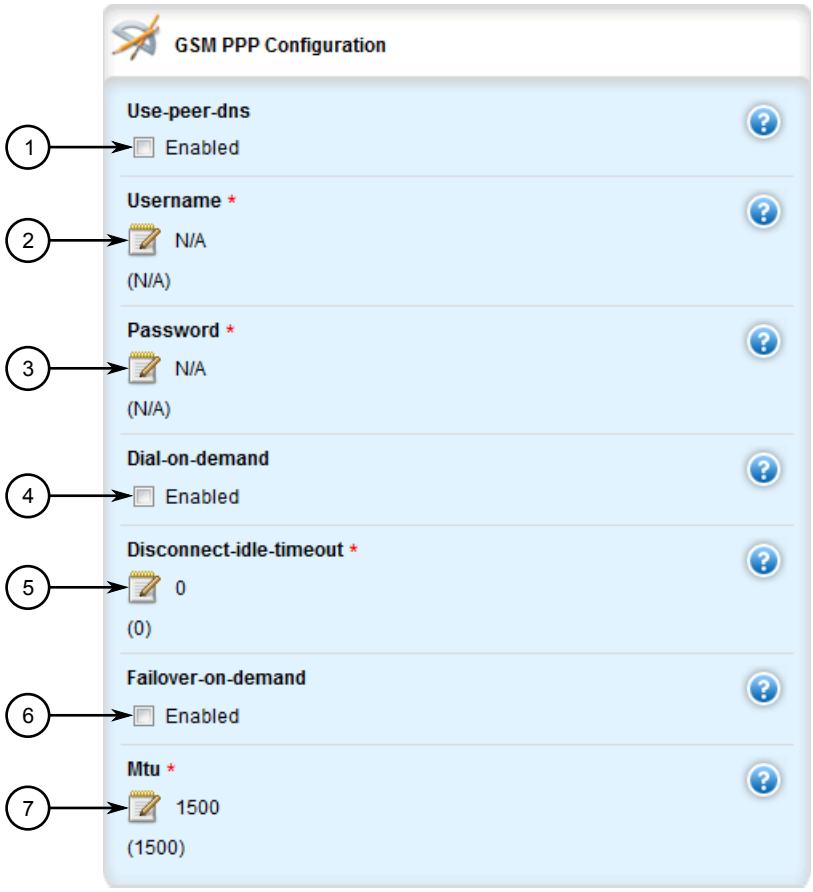


Figure 511: GSM PPP Configuration Form

1. Use Peer DNS Check Box **2.** Username Box **3.** Password Box **4.** Dial On Demand Check Box **5.** Disconnect Idle Timeout Box **6.** Failover On Demand Check Box **7.** MTU Box

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

NOTE
The Access Point Name (APN) is necessary only on GPRS networks (Edge or HSPA). It is the name of the cellular network access point that provides a gateway to the Internet. This information is provided by the wireless network when a data service account is registered.

NOTE
*The dial string is a special command to be sent by the cellular modem to the cellular network to establish a data connection. For example, a typical dial string for GSM/GPRS networks is ***99***1#**. This command will depend on the wireless network. Contact the service provided for the correct dial string command for data service. A regular telephone number is usually not required to connect to a GSM/GPRS network.*

Parameter	Description
APN	**Synopsis:** A string **Default:** none

Parameter	Description
	The name of the wireless network access point.
APN Type	**Synopsis:** { ipv4, ipv6, ipv4v6 } **Default:** ipv4 Specify APN type used to attach to PDN
Dial String	**Synopsis:** A string **Default:** *99***1# The dial string given by the wireless provider to connect to the access point name.
SIM	**Synopsis:** A 32-bit signed integer between 1 and 2 **Default:** 1 Specify SIM index to be used by this profile
Peer Address	**Synopsis:** A string 7 to 15 characters long or a string 6 to 40 characters long The peer address to override the one from carrier.

6. On the **GSM PPP Configuration** form, configure the following parameter(s) as required:

Parameter	Description
Use Peer DNS	Enables the DNS server entries that the PPP server recommends. Enables this option unless you provide your own name servers.
User Name	**Synopsis:** A string **Default:** N/A The user ID to connect to the remote server.
password	**Synopsis:** A string **Default:** N/A The password to be authenticated by the remote server.
Dial-on-Demand	Activates dial-on-demand for this connection. The establishment of the PPP connection is postponed until there is data to be transmitted via the interface. If dial-on-demand is configured, Failover on Demand cannot be configured.
Disconnect Idle Timeout	**Synopsis:** A 32-bit signed integer **Default:** 0 The time in seconds to wait before disconnecting PPP when there is no traffic on the link. This option is only valid when dial-on-demand is enabled.
Failover On Demand	Activates link failover on-demand on this device. PPP link establishment on this device is controlled by link failover. If Failover on Demand is configured, Dial on Demand cannot be configured.
MTU	**Synopsis:** A 32-bit signed integer between 128 and 1500 **Default:** 1500 MTU (Maximum Transmission Unit) value on a PPP interface.
authentication	**Synopsis:** { none, chap, pap } **Default:** none The authentication protocol used to establish a cellular data link

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 11.5.2.3
Deleting a GSM Profile

To delete a GSM Profile, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to ***global » cellular » profiles » gsm***. The **Cellular Network Configuration** table appears.

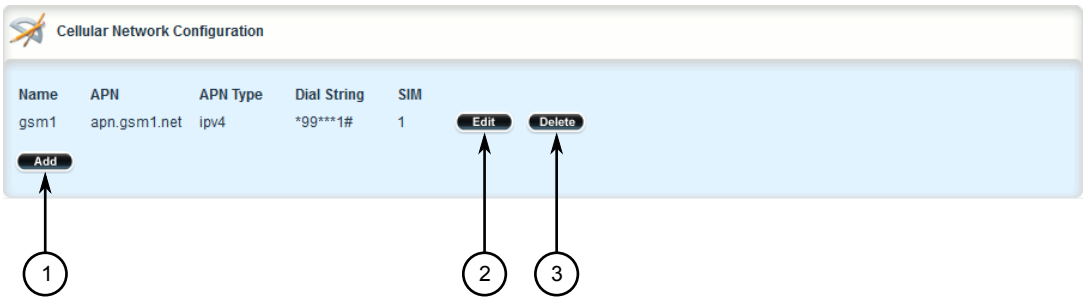


Figure 512: Cellular Network Configuration Table

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

3. Click **Delete** next to the chosen profile.
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 11.6
Managing the LTE Modem

This section describes how to manage the LTE modem.

CONTENTS

Section 11.6.1
Configuring an LTE Modem

To configure an LTE modem, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Enable the LTE modem. For more information, refer to Section 11.6.2, "Enabling/Disabling the LTE Modem".
3. Navigate to ***interface » cellmodem » {interface} » lte***, where *{interface}* is the slot name and port number of the cellular modem port. The **LTE Cellular Modem Configuration** form appears.

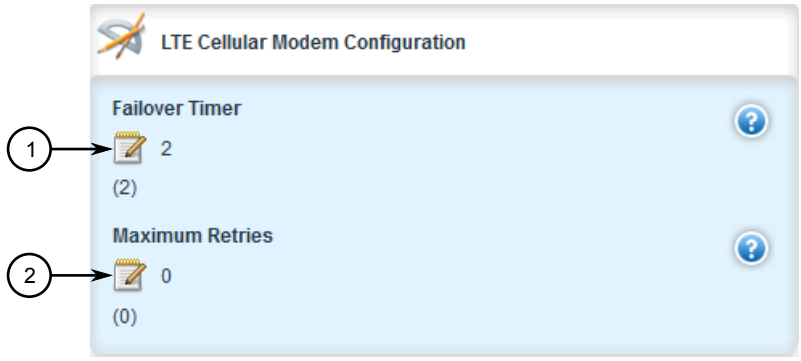


Figure 513: LTE Cellular Modem Configuration Form

1. Failover Timer Box **2.** Maximum Retries Box

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

Parameter	Description
Failover Timer	**Synopsis:** A 32-bit signed integer between 1 and 10 **Default:** 2 Specify SIM card failover timer in minute
Maximum Retries	**Synopsis:** A 32-bit signed integer between 0 and 65535 **Default:** 0 Specify the maximum number of SIM card failover retries. 0 means re-try forever

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. [Optional] Enable GPS. For more information, refer to Section 11.6.4, "Enabling/Disabling GPS".

Section 11.6.2

Enabling/Disabling the LTE Modem

To enable or disable the LTE modem for a cellular modem interface, do the following:

NOTE
The operational state of the LTE modem is determined by the associated cellular modem interface. For more information about enabling or disabling the cellular modem interface, refer to Section 11.2.1, "Enabling/Disabling Cellular Modem Interfaces".

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

2. Navigate to ***interface » cellmodem » {interface}***, where **{interface}** is the cellular modem interface. The **Routable Cellular Modem Interfaces** form appears.

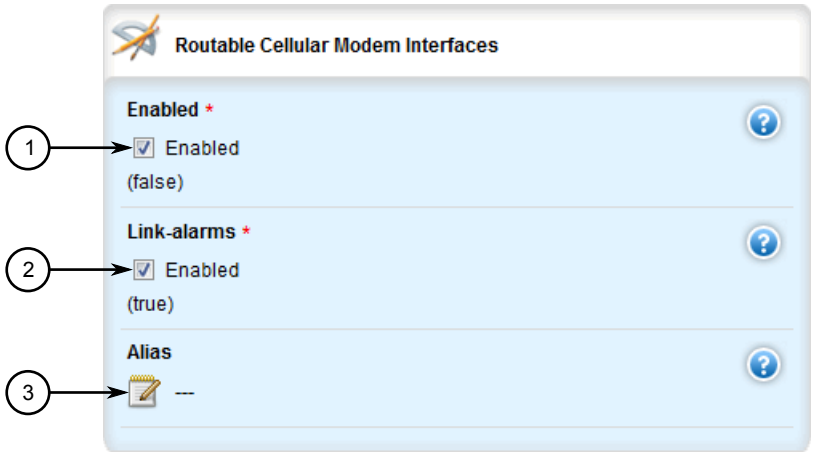


Figure 514: Routable Cellular Modem Interfaces Form

1. Enabled Check Box **2.** Link Alarms Check Box **3.** Alias Box

3. In the menu, click **+** next to **lte** to enable the LTE modem, or click **-** to disable the modem.
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 11.6.3

Resetting the Cellular Modem

To reset a cellular modem, do the following:

1. Navigate to ***interfaces » cellmodem » {slot/port/profile}***, where *{slot/port/profile}* is the slot name, port number and profile configured for the cellular modem.
2. Click **reset** in the menu. The **Trigger Action** form appears.

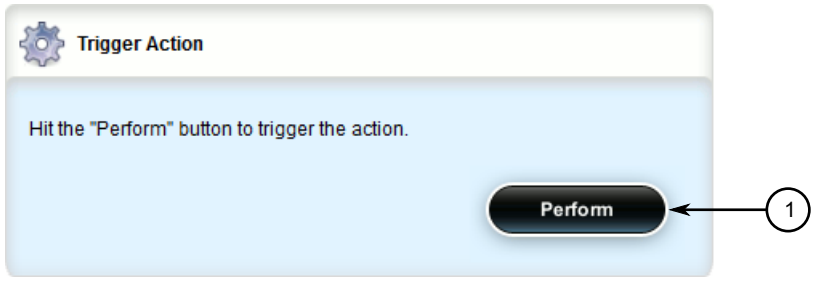


Figure 515: Trigger Action Form

1. Perform Button

3. Click **Perform**.

Section 11.6.4
Enabling/Disabling GPS

When GPS is enabled, users can look up the current location of the device. If configured, RUGGEDCOM ROX II can also send an NMEA GPS data streams via TCP to a server that hosts a GPS application.

To enable or disable GPS on the cellular modem, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to ***interface » cellmodem » {interface} » lte » gps***, where **{interface}** is the cellular modem interface. The **GPS Configuration** form appears.

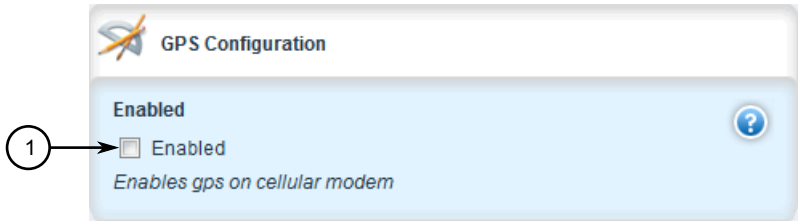


Figure 516: GPS Configuration Form

1. Enabled Check Box

3. Click **Enabled** to enable GPS, or clear **Enabled** to disable GPS.
4. [Optional] Enable or disable NMEA GPS data streams. For more information, refer to Section 11.6.5, "Enabling and Configuring GPS NMEA Data Streams".
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 11.6.5
Enabling and Configuring GPS NMEA Data Streams

When GPS and NMEA are enabled, RUGGEDCOM ROX II can receive NMEA data from the cellular modem and relay it to a remote host upon request. This feature can be enabled or disabled independent of the LTE modem configuration.

To enable and configure GPS NMEA data streams, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to ***interface » cellmodem » {interface} » lte » gps***, where **{interface}** is the cellular modem interface. The **GPS/NMEA Configuration** form appears.

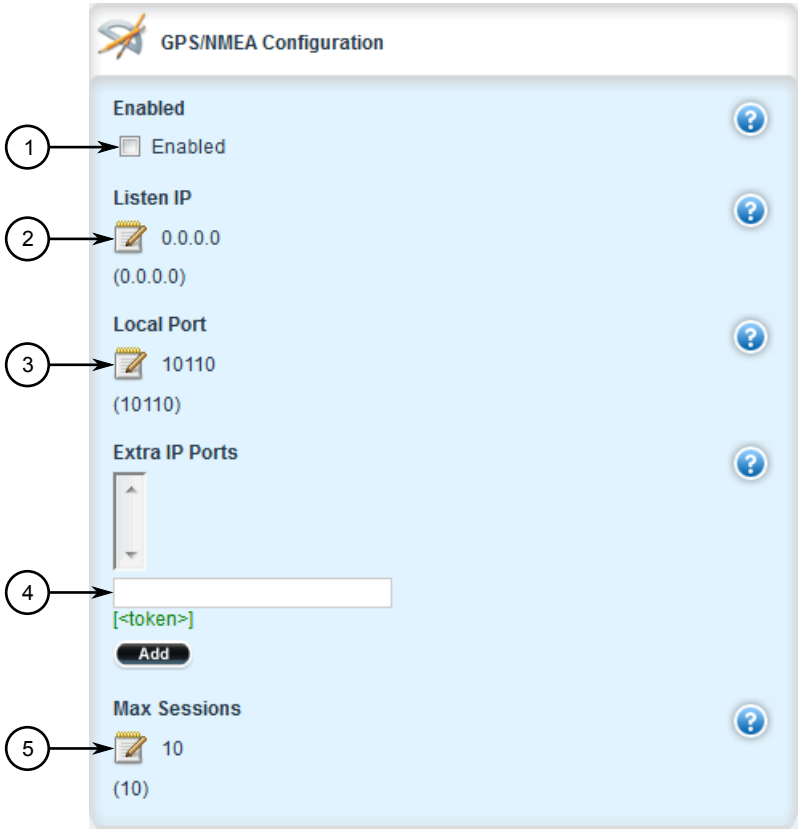


Figure 517: GPS Configuration Form

1. Enabled Check Box **2.** Listen IP Box **3.** Local Port Box **4.** Extra IP Ports Box **5.** Max Sessions Box

3. Configure the following parameters as required:

Parameter	Description
enabled	Enables NMEA stream
Listen IP	**Synopsis:** A string **Default:** 0.0.0.0 The IP Address that device will listen on for remote host request
Local Port	**Synopsis:** A 16-bit unsigned integer between 0 and 65535 **Default:** 10110 The port that device will listen on for remote host request
Extra IP Ports	**Synopsis:** A string The device will also listen on these IP Addresses. For port values, add ':#' to set the non-default port value. (ie. xxx.xxx.xxx.xxx:19343 [::] [::]:16000). If using the default address, do not specify another listen address with the same port.
Max Sessions	**Synopsis:** A 32-bit signed integer between 1 and 32 **Default:** 10 The maximum number of concurrent tcp/ip sessions.

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 11.6.6
Managing Firmware Updates

Firmware for the LTE modem can be upgraded either directly via USB flash drive or wirelessly via a remote HTTP/HTTPS server.

During wireless upgrades, RUGGEDCOM ROX II initiates the connection to the remote server, then pulls and updates the firmware. Firmware can be updated either on-demand or automatically, as defined by the user.

RUGGEDCOM ROX II performs the following actions when updating the firmware:

1. Connects to the USB flash drive or remote server and verifies the firmware version
2. Downloads the new firmware
3. Validates the new firmware to make sure it is valid for the modem
4. Flashes the new firmware to the modem
5. Logs all firmware update events and actions to the system log (Syslog)
6. Brings the modem back to normal operation

CONTENTS

Section 11.6.6.1
Viewing the Firmware Update Status

To view the status of the firmware update, navigate to ***interfaces » cellmodem » {interface} » firmware-update***, where *{interface}* is the cellular modem interface. The **Firmware Update Monitor** form appears.

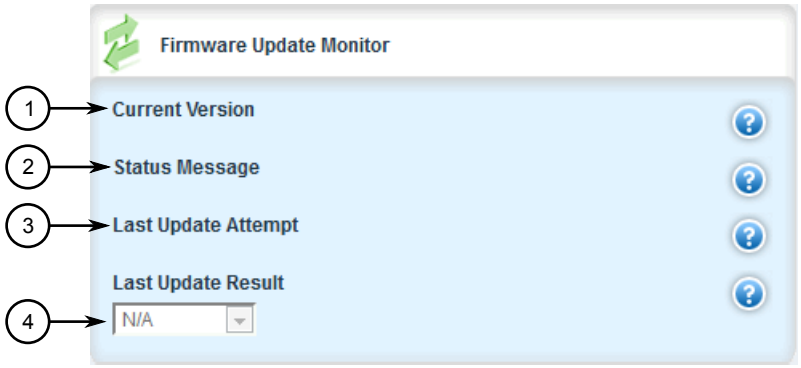


Figure 518: Firmware Update Monitor Form

1. Current Version **2.** Status Message **3.** Last Update Attempt **4.** Last Update Result

This table displays the following information:

Parameter	Description
Current Version	**Synopsis:** A string 1 to 64 characters long The current firmware revision This parameter is mandatory.
Status Message	**Synopsis:** A string 1 to 128 characters long Additional details on the status of the update.
Last Update Attempt	**Synopsis:** A string 1 to 64 characters long The date and time of the completion of the last update attempt.
Last Update Result	**Synopsis:** { N/A, Successful, Failed } Indicates whether or not the last firmware update was completed successfully

Section 11.6.6.2
Configuring the Firmware Update Mode and Source

The method in which RUGGEDCOM ROX II discovers and downloads firmware updates is user configurable. The source can also be configured to point to a remote upgrade server or a local USB flash drive.

To upgrade the firmware update mode and source, do the following:

1. If the firmware will be distributed via a remote upgrade server, make sure the upgrade server is configured and the latest firmware version has been added. This may be the same upgrade server used to distribute software updates. For more information, refer to Section 4.12.2, "Setting Up an Upgrade Server".
2. Make sure a cellular modem interface is enabled. For more information, refer to Section 11.2.2, "Configuring a Cellular Modem Interface".
3. Change the mode to **Edit Private** or **Edit Exclusive**.
4. Navigate to ***interface » wan » {interface} » lte » firmware-upgrade***, where *{interface}* is the cellular modem interface. The **Firmware Update Settings** form appears.

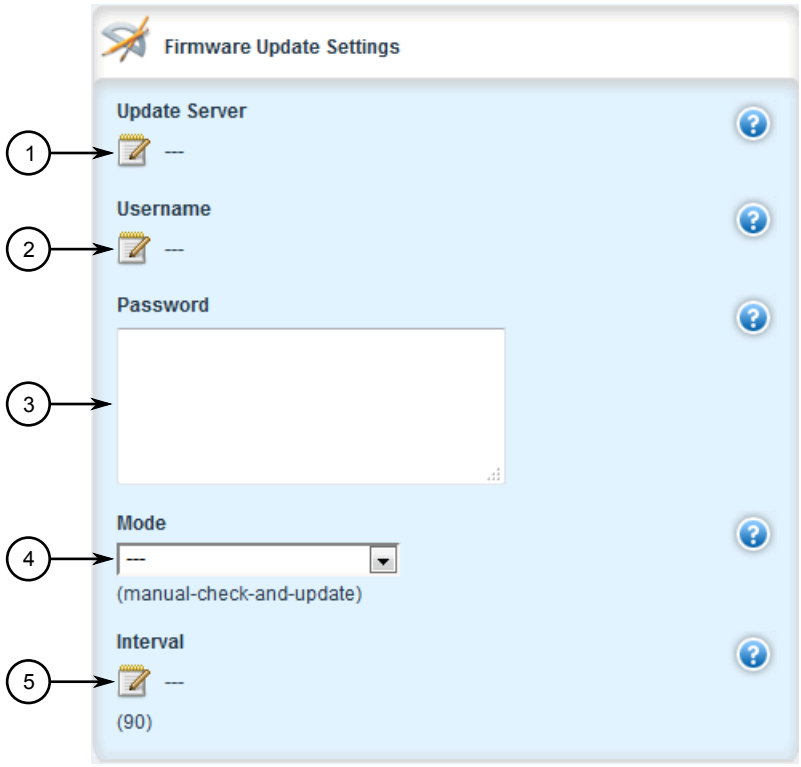


Figure 519: Firmware Update Settings Form

1. Update Server Box **2.** Username Box **3.** Password Box **4.** Mode List **5.** Interval Box

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

Parameter	Description
Update Server	**Synopsis:** A string 1 to 256 characters long The URL of the firmware to download. Supported URIs are HTTP, HTTPS, USB and SD. To update from a USB flash drive or microSD card (if applicable), the URL format is "usb://device-name/path-to-file-on-system" or "sd://device-name/path-to-file-on-system". To determine the device name, insert the storage medium and either navigate "chassis", "storage", "removable" (Web UI) or type "show chassis". For all other protocols, the format is "protocol://host:port/path-to-file". When using the default port for the protocol, omit ":port".
username	**Synopsis:** A string 1 to 64 characters long The user name required to connect with the upgrade server.
password	**Synopsis:** A string 1 to 1024 characters long The password associated with the username
mode	**Synopsis:** { manual-check-and-update, auto-check-manual-update, auto-check-and-update } **Default:** manual-check-and-update The update mode. Options include: * manual-check-and-update - FOTA checks and installs the firmware when initiated by the user

Parameter	Description
	* auto-check-manual-update - FOTA checks for new firmware automatically and installs updates when initiated by the user * auto-check-and-update - FOTA checks for and installs new firmware automatically
interval	**Synopsis:** A 16-bit unsigned integer between 1 and 365 **Default:** 90 The number of days to wait before automatically checking for new firmware.

6. 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 11.6.6.3
Launching a Firmware Update

To manually launch a firmware update, do the following:

NOTE
If the upgrade fails, refer to Section 19.6, "Firmware Updates".

1. Make sure the firmware update mode and source have been configured. For more information, refer to Section 11.6.6.2, "Configuring the Firmware Update Mode and Source".
2. If updating the device via USB flash drive, insert the drive in the device. For more information, refer to the Installation Guide for the RUGGEDCOM RX1500/RX1501/RX1510/RX1511/RX1512.
3. If updating the device remotely, make sure the firmware has been added to the upgrade server. For more information, refer to Section 4.12.2.3, "Adding Firmware Releases to the Upgrade Server".
4. Navigate to ***interfaces » cellmodem » {interface} » firmware-update***, where *{interface}* is the cellular modem interface.
5. Click **launch-update**. The Trigger Action form appears.

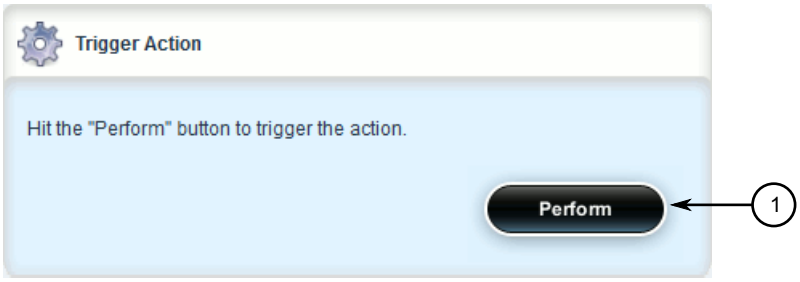


Figure 520: Trigger Action Form

1. Perform Button

IMPORTANT!
If power is interrupted during the upgrade, the device will become unrecoverable. If this occurs, contact Siemens Customer Support.

IMPORTANT!
Changes to the LTE modem configuration are not permitted until the upgrade is complete.

6. On the **Trigger Action** form, click **Perform** to launch the upgrade.

12 Tunneling and VPNs

This chapter describes how to configure various tunnels and Virtual Private Networks (VPNs).

CONTENTS

Section 12.1

Configuring L2TP Tunnels

The Layer Two Tunneling Protocol (L2TP) is used primarily to tunnel Point-to-Point Protocol (PPP) packets through an IP network, although it is also capable of tunneling other Layer 2 protocols.

RUGGEDCOM ROX II utilizes L2TPD in conjunction with Libreswan and PPP to provide support for establishing a secure, private connection with the router using the Microsoft Windows VPN/L2TP client.

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.

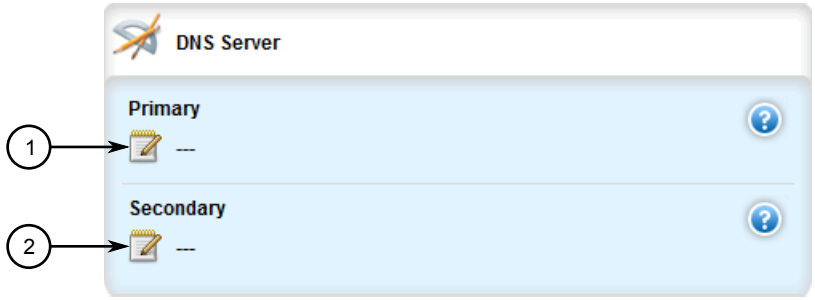


Figure 521: DNS Server Form

1. Primary Box **2.** Secondary Box

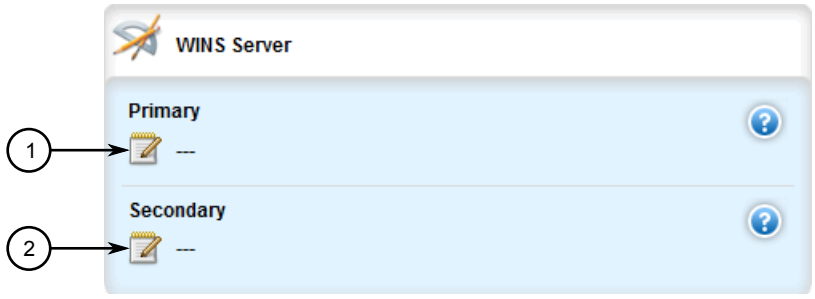


Figure 522: WINS Server Form

1. Primary Box **2.** Secondary Box

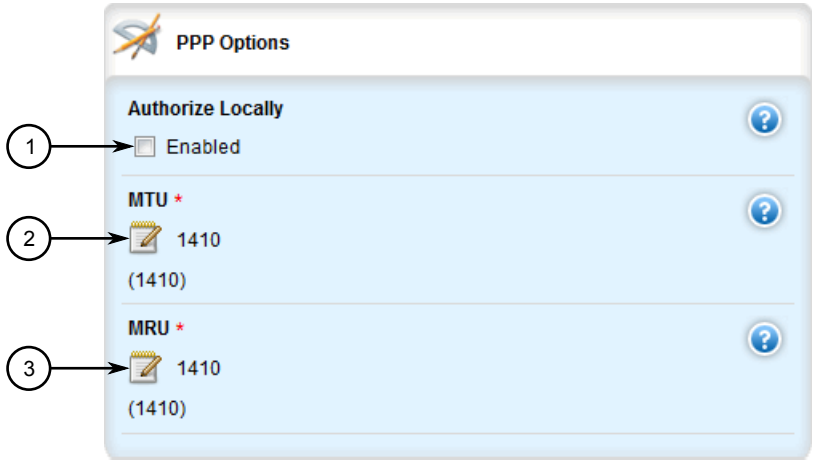


Figure 523: PPP Options Form

1. Authorize Locally Check Box **2.** MTU Box **3.** MRU Box

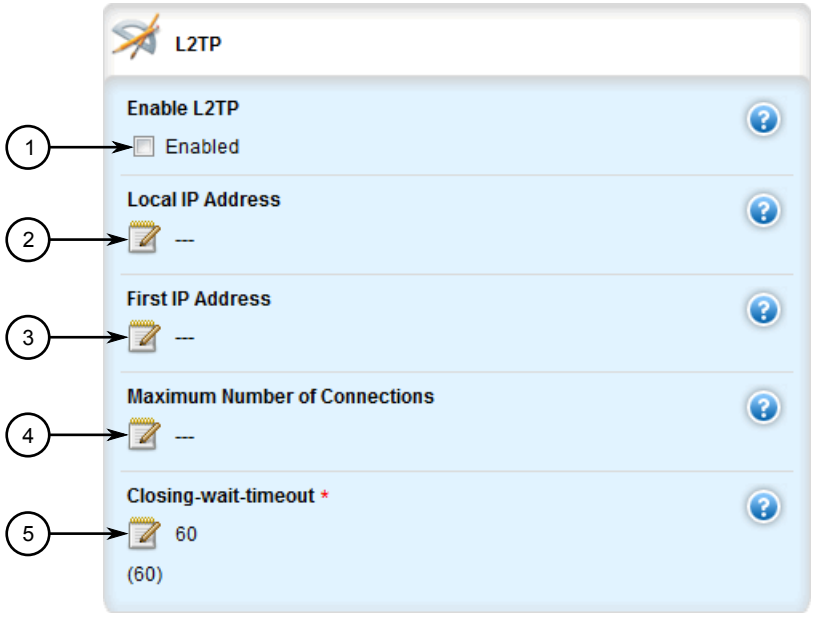


Figure 524: L2TP Form

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	**Synopsis:** A string 7 to 15 characters long The primary DNS server.
Secondary	**Synopsis:** 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	**Synopsis:** A string 7 to 15 characters long The primary WINS server.
Secondary	**Synopsis:** 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 6.6.3.2, "Configuring RADIUS Authentication for PPP Services".*

Parameter	Description
Authorize Locally	Authorizes locally instead of using radius server.
MTU	**Synopsis:** A 32-bit signed integer between 68 and 9216 **Default:** 1410 The Maximum Transmit Unit (MTU) or maximum packet size transmitted.
MRU	**Synopsis:** A 32-bit signed integer between 68 and 9216 **Default:** 1410 The Maximum Receive Unit (MRU) or maximum packet size passed when received.

6. On the **L2TP** form, configure the following parameter(s) as required:

Parameter	Description
Enable L2TP	Enables L2TP.
Local IP Address	**Synopsis:** A string 7 to 15 characters long The local IP address. When set, all L2TP interfaces (l2tp-ppp-0, l2tp-ppp-1, etc.) will use the same IP address. To use different local IP addresses (chosen from an IP pool) for different L2TP interfaces, leave this parameter empty.
First IP Address	**Synopsis:** A string 7 to 15 characters long The first address in the IP address pool. If local-ip is not set, both local and remote IP addresses will be taken from this pool.
Maximum Number of Connections	**Synopsis:** A 32-bit unsigned integer between 1 and 10 The maximum number of connections.
Closing Wait Timeout	**Synopsis:** A 32-bit unsigned integer between 5 and 120 **Default:** 60 The number of seconds to wait before the tunnel is cleaned up after the tunnel moves to closing-wait state.

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 12.2
Managing Virtual Switches

Virtual switches bridge different network segments together in a way that is independent of any particular protocol.

Network traffic between segments is forwarded regardless of the IP and MAC addresses defined in the packet. In a virtual switch, forwarding is done in Layer 2 and allows all network traffic, including Layer 2 Multicast (i.e. GOOSE, ISO), IP Multicast, Unicast and Broadcast messages, to travel through the virtual switch tunnel without any modifications.

A virtual switch can be useful, in particular, for GOOSE messaging when the sender and receiver need to communicate through a routable IP network. Since there is no IP encapsulation for the Layer 2 traffic going through the virtual switch, network latency is minimized for the traffic between end devices.

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

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

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

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

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

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

- Be careful when adding a VLAN interface (assigned to a switch port on a given line module) in the virtual switch. The VLAN tag on a tagged frame received on the VLAN interface of a switch port may not be preserved when the traffic is egressed through a routable interface (i.e. T1/E1 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 6.8.10, "Managing Interfaces".

CONTENTS

Section 12.2.1
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.

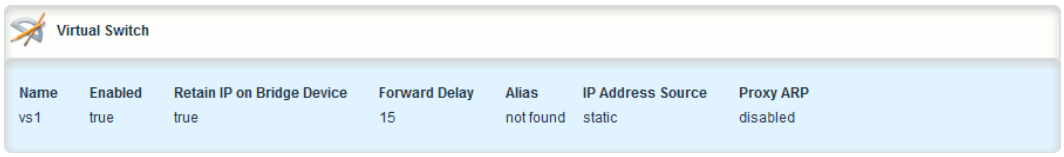


Figure 525: Virtual Switch Table

If no virtual switches have been configured, add virtual switches as needed. For more information, refer to Section 12.2.2, "Adding a Virtual Switch".

Section 12.2.2
Adding a Virtual Switch

To add a 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.

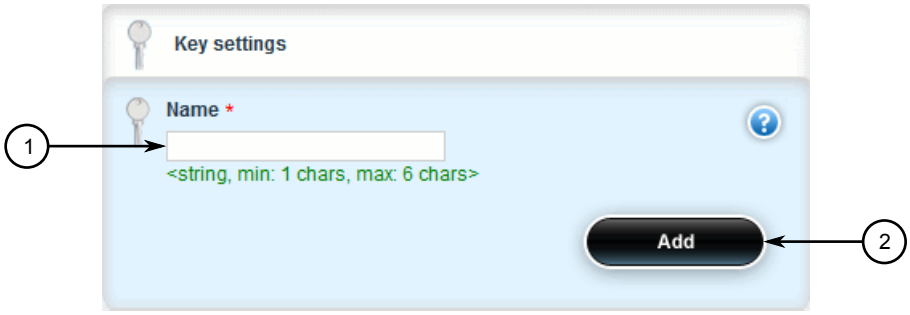


Figure 526: Key Settings Form

1. Name Box **2.** Add Button

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

Parameter	Description
Name	**Synopsis:** A string 1 to 6 characters long 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.

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

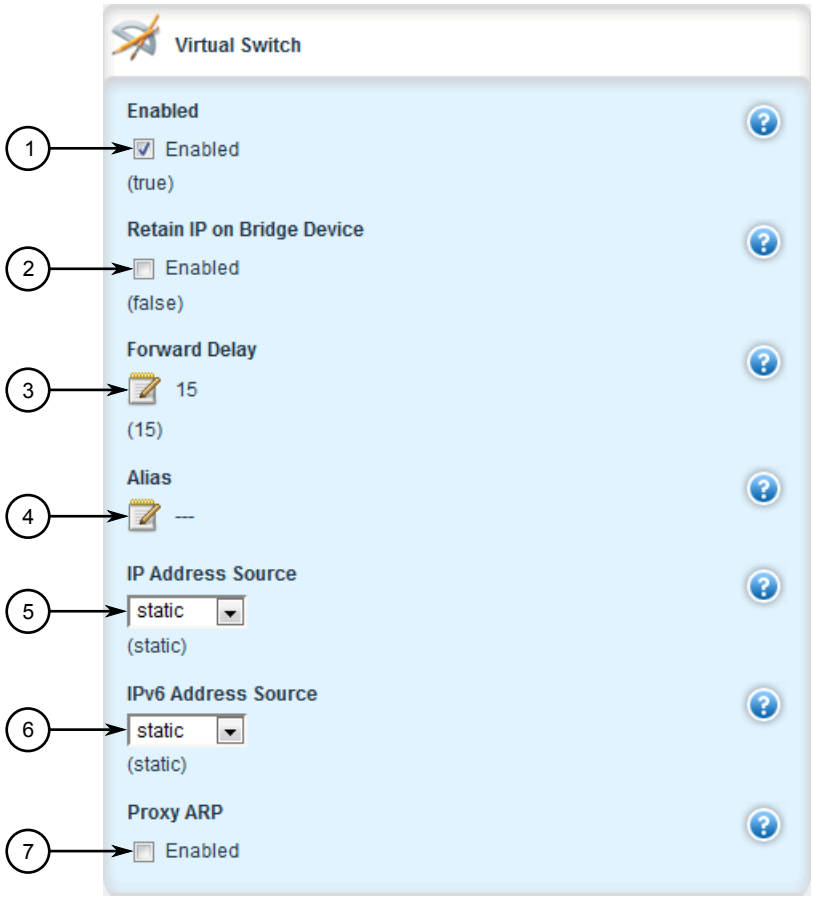


Figure 527: Virtual Switch Form

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.** IPv6 Address Source List **7.** ProxyARP Check Box

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

Parameter	Description
Enabled	**Synopsis:** { true, false } **Default:** true Enables this interface.
Retain IP on Bridge Device	**Synopsis:** { true, false } **Default:** false Retain IP on bridge device.
Forward Delay	**Synopsis:** An 8-bit unsigned integer **Default:** 15 Delay (in seconds) of the listening and learning state before goes to forwarding state.
Alias	**Synopsis:** A string 1 to 64 characters long The SNMP alias name of the interface
IP Address Source	**Synopsis:** { static, dynamic } **Default:** static

Parameter	Description
	Whether the IP address is static or dynamically assigned via DHCP or BOOTP.
IPv6 Address Source	**Synopsis:** { static, dynamic } **Default:** static Whether the IPv6 address is static or dynamically assigned via DHCPv6.
Proxy ARP	Enables/Disables whether the port will respond to ARP requests for hosts other than itself

6. Add one or more interfaces for the virtual switch. For more information, refer to Section 12.2.4.2, "Adding a Virtual Switch Interface".
7. If *`IP Address Source`* or *`IPv6 Address Source`* is set to `static`, assign an IP address to the virtual switch if required. For more information, refer to either Section 7.1.3.2, "Adding an IPv4 Address" or Section 7.1.4.2, "Adding an IPv6 Address".
8. [Optional] Assign one or more VLANs to the virtual switch. For more information, refer to Section 12.2.8.2, "Adding a Virtual Switch VLAN".
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 12.2.3
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.

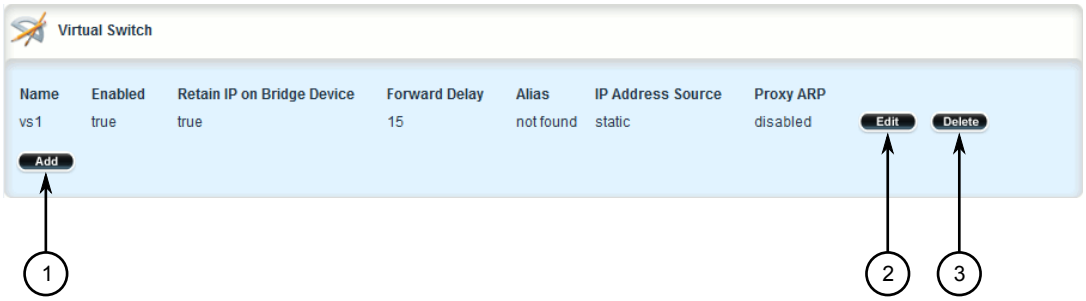


Figure 528: Virtual Switch Table

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

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 12.2.4
Managing Virtual Switch Interfaces

This section describes how to configure and manage interfaces for virtual switches.

CONTENTS

Section 12.2.4.1
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.

Figure 529: Interface Table

If no virtual switch interfaces have been configured, add interfaces as needed. For more information, refer to Section 12.2.4.2, "Adding a Virtual Switch Interface".

Section 12.2.4.2
Adding a Virtual Switch Interface

To add a virtual switch interface, do the following:

IMPORTANT!
At least two interfaces are required for a virtual switch bridge.

CAUTION!
Accessibility hazard – risk of access disruption. Do not select the interface used to the access the Web interface. Active Web sessions will be lost and the Web interface will be unreachable until the virtual switch is disabled.

NOTE
*The **wlan-cl1** interface is not supported as a virtual switch interface.*

1. 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.

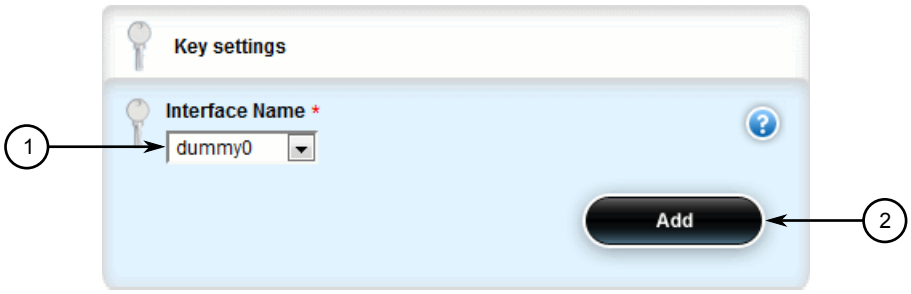


Figure 530: Key Settings Form

1. Interface Name Box **2.** Add Button

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

Parameter	Description
Interface Name	**Synopsis:** A string Interface name.

5. Click **Add** to add the selected interface to the virtual switch. The new virtual switch is now visible under the **ip** menu with the prefix *vsw-* (i.e. vsw-vs1, vsw-vs2, etc.).
6. Assign an IPv4 or IPv6 address to the interface. For more information, refer to Section 7.1.3.2, "Adding an IPv4 Address" or Section 7.1.4.2, "Adding an IPv6 Address".
7. If necessary, add one or more VLANs to the virtual switch interface. For more information, refer to Section 12.2.8.2, "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 12.2.4.3

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.

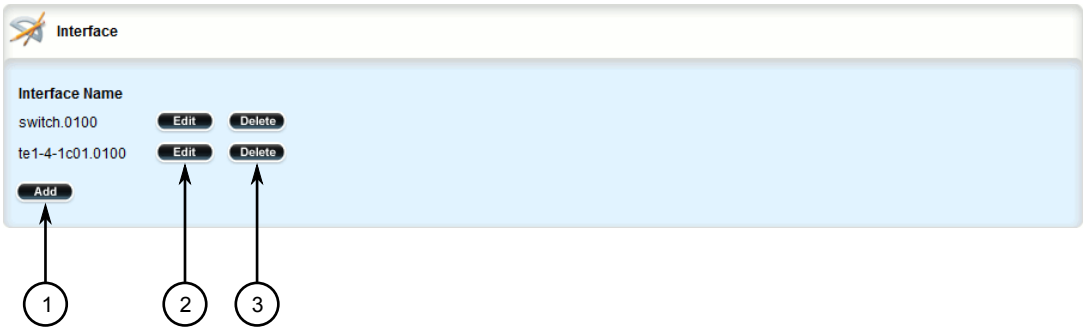


Figure 531: Interface Table

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 12.2.5

Filtering Virtual Switch Traffic

Packets traversing a virtual switch can be filtered based on source MAC address, destination MAC address, and/or protocol (e.g. iso, arp, ipv4, ipv6, etc.). Rules are defined separately and can be applied uniquely to each virtual switch as needed. For example, a single filter can detect traffic destined for a specific MAC address entering via fe-cm-1 and reroute it to switch-001. At the same time, It can also detect and drop any other type of traffic.

CONTENTS

Section 12.2.5.1

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.

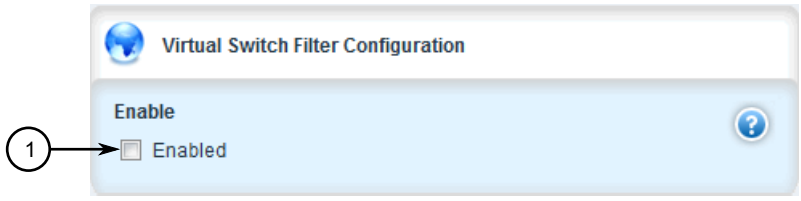


Figure 532: Virtual Switch Filter Configuration Form

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 12.2.2, "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 12.2.5.2
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 **Virtual Switch** table appears.

Figure 533: Virtual Switch Table

If no virtual switch filters have been configured, add filters as needed. For more information, refer to Section 12.2.5.3, "Adding a Virtual Switch Filter".

Section 12.2.5.3
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 12.2.2, "Adding a Virtual Switch".

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

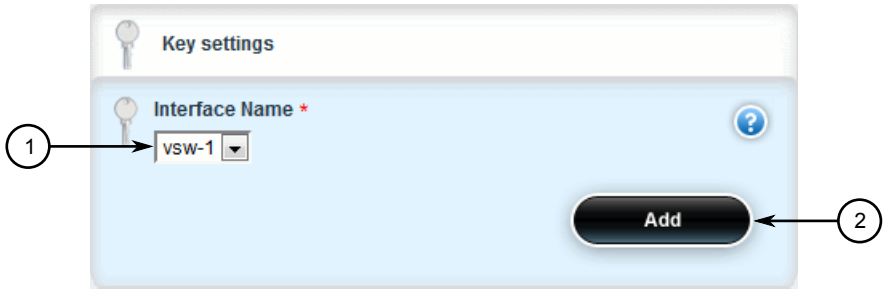


Figure 534: Key Settings Form

1. Interface Name Box **2.** Add Button

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

Parameter	Description
Interface Name	**Synopsis:** A string The name of the target virtual switch. This parameter is mandatory.

5. Configure one or more rules to be used when filtering. For more information, refer to Section 12.2.6.3, "Adding a Rule".
6. Add the desired rules to the virtual switch filter. For more information, refer to Section 12.2.6.4, "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 12.2.5.4

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 **Virtual Switch** table appears.

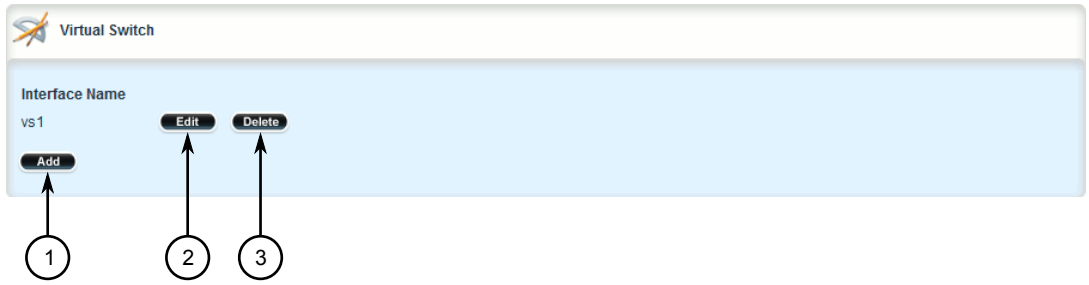


Figure 535: Virtual Switch Table

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 12.2.6

Managing Filtering Rules

A virtual switch filter can apply one or more rules to traffic traversing a virtual switch.

CONTENTS

Section 12.2.6.1

Viewing a List of Rules

To view a list of rules that can be used by a virtual switch filter, navigate to ***security » virtualswitch-filter » rules***. If rules have been configured, the **Filter Rule Configuration** table appears.


Filter Rule Configuration

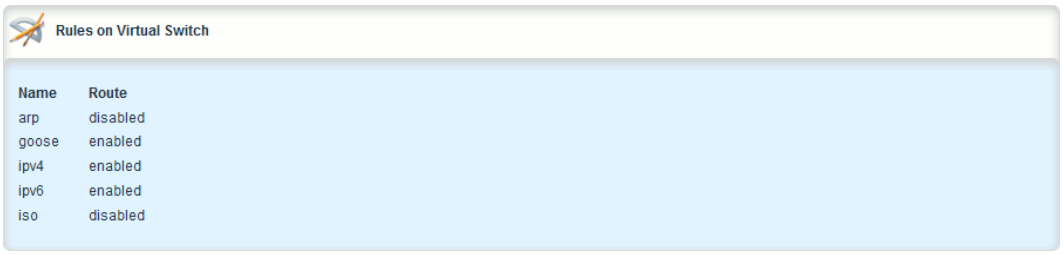
Name	Action	Source MAC Address	Destination MAC Address	Protocol
arp	accept	not found	not found	arp
goose	accept	00:00:00:00:11:11	01:0c:cd:01:00:33	0x88b8
ipv4	accept	00:00:00:00:00:01	00:00:00:00:00:02	ipv4
ipv6	accept	not found	not found	ipv6
iso	accept	not found	not found	iso

Figure 536: Filter Rule Configuration Table

If no rules have been configured, add rules as needed. For more information, refer to Section 12.2.6.3, "Adding a Rule".

Section 12.2.6.2
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.


Rules on Virtual Switch

Name	Route
arp	disabled
goose	enabled
ipv4	enabled
ipv6	enabled
iso	disabled

Figure 537: Rules on Virtual Switch Table

If no rules have been assigned, assign them as needed. For more information, refer to Section 12.2.6.4, "Adding a Rule to a Virtual Switch Filter".

Section 12.2.6.3
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.

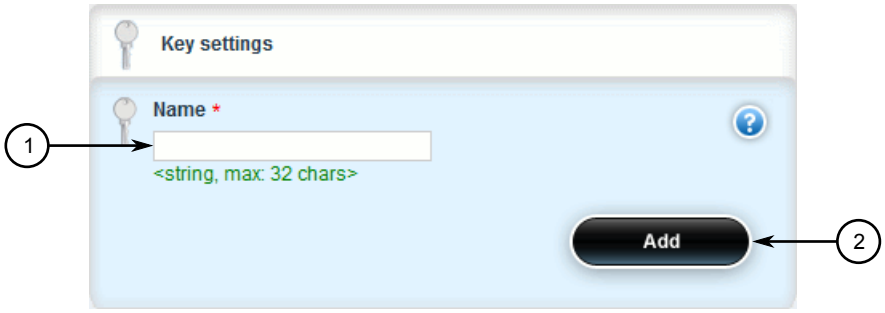


Figure 538: Key Settings Form

1. Name Box **2.** Add Button

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

Parameter	Description
Name	**Synopsis:** A string 1 to 32 characters long Description of vitual switch rule This parameter is mandatory.

4. Click **Add**. The **Virtual Switch Rules** form appears.

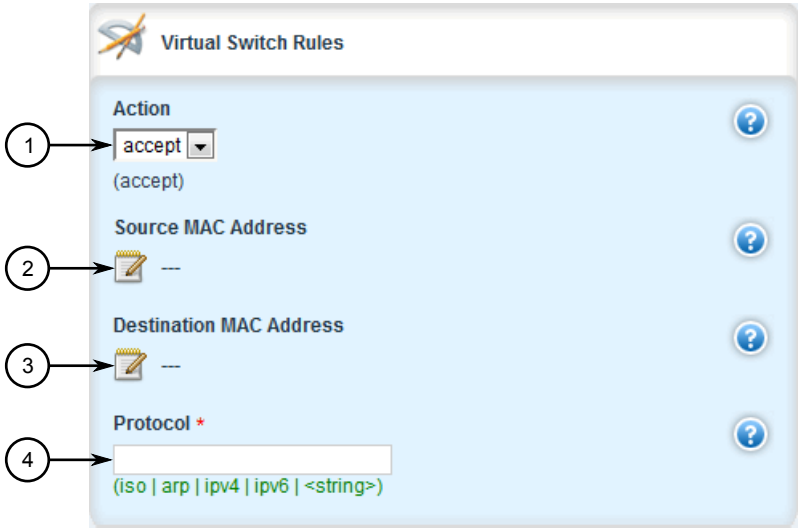


Figure 539: Virtual Switch Rules Form

1. Action List **2.** Source MAC Address Box **3.** Destination MAC Address Box **4.** Protocol Box

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

Parameter	Description
Action	**Synopsis:** { accept, drop } **Default:** accept The action taken when an incoming frame meets the criteria.

Parameter	Description
Source MAC Address	**Synopsis:** A string 17 characters long The required source MAC address for incoming frames.
Destination MAC Address	**Synopsis:** A string 17 characters long The required destination MAC address for incoming frames.
Protocol	**Synopsis:** { iso, arp, ipv4, ipv6 } or a string The pre-defined protocol or hex-string (i.e. 0x88A2) used to create the frames. This parameter is mandatory.

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.
8. Add the rule to a virtual switch filter. For more information, refer to Section 12.2.6.4, "Adding a Rule to a Virtual Switch Filter".

Section 12.2.6.4
Adding a Rule to a Virtual Switch Filter

To add a rule to 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*** and click **<Add rule>**. The **Key Settings** form appears.

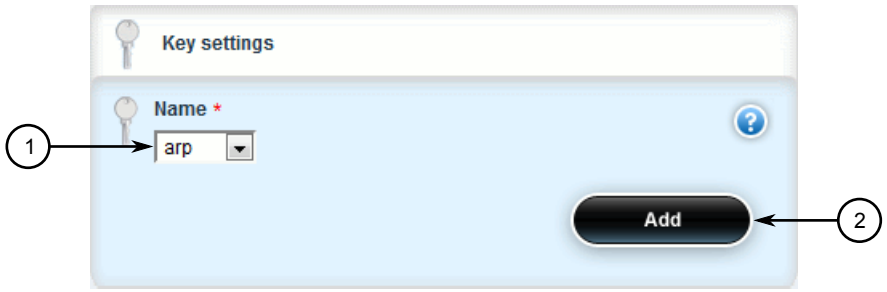


Figure 540: Key Settings Form

1. Name Box **2.** Add Button

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

Parameter	Description
name	**Synopsis:** A string The rule applied to traffic traversing the virtual switch. This parameter is mandatory.
Route	Enables or disables route mode, which routes IP traffic received by the virtual switch interface.

4. Click **Add**. The **Virtual Switch Routing** form appears.

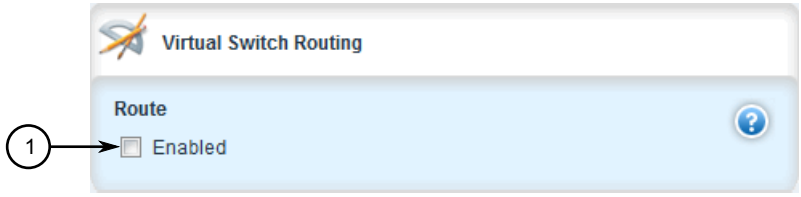


Figure 541: Virtual Switch Routing Form

1. Enabled Check Box

5. Select **Enabled**.
6. Configure the in/out interfaces for the rule. For more information, refer to Section 12.2.7.2, "Adding an In/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 12.2.6.5

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.

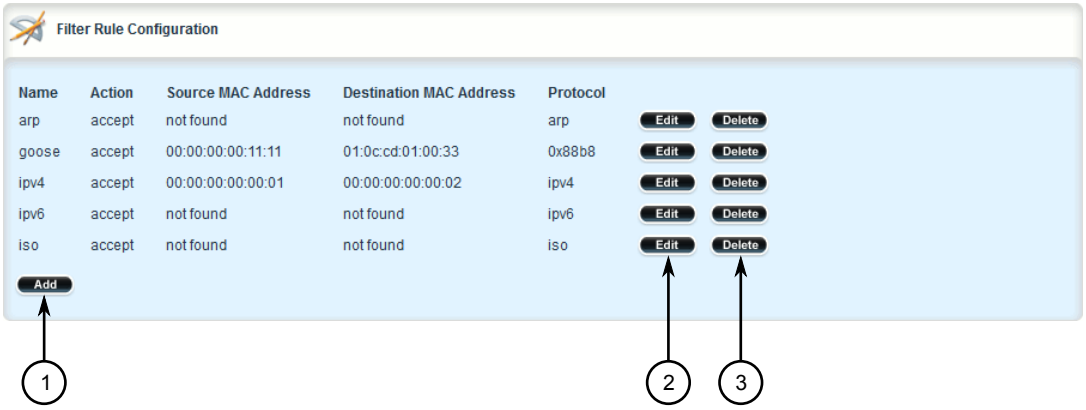


Figure 542: Filter Rule Configuration Table

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

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 12.2.6.6

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.

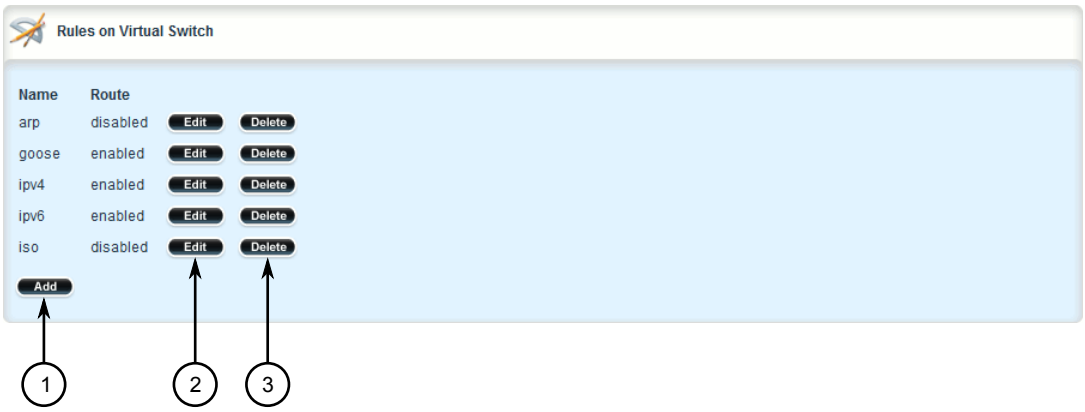


Figure 543: Rules on Virtual Switch Table

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

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 12.2.7

Managing In/Out Interfaces

In/out interfaces for virtual switch filters represent the interface being monitored by the filter (*in* interface) and the destination interface (*out* interface) for network traffic that meets the filter's criteria.

CONTENTS

Section 12.2.7.1
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 Virtual Switch** or **Rules on an Out-Interface Virtual Switch** table appears.

Figure 544: Rules on an In-Interface Virtual Switch Table (Example)

If no in/out interfaces have been configured, add interfaces as needed. For more information, refer to Section 12.2.7.2, "Adding an In/Out Interface".

Section 12.2.7.2
Adding an In/Out Interface

To add an in/out interface that can be used by a virtual switch filter, do the following:

1. 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 545: Key Settings Form

1. Name List **2.** Add Button

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

Parameter	Description
name	**Synopsis:** A string 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 12.2.7.3
Deleting an In/Out Interface

To delete an in/out interface that can be used by a virtual switch filter, do the following:

1. 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 Virtual Switch** or **Rules on an Out-Interface Virtual Switch** table appears.

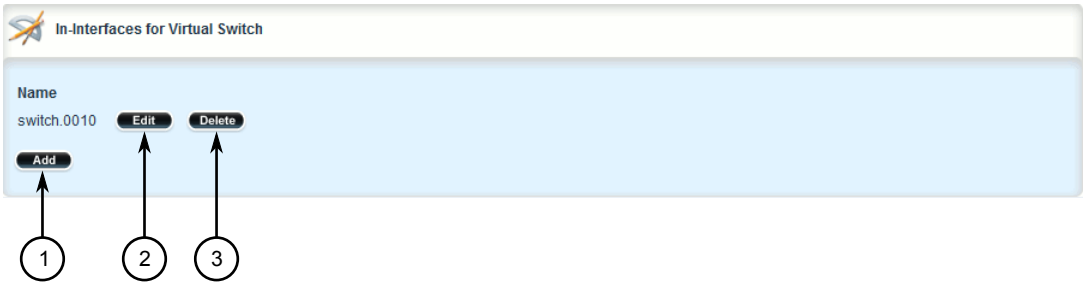


Figure 546: Rules on an In-Interface Virtual Switch Table

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 12.2.8
Managing VLANs for Virtual Switches

This section describes how to configure and manage VLANs for virtual switches.

CONTENTS

Section 12.2.8.1
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.

Figure 547: VLAN Table

If no virtual switch VLANs have been configured, add VLANs as needed. For more information, refer to Section 12.2.8.2, "Adding a Virtual Switch VLAN".

Section 12.2.8.2
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.

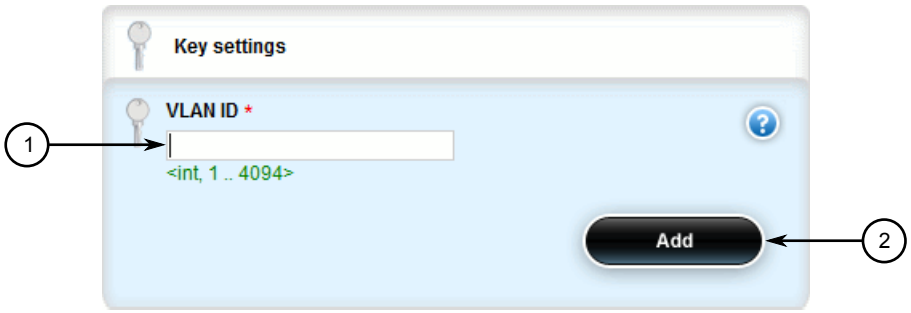


Figure 548: Key Settings Form

1. VLAN ID Box **2.** Add Button

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

Parameter	Description
VLAN ID	**Synopsis:** A 32-bit signed integer between 1 and 4094 VLAN ID for this routable logical interface

5. Click **Add** to create the new VLAN. The **VLAN** form appears.

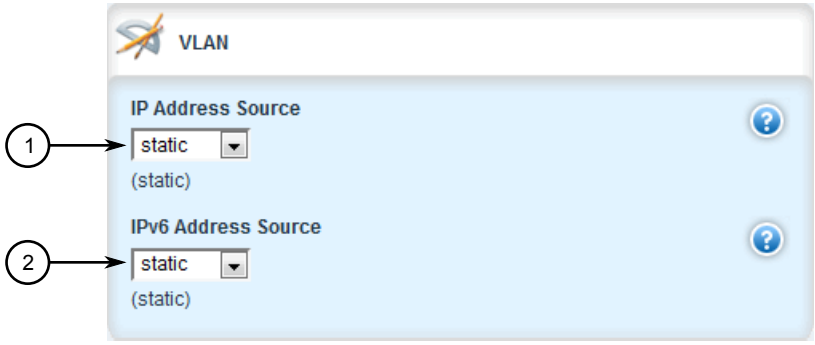


Figure 549: VLAN Form

1. IP Address Source Box **2.** IPv6 Address Source Box

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

Parameter	Description
IP Address Source	**Synopsis:** { static, dynamic } **Default:** static Whether the IP address is static or dynamically assigned via DHCP or BOOTP.
IPv6 Address Source	**Synopsis:** { static, dynamic } **Default:** static Whether the IPv6 address is static or dynamically assigned via DHCPv6

7. [Optional] Add a QoS map. For more information, refer to Section 16.2.7.2, "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 12.2.8.3
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.

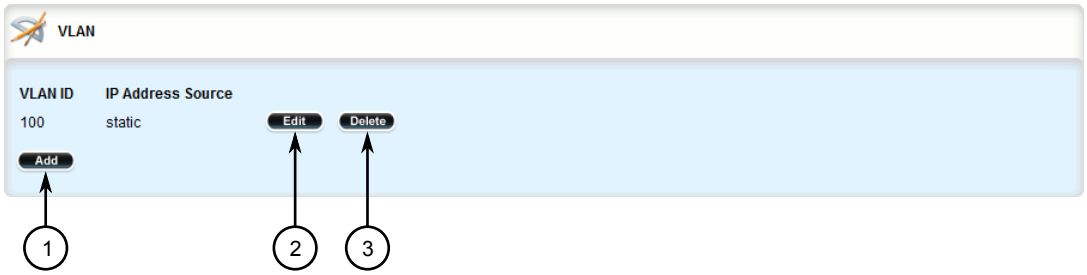


Figure 550: VLAN Table

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 12.3

Managing the Layer2 Tunnel Daemon

RUGGEDCOM ROX II is capable of extending the range of services that communicate solely via Layer 2 protocols (i.e. at the level of Ethernet) by tunneling them over routed IP networks. The Layer 2 Tunnel Daemon supports the IEC61850 GOOSE protocol as well as a generic mechanism for tunneling by Ethernet type.

CONTENTS

Section 12.3.1

Viewing Round Trip Time Statistics

The round trip time statistics reflect the measured round trip time to each remote daemon. The minimum, average, maximum and standard deviation of times is presented. Entries with a large difference between the **Transmitted** and **Received** parameters indicate potential problems.

To view the round trip time statistics, navigate to ***tunnel » l2tunneld » 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 12.6.5, "Managing Remote Daemon IP Addresses for Generic Tunnels".

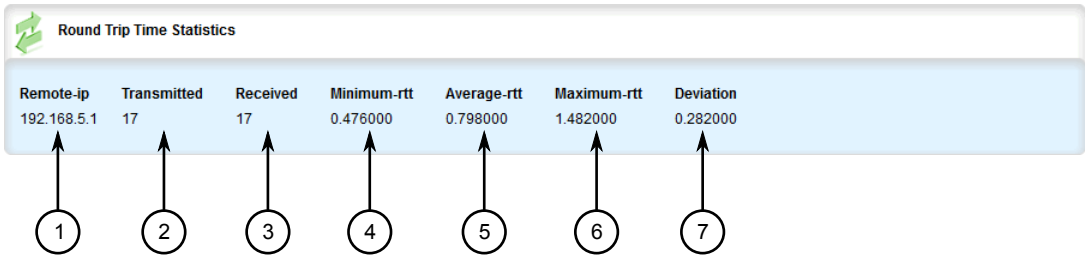


Figure 551: Round Trip Time Statistics Form

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	**Synopsis:** A string 7 to 15 characters long The IP address of remote daemon. This parameter is mandatory.
transmitted	**Synopsis:** A 32-bit unsigned integer The number of beacon frames transmitted through the tunnel. This parameter is mandatory.
received	**Synopsis:** A 32-bit unsigned integer The number of beacon frames received through the tunnel. This parameter is mandatory.
Minimum RTT	**Synopsis:** A string 1 to 32 characters long The Minimum Beacon Round-Trip-Time. This parameter is mandatory.
Average RTT	**Synopsis:** A string 1 to 32 characters long The Average Beacon Round-Trip-Time. This parameter is mandatory.
Maximum RTT	**Synopsis:** A string 1 to 32 characters long The Maximum Beacon Round-Trip-Time. This parameter is mandatory.
deviation	**Synopsis:** A string 1 to 32 characters long The standard deviation. This parameter is mandatory.

Section 12.3.2
Configuring the Layer 2 Tunnel Daemon

To configure the Layer 2 tunnel daemon, do the following:

IMPORTANT!
Make sure there are no traffic loops possible between the substation LAN and other LANs that could forward GOOSE frames to the LAN. Do not employ a GOOSE gateway between substations that are already connected. The GOOSE daemon issues packets to the network with a built in Time-To-Live (TTL) count that is decremented with each transmission. This prevents an infinite loop of packets, but will not prevent excessive network utilization.

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to ***tunnel » l2tunneld***. The **L2 Tunnel Daemon** form appears.

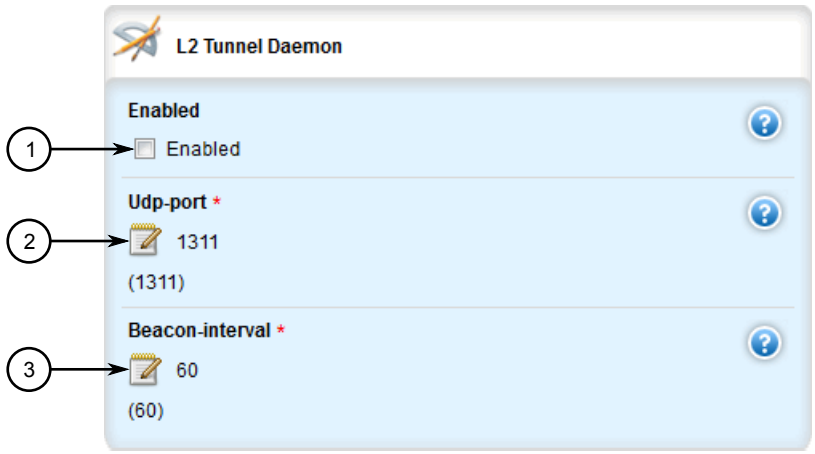


Figure 552: L2 Tunnel Daemon Form

1. Enabled Check Box **2.** UDP Port Box **3.** Beacon Interval Box

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

Parameter	Description
enabled	Enables the Layer 2 protocols server.
UDP Port	**Synopsis:** A 32-bit signed integer between 1 and 65535 **Default:** 1311 The UDP port to communicate with the other daemon.
Beacon Interval	**Synopsis:** { off } or a 32-bit signed integer between 10 and 3600 **Default:** 60 The Round Trip Time (RTT) of the sent message

4. Add GOOSE or generic tunnels as required. For more information, refer to Section 12.5.3, "Adding a GOOSE Tunnel" or Section 12.6.3, "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 12.4

Managing L2TPv3 Tunnels

L2TPv3 (Layer 2 Tunneling Protocol Version 3) provides a pseudo-wire service that encapsulates multi-protocol Layer 2 traffic over IP networks. There are no restrictions on the Layer 2 data formats that can be transmitted or received, unlike L2TP.

L2TPv3 is a simplified alternative to MPLS (Multiprotocol Label Switching) that offers improved performance (e.g. high data packet rate and low CPU consumption) over L2TP and and IP network.

Two types of L2TPv3 tunnels are available:

- **Static**
  A static L2TPv3 tunnel is a fixed connection between two Provider Edge devices (PE), where the session IDs and cookies are defined on both devices. This allows the devices to route Layer 2 traffic as soon as the session connects with the attachment circuit.
- **Dynamic**
  A dynamic LTPv3 tunnel creates sessions based on the dynamic exchange of control messages between the PE devices to determine the type of Layer 2 traffic that needs to be routed. Session IDs and cookies are generated by the devices themselves for each session. This allows L2TPv3 to reestablish sessions automatically in the case of a network failure.

IMPORTANT!
RUGGEDCOM ROX II supports a maximum of 128 tunnel sessions, which in turn support a maximum of 128 VLANs each.

CONTENTS

Section 12.4.1

L2TPv3 Tunnel Scenarios

The following illustrates some of the ways in which L2TPv3 tunnels can be implemented.

» Basic L2TPv3 Tunnel

In the following topology, an L2TPv3 tunnel is established between routers R1 and R2 over a WAN interface. The tunnel interface is assigned an IPv4 address on both devices. Traffic routed from R1 is encapsulated in an L2TPv3 header and decapsulated by R2. The reverse is true when traffic is routed from R2.

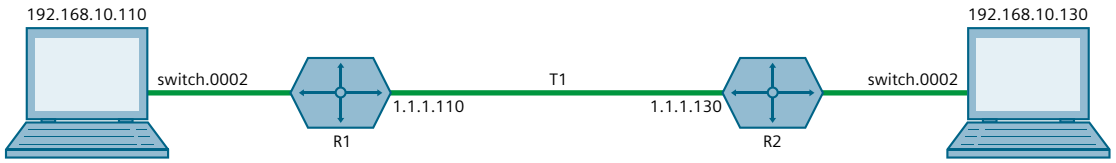


Figure 553: Basic L2TPv3 Tunnel

Multiple Sessions

In the following topology, separate bridges have been created between routers R1 and R2 using sessions. Traffic sent via virtual switch switch.0002 traverses the l2t-1-1 tunnel. Traffic sent via virtual switch switch.0003 traverses the l2t-1-2 tunnel.

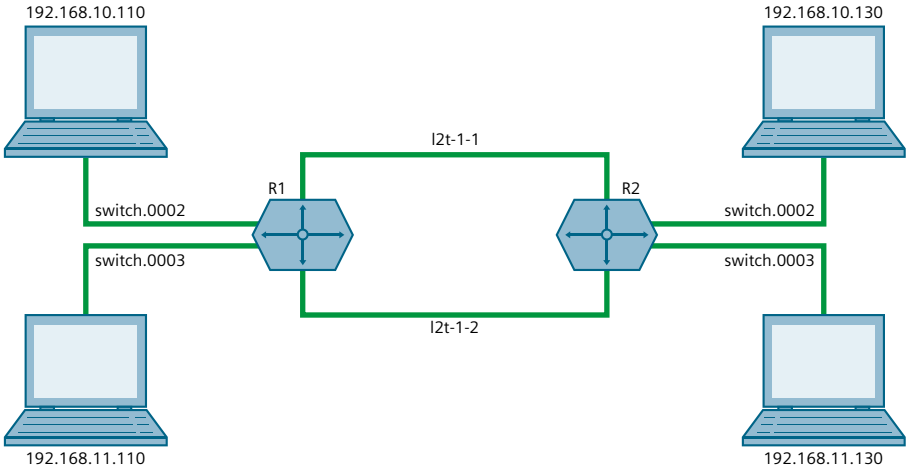


Figure 554: Multiple LAN Extensions Over a Single L2TPv3 Tunnel

Multiple L2TPv3 Tunnels

In the following topology, two L2TPv3 tunnels are configured: one from router R1 to R2, and another from R1 to R3. Each is converted to a bridge by the switch.0002 virtual switch.

Traffic sent from 192.158.10.110 to 192.168.10.130 traverses the l2t-1-1 bridge, and vice versa.

Traffic sent from 192.158.10.110 to 192.168.11.110 traverses the l2t-2-1 bridge, and vice versa.

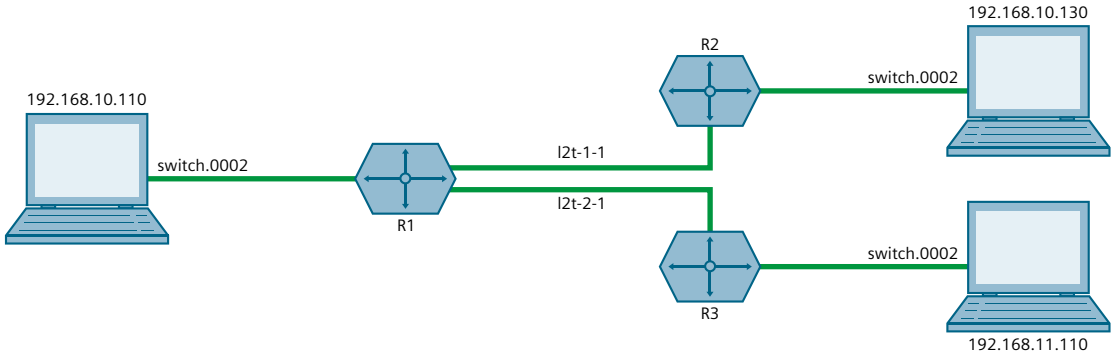


Figure 555: Multiple LAN Extensions Over Multiple L2TPv3 Tunnels

Section 12.4.2

Creating an L2TPv3 Tunnel

To create an L2TPv3 tunnel with another Provider Edge (PE) device, do the following:

1. **Create the L2TPv3 Tunnel Interface**

   An L2TPv3 tunnel interface is created automatically by RUGGEDCOM ROX II whenever a session is defined. The interface is listed under **ip** in the menu and adheres to the following naming convention:

   ```
   l2t-{tunnel-name}-{session-name}
   ```

   For example:

   ```
   l2t-1-2
   ```

   If the session is assigned a VLAN ID, an additional interface is generated in the form of:

   ```
   l2t-{tunnel-name}-{session-name}.{vlan-id}
   ```

   For example:

   ```
   l2t-1-2.0004
   ```

   To create the tunnel interface, start by adding a static or dynamic L2TPv3 tunnel. For more information, refer to either Section 12.4.3.3, “Adding a Static L2TPv3 Tunnel” or Section 12.4.4.3, “Adding a Dynamic L2TPv3 Tunnel”.

2. **Create a Virtual Switch or Assign an IP Address**

   The L2TPv3 tunnel interface is an Ethernet-like interface. As such, it can be added to a virtual switch to form a bridge, or assigned an IP address to route Layer 3 traffic.

   For information about adding the L2TPv3 tunnel interface to a virtual switch, refer to Section 12.2.4.2, “Adding a Virtual Switch Interface”.

   For information about assigning an IP address to the L2TPv3 tunnel interface, refer to either Section 7.1.3, “Managing IPv4 Addresses” or Section 7.1.4, “Managing IPv6 Addresses”.

Section 12.4.3

Managing Static L2TPv3 Tunnels

Configure static L2TPv3 tunnels to manually control tunnel and sessions parameters at both ends of the bridge. These fixed tunnels are referred to as *unmanaged*.

CONTENTS

Section 12.4.3.1

Enabling/Disabling Static L2TPv3 Tunnels

To enable or disable static L2TPv3 tunnels, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to ***tunnel » l2tpv4 » static***. The **Static L2TPv3 Tunnels** form appears.

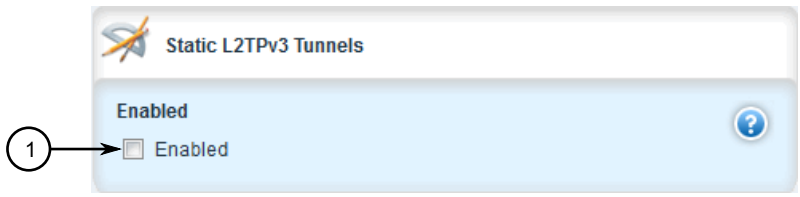


Figure 556: Static L2TPv3 Tunnels Form

1. Enabled Check Box

3. Select **Enabled** to enable static L2TPv3 tunnels, or clear **Enabled** to disable static L2TPv3 tunnels.
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 12.4.3.2

Viewing a List of Static L2TPv3 Tunnels

To view a list of static L2TPv3 tunnels, navigate to ***tunnel » l2tpv3 » static » tunnel***. If tunnels have been configured, the **Static L2TPv3 Tunnels** table appears.

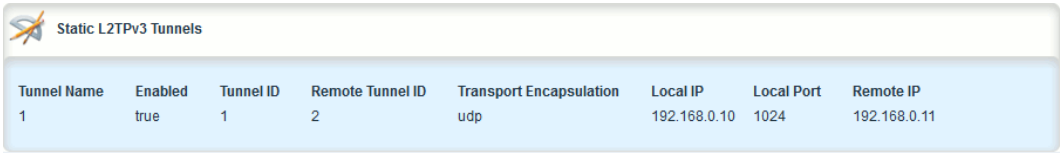


Figure 557: Static L2TPv3 Tunnels Table

If no tunnels have been configured, add tunnels as needed. For more information, refer to Section 12.4.3.3, "Adding a Static L2TPv3 Tunnel".

Section 12.4.3.3

Adding a Static L2TPv3 Tunnel

To add a static L2TPv3 tunnel, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to ***tunnel » l2tpv3 » static » tunnel*** and click **<Add tunnel>**. The **Key Settings** form appears.

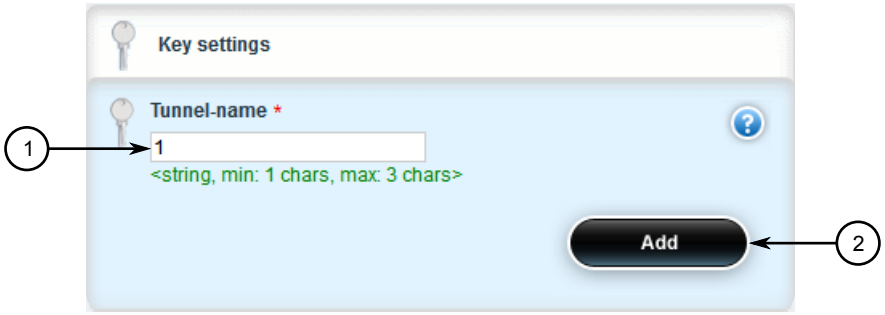


Figure 558: Key Settings Form

1. Tunnel Name Box **2.** Add Button

3. Configure the following parameters as required:

Parameter	Description
Tunnel Name	**Synopsis:** A string Tunnel name

4. Click **Add** to create the new tunnel. The **Static L2TPv3 Tunnels** form appears.

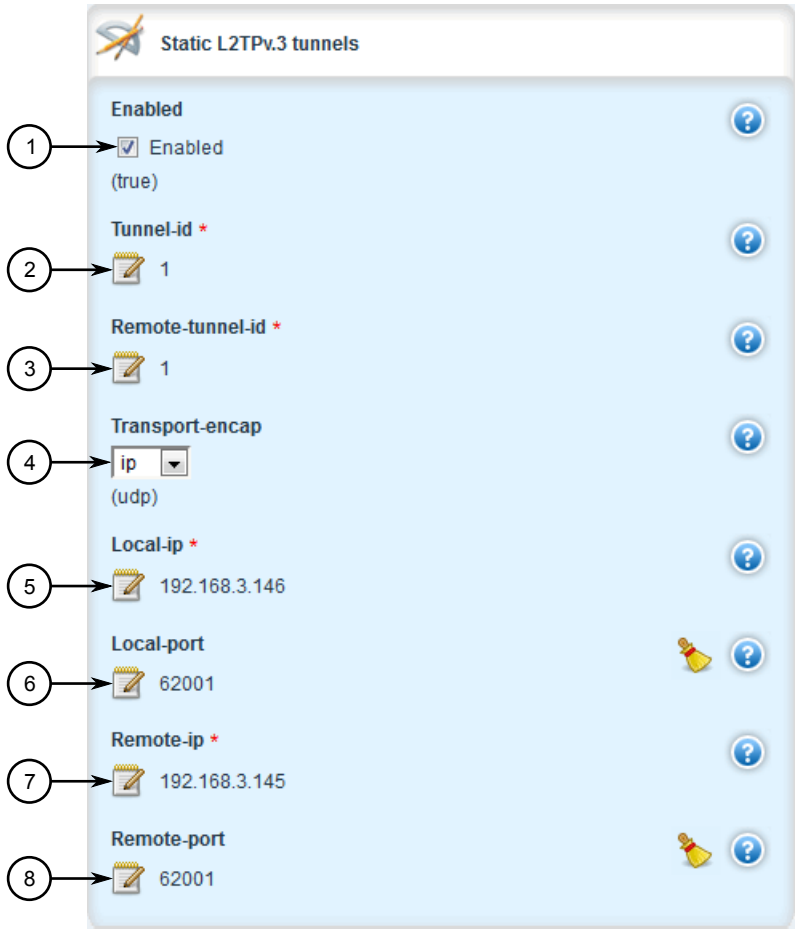


Figure 559: Static L2TPv3 Tunnels Form

1. Enabled Check Box **2.** Tunnel ID Box **3.** Remote Tunnel ID Box **4.** Transparent Encapsulation Box **5.** Local IP Box **6.** Remote IP Box **7.** Remote Port Box

5. Configure the following parameters as required:

Parameter	Description
Enabled	**Synopsis:** { true, false } **Default:** false Enables the static L2TPv3 tunnel.

Parameter	Description
Tunnel ID	**Synopsis:** A 32-bit signed integer Tunnel local id This parameter is mandatory.
Remote Tunnel ID	**Synopsis:** A 32-bit signed integer The remote tunnel-id This parameter is mandatory.
Transport Encapsulation	**Synopsis:** A string

Parameter	Description
	The transport encapsulation (UDP or IP). This parameter is mandatory.
Local IP	**Synopsis:** A string The interface upon which the tunnel is created This parameter is mandatory.
Local port	**Synopsis:** A 32-bit signed integer Local transport port for l2tpv3 service This parameter is mandatory.
Remote IP	**Synopsis:** A string 6 to 40 characters long Ip address of remote tunnel end This parameter is mandatory.
Remote port	**Synopsis:** A 32-bit signed integer Transport port of remote tunnel end This parameter is mandatory.
status	**Synopsis:** A string Current status of tunnel This parameter is mandatory.

6. Add one or more sessions to the tunnel configuration. For more information, refer to Section 12.4.5.2, "Adding a Session".
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 12.4.3.4
Deleting a Static L2TPv3 Tunnel

To delete a static L2TPv3 tunnel, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to ***tunnel » l2tpv3 » static » tunnel***. The **Static L2TPv3 Tunnels** table appears.

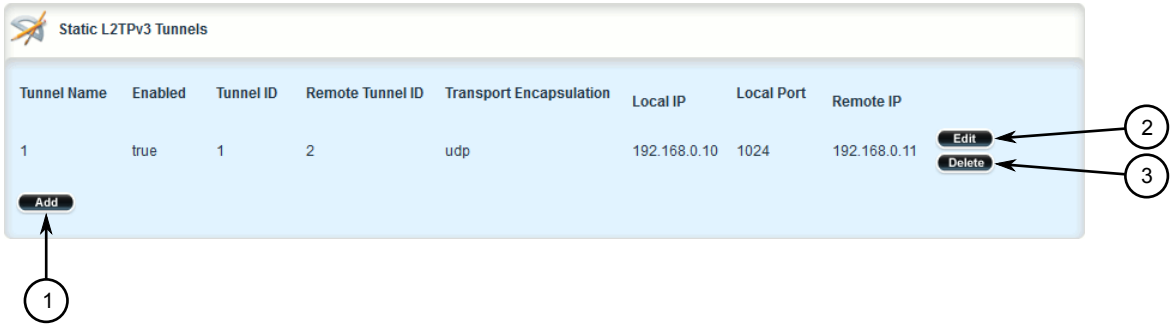


Figure 560: Static L2TPv3 Tunnels Table

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 12.4.4

Managing Dynamic L2TPv3 Tunnels

Configure dynamic L2TPv3 tunnels to carry Point-to-Point Protocol (PPP) traffic, as with L2TPv2, or when static L2TPv3 tunnels are not supported by the peer device. Dynamic L2TPv3 tunnels have the ability to automatically negotiate connections, and reestablish connections in the case of a network failure.

CONTENTS

Section 12.4.4.1

Enabling and Configuring Dynamic L2TPv3 Tunnels

To enable and configure dynamic L2TPv3 tunnels, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to ***tunnel » l2tpv4 » dynamic***. The **Dynamic L2TPv3 Tunnels** form appears.

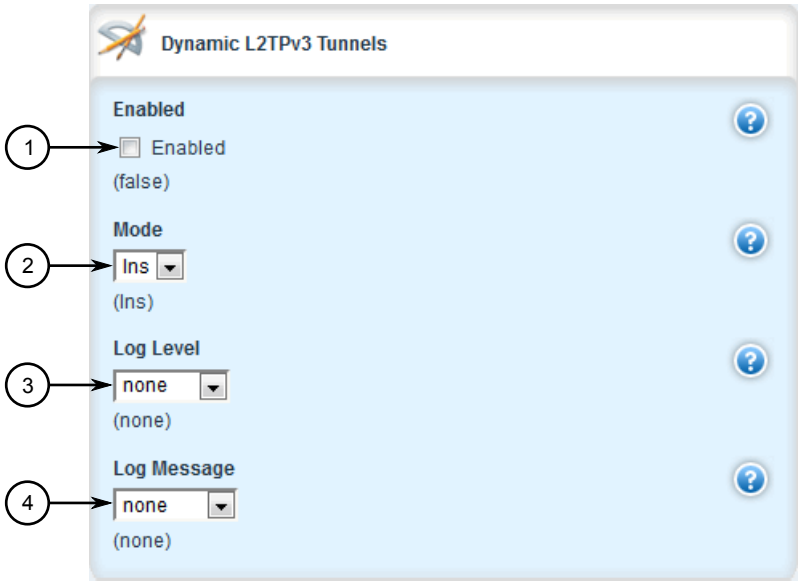


Figure 561: Dynamic L2TPv3 Tunnels Form

1. Enabled Check Box **2.** Mode List **3.** Log Level List **4.** Log Message List

3. Select **Enabled**and then configure the following parameters as required:

Parameter	Description
mode	**Synopsis:** { lac, lns } **Default:** lns The l2tp operational mode
Log Level	**Synopsis:** { none, error, warning, notice, info, all } **Default:** none Logging message level
Log Message	**Synopsis:** { none, protocol, fsm, api, transport, data, ppp, avp, func, system, all } **Default:** none Logging message category

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 12.4.4.2

Viewing a List of Dynamic L2TPv3 Tunnels

To view a list of dynamic L2TPv3 tunnels, navigate to ***tunnel » l2tpv3 » dynamic » tunnel***. If tunnels have been configured, the **Dynamic L2TPv3 Tunnels** table appears.

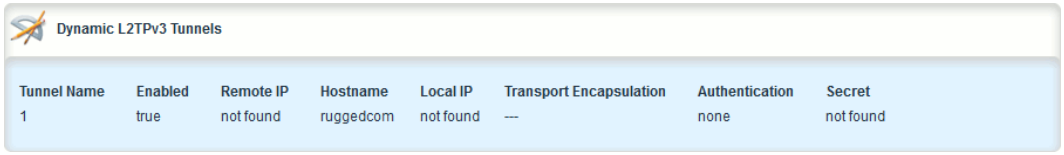


Figure 562: Dynamic L2TPv3 Tunnels Table

If no tunnels have been configured, add tunnels as needed. For more information, refer to Section 12.4.4.3, "Adding a Dynamic L2TPv3 Tunnel".

Section 12.4.4.3

Adding a Dynamic L2TPv3 Tunnel

To add a dynamic L2TPv3 tunnel, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to ***tunnel » l2tpv3 » dynamic » tunnel*** and click **<Add tunnel>**. The **Key Settings** form appears.

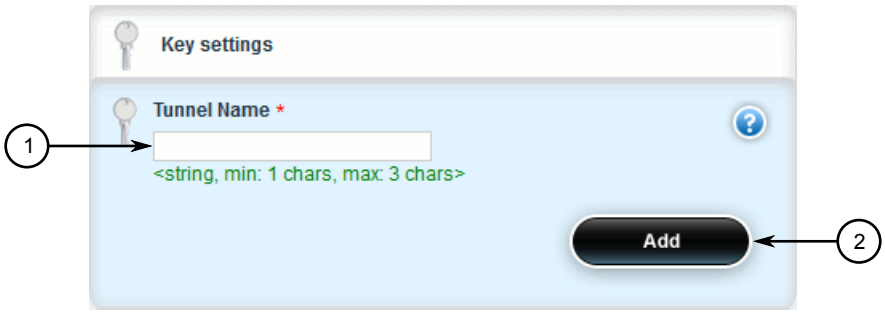


Figure 563: Key Settings Form

1. Tunnel Name Box **2.** Add Button

3. Configure the following parameters as required:

Parameter	Description
Tunnel Name	**Synopsis:** A string Tunnel name

4. Click **Add** to create the new tunnel. The **Dynamic L2TPv3 Tunnels** form appears.

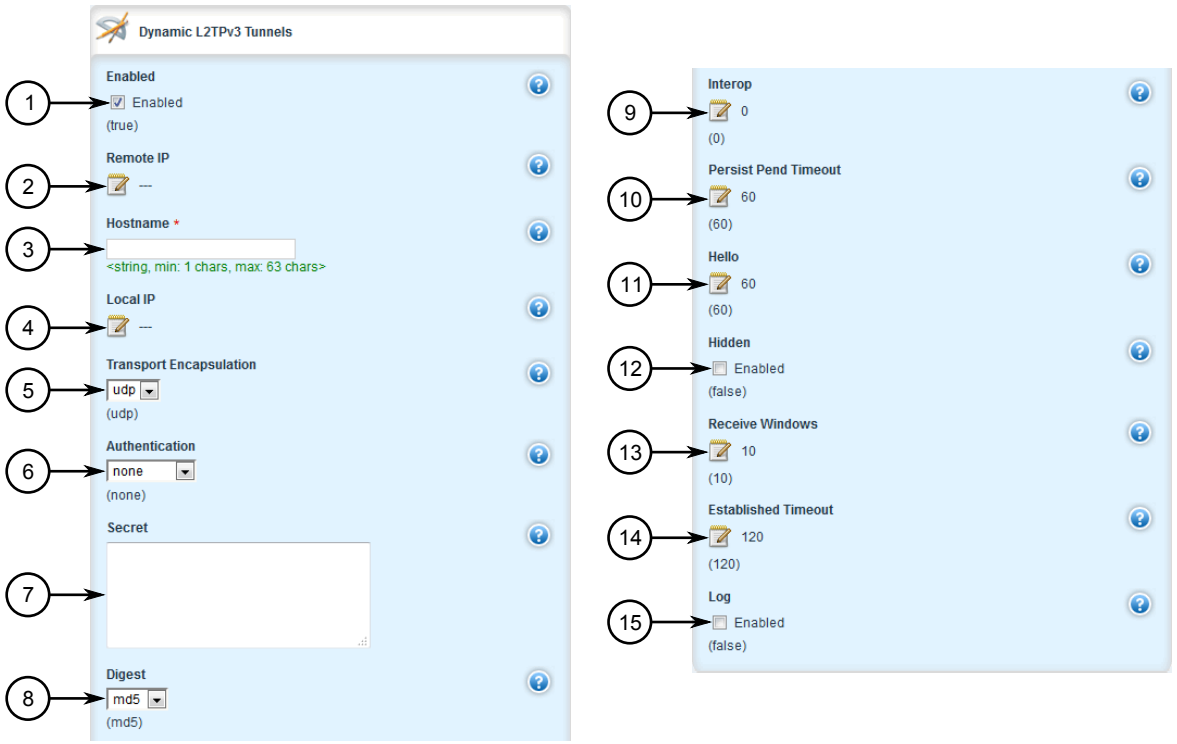


Figure 564: Dynamic L2TPv3 Tunnels Form

1. Enabled Check Box **2.** Remote IP Box **3.** Hostname Box **4.** Local IP Box **5.** Transparent Encapsulation Box **6.** Authentication List **7.** Secret Box **8.** Digest List **9.** Interop Box **10.** Persist Pend Timeout Box **11.** Hello Box **12.** Hidden Check Box **13.** Receive Windows Box **14.** Established Timeout Box **15.** Enabled Check Box

5. Configure the following parameters as required:

NOTE
Transport encapsulation is only configurable when Dynamic L2TPv3 is in `lac` *mode.*

Parameter	Description
enabled	**Synopsis:** { true, false } **Default:** true Enables/Disables the tunnel
Remote IP	**Synopsis:** A string 7 to 15 characters long or a string 6 to 40 characters long Ip address of remote tunnel endpoint
hostname	**Synopsis:** A string 1 to 63 characters long Hostname used in AVP This parameter is mandatory.
Local IP	**Synopsis:** A string 7 to 15 characters long or a string 6 to 40 characters long IP address of local interface that is used as Source IP address of outbound traffic over tunnel.
Transport Encapsulation	**Synopsis:** { udp, ip } **Default:** udp

Parameter	Description
	The transport protocol (UDP or IP) to encapsulate the tunnel messages
authentication	**Synopsis:** { none, challenge } **Default:** none The authentication of tunnel
secret	**Synopsis:** A string 1 to 63 characters long The password of tunnel negotiation
digest	**Synopsis:** { md5, sha1 } **Default:** md5 Message digest AVP encryption
interop	**Synopsis:** A 32-bit signed integer between 0 and 65535 **Default:** 0 Specify a bitmask of flags to control non-standard behaviour for interopability with other L2TPv3 implementation
Persist Pend Timeout	**Synopsis:** A 32-bit signed integer between 10 and 6000 **Default:** 60 The time (in seconds) that a persisting tunnel will wait in RETRY state before trying to establish itself again
hello	**Synopsis:** A 32-bit signed integer between 5 and 1000 **Default:** 60 timeout used for periodic L2TP Hello messages (in seconds)
hidden	**Synopsis:** { true, false } **Default:** false Enables/Disabled AVP hidden
Receive Windows	**Synopsis:** A 32-bit signed integer between 5 and 512 **Default:** 10 Received windows size
Established Timeout	**Synopsis:** A 32-bit signed integer between 30 and 1000 **Default:** 120 The time (in seconds) that a tunnel will wait for the peer to complete the tunnel setup message exchange
log	**Synopsis:** { true, false } **Default:** false Enables/Disables logging tunnel control messages

6. Add one or more sessions to the tunnel configuration. For more information, refer to Section 12.4.5.2, "Adding a Session".
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 12.4.4.4
Deleting a Dynamic L2TPv3 Tunnel

To delete a dynamic L2TPv3 tunnel, do the following:

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

2. Navigate to ***tunnel » l2tpv3 » dynamic » tunnel***. The **Dynamic L2TPv3 Tunnels** table appears.

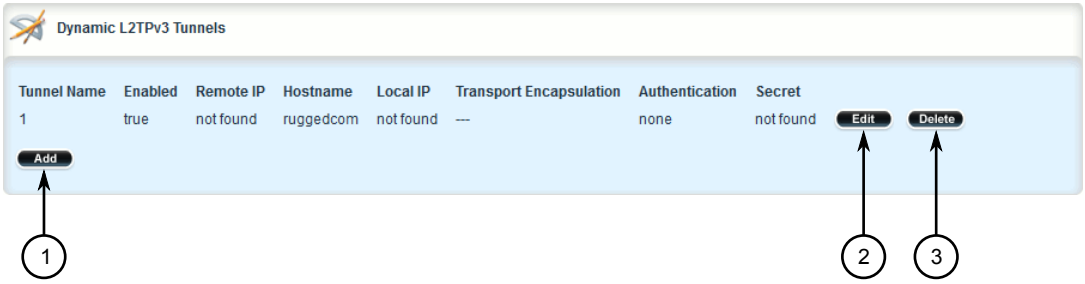


Figure 565: Dynamic L2TPv3 Tunnels Table

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 12.4.5

Managing Sessions for L2TPv3 Tunnels

This section describes how to create and manage sessions for L2TPv3 tunnels. A single L2TPv3 can support up to 128 active sessions.

CONTENTS

Section 12.4.5.1

Viewing a List of Sessions

To view a list of sessions defined for an L2TPv3 tunnel, navigate to ***tunnel » l2tpv3 » static | dynamic » tunnel » {name} » session***, where *{name}* is the name of the L2TPv3 tunnel. If sessions have been configured, the **Static L2TPv3 Sessions** or **Dynamic L2TPv3 Sessions** table appears.

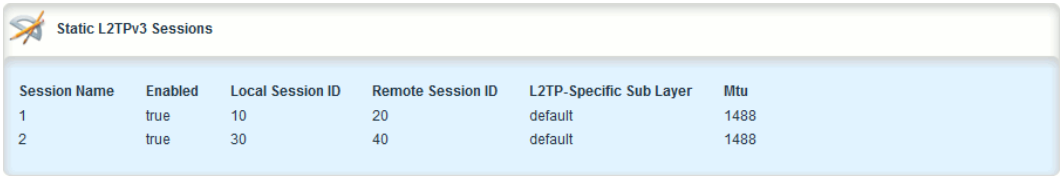


Figure 566: Static L2TPv3 Sessions Table (Example)

If no sessions have been configured, add sessions as needed. For more information, refer to Section 12.4.5.2, "Adding a Session".

Section 12.4.5.2
Adding a Session

To add a session to a static or dynamic L2TPv3 tunnel, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to ***tunnel » l2tpv3 » static | dynamic » tunnel » {name} » session***, where *{name}* is the name of the L2TPv3 tunnel.
3. Click **<Add session>**. The **Key Settings** form appears.

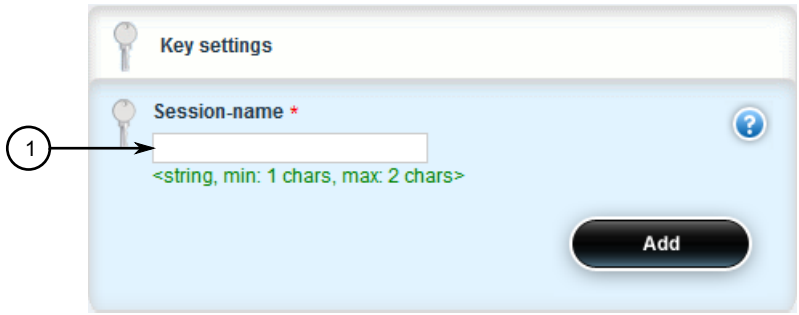


Figure 567: Key Settings Form

1. Session Name Box **2.** Add Button

4. Configure the following parameters as required:

Parameter	Description
Session Name	**Synopsis:** 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)

5. Click **Add** to create the new session. The **Static L2TPv3 Sessions** or **Dynamic L2TPv3 Sessions** form appears, as well as the **Local Cookie** and **Remote Cookie** forms.

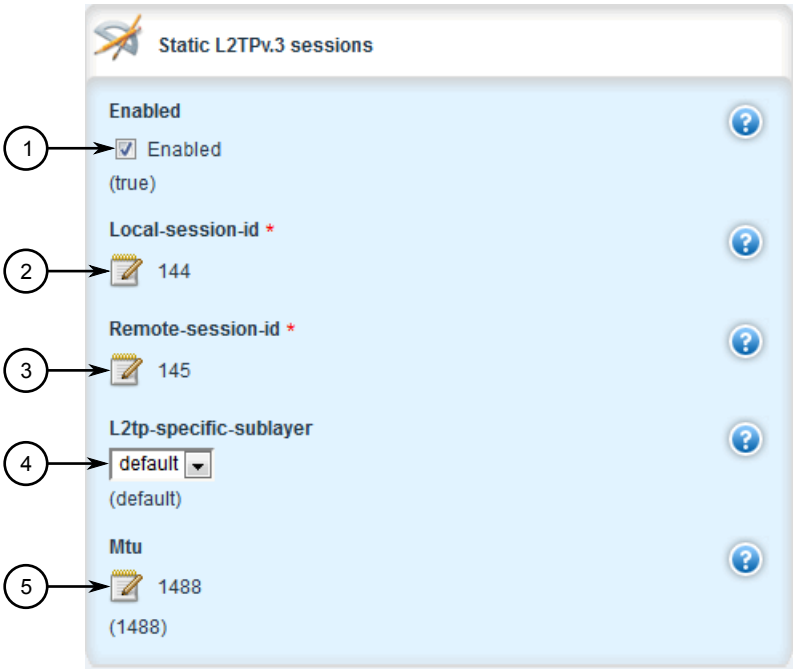


Figure 568: Static L2TPv3 Sessions Form

1. Enabled Check Box **2.** Local Session ID Box **3.** Remote Session ID Box **4.** L2TP-Specific Sub Layer List **5.** MTU Box

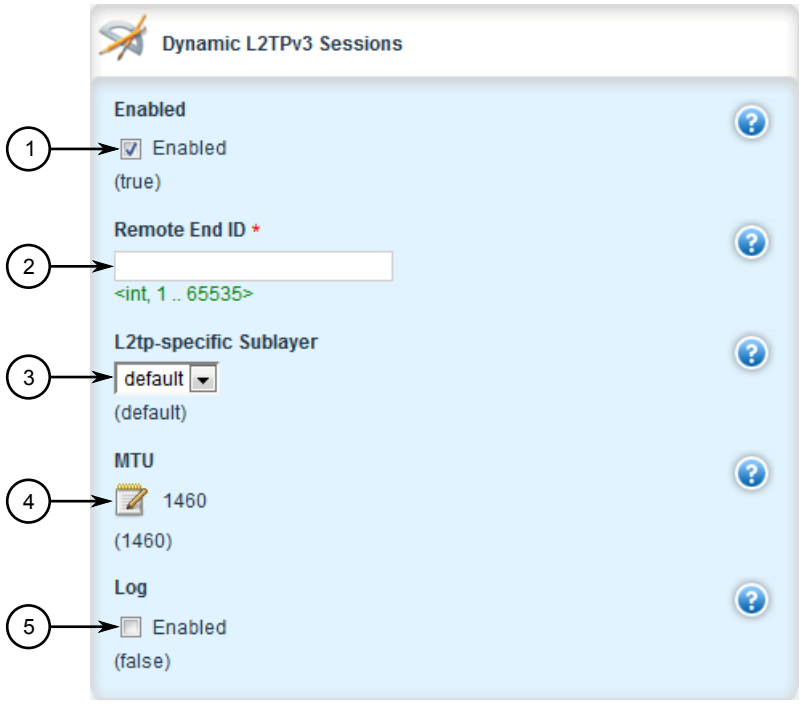


Figure 569: Dynamic L2TPv3 Sessions Form

1. Enabled Check Box **2.** Local Session ID Box **3.** Remote Session ID Box **4.** L2TP-Specific Sub Layer List **5.** MTU Box **6.** Log Box

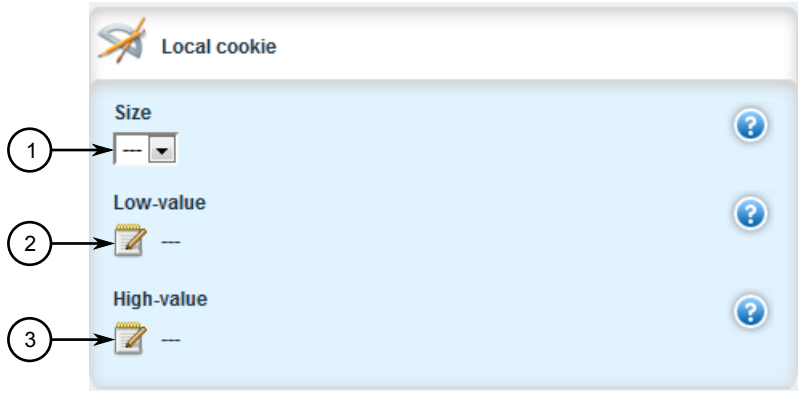


Figure 570: Local Cookie Form

1. Size List **2.** Low Value Box **3.** High Value Box

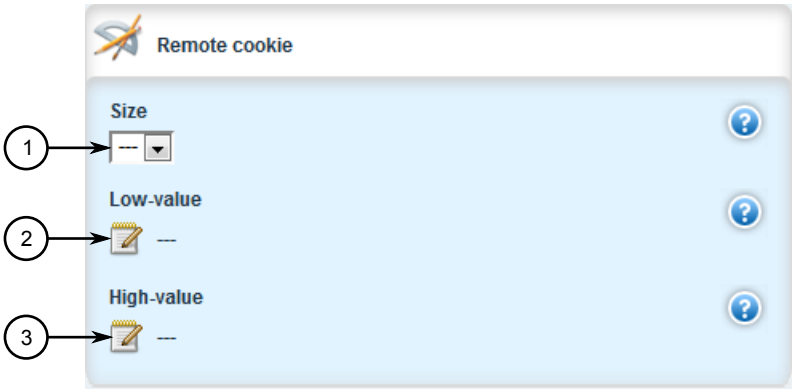


Figure 571: Remote Cookie Form

1. Size List **2.** Low Value Box **3.** High Value Box

6. On the **Static L2TPv3 Sessions** or **Dynamic L2TPv3 Sessions**, configure the following parameters as required:

NOTE
The `Log` parameter is only applicable to dynamic L2TPv3 tunnel sessions.

Parameter	Description
Enabled	**Synopsis:** { true, false } **Default:** true Enables/Disables the session
Local Session ID	**Synopsis:** A 32-bit signed integer between 1 and 65535 The local session-id provides the necessary context for all further packet processing This parameter is mandatory.
Remote Session ID	**Synopsis:** A 32-bit signed integer between 1 and 65535 The remote session-id is used to identify the received data messages from remote session endpoint This parameter is mandatory.
L2TP-Specific Sub Layer	**Synopsis:** { default, none } **Default:** default L2TP specific sublayer processing type
mtu	**Synopsis:** A 32-bit signed integer between 68 and 9216 **Default:** 1488 MTU of network interface

IMPORTANT!
Configuration of the local cookie should match the configuration of the remote cookie on the device at the other end of the L2TPv3 tunnel.

7. On the **Local Cookie**, configure the following parameters as required:

Parameter	Description
Size	**Synopsis:** { 4, 8 } Cookie size in byte.
Low Value	**Synopsis:** A 32-bit unsigned integer Lower value of cookie. This value must match with low-value of other endpoint's remote cookie
High Value	**Synopsis:** A 32-bit unsigned integer Higher value of cookie if the cookie size is 8. This value must match with high-value of other endpoint's remote cookie

IMPORTANT!
Configuration of the remote cookie should match the configuration of the local cookie on the device at the other end of the L2TPv3 tunnel.

8. On the **Remote Cookie**, configure the following parameters as required:

Parameter	Description
Size	**Synopsis:** { 4, 8 } Cookie size in byte
Low Value	**Synopsis:** A 32-bit unsigned integer Lower value of cookie. This value must match with low-value of other endpoint's local cookie
High Value	**Synopsis:** A 32-bit unsigned integer Higher value of cookie if its size is 8. This value must match with high-value of other endpoint's local cookie

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 12.4.5.3
Deleting a Session

To delete a session for a static or dynamic L2TPv3 tunnel, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to ***tunnel » l2tpv3 » static | dynamic » tunnel » {name} » session***, where *{name}* is the name of the L2TPv3 tunnel. The **Static L2TPv3 Sessions** or **Dynamic L2TPv3 Sessions** table appears.

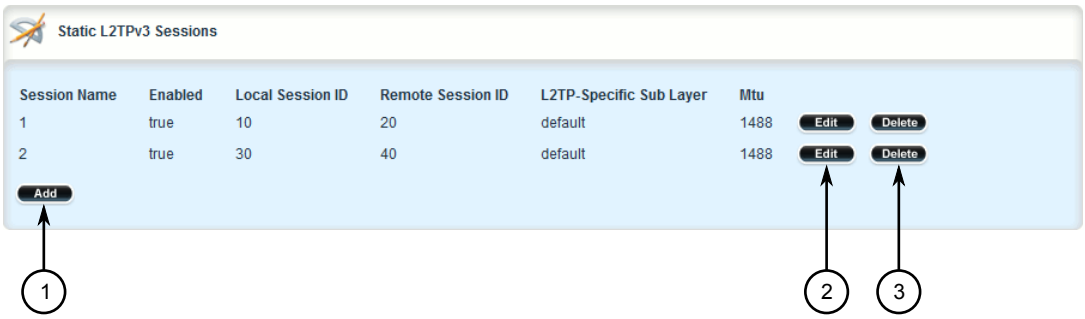


Figure 572: Static L2TPv3 Sessions Table

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

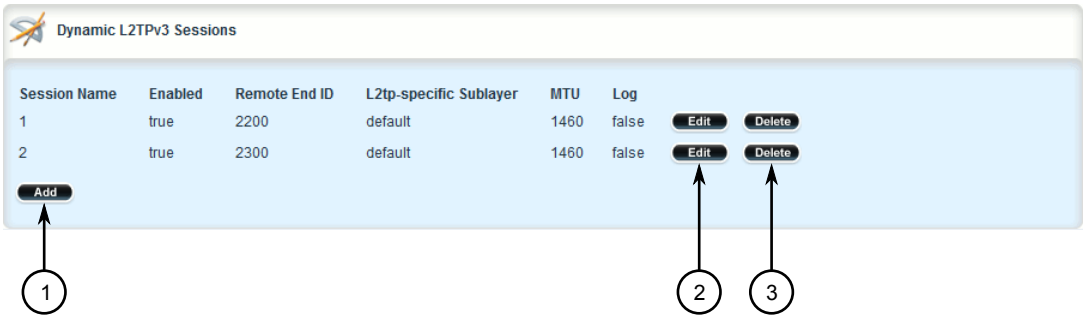


Figure 573: Dynamic L2TPv3 Sessions Table

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 12.4.6

Managing VLANs for L2TPv3 Tunnels

This section describes how to manage VLANs for L2TPv3 tunnel sessions. Each session supports up to 128 VLAN memberships.

CONTENTS

Section 12.4.6.1
Viewing a List of VLANs

To view a list of the VLANs configured for a static or dynamic L2TPv3 tunnel session, navigate to ***tunnel » l2tpv3 » static | dynamic » tunnel » {name} » session » {session}***, where *{name}* is the name of the L2TPv3 tunnel and *{session}* is the name of the tunnel session. The **VLANs** table appears.

Figure 574: VLANs Table

If no VLANs have been configured, add VLANs as needed. For more information, refer to Section 12.4.6.2, "Adding a VLAN".

Section 12.4.6.2
Adding a VLAN

To add a VLAN to a static or dynamic L2TPv3 tunnel session, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to ***tunnel » l2tpv3 » static | dynamic » tunnel » {name} » session » {session}***, where *{name}* is the name of the L2TPv3 tunnel and *{session}* is the name of the tunnel session.
3. Click **<Add vlan>**. The **Key Settings** form appears.

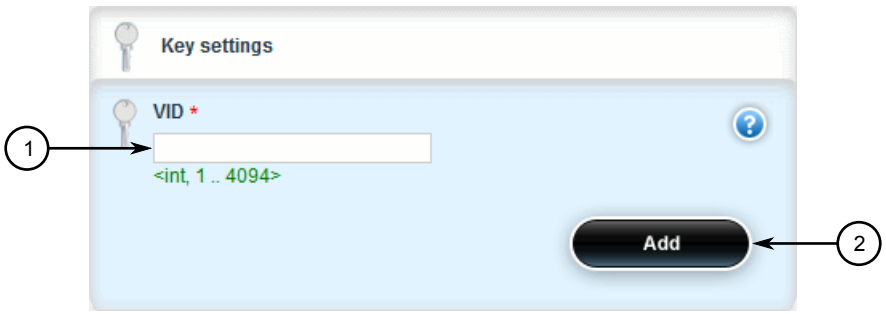


Figure 575: Key Settings Form

1. VID Box **2.** Add Button

4. Configure the following parameters as required:

Parameter	Description
VLAN id	**Synopsis:** A 32-bit signed integer Vlan id

5. Click **Add** to create the new VLAN.

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 12.4.6.3
Deleting a VLAN

To delete a VLAN for a static or dynamic L2TPv3 tunnel session, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to ***tunnel » l2tpv3 » static | dynamic » tunnel » {name} » session » {session}***, where *{name}* is the name of the L2TPv3 tunnel and *{session}* is the name of the tunnel session. The **VLANs** table appears.

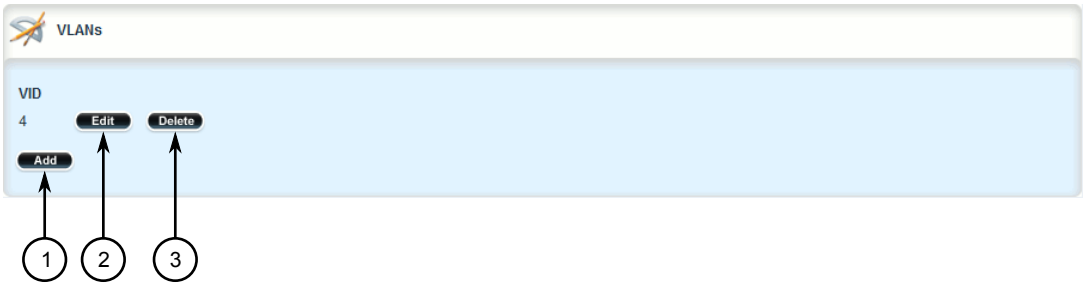


Figure 576: VLANs Table

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

3. Click **Delete** next to the chosen VLAN ID.
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 12.5
Managing GOOSE Tunnels

The GOOSE tunnel feature provides the capability to bridge GOOSE frames over a Wide Area Network (WAN).

GOOSE tunnels provide the following features:

- GOOSE traffic is bridged over the WAN via UDP/IP.
- One GOOSE traffic source can be mapped to multiple remote router Ethernet interfaces in mesh fashion.
- To reduce bandwidth consumption, GOOSE daemons may be located at each of the *legs* and at the center of a star network. The centrally located daemon will accept GOOSE packets and re-distribute them.
- Statistics report availability of remote GOOSE daemons, packet counts and Round Trip Time (RTT) for each remote daemon.
- When the Virtual Router Redundancy Protocol (VRRP) is employed, GOOSE transport is improved by sending redundant GOOSE packets from each VRRP gateway.

- You can enable GOOSE forwarding by configuring a generic Layer 2 tunnel. When configured, the device listens for GOOSE packets on one VLAN and forwards them to another VLAN.

The GOOSE protocol is supported by the Layer 2 Tunnel Daemon. The daemon listens to configured Ethernet interfaces and to the network itself (i.e. for tunnel connections from other daemon instances) on a configurable UDP port.

The Media Access Control (MAC) destination address of frames received from Ethernet is inspected in order to determine which GOOSE group they are in. The frames are then encapsulated in network headers and forwarded (with MAC source and destination addresses intact) to the network as GOOSE packets.

IEC61850 recommends that the MAC destination address should be in the range 01:0c:cd:01:00:00 to 01:0c:cd:01:01:ff.

GOOSE packets received from the network are stripped of their network headers and forwarded to Ethernet ports configured for the same multicast address. The forwarded frames contain the MAC source address or the originating device, and not that of the transmitting interface. The VLAN used will be that programmed locally for the interface and may differ from the original VLAN. The frame will be transmitted with the highest 802.1p priority level (p4).

Packets received from the network will also be forwarded to any other remote daemons included in the group.

To enable forwarding for GOOSE packets, configure a generic Layer 2 tunnel to listen for GOOSE packets on one VLAN and forward them to a second VLAN. To configure the generic Layer 2 tunnel for this operation, set the following for the tunnel:

- Ethernet Interface: select the VLAN on which the GOOSE packets originate
- Ethernet Type: set as 0x88b8
- Remote Daemon: select the VLAN to which to forward the GOOSE packets

CONTENTS

Section 12.5.1

Viewing the GOOSE Tunnel Statistics

To view the GOOSE tunnel statistics, navigate to ***tunnel » l2tunneld » status » goose***. The **GOOSE Tunnel Statistics** form appears.

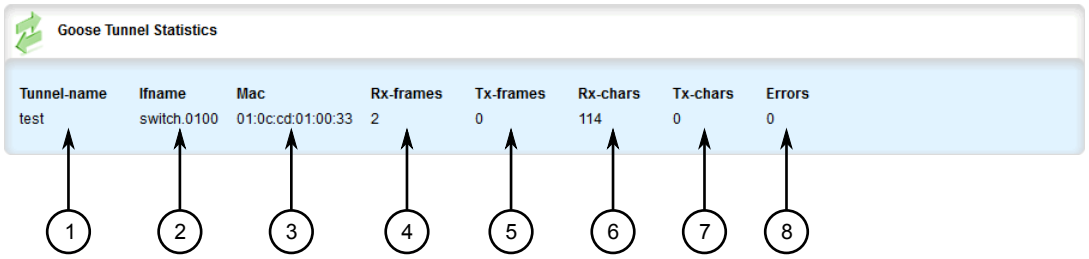


Figure 577: GOOSE Tunnel Statistics Form

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	**Synopsis:** A string 1 to 32 characters long The GOOSE tunnel name. This parameter is mandatory.
ifname	**Synopsis:** A string 1 to 15 characters long The name of the VLAN interface. This parameter is mandatory.
mac	**Synopsis:** A string 17 characters long The Multicast Destination MAC Address of the Goose message. This parameter is mandatory.
RX Frames	**Synopsis:** A 32-bit unsigned integer The number of frames received through the tunnel. This parameter is mandatory.
TX Frames	**Synopsis:** A 32-bit unsigned integer The number of frames transmitted through the tunnel. This parameter is mandatory.
RX Chars	**Synopsis:** A 32-bit unsigned integer The number of bytes received through the tunnel. This parameter is mandatory.
TX Chars	**Synopsis:** A 32-bit unsigned integer The number of bytes transmitted through the tunnel. This parameter is mandatory.
errors	**Synopsis:** A 32-bit unsigned integer The number of errors through the tunnel. This parameter is mandatory.

Section 12.5.2
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 578: GOOSE Tunnel Table

If no GOOSE tunnels have been configured, add tunnels as needed. For more information, refer to Section 12.5.3, "Adding a GOOSE Tunnel".

Section 12.5.3
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 » l2tunneld » goose*** and click **<Add tunnel>**. The **Key Settings** form appears.

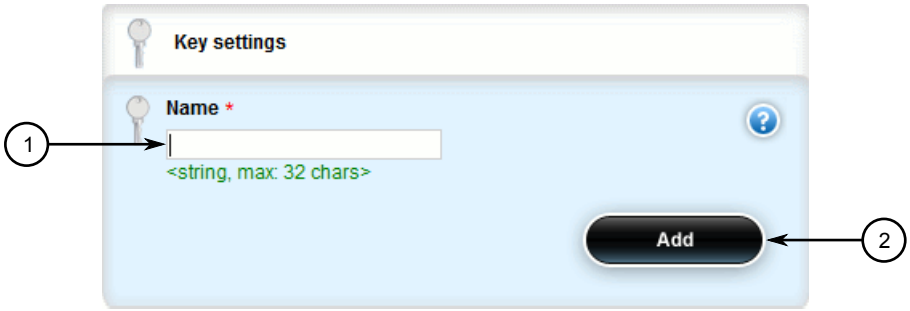


Figure 579: Key Settings Form

1. Name Box **2.** Add Button

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

Parameter	Description
Name	**Synopsis:** A string 1 to 32 characters long Description of the GOOSE tunnel.

4. Click **Add** to create the tunnel. The **GOOSE Tunnel** form appears.

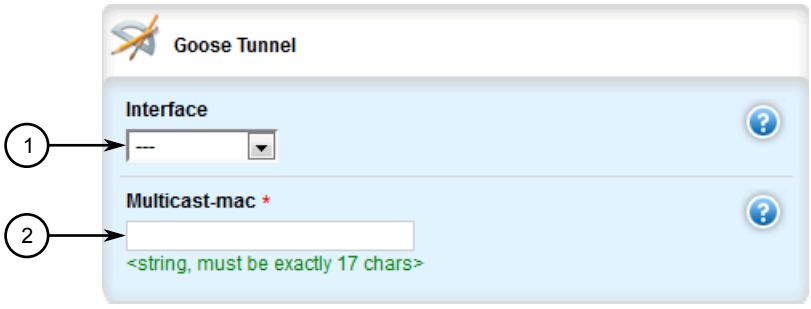


Figure 580: GOOSE Tunnel Form

1. Interface List **2.** Multicast MAC Address Box

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

Parameter	Description
Interface	**Synopsis:** A string The interface to listen on for GOOSE frames.
Multicast MAC	**Synopsis:** A string 17 characters long The multicast MAC address to listen for. This parameter is mandatory.

6. If necessary, configure one or more remote daemons for the tunnel. For more information, refer to Section 12.5.5.2, "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 12.5.4

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.

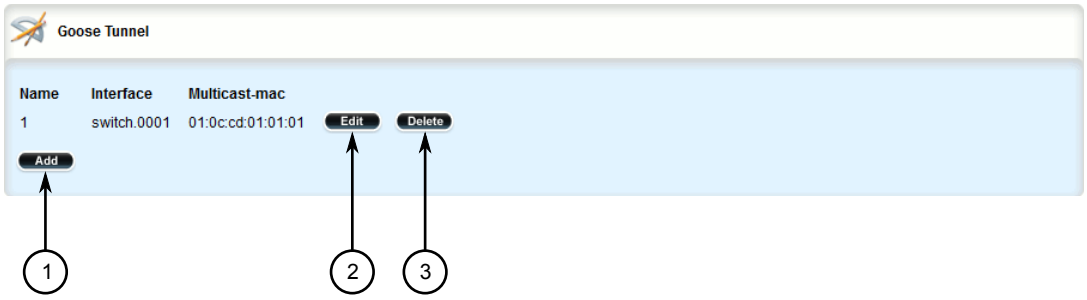


Figure 581: GOOSE Tunnel Table

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 12.5.5

Managing Remote Daemons for GOOSE Tunnels

In place of a local Ethernet interface for the tunnel egress, IP addresses for a remote daemon can be specified. Several endpoints may be added with these fields using successive edits of the tunnel configuration.

CONTENTS

Section 12.5.5.1

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.

Figure 582: Remote Daemon of Goose Tunnel Table

If no remote daemons have been configured, add daemons as needed. For more information, refer to Section 12.5.5.2, "Adding a Remote Daemon".

Section 12.5.5.2
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.

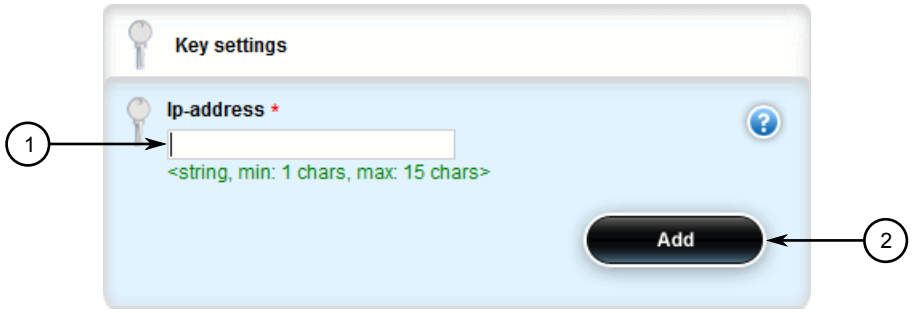


Figure 583: Key Settings Form

1. IP Address Box **2.** Add Button

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

Parameter	Description
IP Address	**Synopsis:** 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 12.5.5.3
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.

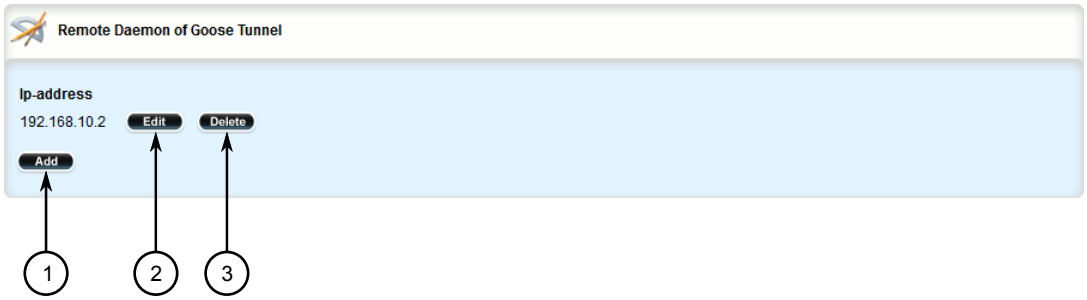


Figure 584: Remote Daemon of Goose Tunnel Table

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

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 12.6

Managing Generic Tunnels

The Layer 2 Tunnel Daemon supports a generic mode of operation based on the Ethernet type of Layer 2 data traffic seen by the router. Multiple tunnels may be configured, each one with:

- an Ethernet type
- a tunnel ingress (Ethernet interface)
- a tunnel egress (either another locally connected Ethernet interface, or the remote IP address of another Layer 2 Tunnel daemon instance running on another Router)

CONTENTS

Section 12.6.1

Viewing the Generic Tunnel Statistics

To view the generic tunnel statistics, navigate to ***tunnel » l2tunneld » status » generic***. The **Generic L2 Tunnel Statistics** form appears.

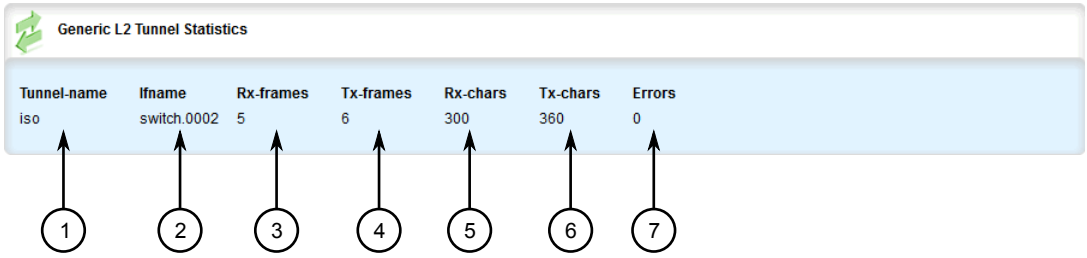


Figure 585: Generic L2 Tunnel Statistics Form

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	**Synopsis:** A string 1 to 32 characters long The generic tunnel name. This parameter is mandatory.
ifname	**Synopsis:** A string 1 to 15 characters long The name of the ingress interface. This parameter is mandatory.
RX Frames	**Synopsis:** A 32-bit unsigned integer The number of frames received through the tunnel. This parameter is mandatory.
TX Frames	**Synopsis:** A 32-bit unsigned integer The number of frames transmitted through the tunnel. This parameter is mandatory.
RX Chars	**Synopsis:** A 32-bit unsigned integer The number of bytes received through the tunnel. This parameter is mandatory.
TX Chars	**Synopsis:** A 32-bit unsigned integer The number of bytes transmitted through the tunnel. This parameter is mandatory.
errors	**Synopsis:** A 32-bit unsigned integer The number of errors received through the tunnel. This parameter is mandatory.

Section 12.6.2
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.

Figure 586: Generic L2 Tunnel Protocol Table

If no generic tunnels have been configured, add tunnels as needed. For more information, refer to Section 12.6.3, "Adding a Generic Tunnel".

Section 12.6.3
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 » l2tunneld » generic*** and click **<Add tunnel>**. The **Key Settings** form appears.

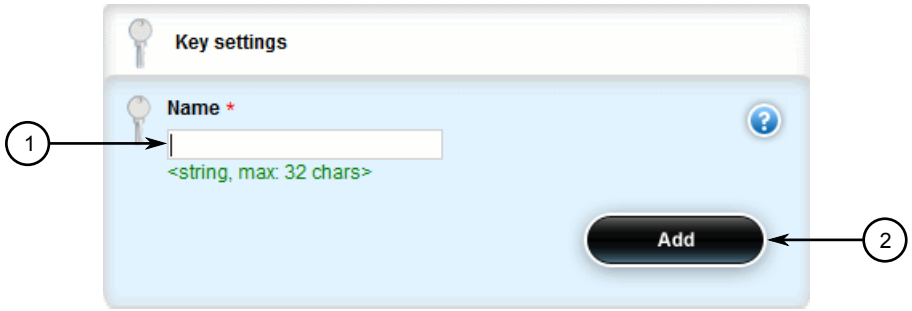


Figure 587: Key Settings Form

1. Name Box **2.** Add Button

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

Parameter	Description
Name	**Synopsis:** 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 588: 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	**Synopsis:** A string The interface to listen on for Ethernet type frames.
Replace MAC	Replaces the sender's MAC with the out-interface's MAC.

6. If necessary, configure one or more remote daemon IP addresses for the tunnel. For more information, refer to Section 12.6.5.2, "Adding an IP Address".
7. If necessary, define one or more Ethernet types to be forwarded. For more information, refer to Section 12.6.7.2, "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 12.6.4

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.

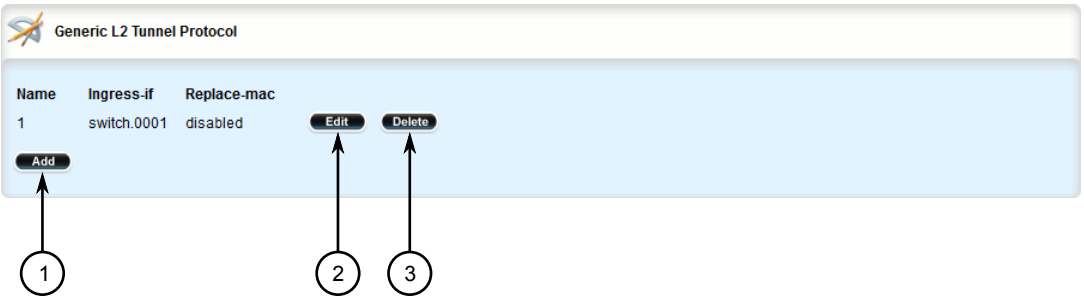


Figure 589: Generic L2 Tunnel Protocol Table

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 12.6.5

Managing Remote Daemon IP Addresses for Generic Tunnels

In place of a local Ethernet interface for the tunnel egress, IP addresses for a remote daemon can be specified. Several endpoints may be added with these fields using successive edits of the tunnel configuration.

NOTE
When a remote daemon IP address is configured, the interface on the receiver side, where traffic leaves, should be configured on the ingress interface (instead of egress interface).

CONTENTS

Section 12.6.5.1

Viewing a List of IP Addresses

To view a list of remote Layer 2 protocol server IP addresses for a generic tunnel configuration, 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.

Figure 590: Remote Daemon IP Address Table

If no generic tunnels have been configured, add tunnels as needed. For more information, refer to Section 12.6.3, "Adding a Generic Tunnel".

Section 12.6.5.2

Adding an IP Address

To add the IP address of a remote Layer 2 protocols server to a generic tunnel configuration, do the following:

1. 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.

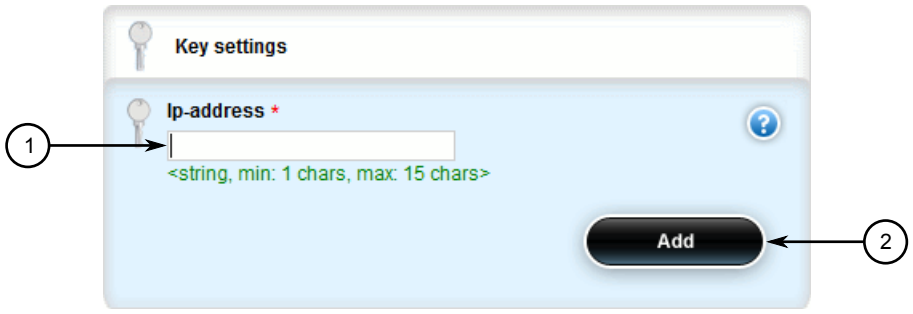


Figure 591: Key Settings Form

1. IP Address Box **2.** Add Button

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

Parameter	Description
IP Address	**Synopsis:** 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 12.6.5.3
Deleting an IP Address

To delete the IP address of a remote Layer 2 protocols server from a generic tunnel configuration, do the following:

1. 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.

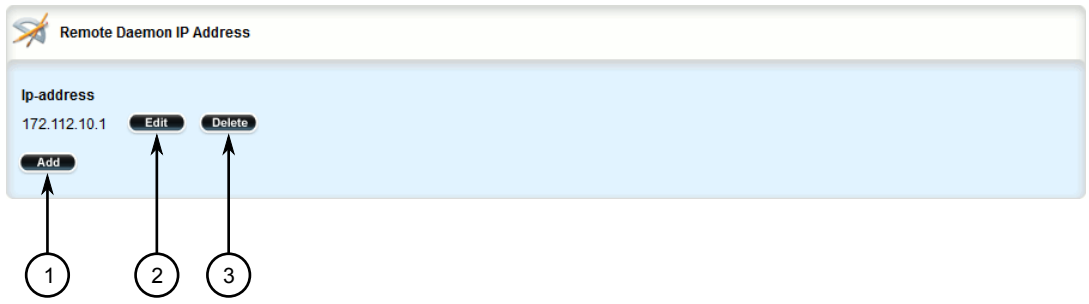


Figure 592: Remote Daemon IP Address Table

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

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 12.6.6
Managing Remote Daemon Egress Interfaces for Generic Tunnels

This section describes how to create and manage remote daemon egress interfaces for generic tunnels.

CONTENTS

Section 12.6.6.1
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.

Figure 593: Generic L2 Tunnel Egress Interface Table

If no egress interfaces have been configured, add interfaces as needed. For more information, refer to Section 12.6.6.2, "Adding an Egress Interface".

Section 12.6.6.2
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 594: Key Settings Form

1. Egress Interface Box **2.** Add Button

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

Parameter	Description
Egress Interface	**Synopsis:** A string 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 12.6.6.3
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.

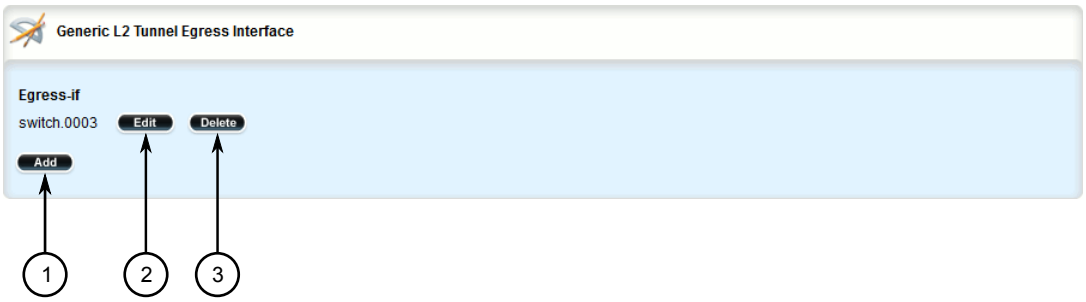


Figure 595: Generic L2 Tunnel Egress Interface Table

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

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 12.6.7
Managing Ethernet Types for Generic Tunnels

This section describes how to define the types of Ethernet protocols that can be forwarded by generic tunnels.

CONTENTS

Section 12.6.7.1
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 596: L2 Ethernet Type Table

If no Ethernet types have been configured, add types as needed. For more information, refer to Section 12.6.7.2, "Adding an Ethernet Type".

Section 12.6.7.2
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.

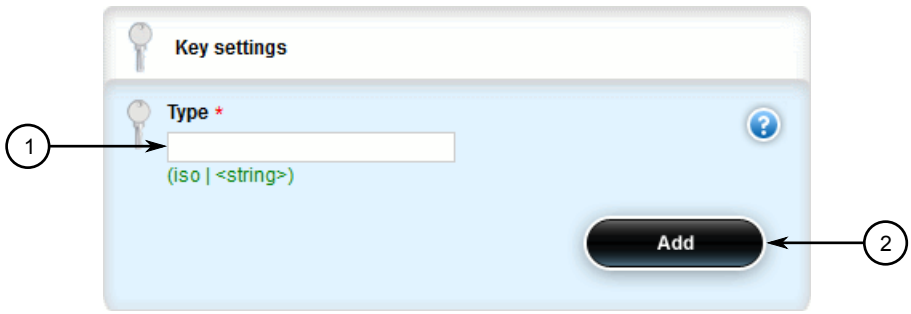


Figure 597: Key Settings Form

1. Type Box **2.** Add Button

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

Parameter	Description
Type	**Synopsis:** { 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 12.6.7.3

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.

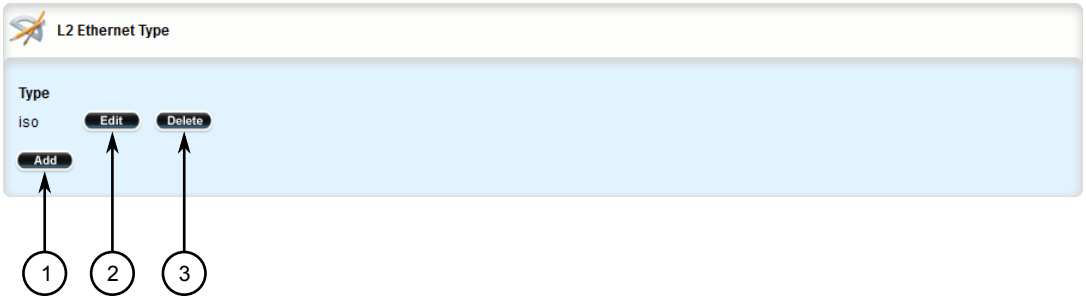


Figure 598: L2 Ethernet Type Table

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

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 12.7

Managing Generic Routing Encapsulation Tunnels

RUGGEDCOM ROX II can employ the Generic Routing Encapsulation (GRE) protocol to encapsulate multicast traffic and IPv6 packets together and transport them through an IPv4 network tunnel. As such, GRE tunnels can transport traffic through any number of intermediate networks.

The key parameters for GRE tunnels is the tunnel name, local router address, remote router address and remote subnet.

The following illustrates a typical GRE tunnel configuration:

Figure 599: Example – GRE Tunnel Configuration

In this example, Router 1 establishes a GRE tunnel to Router 2 using a local router address of 172.16.17.18, a remote router address of 172.19.20.21, and a remote subnet of 192.168.2.0/24.

NOTE
*When connecting a Cisco router (in place of Router 1 in the previous example), the local router address corresponds to the Cisco IOS **source** address and the remote router address corresponds to the **destination** address.*

The cost of the GRE tunnel can also be set if another method of routing between Router 1 and Router 2 becomes available. The packets will automatically flow through the lowest cost route.

Packets can also be restricted by specifying a local egress device, such as w1pp in the case of Router 1 in the previous example.

CONTENTS

Section 12.7.1

Viewing Statistics for GRE Tunnels

To view the statistics collected for GRE tunnels, navigate to ***interfaces » gre***. The **GRE Tunnels Statistics** form appears.

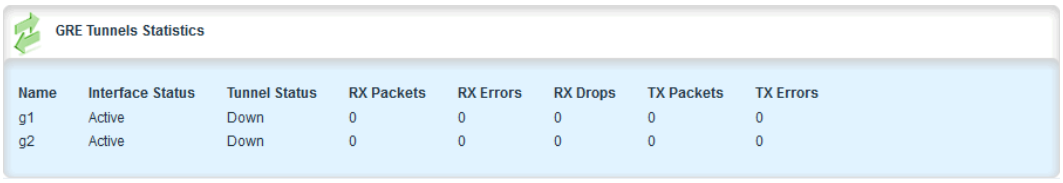


Figure 600: GRE Tunnels Statistics Form

This table provides the following information:

Parameter	Description
Name	**Synopsis:** A string 1 to 10 characters long The GRE tunnel interface name.
Interface Status	**Synopsis:** A string 1 to 20 characters long The status of the GRE tunnel interface, possible values include: • **Active** - GRE tunnel interface is up; • **Inactive** - GRE tunnel interface is down This parameter is mandatory.

Parameter	Description
Tunnel Status	**Synopsis:** A string The status of the GRE tunnel: • **Up** - GRE tunnel is up and running; • **Down** - GRE tunnel interface is inactive or tunnel remote endpoint is not reachable; • **Keepalives Disabled** - Keepalive messages have been disabled, not able to know if the tunnel remote endpoint is reachable or not This parameter is mandatory.
RX Packets	**Synopsis:** A 64-bit unsigned integer The number of packets received through the tunnel. This parameter is mandatory.
RX Errors	**Synopsis:** A 64-bit unsigned integer The error packets received through the tunnel. This parameter is mandatory.
RX Drops	**Synopsis:** A 64-bit unsigned integer The number of packets dropped by the tunnel. This parameter is mandatory.
TX Packets	**Synopsis:** A 64-bit unsigned integer The number of packets transmitted through the tunnel. This parameter is mandatory.
TX Errors	**Synopsis:** A 64-bit unsigned integer The number of error packets transmitted through the tunnel. This parameter is mandatory.
TX Drops	**Synopsis:** A 64-bit unsigned integer The number of packets dropped by the tunnel. This parameter is mandatory.

Section 12.7.2
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.

Figure 601: Generic Routing Encapsulation Interfaces Table

If no GRE tunnels have been configured, add tunnels as needed. For more information, refer to Section 12.7.3, "Adding a GRE Tunnel".

Section 12.7.3

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.

Figure 602: Key Settings Form

1. Name Box **2.** Add Button

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

Parameter	Description
Name	**Synopsis:** 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.

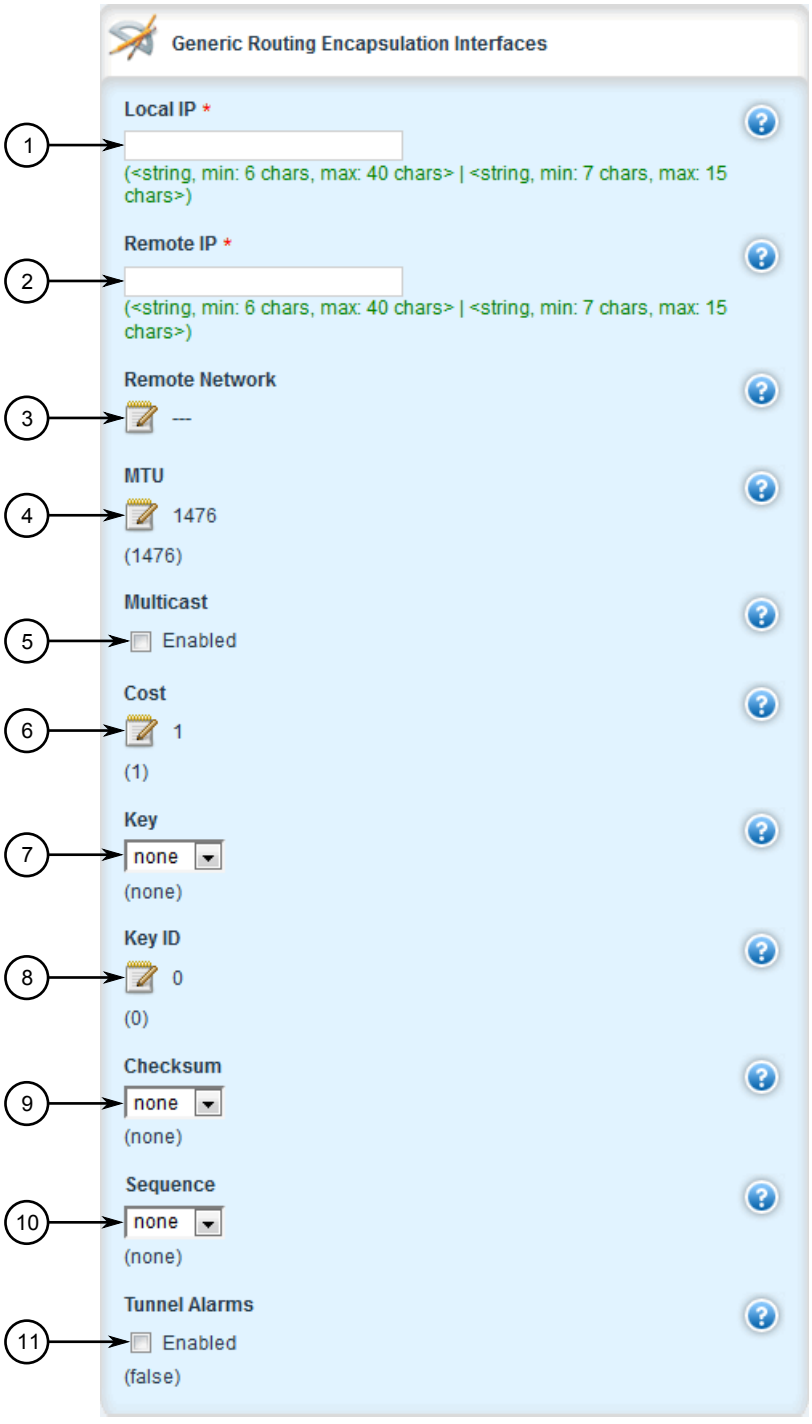


Figure 603: Generic Routing Encapsulation Interfaces Form

1. Local Address Box **2.** Remote Address Box **3.** Remote Subnet Box **4.** MTU Box **5.** Multicast Check Box **6.** Cost Box **7.** Key List **8.** Key ID Box **9.** Checksum List **10.** Sequence List **11.** Tunnel Alarms Check Box

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

Parameter	Description
Local IP	**Synopsis:** A string 7 to 15 characters long or a string 6 to 40 characters long The IP address of the local end of the tunnel. This parameter is mandatory.
Remote IP	**Synopsis:** A string 7 to 15 characters long or a string 6 to 40 characters long The IP address of the remote end of the tunnel. This parameter is mandatory.
Remote Network	**Synopsis:** A string 9 to 18 characters long or a string 4 to 43 characters long The target network of remote end of the tunnel.
MTU	**Synopsis:** A 32-bit signed integer **Default:** 1476 The MTU of the GRE interface.
Multicast	Enables multicast traffic on the tunnel interface.
Cost	**Synopsis:** A 32-bit signed integer between 1 and 255 **Default:** 1 The routing cost associated with networking routing that directs traffic through the tunnel.
key	**Synopsis:** { none, input, output, both } **Default:** none The key for tunneled packets
Key ID	**Synopsis:** A 32-bit unsigned integer between 0 and 4294967295 **Default:** 0 The key ID for tunneled packets
checksum	**Synopsis:** { none, input, output, both } **Default:** none The checksum for tunneled packets
sequence	**Synopsis:** { none, input, output, both } **Default:** none The sequence number for tunneled packets
Tunnel Alarms	**Synopsis:** { true, false } **Default:** false Enables or disables tunnel up and down alarms. Disabling tunnel alarms will prevent alarms from being sent for that tunnel. GRE tunnel alarms may also be controlled for the whole system under **admin > alarm-cfg**.

6. [Optional] Enable keepalive messages so as to monitor the status of the tunnel's remote endpoint. For more information, refer to Section 12.7.5, "Enabling/Disabling Keepalive Messages".
7. [Optional] Configure the method for assigning Differentiated Services Code Point (DSCP) marks to packets traveling through the GRE tunnel. For more information, refer to Section 12.7.4, "Configuring a DSCP Marking for GRE Tunnel Traffic".

   NOTE
   *An interface in the form of **gre-{tunnel}** (e.g. gre-t1) is added automatically to the **ip** menu.*

8. Assign an IP address to the tunnel. For more information, refer to either Section 7.1.3.2, "Adding an IPv4 Address" or Section 7.1.4.2, "Adding an IPv6 Address".

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 12.7.4
Configuring a DSCP Marking for GRE Tunnel Traffic

Each packet traversing a GRE tunnel can be assigned a Differentiated Services Code Point (DSCP) mark either defined by the device or inherited by the original IP header.

To the configure how DSCP marks are assigned for a specific GRE tunnel, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to ***tunnel » gre » {tunnel} » mark-choice***, where *{tunnel}* is the name of the GRE tunnel.
3. In the menu, click the **+** symbol next to **dscpmarking** to enable DSCP marking. The **DSCP Marking** form appears.

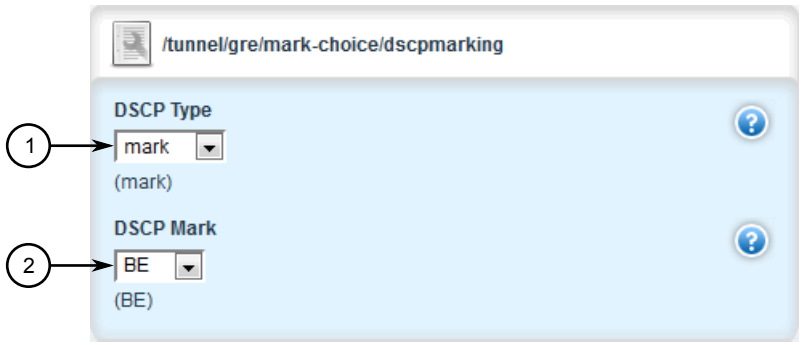


Figure 604: DSCP Marking Form

1. DSCP Type List **2.** DSCP Mark List

4. Under **DSCP Mark**, select one of the following options:
   - `mark` – Assigns the DSCP marking set by **DSCP Mark** to packets traversing the tunnel
   - `forward` – Assigns the DSCP marking defined in the original IP header of each packet traversing the tunnel
5. If `mark` is selected, under **DSCP Mark**, select a DSCP mark to assign. Options include: `BE`, `AF11`, `AF12`, `AF13`, `AF21`, `AF22`, `AF23`, `AF31`, `AF32`, `AF33`, `AF41`, `AF42`, `AF43`, `CS1`, `CS2`, `CS3`, `CS4`, `CS5`, `CS6`, `CS7`, `EF`.
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 12.7.5
Enabling/Disabling Keepalive Messages

Keepalive messages enable endpoints of a GRE tunnel to determine one another's current operational status.

Traditionally, GRE tunnels are stateless, meaning that remote endpoints retain no information about one another. As a result, an endpoint will not know when the other endpoint becomes unreachable and continue sending frames, even though the other end is unable to receive them.

With keepalive messages enabled, RUGGEDCOM ROX II will send keepalive messages to the other endpoint and wait for a response. If a response is not received before the next message is scheduled to be sent, it begins to count the number of consecutive messages sent that did not receive a reply. After so many failures to reply, the other endpoint is considered unreachable and a *Link Down* alarm is raised. This is the cue to the network administrator to bring down the GRE tunnel and investigate.

By default, keepalive messages are sent every 10 seconds and the remote endpoint has three opportunities to reply. These thresholds are user configurable.

To enable or disable keepalive messages for a GRE tunnel, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to ***tunnel » gre***. The **Generic Routing Encapsulation Interfaces** table appears.

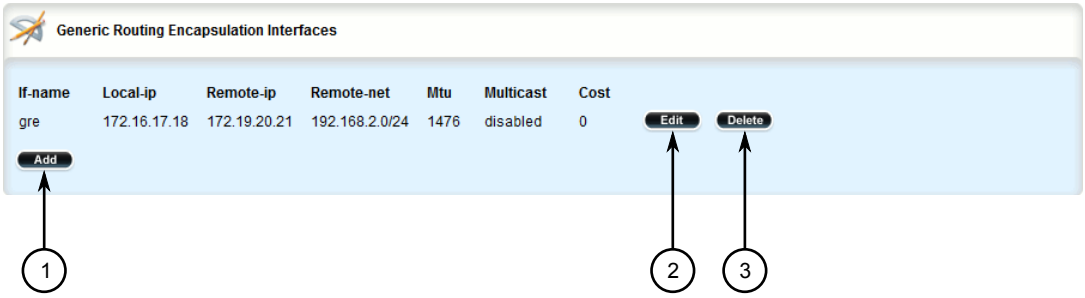


Figure 605: Generic Routing Encapsulation Interfaces Table

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

3. Click **Edit** next to the desired GRE tunnel. The **Generic Routing Encapsulation Keepalive Messages** form appears.

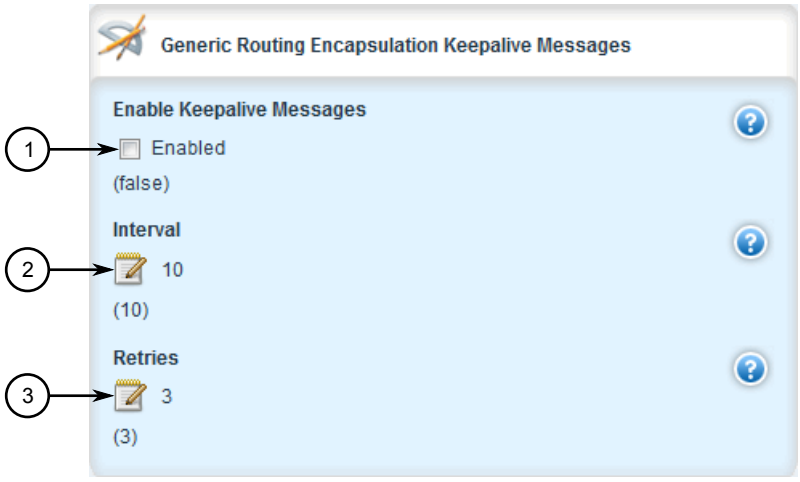


Figure 606: Generic Routing Encapsulation Keepalive Messages Form

1. Enable Keepalive Messages Check Box **2.** Interval Box **3.** Retries Box

4. Select **Enable Keepalive Messages** to enable keep alive messages, or clear the check box to disable the feature.
5. If keepalive messages are enabled, configure the following parameters:

Parameter	Description
interval	**Synopsis:** A 16-bit unsigned integer between 1 and 32767 **Default:** 10 The interval in second(s) at which keepalive messages are sent to the remote endpoint.
retries	**Synopsis:** An 8-bit unsigned integer between 1 and 255 **Default:** 3 The number of keepalive message the remote endpoint can ignore before it is considered unreachable.

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 12.7.6
Deleting a GRE Tunnel

To delete a GRE tunnel, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to ***tunnel » gre***. The **Generic Routing Encapsulation Interfaces** table appears.

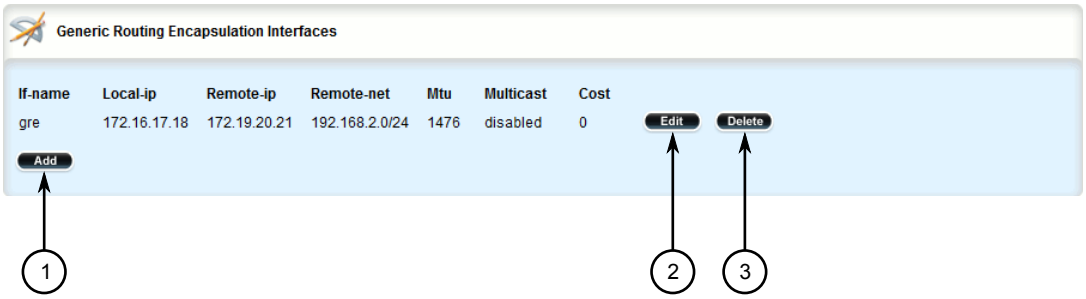


Figure 607: Generic Routing Encapsulation Interfaces Table

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 12.8

Managing IPsec Tunnels

IPsec (Internet Protocol SECurity) uses strong cryptography to provide authentication and encryption services. Authentication ensures that packets are from the right sender and have not been altered in transit. Encryption prevents unauthorized reading of packet contents.

These services allow secure tunnels to be built through untrusted networks. Everything passing through the untrusted network is encrypted by the IPsec gateway and decrypted by the gateway at the other end. The result is a Virtual Private Network (VPN), a network which is effectively private even though it includes machines at several different sites connected by the insecure Internet.

For more information about IPsec tunnels, refer to Section 12.8.1, "IPsec Tunneling Concepts".

IMPORTANT!
IPsec is time-sensitive. To make sure proper re-keying between network peers, the time on both peers must be synchronized. It is strongly recommended that NTP (Network Time Protocol) be used on both IPsec peers to synchronize their clocks. For more information about configuring NTP, refer to Section 17.8, "Managing NTP Servers".

CONTENTS

Section 12.8.1

IPsec Tunneling Concepts

The IPsec suite of protocols were developed by the Internet Engineering Task Force (IETF) and are required as part of IP version 6. Libreswan is the open source implementation of IPsec used by RUGGEDCOM ROX II.

The protocols used by IPsec are the Encapsulating Security Payload (ESP) and Internet Key Exchange (IKE) protocols. ESP provides encryption and authentication (ensuring that a message originated from the expected sender and has not been altered on route). IKE negotiates connection parameters, including keys, for ESP. IKE is

based on the Diffie-Hellman key exchange protocol, which allows two parties without any initial shared secret to create one in a manner immune to eavesdropping.

CONTENTS

Section 12.8.1.1
IPsec Modes

IPsec has two basic modes of operation. In *transport* mode, IPsec headers are added as the original IP datagram is created. The resultant packet is composed of an IP header, IPsec headers and IP payload (including a transport header). Transport mode is most commonly used between IPsec end-stations, or between an end-station and a gateway.

In *tunnel* mode, the original IP datagram is created normally and then encapsulated into a new IP datagram. The resultant packet is composed of a new IP header, IPsec headers, old IP header and IP payload. Tunnel mode is most commonly used between gateways, the gateway acting as a proxy for the hosts behind it.

Section 12.8.1.2
Supported Encryption Protocols

Libreswan supports the following standard encryption protocols:

- **3DES (Triple DES)**

  Uses three Data Encryption Standard (DES) encryptions on a single data block, with at least two different keys, to get higher security than is available from a single DES pass. 3DES is the most CPU intensive cipher.

- **AES**

  The Advanced Encryption Standard (AES) protocol cipher uses a 128-bit block and 128, 192 or 256-bit keys. This is the most secure protocol in use today, and is much preferred to 3DES due to its efficiency.

Section 12.8.1.3
Public and Secret Key Cryptography

In *public key* cryptography, keys are created in matched pairs (called public and private keys). The public key is made public while the private key is kept secret. Messages can then be sent by anyone who knows the public key to the holder of the private key. Only the owner of the private key can decrypt the message.

When this form of encryption is used, each router configures its VPN connection to use the RSA algorithm and includes the public signature of its peer.

In *secret key* cryptography, a single key known to both parties is used for both encryption and decryption.

When this form of encryption is used, each router configures its VPN connection to use a secret pre-shared key. For information about how to configure pre-shared keys, refer to Section 12.8.5, "Managing Pre-Shared Keys".

Section 12.8.1.4
X509 Certificates

In addition to pre-shared keys, IPsec also uses certificates to authenticate connections with hosts and routers. Certificates are digital signatures that are produced by a trusted source, namely a Certificate Authority (CA). For each host, the CA creates a certificate that contains CA and host information. The certificate is "signed" by creating a digest of all the fields in the certificate and then encrypting the hash value with its private key. The host's certificate and the CA public key are installed on all gateways that the host connects to.

When the gateway receives a connection request, it uses the CA public key to decrypt the signature back into the digest. It then recomputes its own digest from the plain text in the certificate and compares the two. If both digests match, the integrity of the certificate is verified (it was not tampered with), and the public key in the certificate is assumed to be the valid public key of the connecting host.

Section 12.8.1.5
NAT Traversal

Historically, IPsec has presented problems when connections must traverse a firewall providing Network Address Translation (NAT). The Internet Key Exchange (IKE) used in IPsec is not NAT-translatable. When IPsec connections must traverse a firewall, IKE messages and IPsec-protected packets must be encapsulated as User Datagram Protocol (UDP) messages. The encapsulation allows the original untranslated packet to be examined by IPsec.

Encapsulation is enabled during the IPsec configuration process. For more information, refer to Section 12.8.2, "Configuring IPsec Tunnels".

Section 12.8.1.6
Remote IPsec Client Support

If the router is to support a remote IPsec client and the client will be assigned an address in a subnet of a local interface, a proxy ARP must be activated for that interface. This will cause the router to respond to ARP requests on behalf of the client and direct traffic to it over its connection.

IPsec relies upon the following protocols and ports:

- protocol 51, IPSEC-AH Authentication Header (RFC2402)
- protocol 50, IPSEC-ESP Encapsulating Security Payload (RFC2046)
- UDP port 500

The firewall must be configured to accept connections on these ports and protocols. For more information, refer to Section 6.8.6, "Configuring the Firewall for a VPN".

Section 12.8.1.7

IPsec and Router Interfaces

If IPsec works on an interface which could disappear, such as a PPP connection, or if the IP address could change, the **Monitor Interface** option must be set for the IPsec connection. When this option is set, IPsec will restart when the interface disappears and reappears, or the IP address is changed.

The **Monitor Interface** option is set on the **Connection** form available for each connection. For more information about connections, refer to Section 12.8.6, "Managing Connections".

Section 12.8.2

Configuring IPsec Tunnels

To configure IPsec tunnels, do the following:

NOTE

RUGGEDCOM ROX II supports the creation of policy-based VPNs, which can be characterized as follows:

- *No IPsec network interfaces have been created.*
- *The routing table is not involved in directing packets to IPsec.*
- *Only data traffic matching the tunnel's local and remote subnets is forwarded to the tunnel. Normal traffic is routed by one set of firewall rules and VPN traffic is routed based on separate rules.*
- *The firewall is configured with a VPN zone of type **ipsec**.*
- *As IPsec packets are received, they are decoded, flagged as IPsec-encoded, and presented as having arrived directly from the same network interface on which they were originally received.*
- *Firewall rules are written to allow traffic to and from VPN tunnels. These are based on the normal form of source/destination IP addresses, and IP protocol and port numbers. These rules, by virtue of the zones they match, use the policy flags inserted by the netkey to route matching data traffic to the proper interface.*

For more information about configuring a policy-based VPN, refer to Section 6.8, "Managing Firewalls".

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to ***tunnel » ipsec***. The **IPsec** forms appear.

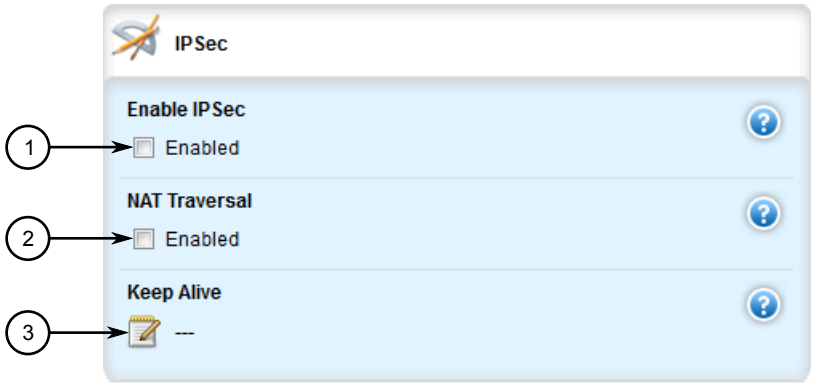


Figure 608: IPsec Form

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	Enables IPsec.
NAT Traversal	This parameter is not supported and any value is ignored by the system. nat-traversal is always enabled in the IPSec VPN system.
Keep Alive	**Synopsis:** A 32-bit unsigned integer between 1 and 86400 **Default:** 20 The delay (in seconds) for sending keepalive packets to prevent a NAT router from closing its port when there is not enough traffic on the IPsec connection.

4. Configure one or more pre-shared keys. For more information, refer to Section 12.8.5.2, "Adding a Pre-Shared Key".
5. Configure one or more encrypted connections. For more information, refer to Section 12.8.6.2, "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 12.8.3

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 6.7.4.3, "Adding a CA Certificate and CRL".
3. Add a private key. For more information, refer to Section 6.7.5.2, "Adding a Private Key".
4. Add a certificate. For more information, refer to Section 6.7.7.3, "Adding a Certificate".
5. Add a public key. For more information, refer to Section 6.7.6.2, "Adding a Public Key".

6. Navigate to ***tunnel » ipsec » connection » {connection} » {end}***, where *{connection}* is the name of the connection and *{end}* is the either the left (local router) or right (remote router) connection end. The **System Public Key** and **System Identifier** forms appear.

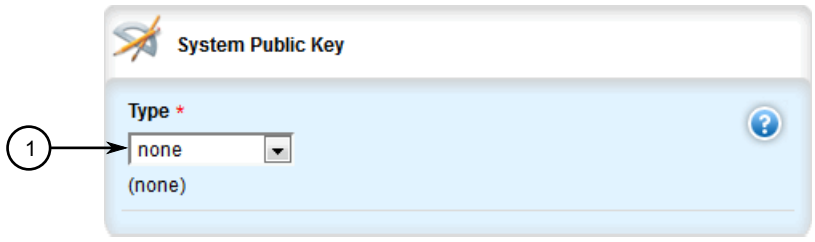


Figure 609: System Public Key Form

1. Type List **2.** Certificate List (Hidden) **3.** RSA Signature List (Hidden)

Figure 610: 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 12.8.4

Viewing the IPsec Tunnel Status

To view the status of the IPsec tunnel, navigate to ***tunnel » ipsec***. The **IPSec Status** form appears.

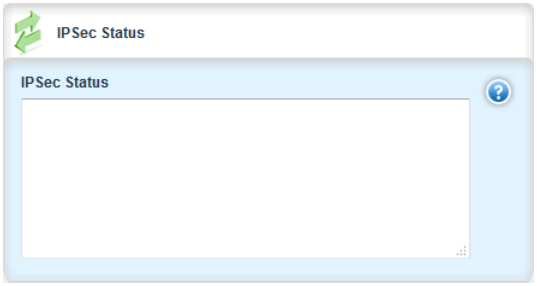


Figure 611: IPSec Status Form

This form provides a detailed log of all IPsec activity.

Section 12.8.5
Managing Pre-Shared Keys

Pre-shared keys are used in *secret key* cryptography. For more information about *secret key* cryptography and pre-shared keys, refer to Section 12.8.1.3, "Public and Secret Key Cryptography".

CONTENTS

Section 12.8.5.1
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.

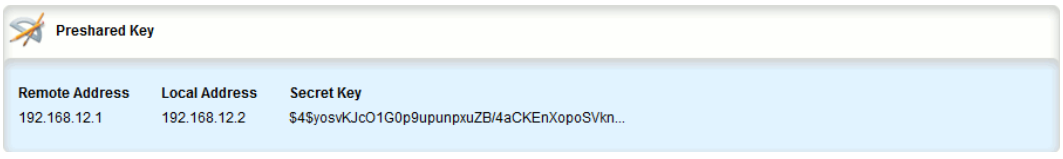


Figure 612: Preshared Key Table

If no pre-shared keys have been configured, add pre-shared keys as needed. For more information, refer to Section 12.8.5.2, "Adding a Pre-Shared Key".

Section 12.8.5.2
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.

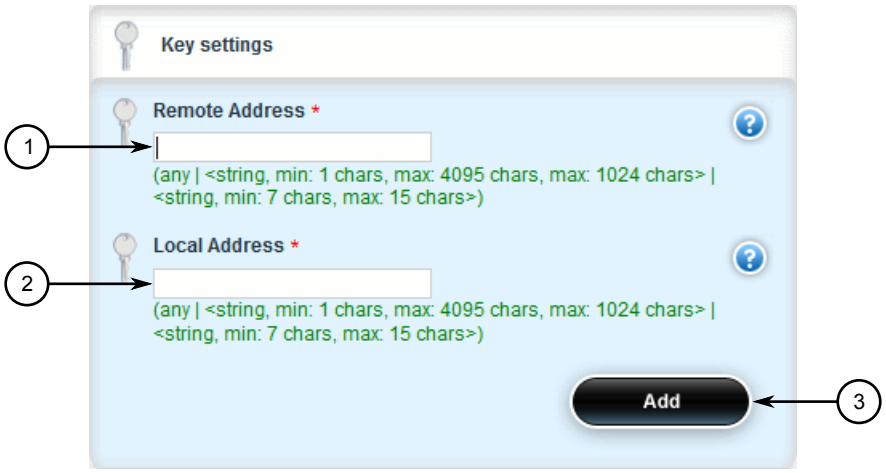


Figure 613: Key Settings Form

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	**Synopsis:** { any } or a string 7 to 15 characters long The remote address.
Local Address	**Synopsis:** { any } or a string 7 to 15 characters long The local address.

4. Click **Add** to create the new pre-shared key. The **Preshared Key** form appears.

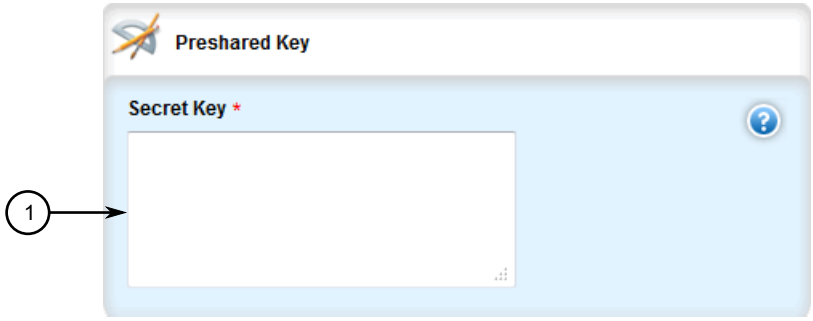


Figure 614: Preshared Key Form

1. Secret Key Box

5. In the **Preshared Key** form, configure the following parameters as required:

Parameter	Description
Secret Key	**Synopsis:** A string 1 to 8192 characters long The pre-shared key. This parameter is mandatory.

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 12.8.5.3

Deleting a Pre-Shared Key

To delete a pre-shared key, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to ***tunnel » ipsec » preshared-key***. The **Preshared Key** table appears.

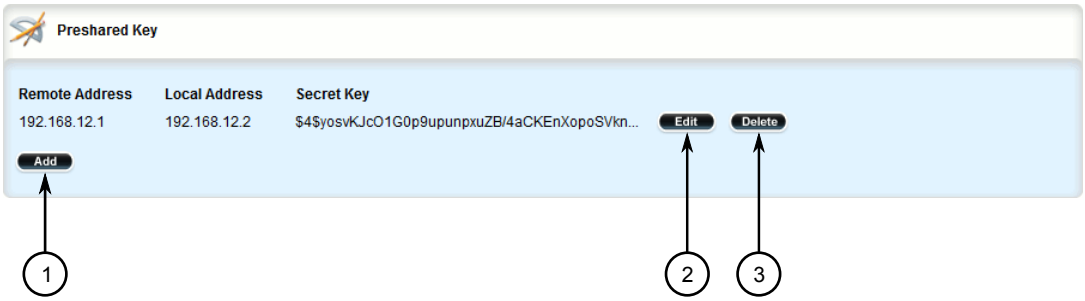


Figure 615: Preshared Key Table

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

3. Click **Delete** next to the chosen pre-shared 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 12.8.6
Managing Connections

An IPsec connection is an encrypted connection between two devices who share the same pre-authorized authentication key.

CONTENTS

Section 12.8.6.1
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.

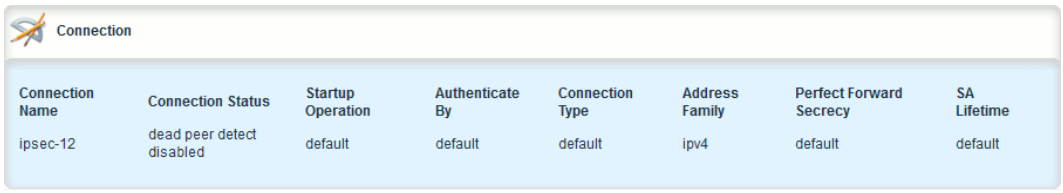


Figure 616: Connection Table

If no connections have been configured, add connections as needed. For more information, refer to Section 12.8.6.2, "Adding a Connection".

Section 12.8.6.2
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.

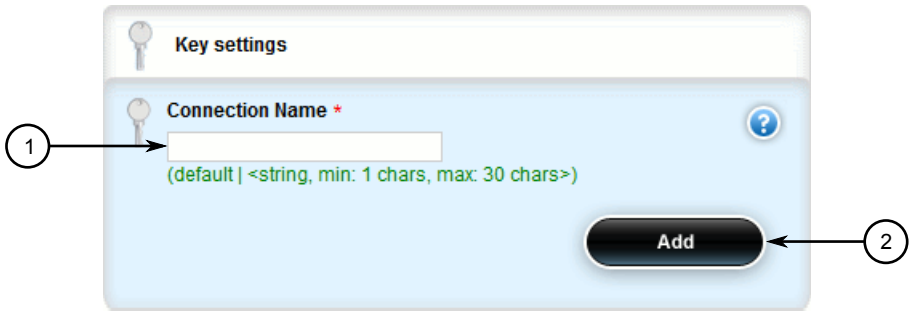


Figure 617: Key Settings Form

1. Connection Name Box **2.** Add Button

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

Parameter	Description
Connection Name	**Synopsis:** { 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. If this connection is to be used with NHRP, the name given here must exactly match the interface name of the corresponding GRE tunnel interface.

4. Click **Add** to create the new connection. The **Connection** form appears.

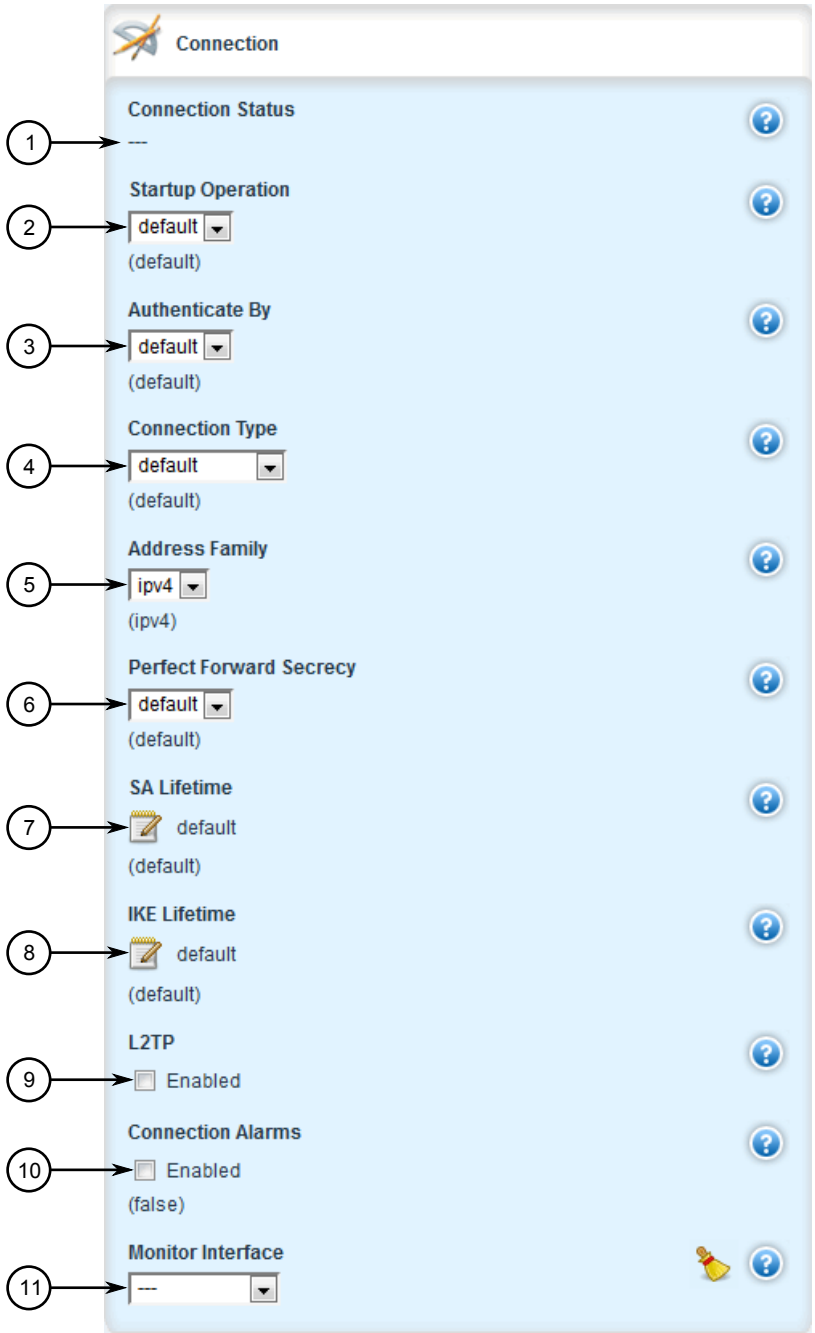


Figure 618: Connection Form

1. Connection Status **2.** Startup Operation List **3.** Authenticate By List **4.** Connection Type List **5.** Address Family List **6.** Perfect Forward Secrecy List **7.** SA Lifetime Box **8.** IKE Lifetime Box **9.** L2TP Check Box **10.** Connection Alarms Check Box **11.** Monitor Interface List

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

Parameter	Description
Startup Operation	**Synopsis:** { ignore, add, start, route, default } **Default:** default The action to take when IPsec is initialized. The default value is 'ignore' unless overwritten by the default connection setting.
Authenticate By	**Synopsis:** { default, rsasig, secret } **Default:** default The authentication method. The default value is 'default' unless overwritten by the default connection setting.
Connection Type	**Synopsis:** { tunnel, transport, passthrough, default } **Default:** default The connection type/mode. Options include: • tunnel: Encrypts traffic on host-to-host, host-to-subnet or subnet-to-subnet tunnels. This is the default type/mode unless overwritten by the default connection setting. • transport: Encrypts traffic on a host-to-host tunnel. • passthrough: Traffic is not encrypted.
Address Family	**Synopsis:** { ipv4, ipv6 } **Default:** ipv4 The address-family to run for the connection. Accepted values include 'ipv4' (default) and 'ipv6'. All addresses used in the connection must have the same address family.
Perfect Forward Secrecy	**Synopsis:** { default, yes, no } **Default:** default Enables/disables Perfect Forwarding Secrecy (PFS). When enabled, IPsec negotiates new keys for each session. If an attacker compromises a key, only the session protected by the key is revealed. Not all clients support PFS. The default value is 'yes' unless overwritten by the default connection setting.
SA Lifetime	**Synopsis:** { default } or a 32-bit unsigned integer between 1081 and 28800 **Default:** default The lifetime in seconds for the Security Association (SA) key. This determines how long a particular instance of a connection should last, from successful negotiation to expiry. Normally, the connection is renegotiated before it expires. The default value is 28800 unless overwritten by the default connection setting. Peers can specify different lifetime intervals. However, if peers do not agree, an excess of superseded connections will occur on the peer that believes the SA lifetime is longer.
IKE Lifetime	**Synopsis:** { default } or a 32-bit unsigned integer between 60 and 86400 **Default:** default The lifetime in seconds for for the IKE protocol. This determines how long the IKE keying channel of a connection should last before being renegotiated. The default value is 3600 unless overwritten by the default connection setting. Peers can specify different lifetime intervals. However, if peers do not agree, an excess of superseded connections will occur on the peer that believes the IKE lifetime is longer.
L2TP	Enables/disables L2TP for this connection.
Connection Alarms	**Synopsis:** { true, false } **Default:** false Enables or disables connection up and down alarms. Disabling connection alarms will prevent alarms from being sent for that connection. Connection alarms may also be controlled for the whole system under **admin > alarm-cfg**.
Monitor Interface	**Synopsis:** A string The interface to monitor. If the selected interface goes down and then up, this connection will be restarted.

6. If required, enable and configure dead peer detection. For more information, refer to Section 12.8.6.3, "Configuring Dead Peer Detection".
7. If required, configure the Internet Key Exchange (IKE) protocol by adding one or more algorithms. For more information, refer to Section 12.8.7.2, "Adding an IKE Algorithm".
8. If required, configure Encapsulated Security Payload (ESP) encryption for the connection. For more information, refer to Section 12.8.8, "Managing the Encapsulated Security Payload (ESP) Protocol".
9. If required, configure the left (local router) and right (remote router) ends of the connection. For more information, refer to Section 12.8.9, "Configuring the Connection Ends".
10. If required, configure L2TP tunnels. For more information, refer to Section 12.1, "Configuring L2TP Tunnels".
11. If certificates and keys are required, make sure they are configured on the device. For more information, refer to Section 12.8.3, "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 12.8.6.3
Configuring Dead Peer Detection

Dead Peer Detection (DPD), as defined in RFC 3706 [http://tools.ietf.org/html/rfc3706] is used to detect dead Internet Key Exchange (IKE) peers. In this method, peers exchange DPD Request (ISAKMP R-U-THERE) and DPD Response (ISAKMP R-U-THERE-ACK) messages. If a DPD Response is not received by a peer after a specified time and/or number of attempts, the other peer is considered *dead*. The remaining peer can either hold the connection until other peer responds, clear the connection, restart the connection and renegotiate the Security Association (SA), or restart all SA's to the dead peer.

In RUGGEDCOM ROX II, DPD Requests are sent when there is no traffic detected by the peer. How long to wait before sending a DPD Request and how long to wait for a DPD Response is user configurable.

It is generally recommended that DPD be configured to clear connections with any dead peers.

To configure dead peer detection for an IPsec connection, do the following:

1. 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.

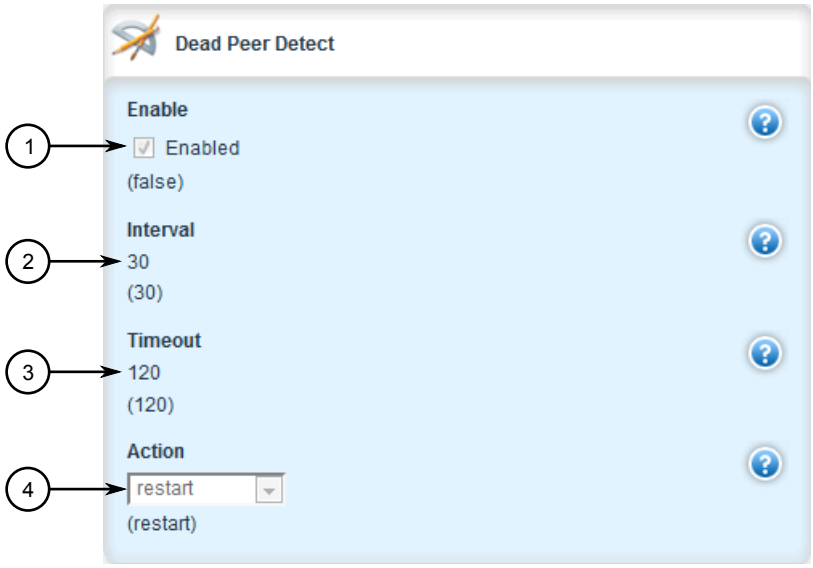


Figure 619: Dead Peer Detect Form

1. Enabled Check Box **2.** Interval Box **3.** Timeout Box **4.** Action List

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

NOTE
The timeout period must be two minutes longer than the interval period.

Parameter	Description
Enable	**Synopsis:** { true, false } **Default:** false Enables Dead Peer Detection (DPD) for this connection.
Interval	**Synopsis:** A 32-bit unsigned integer between 1 and 3600 **Default:** 30 The interval (in seconds) between Dead Peer Detection keepalive messages sent for this connection when no traffic (idle) appears to be sent by a DPD enabled peer.
Timeout	**Synopsis:** A 32-bit unsigned integer between 1 and 28800 **Default:** 120 The time in seconds to wait before a peer is declared dead.
Action	**Synopsis:** { hold, clear, restart, restart-all-sa } **Default:** restart The action to be taken when a DPD enabled peer is declared dead. Options include: • hold: The route will be put on hold status. • clear: The route and Security Association (SA) will both be cleared • restart: The SA will immediately be renegotiated • restart-all-sa: All SA's to the dead peer will be renegotiated

4. 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 12.8.6.4
Deleting a Connection

To delete a connection for a VPN, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to ***tunnel » ipsec » connection***. The **Connection** table appears.

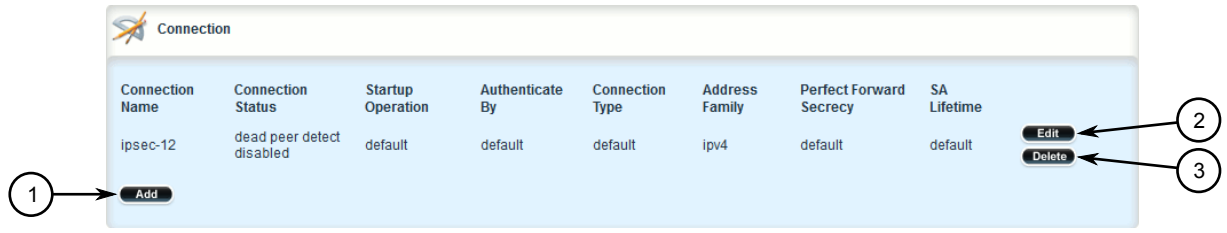


Figure 620: Connection Table

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 12.8.6.5
Viewing the Status of a Connection

To view the status of an IPsec connection, navigate to ***tunnel » ipsec » connection » {connection}***, where *{connection}* is the desired connection. The current status of the connection is listed under **Connection Status** on the **Connection** form.

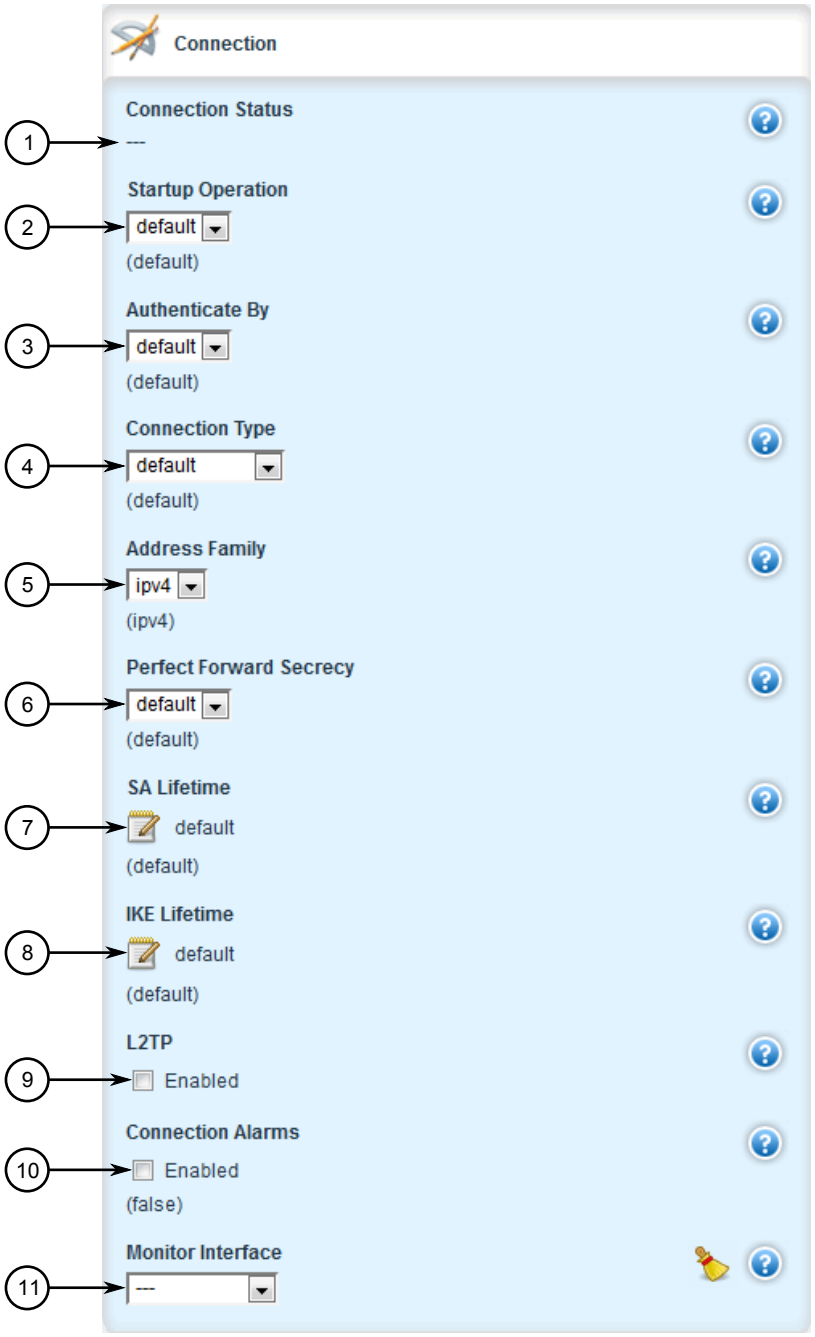


Figure 621: Connection Form

1. Connection Status **2.** Startup Operation List **3.** Authenticate By List **4.** Connection Type List **5.** Address Family List **6.** Perfect Forward Secrecy List **7.** SA Lifetime Box **8.** IKE Lifetime Box **9.** L2TP Check Box **10.** Connection Alarms Check Box **11.** Monitor Interface List

Possible values include:

- `dead peer detect disabled` – Dead Peer Detection (DPD) is disabled. DPD must be enabled to report the status of the connection.

- `inactive` – There are currently no established connections on the selected tunnel.
- `active` – There are established peer connections on the selected tunnel. The number of active peers is defined in brackets.
- `IPsec disabled` – IPsec is disabled.

Section 12.8.7

Managing the Internet Key Exchange (IKE) Protocol

The Internet Key Exchange (IKE) protocol negotiates connection parameters, including keys, for the Encapsulated Security Payload (ESP) protocol employed by IPsec. IKE is based on the Diffie-Hellman key exchange protocol, which allows two parties without any initially shared secret to create one in a manner immune to eavesdropping.

CONTENTS

Section 12.8.7.1

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 622: Algorithm Table

If no algorithms have been configured, add algorithms as needed. For more information, refer to Section 12.8.7.2, "Adding an IKE Algorithm".

Section 12.8.7.2

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.

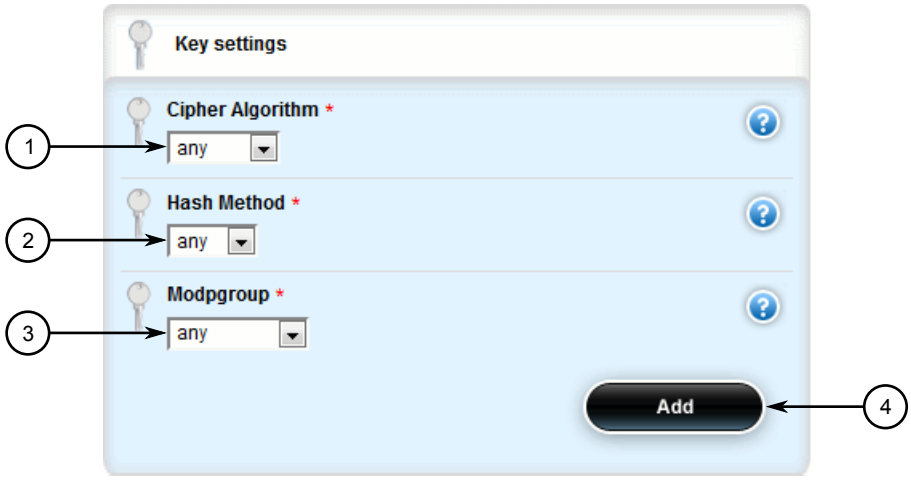


Figure 623: Key Settings Form

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	**Synopsis:** { 3des, aes, aes256, aes192, aes128, any } The cipher algorithm. The default value is '3des' or 'aes' unless overwritten by the default connection setting. The value 'any' means to use the default value.
Hash Method	**Synopsis:** { sha1, md5, sha2, any } The hash method. The default value is 'sha1' or 'md5' unless overwritten by the default connection setting. The value 'any' means to use the default value.
Modpgroup	**Synopsis:** { 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. The value 'any' means to use the default value.

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 12.8.7.3
Deleting an IKE Algorithm

To delete an 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. The **Algorithm** table appears.

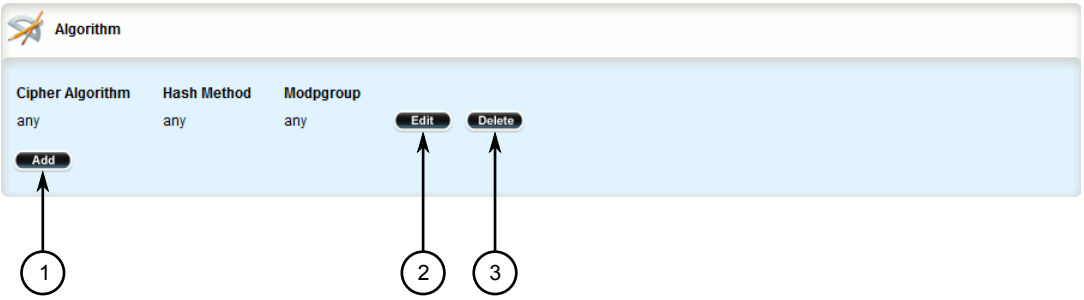


Figure 624: Algorithm Table

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

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 12.8.8

Managing the Encapsulated Security Payload (ESP) Protocol

The Encapsulated Security Payload (ESP) employed by IPsec provides encryption and authentication, making sure that messages originated from the expected sender have not been altered in transit.

CONTENTS

Section 12.8.8.1

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.

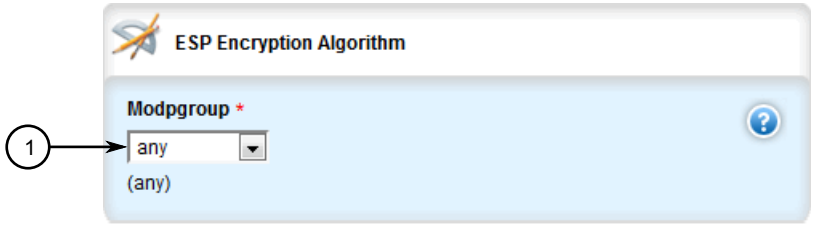


Figure 625: ESP Encryption Algorithm Form

1. Mod Group List

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

Parameter	Description
Modpgroup	**Synopsis:** { modp1024, modp1536, modp2048, modp3072, modp4096, modp6144, modp8192, any } **Default:** any The Modular Exponential (MODP) group. The default value is 'modp1024' or 'modp1536' unless overwritten by the default connection setting. The value 'any' means to use the default value.

4. If required, add additional cipher algorithms. For more information on how to add algorithms, refer to Section 12.8.8.3, "Adding an ESP Algorithm".
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 12.8.8.2
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.

Figure 626: Algorithm Table

If no algorithms have been configured, add algorithms as needed. For more information, refer to Section 12.8.8.3, "Adding an ESP Algorithm".

Section 12.8.8.3
Adding an ESP Algorithm

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.

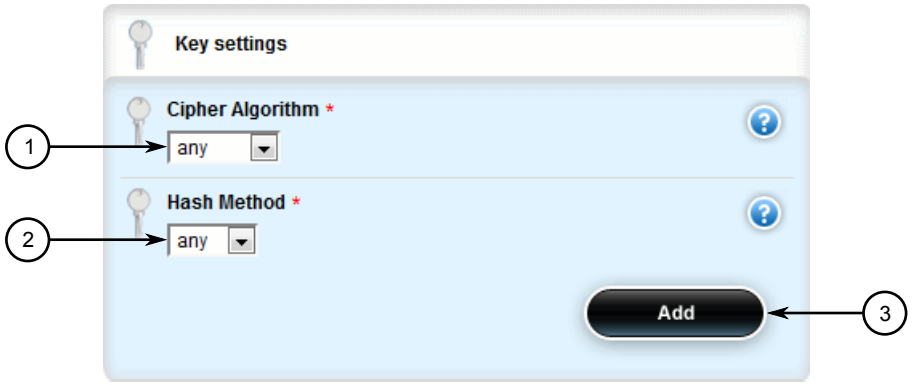


Figure 627: Key Settings Form

1. Cipher Algorithm Box **2.** Hash Method Box **3.** Add Button

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

Parameter	Description
Cipher Algorithm	**Synopsis:** { 3des, aes, aes256, aes192, aes128, any } The cipher algorithm. The default value is '3des' or 'aes' unless overwritten by the default connection setting. The value 'any' means to use the default value.
Hash Method	**Synopsis:** { sha1, md5, sha2, any } The hash method. The default value is 'sha1' or 'md5' unless overwritten by the default connection setting. The value 'any' means to use the default value.

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 12.8.8.4
Deleting an ESP Algorithm

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.

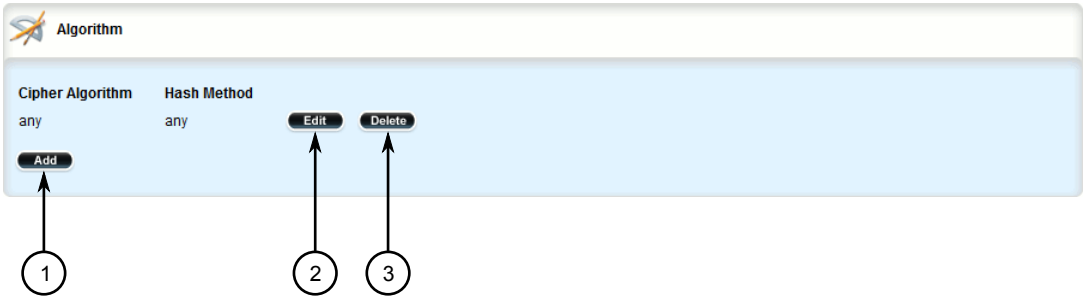


Figure 628: Algorithm Table

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

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 12.8.9

Configuring the Connection Ends

Each IPsec tunnel has two ends: the local router and the remote router. These are otherwise referred to as the left and right connections, respectively. Both ends can have the same configuration or a unique configuration.

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 the either the left (local router) or right (remote router) connection end. The **Public IP Address**, **System Public Key**, **System Identifier**, **Nexthop to Other System** and **Left/Right** forms appear.

Figure 629: Public IP Address Form

1. Type List **2.** Host Name or IP Address Box

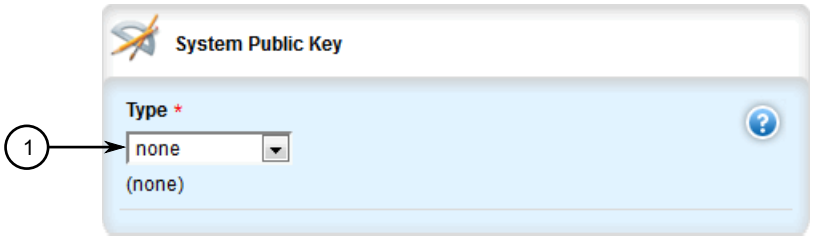


Figure 630: System Public Key Form

1. Type List **2.** Certificate List (Hidden) **3.** RSA Signature List (Hidden)

Figure 631: System Identifier Form

1. Type List **2.** Host Name or IP Address Box

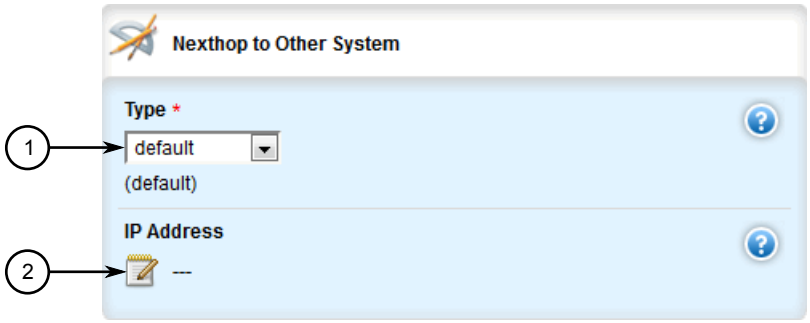


Figure 632: Nexthop to Other System Form

1. Type List **2.** IP Address Box

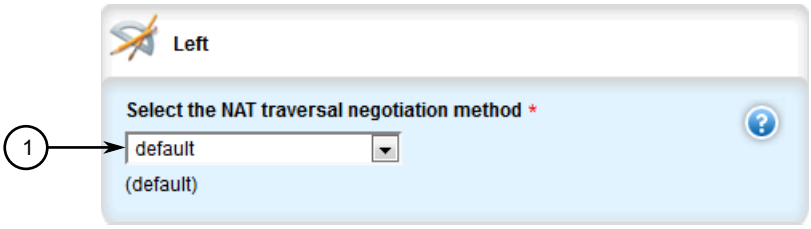


Figure 633: Left/Right Form

1. NAT Traversal Negotiation Method List

3. In the **Public IP Address** form, configure the following parameters:

IMPORTANT!
Do not use a Virtual IP Address (VRIP) as the connection's public IP address if `Use Virtual MAC` *is enabled under VRRP.*

Parameter	Description
Type	**Synopsis:** { none, default-route, any, address, hostname } **Default:** none The public IP address type.
Hostname or IP Address	**Synopsis:** 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	**Synopsis:** { none, rsasig, certificate-any, certificate } **Default:** none

Parameter	Description
	Key type.
RSA Signature	**Synopsis:** A string The RSA signature key name.
RSA Signature in ipsec format	**Synopsis:** A string 1 to 8192 characters long The RSA signature in IPsec format.
Certificate	**Synopsis:** A string The selected certificate.

5. In the **System Identifier** form, configure the following parameters:

Parameter	Description
type	**Synopsis:** { default, none, from-certificate, address, hostname, der-asn1-dn, user-fqdn } **Default:** default The system identifier type. The default value is 'left side public-ip' unless overwritten by the default connection setting.
Hostname, IP Address or Distinguished Name in Certificate	**Synopsis:** 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	**Synopsis:** { default, default-route, address } **Default:** default The next hop type. The default value is 'right side public-ip' unless overwritten by the default connection setting.
IP Address	**Synopsis:** A string 7 to 15 characters long The IP address of the next hop that can be used to reach the destination network.

7. In the *Left*/*Right* form, configure the following parameters:

Parameter	Description
NAT Traversal Negotiation Method	**Synopsis:** { default, draft-ietf-ipsec-nat-t-ike-02, rfc-3947 } **Default:** default The NAT traversal negotiation method. Some IPsec endpoints prefer RFC 3947 over draft-ietf-ipsec-nat-t-ike-02 when connecting with Libreswan, as these implementations use different identifiers when NAT is involved. For example, when a Windows XP/2003 client connects, Libreswan reports the main mode peer ID is ID_FQDN: '@example.com', but when a Vista, Windows 7 or other RFC 3947 compliant client connects, Libreswan reports the main mode peer ID is ID_IPV4_ADDR: '192.168.1.1'. This will cause issues connecting to the IPsec server. In such cases, setting this option to draft-ietf-ipsec-nat-t-ike-02 will solve this problem. The default value is 'rfc-3947' unless overwritten by the default connection setting.

8. If required, configure a subnet for the connection end. For more information, refer to Section 12.8.10.3, "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 12.8.10

Managing Private Subnets

If the device is connected to an internal, private subnet, access to the subnet can be granted to the device at the other end of the IPsec tunnel. Only the IP address and mask of the private subnet is required.

CONTENTS

Section 12.8.10.1

Configuring Private Subnets for Connection Ends

To configure a private subnet for either the left (local router) or right (remote router) connection ends in a VPN, do the following:

1. 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.

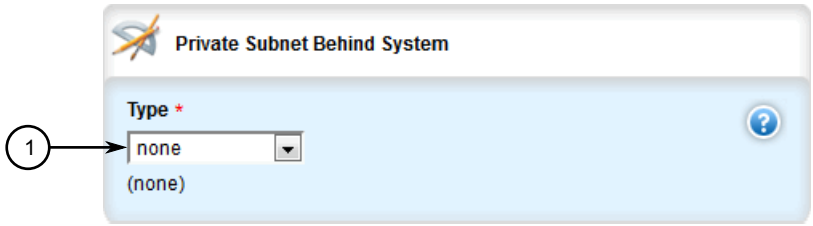


Figure 634: Private Subnet Behind System Form

1. Type List

3. Configure the following parameter(s):

Parameter	Description
Subnet Address	**Synopsis:** A string 9 to 18 characters long The IP address/prefix.

4. Add one or more subnet addresses. For more information, refer to Section 12.8.10.3, "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 12.8.10.2
Viewing a List of Addresses for Private Subnets

To view a list of IP addresses configured for private subnets, navigate to ***tunnel » ipsec » connection » {name} » {end} » subnet***, where *{name}* is the name of the connection and *{end}* is the either the left (local router) or right (remote router) connection end. If IP addresses have been configured, the **Private Subnet Behind System** table appears.

Figure 635: Private Subnet Behind System Table

If no IP addresses have been configured, add addresses as needed. For more information, refer to Section 12.8.10.3, "Adding an Address for a Private Subnet".

Section 12.8.10.3
Adding an Address for a Private Subnet

To add an IP address for a private subnet, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to ***tunnel » ipsec » connection » {name} » {end} » subnet » network***, where *{name}* is the name of the connection and *{end}* is the either the left (local router) or right (remote router) connection end.
3. Click **<Add network>**. The **Key Settings** form appears.

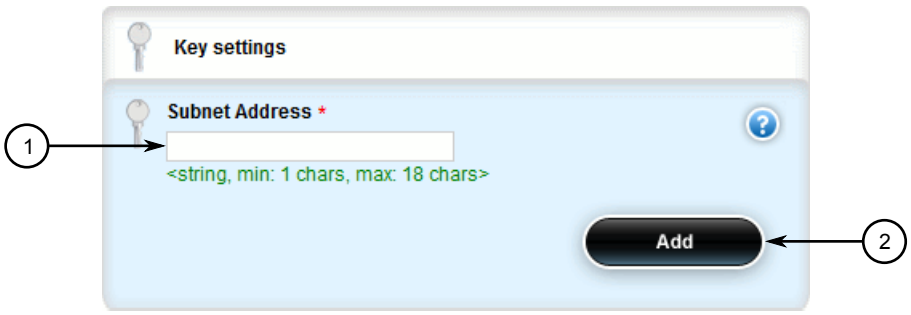


Figure 636: Key Settings Form

1. Subnet Address Box **2.** Add Button

4. Under **Subnet Address** type the IPv4 address and prefix, then 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 12.8.10.4
Deleting an Address for a Private Subnet

To delete an IP address for a private subnet, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to ***tunnel » ipsec » connection » {name} » {end} » subnet***, where *{name}* 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.

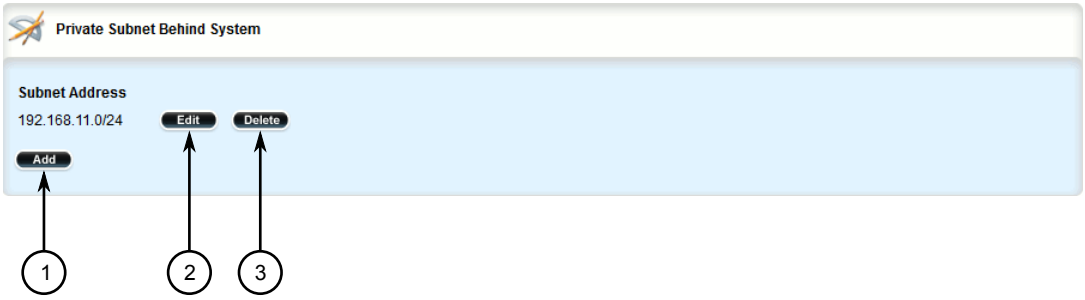


Figure 637: Private Subnet Behind System Table

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

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 12.8.11
Example: Configuring an Encrypted VPN Tunnel

This example describes how to configure an encrypted VPN tunnel over a public network using Layer 3 RUGGEDCOM ROX II devices.

IMPORTANT!
The values shown are specific to the provided topology. Actual values can vary based on the user's configuration.

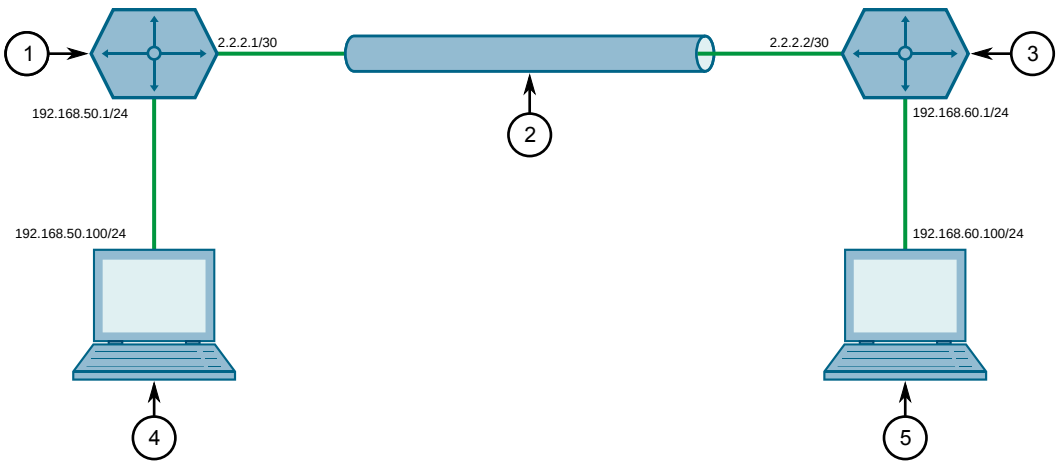


Figure 638: Topology – Site-to-Site Encrypted VPN Tunnel with a Pre-Shared Key

1. Device A **2.** IPsec Encrypted VPN Tunnel **3.** Device B **4.** Client 1 **5.** Client 2

To configure a VPN tunnel, do the following:

1. Configure a connection name for the VPN. For more information, refer to Section 12.8.6.2, "Adding a Connection".
2. Configure Device A:
   a. Configure a host name for the device. For more information, refer to Section 5.2, "Configuring the Host Name".
   b. Add a unique pre-shared key and configure the following parameters:

Parameter	Value
Local Address	2.2.2.1/30
Remote Address	2.2.2.2/30

   For more information, refer to Section 12.8.5.2, "Adding a Pre-Shared Key".
   c. Add an IPsec connection and configure the following parameters:

Parameter	Value
Startup Operation	start
Authenticate By	secret
Connection Type	tunnel

   For more information about IPsec connections, refer to Section 12.8.6.2, "Adding a Connection".
   d. Configure an Internet Key Exchange (IKE) algorithm with default values. For more information, refer to Section 12.8.7.2, "Adding an IKE Algorithm".
   e. Configure an Encapsulated Security Payload (ESP) algorithm with default values. For more information, refer to Section 12.8.8.3, "Adding an ESP Algorithm".
   f. Configure the left connection end for the IPsec tunnel with the following public IP address parameters:

Parameter	Value
Type	address
Value	2.2.2.1

For more information about configuring connection ends, refer to Section 12.8.9, "Configuring the Connection Ends".

g. Add subnet *192.168.50.0/24* for the left connection end. For more information, refer to Section 12.8.10.3, "Adding an Address for a Private Subnet".

h. Configure the right connection end for the IPsec tunnel with the following public IP address parameters:

Parameter	Value
Type	address
Value	2.2.2.2

For more information about configuring connection ends, refer to Section 12.8.9, "Configuring the Connection Ends".

i. Add subnet *192.168.60.0/24* for the right connection end. For more information, refer to Section 12.8.10.3, "Adding an Address for a Private Subnet".

3. Configure Device B:

a. Configure a host name for the device. For more information, refer to Section 5.2, "Configuring the Host Name".

b. Add a unique pre-shared key and configure the following parameters:

Parameter	Value
Local Address	2.2.2.2/30
Remote Address	2.2.2.1/30

For more information, refer to Section 12.8.5.2, "Adding a Pre-Shared Key".

c. Add an IPsec connection and configure the following parameters:

Parameter	Value
Startup Operation	start
Authenticate By	secret
Connection Type	tunnel

For more information about IPsec connections, refer to Section 12.8.6.2, "Adding a Connection".

d. Configure an Internet Key Exchange (IKE) algorithm with default values. For more information, refer to Section 12.8.7.2, "Adding an IKE Algorithm".

e. Configure an Encapsulated Security Payload (ESP) algorithm with default values. For more information, refer to Section 12.8.8.3, "Adding an ESP Algorithm".

f. Configure the right connection end for the IPsec tunnel with the following public IP address parameters:

Parameter	Value
Type	address

Parameter	Value
Value	2.2.2.2

For more information about configuring connection ends, refer to Section 12.8.9, "Configuring the Connection Ends".

g. Add subnet *192.168.60.0/24* for the right connection end. For more information, refer to Section 12.8.10.3, "Adding an Address for a Private Subnet".

h. Configure the left connection end for the IPsec tunnel with the following public IP address parameters:

Parameter	Value
Type	address
Value	2.2.2.1

For more information about configuring connection ends, refer to Section 12.8.9, "Configuring the Connection Ends".

i. Add subnet *192.168.50.0/24* for the left connection end. For more information, refer to Section 12.8.10.3, "Adding an Address for a Private Subnet".

4. Enable the IPsec tunnel. For more information, refer to Section 12.8.2, "Configuring IPsec Tunnels".
5. Verify the tunnel status and make sure the traffic between the two sites is encrypted:
   a. View the IPsec tunnel status and look for a message that includes the connection name and the words *erouted; eroute owner:*. For example:

```
000 "ipsec-12": 192.168.22.0/24===192.168.12.2<192.168.12.2>[C=CA, ST=Ontario, O=RuggedCom,
 CN=router2, E=router2@example.com,+S=C]...192.168.12.1<192.168.12.1>[C=CA, ST=Ontari o,
 O=RuggedCom, CN=router1, E=router1@example.com,+S=C]===192.168.11.0/24; erouted; eroute owner:
 #2
```

   This indicates the IPsec tunnel is active.

   For more information, refer to Section 12.8.4, "Viewing the IPsec Tunnel Status".

   b. Capture the packets using Tcpdump on one of the tunnel interfaces. Encrypted traffic will display an *ESP* header. For more information about using the Tcpdump utility, refer to Section 2.5.9, "Capturing Packets from a Network Interface".

Final Configuration Example

The following configuration reflects the topology:

Device A

```
# show full-configuration
tunnel
ipsec
  enabled
  preshared-key 2.2.2.2 2.2.2.1
   key SiEm3nsRu993dc@m
  !
  connection test
   startup         start
   authenticate    secret
   connection-type tunnel
```

```
      ike algorithm any any any
   !
   esp algorithm any any
   !
   left
    public-ip type address
    public-ip value 2.2.2.1
    subnet 192.168.50.0/24
   !
   right
    public-ip type address
    public-ip value 2.2.2.2
    subnet 192.168.60.0/24
```

» Device B

```
# show full-configuration
tunnel
ipsec
  enabled
  preshared-key 2.2.2.1 2.2.2.2
   key SiEm3nsRu993dc@m
  !
  connection test
   startup         start
   authenticate    secret
   connection-type tunnel
      ike algorithm any any any
   !
   esp algorithm any any
   !
   left
    public-ip type address
    public-ip value 2.2.2.1
    subnet 192.168.50.0/24
   !
   right
    public-ip type address
    public-ip value 2.2.2.2
    subnet 192.168.60.0/24
```

Section 12.9

Managing 6in4 and 4in6 Tunnels

In networks where IPv4 and IPv6 operate simultaneously, 6in4 and 4in6 tunnels can be used to enable IPv6/IPv4 hosts to reach services using the opposite protocol. IPv6/IPv4 hosts and networks isolated from one another can also use these tunnels to access one another.

In a 6in4 tunnel, IPv6 traffic is encapsulated over configured IPv4 links, and vice versa for 4in6 tunnels.

NOTE
For information about how to monitor traffic through the tunnel, refer to Section 7.1.2, "Viewing Statistics for Routable Interfaces".

CONTENTS

Section 12.9.1
Enabling/Disabling 6in4 or 4in6 Tunnels

To enable or disable all 6in4 or 4in6 tunnels, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to ***tunnel » ip6in4 | ip4in6***. The **IP6in4 Tunnel** or **IP4in6 Tunnel** form appears.

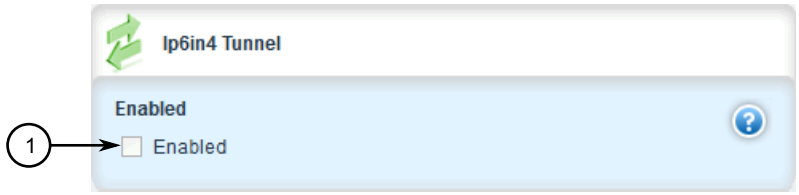


Figure 639: IP6in4 Tunnel Form (Example)

1. Enabled Check Box

3. Click **Enabled** to enable 6in4 or 4in6 tunnels, or clear **Enabled** to disable 6in4 or 4in6 tunnels.
4. Select or clear **Enabled**.
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 12.9.2
Viewing a List of 6in4 or 4in6 Tunnels

To view a list of 6in4 or 4in6 tunnels configured on the device, navigate to ***tunnel » ip6in4 | ip4in6 » tunnel***. The **IP6in4 Tunnels** or **IP4in6 Tunnels** table appears.

Figure 640: IP6in4 Tunnels Table (Example)

Section 12.9.3

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.

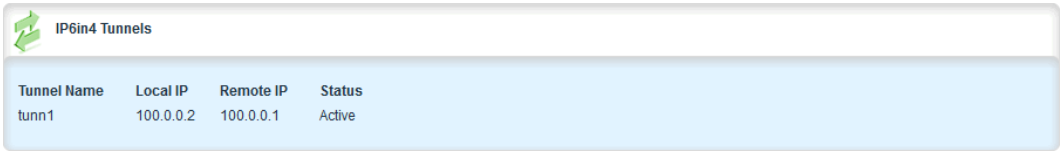


Figure 641: IP6in4 Tunnels Table (Example)

Section 12.9.4

Adding a 6in4 or 4in6 Tunnel

To add a 6in4 or 4in6 tunnel, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to ***tunnel » ip6in4 | ip4in6 » tunnel*** and click **<Add tunnel>**. The **Key Settings** form appears.

Figure 642: 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	**Synopsis:** A string Tunnel name

4. Click **Add** to create the new tunnel. The **IP6in4 Tunnels** or **IP4in6 Tunnels** form appears.

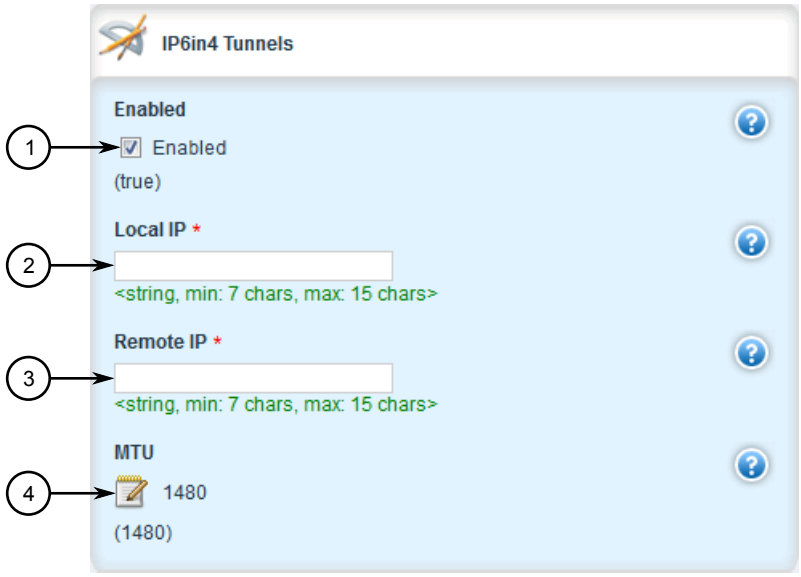


Figure 643: IP6in4 Tunnels Form (Example)

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	**Synopsis:** A string 7 to 15 characters long The interface upon which the tunnel is created This parameter is mandatory.
Remote IP	**Synopsis:** A string 7 to 15 characters long Ip address of remote tunnel end This parameter is mandatory.
Status	**Synopsis:** A string Current status of tunnel This parameter is mandatory.

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 12.9.5

Deleting a 6in4 or 4in6 Tunnel

To delete a 6in4 or 4in6 tunnel, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to ***tunnel » ip6in4 | ip4in6 » tunnel***. The **IP6in4 Tunnels** or **IP4in6 Tunnels** table appears.

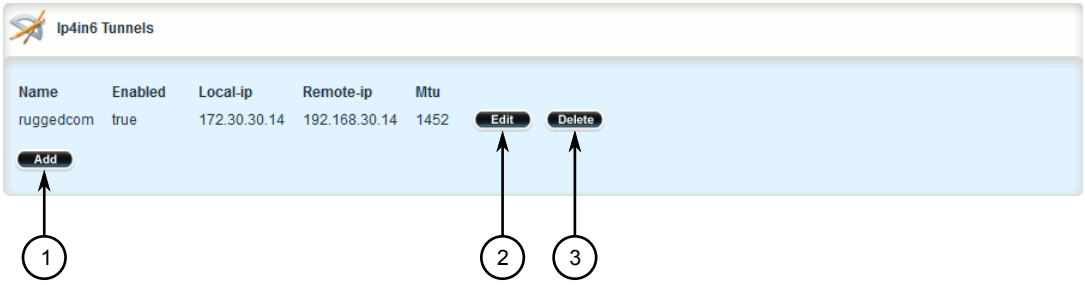


Figure 644: IP6in4 Tunnels Table (Example)

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 12.10

Managing DMVPN

This section describes how to configure the device as a spoke in a Dynamic Multipoint Virtual Private Network (DMVPN) hub-and-spoke network.

CONTENTS

Section 12.10.1

Understanding DMVPN

Dynamic Multipoint Virtual Private Network (DMVPN) is a routing solution for building scalable and secure VPN networks. It allows network designers to rapidly deploy routers for medium to large enterprises without having to configure static connections between all devices.

DMPVN can be deployed in one of two ways.

- Hub-and-Spoke
- Spoke-to-Spoke

RUGGEDCOM ROX II supports hub-and-spoke deployments where a central router (the hub) uses Multipoint Generic Routing Encapsulation (mGRE) to establish GRE tunnels with one or more routers (the spokes). When spokes need to send traffic to one another, they send it to the hub first and the hub directs the data packets to the

appropriate destination. This method allows network designers to avoid the complex task of defining static GRE tunnels for each possible connection.

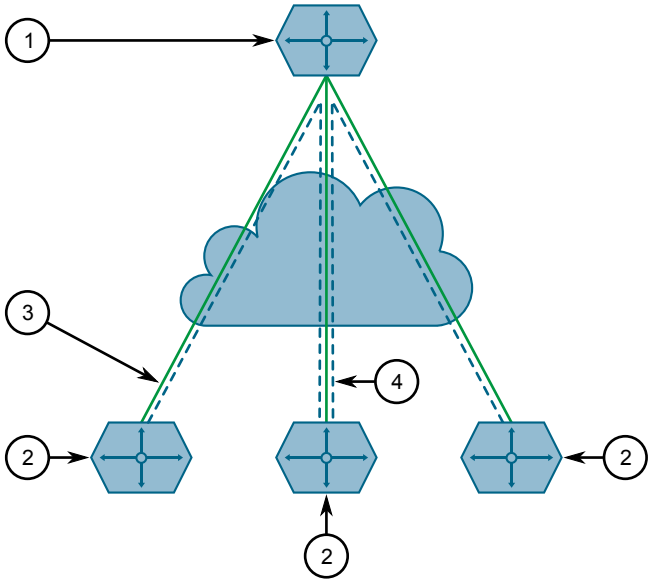


Figure 645: Hub-and-Spoke Topology – Single Hub

1. Hub (Static IP Address) **2.** Spoke (Static IP Address) **3.** Hub-to-Spoke GRE/IPsec Tunnel

Spokes can also be connected to a secondary hub when redundancy is required.

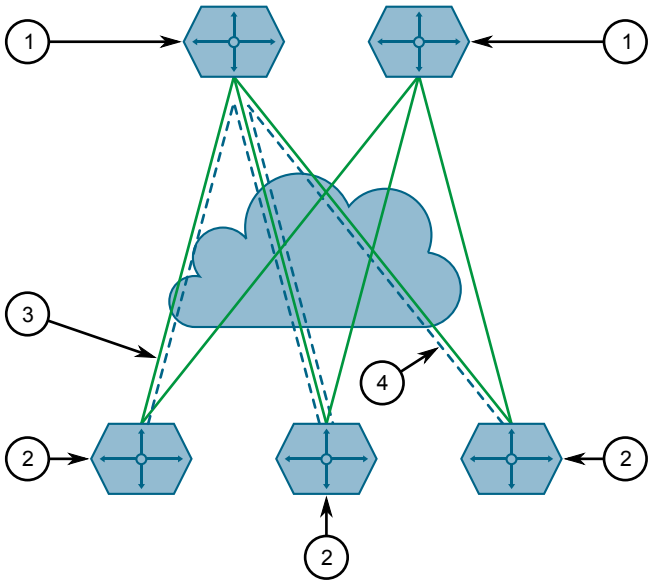


Figure 646: Hub-and-Spoke Topology – Dual Hub

1. Hub (Static IP Address) **2.** Spoke (Static IP Address) **3.** Hub-to-Spoke GRE/IPsec Tunnel

Section 12.10.2
Configuring DMVPN

To configure the device to act as a spoke in a hub-and-spoke network, do the following:

NOTE
RUGGEDCOM ROX II supports connections with up to two hubs.

1. Determine the static IP address of the hub router.
2. Configure a GRE tunnel to the hub. For more information, refer to Section 12.7.3, "Adding a GRE Tunnel".
3. Configure IPsec for the GRE tunnel, making sure the connection name matches the name of the GRE interface (e.g. gre-t1). For more information, refer to Section 12.8.2, "Configuring IPsec Tunnels".
4. Configure a BGP route for the GRE tunnel. For more information, refer to Section 13.8.1, "Configuring BGP".
5. Navigate to ***services » nhrp***. The **NHRP** form appears.

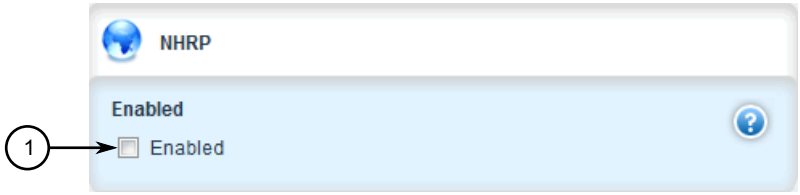


Figure 647: NHRP Form

6. Click **Enabled** to enable the DMPVN service.

NOTE
RUGGEDCOM ROX II supports up to two DMVPN interfaces, each of which can be assigned to different GRE tunnels.

7. Configure a DMVPN interface for the GRE tunnel. For more information, refer to Section 12.10.3.2, "Adding a DMVPN Interface".
8. Configure an IPsec/GRE tunnel from the hub to the device, using the IP address defined for the device's DMVPN interface.
9. Verify the status of the DMVPN connection. For more information, refer to Section 12.10.4, "Viewing the Status of DMVPN".

Section 12.10.3
Managing DMVPN Interfaces

Configure a DMVPN interface to connect with a host. Up to two interfaces can be configured, allowing the device to connect with two hubs.

CONTENTS

Section 12.10.3.1
Viewing a List of DMVPN Interfaces

To view a list of DMVPN interfaces, navigate to ***services » nhrp » interface-nhrp***. If interfaces have been configured, the **NHRP Interfaces** table appears.

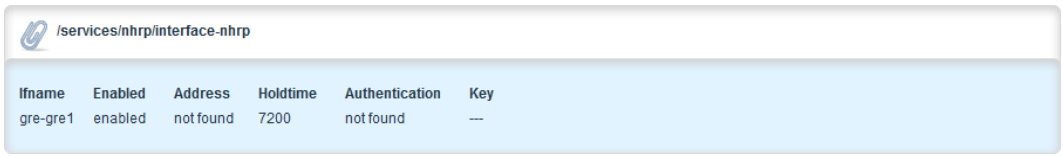


Figure 648: NHRP Interfaces Table

If no interfaces have been configured, add interfaces as needed. For more information, refer to Section 12.10.3.2, "Adding a DMVPN Interface".

Section 12.10.3.2
Adding a DMVPN Interface

To add a DMVPN interface, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to ***services » nhrp » interface-nhrp***.
3. Click **<Add interface-nhrp>**. The **Key Settings** form appears.

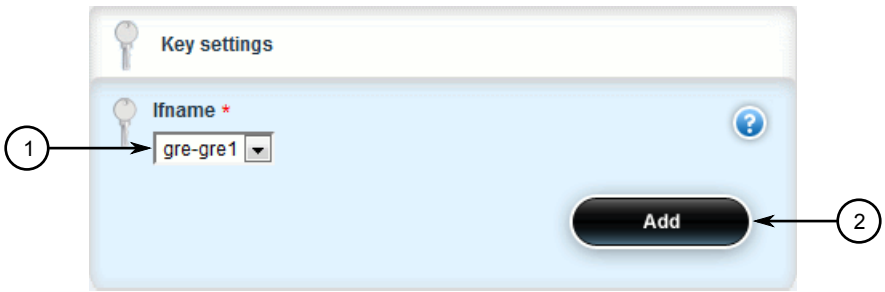


Figure 649: Key Settings Form

1. Interface Name List **2.** Add Button

4. Configure the following parameter:

Parameter	Description
ifname	**Synopsis:** A string

Parameter	Description
	Interface name for the Generic Routing Encapsulation (GRE) tunnel to be used for NHRP: Note that the ipsec connection to be used for this interface must be configured with the same name as this interface. Maximum number of interfaces is 2.

5. Click **Add**. The **NHRP Interfaces** form apppears.

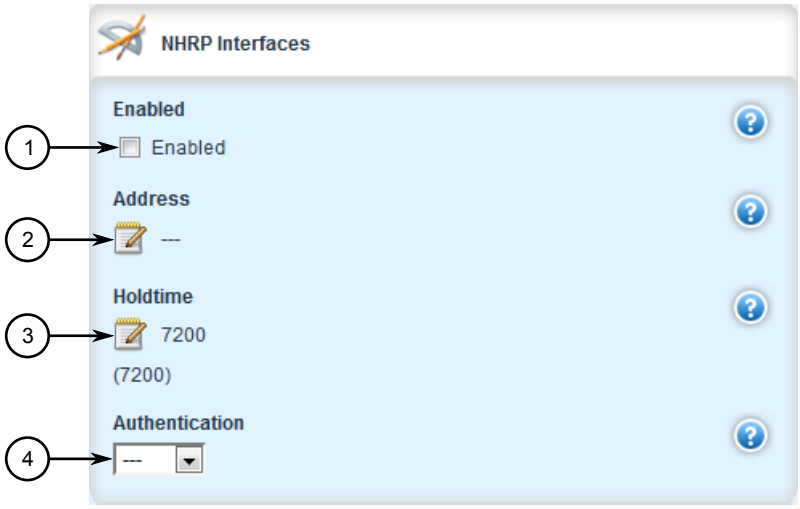


Figure 650: NHRP Interfaces Form

1. Enabled Check Box **2.** Address Box **3.** Hold Time Box **4.** Authentication Mode List **5.** Authentication Key Box

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

CAUTION!
Security hazard – risk of unauthorized access and/or exploitation. For increased security, Siemens recommends configuring a key to authenticate the NHRP interface.

Parameter	Description
enabled	A boolean flag to indicate Next Hop Resolution Protocol (NHRP) is enabled on this interface.
address	**Synopsis:** A string 9 to 18 characters long IPv4 address of remote GRE interface to be used for this NHRP session.
holdtime	**Synopsis:** A 32-bit unsigned integer **Default:** 7200 The time (in seconds) that Non-Broadcast Multi-Access (NBMA) addresses are advertised as valid in authoritative NHRP responses. Default is 7200 seconds.
authentication	**Synopsis:** { none, cisco } The authentication string to allow intercommunication between source and destination NHRP nodes. Maximum length is 8 characters. Currently, only CISCO authentication is supported.
key	**Synopsis:** A string The authentication key to allow intercommunication between source and destination NHRP nodes. Maximum length is 8 characters.

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 12.10.3.3
Deleting a DMVPN Interface

To delete a DMVPN interface, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to ***services » nhrp » interface-nhrp***. The **NHRP Interfaces** table appears.

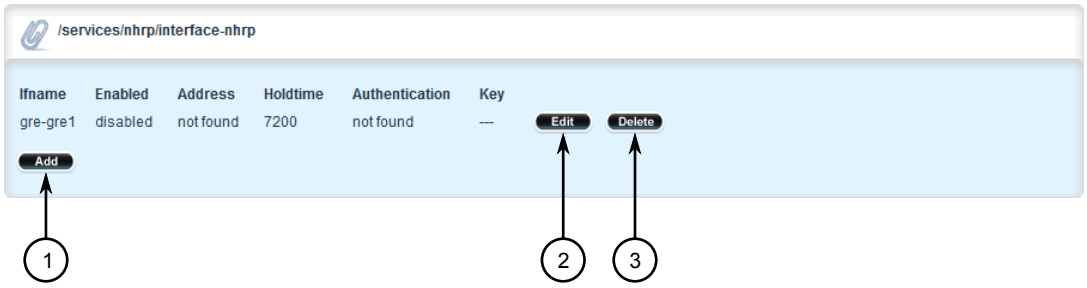


Figure 651: NHRP Interfaces Table

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 12.10.4
Viewing the Status of DMVPN

To view the status of the DMVPN service, navigate to ***services » nhrp » status***. If DMVPN interfaces have been configured, the **DMVPN Status** table appears.

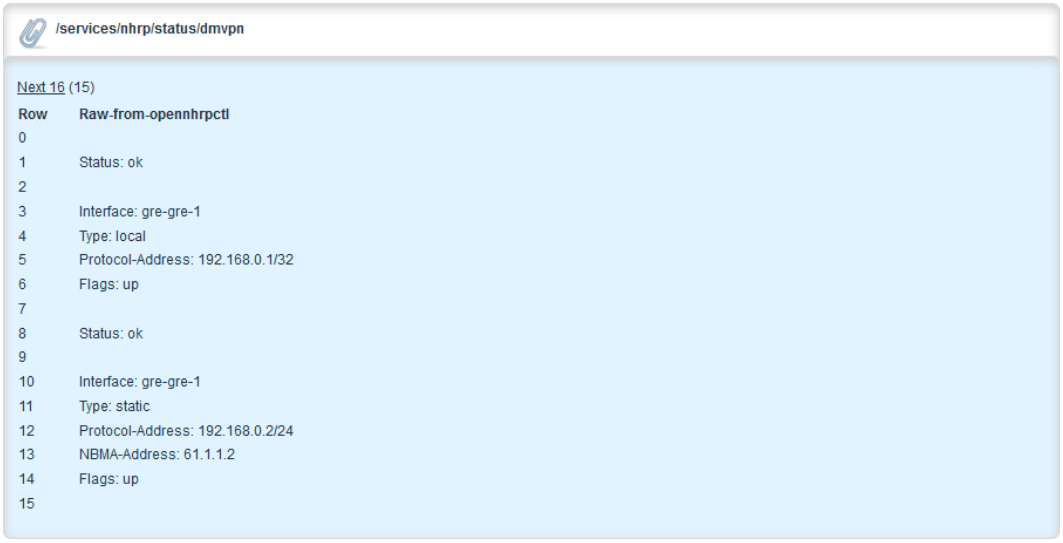


Figure 652: DMVPN Status Table

Information provided is taken directly from NHRP. The following are some of the fields that may be displayed:

NOTE
Some fields only display when applicable.

Field	Description	Example
Status	The status of the interface.	Status: ok
Interface	The name of the interface.	Interface: gre-t1
Type	The NHRP peer type. Possible values: • `shortcut-route` – Received or relayed resolution for the route • `incomplete` – Resolution request sent but no reponse received yet • `negative` – Negative cached • `cached` – Received or relayed resolution • `dynamic` – NHC registration • `dynamic-nhs` – Dynamic NHS from DNS map • `static` – Static map from the configuration file • `static-dns` – Static DNS map from the configuration file • `local-route` – Non-local destination, with local route • `local` – Local destination, IP or off-NBMA subnet	Type: local
Protocol-Address	The interface's IP address.	Protocol-Address: 172.30.168.2/32
Flags	The flag(s) assigned to the last NHRP registration request packet. Possible values: • `unique` – The NHRP peer is unique. Its NRHP mapping entry cannot be overwritten by a mapping entry with the same IP address, even if the associated peer has a different NBMA address. • `used` – The NHRP peer is in the kernel ARP table.	Flags: up

Field	Description	Example
	• `up` – A connection with the NHRP peer has been established and the link is up. • `lower-up` – A connection with the NHRP peer has been established.	
NBMA-Address	The interface's NBMA address.	NBMA-Address: 172.19.20.21
NBMA-NAT_OA-Address	The interface's external IP address and mask. Displays only when the hub is behind a NAT-enabled router.	NBMA-NAT_OA-Address: 172.16.0.0/12
Expires-in	The time in seconds before the NBMA information of the responder is considered invalid and discarded. Displays only when the *`Hold Time`* is configured.	Expires-in: 120
Hostname	The host name of the NBMA responder, when available.	Hostname: ruggedcom

13 Unicast and Multicast Routing

This chapter describes how to configure, monitor and manage static and dynamic routes unicast and multicast traffic.

CONTENTS

Section 13.1

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.

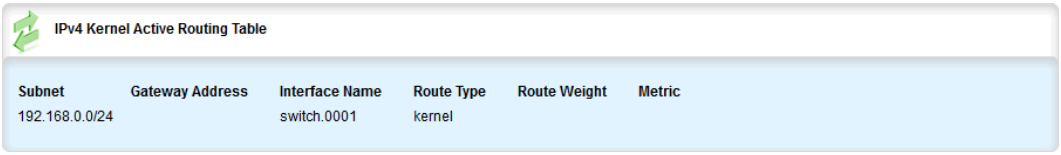


Figure 653: IPv4 Kernel Active Routing Table

This table provides the following information:

Parameter	Description
Subnet	**Synopsis:** A string The network/prefix.
Gateway Address	**Synopsis:** A string The gateway address.
Interface Name	**Synopsis:** A string The interface name.
Route Type	**Synopsis:** A string The route type.
Route Weight	**Synopsis:** A string The route weight.
Metric	**Synopsis:** A string The route metric value.

If no IPv4 routes have been configured, add routes as needed. For more information, refer to Section 7.1.3.2, "Adding an IPv4 Address".

Section 13.2

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.

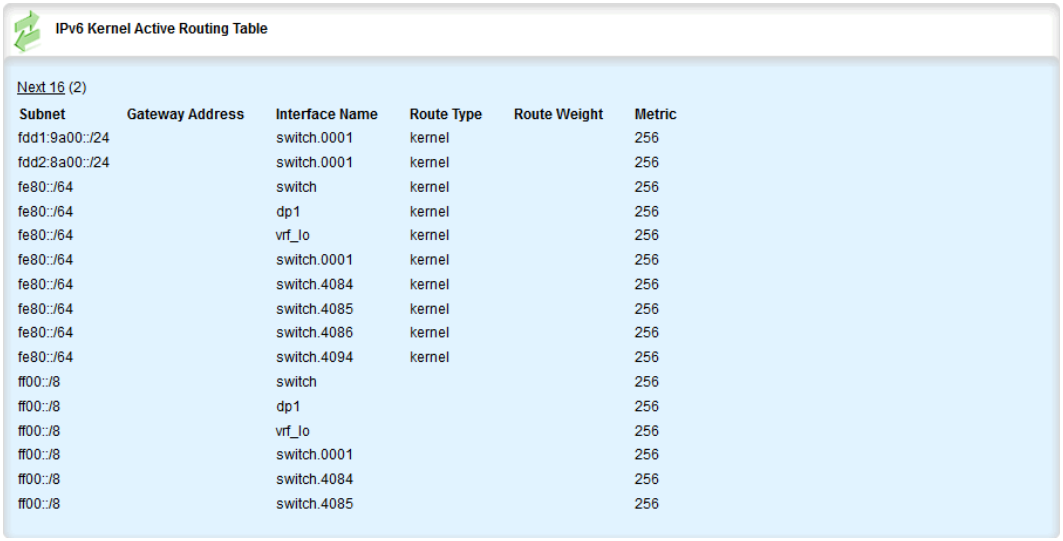


Figure 654: IPv6 Kernel Active Routing Table

This table provides the following information:

Parameter	Description
Subnet	**Synopsis:** A string The network/prefix.
Gateway Address	**Synopsis:** A string The gateway address.
Interface Name	**Synopsis:** A string The interface name.
Route Type	**Synopsis:** A string The route type.
Route Weight	**Synopsis:** A string The route weight.
Metric	**Synopsis:** A string The metric value.

If no IPv6 routes have been configured, add routes as needed. For more information, refer to Section 13.12.3, "Adding an IPv6 Static Route".

Section 13.3

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.

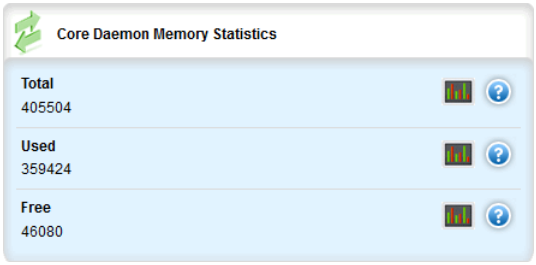


Figure 655: Core Daemon Memory Statistics Form

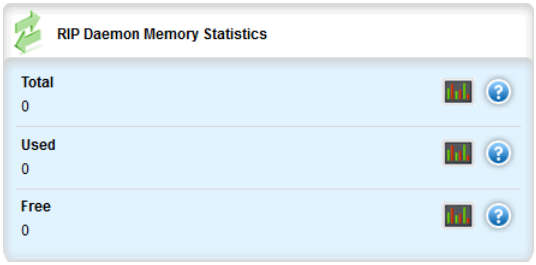


Figure 656: RIP Daemon Memory Statistics Form

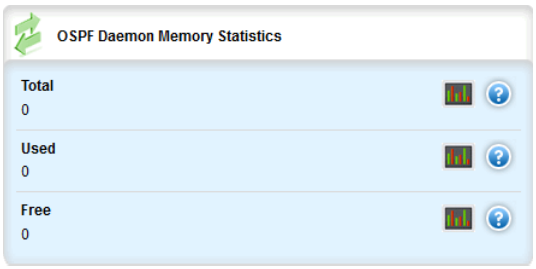


Figure 657: OSPF Daemon Memory Statistics Form

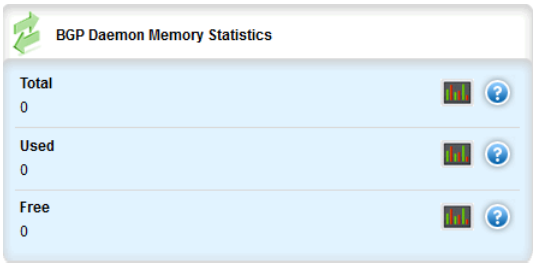


Figure 658: BGP Daemon Memory Statistics Form

These forms provides the following information:

Parameter	Description
total	**Synopsis:** A 32-bit unsigned integer

Parameter	Description
	The total heap allocated (in bytes). This parameter is mandatory.
used	**Synopsis:** A 32-bit unsigned integer The number of used ordinary blocks (in bytes). This parameter is mandatory.
free	**Synopsis:** A 32-bit unsigned integer The number of free ordinary blocks (in bytes). This parameter is mandatory.

Section 13.4

Configuring ICMP

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.

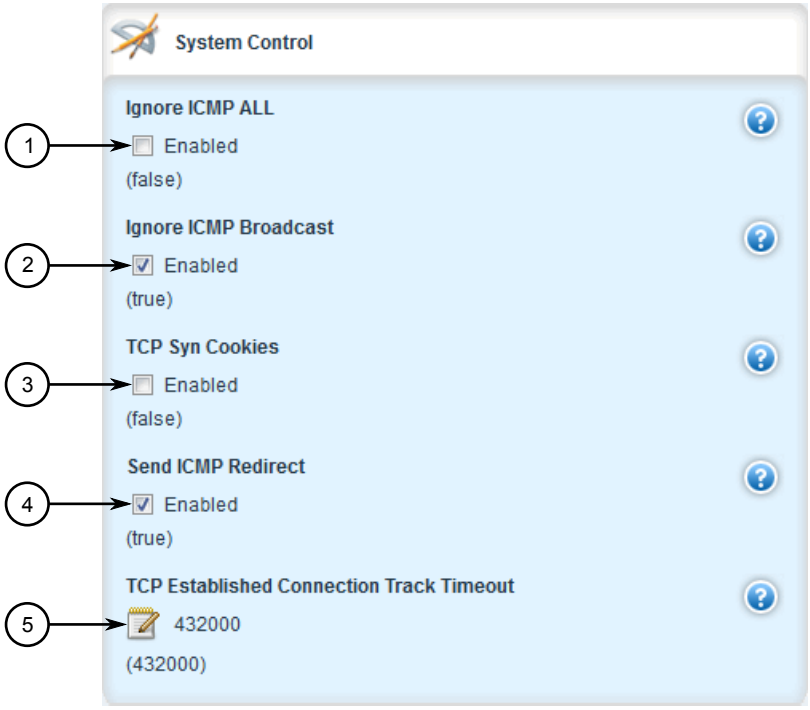


Figure 659: System Control Form

1. Ignore ICMP ALL Check Box **2.** Ignore ICMP Broadcast Check Box **3.** TCP Syn Cookies Check Box **4.** Send ICMP Redirect Check Box **5.** TCP Established Connection Track Timeout Box

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	**Synopsis:** { true, false } **Default:** false Ignores all ICMP echo requests sent to it.
Ignore ICMP Broadcast	**Synopsis:** { true, false } **Default:** true Ignores all ICMP ECHO and TIMESTAMP requests sent to it via broadcast/multicast.
Send ICMP Redirect	**Synopsis:** { true, false } **Default:** true Sends the ICMP redirect.

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 13.5
Managing Event Trackers

Trackers monitor the availability of hosts or devices by periodically transmitting ICMP messages (or pings). Based on the ICMP results, the tracker updates operational data with the status of the host or device as it changes (i.e. between "up " and "down" states). Other parts of the system can then subscribe to the operational data to be notified when changes take place.

Where available, a tracker can allow a user greater flexibility when configuring a feature. For example, advertised or received routes can be filtered or blocked entirely, based on the status of the tracker.

NOTE
Trackers only use ICMP messages to ping an IP target. Therefore, it can only provide availability for an IP device, and only up to the IP layer.

CONTENTS

Section 13.5.1

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.

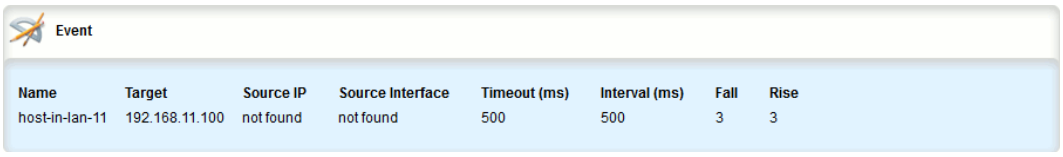


Figure 660: Event Table

If no event trackers have been configured, add event trackers as needed. For more information, refer to Section 13.5.3, "Adding an Event Tracker".

Section 13.5.2

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.

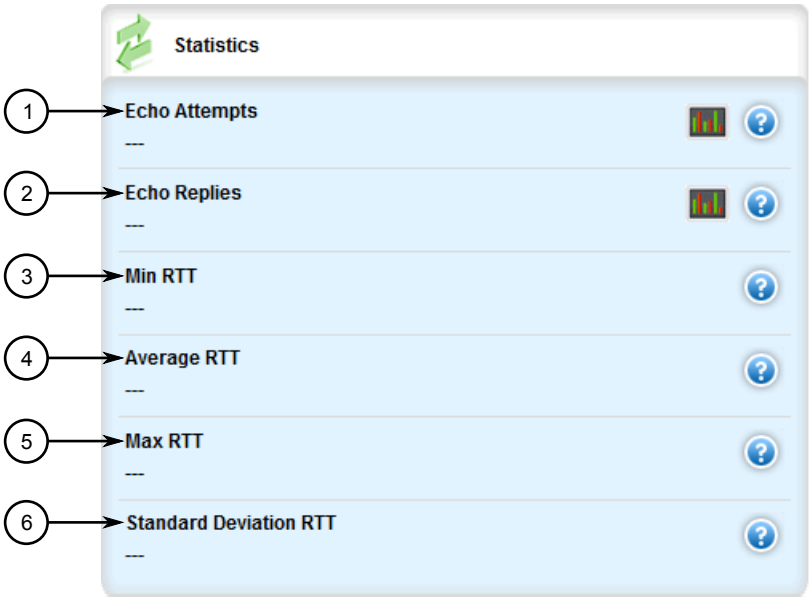


Figure 661: Statistics Form

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	**Synopsis:** A 32-bit unsigned integer The number of echo attempts.
Echo Replies	**Synopsis:** A 32-bit unsigned integer The number of echo replies.
Min RTT	**Synopsis:** A string The minimum of the round trip time (in milliseconds).
Average RTT	**Synopsis:** A string The average of the round trip time (in milliseconds).
Max RTT	**Synopsis:** A string The maximum of the round trip time (in milliseconds).
Standard Deviation RTT	**Synopsis:** A string The standard deviation of the round trip time (in milliseconds).

Section 13.5.3
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.

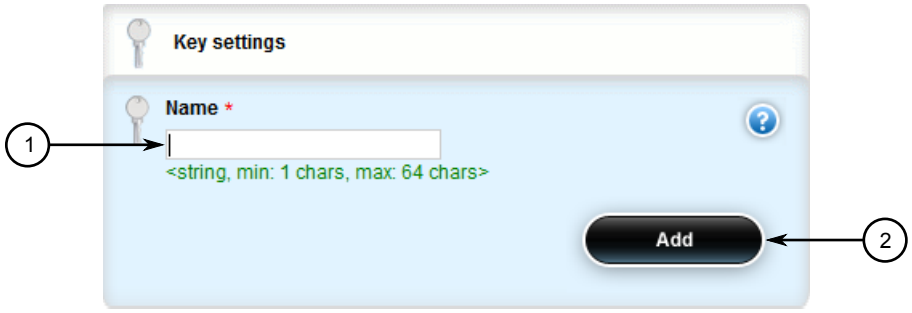


Figure 662: Key Settings Form

1. Name Box **2.** Add Button

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

Parameter	Description
Name	**Synopsis:** A string 1 to 4095 characters long The name of the event.

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

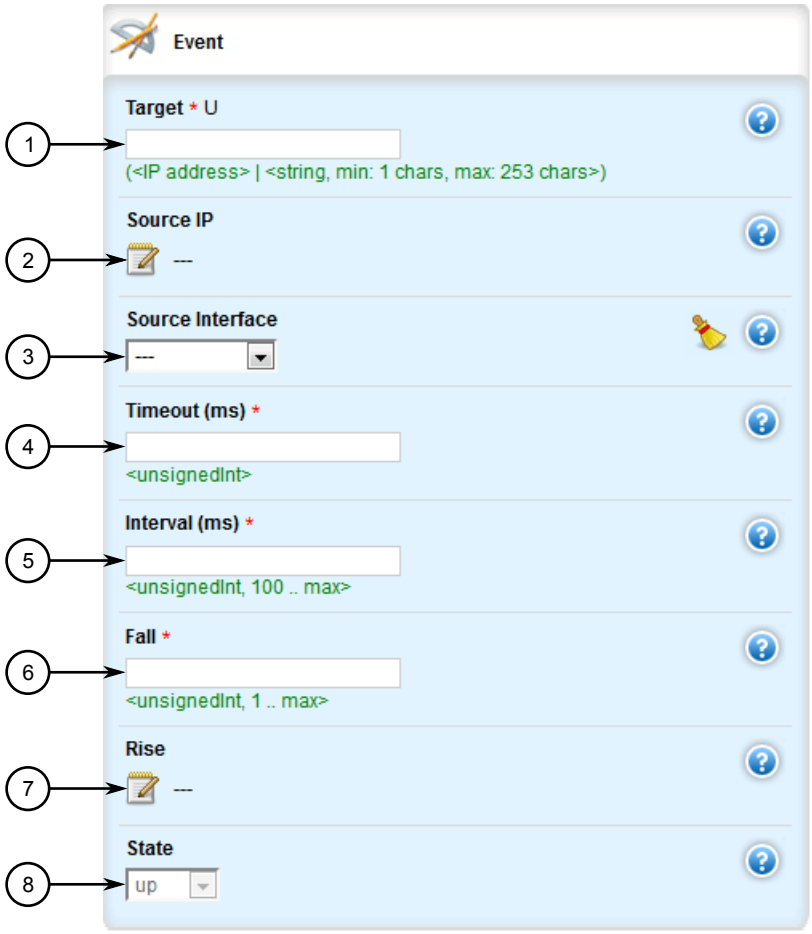


Figure 663: Event Form

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	**Synopsis:** A string 1 to 253 characters long Configures the ping target as an IPv4 address or hostname.domain. This parameter is mandatory.
Source IP	**Synopsis:** A string 7 to 15 characters long or a string 6 to 40 characters long Sets the source address to a specified IPv4 address.
Source Interface	**Synopsis:** A string Forces a ping on a selected interface.
Timeout (ms)	**Synopsis:** A 32-bit unsigned integer Determines how many milliseconds to wait for the ICMP response. This parameter is mandatory.
Interval (ms)	**Synopsis:** A 32-bit unsigned integer equaling 100 or higher Determines how many milliseconds to wait before sending another ICMP request.

Parameter	Description
	This parameter is mandatory.
Fall	**Synopsis:** A 32-bit unsigned integer equaling 1 or higher The number of times a failure occurs before changing the tracking state from up to down. This parameter is mandatory.
Rise	**Synopsis:** A 32-bit unsigned integer equaling 1 or higher The number of times success occurs before changing the tracking state from down to up.
state	**Synopsis:** { up, down } **Default:** up The state of the event.

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 13.5.4

Deleting an Event Tracker

To delete an event tracker, do the following:

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

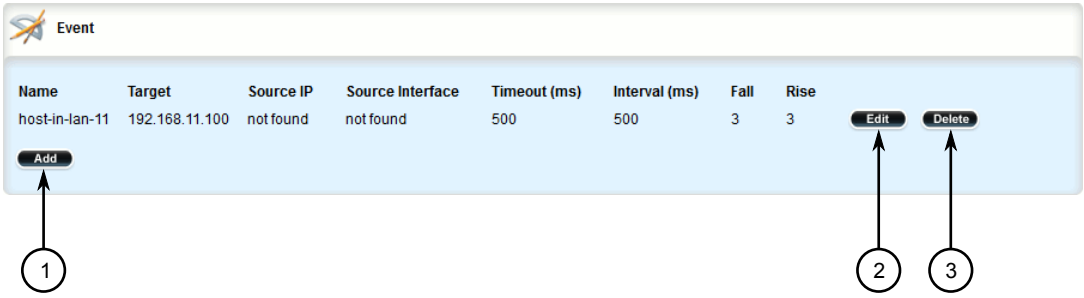


Figure 664: Event Table

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

3. Click **Delete** next to the chosen event tracker.
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 13.6
Managing IS-IS

Intermediate System - Intermediate System (IS-IS) is one of a suite of routing protocols tasked with sharing routing information between routers. The job of the router is to enable the efficient movement of data over sometimes complex networks. Routing protocols are designed to share routing information across these networks and use sophisticated algorithms to decide the shortest route for the information to travel from point A to point B. One of the first link-state routing protocols was IS-IS developed in 1986 and later published in 1987 by ISO as ISO/IEC 10589. It was later republished as an IETF standard (RFC 1142 [http://tools.ietf.org/html/rfc1142]).

CONTENTS

Section 13.6.1
IS-IS Concepts

IS-IS is an Interior Gateway Protocol (IGP) meant to exchange information within Autonomous Systems (AS). It is designed to operate within an administrative domain or network using link-state information to decide optimal data packet routing, similar to OSPF. IS-IS floods the network with link-state information and builds a database of the network's topology. The protocol computes the best path through the network (using Dijkstra's algorithm) and then forwards packets to their destination along that path.

Although it was originally designed as an ISO Connectionless-mode Network Protocol (CLNP), it was later adapted for IP network use (Dual IS-IS) in RFC 1195 [http://tools.ietf.org/html/rfc1195]. IS-IS is used primarily in ISP environments and better suited to *stringy* networks as opposed to central core based networks.

NOTE
In complex legacy networks, RIP, OSPF, BGP and IS-IS may all be active on the same router at the same time. Typically, however, only one dynamic routing protocol is employed at one time.

CONTENTS

Section 13.6.1.1
IS-IS Routers

IS-IS routers can be defined as Level-1, Level-2, or both. Level 1 routers form the area, while Level 2 routers form the backbone of the network. By default, RUGGEDCOM ROX II configures areas to be both (or Level-1-2). This allows the device to inter-operate between different areas with minimal configuration.

- **Level-1** routers are intra-area routers. They maintain a single Link-State Database (LSD) that only contains information about the Level-1 and Level-2 neighbors in its area. To communicate with routers in another area, Level-1 routers forward traffic through their closest Level-2 router.
- **Level-2** routers are inter-area routers, meaning they can communicate with routers in other areas. They also maintain a single LSD, but it only contains information about other Level-2 routers from the router's area or other areas. The router knows nothing about the Level-1 routers in its area.
- **Level-1-2** routers are both inter- and intra-area routers, meaning they can communicate with Level-1 and Level-2 routers in any area. They maintain separate LSDs for Level-1 and Level-2 routers in and outside the router's area.

Section 13.6.1.2
Network Entity Title (NET) Addresses

IS-IS routers are identified by their Network Entity Title (NET) address, which is in Network Service Access Point (NSAP) format (RFC 1237 [http://tools.ietf.org/html/rfc1237]). NSAP addresses range from 8 to 20 octets and consist of the Authority and Format Identifier (1 byte), the Area ID (0 to 12 bytes), the System ID (6 bytes) and the selector (1 byte).

The following is an example of an NSAP address:

```
NSAP address: 49.0001.1921.6800.1001.00

AFI: 49 (typical for IS-IS NET addresses)
Area ID: 0001 (typically 4 bytes)
System ID: 1921.6800.1001 (equates to the IP address 192.168.1.1)
Selector: 00 (NET addresses always have a selector of 00)
```

Section 13.6.1.3
Advantages and Disadvantages of Using IS-IS

The advantages and disadvantages of using IS-IS include the following:

Advantages

- runs natively on the OSI network layer
- can support both IPv4 and IPv6 networks due to it's independence from IP addressing
- IS-IS concept of areas is simpler to understand and implement
- IS-IS updates grouped together and sent as one LSP, rather than several small LSAs as with OSPF

Disadvantages

- used mostly by service providers
- limited support by network stack vendors and equipment makers
- CLNP addressing can be new and confusing to many users

- better scalability than OSPF due to a leaner daemon with less overhead
- gaining popularity among service providers
- integrates with MPLS
- protects from *spoofing* and Denial of Service (DoS) attacks due to use of the data link layer

Section 13.6.2
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.

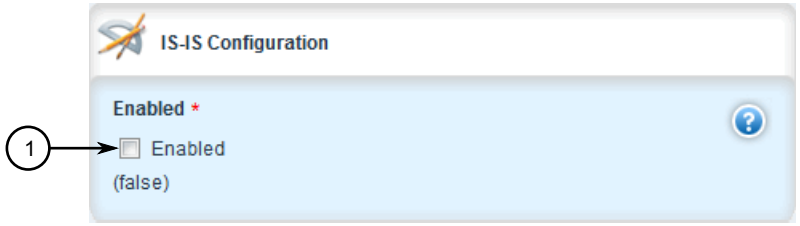


Figure 665: IS-IS Configuration Form

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 13.6.5, "Managing Area Tags".
5. Configure one or more interfaces on which to perform IS-IS routing. For more information, refer to Section 13.6.6, "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.

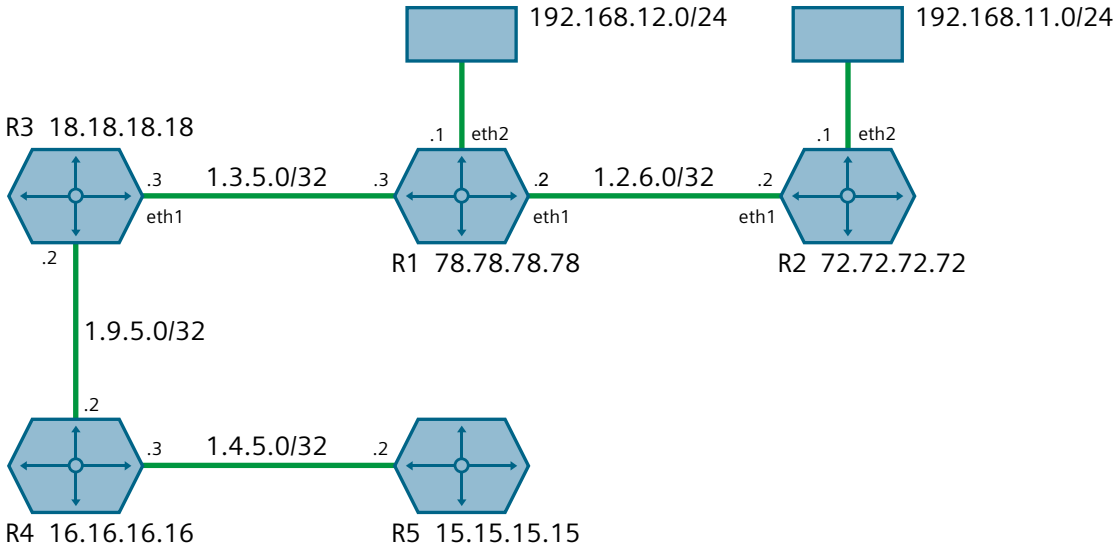


Figure 666: Multi-Level IS-IS Configuration

Section 13.6.3

Viewing the Status of Neighbors

To view the status of neighboring devices on an IS-IS network, do the following:

1. Make sure IS-IS is configured. For more information, refer to Section 13.6.2, "Configuring IS-IS".
2. Navigate to ***routing » status » isis » isis-neighbors-status***. The **Trigger Action** form appears.

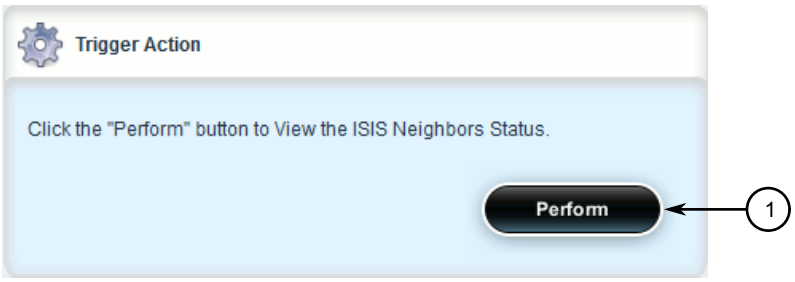


Figure 667: Trigger Action Form

1. Perform Button

3. Click **Perform**. The **ISIS Neighbors Status** form appears.

Figure 668: 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. Possible levels are `1`, `2` and `3`, where `3` represents levels 1 and 2.
State	Adjacency state.
Holdtime	The remaining hold time in seconds.
SNPA	The MAC address of the Sub-Network Point of Attachment (SNPA).

Section 13.6.4

Viewing the Status of the Link-State Database

To view the basic status of the link-state database for the IS-IS network, do the following:

1. Make sure IS-IS is configured. For more information, refer to Section 13.6.2, "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.

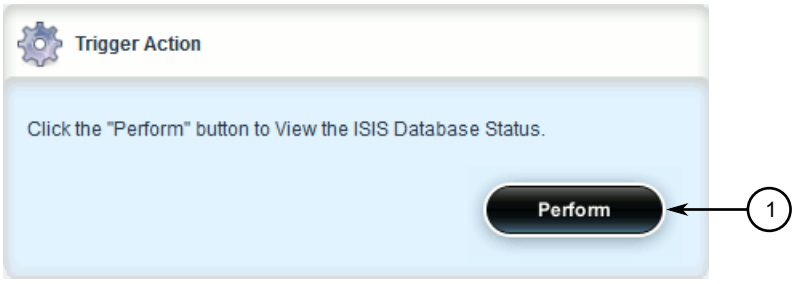


Figure 669: Trigger Action Form - Basic View

1. Perform Button

3. Click **Perform**. The **ISIS Database Status** or **ISIS Database Detail Status** form appears.

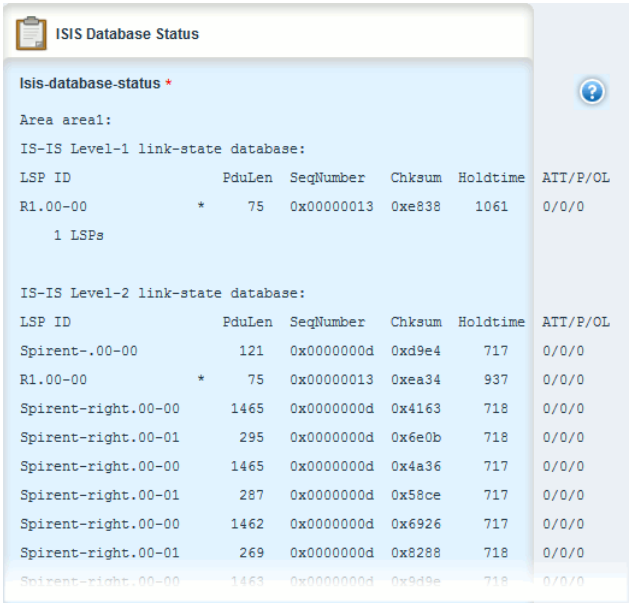


Figure 670: ISIS Database Status Form

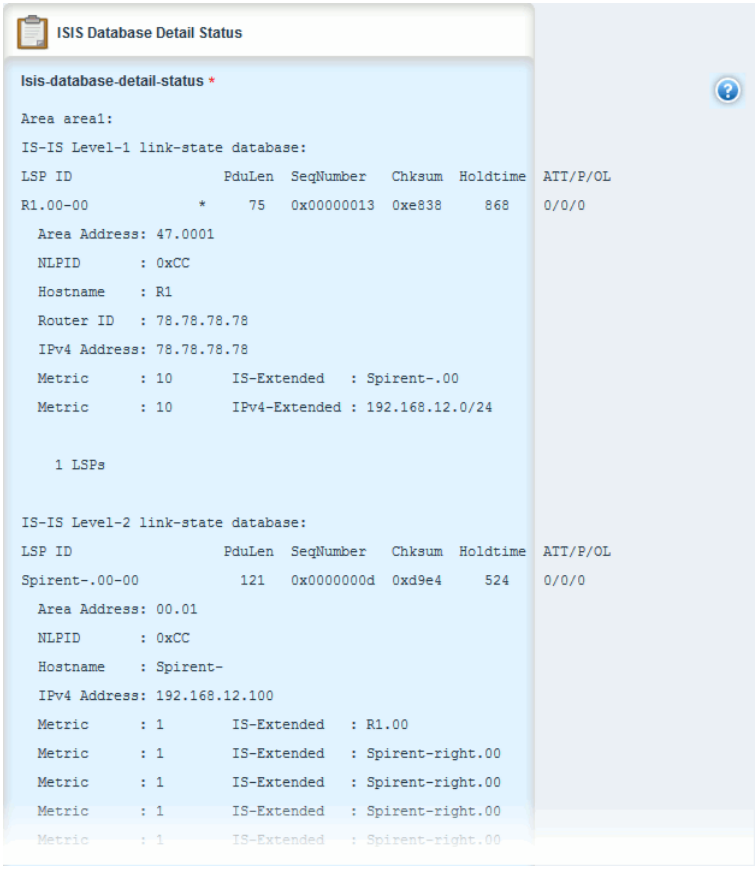


Figure 671: ISIS Database Detail Status Form

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 13.6.5

Managing Area Tags

An IS-IS area is a grouping of inter-connected (or neighboring) IS-IS configured routers. As opposed to OSPF, where an Area Border Router (ABR) can exist in two areas at once, IS-IS routers reside only in one area. It is the link between routers in two different areas that forms the border. This is because an IS-IS router has only one Network Service Access Point (NSAP) address.

A single router can be configured to act as a Level-1, Level-2 or Level-1-2 router in one or more areas.

Routers are associated with areas by area tags, which define the routing type, metric, and authentication/ authorization rules.

CONTENTS

Section 13.6.5.1

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.

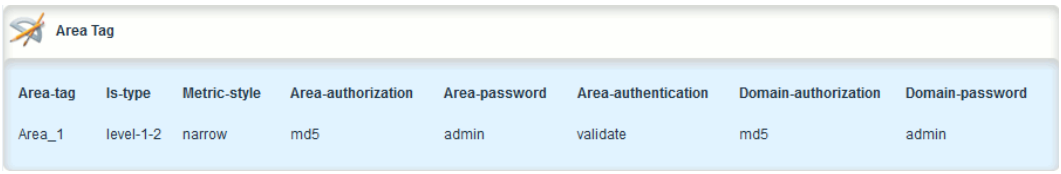


Figure 672: Area Tag Table

If no area tags have been configured, add area tags as needed. For more information, refer to Section 13.6.5.2, "Adding an Area Tag".

Section 13.6.5.2

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.

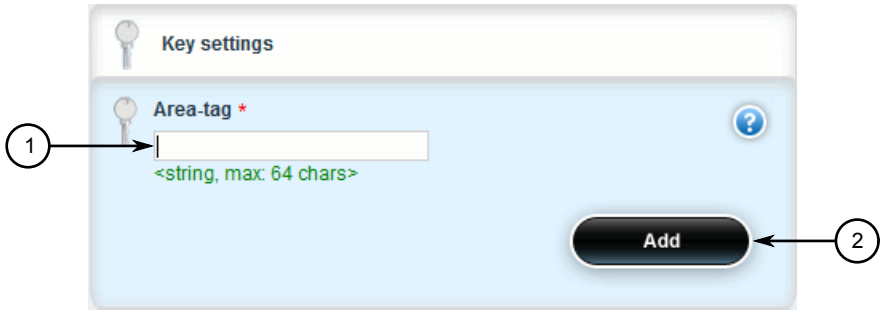


Figure 673: Key Settings Form

1. Area Tag Box **2.** Add Button

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

Parameter	Description
Area Tag	**Synopsis:** 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.

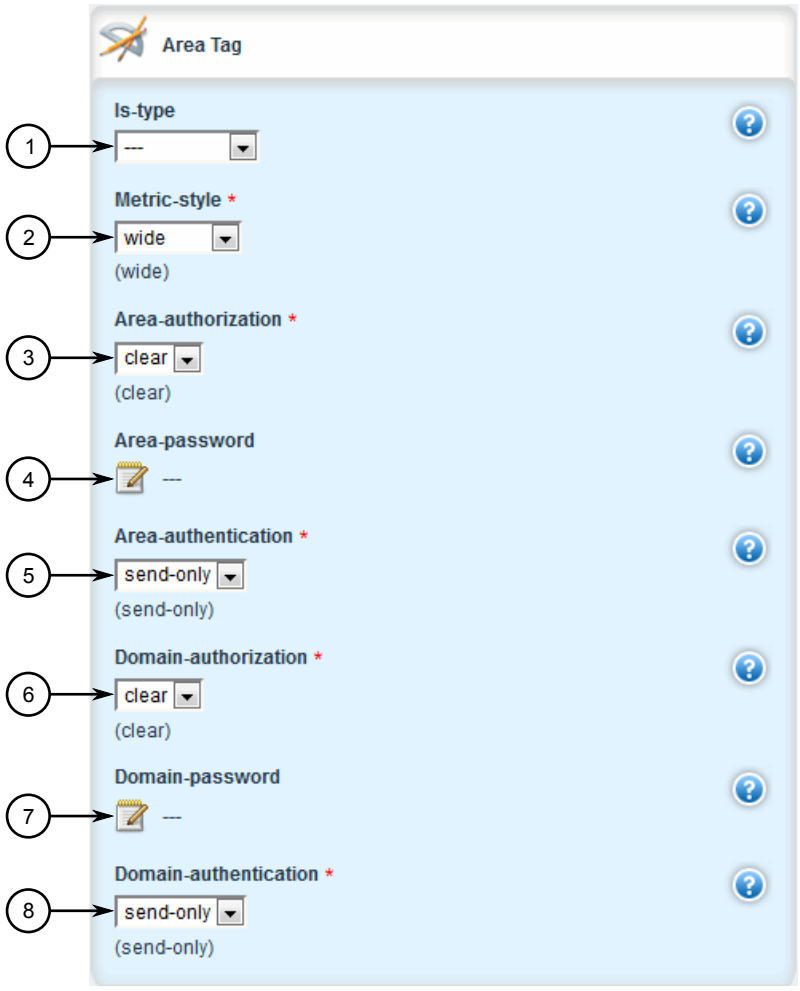


Figure 674: Area Tag Form

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	**Synopsis:** { level-1-only, level-2-only, level-1-2 } The IS type for this area: level-1-only, level-2-only or level-1-2. Level-1 routers have neighbors only on the same area. Level-2-only (backbone) can have neighbors on different areas. Level-1-2 can have neighbors on any areas. Default is level-1-2.
Metric Style	**Synopsis:** { narrow, transition, wide } **Default:** wide The metric style Type Length Value (TLV) for this area: narrow, transition or wide. Default is wide.
Area Authorization	**Synopsis:** { clear, md5 } **Default:** clear The authorization type for the area password. Default is clear.

Parameter	Description
Area Password	**Synopsis:** A string 1 to 254 characters long The area password to be used for transmission of level-1 LSPs.
Area Authentication	**Synopsis:** { send-only, validate } **Default:** send-only The authentication option to be used with the area password on SNP PDUs. Default is send-only.
Domain Authorization	**Synopsis:** { clear, md5 } **Default:** clear The authorization type for the domain password. Default is clear.
Domain Password	**Synopsis:** A string 1 to 254 characters long The domain password to be used for transmission of level-2 LSPs.
Domain Authentication	**Synopsis:** { send-only, validate } **Default:** send-only The authentication option to be used with the domain password on SNP PDUs. Default is send-only.

6. Add one or more Network Entity Titles (NETs). For more information, refer to Section 13.6.11, "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 13.6.7, "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 13.6.10, "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 13.6.8, "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 13.6.9, "Managing the Lifetime of LSPs".
11. If necessary, define rules for redistributing static, RIP, BGP or OSPF routes. For more information, refer to Section 13.6.12, "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 13.6.5.3
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.

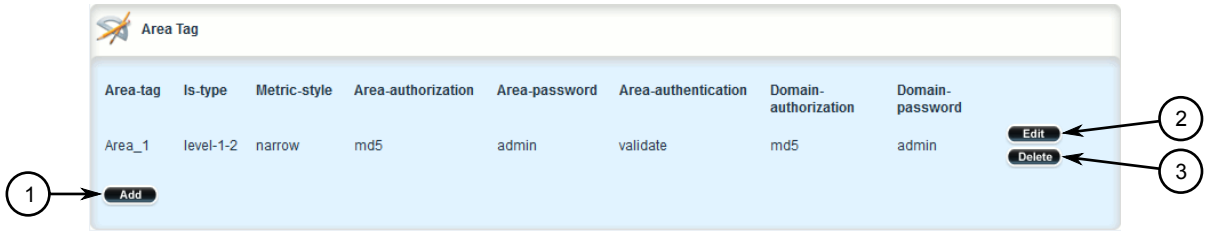


Figure 675: Area Tag Table

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

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 13.6.6

Managing Interfaces

IS-IS transmits hello packets and Link-State Packets (LSPs) through IS-IS enabled interfaces.

NOTE
IS-IS is only supported on Ethernet and WAN (HDLC-ETH) interfaces.

CONTENTS

Section 13.6.6.1

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.

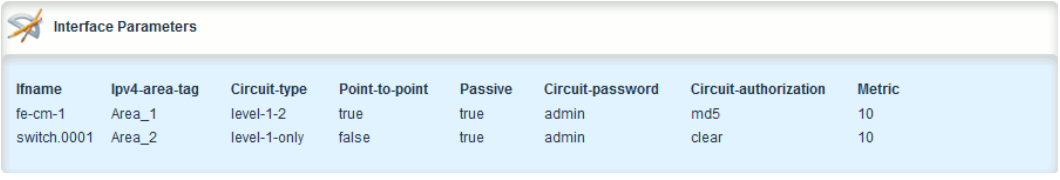


Figure 676: Interface Parameters Table

Interfaces are added automatically when a VLAN is created. For more information about creating a VLAN, refer to Section 8.5, "Managing VLANs".

Section 13.6.6.2
Configuring an Interface

When IS-IS is enabled, two interfaces are already configured: *fe-cm-01* and *switch.0001*.

To configure optional parameters for these and any other interfaces that have been added for IS-IS, do the following:

1. 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.

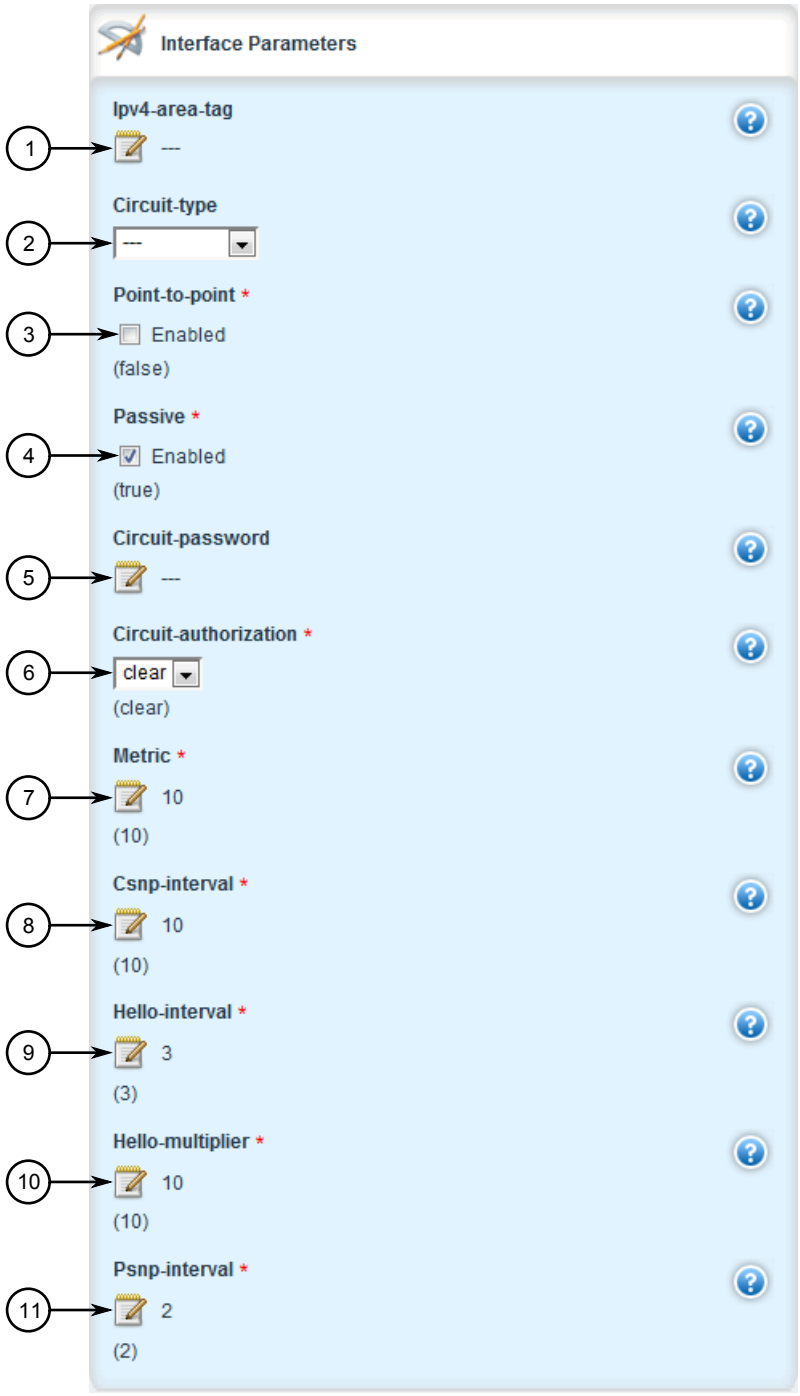


Figure 677: Interface Parameters Form

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
Interface Name	**Synopsis:** A string Interface name.
IPv4 Area Tag	**Synopsis:** A string Name of Area Tag to be used for IS-IS over IPv4.
Circuit Routing Type	**Synopsis:** { level-1-only, level-2-only, level-1-2 } The IS-IS Circuit Type. Level-1 routers have neighbors only on the same area. Level-2 (backbone) can have neighbors on different areas. Level-1-2 can have neighbors on any areas. Default is level-1-2.
Point-to-Point	**Synopsis:** { true, false } **Default:** false Enable or disable point-to-point network communication
passive	**Synopsis:** { true, false } **Default:** true Whether an interface is active or passive. Passive interfaces do not send packets to other routers and are not part of an IS-IS area.
Password	**Synopsis:** A string 1 to 254 characters long The value to be used as a transmit password in IIH PDUs transmitted by this Intermediate System.
Authorization	**Synopsis:** { clear, md5 } **Default:** clear The authorization type ot be associated with the transmit password in IIH PDUs transmitted by this Intermediate System.
Metric	**Synopsis:** A 32-bit signed integer between 1 and 16777214 **Default:** 10 Metric assigned to the link, used to calculate the cost of the route. Value ranges from 1 to 16777214. Default is 10.
CSNP Interval	**Synopsis:** A 16-bit unsigned integer between 1 and 600 **Default:** 10 CSNP interval in seconds, ranging from 1 to 600. Default is 10.
Hello Interval	**Synopsis:** A 16-bit unsigned integer between 1 and 600 **Default:** 3 Hello interval in seconds, ranging from 1 to 600. Default is 3.
Hello Multiplier	**Synopsis:** A 16-bit unsigned integer between 2 and 100 **Default:** 10 Multiplier for Hello holding time. Value ranges from 2 to 100. Default is 10.
PSNP Interface	**Synopsis:** An 8-bit unsigned integer between 1 and 120 **Default:** 2 PSNP interval in seconds, ranging from 1 to 120. Default is 2.

4. 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 13.6.7

Managing LSP Generation

IS-IS generates new Link-State Packets (LSPs) every 30 seconds by default. However, the interval can be configured anywhere between 1 and 120 seconds.

Since the introduction of a new LSP causes other routers in the area to recalculate routes, it is recommended to increase the interval to decrease flooding during periods of network instability, so as to reduce the load on other routers in the area.

CONTENTS

Section 13.6.7.1

Viewing a List of LSP Generation Intervals

To view a list of LSP generation intervals configured for an IS-IS area, 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.

Figure 678: LSP Generic Interval Routing Type Table

If no intervals have been configured, add intervals as needed. For more information, refer to Section 13.6.7.2, "Adding an LSP Generation Interval".

Section 13.6.7.2

Adding an LSP Generation Interval

To add an LSP generation interval to an IS-IS area, do the following:

1. Navigate to ***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.

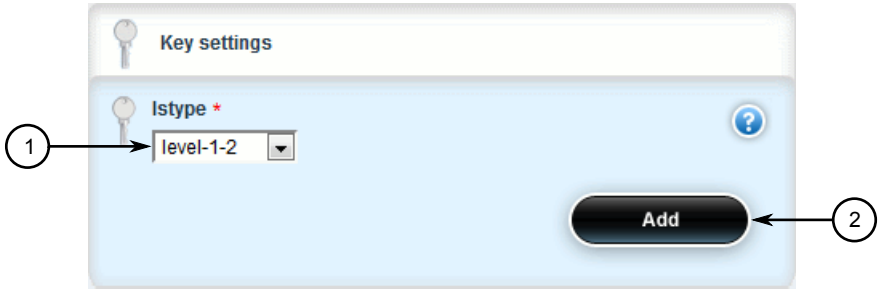


Figure 679: Key Settings Form

1. Routing Type List **2.** Add Button

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

Parameter	Description
Routing Type	**Synopsis:** { 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.

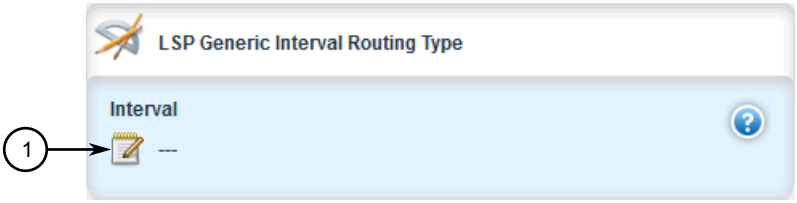


Figure 680: LSP Generic Interval Routing Type Form

1. Interval Box

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

Parameter	Description
Interval	**Synopsis:** An 8-bit unsigned 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 13.6.7.3

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.

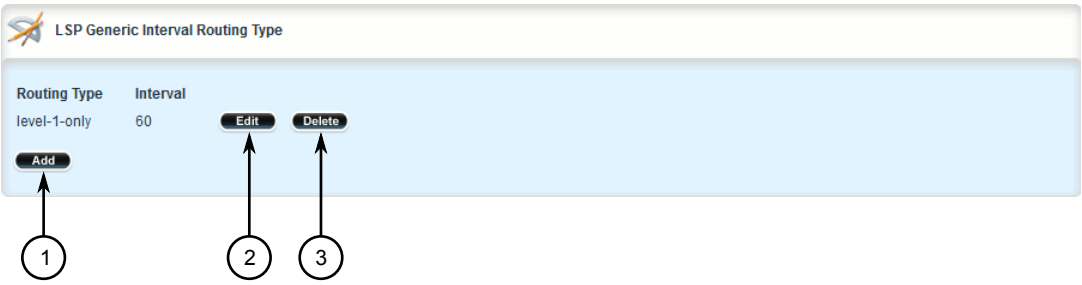


Figure 681: LSP Generic Interval Routing Type

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 13.6.8

Managing SPF Calculations

IS-IS uses the Shortest Path First (SPF) algorithm to determine the best routes to every known destination in the network. When the network topology (not external links) changes, a partial recalculation is required.

IS-IS can be configured to perform the SPF calculation every 1 to 120 seconds. By default, IS-IS performs the SPF calculation every second. which could potentially be processor intensive, depending on the size of the area and how often the topology changes.

CONTENTS

Section 13.6.8.1

Viewing a List of SPF Calculation Intervals

To view a list of SPF calculation intervals configured for an IS-IS area, 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.

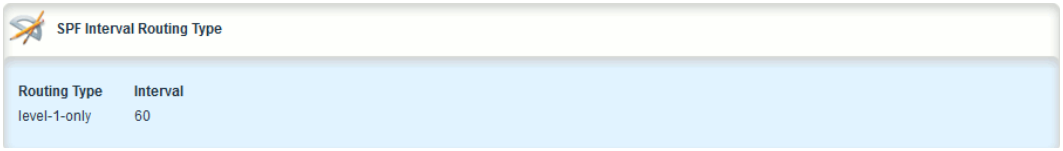


Figure 682: SPF Interval Routing Type

If no intervals have been configured, add intervals as needed. For more information, refer to Section 13.6.8.2, "Adding an SPF Calculation Interval".

Section 13.6.8.2
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.

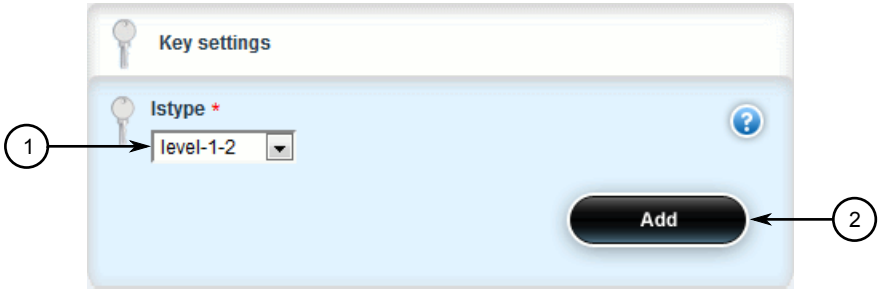


Figure 683: Key Settings Form

1. Routing Type List **2.** Add Button

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

Parameter	Description
Routing Type	**Synopsis:** { 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.

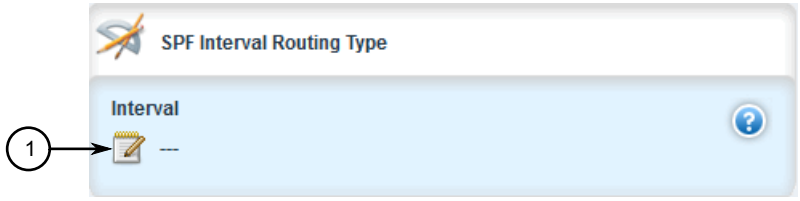


Figure 684: SPF Interval Routing Type Form

1. Interval Box

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

Parameter	Description
Interval	**Synopsis:** An 8-bit unsigned 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 13.6.8.3

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.

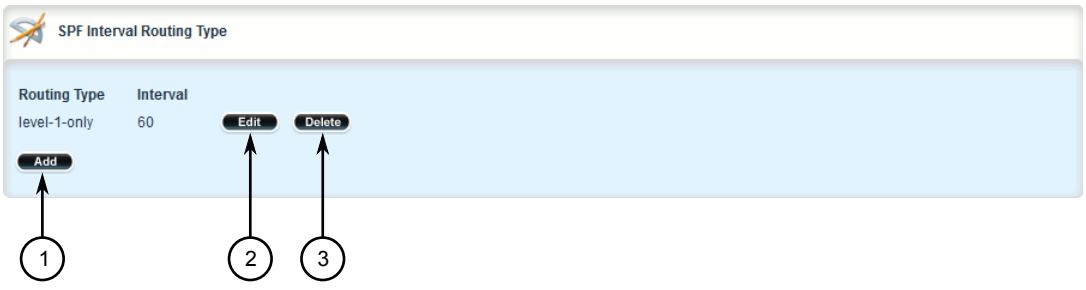


Figure 685: SPF Interval Routing Type

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 13.6.9

Managing the Lifetime of LSPs

IS-IS retains Link-State Packets (LSP) in the Link-State Database (LSDB) for only a short period of time unless they are refreshed. By default, the maximum time limit is 1200 seconds. However, this interval can be customized for different routing types within the range of 350 to 65535 seconds if needed.

Th lifetime interval is configurable for each area and routing type in the IS-IS network.

NOTE
For information about configuring the refresh interval for an LSP, refer to Section 13.6.10, "Managing LSP Refresh Intervals".

CONTENTS

Section 13.6.9.1

Viewing a List of LSP Lifetime Intervals

To view a list of LSP lifetime intervals configured for an IS-IS area, 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.

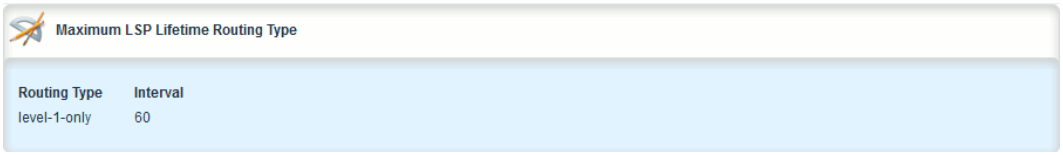


Figure 686: Maximum LSP Lifetime Routing Type

If no intervals have been configured, add intervals as needed. For more information, refer to Section 13.6.9.2, "Adding an LSP Lifetime Interval".

Section 13.6.9.2

Adding an LSP Lifetime Interval

To add an LSP lifetime interval to an IS-IS area, do the following:

IMPORTANT!
The LSP lifetime interval must be 300 seconds higher than the LSP refresh interval. For more information about LSP refresh intervals, refer to Section 13.6.10, "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.

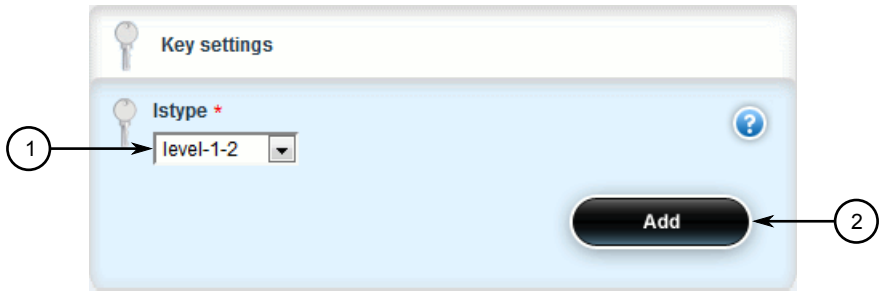


Figure 687: Key Settings Form

1. Routing Type List **2.** Add Button

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

Parameter	Description
Routing Type	**Synopsis:** { 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.

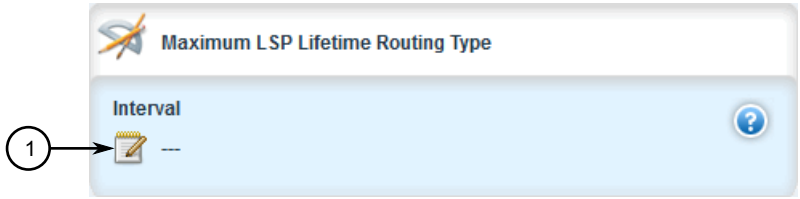


Figure 688: Maximum LSP Lifetime Routing Type Form

1. Interval Box

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

Parameter	Description
Interval	**Synopsis:** A 16-bit unsigned 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 13.6.9.3

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.

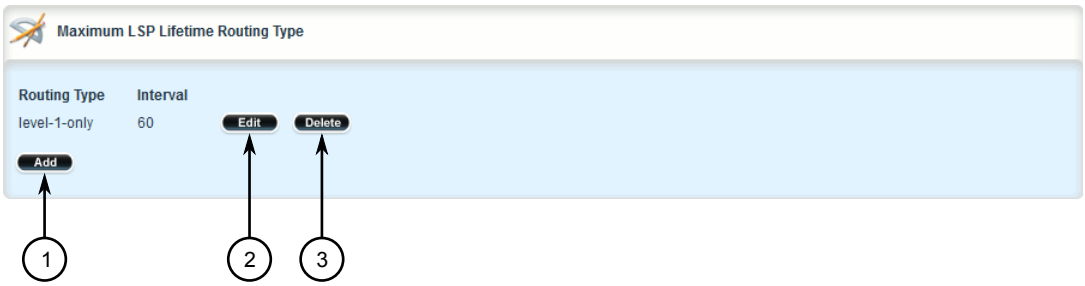


Figure 689: Maximum LSP Lifetime Routing Type

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 13.6.10
Managing LSP Refresh Intervals

IS-IS retains Link-State Packets (LSP) in the Link-State Database (LSDB) for only a short period of time unless they are refreshed. By default, LSPs are retained in the LSDB for 1200 seconds (this is referred to as the *lifetime* of the LSP) and are refreshed every 900 seconds.

The refresh interval is configurable for each area and routing type in the IS-IS network.

NOTE
For information about configuring the lifetime of an LSP, refer to Section 13.6.9, "Managing the Lifetime of LSPs".

CONTENTS

Section 13.6.10.1
Viewing a List of LSP Refresh Intervals

To view a list of LSP refresh intervals configured for an IS-IS area, 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.

Figure 690: LSP Refresh Interval Routing Type

If no intervals have been configured, add intervals as needed. For more information, refer to Section 13.6.10.2, "Adding an LSP Refresh Interval".

Section 13.6.10.2
Adding an LSP Refresh Interval

To add an LSP refresh interval to an IS-IS area, do the following:

IMPORTANT!
The LSP refresh interval must be 300 seconds less than the LSP lifetime interval. For more information about LSP refresh intervals, refer to Section 13.6.9, "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.

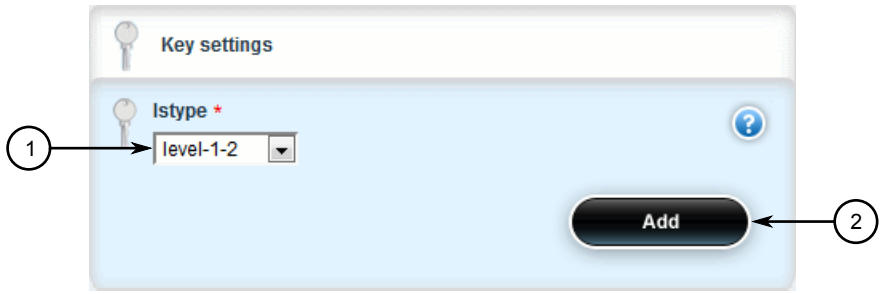


Figure 691: Key Settings Form

1. Routing Type List **2.** Add Button

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

Parameter	Description
Routing Type	**Synopsis:** { 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 Refresh Interval Routing Type** form appears.

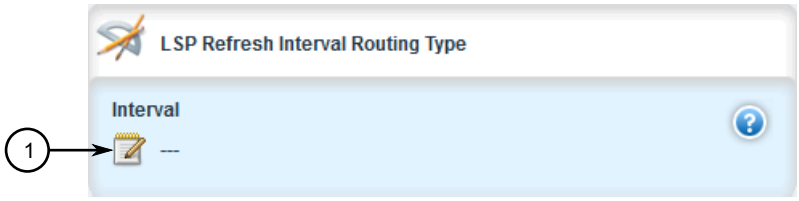


Figure 692: LSP Refresh Interval Routing Type Form

1. Interval Box

5. Configure the following parameter(s) as required:

Parameter	Description
Interval	**Synopsis:** A 16-bit unsigned integer between 1 and 65235 Minimum interval in seconds, ranging from LSP generating interval to Maximum LSP lifetime less 300 seconds. Default is 900.

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 13.6.10.3

Deleting an LSP Refresh Interval

To delete an LSP refresh 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-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.

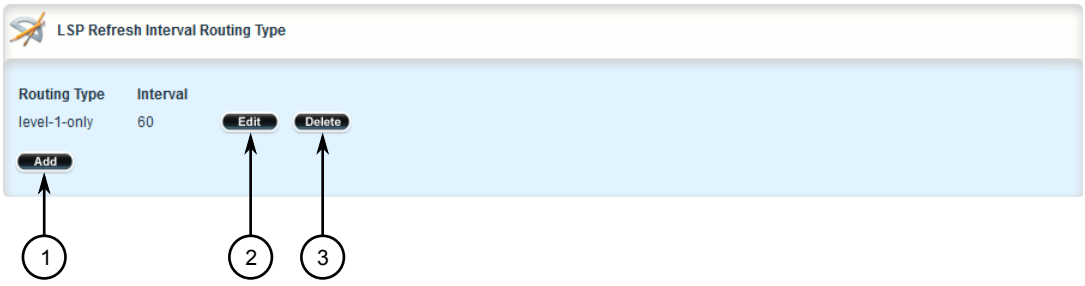


Figure 693: LSP Refresh Interval Routing Type

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 13.6.11

Managing Network Entity Titles (NETs)

Network Entity Titles (NETs) define the area address and system ID for the router. Traffic received from another router that shares the same area address and system ID will be forwarded to this router.

RUGGEDCOM ROX II supports IS-IS multi-homing, which allows for multiple NETs to be defined for a single router and increases the list of possible traffic sources.

Each NET has a hexadecimal value, which can be between 8 and 20 octets long, although 10 octets is most common. The value includes an Authority and Format Identifier (AFI), an area ID, a system identifier, and a selector. The following is an example of an NET address:

```
0001.1921.6800.1001.00
```

- *49* is the AFI. Use *49* for private addressing.
- *0001* is the area ID. In this example, the area is *1*.
- *1921.6800.1001* is the system identifier. Any number can be used, but typically the system identifier is a modified form of the router's IP address. For example, the system identifier in this example translates to *192.168.1.1*. To convert the address in the opposite direction, pad the IP address with zeros (0) and rearrange the decimal points to form to make three two-byte numbers.
- *00* is the selector.

IMPORTANT!
The system identifier must be unique to the network.

CONTENTS

Section 13.6.11.1

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.

Figure 694: Network Entity Title Table

If no NETs have been configured, add NETs as needed. For more information, refer to Section 13.6.11.2, "Adding a NET".

Section 13.6.11.2
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.

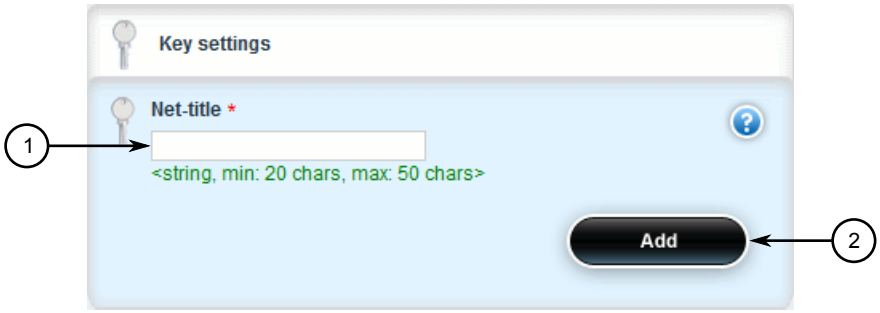


Figure 695: Key Settings Form

1. Net-title Box **2.** Add Button

4. Configure the following parameter(s) as required:

Parameter	Description
Title	**Synopsis:** A string 20 to 50 characters long The Network Entity Title (NET) for the device. The title must consist of an Authority and Format Identifier (AFI), a two-octet area ID, a six-octet system ID and a one-octet selector. For example: 49.0001.1921.68590.1001.00. The selector must be unique to the network.

5. Click **Add** to create the new NET.
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 13.6.11.3
Deleting a NET

To delete 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. The **Network Entity Title** table appears.

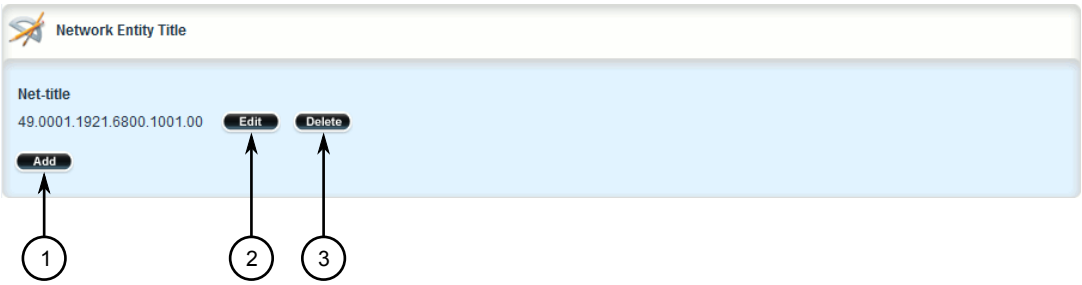


Figure 696: Network Entity Table Form

1. Add Button **2.** Edit Button **3.** Delete Button

3. 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 13.6.12

Managing Redistribution Metrics

Redistribution in general is the advertisement of routes by one protocol that have been learned via another dynamic routing protocol, a static route, or a directly connected router. It is deployed to promote interoperability between networks running different routing protocols.

The redistribution of a route is achieved by defining a metric for the source routing protocol. As each routing protocol calculates routes differently, care must be taken to define a metric that is understood by the protocol.

There are two types of metrics: internal and external. Both types can be assigned a value between 0 and 63. However, to prevent external metrics from competing with internal metrics, 64 is automatically added to any external metric. This puts external metrics in the range of 64 to 128, even though the metric value defined is only in the range of 0 to 63.

There is no default metric for IS-IS. A metric should be defined for each routing protocol, otherwise a metric value of zero (0) is automatically applied.

CONTENTS

Section 13.6.12.1

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.

Figure 697: Redistribute Table

If no redistribution metrics have been configured, add metrics as needed. For more information, refer to Section 13.6.12.2, "Adding a Redistribution Metric".

Section 13.6.12.2
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.

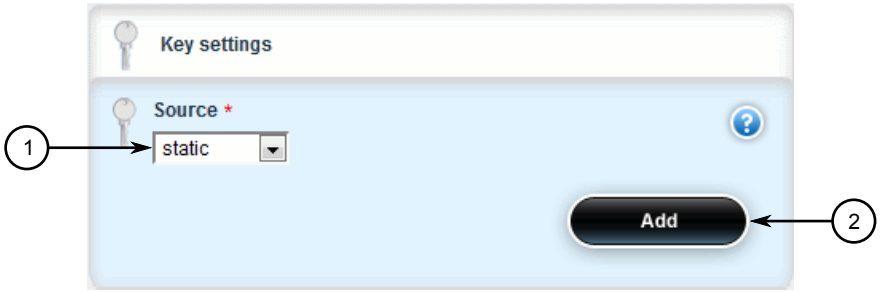


Figure 698: Key Settings Form

1. Source List **2.** Add Button

4. Configure the following parameter(s) as required:

Parameter	Description
Source	**Synopsis:** { 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>

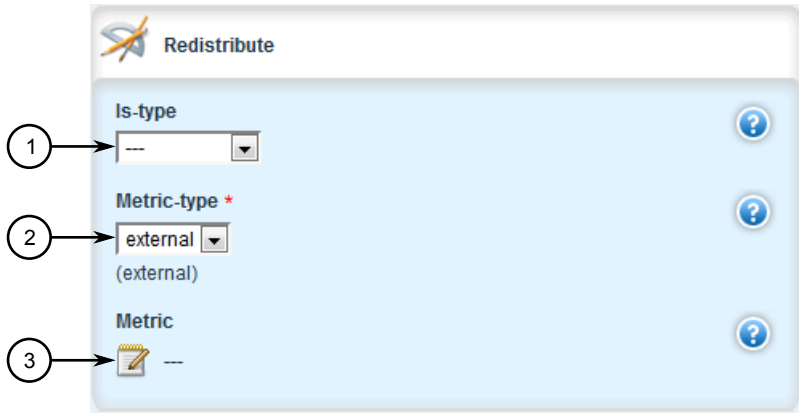


Figure 699: Redistribute Form

1. IS-Type List **2.** Metric-Type List **3.** Metric Box

6. Configure the following parameter(s) as required:

Parameter	Description
Routing Type	**Synopsis:** { level-1-only, level-2-only, level-1-2 } IS type of the IS-IS information, specified as level-1-only, level-2-only or level-1-2. If not provided, uses IS type from area.
Metric Type	**Synopsis:** { internal, external } **Default:** external The IS-IS metric type for redistributed routes. Default is external
Metric	**Synopsis:** A 32-bit unsigned integer between 0 and 16777214 The metric for redistributed routes.

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 13.6.12.3
Deleting a Redistribution Metric

To delete 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. The **Redistribute** table appears.

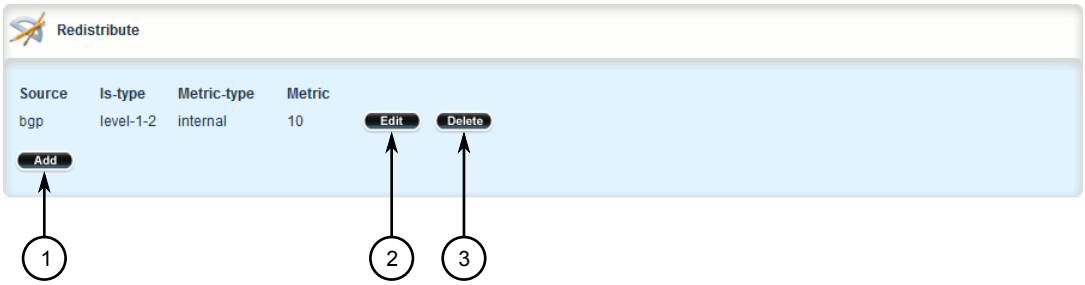


Figure 700: Redistribute Table

1. Add Button **2.** Edit Button **3.** Delete Button

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 13.7

Managing RIP

The Routing Information Protocol (RIP) determines the best path for routing IP traffic over a TCP/IP network based on the number of hops between any two routers. It uses the shortest route available to a given network as the route to use for sending packets to that network.

The RUGGEDCOM ROX II RIP daemon is an RFC 1058 [http://tools.ietf.org/rfc/rfc1058.txt] compliant implementation of RIP that supports RIP version 1 and 2. RIP version 1 is limited to obsolete class-based networks, while RIP version 2 supports subnet masks, as well as simple authentication for controlling which routers to accept route exchanges with.

RIP uses network and neighbor entries to control which routers it will exchange routes with. A network is either a subnet or a physical (broadcast-capable) network interface. Any router that is part of that subnet or connected to that interface may exchange routes. A neighbor is a specific router, specified by its IP address, to exchange routes with. For point to point links (i.e. T1/E1 links), neighbor entries must be used to add other routers to exchange routes with. The maximum number of hops between two points on a RIP network is 15, placing a limit on network size.

Link failures will eventually be noticed when using RIP, although it is not unusual for RIP to take many minutes for a dead route to disappear from the whole network. Large RIP networks could take over an hour to converge when link or route changes occur. For fast convergence and recovery, OSPF is recommended. For more information about OSPF, refer to Section 13.9, “Managing OSPF”.

RIP is a legacy routing protocol that has mostly been superseded by OSPF.

NOTE
In complex legacy networks, RIP, OSPF, BGP and IS-IS may all be active on the same router at the same time. Typically, however, only one dynamic routing protocol is employed at one time.

CONTENTS

Section 13.7.1

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.

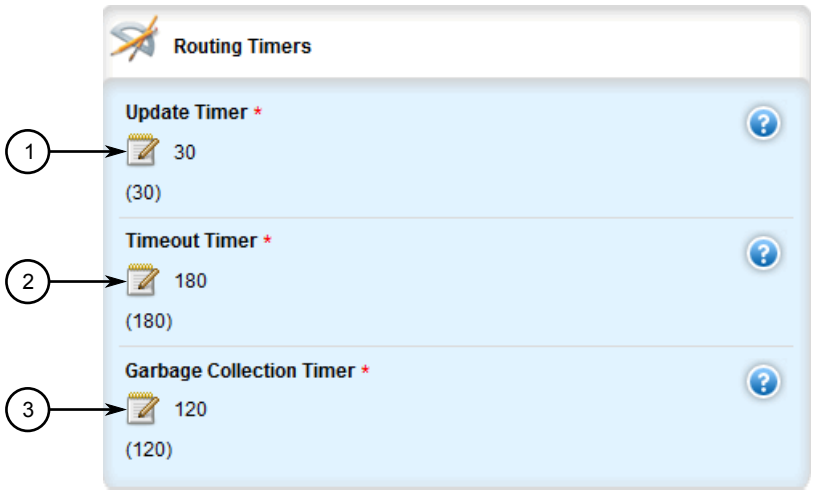


Figure 701: Routing Timers Form

1. Update Timer Box **2.** Timeout Timer Box **3.** Garbage Collection Timer Box

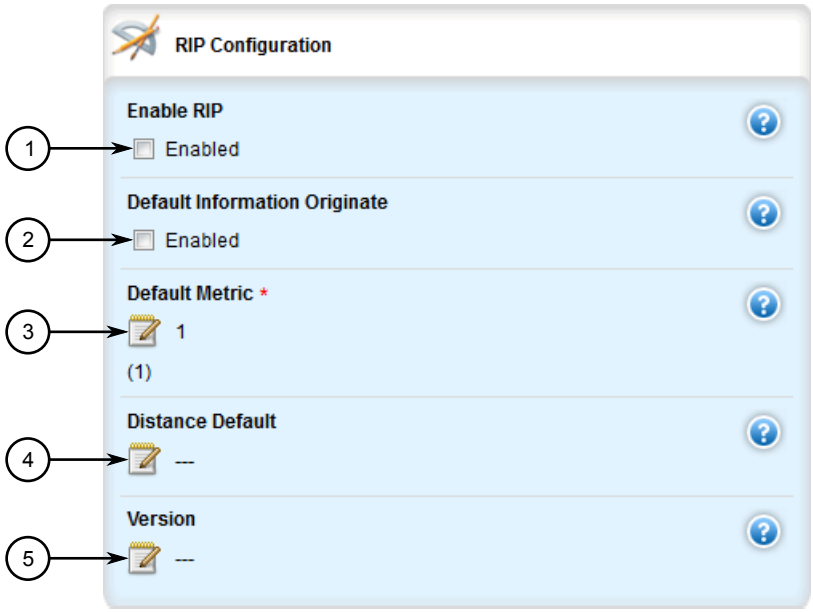


Figure 702: RIP Configuration

1. Enable RIP Check Box **2.** Default Information Originate Check Box **3.** Default Metric Box **4.** Distance Default Box **5.** Version Box

3. In the **Routing Timers** form, configure the following parameters:

Parameter	Description
Update Timer	**Synopsis:** A 32-bit unsigned integer between 5 and 2147483647 **Default:** 30 The routing table update timer (in seconds).
Timeout Timer	**Synopsis:** A 32-bit unsigned integer between 5 and 2147483647 **Default:** 180 The routing information timeout timer (in seconds).
Garbage Collection Timer	**Synopsis:** A 32-bit unsigned integer between 5 and 2147483647 **Default:** 120 The garbage collection timer (in seconds).

4. In the **RIP Configuration** form, configure the following parameters:

Parameter	Description
Enable RIP	Enables the RIP dynamic routing protocol.
Default Information Originate	The route element makes a static route only inside RIP. This element should be used only by advanced users who are particularly knowledgeable about the RIP protocol. In most cases, we recommend creating a static route and redistributing it in RIP using the redistribute element with static type.
Default Metric	**Synopsis:** An 8-bit signed integer between 1 and 16 **Default:** 1 Sets the default metric. With the exception of connected route types, the default metric is advertised when a metric has not been configured for a redistributed route. For connected route types, the default metric is 1 despite the value of this parameter.

Parameter	Description
Distance Default	**Synopsis:** A 32-bit unsigned integer between 1 and 255 Sets the default RIP distance.
Version	**Synopsis:** An 8-bit signed integer between 1 and 2 Set the RIP version to accept for reads and send. The version can be either 1 or 2. Disabling RIPv1 by specifying version 2 is STRONGLY encouraged.

5. Configure prefix lists. For more information, refer to Section 13.7.3.3, "Adding a Prefix List".
6. Configure a network. For more information, refer to Section 13.7.4.1, "Configuring a Network".
7. Configure the prefix list distribution. For more information, refer to Section 13.7.8.2, "Adding a Prefix List Distribution Path".
8. Configure key chains. For more information, refer to Section 13.7.9.3, "Adding a Key Chain".
9. Configure redistribution metrics. For more information, refer to Section 13.7.10.2, "Adding a Redistribution Metric".
10. Configure interfaces. For more information, refer to Section 13.7.11.2, "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 13.7.2
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.

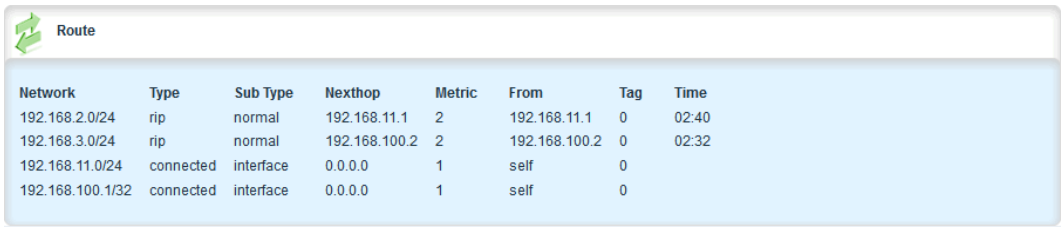


Figure 703: Route Table

The **Route** table provides the following information:

Parameter	Description
Network	**Synopsis:** A string The network.
Type	**Synopsis:** A string The route type.
Sub Type	**Synopsis:** A string The route sub type.

Parameter	Description
Nexthop	**Synopsis:** A string The next hop.
Metric	**Synopsis:** A string The metric value.
From	**Synopsis:** A string Where this route comes from.
Tag	**Synopsis:** A string Tag.
Time	**Synopsis:** A string The route update time.

To view the name of the interface associated with the route, navigate to ***routing » status » rip » interface***. The **Interface** table appears.

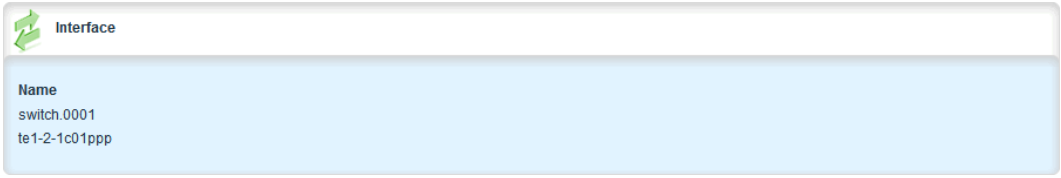


Figure 704: Interface Table

The **Interface** table provides the following information:

Parameter	Description
Interface	**Synopsis:** 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.

Figure 705: Advertised Route Table

The **Advertised Route** table provides the following information:

Parameter	Description
Network	**Synopsis:** A string The network.
Type	**Synopsis:** A string

Parameter	Description
	The route type.
Sub Type	**Synopsis:** A string The route sub type.
Nexthop	**Synopsis:** A string Next hop.
Metric	**Synopsis:** A string The metric value.
From	**Synopsis:** A string Where this route comes from.
Tag	**Synopsis:** A string Tag.
Time	**Synopsis:** A string The route update time.

If no dynamic RIP routes have been configured, configure RIP and add routes as needed. For more information about configuring RIP, refer to Section 13.7.1, "Configuring RIP".

Section 13.7.3
Managing Prefix Lists and Entries

Neighbors can be associated with prefix lists, which allow the RIPs daemon to filter incoming or outgoing routes based on the *allow* and *deny* entries in the prefix list.

CONTENTS

Section 13.7.3.1
Viewing a List of Prefix Lists

To view a list of prefix lists for dynamic RIP routes, navigate to ***routing » dynamic » rip » filter***. If prefix lists have been configured, the **Prefix List** table appears.

Figure 706: Prefix List Table

If no prefix lists have been configured, add lists as needed. For more information, refer to Section 13.7.3.3, "Adding a Prefix List".

Section 13.7.3.2
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.

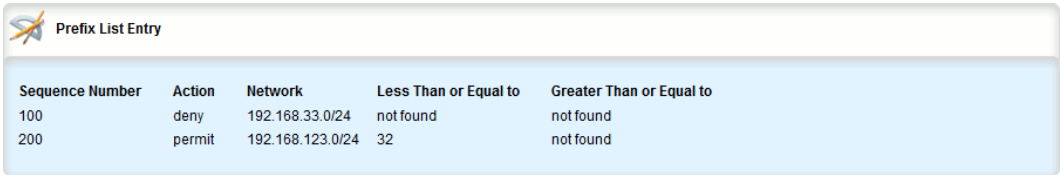


Figure 707: Prefix List Entry Table

If no entries have been configured, add entries as needed. For more information, refer to Section 13.7.3.4, "Adding a Prefix Entry".

Section 13.7.3.3
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.

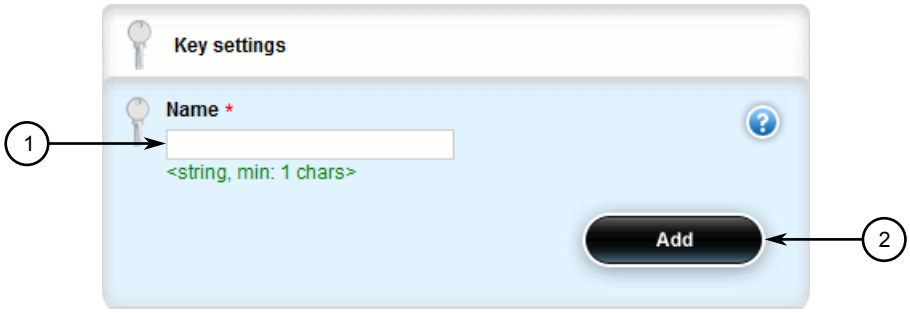


Figure 708: Key Settings Form

1. Name Box **2.** Add Button

3. Configure the following parameter(s) as required:

Parameter	Description
Name	**Synopsis:** 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.

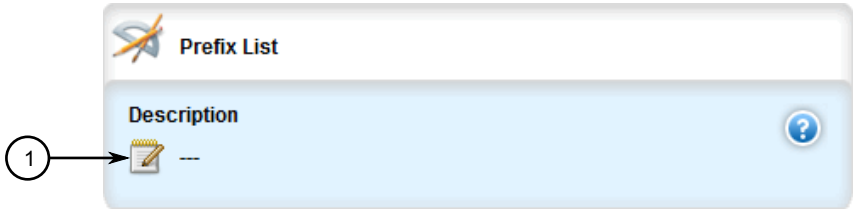


Figure 709: Prefix List Form

1. Description Box

5. Configure the following parameter(s) as required:

Parameter	Description
Description	**Synopsis:** 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 13.7.3.4, "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 13.7.3.4
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.

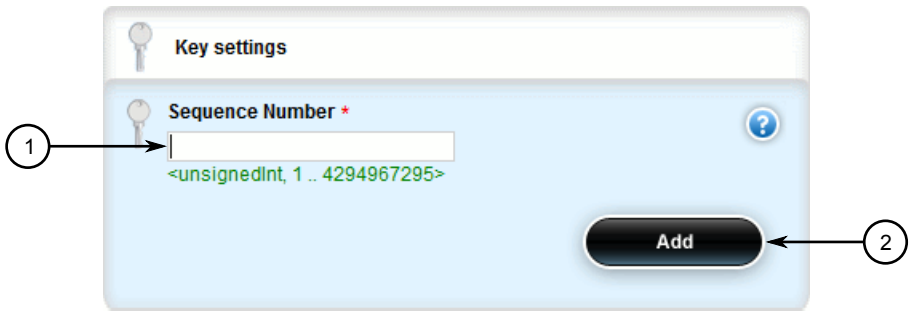


Figure 710: Key Settings Form

1. Sequence Number Box **2.** Add Button

4. Configure the following parameter(s) as required:

Parameter	Description
Sequence Number	**Synopsis:** A 32-bit unsigned 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.

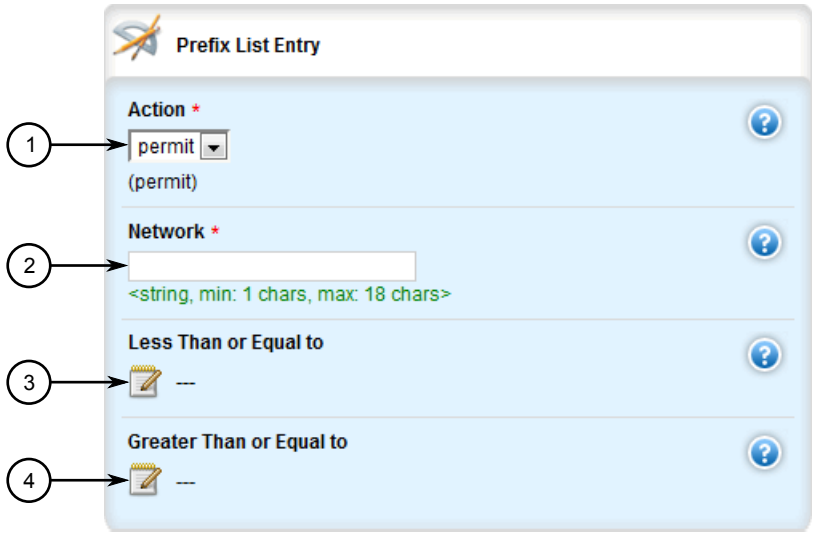


Figure 711: Prefix List Entry Form

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	**Synopsis:** { deny, permit } **Default:** permit The action that will be performed.
Network	**Synopsis:** A string 9 to 18 characters long The IPv4 network address and prefix. This parameter is mandatory.
Less Than or Equal to	**Synopsis:** An 8-bit unsigned integer between 1 and 32 The maximum prefix length to be matched.
Greater Than or Equal to	**Synopsis:** An 8-bit unsigned 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 13.7.3.5
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.

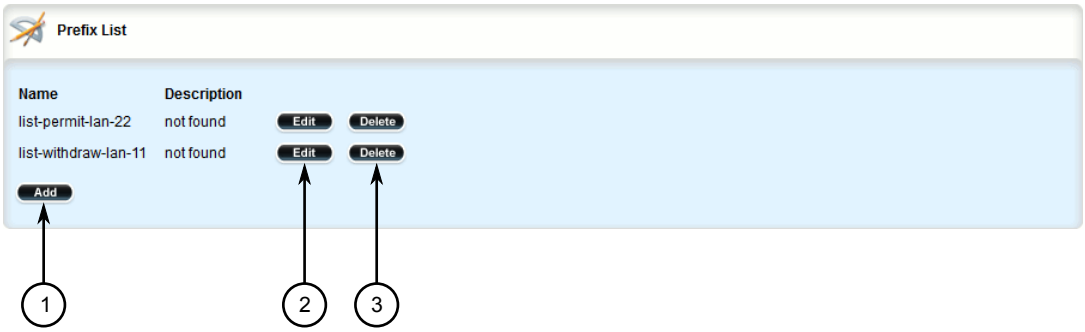


Figure 712: Prefix List Table

1. Add Button **2.** Edit Button **3.** Delete Button

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 13.7.3.6
Deleting a Prefix Entry

To delete 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. The **Prefix List Entry** table appears.

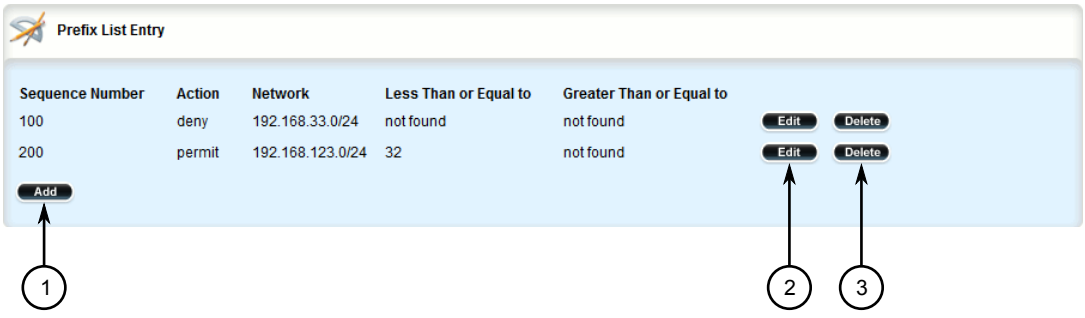


Figure 713: Prefix List Entry Table

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 13.7.4
Managing Networks

As opposed to neighbors, which are specific routers with which to exchange routes, networks are groups of routers that are either part of a specific subnet or connected to a specific network interface. They can be used at the same time as neighbors.

NOTE
For point to point links, such as T1/E1 links, specify neighbors instead of a network. For more information, refer to Section 13.7.7.2, "Adding a Neighbor".

NOTE
RIP v1 does not send subnet mask information in its updates. Any networks defined are restricted to the classic (i.e. Class A, B and C) networks.

NOTE
If neighbors are specified but no networks are specified, the router will receive routing information from its neighbors but will not advertise any routes to them. For more information about neighbors, refer to Section 13.7.7, "Managing Neighbors".

CONTENTS

Section 13.7.4.1
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 13.7.5.2, "Adding a Network IP Address".
3. Add one or more network interfaces. For more information, refer to Section 13.7.6.2, "Adding a Network Interface".
4. Add one or more neighbors. For more information, refer to Section 13.7.7.2, "Adding a Neighbor".

Section 13.7.4.2
Tracking Commands

Network commands can be tracked using event trackers configured under ***global » tracking***. For more information about event trackers, refer to Section 13.5, "Managing Event Trackers".

A network command is activated based on the event tracker's state. The **Apply When** parameter determines when the command is activated. For example, if the **Apply When** parameter is set to **down**, the network command becomes active (thereby advertising the network to a router's RIP peers) when the tracked target is unavailable.

To track a command for a RIP network, do the following:

1. 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 13.7.8, "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

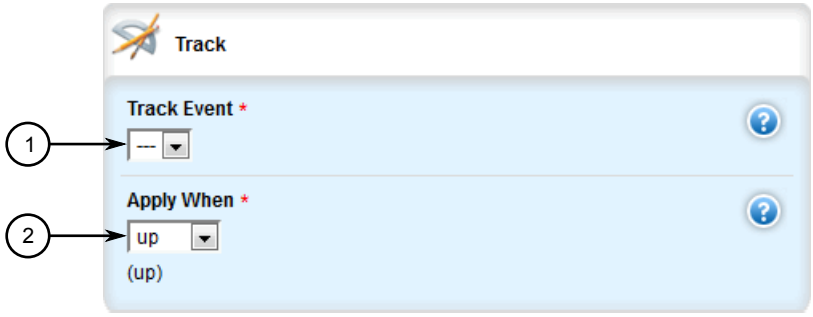


Figure 714: Track Form

1. Track Event List **2.** Apply When List

5. Configure the following parameter(s) as required:

Parameter	Description
Track Event	**Synopsis:** A string Selects an event to track. The distribute-prefix-list is applied only when the tracked event is in the UP state. This parameter is mandatory.
Apply When	**Synopsis:** { up, down } **Default:** 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 13.7.5

Managing Network IP Addresses

This section describes how to manage IP addresses for RIP networks.

CONTENTS

Section 13.7.5.1

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.

Figure 715: Subnet Table

If no IP addresses have been configured, add addresses as needed. For more information, refer to Section 13.7.5.2, "Adding a Network IP Address".

Section 13.7.5.2

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.

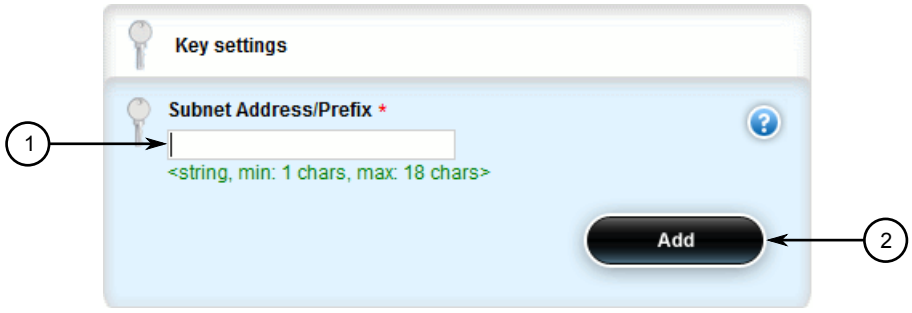


Figure 716: Key Settings Form

1. Subnet Address/Prefix Box **2.** Add Button

3. Configure the following parameter(s) as required:

Parameter	Description
Subnet Address/Prefix	**Synopsis:** A string 9 to 18 characters long The IPv4 network address and prefix.

4. Click **Add** to add the 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 13.7.5.3

Deleting a Network IP Address

To delete an IP address from a RIP network, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to ***routing » dynamic » rip » network » ip***. The **Subnet** table appears.

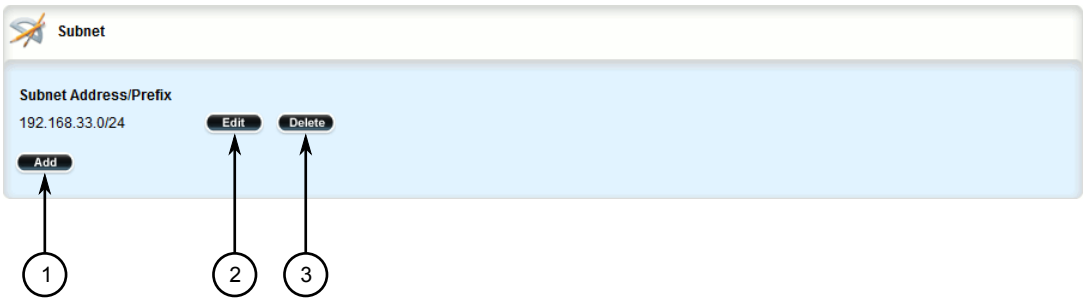


Figure 717: Subnet Table

1. Add Button **2.** Edit Button **3.** Delete Button

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 13.7.6
Managing Network Interfaces

This section describes how to manage interfaces used by RIP networks.

CONTENTS

Section 13.7.6.1
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.

Figure 718: Interface Table

If no interfaces have been configured, add neighbors as needed. For more information, refer to Section 13.7.7.2, "Adding a Neighbor".

Section 13.7.6.2
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.

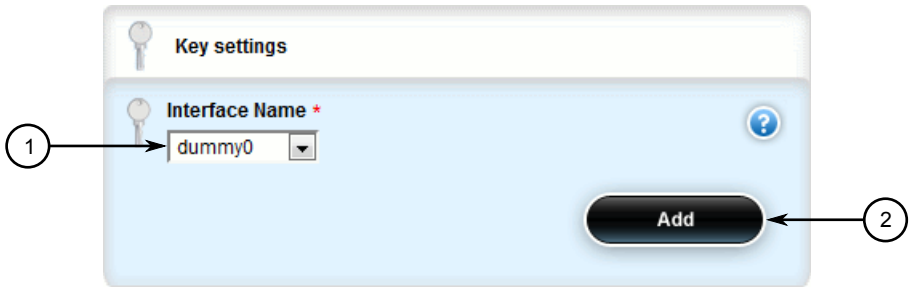


Figure 719: Key Settings Form

1. Interface Name List **2.** Add Button

3. Configure the following parameter(s) as required:

Parameter	Description
Interface Name	**Synopsis:** A string 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 13.7.6.3

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.

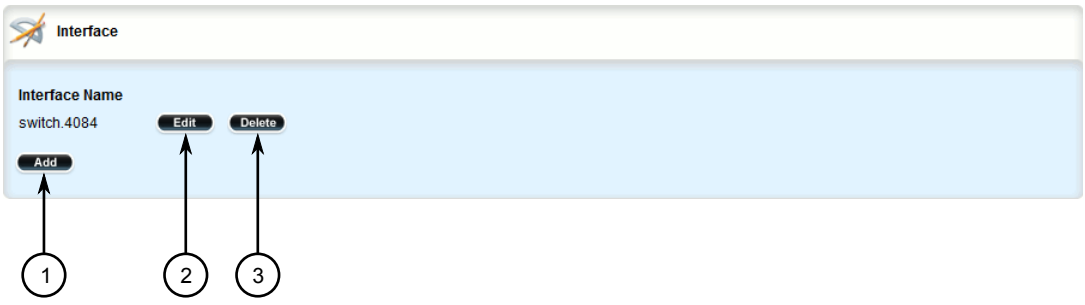


Figure 720: Interface Table

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 13.7.7
Managing Neighbors

Neighbors are other routers with which to exchange routes.

CONTENTS

Section 13.7.7.1
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.

Figure 721: Neighbor Table

If no neighbors have been configured, add neighbors as needed. For more information, refer to Section 13.7.7.2, "Adding a Neighbor".

Section 13.7.7.2
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.

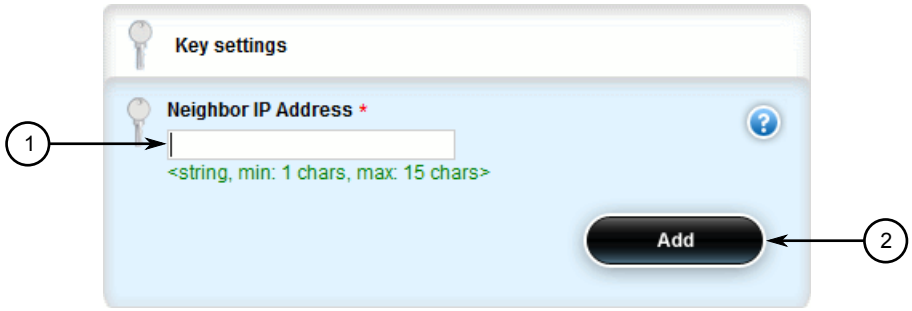


Figure 722: Key Settings Form

1. Neighbor IP Address Box **2.** Add Button

3. Configure the following parameter(s) as required:

Parameter	Description
Neighbor IP Address	**Synopsis:** 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 13.7.7.3

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.

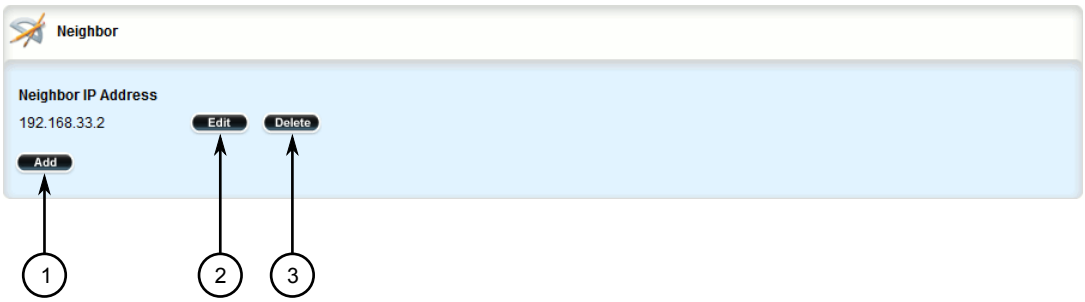


Figure 723: Neighbor Table

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 13.7.8
Managing the Prefix List Distribution

This section describes how to manage the distribution of prefix lists.

CONTENTS

Section 13.7.8.1
Viewing a List of Prefix List Distribution Paths

To view a list of prefix list distribution paths for dynamic RIP routes, navigate to ***routing » dynamic » rip » distribute-prefix-list***. If distribution paths have been configured, the **Distribute Prefix List** table appears.

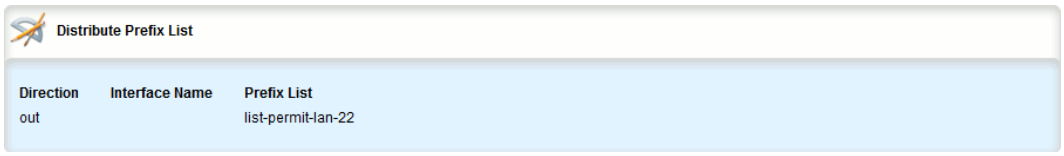


Figure 724: Distribute Prefix List Table

If no prefix list distribution paths have been configured, add distribution paths as needed. For more information, refer to Section 13.7.8.2, "Adding a Prefix List Distribution Path".

Section 13.7.8.2
Adding a Prefix List Distribution Path

To add a prefix list distribution path for dynamic RIP routes, do the following:

1. 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.

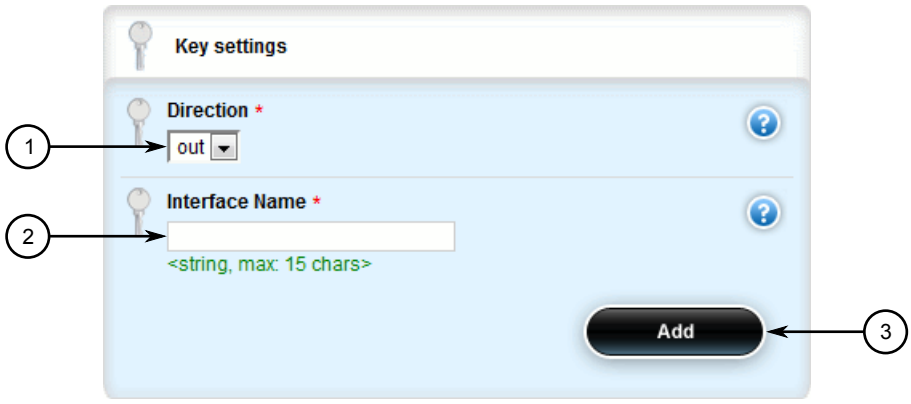


Figure 725: Key Settings Form

1. Direction List **2.** Interface Name Box **3.** Add Button

3. Configure the following parameter(s) as required:

Parameter	Description
Direction	**Synopsis:** { in, out } Filters incoming or outgoing routing updates.
Interface Name	**Synopsis:** 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.

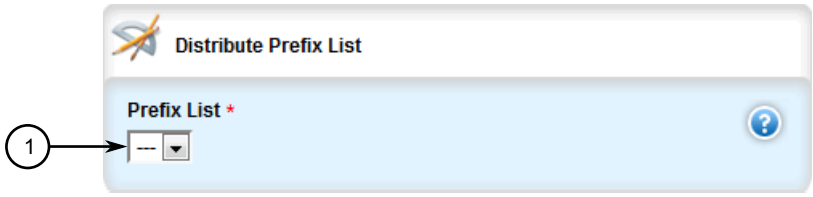


Figure 726: Distribute Prefix List Form

1. Prefix List List

5. Configure the following parameter(s) as required:

Parameter	Description
Prefix List	**Synopsis:** A string The name of the prefix list. This parameter is mandatory.

6. If necessary, configure an event tracker to track network commands. For more information, refer to Section 13.7.4.2, "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 13.7.8.3
Deleting a Prefix List Distribution Path

To delete a prefix list distribution path for dynamic RIP routes, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to ***routing » dynamic » rip » distribute-prefix-list***. The **Distribute Prefix List** table appears.

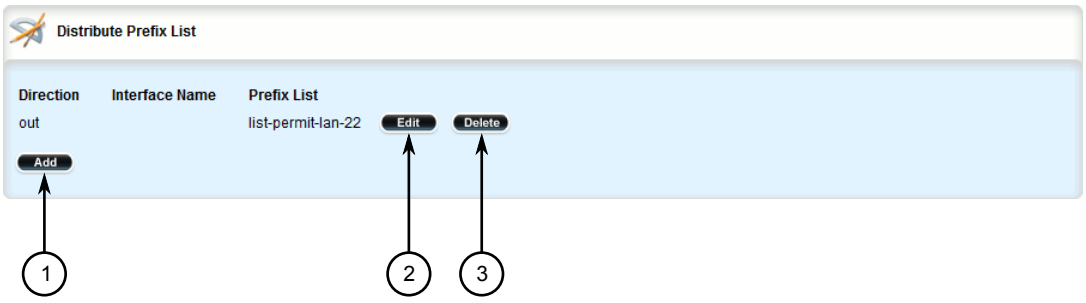


Figure 727: Distribute Prefix List Table

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 13.7.9
Managing Key Chains and Keys

Key chains are collections of keys (or shared secrets), which are used to authenticate communications over a dynamic RIP network. Only routers with the same key are able to send and receive advertisements.

Multiple key chains can be configured for different groups of interfaces and the lifetime for each key within a chain can be separately configured.

CONTENTS

Section 13.7.9.1
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.

Figure 728: Key Chain Management Table

If no key chains have been configured, add key chains as needed. For more information, refer to Section 13.7.9.3, "Adding a Key Chain".

Section 13.7.9.2
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.

Figure 729: Key Configuration Table

If no keys have been configured, add keys as needed. For more information, refer to Section 13.7.9.4, "Adding a Key".

Section 13.7.9.3
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.

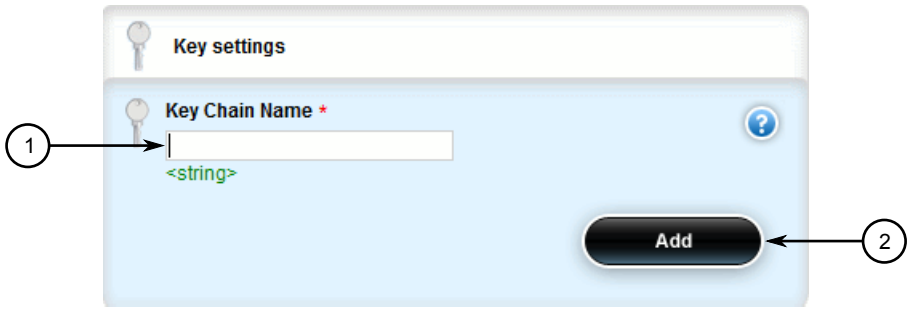


Figure 730: Key Settings Form

1. Key Chain Name Box **2.** Add Button

3. Configure the following parameter(s) as required:

Parameter	Description
Key Chain Name	**Synopsis:** 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 13.7.9.4, "Adding a Key".
6. Configure a routing interface to use the key chain for authentication purposes. For more information, refer to Section 13.7.11.2, "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 13.7.9.4

Adding a Key

Keys (or shared secrets) are used to authenticate communications over a RIP network. To maintain network stability, each key is assigned an accept and send lifetime.

The *accept* lifetime is the time period in which the key is accepted by the device.

The *send* lifetime is the time period in which they key can be sent to other devices.

This is referred to as hitless authentication key rollover, a method for seamlessly updating authentication keys without having to reset network sessions.

To add a key to a key chain, do the following:

1. 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.

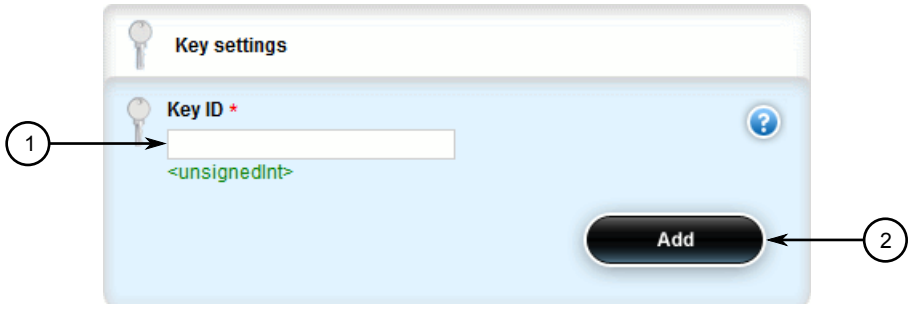


Figure 731: Key Settings Form

1. Key ID Box **2.** Add Button

4. Configure the following parameter(s) as required:

Parameter	Description
Key ID	**Synopsis:** A 32-bit unsigned integer The key identifier number.

5. Click **Add** to add the key chain. The **Key Configuration**, **Accept Life Time** and **Send Life Time** forms appear.

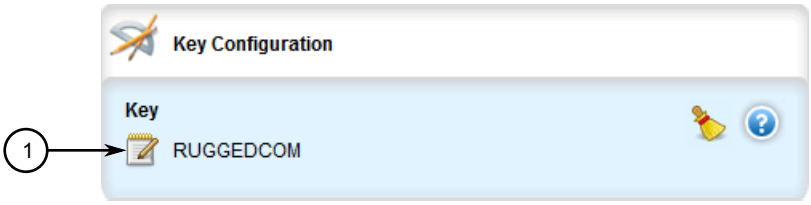


Figure 732: Key Configuration Form

1. Key Box

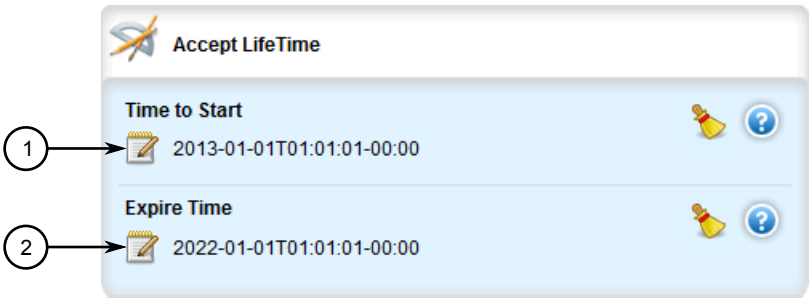


Figure 733: Accept Life Time Form

1. Time to Start Box **2.** Expire Time Box

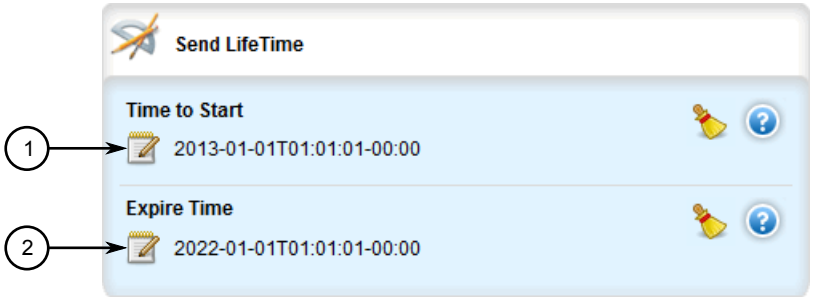


Figure 734: Send Life Time Form

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	**Synopsis:** A string Sets the key string.

7. On the **Accept Life Time** form, configure the following parameter(s) as required:

Parameter	Description
Time to Start	**Synopsis:** A string The beginning time in which the key is considered valid.
Expire Time	**Synopsis:** { infinite } or a string Expire time.

8. On the **Send Life Time** form, configure the following parameter(s) as required:

Parameter	Description
Time to Start	**Synopsis:** A string Sets the time period in which the key on the key chain is considered valid.
Expire Time	**Synopsis:** { infinite } or a string The time at which the key expires.

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 13.7.9.5

Deleting a Key Chain

To delete 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***. The **Key Chain Management** table appears.

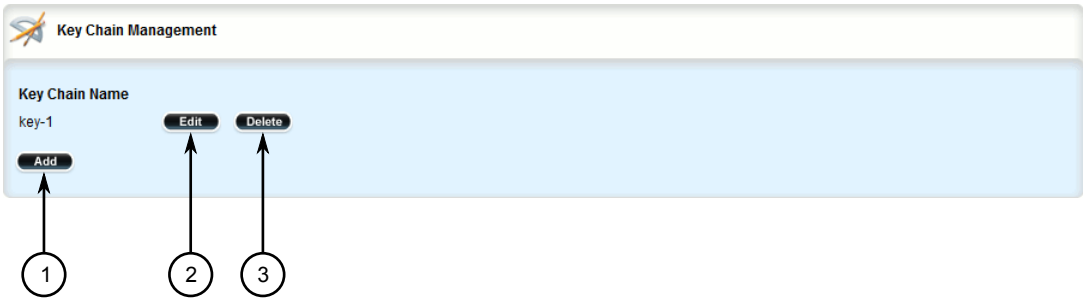


Figure 735: Key Chain Management Table

1. Add Button **2.** Edit Button **3.** Delete Button

3. Click **Delete** next to the chosen key chain.
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 13.7.9.6

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.

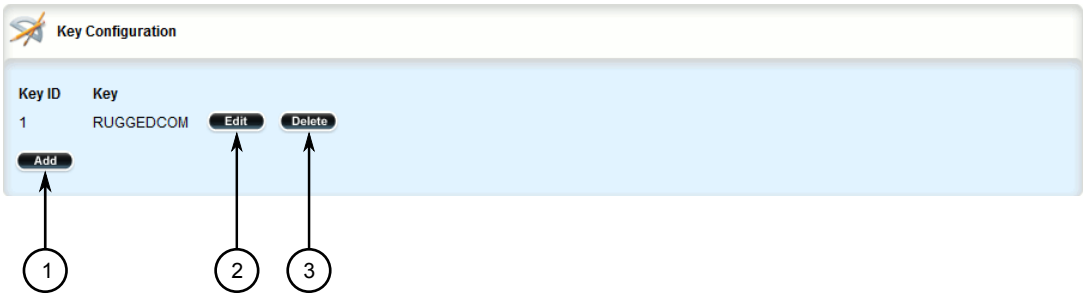


Figure 736: Key Configuration Table

1. Add Button **2.** Edit Button **3.** Delete Button

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 13.7.10

Managing Redistribution Metrics

Redistribution metrics redistribute routing information from other routing protocols, static routes or routes handled by the kernel. Routes for subnets that are directly connected to the router, but not part of the RIP networks, can also be advertised.

CONTENTS

Section 13.7.10.1

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.

Figure 737: Redistribute Route from Other Protocols Table

If no redistribution metrics have been configured, add metrics as needed. For more information, refer to Section 13.7.10.2, "Adding a Redistribution Metric".

Section 13.7.10.2

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.

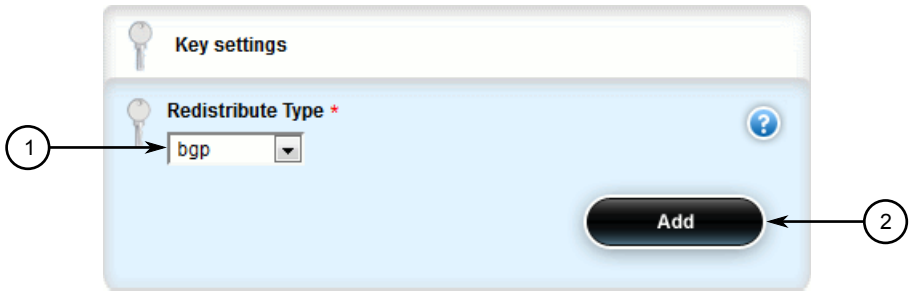


Figure 738: Key Settings Form

1. Redistribute Type List **2.** Add Button

3. Configure the following parameter(s) as required:

Parameter	Description
Redistribute Type	**Synopsis:** { kernel, static, connected, ospf, bgp } Redistribute route type.
Metric	**Synopsis:** An 8-bit signed integer between 0 and 16 The metric for redistributed routes.

4. Click **Add** to add the metric. The **Redistribute Route from Other Protocols** form appears.

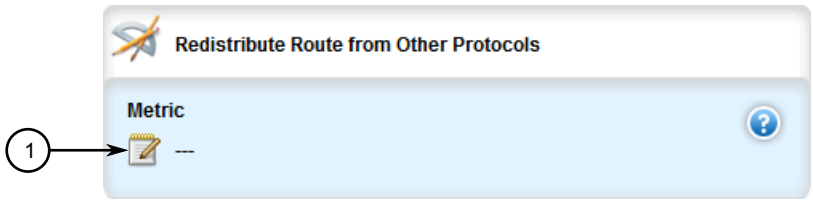


Figure 739: Redistribute Route from Other Protocols Form

1. Metric Box

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 13.7.10.3

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.

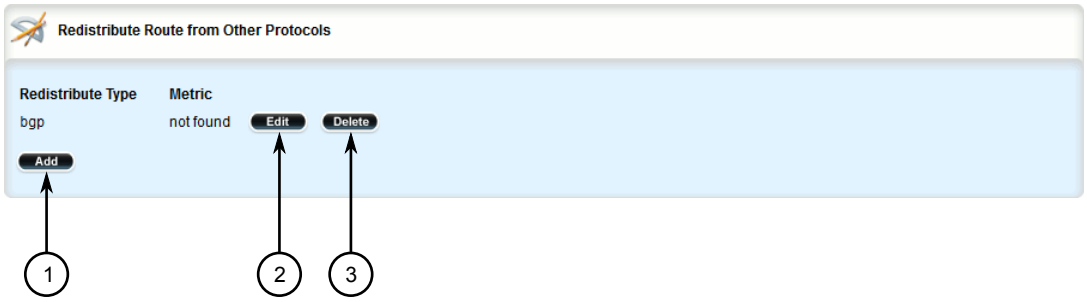


Figure 740: Redistribute Route from Other Protocols Table

1. Add Button **2.** Edit Button **3.** Delete Button

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 13.7.11

Managing Routing Interfaces

This section describes how to manage interfaces for RIP routes.

CONTENTS

Section 13.7.11.1

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.

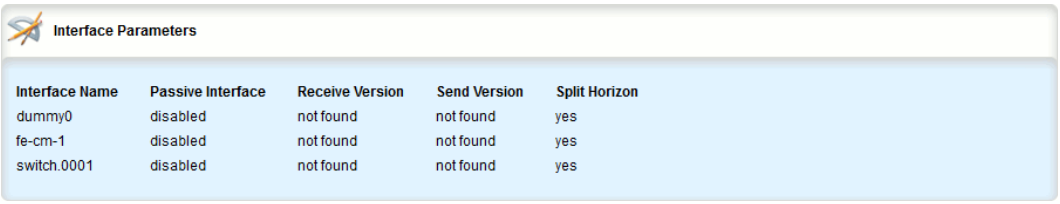


Figure 741: Interface Parameters Table

Section 13.7.11.2
Configuring a Routing Interface

To configure a routing interface for a RIP network, do the following:

NOTE
OSPF regards router interfaces as either passive or active, sending OSPF messages on active interfaces and ignoring passive interfaces.

1. 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.

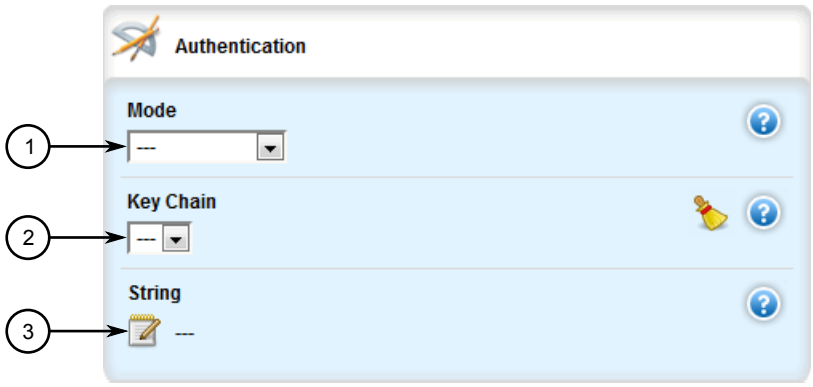


Figure 742: Authentication Form

1. Mode List **2.** Key Chain List **3.** String Box

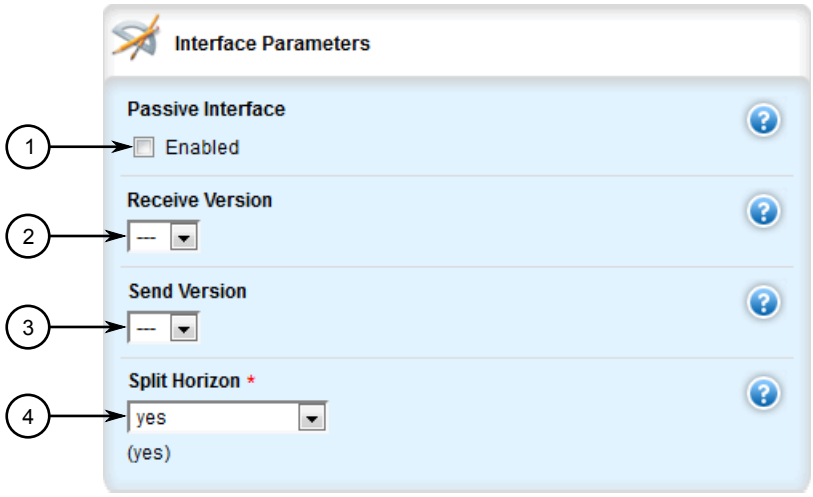


Figure 743: Interface Parameters Form

1. Passive Interface Check Box **2.** Receive Version List **3.** Send Version List **4.** Split Horizon List

3. On the **Authentication** form, configure the following parameter(s) as required:

Parameter	Description
Mode	**Synopsis:** { md5-rfc, md5-old-ripd, text, none } The authentication mode.
Key Chain	**Synopsis:** A string The authentication key chain.
String	**Synopsis:** A string 1 to 16 characters long The authentication string.

4. On the **Interface Parameters** form, configure the following parameter(s) as required:

Parameter	Description
Interface Name	**Synopsis:** A string 1 to 32 characters long The name of the interface.
Passive Interface	The specified interface is set to passive mode. In passive mode, all received packets are processed normally and RIPd sends neither multicast nor unicast RIP packets except to RIP neighbors specified with a neighbor element.
Receive Version	**Synopsis:** { 1, 2, 1,2, 2,1 } The version of RIP packets that will be accepted on this interface. By default, version 1 and version 2 packets will be accepted.
Send Version	**Synopsis:** { 1, 2, 1,2, 2,1 } The version of RIP to send packets with. By default, version 2 packets will be sent.
Split Horizon	**Synopsis:** { yes, no, poisoned-reverse } **Default:** yes A split horizon.
Mode	**Synopsis:** { md5-rfc, md5-old-ripd, text, none } The authentication mode.
Key Chain	**Synopsis:** A string The authentication key chain.
String	**Synopsis:** A string 1 to 16 characters long The authentication string.

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 13.8
Managing BGP

The Border Gateway Protocol (BGP) as defined by RFC 4271 [http://tools.ietf.org/rfc/rfc4271.txt] is a robust and scalable routing protocol. BGP is designed to manage a routing table of up to 90000 routes. Therefore, it is used in large networks or among groups of networks which have common administrative and routing policies. External BGP (eBGP) is used to exchange routes between different Autonomous Systems (AS). Interior BGP (iBGP) is used to exchange routes within autonomous system (AS).

BGP is used by the bgpd daemon to handle communications with other routers. The daemon also determines which routers it prefers to forward traffic to for each known network route.

NOTE
In complex legacy networks, RIP, OSPF, BGP and IS-IS may all be active on the same router at the same time. Typically, however, only one dynamic routing protocol is employed at one time.

CONTENTS

Section 13.8.1

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.

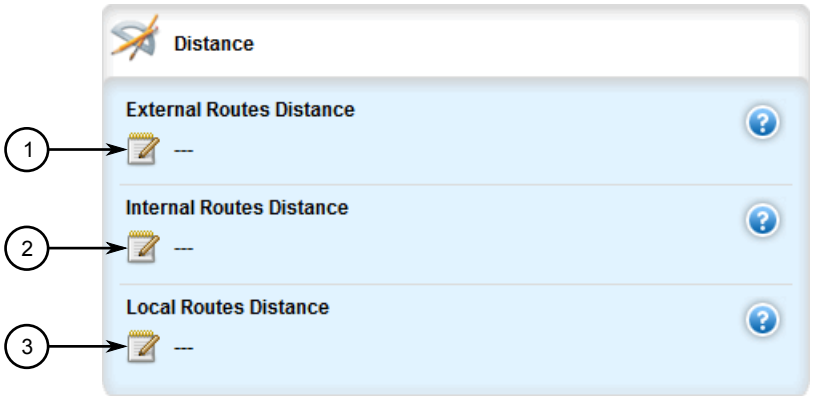


Figure 744: Distance Form

1. External Routes Distance Box **2.** Internal Routes Distance Box **3.** Local Routes Distance Box

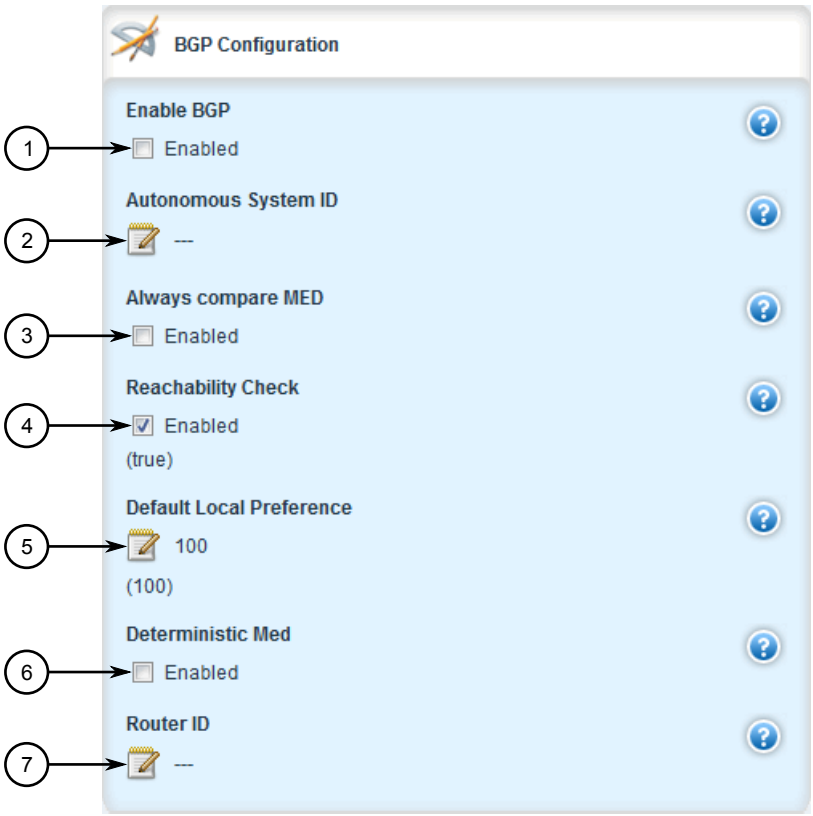


Figure 745: BGP Configuration

1. Enable BGP Check Box **2.** Autonomous System ID Box **3.** Always Compare MED Check Box **4.** Reachability Check Check Box **5.** Default Local Preference Box **6.** Deterministic MED Check Box **7.** Router ID Box

3. In the **Distance** form, configure the following parameters:

Parameter	Description
External Routes Distance	**Synopsis:** A 32-bit unsigned integer between 1 and 255 Distance value for external routes.
Internal Routes Distance	**Synopsis:** A 32-bit unsigned integer between 1 and 255 Distance value for internal routes.
Local Routes Distance	**Synopsis:** A 32-bit unsigned integer between 1 and 255 Distance value for local routes.

4. In the **BGP Configuration** form, configure the following parameters:

Parameter	Description
Enable BGP	Enables BGP.
Autonomous System ID	**Synopsis:** A 32-bit unsigned integer between 1 and 65535 Autonomous System ID.
Always compare MED	Always comparing MED from different neighbors.
Reachability Check	**Synopsis:** { true, false } **Default:** true Enables or disables the reachability check for advertised routes. When enabled, before advertising a self-generated BGP route to other BGP peers, the BGP daemon checks if the advertised route is reachable locally by default before advertising it to other BGP peers. The route is only advertised if it exists in the kernel routing table.
Default Local Preference	**Synopsis:** A 32-bit unsigned integer **Default:** 100 Default local preference value.
Deterministic Med	Pick the best-MED path among paths advertised from neighboring AS.
Router ID	**Synopsis:** A string 7 to 15 characters long Router ID for BGP.

5. Configure autonomous system path filters. For more information, refer to Section 13.8.5.3, "Adding an Autonomous System Path Filter".
6. Configure prefix list filters. For more information, refer to Section 13.8.4.3, "Adding a Prefix List".
7. Configure route map filters. For more information, refer to Section 13.8.2.3, "Adding a Route Map Filter".
8. Configure a network. For more information, refer to Section 13.8.7.2, "Adding a Network".
9. Configure IP addresses for neighbors. For more information, refer to Section 13.8.6.2, "Adding a Neighbor".
10. Configure aggregate addresses. For more information, refer to Section 13.8.8.2, "Adding an Aggregate Address".
11. Configure redistribution metrics. For more information, refer to Section 13.8.10.2, "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.

NOTE
Following a change in the routing policy due to a configuration change, the BGP session must be reset for the new policy to take effect.

14. Reset the BGP session. For more information, refer to Section 13.8.13, "Resetting a BGP Session".

Section 13.8.2
Managing Route Maps

Route maps are sequential statements used to filter routes that meet the defined criteria. If a route meets the criteria of the applied route map, it can either be excluded from the routing table or prevented from being redistributed.

Each route map requires a sequence number (e.g. 10, 20, 30, etc.), which allows for multiple route maps to be run in sequence until a match is found. It is recommended to create sequence numbers in intervals of 10, in case a new route map is required later between two existing route maps.

CONTENTS

Section 13.8.2.1
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.

Figure 746: Route Map Table

If no filters have been configured, add filters as needed. For more information, refer to Section 13.8.5.3, "Adding an Autonomous System Path Filter".

Section 13.8.2.2
Viewing a List of Route Map Filter Entries

To view a list of entries for a route map filter for either BGP, 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.

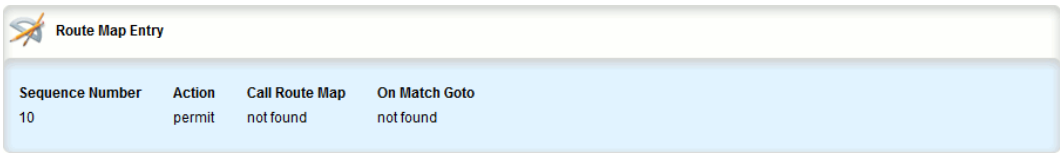


Figure 747: Route Map Entry Table

If no filters have been configured, add filters as needed. For more information, refer to Section 13.8.5.3, "Adding an Autonomous System Path Filter".

Section 13.8.2.3
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.

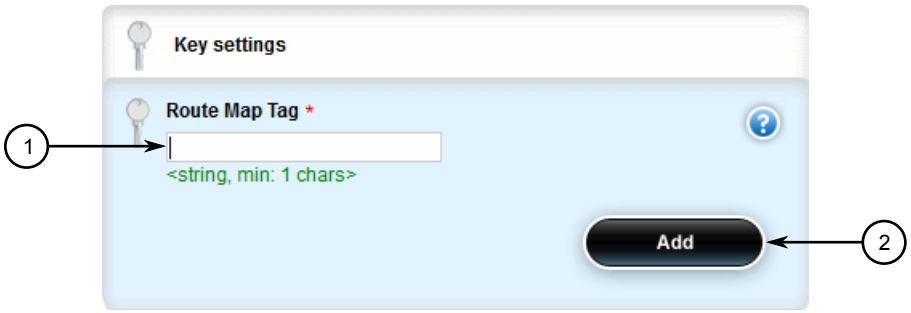


Figure 748: Key Settings Form

1. Route Map Tag Box **2.** Add Button

3. Configure the following parameter(s) as required:

Parameter	Description
Route Map Tag	**Synopsis:** 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 13.8.2.4, "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 13.8.2.4
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.

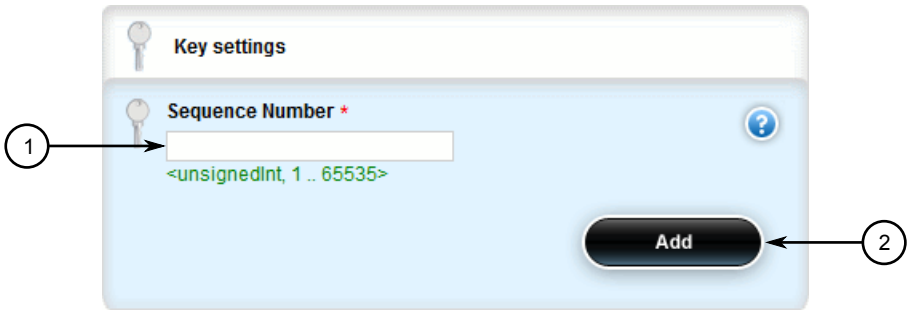


Figure 749: Key Settings Form

1. Sequence Number Box **2.** Add Button

4. Configure the following parameter(s) as required:

Parameter	Description
Sequence Number	**Synopsis:** A 32-bit unsigned 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.

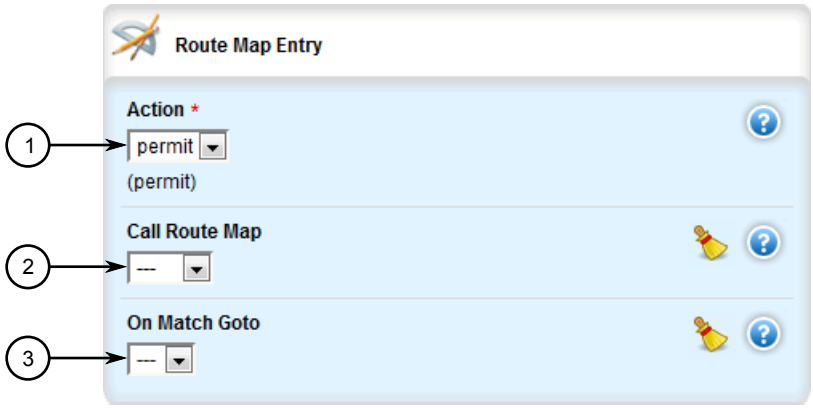


Figure 750: Route Map Entry Form

1. Action List **2.** Call Route Map List **3.** On Match Goto List

6. Configure the following parameter(s) as required:

Parameter	Description
Action	**Synopsis:** { deny, permit } **Default:** permit Action.
Call Route Map	**Synopsis:** A string Jump to another route-map after match+set.
On Match Goto	**Synopsis:** A string Go to this entry on match.

7. Configure the match rules for the route map filter. For more information, refer to Section 13.8.2.7, "Configuring Match Rules".
8. Configure a set for the route map filter. For more information, refer to Section 13.8.2.8, "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 13.8.2.5
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.

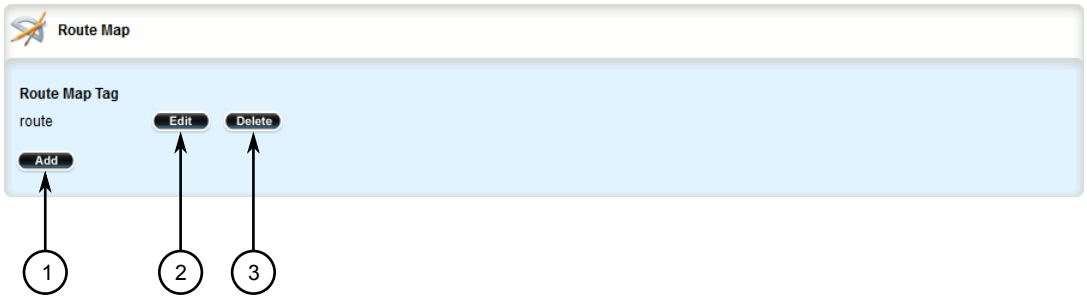


Figure 751: Route Map Table

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 13.8.2.6

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.

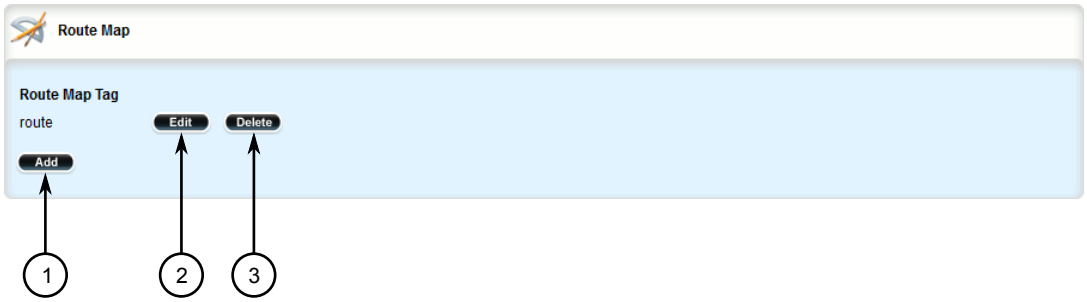


Figure 752: Route Map Entry Table

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 13.8.2.7
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.

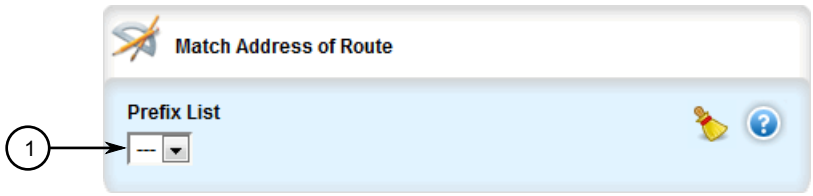


Figure 753: Match Address of Route Form

1. Prefix List List

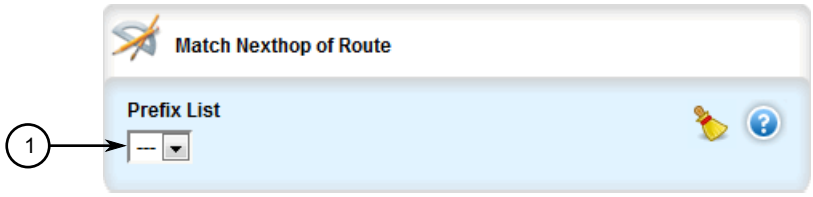


Figure 754: Match Nexthop of Route Form

1. Prefix List List

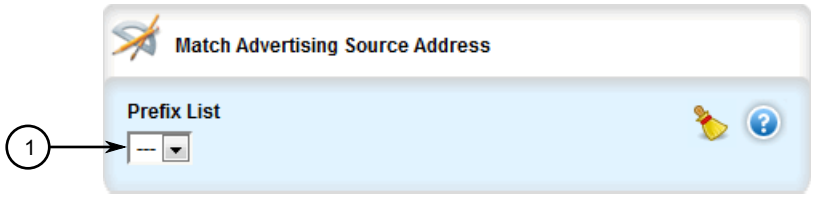


Figure 755: Match Advertising Source Address Form

1. Prefix List List

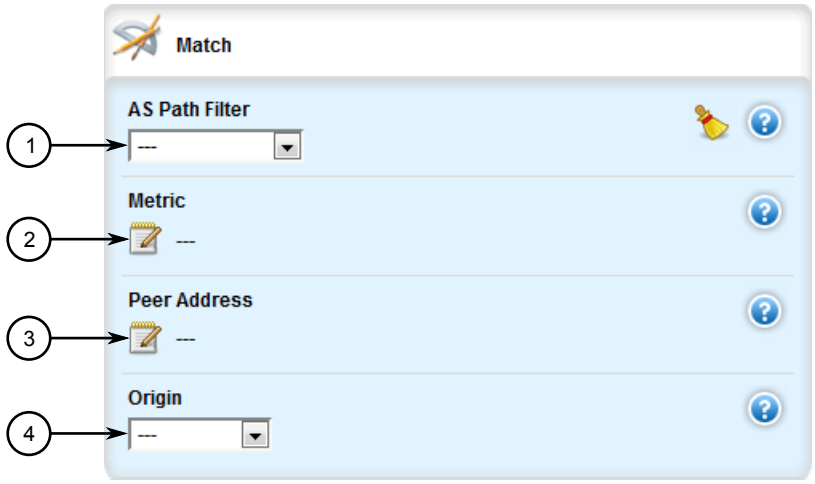


Figure 756: Match Form

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	**Synopsis:** A string The prefix list name.

4. On the **Match Nexthop of Route** form, configure the following parameters as required:

Parameter	Description
Prefix List	**Synopsis:** A string The prefix list name.

5. On the **Match Advertising Source Address** form, configure the following parameters as required:

Parameter	Description
Prefix List	**Synopsis:** A string The prefix list name.

6. On the **Match** form, configure the following parameters as required:

Parameter	Description
AS Path Filter	**Synopsis:** A string Match the BGP AS path filter.
Metric	**Synopsis:** A 32-bit unsigned integer Match the route metric.
Peer Address	**Synopsis:** A string 7 to 15 characters long This parameter is not supported and any value is ignored by the system.s
Origin	**Synopsis:** { egp, igp, incomplete }

Parameter	Description
	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 13.8.2.8
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.

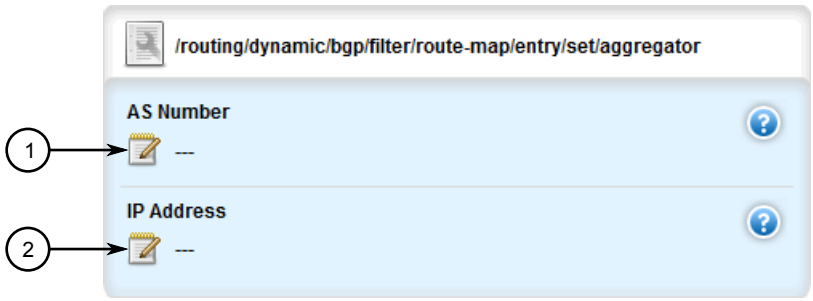


Figure 757: Aggregator Form

1. AS Number Box **2.** IP Address Box

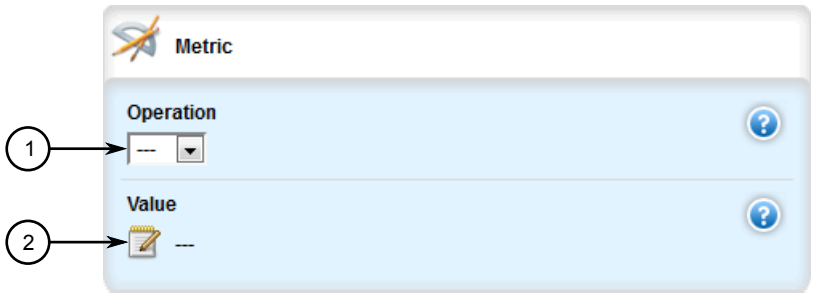


Figure 758: Metric Form

1. Operation List **2.** Value Box

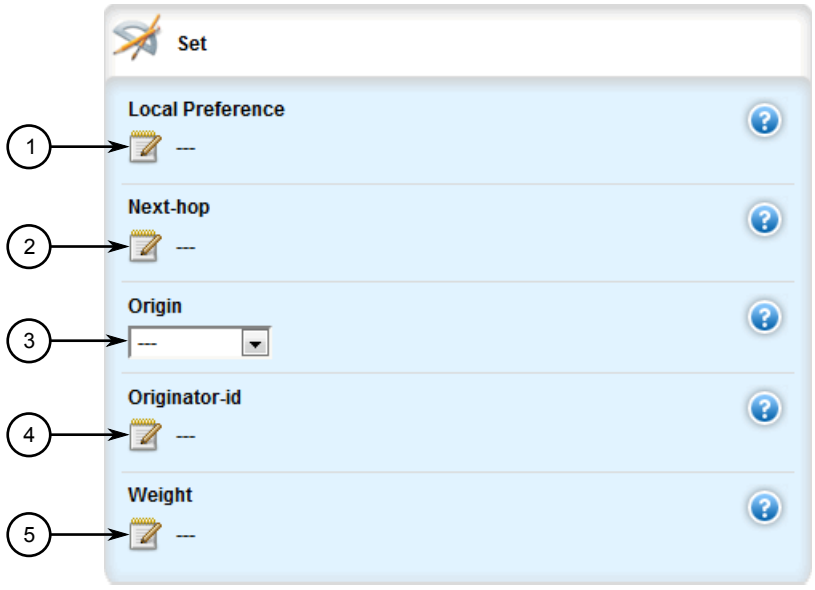


Figure 759: Set Form

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	**Synopsis:** A 32-bit unsigned integer between 1 and 4294967295 AS number.
IP Address	**Synopsis:** A string 7 to 15 characters long IP address of aggregator.

4. On the **Metric** form, configure the following parameters as required:

Parameter	Description
operation	**Synopsis:** { set, add, sub } Set , add or subtract the metric value.
value	**Synopsis:** A 32-bit unsigned integer Value.

5. On the **Set** form, configure the following parameters as required:

Parameter	Description
Local Preference	**Synopsis:** A 32-bit unsigned integer Local preference.
Next Hop	**Synopsis:** { peer } or a string 7 to 15 characters long The next hop address (xxx.xxx.xxx.xxx/xx or peer to use peer address).
origin	**Synopsis:** { egp, igp, incomplete } The origin code.

Parameter	Description
Originator ID	**Synopsis:** A string 7 to 15 characters long This parameter is not supported and any value is ignored by the system.
weight	**Synopsis:** A 32-bit unsigned integer Weight.

6. Add pre-pended and/or excluded autonomous system paths. For more information, refer to Section 13.8.3.3, "Adding a Prepended Autonomous System Path Filter" and/or Section 13.8.3.4, "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 13.8.3
Managing Prepended and Excluded Autonomous System Path Filters

This section describes how to configure and manage prepended and excluded autonomous system path filters.

CONTENTS

Section 13.8.3.1
Viewing a List of Prepended Autonomous System Path Filters

To view a list of prepended autonomous system path filters configured for a BGP route map entry, 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.

Figure 760: AS Path to Prepend Table

If no prepended autonomous system path filters have been configured, add filters as needed. For more information, refer to Section 13.8.3.3, "Adding a Prepended Autonomous System Path Filter".

Section 13.8.3.2
Viewing a List of Excluded Autonomous System Paths

To view a list of excluded autonomous system path filters configured for a BGP route map entry, 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.

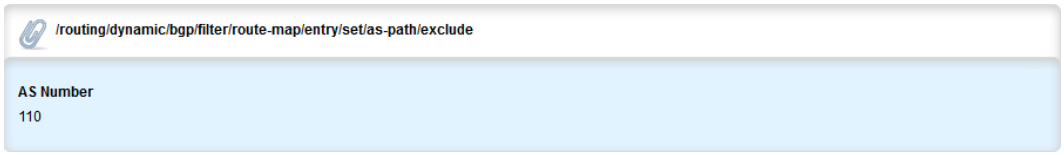


Figure 761: AS Path to Exclude Table

If no excluded autonomous system path filters have been configured, add filters as needed. For more information, refer to Section 13.8.3.4, "Adding an Excluded Autonomous System Path filter".

Section 13.8.3.3
Adding a Prepended Autonomous System Path Filter

To add a prepended autonomous system path filter to a BGP route map entry, do the following:

1. 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.

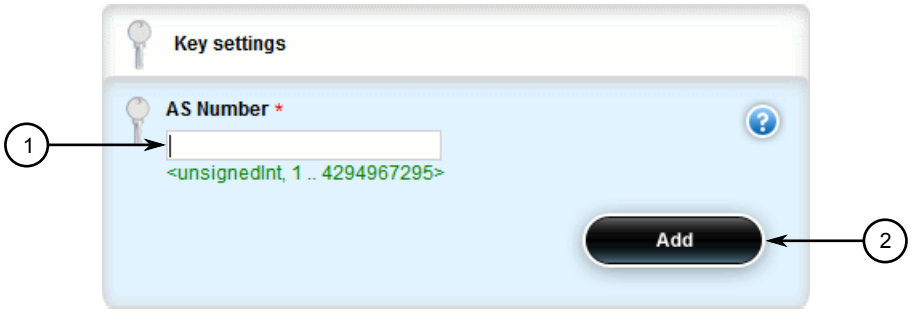


Figure 762: Key Settings Form

1. AS Number Box **2.** Add Button

4. Configure the following parameter(s) as required:

Parameter	Description
AS Number	**Synopsis:** A 32-bit unsigned 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 13.8.3.4

Adding an Excluded Autonomous System Path filter

To add an excluded autonomous system path filter to a BGP route map entry, do the following:

1. 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.
3. Click **<Add prepend>**. The **Key Settings** form appears.

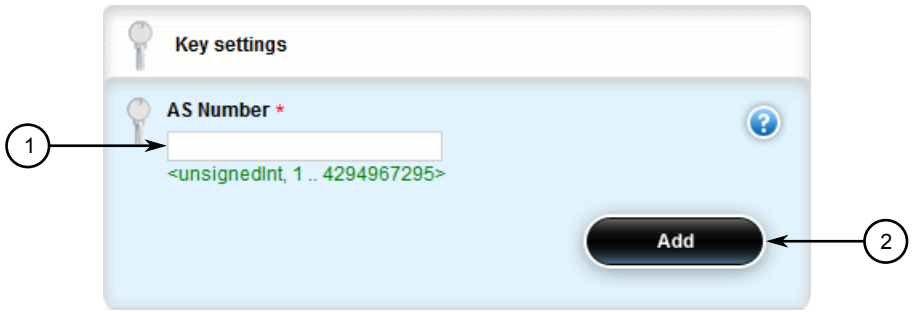


Figure 763: Key Settings Form

1. AS Number Box **2.** Add Button

4. Configure the following parameter(s) as required:

Parameter	Description
AS Number	**Synopsis:** A 32-bit unsigned 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 13.8.3.5
Deleting a Prepended Autonomous System Path Filter

To delete a prepended autonomous system path filter from a BGP route map entry, do the following:

1. 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.

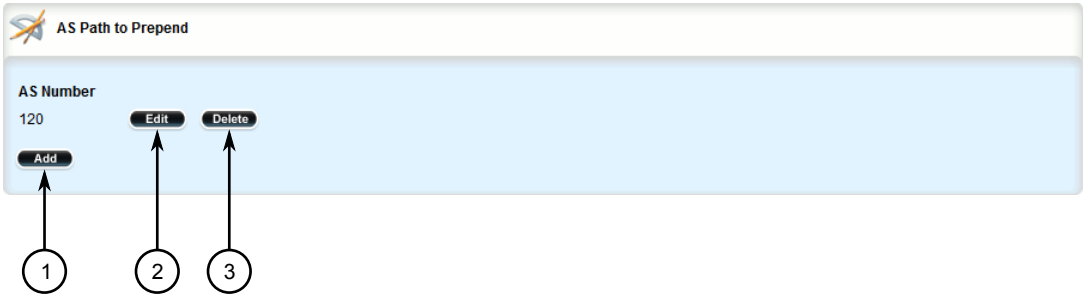


Figure 764: AS Path to Prepend Table

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 13.8.3.6
Deleting an Excluded Autonomous System Path Filter

To delete an excluded autonomous system path filter from a BGP route map entry, do the following:

1. 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.

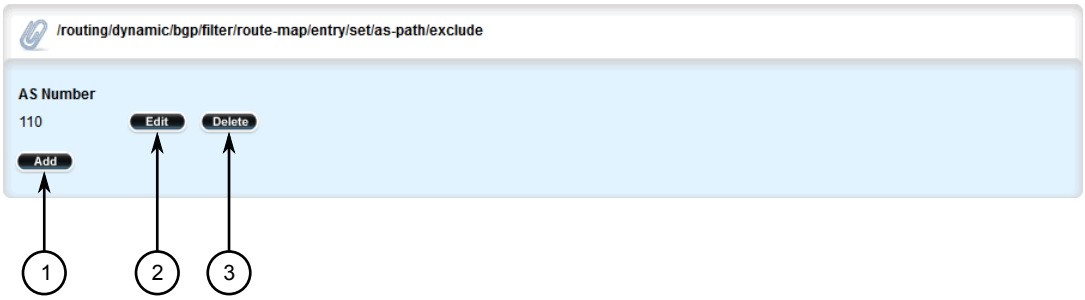


Figure 765: AS Path to Exclude Table

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 13.8.4

Managing Prefix Lists and Entries

Neighbors can be associated with prefix lists, which allow the BGP daemon to filter incoming or outgoing routes based on the *allow* and *deny* entries in the prefix list.

CONTENTS

Section 13.8.4.1

Viewing a List of Prefix Lists

To view a list of prefix lists for dynamic BGP routes, navigate to ***routing » dynamic » bgp » filter » prefix-list***. If prefix lists have been configured, the **Prefix List** table appears.

Figure 766: Prefix List Table

If no prefix lists have been configured, add lists as needed. For more information, refer to Section 13.8.4.3, "Adding a Prefix List".

Section 13.8.4.2
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.

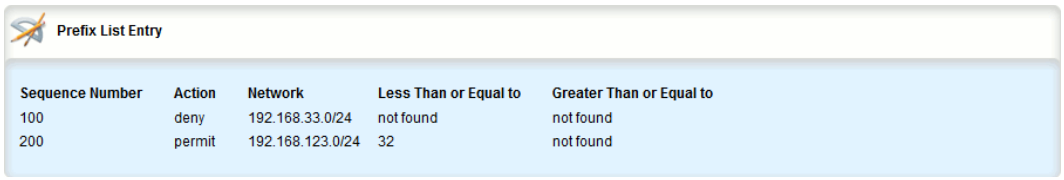


Figure 767: Prefix List Entry Table

If no entries have been configured, add entries as needed. For more information, refer to Section 13.8.4.4, "Adding a Prefix Entry".

Section 13.8.4.3
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.

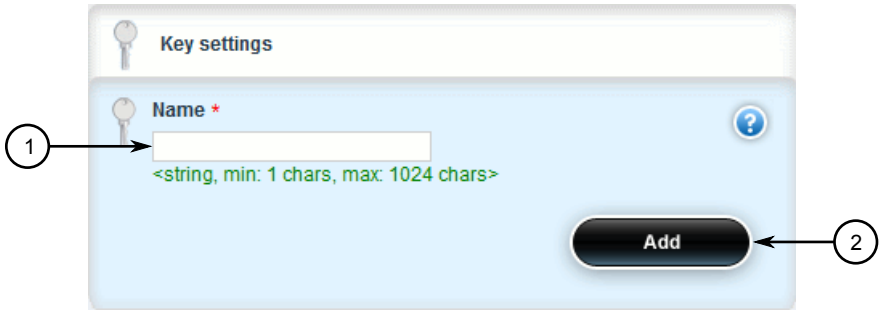


Figure 768: Key Settings Form

1. Name Box **2.** Add Button

3. Configure the following parameter(s) as required:

Parameter	Description
Name	**Synopsis:** 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.

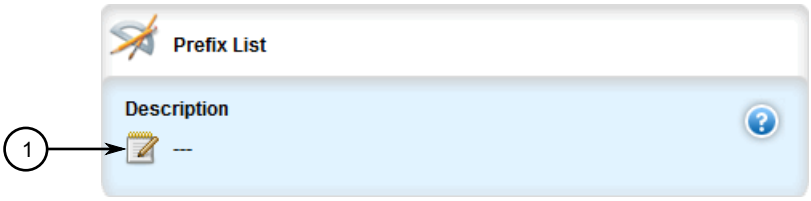


Figure 769: Prefix List Form

1. Description Box

5. Configure the following parameter(s) as required:

Parameter	Description
Description	**Synopsis:** 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 13.8.4.4, "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 13.8.4.4

Adding a Prefix Entry

To add 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 » rip » filter » {name} » entry***, where *{name}* is the name of the prefix list.
3. Click **<Add entry>**. The **Key Settings** form appears.

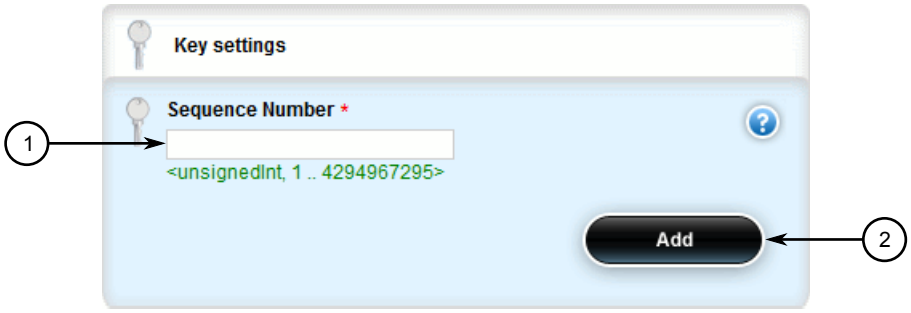


Figure 770: Key Settings Form

1. Sequence Number Box **2.** Add Button

4. Configure the following parameter(s) as required:

Parameter	Description
Sequence Number	**Synopsis:** A 32-bit unsigned integer between 1 and 4294967295 Sequence number of the entry.

5. Click **Add** to create the new entry. The **Prefix List Entry** form appears.

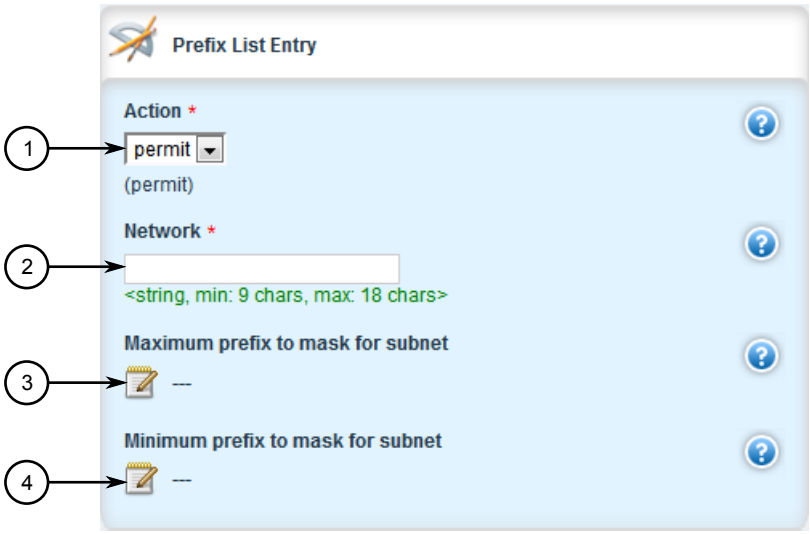


Figure 771: Prefix List Entry Form

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	**Synopsis:** { deny, permit } **Default:** permit Action.
Network	**Synopsis:** A string 9 to 18 characters long Network (xxx.xxx.xxx.xxx/xx). This parameter is mandatory.
Maximum prefix to mask for subnet	**Synopsis:** An 8-bit unsigned integer between 1 and 32 The maximum prefix length to match ipaddress within subnet.
Minimum prefix to mask for subnet	**Synopsis:** An 8-bit unsigned 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 13.8.4.5
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.

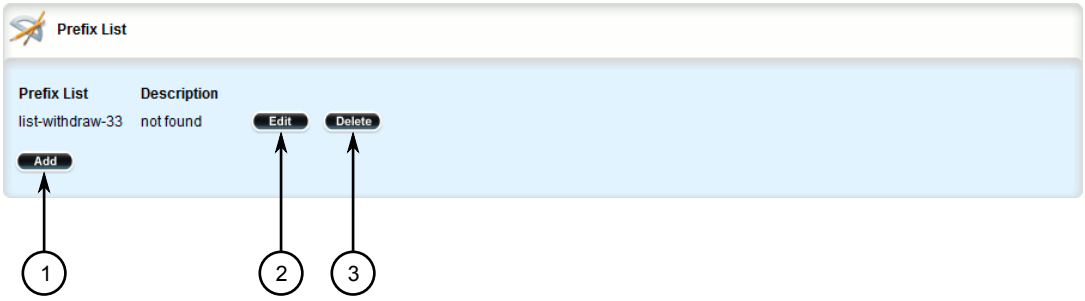


Figure 772: Prefix List Table

1. Add Button **2.** Edit Button **3.** Delete Button

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 13.8.4.6
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.

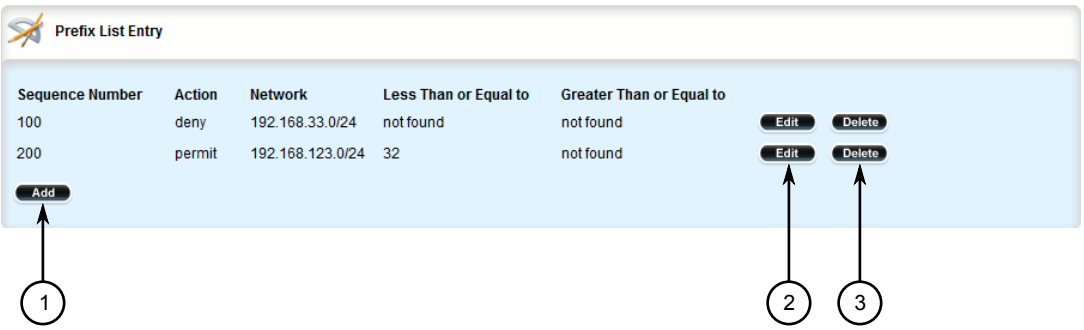


Figure 773: Prefix List Entry Table

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 13.8.5
Managing Autonomous System Paths and Entries

This section describes how to configure autonomous system paths and entries for dynamic BGP routes.

CONTENTS

Section 13.8.5.1
Viewing a List of Autonomous System Paths

To view a list of autonomous system path filters for dynamic BGP routes, navigate to ***routing » dynamic » bgp » filter » as-path***. If filters have been configured, the **Autonomous System Path Filter** table appears.

Figure 774: Autonomous System Path Filter Table

If no filters have been configured, add filters as needed. For more information, refer to Section 13.8.5.3, "Adding an Autonomous System Path Filter".

Section 13.8.5.2
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.

Figure 775: Entry Table

If no filters have been configured, add filters as needed. For more information, refer to Section 13.8.5.3, "Adding an Autonomous System Path Filter".

Section 13.8.5.3
Adding an Autonomous System Path Filter

To add an autonomous system path filter for dynamic BGP routes, do the following:

1. 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.

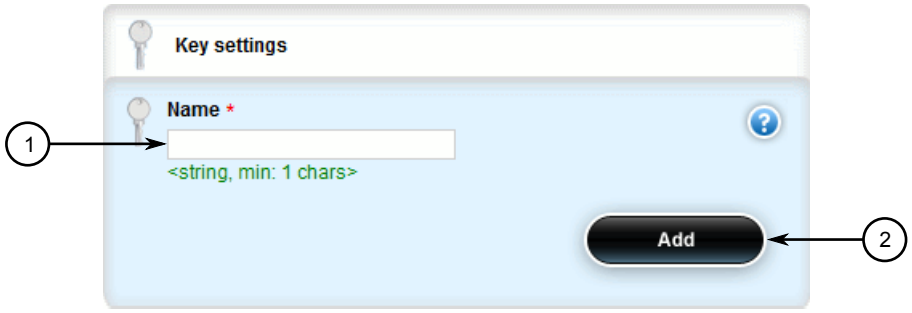


Figure 776: Key Settings Form

1. Name Box **2.** Add Button

3. Configure the following parameter(s) as required:

Parameter	Description
Name	**Synopsis:** 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 13.8.5.4, "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 13.8.5.4

Adding an Autonomous System Path Filter Entry

Create an entry for an autonomous system path filter to match a string or integer value in AS path and then perform an action. The match criteria is defined using regular expressions. 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)

Character	Description	Example
[]	Matches any character other than those specified	[^abc]
_ (underscore)	The underscore character has special meanings in an autonomous system path. It matches to: • Each space ( ) and comma (,) • Each AS set delimiter (e.g. *{* and *}*) • Each AS confederation delimiter (e.g. *(* and *)*) • The beginning and end of the line Therefore, the underscore can be used to match AS values.	_100,100_, _100_

To add an entry for an autonomous system path filter, do the following:

1. 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.

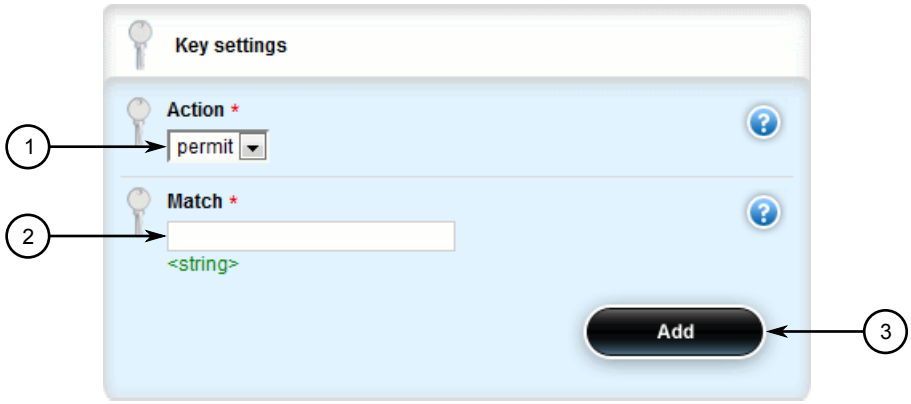


Figure 777: Key Settings Form

1. Action List **2.** Match Box **3.** Add Button

4. Configure the following parameter(s) as required:

Parameter	Description
Action	**Synopsis:** { deny, permit } Action.
Match	**Synopsis:** 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. This parameter is mandatory.

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 13.8.5.5
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.

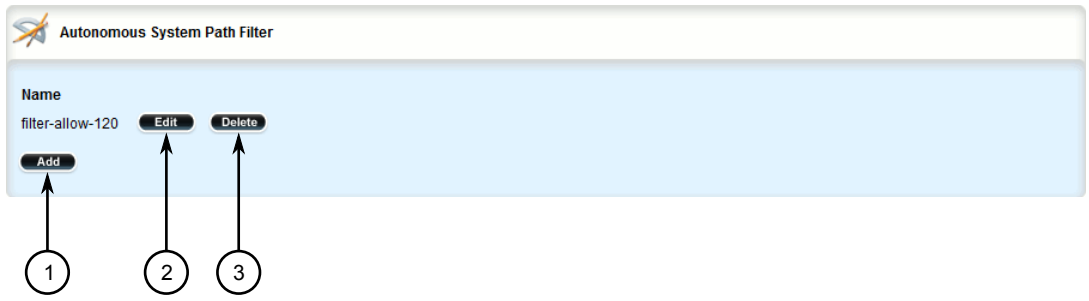


Figure 778: Autonomous System Path Filter Table

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 13.8.5.6
Deleting an Autonomous System Path Filter Entry

To delete an entry for an autonomous system path filter, do the following:

1. 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.

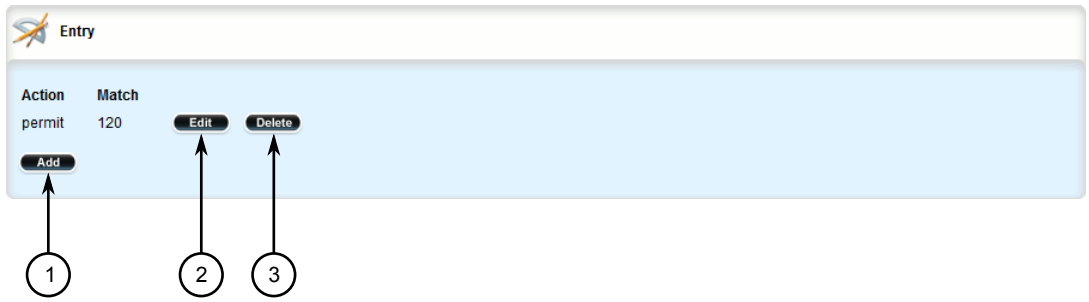


Figure 779: Entry Table

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 13.8.6

Managing Neighbors

Neighbors are other routers with which to exchange routes. One or more neighbors must be specified in order for BGP to operate.

NOTE
If neighbors are specified but no networks are specified, the router will receive BGP routing information from its neighbors but will not advertise any routes to them. For more information about networks, refer to Section 13.8.7, "Managing Networks".

CONTENTS

Section 13.8.6.1

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.

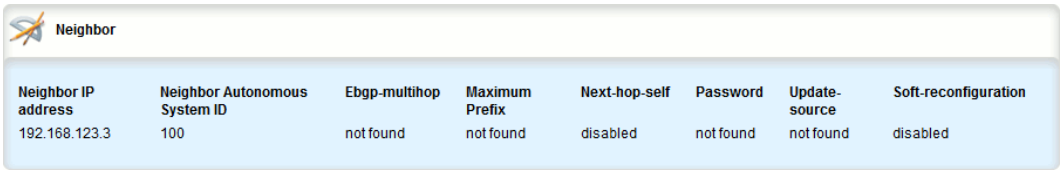


Figure 780: Neighbor Table

If no neighbors have been configured, add neighbors as needed. For more information, refer to Section 13.8.6.2, "Adding a Neighbor".

Section 13.8.6.2
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.

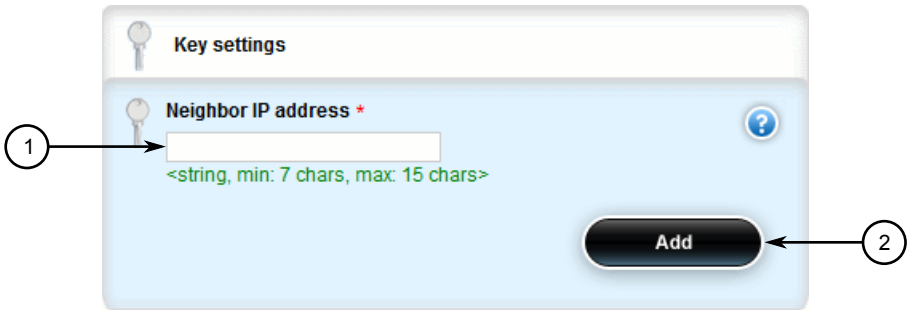


Figure 781: Key Settings Form

1. Neighbor IP Address Box **2.** Add Button

3. Configure the following parameter(s) as required:

Parameter	Description
Neighbor IP Address	**Synopsis:** A string 7 to 15 characters long The neighbor IP address.

4. Click **Add** to add the address. The **Route Reflector Client**, **Route Map** and **Neighbor** forms appear.

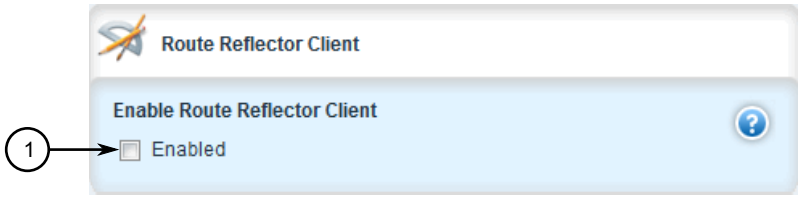


Figure 782: Route Reflector Client Form

1. Enable Check Box

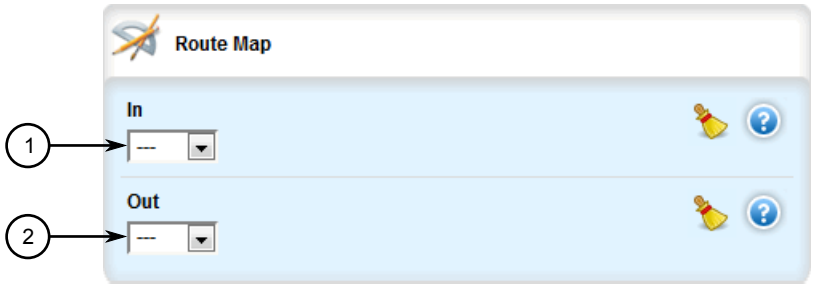


Figure 783: Route Map Form

1. In List **2.** Out List

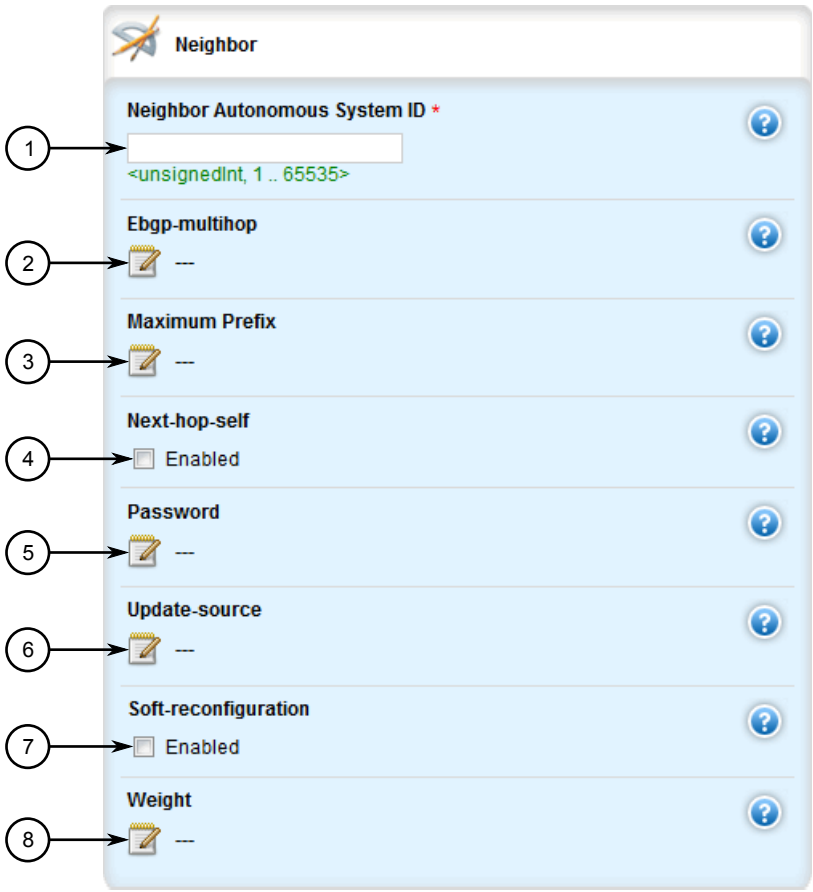


Figure 784: Neighbor Form

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. [Optional] On the **Route Reflector Client** form, enable the neighbor as a route reflector client by configuring the following parameter:

Parameter	Description
Enable Route Reflector Client	If enabled and Route Reflector enabled, makes this neighbor a client for Route Reflector.

6. [Optional] On the **Route Map** form, configure the following parameter(s) as required:

Parameter	Description
in	**Synopsis:** A string Apply route map to incoming routes.
out	**Synopsis:** A string Apply route map to outbound routes.

7. [Optional] On the **Neighbor** form, configure the following parameter(s) as required:

Parameter	Description
Neighbor Autonomous System ID	**Synopsis:** A 32-bit unsigned integer between 1 and 65535 A BGP neighbor. This parameter is mandatory.
EBGP Multihop Count	**Synopsis:** An 8-bit unsigned integer between 1 and 255 The maximum hop count. This allows EBGP neighbors not on directly connected networks.
Maximum Prefix	**Synopsis:** A 32-bit unsigned integer between 1 and 4294967295 The maximum prefix number accepted from this peer.
Next Hop Itself	Disables the next hop calculation for this neighbor.
password	**Synopsis:** A string 1 to 1024 characters long Password.
Update Source	**Synopsis:** A string 7 to 15 characters long Source IP address of routing updates.
Disable Connected Check	Disables connection verification when establishing an eBGP peering session with a single-hop peer that uses a loopback interface.
Soft Reconfiguration	Per neighbor soft reconfiguration.
weight	**Synopsis:** A 16-bit unsigned integer The default weight for routes from this neighbor.

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 13.8.6.3
Configuring the Distribution of Prefix Lists

To configure the distribution of prefix lists for a neighbor in a BGP network, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Make sure the desired prefix list is configured for the BGP network. For more information, refer to Section 13.8.4.3, “Adding a Prefix List”.

3. Navigate to ***routing » dynamic » bgp » neighbor » {address} » distribute-prefix-list***, where *{address}* is the IP address of the neighbor.
4. 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.

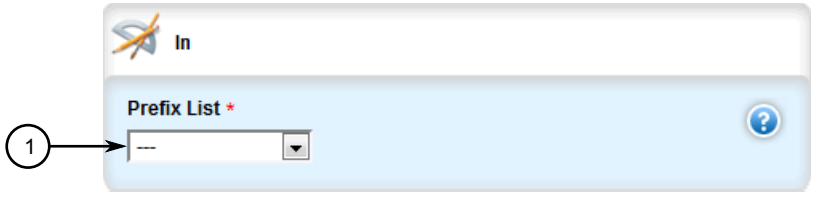


Figure 785: In Form (Example)

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 13.8.6.4, "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 13.8.6.4

Tracking Commands for BGP Neighbors

Network commands can be tracked using event trackers configured under ***global » tracking***. For more information about event trackers, refer to Section 13.5, "Managing Event Trackers".

The network command is activated based on the event tracker's state. The **Apply When** parameter determines when the command is activated. For example, if the **Apply When** parameter is set to **down**, the network command becomes active (thereby advertising the network to a router's BGP peers) when the tracked target is unavailable.

To track a command for a BGP neighbor, do the following:

1. 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

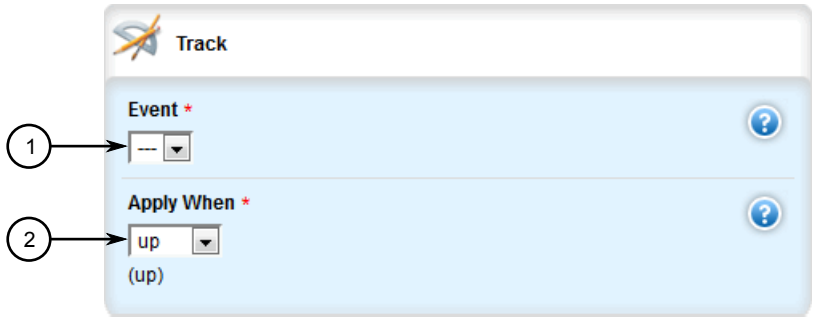


Figure 786: Track Form

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 13.5.3, "Adding an Event Tracker".

Parameter	Description
Event	**Synopsis:** A string Select to track an event, apply the distribute-prefix-list only when the tracked event goes to UP state. This parameter is mandatory.
Apply When	**Synopsis:** { up, down } **Default:** up Applies the distribute-prefix-list when the tracked event goes UP or DOWN.

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 13.8.6.5
Deleting a Neighbor

To delete a neighbor from a BGP network, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to ***routing » dynamic » bgp » neighbor***. The **Neighbor** table appears.

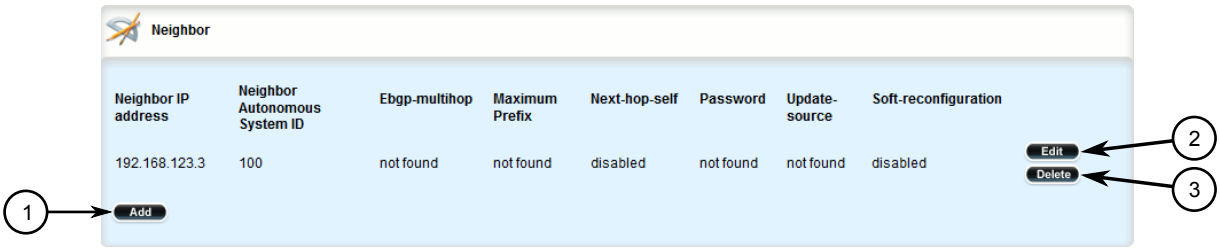


Figure 787: Neighbor Table

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 13.8.7

Managing Networks

As opposed to neighbors, which are specific routers with which to exchange routes, networks are groups of routers that are either part of a specific subnet or connected to a specific network interface. They can be used at the same time as neighbors.

NOTE
For point-to-point links, such as T1/E1 links, specify neighbors instead of a network. For more information, refer to Section 13.8.6.2, "Adding a Neighbor".

NOTE
Networks for the BGP protocol do not require a valid entry in the routing table. Since BGP is a broader gateway protocol, a more general network specification would typically be entered. For example, if a routed network inside the Autonomous System (AS) was comprised of many different Class C subnets (/24) of the 192.168.0.0/16 range, it is more efficient to advertise the one Class B network specification, 192.168.0.0/16, to its BGP neighbors.

NOTE
If neighbors are specified but no networks are specified, the router will receive routing information from its neighbors but will not advertise any routes to them. For more information about neighbors, refer to Section 13.8.6, "Managing Neighbors".

CONTENTS

Section 13.8.7.1
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.

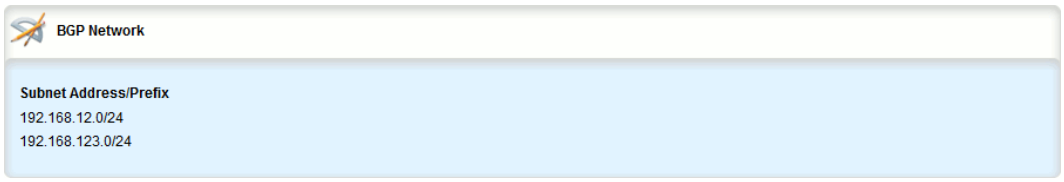


Figure 788: BGP Network Table

If no networks have been configured, add networks as needed. For more information, refer to Section 13.8.7.2, "Adding a Network".

Section 13.8.7.2
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.

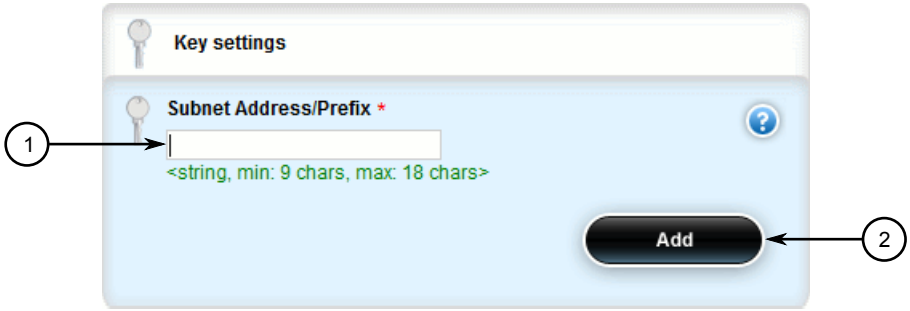


Figure 789: Key Settings Form

1. Subnet Address/Prefix Box **2.** Add Button

3. Configure the following parameter(s) as required:

Parameter	Description
Subnet Address/Prefix	**Synopsis:** 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 13.8.7.3, "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 13.8.7.3
Tracking Commands for a BGP Network

Network commands can be tracked using event trackers configured under ***global » tracking***. For more information about event trackers, refer to Section 13.5, "Managing Event Trackers".

The network command is activated based on the event tracker's state. The **Apply When** parameter determines when the command is activated. For example, if the **Apply When** parameter is set to **down**, the network command becomes active (thereby advertising the network to a router's BGP peers) when the tracked target is unavailable.

To track a command for a BGP network, do the following:

1. 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

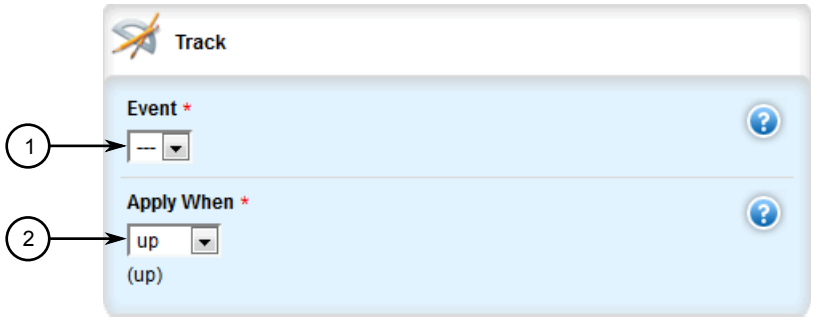


Figure 790: Track Form

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 13.5.3, "Adding an Event Tracker".*

Parameter	Description
Event	**Synopsis:** A string Select an event. This parameter is mandatory.
Apply When	**Synopsis:** { up, down } **Default:** up Advertises the network when the tracked event state goes UP or stops advertising the network when the tracked event goes DOWN.

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 13.8.7.4
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.

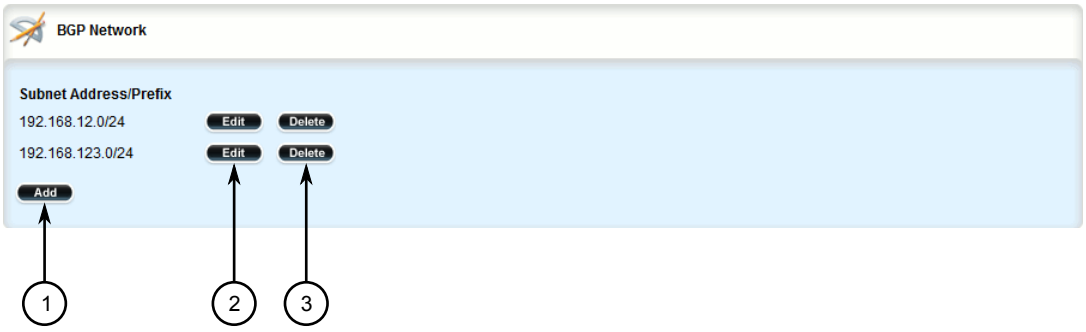


Figure 791: BGP Network Table

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 13.8.8
Managing Aggregate Addresses

This section describes how to aggregate multiple addresses into a single dynamic BGP route.

CONTENTS

Section 13.8.8.1
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 792: Aggregate Network Table

If no aggregate addresses have been configured, add addresses as needed. For more information, refer to Section 13.8.8.2, "Adding an Aggregate Address".

Section 13.8.8.2
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.

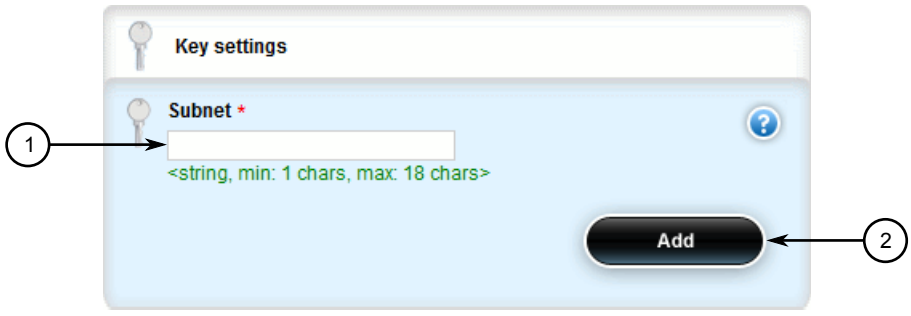


Figure 793: Key Settings Form

1. Subnet Box **2.** Add Button

3. Configure the following parameter(s) as required:

Parameter	Description
subnet	**Synopsis:** 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 13.8.9.2, "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 13.8.8.3
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.

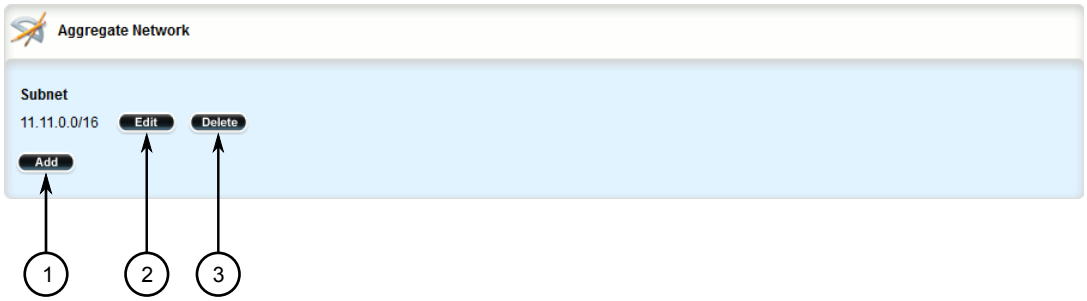


Figure 794: Aggregate Network Table

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 13.8.9
Managing Aggregate Address Options

This section describes how to set the `as-set` and `summary-only` options for BGP aggregate addresses.

CONTENTS

Section 13.8.9.1
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 795: Aggregate Network Options Table

If no options have been configured, add options as needed. For more information, refer to Section 13.8.9.2, "Adding an Aggregate Address Option".

Section 13.8.9.2
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.

Figure 796: Key Settings Form

1. Value List **2.** Add Button

4. Configure the following parameter(s) as required:

Parameter	Description
value	**Synopsis:** { 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 13.8.9.3
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.

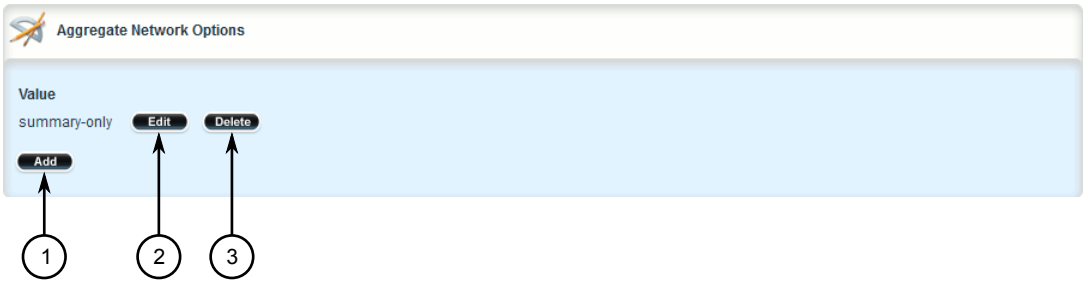


Figure 797: Aggregate Network Options Table

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 13.8.10
Managing Redistribution Metrics

Redistribution metrics redistribute routing information from other routing protocols, static routes or routes handled by the kernel. Routes for subnets that are directly connected to the router, but not part of the BGP network, can also be advertised.

CONTENTS

Section 13.8.10.1
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.

Figure 798: Redistribute Route from Other Protocols Table

If no redistribution metrics have been configured, add metrics as needed. For more information, refer to Section 13.8.10.2, "Adding a Redistribution Metric".

Section 13.8.10.2
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.

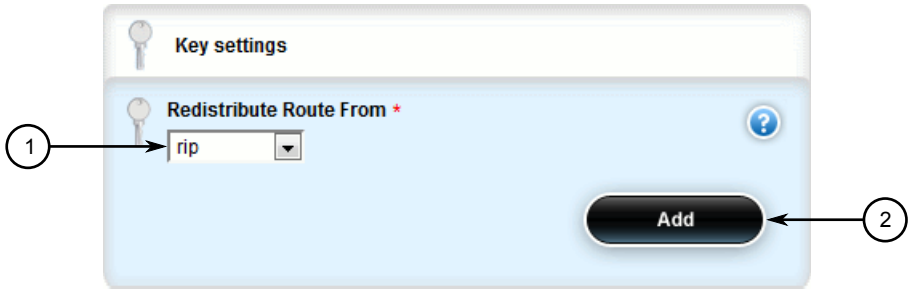


Figure 799: Key Settings Form

1. Redistribute Route From List **2.** Add Button

3. Configure the following parameter(s) as required:

Parameter	Description
Redistribute Route From	**Synopsis:** { kernel, static, connected, ospf, rip } Redistribute route type.
Metric	**Synopsis:** A 32-bit unsigned integer Metric value for redistributed routes.

4. Click **Add** to add the metric. The **Redistribute Route From Other Protocols** form appears.

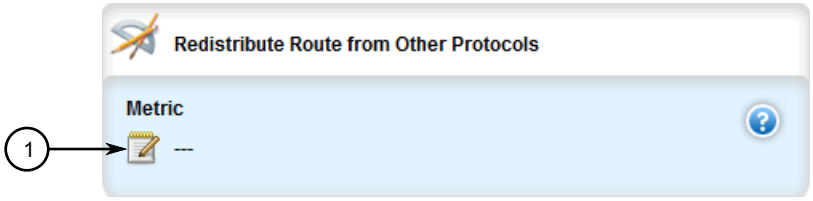


Figure 800: Redistribute Route From Other Protocols Form

1. Metric Box

5. Configure the following parameter(s) as required:

Parameter	Description
Redistribute Route From	**Synopsis:** { kernel, static, connected, ospf, rip } Redistribute route type.
Metric	**Synopsis:** A 32-bit unsigned integer 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 13.8.10.3

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.

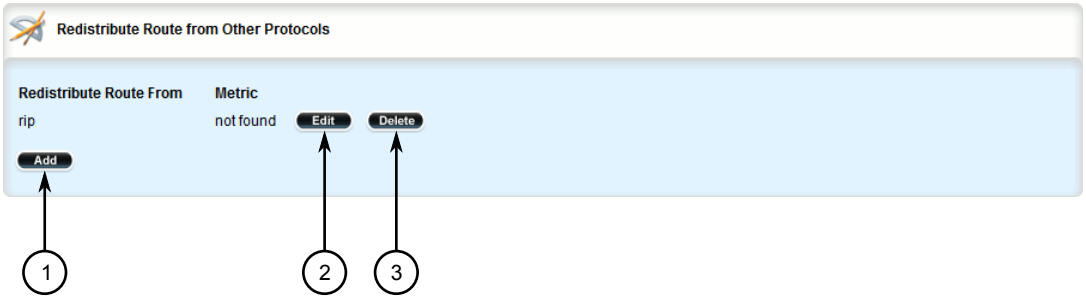


Figure 801: Redistribute Route from Other Protocols Table

1. Add Button **2.** Edit Button **3.** Delete Button

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 13.8.11
Managing Route Reflector Options

This section describes how to configure the device as a route reflector for BGP networks.

CONTENTS

Section 13.8.11.1
Understanding Route Reflectors

Route reflectors offer a method for simplifying BGP network topologies and improving scalability.

The Full-Mesh Requirement

Due to BGP route advertisement rules, BGP requires a logical full-mesh topology, wherein each router advertises and forwards its routes to each of its neighbors. This requirement is easily met by external BGP (eBGP) networks, where connections are established between Autonomous Systems (AS). Routers can easily avoid loops by dropping any routes that share the same AS numeric identifier. However, in internal BGP (iBGP), each router shares the same AS numeric identifier, so all routes received by a router would be dropped.

One method for solving this problem is to have each iBGP router establish neighborship with its peers, but that would result in a significant number of BGP sessions and unnecessary traffic on large networks. The formula for determining the number of BGP sessions for X number of routers is **X*(X-1)/2**. Therefore, 20 iBGP routers would generate 190 BGP sessions (20*[20-1]/2 = 190).

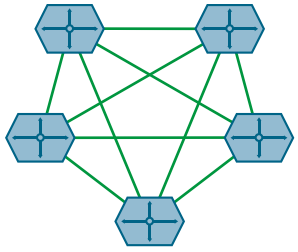


Figure 802: A Simple BGP Topology Without a Route Reflector

The Route Reflector Solution

Route reflectors simplify the topology by grouping routers into a cluster. In the cluster, the route reflector establishes a BGP session with each client (BGP neighbor). The clients are not required to establish BGP sessions with each other, nor are they required to be fully-meshed. All routes are advertised to the route reflector, who in turn re-advertises the routes to its clients, thus meeting the logical full-mesh requirement.

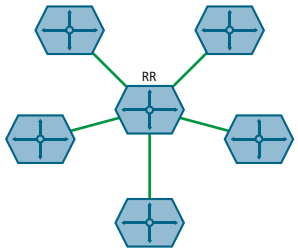


Figure 803: A Simple BGP Topology With a Route Reflector

Route reflectors can also share routes with routers outside of their clusters. These are referred to as *non-clients*. Non-clients are required to be fully-meshed.

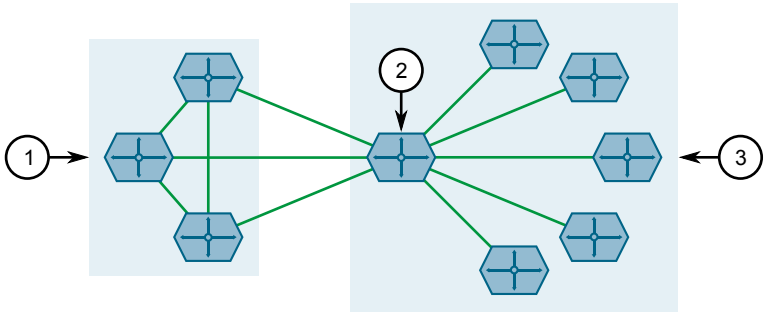


Figure 804: A Complex BGP Topology

1. Fully Meshed iBGP Peers (Non-Clients) **2.** Route Reflector **3.** Cluster (Clients)

Combining Clusters for Scalability

Multiple clusters can be linked together via their route reflectors to form a full-mesh topology of internal peers. In this configuration, routes advertised to a route reflector are not only re-advertised to its clients, but also with the other route reflectors who in turn advertise the routes to their clients. This allows routes to propagate through the entire AS without the scaling problems associated with the full-mesh requirement.

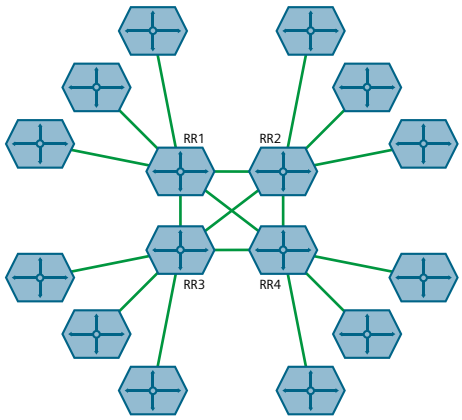


Figure 805: Multiple Clusters Fully-Meshed

Route reflectors can also be partially-meshed by combining them in a cluster of their own.

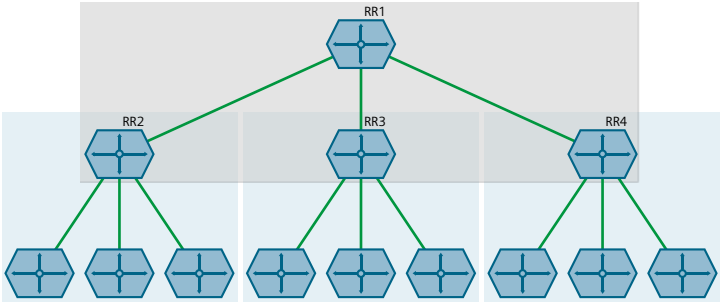


Figure 806: Multiple Clusters Partially-Meshed

Redundant Route Reflectors

To avoid a single point of failure in the BGP network, each cluster should be served by more than one route reflector to provide redundancy in case of failure. In this arrangement, each route reflectors are configured to have the same BGP neighbors as clients.

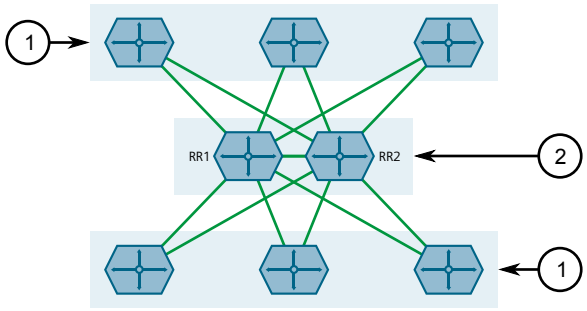


Figure 807: Redundant Route Reflector Topology

1. Cluster **2.** Route Reflector

Section 13.8.11.2

Configuring the Device as a Route Reflector

To configure the device to be a route reflector for a specific cluster, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to ***routing » dynamic » bgp***. The **Route Reflector** form appears.

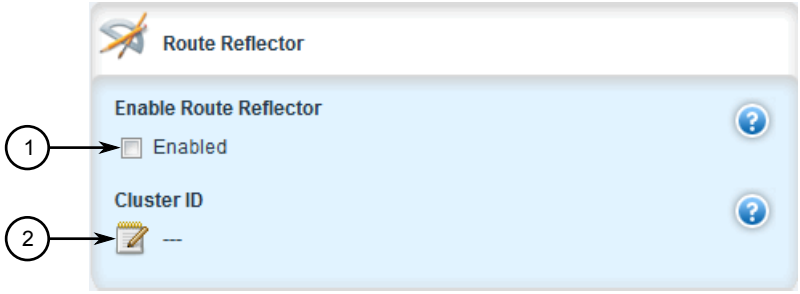


Figure 808: Route Reflector Form

1. Enable Route Reflector Check Box **2.** Cluster ID Box

3. Configure the following parameters as required:

Parameter	Description
Enable Route Reflector	When enabled, sets this router as a Route Reflector.
Cluster ID	**Synopsis:** A string 7 to 15 characters long The ID of the BGP cluster to which the device belongs. The ID is expressed as an IPv4 address (e.g. 1.2.3.4).

4. Configure one or more BGP neighbors to be clients of the device. For more information, refer to Section 13.8.11.3, "Configuring BGP Neighbors as Clients".
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 13.8.11.3
Configuring BGP Neighbors as Clients

When the device is configured to be a route reflector, BGP neighbors can then be configured to be clients of the reflector.

BGP Neighbors

To configure a BGP neighbor to be a client of the device, do the following:

1. Make sure a BGP neighbor is defined. For more information, refer to Section 13.8.6.2, "Adding a Neighbor".
2. Navigate to ***routing » dynamic » bgp » neighbor » {address}***, where *{address}* is the IP address of the BGP neighbor. The **Route Reflector Client** form appears.

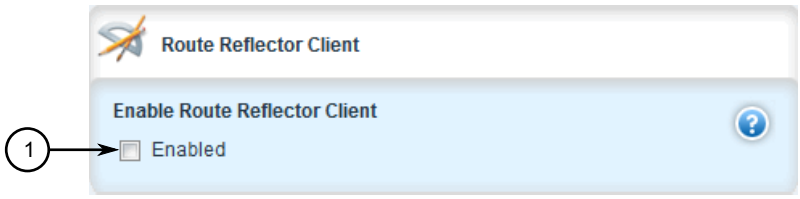


Figure 809: Route Reflector Client Form

1. Enable Route Reflector Client Check Box

3. Under **Enable Route Reflector Client**, select **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.

BGP Neighbors In an IPv4 Address Family

To configure a BPG neighbor that belongs to an IPv4 address family to be a client of the device, do the following:

1. Make sure an IPv4 address family is defined. For more information, refer to Section 13.11.10.2, "Adding an IPv4 Address Family".
2. Navigate to ***routing » dynamic » bgp » address-family » ipv4 » vrf » {definition} » neighbor » {address}***, where *{definition}* is the name of the VRF definition and *{address}* is the IP address of the desired BGP neighbor. The **Route Reflector Client** form appears.

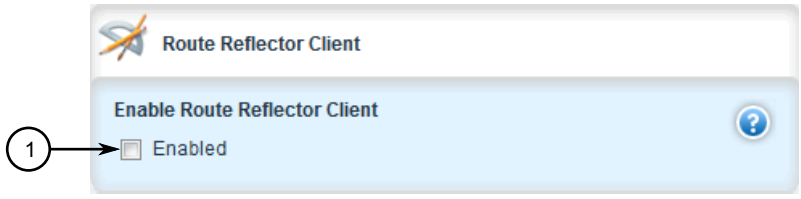


Figure 810: Route Reflector Client Form

1. Enable Route Reflector Client Check Box

3. Under **Enable Route Reflector Client**, select **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.

» BGP Neighbors In a VPNv4 Address Family

To configure a BPG neighbor that belongs to a VPNv4 address family to be a client of the device, do the following:

1. Make sure a VPNv4 address family is defined. For more information, refer to Section 13.11.9.2, "Adding a Neighbor".
2. Navigate to ***routing » dynamic » bgp » address-family » vpnv4 » {address}***, where *{address}* is the IP address of the desired BGP neighbor. The **Route Reflector Client** form appears.

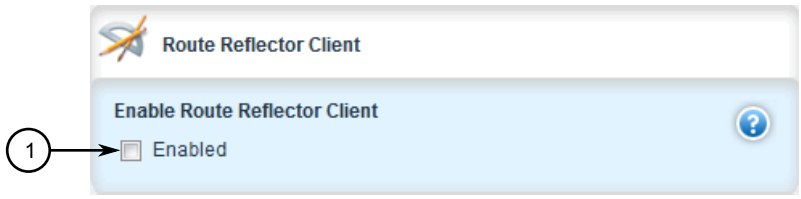


Figure 811: Route Reflector Client Form

1. Enable Route Reflector Client Check Box

3. Under **Enable Route Reflector Client**, select **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 13.8.11.4

Example: Basic Route Reflection

This example demonstrates how to configure a partially-meshed Autonomous System (AS) where a route reflector advertises routes to clients and non-clients.

Overview

In the following topology, routes advertised by the external BGP (eBGP) router (labeled as R1) are forwarded to the route reflector (labeled as RR). The route reflector then in turn readvertises the routes to its BGP neighbors. Neighbors within the route reflector's cluster are the clients (labeled C1, C2 and C3). Neighbors outside of the cluster are non-clients (labeled NC1, NC2 and NC3).

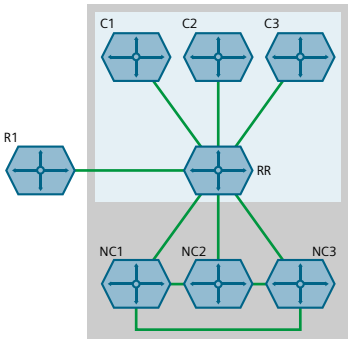


Figure 812: Basic Route Reflection Topology

Similarly, routes advertised by a non-client (NC1, NC2 or NC3) are forwarded to its BGP neighbors, including the route reflector. The route reflector in turn readvertises the routes to its BGP neighbors, which includes those in its cluster and the eBGP router (R1).

With the exception of the eBGP router (R1), all devices are within the same Autonomous System (AS).

Configuration

To configure the device to act as the route reflector in this scenario, do the following:

1. Enable the route reflector feature and assign a cluster ID to the device. For more information, refer to Section 13.8.11.2, "Configuring the Device as a Route Reflector".
2. For each router that advertises and forwards routes to the route reflector, define a BGP neighbor. Make sure each belongs to the same AS. For more information, refer to Section 13.8.6.2, "Adding a Neighbor".
3. For each BGP neighbor that belongs to the route reflector's cluster, enable the neighbor as a route reflector client. For more information, refer to Section 13.8.11.3, "Configuring BGP Neighbors as Clients".

Final Configuration Example

```
routing bgp
 enabled
 as-id              100
 route-reflector enabled
 route-reflector cluster-id 10.11.12.13
 !
 neighbor 172.30.140.10                  { Client }
  remote-as 100
  route-reflector-client enabled
 !
 neighbor 172.30.140.20                  { Client }
  remote-as 100
  route-reflector-client enabled
 !
 neighbor 172.30.140.30                  { Client }
```

```
  remote-as 100
  route-reflector-client enabled
 !
 neighbor 172.30.150.10                    { Non-Client }
  remote-as 100
  no route-reflector-client enabled
 !
 neighbor 172.30.150.20                    { Non-Client }
  remote-as 100
  no route-reflector-client enabled
 !
 neighbor 172.30.150.30                    { Non-Client }
  remote-as 100
  no route-reflector-client enabled
 !
!
```

Section 13.8.11.5

Example: Linking Clusters

This example demonstrates how to link two multiple clusters together by connecting each route reflector in a full-mesh topology.

Overview

In the following topology, three route reflectors (RR1, RR2 and RR3) are internal peers of one another.

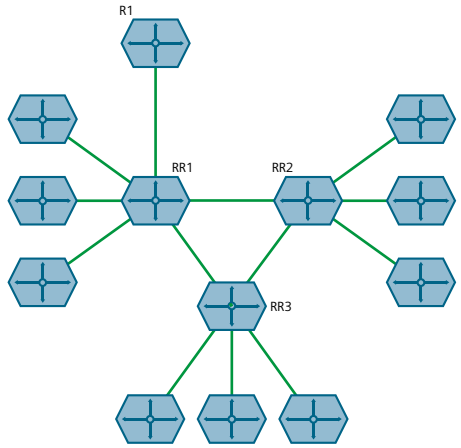


Figure 813: Linked Clusters

When an external BGP (eBGP) router (R1) advertises routes to RR1, RR1 readvertises the routes to RR2, RR3 and its clients. RR2 and RR3 then readvertise the routes again to their clients.

Configuration

To configure this topology, do the following:

1. Configure the clusters for RR1, RR2, RR3. For more information, refer to Section 13.8.11.2, "Configuring the Device as a Route Reflector".

2. For each route reflector, define the other route reflectors as BGP neighbors. For more information, refer to Section 13.8.6.2, "Adding a Neighbor".

Final Configuration Example

RR1 (172.30.110.10)

```
routing bgp
 enabled
 as-id              100
 route-reflector cluster-id 0.1.2.3
 !
 neighbor 172.30.110.20                  { RR2 }
  remote-as 100
  no route-reflector-client enabled
 !
 neighbor 172.30.110.30                  { RR3 }
  remote-as 100
  no route-reflector-client enabled
 !
 neighbor 172.30.140.10                  { Client }
  remote-as 100
  route-reflector-client enabled
 !
 neighbor 172.30.140.20                  { Client }
  remote-as 100
  route-reflector-client enabled
 !
 neighbor 172.30.140.30                  { Client }
  remote-as 100
  route-reflector-client enabled
 !
!
```

RR2 (172.30.110.20)

```
routing bgp
 enabled
 as-id              100
 route-reflector cluster-id 10.11.12.13
 !
 neighbor 172.30.110.10                  { RR1 }
  remote-as 100
  no route-reflector-client enabled
 !
 neighbor 172.30.110.30                  { RR3 }
  remote-as 100
  no route-reflector-client enabled
 !
 neighbor 172.30.150.10                  { Client }
  remote-as 100
  route-reflector-client enabled
 !
 neighbor 172.30.150.30                  { Client }
  remote-as 100
  route-reflector-client enabled
 !
 neighbor 172.30.150.20                  { Client }
  remote-as 100
  route-reflector-client enabled
 !
!
```

RR3 (172.30.110.30)

```
routing bgp
 enabled
 as-id              100
 route-reflector cluster-id 20.21.22.23
 !
 neighbor 172.30.110.10                  { RR1 }
  remote-as 100
  no route-reflector-client enabled
 !
 neighbor 172.30.110.20                  { RR2 }
  remote-as 100
  no route-reflector-client enabled
 !
 neighbor 172.30.160.10                  { Client }
  remote-as 100
  route-reflector-client enabled
 !
 neighbor 172.30.160.20                  { Client }
  remote-as 100
  route-reflector-client enabled
 !
!
```

Section 13.8.11.6

Example: Clusters in Clusters

This example demonstrates how to group clusters into a hierarchical structure (clusters of clusters).

Overview

In the following topology, a route reflector (RR1) forms a cluster with two other route reflectors (RR2 and RR3). RR2 and RR3 are also part of their own individual clusters, each of which consists of three clients.

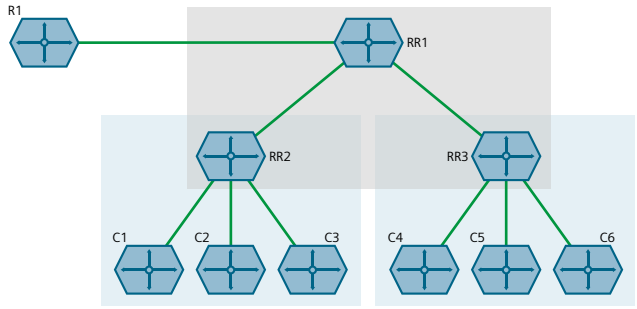


Figure 814: Hierarchical Clusters Topology

When an external BGP (eBGP) router (R1) advertises routes to RR1, RR1 readvertises the routes to RR2 and RR3. RR2 and RR3 then readvertise the routes again to their clients.

Configuration

To configure this topology, do the following:

1. Configure the clusters for RR2 and RR3. For more information, refer to Section 13.8.11.2, "Configuring the Device as a Route Reflector".
2. Configure RR1 as a route reflector and define RR2 and RR3 as its clients. For more information, refer to Section 13.8.11.2, "Configuring the Device as a Route Reflector".

Final Configuration Example

RR1 (172.30.140.10)

```
routing bgp
 enabled
 as-id              100
 route-reflector enabled
 route-reflector cluster-id 0.1.2.3
 !
 neighbor 172.30.140.20                  { RR2 }
  remote-as 100
  route-reflector-client enabled
 !
 neighbor 172.30.140.30                  { RR3 }
  remote-as 100
  route-reflector-client enabled
 !
```

RR2 (172.30.140.20)

```
routing bgp
 enabled
 as-id              100
 route-reflector enabled
 route-reflector cluster-id 10.11.12.13
 !
 neighbor 172.30.140.10                  { RR1 }
  remote-as 100
  no route-reflector-client enabled
 !
 neighbor 172.30.150.10                  { Client }
  remote-as 100
  route-reflector-client enabled
 !
 neighbor 172.30.150.20                  { Client }
  remote-as 100
  route-reflector-client enabled
 !
 neighbor 172.30.150.30                  { Client }
  remote-as 100
  route-reflector-client enabled
 !
!
```

RR3 (172.30.140.30)

```
routing bgp
 enabled
 as-id              100
 route-reflector enabled
 route-reflector cluster-id 20.21.22.23
 !
 neighbor 172.30.140.10                  { RR1 }
  remote-as 100
  no route-reflector-client enabled
 !
 neighbor 172.30.160.10                  { Client }
```

```
  remote-as 100
  route-reflector-client enabled
 !
 neighbor 172.30.160.20                    { Client }
  remote-as 100
  route-reflector-client enabled
 !
 neighbor 172.30.160.30                    { Client }
  remote-as 100
  route-reflector-client enabled
 !
!
```

Section 13.8.11.7

Example: Route Reflection in a VRF Instance

This example demonstrates how to configure BGP route reflection in a VRF instance.

Overview

In the following topology, router RR is a BGP route reflector configured with a VRF instance (VRF1). The VRF instance is configured with a single IPv4 address family consisting of routers R2 and R3. All three routers belong to the same autonomous system (AS1).

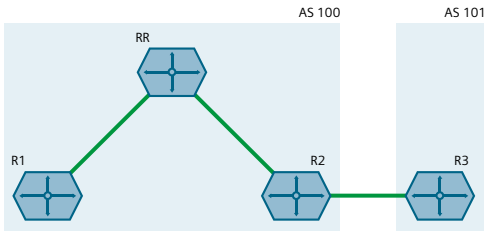


Figure 815: Route Reflection in a VRF Instance

RR receives BGP routing information from R2 via its VRF interface, 1.1.2.1. It then readvertises the information to its client, R1.

R2 receives BGP routing information from R3, an external BGP (eBGP) router.

Configuration

To configure this topology, do the following:

1. **Configure RR**
   a. Configure a VRF definition for *VRF1* with a route distinguisher of **100:1**. For more information, refer to Section 13.11.5.2, "Adding a VRF Definition".
   b. Define a route target for VRF1 of type `both` with the export community set to **100:1**. For more information, refer to Section 13.11.6.2, "Adding a Route Target".
   c. Make sure interfaces are configured with the IP addresses 1.1.12/24 and 1.1.2.1/24.
   d. Assign the interfaces in Step 1.c to forward traffic to VRF1. For more information, refer to Section 13.11.4, "Configuring a VRF Interface".

e. Enable BGP and configure the following parameters:

Parameter	Value
Autonomous System ID	100
Router ID	5.5.5.5

f. Enable the router as a BGP route reflector and set the cluster ID to **5.5.5.5**. For more information, refer to Section 13.8.11.2, "Configuring the Device as a Route Reflector".

g. Define an IPv4 address family for VRF1 with the following neighbors:

- **Neighbor 1.1.1.1**

Parameter	Value
Neighbor IP Address	1.1.1.1
Autonomous System ID	100
Route Reflector Client	Enabled

- **Neighbor 1.1.2.2**

Parameter	Value
Neighbor IP Address	1.1.2.2
Autonomous System ID	100
Route Reflector Client	Enabled

For more information, refer to Section 13.11.10.2, "Adding an IPv4 Address Family".

h. Define a redistribution metric for IPv4 family of type `connected`. For more information, refer to Section 13.11.11.2, "Adding a Redistribution".

2. **Configure R1**

a. Enable BGP and configure the following parameters:

Parameter	Value
Autonomous System ID	100
Router ID	5.5.5.1

For more information, refer to Section 13.8.1, "Configuring BGP".

b. Define the following BGP neighbor:

Parameter	Value
Neighbor IP Address	1.1.1.2
Autonomous System ID	100

For more information, refer to Section 13.8.6.2, "Adding a Neighbor".

c. Define a redistribution metric for BGP of type `connected`. For more information, refer to Section 13.8.10.2, "Adding a Redistribution Metric".

3. **Configure R2**

a. Enable BGP and configure the following parameters:

Parameter	Value
Autonomous System ID	100
Router ID	5.5.5.2

For more information, refer to Section 13.8.1, "Configuring BGP".

b. Define the following BGP neighbors:

- **Neighbor 1.1.2.1**

Parameter	Value
Neighbor IP Address	1.1.2.1
Autonomous System ID	100

- **Neighbor 1.1.3.2**

Parameter	Value
Neighbor IP Address	1.1.3.2
Autonomous System ID	101

For more information, refer to Section 13.8.6.2, "Adding a Neighbor".

c. Define a redistribution metric for BGP of type `connected`. For more information, refer to Section 13.8.10.2, "Adding a Redistribution Metric".

4. **Configure R3**

a. Enable BGP and configure the following parameters:

Parameter	Value
Autonomous System ID	101
Router ID	5.5.5.3

For more information, refer to Section 13.8.1, "Configuring BGP".

b. Define the following BGP neighbor:

Parameter	Value
Neighbor IP Address	1.1.3.1
Autonomous System ID	101

For more information, refer to Section 13.8.6.2, "Adding a Neighbor".

c. Define a redistribution metric for BGP of type `connected`. For more information, refer to Section 13.8.10.2, "Adding a Redistribution Metric".

» Verification

Verify the configuration by navigating to ***routing » status » bgp » route*** on R1. The following routes should be displayed:

```
                                                    LOCAL              AS
NETWORK       ADDRESS      SELECTED  INTERNAL  METRIC  PREFERENCE  WEIGHT  PATH  ORIGIN
-------------------------------------------------------------------------------------------
1.1.1.0/30
     1.1.1.2           true      true      0       100         0             Unspecified
```

```
1.1.2.0/30
     1.1.1.2           true      true      0       100         0             Unspecified
1.1.3.0/30
     1.1.2.2           true      true      0       100         0             Unspecified
```

» Final Configuration Example

RR Configuration

```
global
 vrf
  definition vrf1
   rd 100:1
   route-target both 100:1
ip fe-1-1
 vrf-forwarding vrf1
 ipv4
  address 1.1.1.2/30
ip fe-1-2
 vrf-forwarding vrf1
 ipv4
  address 1.1.2.1/30
routing bgp
 enabled
 as-id               100
 router-id           5.5.5.5
 route-reflector enabled
 route-reflector cluster-id 5.5.5.5
 address-family ipv4
  vrf vrf1
   redistribute connected
   neighbor 1.1.1.1
    remote-as 100
    route-reflector-client enabled
   neighbor 1.1.2.2
    remote-as 100
    route-reflector-client enabled
```

R1 Configuration

```
routing bgp
 enabled
 as-id 100
 router-id 5.5.5.1
  neighbor 1.1.1.2
    remote-as 100
 redistribute connected
```

R2 Configuration

```
routing bgp
 enabled
 as-id 100
 router-id 5.5.5.2
  neighbor 1.1.2.1
    remote-as 100
  neighbor 1.1.3.2
    remote-as 101
 redistribute connected
```

R3 Configuration

```
routing bgp
 enabled
 as-id 100
 router-id 5.5.5.3
  neighbor 1.1.3.1
    remote-as 100
 redistribute connected
```

Section 13.8.11.8

Example: Route Reflection with VPNv4 Clients

BGP route reflection can be used to advertise VPNv4 routes between Provider Edge (PE) devices inside a provider network. This specific application is complicated by the fact that VPNv4 routes to the Customer Edge (CE) devices are within VRFs that are not known to the global VRF shared by each PE device.

For more information about configuring this type of topology, refer to the application description *Using BGP Route Reflection with VPNv4 Clients [https://support.industry.siemens.com/cs/ww/en/view/109757209]*.

Section 13.8.12

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.

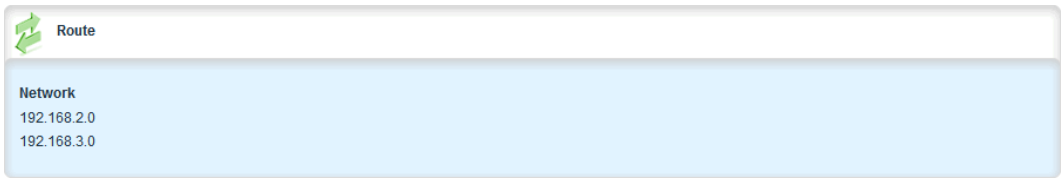


Figure 816: Route Table

The **Route** table provides the following information:

Parameter	Description
Network	**Synopsis:** 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.

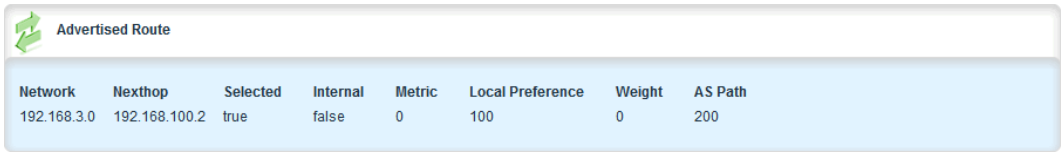


Figure 817: Advertised Route Table

The **Advertised Route** table provides the following information:

Parameter	Description
Network	**Synopsis:** A string Network.
Nexthop	**Synopsis:** A string Next-hop address.
Selected	**Synopsis:** { true, false } Selected next-hop for this route.
Internal	**Synopsis:** { true, false } Internal route.
Metric	**Synopsis:** A 32-bit signed integer Metric value.
Local Preference	**Synopsis:** A string Local preference.
Weight	**Synopsis:** A 32-bit signed integer Weight.
AS Path	**Synopsis:** A string Path.
Origin	**Synopsis:** A string

Parameter	Description
	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 13.8.1, "Configuring BGP".

Section 13.8.13
Resetting a BGP Session

Whenever there is a change in the routing policy due to a configuration change, the BGP session must be reset for the new policy to take effect.

RUGGEDCOM ROX II allows users to perform either a hard or soft reset on both incoming and outbound sessions, as selected.

A BGP session can be reset for all routing tables, or for a specified neighbor.

» Resetting All BGP Sessions

To reset all BGP sessions, do the following:

1. Navigate to ***routing » dynamic » bgp » all-peers-reset***. The **Reset All Peer Sessions** and **Trigger Action** forms appear.

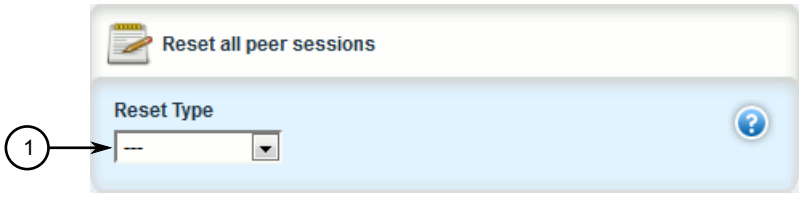


Figure 818: Reset All Peer Sessions Form

1. Reset Type Options

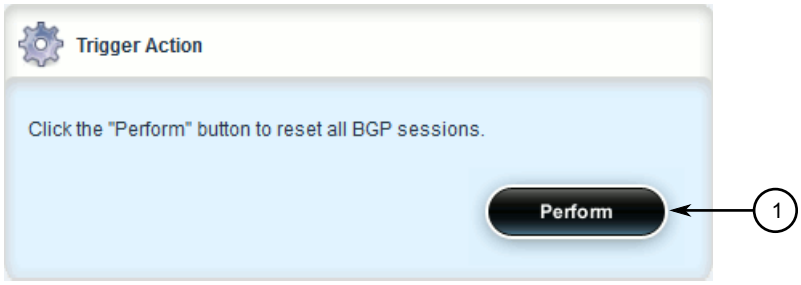


Figure 819: Trigger Action Form

1. Perform Button

2. Configure the following parameter(s) as required:

Parameter	Description
Reset Type	**Synopsis:** { hard, soft-inbound, soft-outbound, soft } The method for resetting all BGP peering sessions. Options include: • hard: Tears down and re-establishes all BGP sessions. • soft: The existing peering sessions continue to run while running both inbound and outbound actions. • soft-inbound: The existing peering sessions continue to run while generating inbound updates from all neighbors. • soft-outbound: The existing peering sessions continue to run while sending outbound updates to all neighbors.

3. On the **Trigger Action** form, click **Perform** to reset all BGP sessions as configured.

» Resetting a BGP Session for a Specified Neighbor

To reset a BGP session for a specified neighbor, do the following:

1. Navigate to ***routing » dynamic » bgp » neighbor » {ip address} » peer-reset***, where *{ip address}* is the ip address of the neighbor. The **Reset the Peer Session** and **Trigger Action** forms appear.

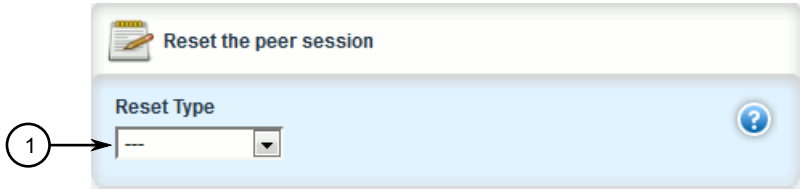


Figure 820: Reset the Peer Session Form

1. Reset Type Options

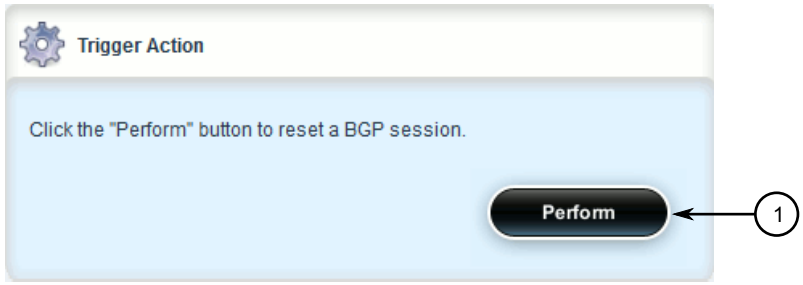


Figure 821: Trigger Action Form

1. Perform Button

2. Configure the following parameter(s) as required:

Parameter	Description
Reset Type	**Synopsis:** { hard, soft-inbound, soft-outbound, soft } The method for resetting the selected BGP peering session. Options include: • hard: Tears down the existing peering session then re-establishes it.

Parameter	Description
	• soft: The existing peering session continues to run while running both inbound and outbound actions. • soft-inbound: The existing peering session continues to run while generating inbound updates from its neighbor. • soft-outbound: The existing peering session continues to run while sending outbound updates to its neighbor.

3. On the **Trigger Action** form, click **Perform** to reset the peer session for the selected neighbor.

Section 13.9
Managing OSPF

The Open Shortest Path First (OSPF) protocol determines the best path for routing IP traffic over a TCP/IP network based on link cost and quality. Unlike static routing, OSPF takes link failures and other network topology changes into account. OSPF also differs from RIP in that it provides less router to router update traffic.

The RUGGEDCOM ROX II OSPF daemon (ospfd) is an RFC 2178 [http://tools.ietf.org/html/rfc2178] compliant implementation of OSPF version 2. The daemon also adheres to the Opaque LSA (RFC 2370 [http://tools.ietf.org/html/rfc2370]) and ABR-Types (RFC 3509 [http://tools.ietf.org/html/rfc3509]) extensions.

OSPF network design usually involves partitioning a network into a number of self-contained areas. The areas are chosen to minimize intra-area router traffic, making more manageable and reducing the number of advertised routes. Area numbers are assigned to each area. All routers in the area are known as Area routers. If traffic must flow between two areas a router with links in each area is selected to be an Area Border router, and serves as a gateway.

NOTE
*The **Router ID** parameter defines the ID of the router. By default this is the highest IP assigned to the router. It is recommended to configure this value manually to avoid the ID changing if interfaces are added or deleted from the router. During elections for the master router, the ID is one of the values used to pick the winner. Keeping the ID fixed will avoid any unexpected changes in the election of the master router.*

NOTE
In complex legacy networks, RIP, OSPF, BGP and IS-IS may all be active on the same router at the same time. Typically, however, only one dynamic routing protocol is employed at one time.

NOTE
Specific routes for Virtual Routing and Forwarding (VRF) interfaces can be configured. For more information about VRF, refer to Section 13.11, "Managing Virtual Routing and Forwarding (VRF)".

CONTENTS

Section 13.9.1
OSPF Concepts

When an OSPF configured router starts operating, it issues a *hello* packet. Routers having the same OSPF Area, hello-interval and dead-interval timers will communicate with each other and are said to be neighbors.

After discovering its neighbors, a router will exchange Link State Advertisements in order to determine the network topology.

Every 30 minutes (by default), the entire topology of the network must be sent to all routers in an area.

If the link speeds are too low, the links are too busy or there are too many routes, some routes may fail to get re-announced and will be aged out.

Splitting the network into smaller areas to reduce the number of routes within an area or reducing the number of routes to be advertised may help to avoid this problem.

In shared access networks (i.e. routers connected by switches or hubs) a designated router and a backup designated are elected to receive route changes from subnets in the area. Once a designated router is picked, all routing state changes are sent to the designated router, which then sends the resulting changes to all the routers.

The election is decided based on the priority assigned to the interface of each router. The highest priority wins. If the priority is tied, the highest router-id wins.

Section 13.9.2
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.

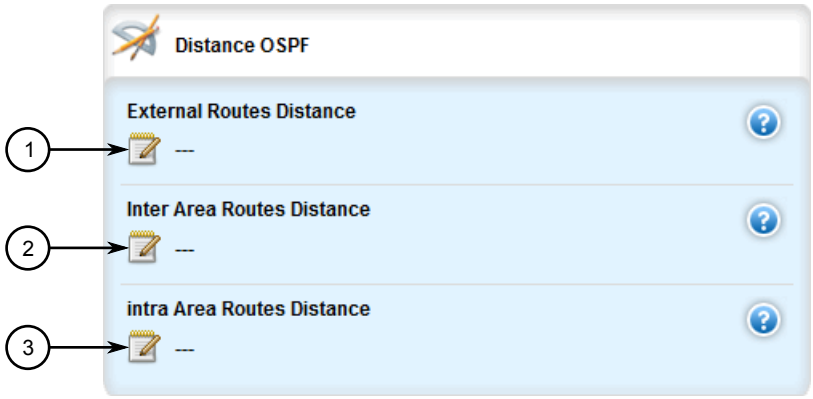


Figure 822: Distance OSPF Form

1. External Routes Distance Box **2.** Inter Area Routes Distance Box **3.** Intra Area Routes Distance Box

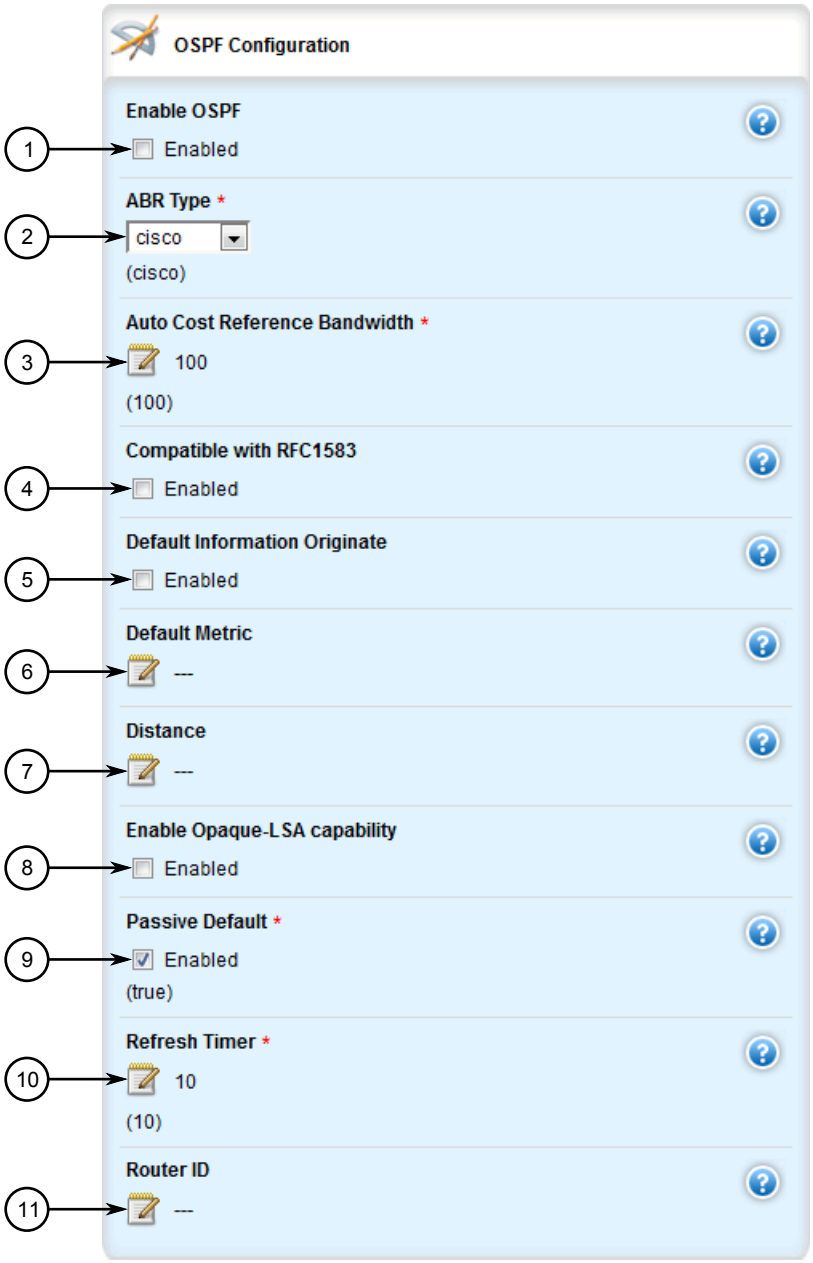


Figure 823: OSPF Configuration Form

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	**Synopsis:** A 32-bit unsigned integer between 1 and 255 The administrative distance for external routes.

Parameter	Description
Inter Area Routes Distance	**Synopsis:** A 32-bit unsigned integer between 1 and 255 The administrative distance for inter-area routes.
intra Area Routes Distance	**Synopsis:** A 32-bit unsigned 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	Enables the OSPF dynamic routing protocol.
ABR Type	**Synopsis:** { cisco, ibm, shortcut, standard } **Default:** cisco The OSPF ABR type.
Auto Cost Reference Bandwidth	**Synopsis:** A 32-bit unsigned integer between 1 and 4294967 **Default:** 100 Calculates the OSPF interface cost according to bandwidth [1-4294967 Mbps]
Compatible with RFC1583	Enables the compatibility with the obsolete RFC1583 OSPF (the current is RFC2178)
Default Information Originate	Advertises the default route.
Default Metric	**Synopsis:** A 32-bit unsigned integer between 0 and 16777214 The default metric of redistribute routes.
Distance	**Synopsis:** A 32-bit unsigned integer between 1 and 255 The administrative distance.
Enable Opaque-LSA capability	Enables the Opaque-LSA capability (RFC2370).
Passive Default	**Synopsis:** { true, false } **Default:** true Default passive value for new interface.
Refresh Timer	**Synopsis:** A 16-bit unsigned integer between 10 and 1800 **Default:** 10 The refresh timer.
Router ID	**Synopsis:** 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.

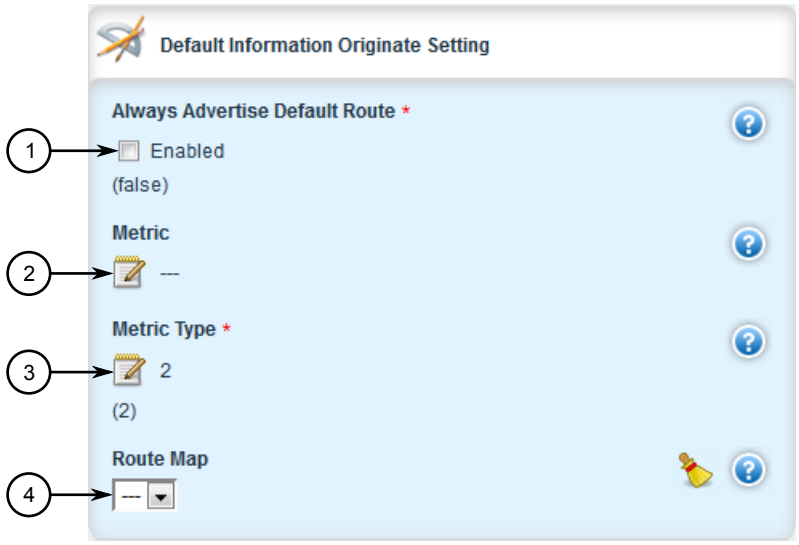


Figure 824: Default Information Originate Form

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	**Synopsis:** { true, false } **Default:** false Always advertise default route even when there is no default route present in routing table.
Metric	**Synopsis:** A 32-bit unsigned integer between 0 and 16777214 The metric value for default route.
Metric Type	**Synopsis:** An 8-bit signed integer between 1 and 2 **Default:** 2 The metric type for default route.
Route Map	**Synopsis:** A string The route map name.

7. Configure prefix list filters. For more information, refer to Section 13.9.4.3, "Adding a Prefix List".
8. Configure areas. For more information, refer to Section 13.9.5.2, "Adding an Area".
9. Configure route map filters. For more information, refer to Section 13.9.6.3, "Adding a Route Map Filter".
10. Configure redistribution metrics. For more information, refer to Section 13.9.8.2, "Adding a Redistribution Metric".
11. Configure interfaces. For more information, refer to Section 13.9.9.2, "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 13.9.3

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.

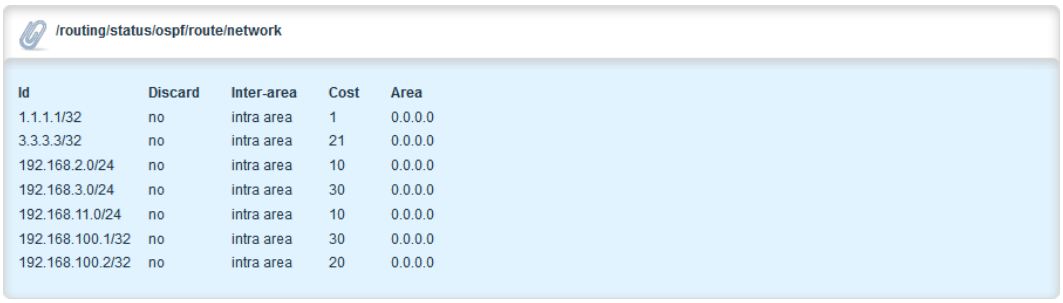


Figure 825: Network Table

The **Network** table provides the following information:

Parameter	Description
Network Prefix	**Synopsis:** A string Network Prefix.
destination	**Synopsis:** A string Destination (network or discard).
Path Type	**Synopsis:** A string Path type (inter-area or intra-area).
cost	**Synopsis:** A string Cost.
area	**Synopsis:** A string Area.

If no dynamic OSPF routes have been configured, configure OSPF and add routes as needed. For more information about configuring OSPF, refer to Section 13.9.2, "Configuring OSPF".

Section 13.9.4

Managing Prefix Lists and Entries

Neighbors can be associated with prefix lists, which allow the OSPF daemon to filter incoming or outgoing routes based on the *allow* and *deny* entries in the prefix list.

CONTENTS

Section 13.9.4.1
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.

Figure 826: Prefix List Table

If no prefix lists have been configured, add lists as needed. For more information, refer to Section 13.9.4.3, "Adding a Prefix List".

Section 13.9.4.2
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.

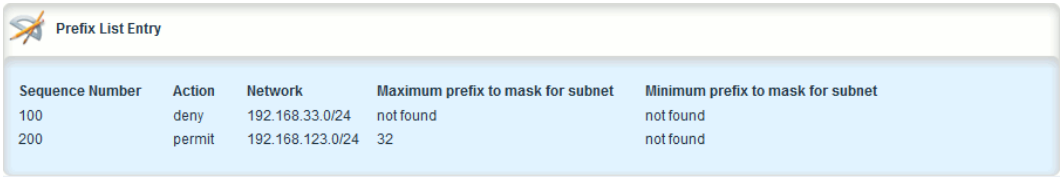


Figure 827: Prefix List Entry Table

If no entries have been configured, add entries as needed. For more information, refer to Section 13.9.4.4, "Adding a Prefix Entry".

Section 13.9.4.3
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.

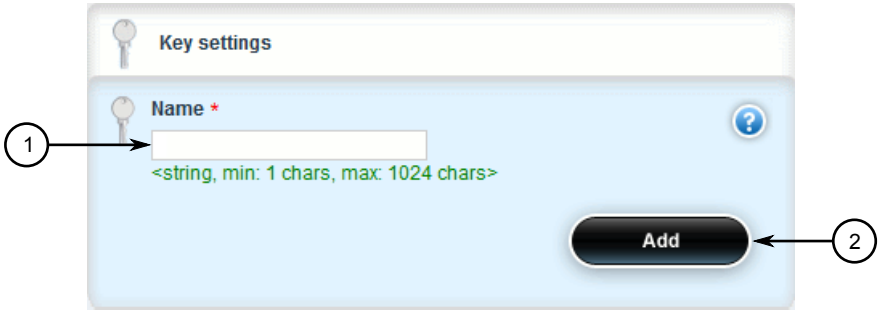


Figure 828: Key Settings Form

1. Name Box **2.** Add Button

4. Configure the following parameter(s) as required:

Parameter	Description
Name	**Synopsis:** 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.

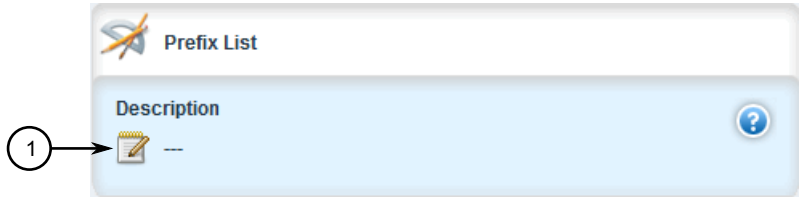


Figure 829: Prefix List Form

1. Description Box

6. Configure the following parameter(s) as required:

Parameter	Description
Description	**Synopsis:** 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 13.9.4.4, "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 13.9.4.4
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.

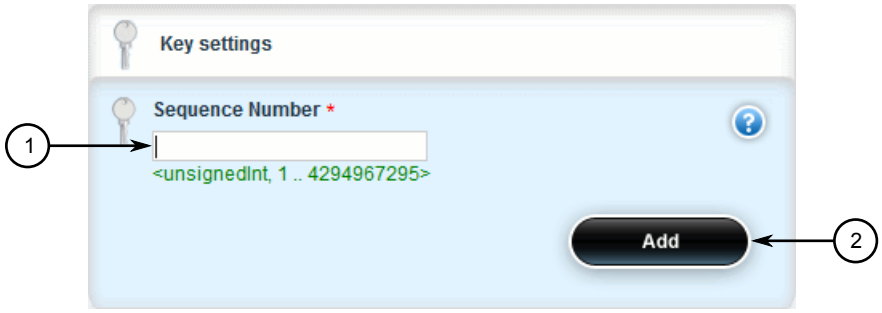


Figure 830: Key Settings Form

1. Sequence Number Box **2.** Add Button

4. Configure the following parameter(s) as required:

Parameter	Description
Sequence Number	**Synopsis:** A 32-bit unsigned integer between 1 and 4294967295 Sequence number of the entry.

5. Click **Add** to create the new entry. The **Prefix List Entry** form appears.

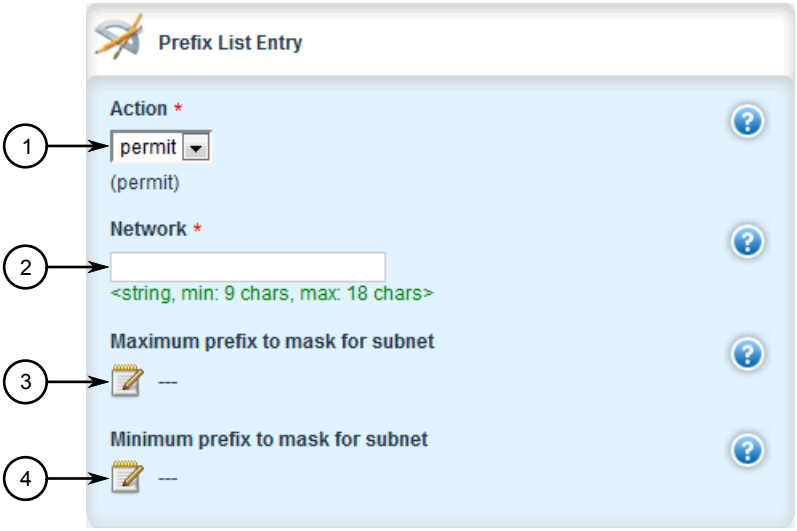


Figure 831: Prefix List Entry Form

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	**Synopsis:** { deny, permit } **Default:** permit Action.
Network	**Synopsis:** A string 9 to 18 characters long

Parameter	Description
	Network (xxx.xxx.xxx.xxx/xx). This parameter is mandatory.
Maximum prefix to mask for subnet	**Synopsis:** An 8-bit unsigned integer between 1 and 32 The maximum prefix length to match ipaddress within subnet.
Minimum prefix to mask for subnet	**Synopsis:** An 8-bit unsigned 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 13.9.4.5
Deleting a Prefix List

To delete 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

   The **Prefix List** table appears.

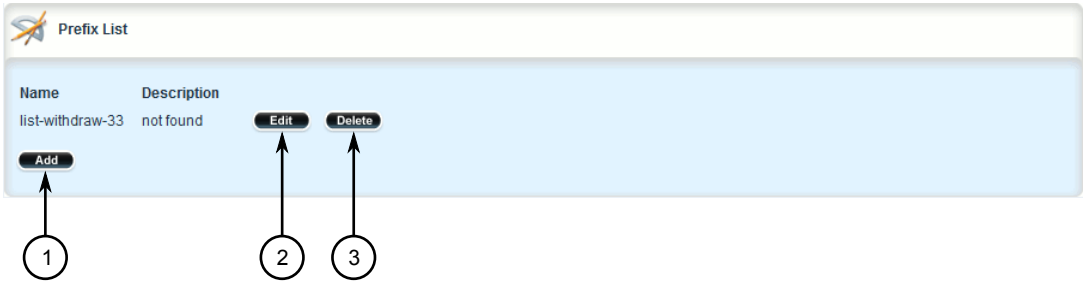


Figure 832: Prefix List Table

1. Add Button **2.** Edit Button **3.** Delete Button

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 13.9.4.6
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.

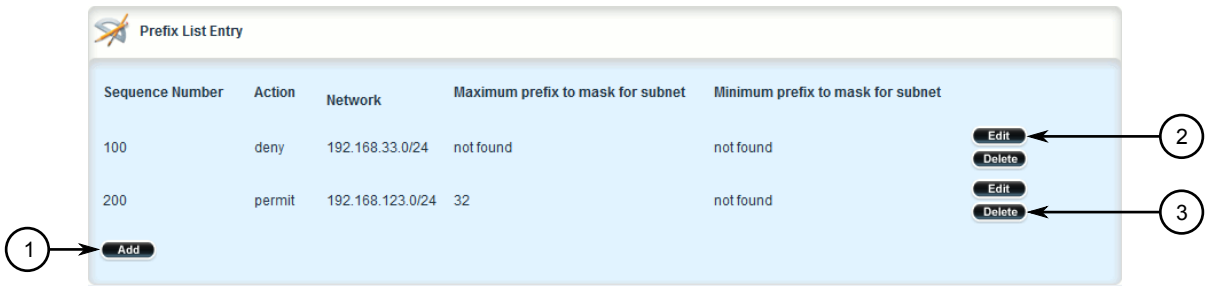


Figure 833: Prefix List Entry Table

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 13.9.5
Managing Areas

Network areas determine the regions within which routes are distributed to other routers. The subnets at a particular router can be added to its OSPF Area. The router will advertise these subnets to all routers in its area.

OSPF areas must be designed such that no single link failure will cause the network to be split into two disjointed networks.

A router can be part of multiple areas and function as a gateway between areas. When multiple areas are used on a network, area zero (0) is the backbone area. All areas must have a router connecting them to area zero (0).

CONTENTS

Section 13.9.5.1
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.

Figure 834: OSPF Area Table

If no areas have been configured, add areas as needed. For more information, refer to Section 13.9.5.2, "Adding an Area".

Section 13.9.5.2
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.

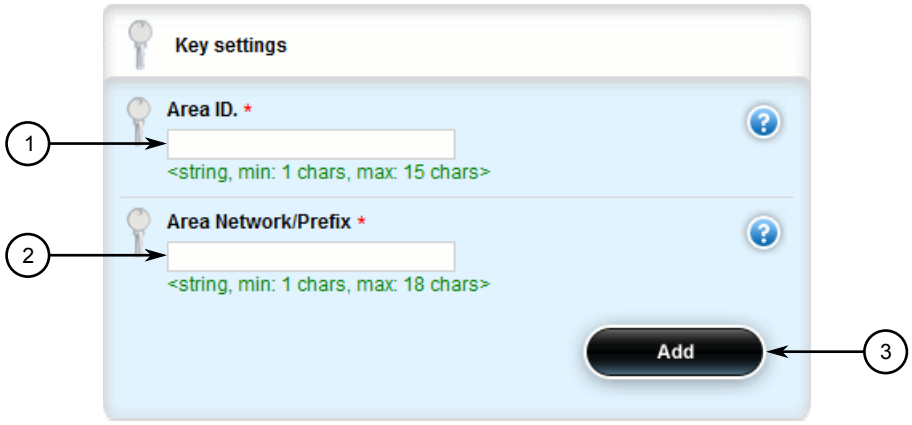


Figure 835: Key Settings Form

1. Area ID Box **2.** Area Network/Prefix Box **3.** Add Button

4. Configure the following parameter(s) as required:

Parameter	Description
Area ID	**Synopsis:** A string 7 to 15 characters long The OSPF Area ID (format: A.B.C.D).
Area Network/Prefix	**Synopsis:** 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.

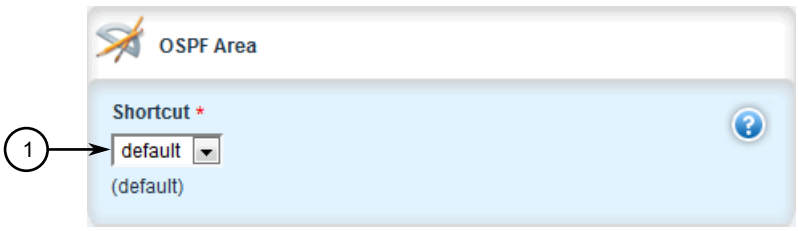


Figure 836: OSPF Area Form

1. Shortcut List

6. Configure the following parameter(s) as required:

Parameter	Description
shortcut	**Synopsis:** { default, disable, enable } **Default:** default Sets the area's shortcutting mode. Options include:

Parameter	Description
	• Default: If the Area Border Router (ABR) has an active backbone connection, the area is not used for shortcutting and a new bit (S-bit) is not set by the ABR in the router-LSA originated for the area. The opposite is true if the ABR does not have an active backbone connection. • Enable: If the ABR has an active backbone connection, it sets the new bit (S-bit) in the router-LSA originated for the area and uses it for shortcutting. Other ABRs in the area must also report the new bit. However, if the ABR does not have an active backbone connection, it uses the area unconditionally for shortcutting and sets the new bit in the router-LSA originated for the area. • Disable: The ABR does not use this area for shortcutting, or set the new bit (S-bit) in the router-LSA originated for it.

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 13.9.5.3
Deleting an Area

To delete 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

   The **OSPF Area** table appears.

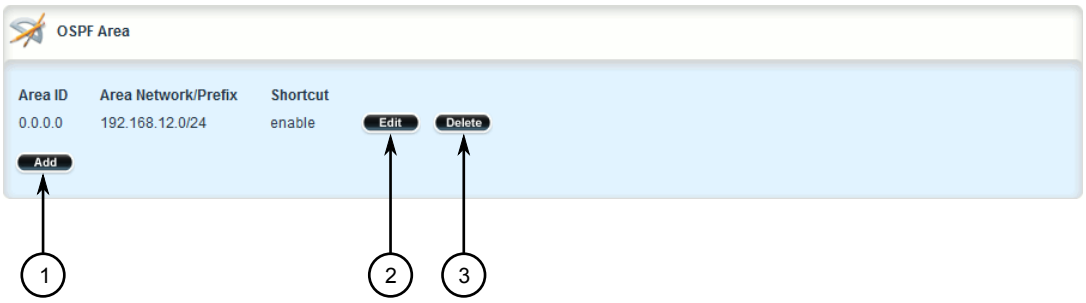


Figure 837: OSPF Area Table

1. Add Button **2.** Edit Button **3.** Delete Button

3. 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 13.9.6

Managing Route Maps

Route maps are sequential statements used to filter routes that meet the defined criteria. If a route meets the criteria of the applied route map, it can either be excluded from the routing table or prevented from being redistributed. In RUGGEDCOM ROX II, route maps are configured to filter routes based on their metric value, which defines the cost of the route. Once a match is found, the assigned action is taken.

Each route map requires a sequence number (e.g. 10, 20, 30, etc.), which allows for multiple route maps to be run in sequence until a match is found. It is recommended to create sequence numbers in intervals of 10, in case a new route map is required later between two existing route maps.

CONTENTS

Section 13.9.6.1

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.

Figure 838: Route Map Table

If no filters have been configured, add filters as needed. For more information, refer to Section 13.9.6.3, "Adding a Route Map Filter".

Section 13.9.6.2
Viewing a List of Route Map Filter Entries

To view a list of entries for a route map filter for either OSPF, 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.

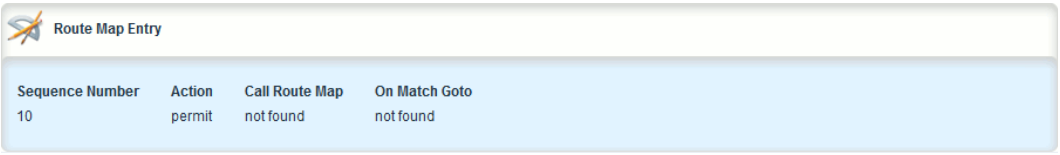


Figure 839: Route Map Entry Table

If no filters have been configured, add filters as needed. For more information, refer to Section 13.9.6.4, "Adding a Route Map Filter Entry".

Section 13.9.6.3
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.

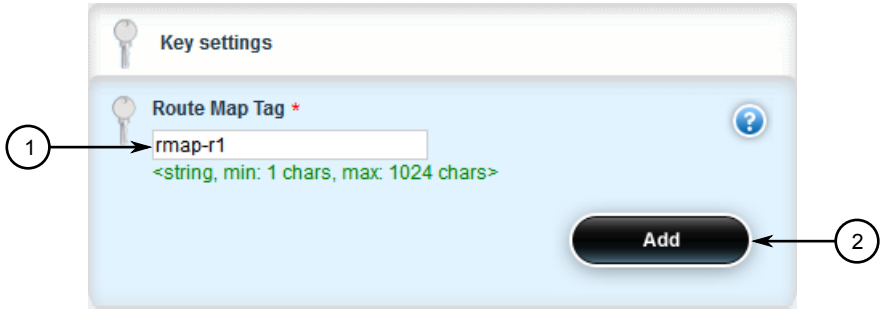


Figure 840: Key Settings Form

1. Route Map Tag Box **2.** Add Button

4. Configure the following parameter(s) as required:

Parameter	Description
Route Map Tag	**Synopsis:** 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 13.9.6.4, "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 13.9.6.4

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.

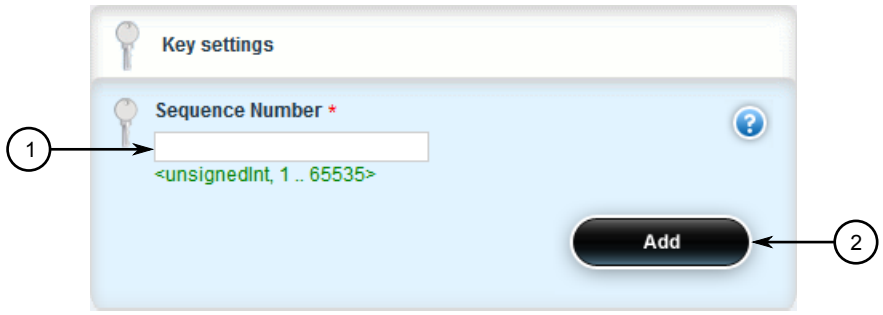


Figure 841: Key Settings Form

1. Sequence Number Box **2.** Add Button

4. Configure the following parameter(s) as required:

Parameter	Description
Sequence Number	**Synopsis:** A 32-bit unsigned 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.

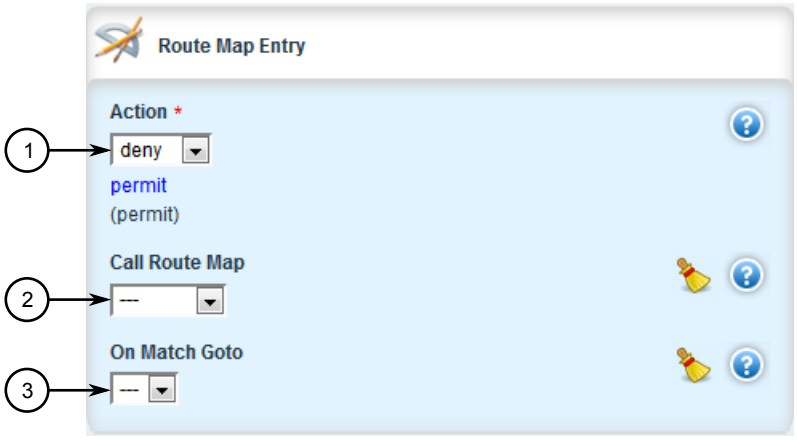


Figure 842: Route Map Entry Form

1. Action List **2.** Call Route Map List **3.** On Match Goto List

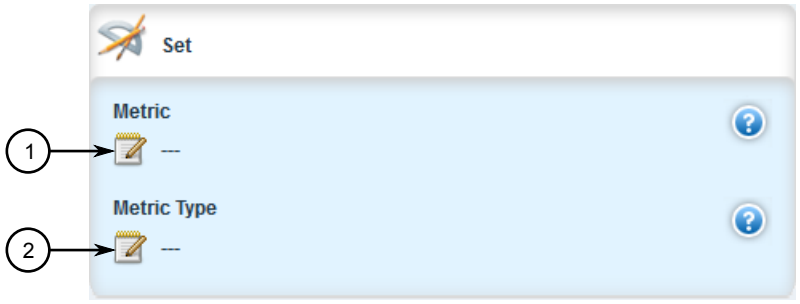


Figure 843: Set Form

1. Metric Box **2.** Metric Type Box

6. On the **Route Map Entry** form, configure the following parameter(s) as required:

Parameter	Description
Action	**Synopsis:** { deny, permit } **Default:** permit Action.
Call Route Map	**Synopsis:** A string Jump to another route-map after match+set.
On Match Goto	**Synopsis:** A string Go to this entry on match.

7. On the **Set** form, configure the following parameter(s) as required:

Parameter	Description
Metric	**Synopsis:** A 32-bit unsigned integer Metric value.
Metric Type	**Synopsis:** An 8-bit signed integer between 1 and 2 External route type.

8. Configure the match rules for the route map filter. For more information, refer to Section 13.9.6.7, "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 13.9.6.5

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.

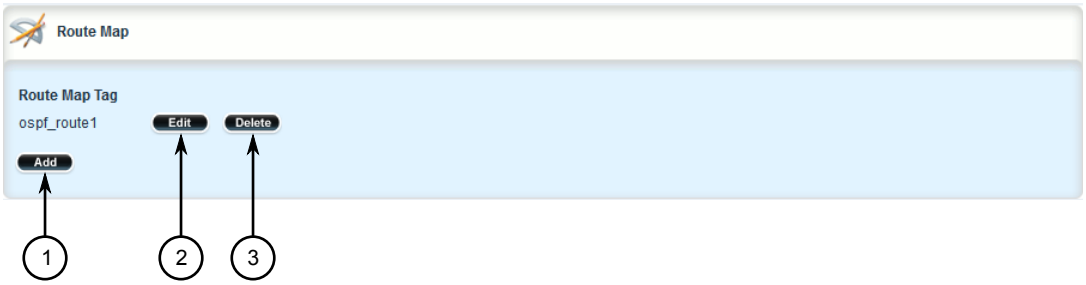


Figure 844: Route Map Table

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 13.9.6.6

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.

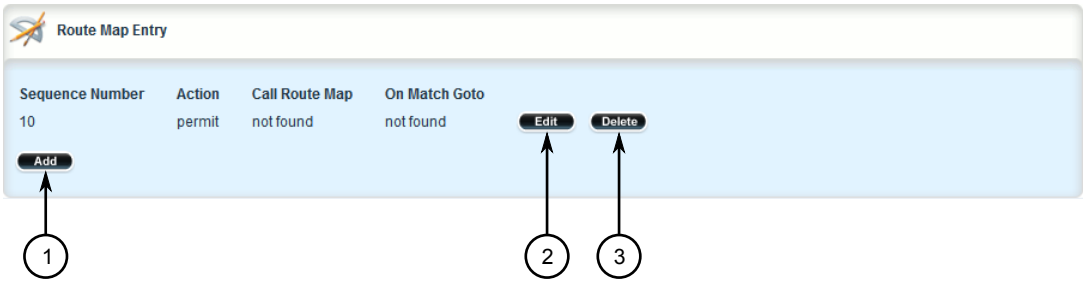


Figure 845: Route Map Entry Table

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 13.9.6.7

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 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.

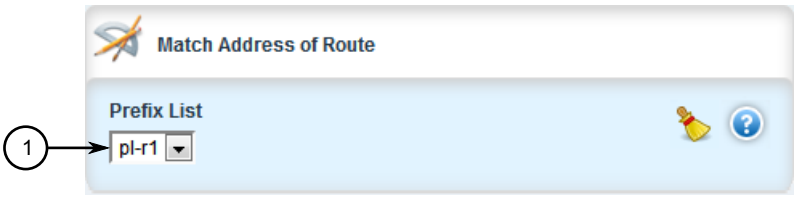


Figure 846: Match Address of Route Form

1. Prefix List List

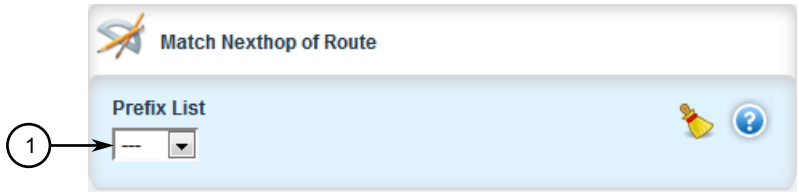


Figure 847: Match Nexthop of Route Form

1. Prefix List List

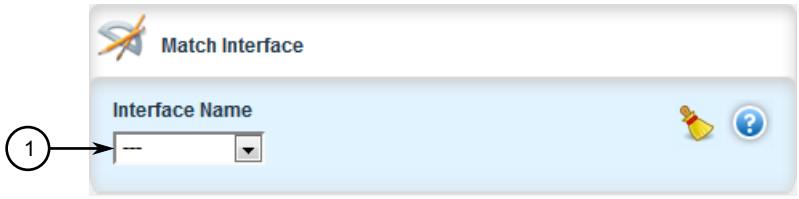


Figure 848: Match Interface Form

1. Interface Name List

3. On the **Match Address of Route** form, configure the following parameters as required:

Parameter	Description
Prefix List	**Synopsis:** A string The prefix list name.

4. On the **Match Nexthop of Route** form, configure the following parameters as required:

Parameter	Description
Prefix List	**Synopsis:** A string The prefix list name.

5. On the **Match** form, configure the following parameters as required:

Parameter	Description
Interface Name	**Synopsis:** A string The interface 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 13.9.7

Managing Incoming Route Filters

Incoming route advertisements can be filtered by assigning one or route map filters. This can be useful for excluding specific OSPF routes from the routing table.

NOTE
For more information about route map filters, refer to Section 13.9.6, "Managing Route Maps".

CONTENTS

Section 13.9.7.1

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 849: Incoming Route Filter Table

If no route filters have been configured, add filters as needed. For more information, refer to Section 13.9.7.2, "Adding an Incoming Route Filter".

Section 13.9.7.2

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 13.9.6, "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.

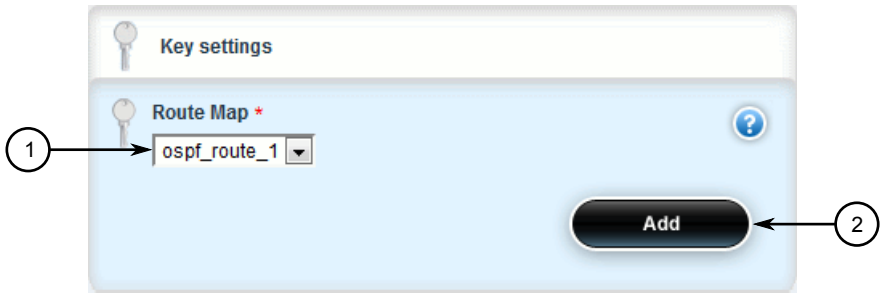


Figure 850: Key Settings Form

1. Route Map List **2.** Add Button

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 13.9.7.3

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.

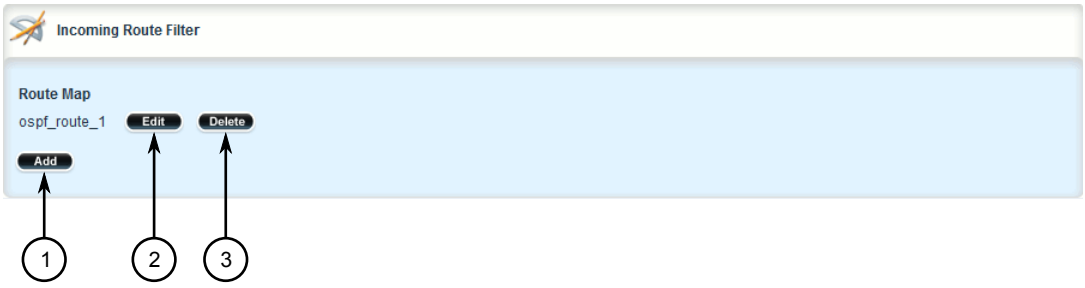


Figure 851: Incoming Route Filter Table

1. Add Button **2.** Edit Button **3.** Delete Button

3. Click **Delete** next to the chosen incoming route 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 13.9.8

Managing Redistribution Metrics

Redistribution metrics redistribute routing information from other routing protocols, static routes or routes handled by the kernel. Routes for subnets that are directly connected to the router, but not part of the OSPF areas, can also be advertised.

CONTENTS

Section 13.9.8.1

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.

Figure 852: Redistribute Route from Other Protocols Table

If no redistribution metrics have been configured, add metrics as needed. For more information, refer to Section 13.9.8.2, "Adding a Redistribution Metric".

Section 13.9.8.2
Adding a Redistribution Metric

To add a redistribution metric 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 » 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.

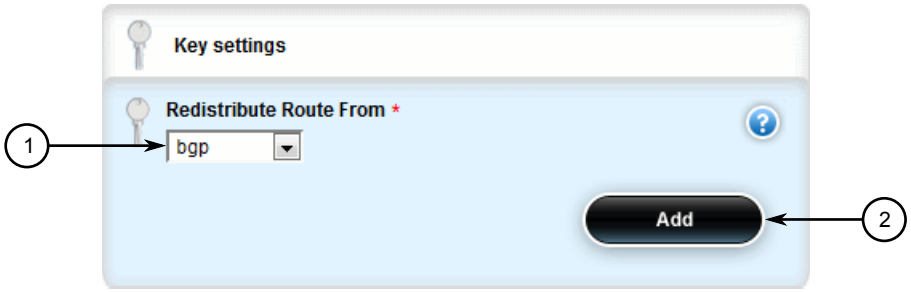


Figure 853: Key Settings Form

1. Redistribute Route From List **2.** Add Button

4. Configure the following parameter(s) as required:

Parameter	Description
Redistribute Route From	**Synopsis:** { kernel, static, connected, rip, bgp } Redistributes the route type.

5. Click **Add** to add the metric. The **Redistribute From Other Routing Protocols** form appears.

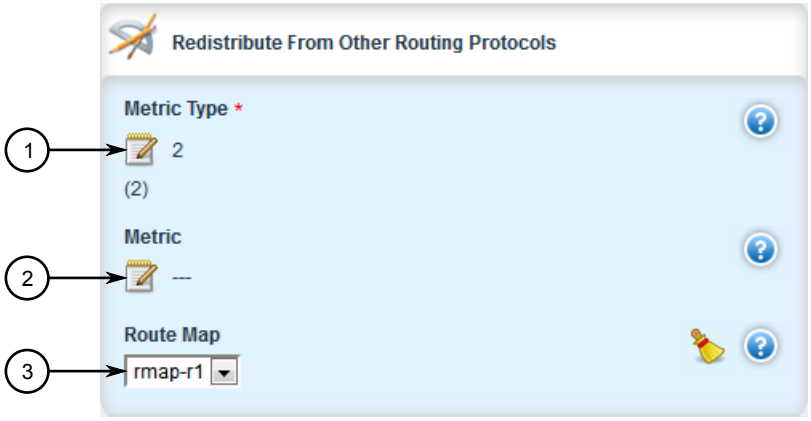


Figure 854: Redistribute From Other Routing Protocols Form

1. Metric Type Box **2.** Metric Box **3.** Route Map List

6. Configure the following parameter(s) as required:

Parameter	Description
Metric Type	**Synopsis:** An 8-bit signed integer between 1 and 2 **Default:** 2 The OSPF exterior metric type for redistributed routes.
Metric	**Synopsis:** A 32-bit unsigned integer between 0 and 16777214 The metric for redistributed routes.
Route Map	**Synopsis:** A string 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 13.9.8.3
Deleting a Redistribution Metric

To delete a redistribution metric 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 » 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.

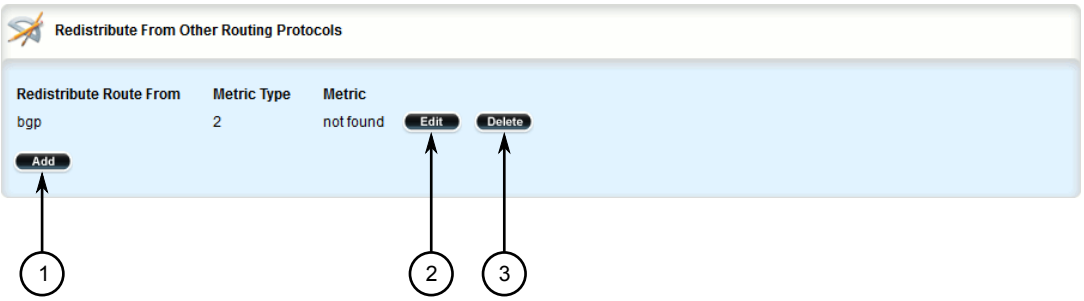


Figure 855: Redistribute From Other Routing Protocols Table

1. Add Button **2.** Edit Button **3.** Delete Button

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 13.9.9
Managing Routing Interfaces

This section describes how to manage interfaces for OSPF routes.

CONTENTS

Section 13.9.9.1
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.

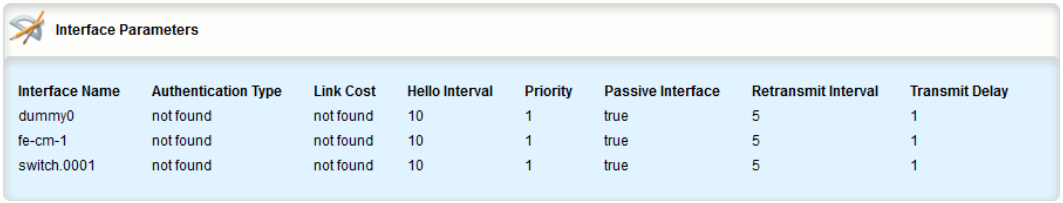


Figure 856: Interface Parameters Table

Section 13.9.9.2

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.

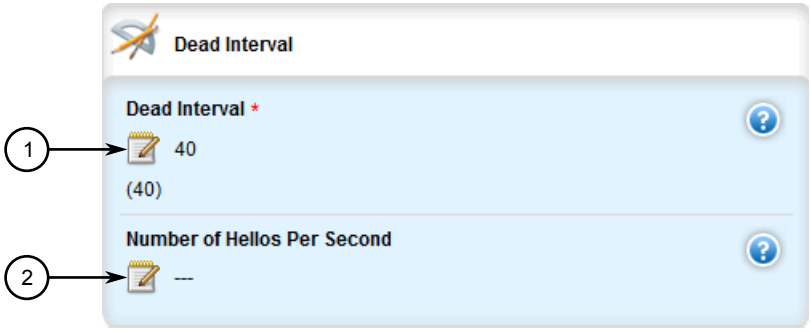


Figure 857: Dead Interval Form

1. Dead Interval Box **2.** Number of Hellos Per Second Box

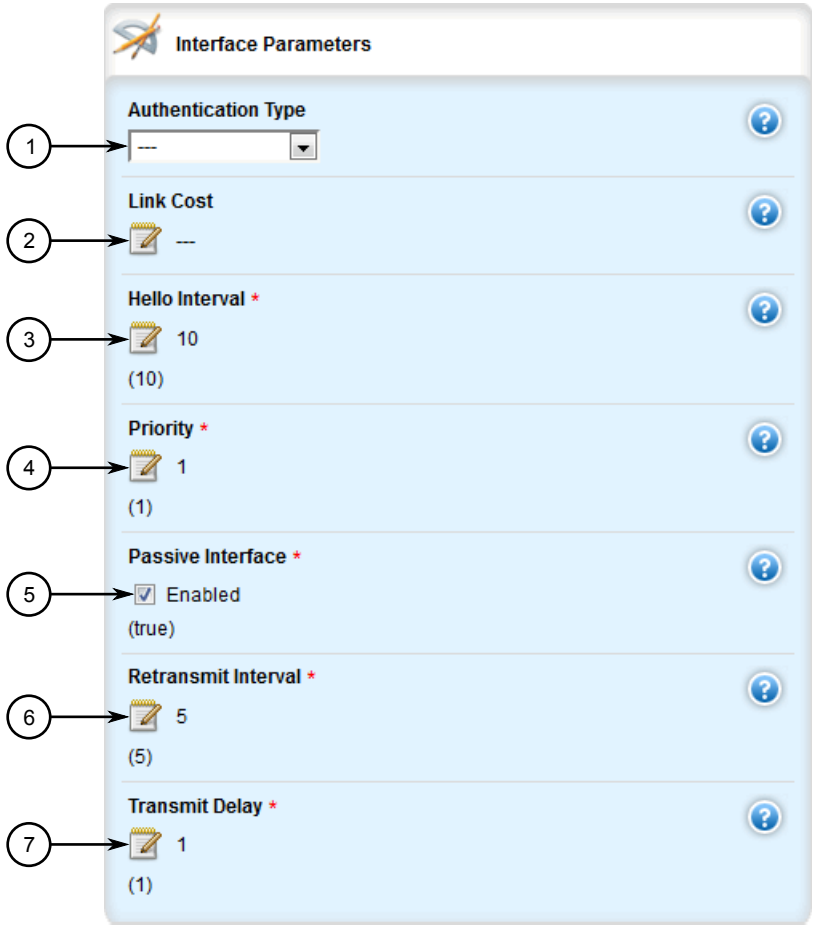


Figure 858: Interface Parameters Form

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

3. 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	**Synopsis:** A 32-bit unsigned integer between 1 and 65535 **Default:** 40 The time before considering a router dead (in seconds).
Number of Hellos Per Second	**Synopsis:** An 8-bit unsigned integer between 1 and 10 The number of times a hello message can be sent within one second.

4. 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 7.1.1, "Configuring Costing for Routable Interfaces".*

The default OSPF reference bandwidth for link cost calculations is 100 Mbit. The reference bandwidth divided by the link bandwidth gives the default cost for a link, which by default is 10. If a specific bandwidth is assigned to each link, the costs take this into account.

Link costs can be assigned manually under OSPF to each routable interface. This should be done when the speed of the link should not be used as the method for choosing the best link.

Parameter	Description
Interface Name	**Synopsis:** A string 1 to 32 characters long Interface name.
Authentication Type	**Synopsis:** { message-digest, null } The authentication type on this interface.
Link Cost	**Synopsis:** A 32-bit unsigned 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	**Synopsis:** A 32-bit unsigned integer between 1 and 65535 **Default:** 10 The time (in seconds) between sending hello packets.
priority	**Synopsis:** An 8-bit unsigned integer between 0 and 255 **Default:** 1 Priority of interface.
Passive Interface	**Synopsis:** { true, false } **Default:** true Whether an interface is active or passive. Passive interfaces do not send LSAs to other routers and are not part of an OSPF area.

Parameter	Description
Retransmit Interval	**Synopsis:** A 32-bit unsigned integer between 1 and 65535 **Default:** 5 Time (in seconds) between retransmitting lost link state advertisements.
Transmit Delay	**Synopsis:** A 32-bit unsigned integer between 1 and 65535 **Default:** 1 The link state transmit delay (in seconds).
Dead Interval	**Synopsis:** A 32-bit unsigned integer between 1 and 65535 **Default:** 40 The time before considering a router dead (in seconds).
Number of Hellos Per Second	**Synopsis:** An 8-bit unsigned integer between 1 and 10 The number of times a hello message can be sent within one second.

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 13.9.10

Managing Message Digest Keys

Message digest keys use the MD5 algorithm to authenticate OSPF neighbors and prevent unauthorized routers from joining the OSPF network. By enabling authentication and configuring a shared key on all the routers, only routers which have the same authentication key will be able to send and receive advertisements within the OSPF network.

An ID for each key allows the router to use multiple passwords and prevent replay attacks where OSPF packets are captured, modified and transmitted to a router. To change passwords, simply create a new key and delete the old key.

IMPORTANT!
The router can only share routing information with neighbors that use the same authentication method and password.

NOTE
Authentication adds a small overhead due to the encryption of messages. It is not recommended for completely private networks with controlled access.

CONTENTS

Section 13.9.10.1
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.

Figure 859: Message Digest Table

If no message digest keys have been configured, add keys as needed. For more information, refer to Section 13.9.10.2, "Adding a Message Digest Key".

Section 13.9.10.2
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.

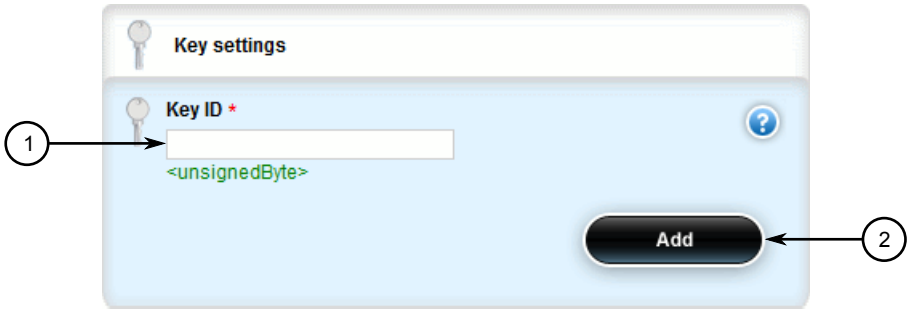


Figure 860: Key Settings Form

1. Key ID Box **2.** Add Button

4. Configure the following parameter(s) as required:

Parameter	Description
Key ID	**Synopsis:** An 8-bit unsigned integer between 0 and The key ID.
Password (key)	**Synopsis:** A string 1 to 1024 characters long The OSPF password (key). This parameter is mandatory.

5. Click **Add** to add the key. The **Message Digest** form appears.

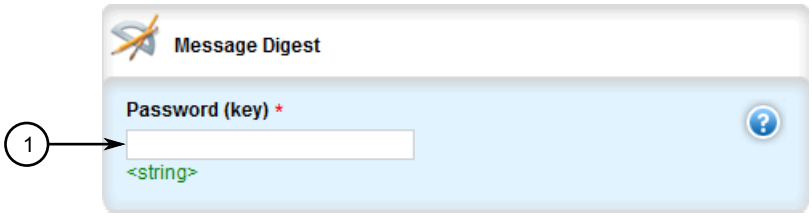


Figure 861: Message Digest Form

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 13.9.10.3

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.

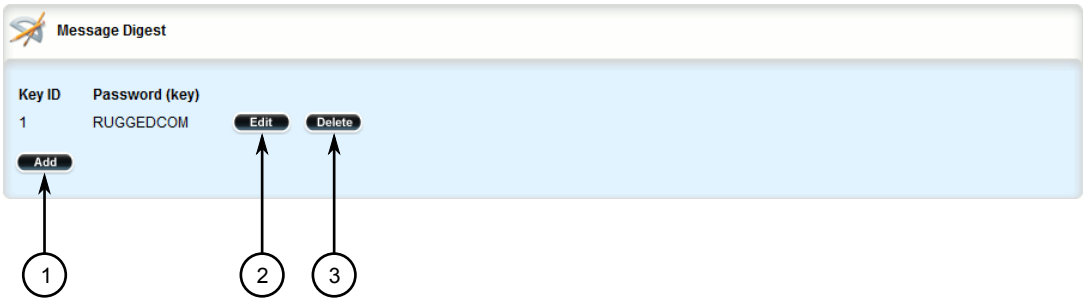


Figure 862: Message Digest Table

1. Add Button **2.** Edit Button **3.** Delete Button

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 13.10

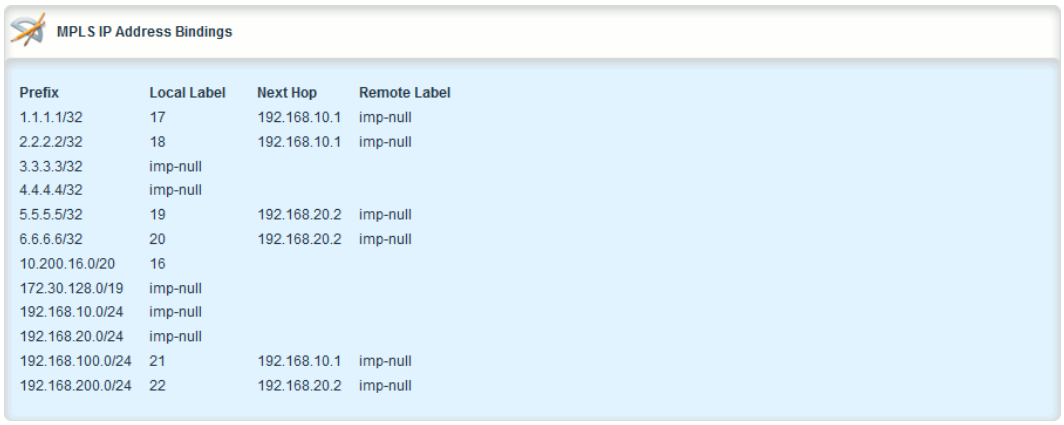
Managing MPLS

MPLS (Multi-Protocol Label Switching) operates between Layer 2 and Layer 3 of the OSI (Open Systems Interconnection) model and provides a mechanism to carry traffic for any network layer protocol. MPLS makes forwarding decisions based on labels where the labels are mapped to destination IP networks. MPLS traffic flows are connection-oriented, as they operate on pre-configured LSPs (Label Switch Paths) built based on the dynamic Label Distribution Protocol (LDP), or through static label bindings.

CONTENTS

Section 13.10.1
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.


MPLS IP Address Bindings

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 863: MPLS IP Address Bindings Table

This table provides the following information:

Parameter	Description
Prefix	**Synopsis:** A string The destination address prefix.
Local Label	**Synopsis:** A string The incoming (local) label.
Next Hop	**Synopsis:** A string The destination next hop router.
Remote Label	**Synopsis:** A string The remote label

Section 13.10.2
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.

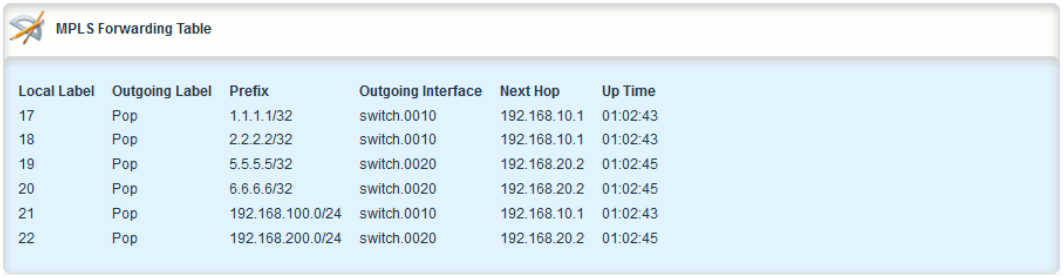


Figure 864: MPLS Forwarding Table

This table provides the following information:

Parameter	Description
Local Label	**Synopsis:** A string The incoming (local) label
Outgoing Label	**Synopsis:** A string The outgoing (remote) label.
Prefix	**Synopsis:** A string The destination address prefix.
Outgoing Interface	**Synopsis:** A string The outgoing interface.
Next Hop	**Synopsis:** A string The destination next hop router.
Up Time	**Synopsis:** A string The time this entry has been up.

Section 13.10.3

Enabling/Disabling MPLS

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.

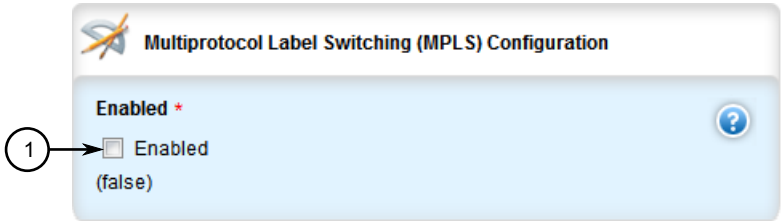


Figure 865: Multiprotocol Label Switching (MPLS) Configuration Form

1. Enabled Check Box

3. Configure the following parameter(s) as required:

Parameter	Description
Enable MPLS	**Synopsis:** { true, false } **Default:** 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 13.10.4

Managing the MPLS Interfaces

This section describes how to manage the MPLS interfaces.

CONTENTS

Section 13.10.4.1

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.

Figure 866: MPLS Status Interface List Table

This table provides the following information:

Parameter	Description
MPLS Interfaces	**Synopsis:** A string The interface that has been enabled for MPLS.
Status	**Synopsis:** A string The operational status.

If no MPLS interface has been enabled, enable interfaces as needed. For more information about enabling MPLS interfaces, refer to Section 13.10.4.3, "Enabling/Disabling an MPLS Interface".

Section 13.10.4.2
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.

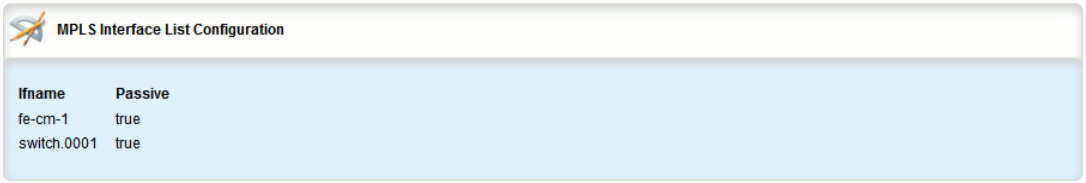


Figure 867: MPLS Interface List Configuration Table

If no MPLS interfaces have been configured, enable interfaces as needed. For more information about enabling MPLS interfaces, refer to Section 13.10.4.3, "Enabling/Disabling an MPLS Interface".

Section 13.10.4.3
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.

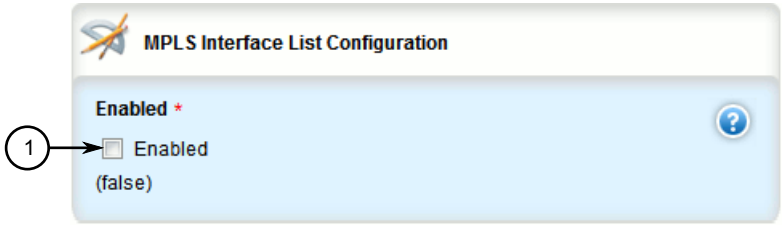


Figure 868: MPLS Interface List Configuration Form

1. Enable Check Box

3. Configure the following parameter(s) as required:

Parameter	Description
Name	**Synopsis:** A string Interface name.
Enabled	**Synopsis:** { true, false } **Default:** 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 13.10.5
Managing Static Label Binding

This section describes how to bind (or reserve) labels for IPv4 or network prefixes.

CONTENTS

Section 13.10.5.1
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.

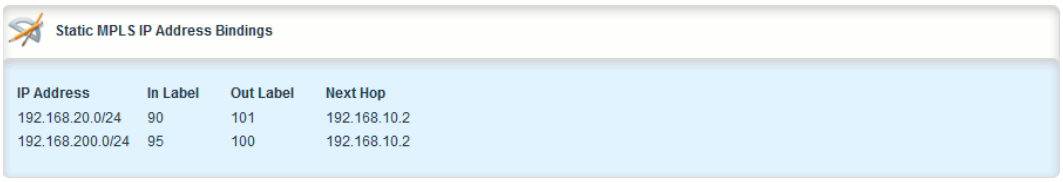


Figure 869: Static MPLS IP Address Bindings Table

This table provides the following information:

Parameter	Description
IP Address	**Synopsis:** A string The destination address prefix.
In Label	**Synopsis:** A string The incoming (local) label.
Out Label	**Synopsis:** A string The outgoing (remote) label.
Next Hop	**Synopsis:** A string The destination next hop router.

If no static label binding has been configured, configure binding as needed. For more information about configuring static-binding, refer to Section 13.10.5.3, "Adding a Static Label".

Section 13.10.5.2
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.

Figure 870: 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 13.10.5.3, "Adding a Static Label".

Section 13.10.5.3
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.*

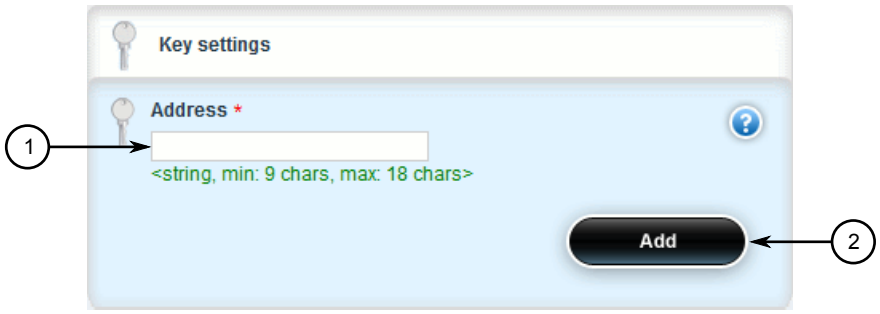


Figure 871: Key Settings Form

1. Address Box **2.** Add Button

4. Configure the following parameter(s) as required:

Parameter	Description
Address	**Synopsis:** A string 9 to 18 characters long The destination address/prefix.

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.

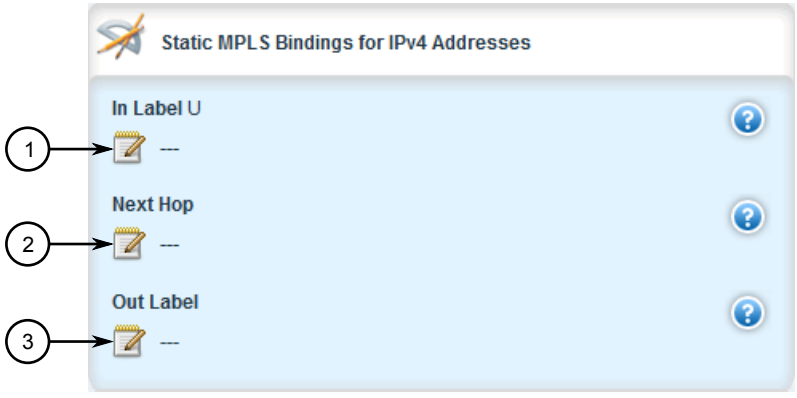


Figure 872: Static MPLS Bindings for IPv4 Addresses Form (Example)

1. In Label Box **2.** Next Hop Box **3.** Out Label Box

6. Configure the following parameter(s) as required:

Parameter	Description
In Label	**Synopsis:** A 32-bit unsigned integer between 16 and 1048575

Parameter	Description
	The incoming label: integer 16 -> 1048575.
Next Hop	**Synopsis:** A string 7 to 15 characters long The IP address for the destination next-hop router.
Out Label	**Synopsis:** { explicit-null, implicit-null } or a 32-bit unsigned integer between 16 and 1048575 The outgoing label: • *implicit null* - The label has a value of 3, meaning the penultimate (next-to-last) router performs a pop operation and forwards the remainder of the packet to the egress router. Penultimate Hop Popping (PHP) reduces the number of label lookups that need to be performed by the egress router • *explicit null* - The label has a value of 0, meaning that, in place of a pop operation, the penultimate (next-to-last) router forwards an IPv4 packet with an outgoing MPLS label of 0 to the egress router

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 13.10.5.4
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.

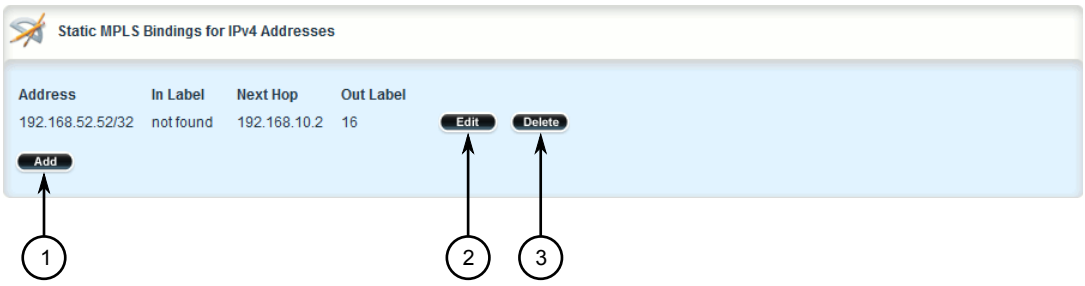


Figure 873: Static MPLS Bindings for IPv4 Addresses Table (Example)

1. Add Button **2.** Edit Button **3.** Delete Button

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 13.10.6

Managing Static Cross-Connects

Configure MPLS static cross-connects when the device is the core MPLS router. Cross-connects build Label Switch Paths (LSPs) when neighboring routers do not deploy the Label Distribution Protocol (LDP). The entry for static cross-connects is added to the Label Forwarding Information Base (LFIB). And, as such, label binding is not required in the Label Information Base (LIB).

CONTENTS

Section 13.10.6.1

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.

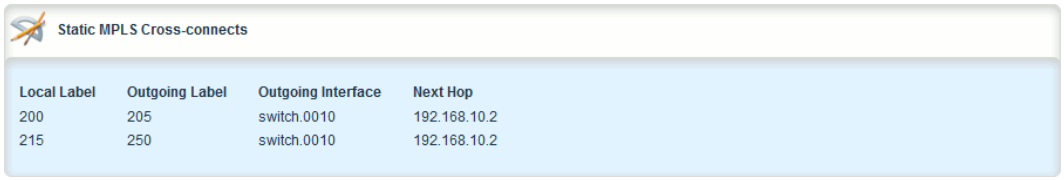


Figure 874: Static MPLS Cross-connects Table

This table provides the following information:

Parameter	Description
Local Label	**Synopsis:** A string The incoming (local) label.
Outgoing Label	**Synopsis:** A string The outgoing (remote) label.
Outgoing Interface	**Synopsis:** A string The outgoing interface.
Next Hop	**Synopsis:** A string The destination next hop router.

If no static cross-connects have been configured, add cross-connects as needed. For more information about adding static cross-connects, refer to Section 13.10.6.3, "Adding a Static Cross-Connect".

Section 13.10.6.2
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.

Figure 875: 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 13.10.6.3, "Adding a Static Cross-Connect".

Section 13.10.6.3
Adding a Static Cross-Connect

To add a static cross-connect, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to ***mpls » static-mpls » crossconnect*** and click **<Add dest-address>**. The **Key Settings** form appears.

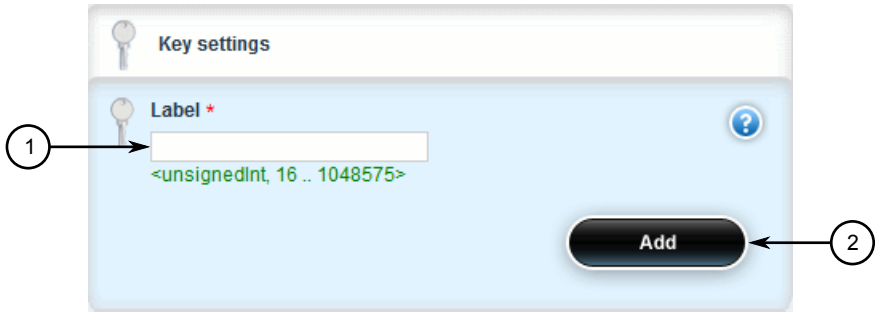


Figure 876: Key Settings Form

1. Label Box **2.** Add Button

3. Configure the following parameter(s) as required:

Parameter	Description
label	**Synopsis:** A 32-bit unsigned integer between 16 and 1048575 The incoming label.

4. Click **Add** to add the cross-connect label. The **Static MPLS Cross-Connects** form appears.

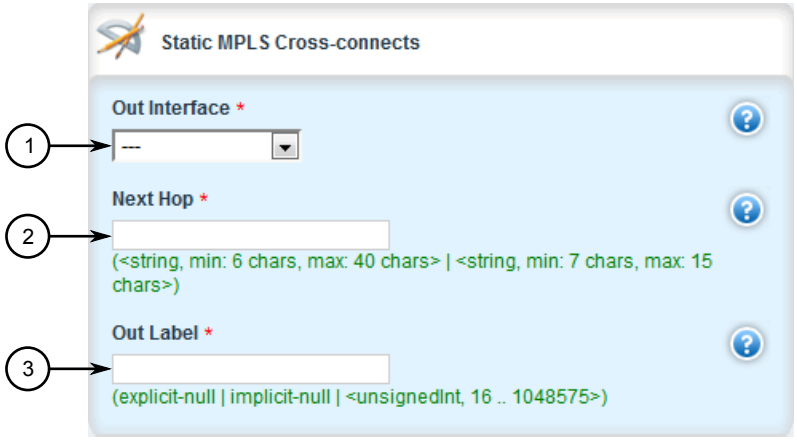


Figure 877: Static MPLS Cross-Connects Form

1. Out Interface List **2.** Next Hop Box **3.** Out Label Box

5. Configure the following parameter(s) as required:

Parameter	Description
Out Interface	**Synopsis:** A string The outgoing interface. This parameter is mandatory.
Next Hop	**Synopsis:** A string 7 to 15 characters long or a string 6 to 40 characters long The destination next-hop router (IPv4 or IPv6 format). This parameter is mandatory.
Out Label	**Synopsis:** { explicit-null, implicit-null } or a 32-bit unsigned integer between 16 and 1048575 The outgoing label: 'explicit-null', 'implicit-null' or integer 16 -> 1048575. This parameter is mandatory.

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 13.10.6.4

Deleting a Static Cross-Connect

To delete a static cross-connect, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to ***mpls » static-mpls » crossconnect***. The **Static MPLS Cross-Connects** table appears.

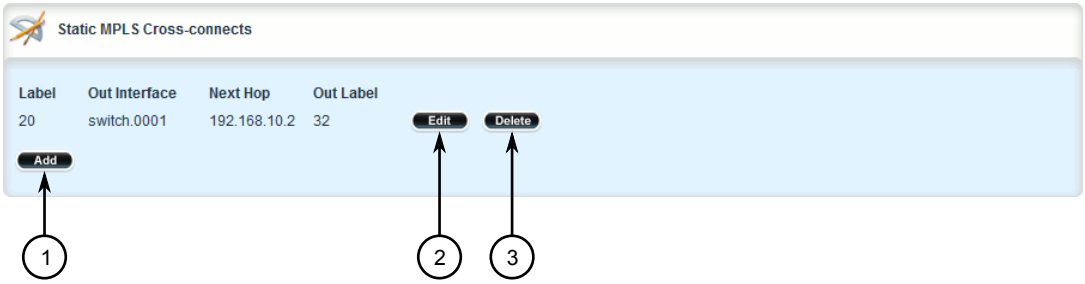


Figure 878: Static MPLS Cross-Connects Table

1. Add Button **2.** Edit Button **3.** Delete Button

3. Click **Delete** next to the chosen cross-connect 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 13.10.7

Managing LDP

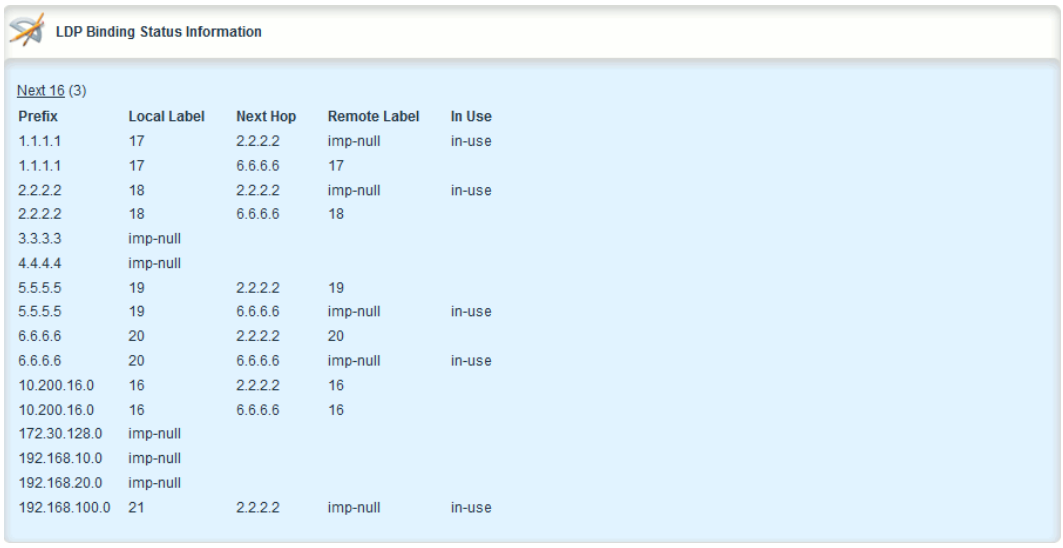
LDP (Label Distribution Protocol), defined by RFC 5036 [http://tools.ietf.org/html/rfc5036], is a protocol that enables an MPLS capable router to exchange MPLS label information. The labels are distributed in both directions so that an LSP (Label Switched Path) can be established and managed within an MPLS network dynamically, as opposed to configuring static routes. LDP takes advantage of already established routing information (using OSPF or IS-IS) to distribute label information amongst the MPLS enabled routers).

LDP works by enabling Label Switch Routers (LSRs) to discover and bind labels to their neighbors within the MPLS network. The LSRs then identify their peers and exchange their label information with one another. Label information is stored in Label Information Base (LIB) and Label Forwarding Information Base (LFIB) tables.

CONTENTS

Section 13.10.7.1
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.



LDP Binding Status Information

Next 16 (3)

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 879: LDP Binding Status Information Table

This table provides the following information:

Parameter	Description
Prefix	**Synopsis:** A string The LDP transport prefix.
Local Label	**Synopsis:** A string The incoming (local) label.
Next Hop	**Synopsis:** A string The destination next hop router.
Remote Label	**Synopsis:** A string The LDP remote label.
In Use	**Synopsis:** A string The LDP in-use flag.

Section 13.10.7.2
Viewing the Status of the LDP Discovery Interfaces

To view the status of the LDP discovery interfaces on the device, navigate to ***mpls » ldp » status » discovery » interfaces***. If LDP interfaces have been configured, the **LDP Discovery Interfaces Status Information** table appears.

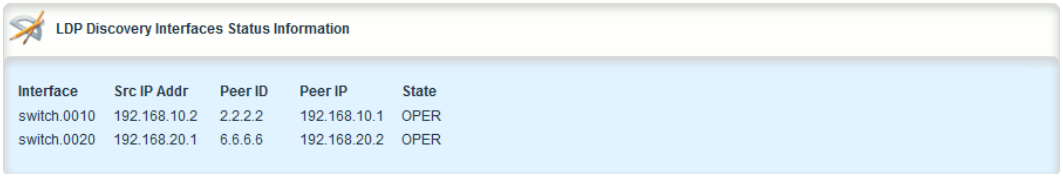


Figure 880: LDP Discovery Interfaces Status Information Table

This table provides the following information:

Parameter	Description
Interface	**Synopsis:** A string The LDP discovery interface.
Src IP Addr	**Synopsis:** A string The LDP discovery source IP address.
Peer ID	**Synopsis:** A string The LDP discovery peer ID.
Peer IP	**Synopsis:** A string LDP discovery peer IP address
State	**Synopsis:** A string The LDP discovery interface state.

For more information about configuring LDP discovery interfaces, refer to Section 13.10.7.9, "Enabling/Disabling an LDP Interface".

Section 13.10.7.3

Viewing the Status of the LDP Neighbor Local Node Information

To view the status of the local node(s) for the LDP neighbor on the device, navigate to ***mpls » ldp » status » neighbor » local-node-information***. The **LDP Neighbor Local Node Status Information** table appears.

Figure 881: LDP Neighbor Local Node Status Information Table

This table provides the following information:

Parameter	Description
LDP ID	**Synopsis:** A string The LDP ID of the neighbor local node.
Hello Holdtime	**Synopsis:** A string LDP hello holdtime of the neighbor local node.

Parameter	Description
Session Holdtime	**Synopsis:** A string The LDP session holdtime of the neighbor local node.

Section 13.10.7.4
Viewing the Status of the LDP Neighbor Connection Information

To view the status of the LDP neighbor connection on the device, navigate to ***mpls » ldp » status » neighbor » connection-information***. The **LDP Neighbor Connection Status Information** table appears.

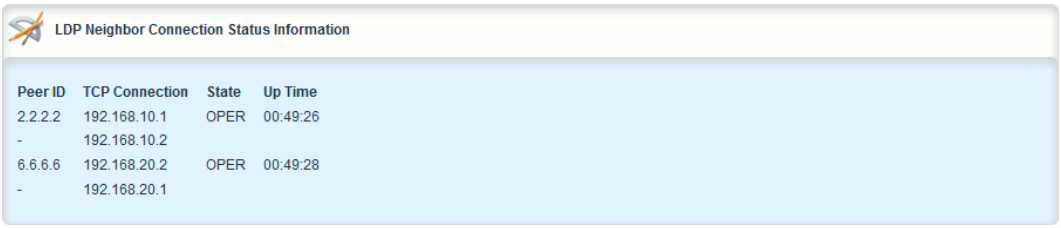


Figure 882: LDP Neighbor Connection Status Information Table

This table provides the following information:

Parameter	Description
Peer ID	**Synopsis:** A string The peer ID of the LDP neighbor connection.
TCP Connection	**Synopsis:** A string The TCP connection of the LDP neighbor connection.
state	**Synopsis:** A string The state of the LDP neighbor connection.
Up Time	**Synopsis:** A string The up time of the LDP neighbor connection.

Section 13.10.7.5
Viewing the Status of the LDP Neighbor Discovery Information

To view the status of the LDP neighbor discovery information on the device, navigate to ***mpls » ldp » status » neighbor » discovery-information***. The **LDP Neighbor Discovery Status Information** table appears.

Figure 883: LDP Neighbor Discovery Status Information Table

This table provides the following information:

Parameter	Description
Peer ID	**Synopsis:** A string The peer ID of the LDP neighbor discovery.
Peer IP	**Synopsis:** A string The peer ID of the LDP neighbor discovery.
Interface	**Synopsis:** A string The local IP address of the LDP neighbor discovery.
Local IP	**Synopsis:** A string LDP neighbor discovery state.
Peer Hello Holdtime	**Synopsis:** A string The peer hello holdtime of the LDP neighbor discovery.
Agreed Hello Holdtime	**Synopsis:** A string The agreed upon hello holdtime (shorter holdtime of local/peer) of the LDP neighbor discovery.
Peer Session Holdtime	**Synopsis:** A string The peer session holdtime of the LDP neighbor discovery.

Section 13.10.7.6
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.

Figure 884: Label Discovery Protocol (LDP) Configuration Form

1. Enabled Check Box **2.** Holdtime Box

3. Configure the following parameter(s) as required:

Parameter	Description
Enable LDP	**Synopsis:** { true, false } **Default:** false A boolean flag to indicate that Label Distribution Protocol (LDP) is enabled.
LDP Holdtime	**Synopsis:** A 32-bit unsigned integer **Default:** 180 The session holdtime (in seconds), used as the keepalive timeout to maintain the Label Distribution Protocol (LDP) session in the absence of LDP messages from the session peer.

NOTE
MPLS must be enabled and MPLS label bindings must be removed before enabling LDP. Refer to Section 13.10.3, "Enabling/Disabling MPLS" and Section 13.10.5.4, "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 13.10.7.7
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.

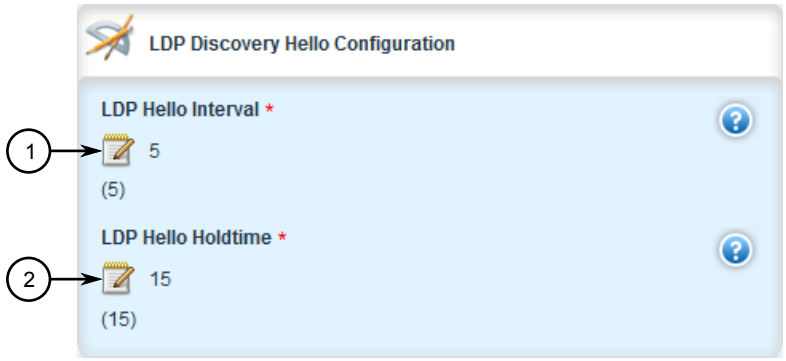


Figure 885: LDP Discovery Hello Configuration Form

1. LDP Hello Interval Box **2.** LDP Hello Holdtime Box

3. Configure the following parameter(s) as required:

Parameter	Description
LDP Hello Interval	**Synopsis:** A 32-bit unsigned integer **Default:** 5 The time (in seconds) between the sending of consecutive Hello messages.
LDP Hello Holdtime	**Synopsis:** A 32-bit unsigned integer **Default:** 15 The time (in seconds) that a discovered LDP neighbor is remembered without receipt of an LDP Hello message from the neighbor.

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 13.10.7.8

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.

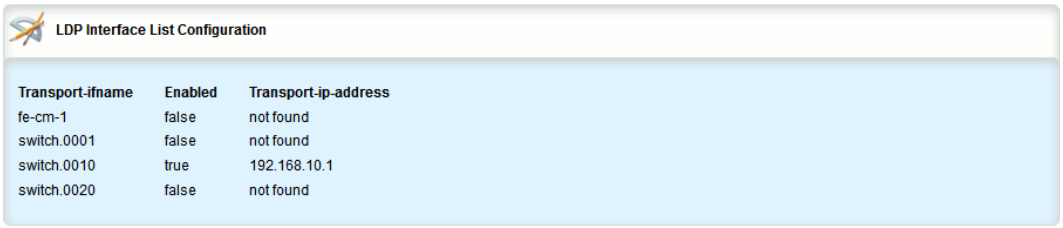


Figure 886: LDP Interface List Configuration Table

For more information about enabling LDP interfaces, refer to Section 13.10.7.9, "Enabling/Disabling an LDP Interface".

Section 13.10.7.9
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.

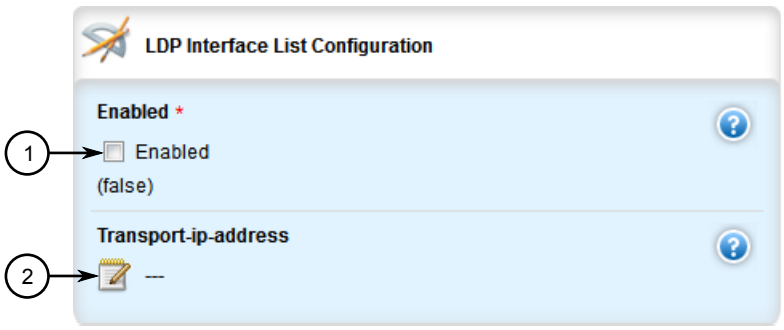


Figure 887: LDP Interface List Configuration Form

1. Enable Check Box **2.** Transport IP Address Box

3. Configure the following parameter(s) as required:

Parameter	Description
Transport Interface	**Synopsis:** A string Transport interface name
Enabled	**Synopsis:** { true, false } **Default:** false A boolean flag to indicate a transport interface is LDP-enabled or not. Only LDP-enabled interfaces are used for LDP.
IP Address	**Synopsis:** A string 7 to 15 characters long or a string 6 to 40 characters long The transport IP address (IPv4 or IPv6 format). If not provided, *interface* 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.

Section 13.11

Managing Virtual Routing and Forwarding (VRF)

Virtual Routing and Forwarding (VRF) allows multiple routing instances to exist at the same time on a network router without conflicting with one another or the global routing table. This feature is used typically by service providers to route different types of traffic emanating from the same router.

Each routing instance is completely isolated and has its own set of interfaces. Any traffic sent on those interfaces is considered to be part of that VRF only.

An MPLS label can be applied as well to traffic traversing the tunnel to improve security. This is considered full VRF, as compared to VRF-Lite (first introduced by Cisco).

RUGGEDCOM RX1500/RX1501/RX1510/RX1511/RX1512 devices can be configured to act as a CE, PE or P (provider core) router.

CONTENTS

Section 13.11.1

VRF Concepts

This section describes some of the concepts important to the implementation of Virtual Routing and Forwarding (VRF) in RUGGEDCOM ROX II.

CONTENTS

Section 13.11.1.1
VRF and VRF-Lite

Both full VRF and VRF-Lite employ the concept of VRFs to isolate interfaces, provide IP address reuse and manage routing tables. Both also provide a level of security for those interfaces forward to the VRFs. Under full VRF, MPLS is used in conjunction with IP/VPNs to provide a greater level of security than VRF-Lite.

RUGGEDCOM ROX II supports both VRF and VRF-Lite simultaneously. Use of full VRF interfaces and VRF-Lite interfaces can be mixed.

Section 13.11.1.2
Advantages and Disadvantages of Using VRF

The advantages and disadvantages of using VRF include the following:

Advantages

- Create multiple isolated network pipes for various data streams
- Provide individualized security for each VRF
- Manage each VRF separately for audit and billing purposes
- Create separate Intranets within one work environment
- Create VRFs based on differing services (e.g. Finance, engineering, HR, etc.)
- Reduce the size of routing tables
- Re-use of IP addresses or subnets
- MPLS IP VPNs can replace much more expensive, leased T1/E1 lines, while providing the same level of security

Disadvantages

- Greater memory consumption. Each VRF configured results in BGP route replication and requires new FIBs and IP routing tables
- Extra processing (overhead) and memory consumption due to namespace management

Section 13.11.2
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.

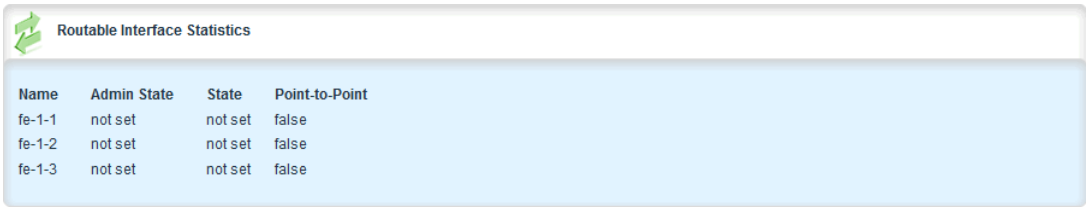


Figure 888: Routable Interface Statistics Form

This table provides the following information:

Parameter	Description
Name	**Synopsis:** A string 1 to 15 characters long The name of the interface.
Admin State	**Synopsis:** { not set, up, down, testing, unknown, dormant, notPresent, lowerLayerDown } The port's administrative status. This parameter is mandatory.
State	**Synopsis:** { not set, up, down, testing, unknown, dormant, notPresent, lowerLayerDown } Shows whether the link is up or down. This parameter is mandatory.
Point-to-Point	**Synopsis:** { true, false } The point-to-point link. This parameter is mandatory.
Bytes	**Synopsis:** A 64-bit unsigned integer The number of bytes received. This parameter is mandatory.
Packets	**Synopsis:** A 64-bit unsigned integer The number of packets received. This parameter is mandatory.
Errors	**Synopsis:** A 32-bit unsigned integer The number of error packets received. This parameter is mandatory.
Dropped	**Synopsis:** A 32-bit unsigned integer The number of packets dropped by the receiving device. This parameter is mandatory.
Bytes	**Synopsis:** A 64-bit unsigned integer The number of bytes transmitted. This parameter is mandatory.
Packets	**Synopsis:** A 64-bit unsigned integer The number of packets transmitted. This parameter is mandatory.
Errors	**Synopsis:** A 32-bit unsigned integer The number of error packets transmitted. This parameter is mandatory.
Dropped	**Synopsis:** A 32-bit unsigned integer The number of packets dropped by the transmitting device. This parameter is mandatory.
Collisions	**Synopsis:** A 32-bit unsigned integer The number of collisions detected on the port. This parameter is mandatory.

Section 13.11.3
Configuring VRF

To configure Virtual Routing and Forwarding (VRF), do the following:

IMPORTANT!
BGP routing must be enabled before VRF is configured.

Full VRF Configuration

1. Make sure BGP is enabled and configure the Autonomous System ID for the Border Gateway Protocol (BGP). For more information, refer to Section 13.8.1, "Configuring BGP".
2. Configure a VRF definition and route targets for each Customer Edge (CE) router. For more information, refer to Section 13.11.5.2, "Adding a VRF Definition".
3. Configure a routable interface and IP address for each VRF definition. For more information, refer to Section 13.11.4, "Configuring a VRF Interface".
4. Enable OSPF. For more information, refer to Section 13.9.2, "Configuring OSPF".
5. Configure one or more VRF instances for OSPF. For more information, refer to Section 13.9.2, "Configuring OSPF".
6. Add one or more BGP neighbors. For more information, refer to Section 13.8.6.2, "Adding a Neighbor".
7. Configure one or more IP/VPN tunnels for each interface. For more information, refer to Section 13.11.8.2, "Adding an IP/VPN Tunnel".
8. Add one or more BGP neighbors to the VPNv4 address family. For more information, refer to Section 13.11.9.2, "Adding a Neighbor".
9. Verify the network configuration.

VRF-Lite Configuration

1. Make sure BGP is enabled and configure the Autonomous System ID for the Border Gateway Protocol (BGP). For more information, refer to Section 13.8.1, "Configuring BGP".
2. Configure a VRF definition and route targets for each Customer Edge (CE) router. For more information, refer to Section 13.11.5.2, "Adding a VRF Definition".
3. Configure a routable interface and IP address for each VRF definition. For more information, refer to Section 13.11.4, "Configuring a VRF Interface".
4. Enable OSPF. For more information, refer to Section 13.9.2, "Configuring OSPF".
5. Configure one or more VRF instances for OSPF. For more information, refer to Section 13.9.2, "Configuring OSPF".
6. Configure an IPv4 address family for each VRF instance. For more information, refer to Section 13.11.10.2, "Adding an IPv4 Address Family".
7. Configure one or more static VRF routes. For more information, refer to Section 13.11.13.2, "Adding a Static VRF Route".
8. Verify the network configuration.

Section 13.11.4
Configuring a VRF Interface

Each VRF definition must be associated with at least one routable interface that has been assigned an IP address.

To configure a routable interface to forward VRF traffic for a specific VRF definition, do the following:

1. 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.*

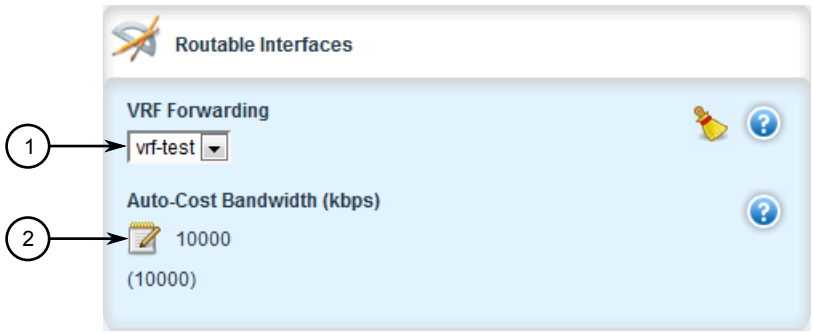


Figure 889: Routable Interfaces Form

1. VRF Forwarding List **2.** Auto-Cost Bandwidth Box

3. Configure the following parameter(s) as required:

Parameter	Description
VRF Forwarding	**Synopsis:** A string The VRF to which this interface is to be forwarded. When forwarded, this interface will be made available when that VRF is configured in the IS-IS and OSPF routing protocols. When forwarding is changed/removed for this interface, a validation error will be emitted if the interface is configured for use with that VRF in any of those protocols.

4. Configure an IPv4 or IPv6 address for the interface. For more information, refer to Section 7.1.3.2, "Adding an IPv4 Address" or Section 7.1.4.2, "Adding an IPv6 Address".
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 13.11.5
Managing VRF Definitions

VRF definitions represent individual Customer Edge (CE) routers in the VRF topology. RUGGEDCOM ROX II supports up to eight definitions in total, each composed of a unique VRF name, an optional description and a Route

Distinguisher (RD). The Route Distinguisher is an 8 octet field typically made up of an AS number or IP address followed by a colon (:) and the site ID (e.g. 6500:20 or 172.20.120.12:10). When prefixed to the IPv4 address of the associated interface, it uniquely identifies each IP packet, allowing the Provider Edge (PE) to determine which VPN tunnel the packet belongs to.

Each VRF definition can also be associated with one or more route targets.

CONTENTS

Section 13.11.5.1

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.

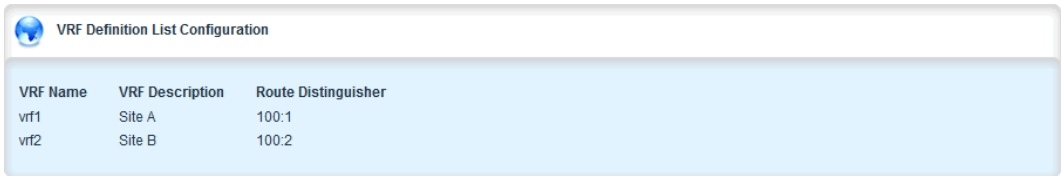


Figure 890: VRF Definition List Configuration Table

If no VRF definitions have been configured, add definitions as needed. For more information, refer to Section 13.11.5.2, "Adding a VRF Definition".

Section 13.11.5.2

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.

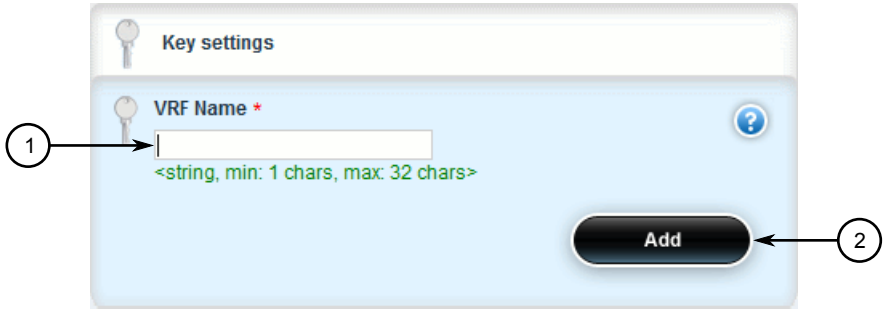


Figure 891: Key Settings Form

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	**Synopsis:** 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.

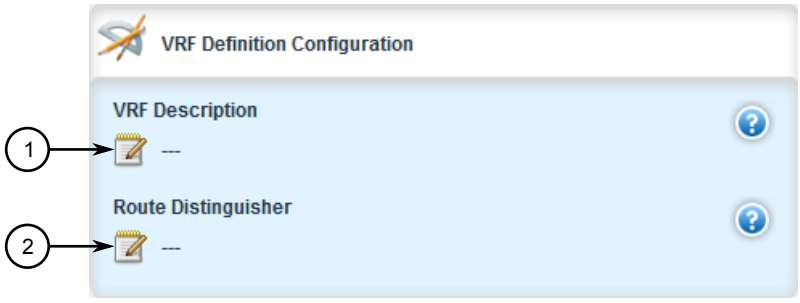


Figure 892: VRF Definition Configuration Form

1. VRF Description Box **2.** Route Distinguisher Box

5. Configure the following parameter(s) as required:

Parameter	Description
VRF Description	**Synopsis:** 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	**Synopsis:** A string 0 to 32 characters long The VRF's route distinguisher: 8-byte value, typical format is (as-number:id | ip-address:id) (e.g. 6500:20). It will be prepended to the IPv4 prefix to create the VPN IPv4 prefix. Note that changing the route distinguisher will affect the route targets: it is recommended that you verify that the configured route targets used in your network will still be correct.

6. Add one or more route targets. For more information, refer to Section 13.11.6.2, "Adding a Route Target".
7. Configure a routable interface for the VRF instance. For more information, refer to Section 13.11.4, "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 13.11.5.3
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 13.11.7.3, "Deleting a VRF Instance".
4. Delete the associated IPv4 address family under BGP. For more information, refer to Section 13.11.10.3, "Deleting an IPv4 Address Family".
5. Navigate to ***global » vrf***. The **VRF Definition List Configuration** table appears.

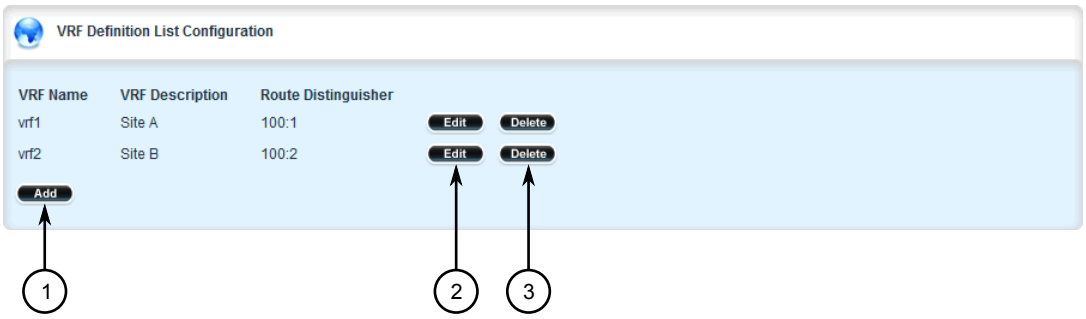


Figure 893: VRF Definition List Configuration Table

1. Add Button **2.** Edit Button **3.** Delete Button

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 13.11.6
Managing Route Targets

Route targets identify those routes to import/export within the Multi-Protocol BGP (MBGP) network. Similar to the normal global routing instance, the route target sets the route import and export parameters for BGP. This parameter enables users to specify which prefixes they wish to import to other neighbors and which ones to export.

CONTENTS

Section 13.11.6.1
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.

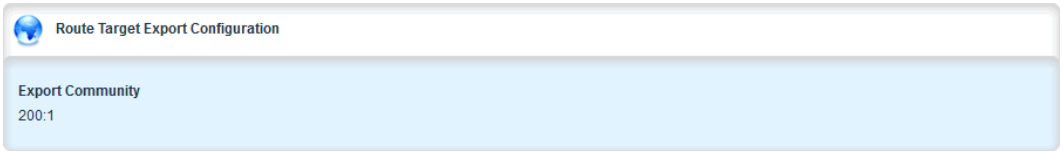


Figure 894: Route Target Export Configuration Table (Example)

If no VRF definitions have been configured, add definitions as needed. For more information, refer to Section 13.11.5.2, "Adding a VRF Definition".

Section 13.11.6.2
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.

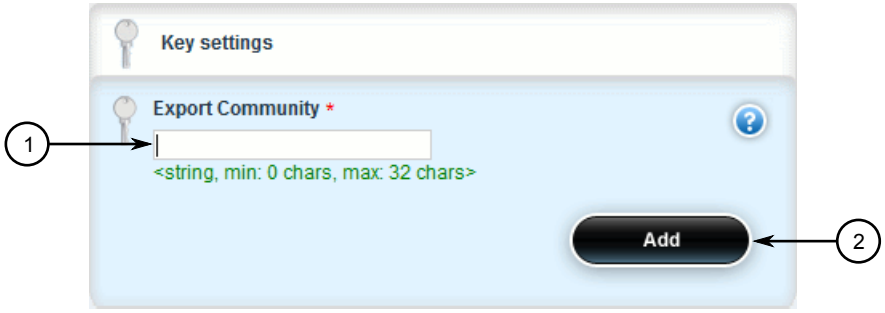


Figure 895: Key Settings Form – Export (Example)

1. VRF Name Box **2.** Add Button

4. Configure the following parameter(s) as required:

Parameter	Description
Export Community	**Synopsis:** 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 13.11.6.3
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.

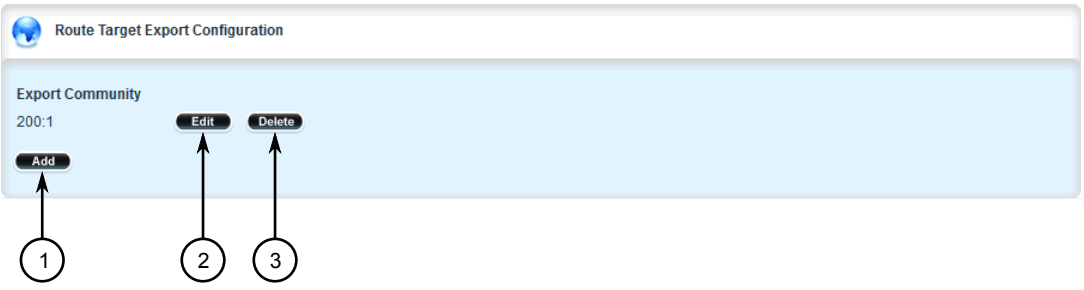


Figure 896: Route Target Export Configuration Table (Example)

1. Add Button **2.** Edit Button **3.** Delete Button

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 13.11.7
Managing VRF Instances and OSPF

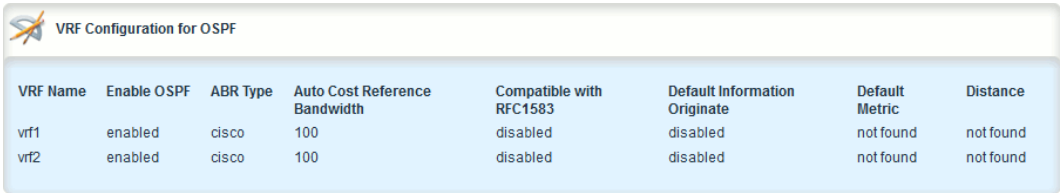
OSPF can be configured for one or more VRF definitions. This is done by by enabling OSPF for a VRF instance and then configuring the required OSPF parameters.

OSPF can be run on any physical or switched interface, as well as VRF-Lite interfaces (IPv4) and full VRF interfaces (IP/VPN using MPLS).

CONTENTS

Section 13.11.7.1
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 897: VRF Configuration for OSPF Table

If no VRF definitions have been configured, add definitions as needed. For more information, refer to Section 13.11.5.2, "Adding a VRF Definition".

Section 13.11.7.2
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.

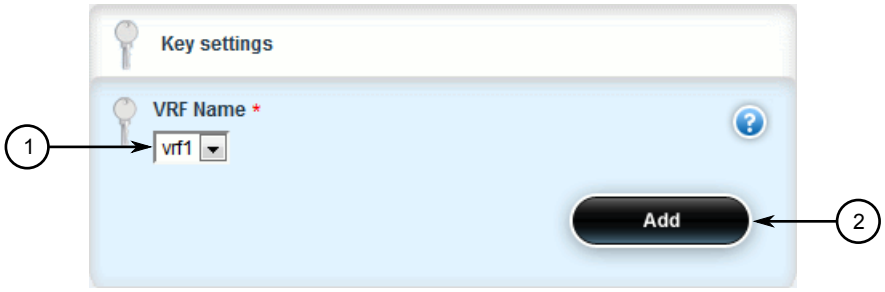


Figure 898: Key Settings Form

1. VRF Name List **2.** Add Button

3. Configure the following parameter(s) as required:

Parameter	Description
VRF Name	**Synopsis:** A string The VRF name.

4. Click **Add**. The **Distance OSPF for VRF** and **OSPF Configuration for VRF** forms appear.

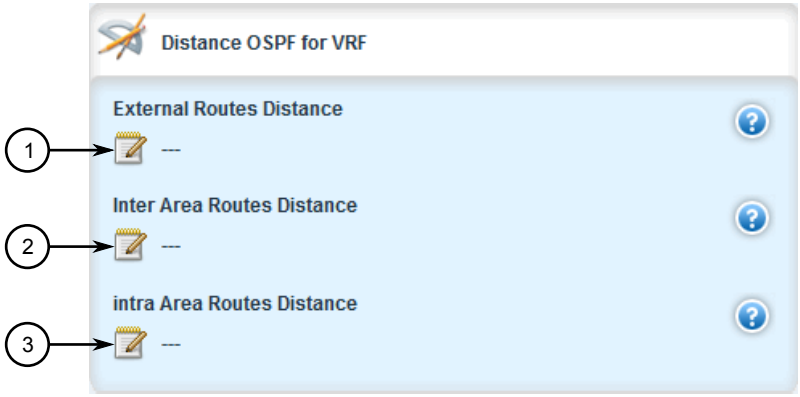


Figure 899: Distance OSPF for VRF Form

1. External Routes Distance Box **2.** Inter Area Routes Distance Box **3.** Intra Area Routes Distance Box

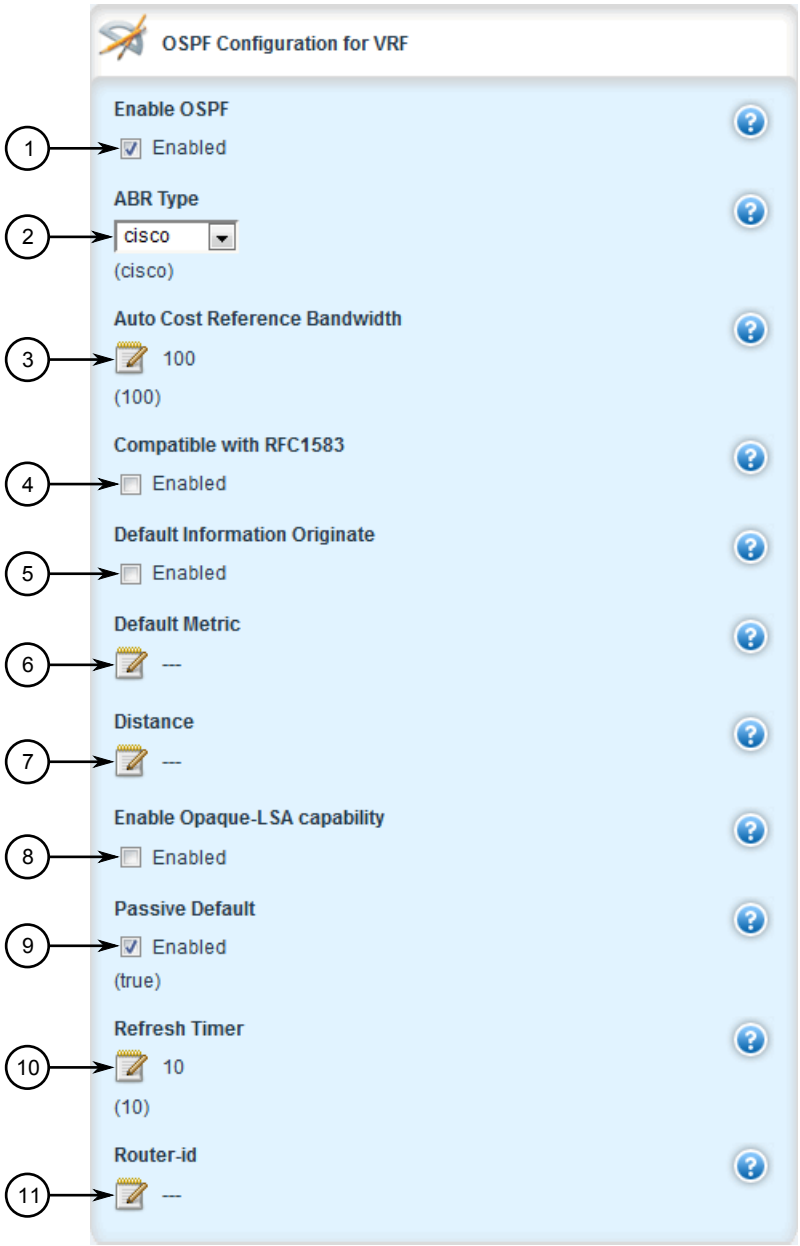


Figure 900: OSPF Configuration for VRF Form

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	**Synopsis:** A 32-bit unsigned integer between 1 and 255 The administrative distance for external routes.

Parameter	Description
Inter Area Routes Distance	**Synopsis:** A 32-bit unsigned integer between 1 and 255 The administrative distance for inter-area routes.
intra Area Routes Distance	**Synopsis:** A 32-bit unsigned 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	Enables the OSPF dynamic routing protocol.
ABR Type	**Synopsis:** { cisco, ibm, shortcut, standard } **Default:** cisco The OSPF ABR type.
Auto Cost Reference Bandwidth	**Synopsis:** A 32-bit unsigned integer between 1 and 4294967 **Default:** 100 Calculates the OSPF interface cost according to bandwidth [1-4294967 Mbps]
Compatible with RFC1583	Enables the compatibility with the obsolete RFC1583 OSPF (the current is RFC2178)
Default Information Originate	Advertises the default route.
Default Metric	**Synopsis:** A 32-bit unsigned integer between 0 and 16777214 The default metric of redistribute routes.
Distance	**Synopsis:** A 32-bit unsigned integer between 1 and 255 The administrative distance.
Enable Opaque-LSA capability	Enables the Opaque-LSA capability (RFC2370).
Passive Default	**Synopsis:** { true, false } **Default:** true Default passive value for new interface.
Refresh Timer	**Synopsis:** A 16-bit unsigned integer between 10 and 1800 **Default:** 10 The refresh timer.
router-id	**Synopsis:** 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.

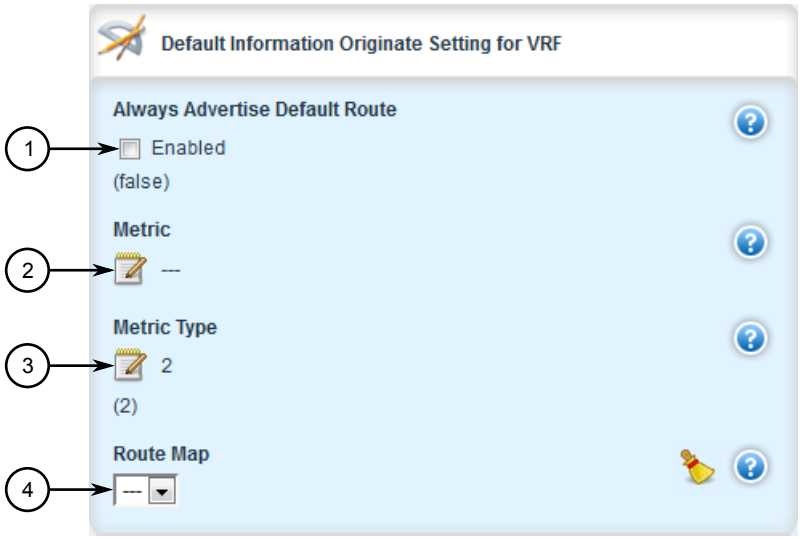


Figure 901: Default Information Originate for VRF Form

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	**Synopsis:** { true, false } **Default:** false Always advertise default route even when there is no default route present in routing table.
Metric	**Synopsis:** A 32-bit unsigned integer between 0 and 16777214 The metric value for default route.
Metric Type	**Synopsis:** An 8-bit signed integer between 1 and 2 **Default:** 2 The metric type for default route.
Route Map	**Synopsis:** A string The route map name.

9. Configure prefix list filters for the VRF instance. For more information, refer to Section 13.9.4.3, "Adding a Prefix List".
10. Configure areas for the VRF instance. For more information, refer to Section 13.9.5.2, "Adding an Area".
11. Configure route map filters for the VRF instance. For more information, refer to Section 13.9.6.3, "Adding a Route Map Filter".
12. Configure redistribution metrics for the VRF instance. For more information, refer to Section 13.9.8.2, "Adding a Redistribution Metric".
13. Configure interfaces for the VRF instance. For more information, refer to Section 13.9.9.2, "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 13.11.7.3
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.

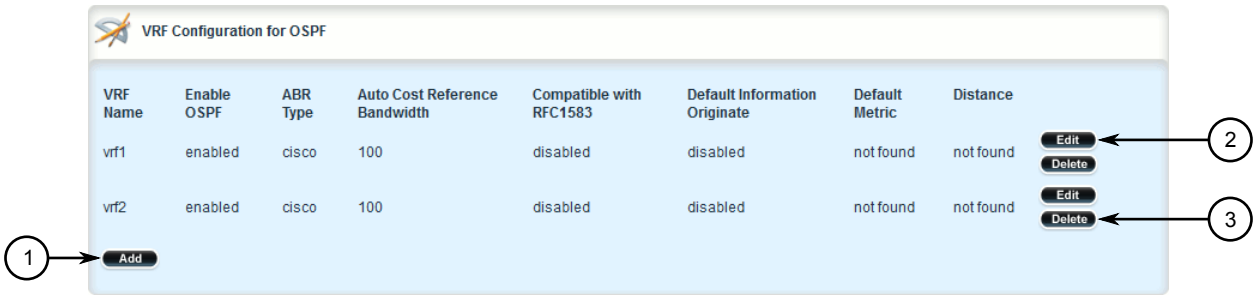


Figure 902: VRF Configuration for OSPF Table

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 13.11.8
Managing IP/VPN Tunnels

IP/VPN tunnels use the VPNv4 protocol to exchange customer prefixes (i.e. route distributions and route targets) and labels between Provider Edge (PE) routers. IP/VPNs provide isolation of the interfaces connecting each end of the VPN.

NOTE
VRF maintains a table listing each interface belonging to each IP/VPN tunnel.

CONTENTS

Section 13.11.8.1
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.

Figure 903: VPNv4 Neighbor Configuration Table (Example)

Section 13.11.8.2
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.

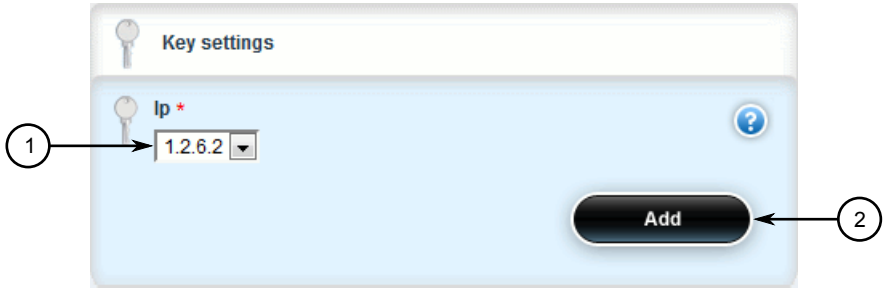


Figure 904: Key Settings Form

1. IP Box **2.** Add Button

3. Configure the following parameter as required:

Parameter	Description
ip	**Synopsis:** A string The neighbor IP address.

4. Click **Add** to add the address. The **VPNv4 Neighbor** and **Route Reflector Client** forms appear.

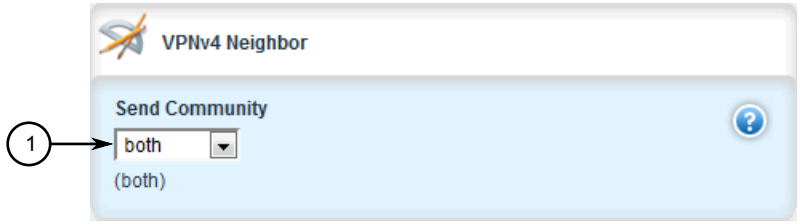


Figure 905: VPNv4 Neighbor Form

1. Send Community List

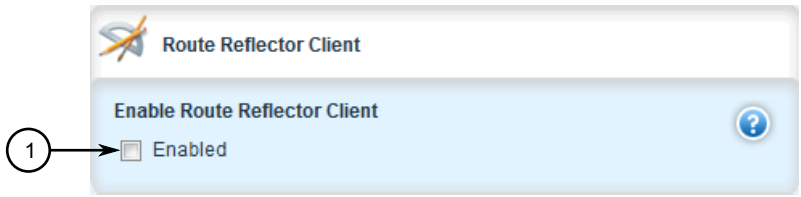


Figure 906: Route Reflector Client Form

1. Enable Check Box

5. [Optional] On the **VPNv4 Neighbor** form, set the send community by configuring the following parameter:

Parameter	Description
Send Community	**Synopsis:** { standard, extended, both, none } **Default:** both Identifies the send Community. Default is both.

6. [Optional] On the **Route Reflector Client** form, enable the IP/VPN tunnel as a VPNv4 route reflector client by configuring the following parameter:

Parameter	Description
Enable Route Reflector Client	When enabled, the neighbor is a VPNv4 route reflector client.

7. 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 13.11.8.3
Deleting an IP/VPN Tunnels

To delete an IP/VPN tunnel, 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.

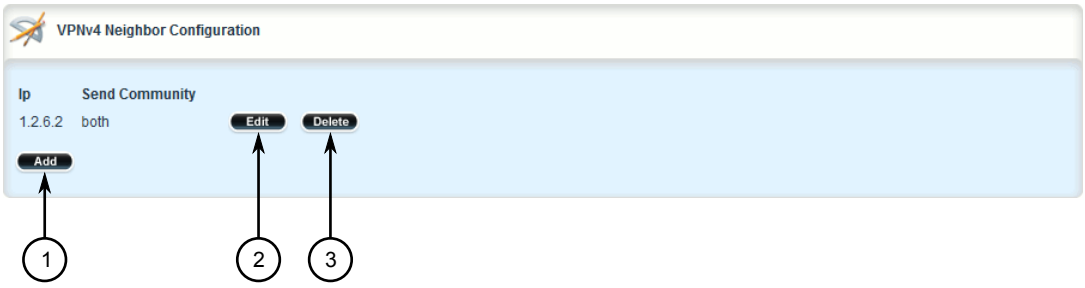


Figure 907: VPNv4 Neighbor Configuration Table (Example)

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 13.11.9

Managing VPNv4 Neighbors

VPNv4 neighbors are other routers with which to exchange routes. One or more neighbors must be specified in order for VRF-Lite to operate.

CONTENTS

Section 13.11.9.1

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.

Figure 908: VPNv4 Neighbor Configuration Table

If no neighbors have been configured, add neighbors as needed. For more information, refer to Section 13.11.12.2, "Adding a Neighbor".

Section 13.11.9.2
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 13.8.6.2, "Adding a Neighbor".
3. Navigate to ***routing » dynamic » bgp » address-family » vpnv4*** and click **<Add neighbor>**. The **Key Settings** form appears.

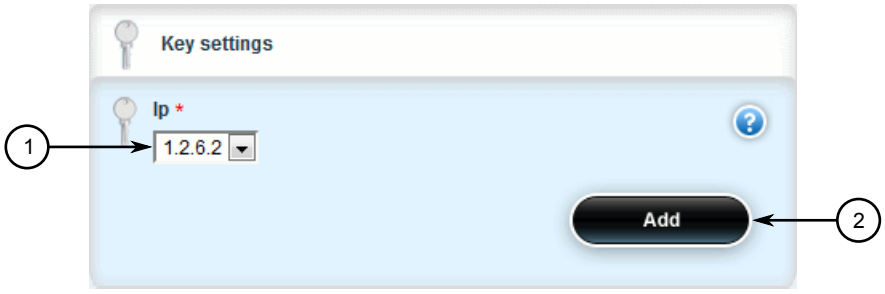


Figure 909: Key Settings Form

1. IP Box **2.** Add Button

4. Configure the following parameter as required:

Parameter	Description
ip	**Synopsis:** A string The neighbor IP address.

5. Click **Add** to add the address. The **VPNv4 Neighbor** and **Route Reflector Client** forms appear.

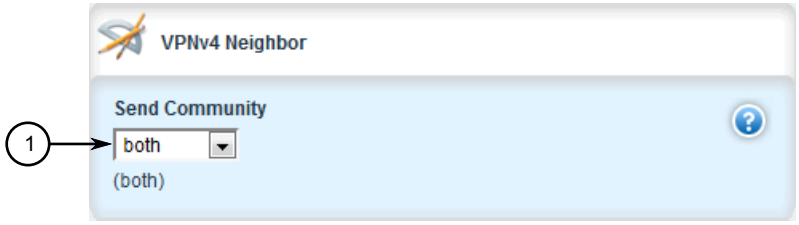


Figure 910: VPNv4 Neighbor Form

1. Send Community List

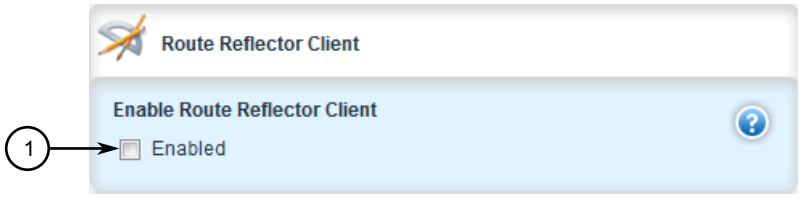


Figure 911: Route Reflector Client Form

1. Enable Check Box

6. [Optional] On the **VPNv4 Neighbor** form, set the send community by configuring the following parameter:

Parameter	Description
Send Community	**Synopsis:** { standard, extended, both, none } **Default:** both Identifies the send Community. Default is both.

7. [Optional] On the **Route Reflector Client** form, enable the neighbor as a route reflector client by configuring the following parameter:

Parameter	Description
Enable Route Reflector Client	When enabled, the neighbor is a VPNv4 route reflector client.

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 13.11.9.3
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.

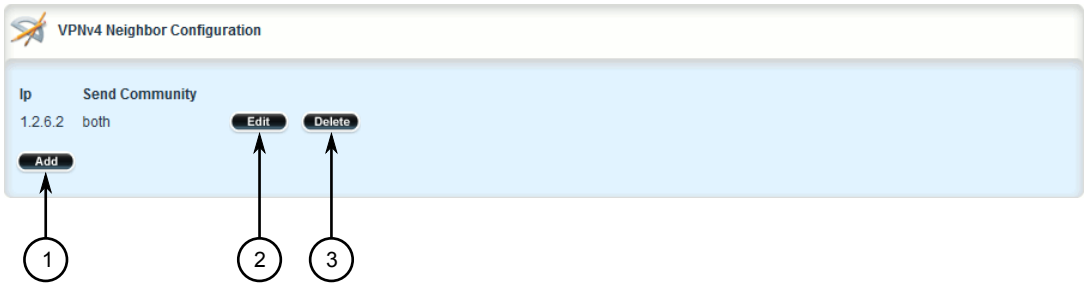


Figure 912: VPNv4 Neighbor Configuration Table

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 13.11.10

Managing IPv4 Address Families

IPv4 address families are configured when deploying VRF-Lite. Address families under BGP specify the neighbors with whom the router will share VRF routing information and what type of routing distribution method is permitted. One or more address families can be configured for each VRF instance.

Route distribution can be limited directly connected routes, static routes, or OSPF learned routes.

CONTENTS

Section 13.11.10.1

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.

Figure 913: VRF Configuration Form

If no IPv4 address families have been configured, add them as needed. For more information, refer to Section 13.11.10.2, "Adding an IPv4 Address Family".

Section 13.11.10.2
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.

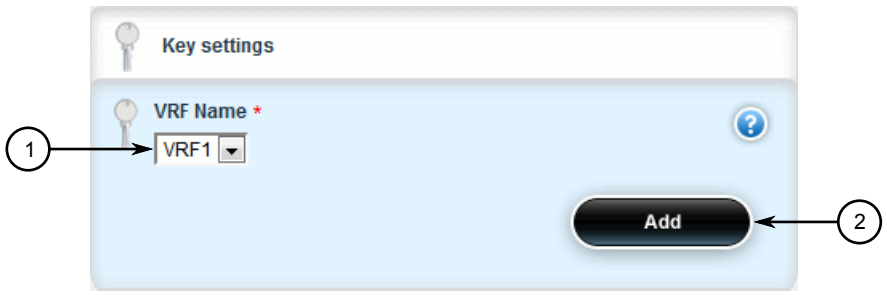


Figure 914: Key Settings Form

1. VRF Name List **2.** Add Button

3. Select the desired VRF and then click **Add**. The **Route Map** and **Neighbor** forms appear.
4. [Optional] Add one or more neighbors. For more information, refer to Section 13.11.12.2, "Adding a Neighbor".
5. [Optional] Add one or more redistributions. For more information, refer to Section 13.11.11.2, "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 13.11.10.3
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.

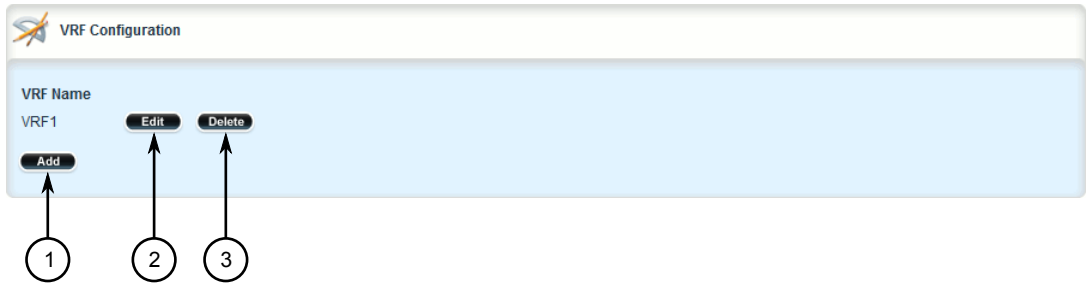


Figure 915: VRF Configuration Form

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 13.11.11

Managing Redistribution for IPv4 Address Families

Redistribution in general is the advertisement of routes by one protocol that have been learned via another dynamic routing protocol, a static route, or a directly connected router. It is deployed to promote interoperability between networks running different routing protocols. In the case of VRF, the OSPF dynamic routing protocol is supported.

For each VRF instance, one or more redistributions can be defined. A redistribution defines the source of the routing information, a metric and (optional) a pre-defined routing map.

The metric is used for route decision making within the Autonomous System (AS). Care must be taken to define a metric that is understood by the OSPF routing protocol.

CONTENTS

Section 13.11.11.1

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.

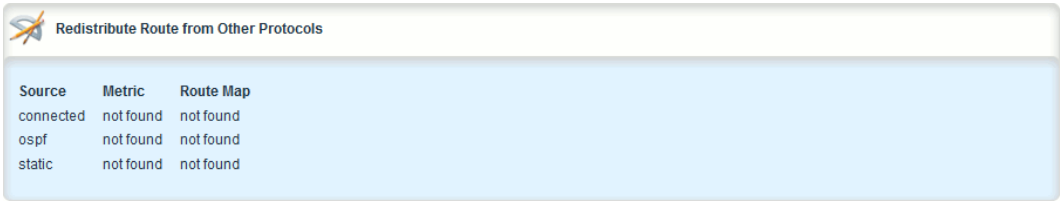


Figure 916: Redistribute Route from Other Protocols Table

If no redistributions have been configured, add them as needed. For more information, refer to Section 13.11.11.2, "Adding a Redistribution".

Section 13.11.11.2

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.

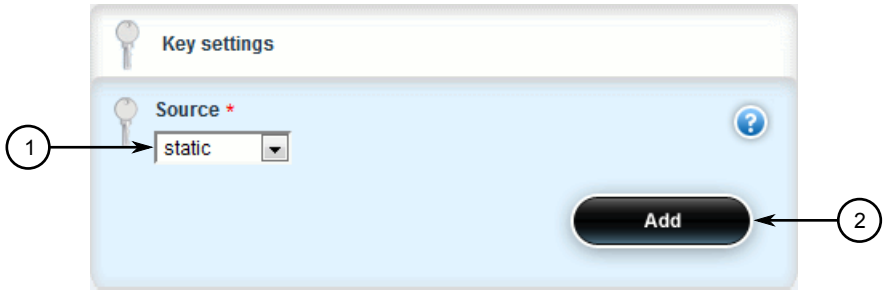


Figure 917: Key Settings Form

1. Redistribute Route From List **2.** Add Button

4. Configure the following parameter(s) as required:

Parameter	Description
source	**Synopsis:** { connected, ospf, static } Protocol that is source of VRF information. Mandatory field.

5. Click **Add** to add the redistribution. The **Redistribute Configuration** form appears.

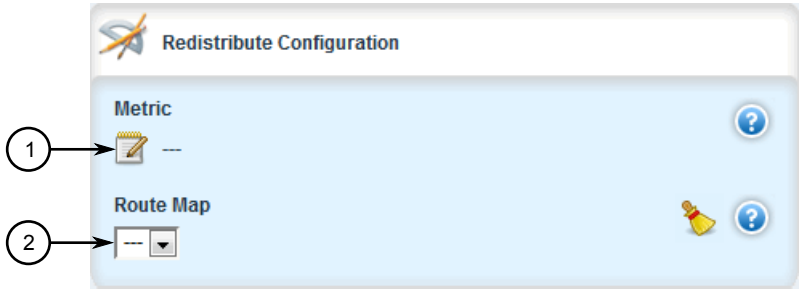


Figure 918: Redistribute Configuration Form

1. Metric Box

6. Configure the following parameter(s) as required:

Parameter	Description
metric	**Synopsis:** A 32-bit unsigned integer between 0 and 4294967295 The metric for redistributed routes.
Route Map	**Synopsis:** A string 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 13.11.11.3

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.

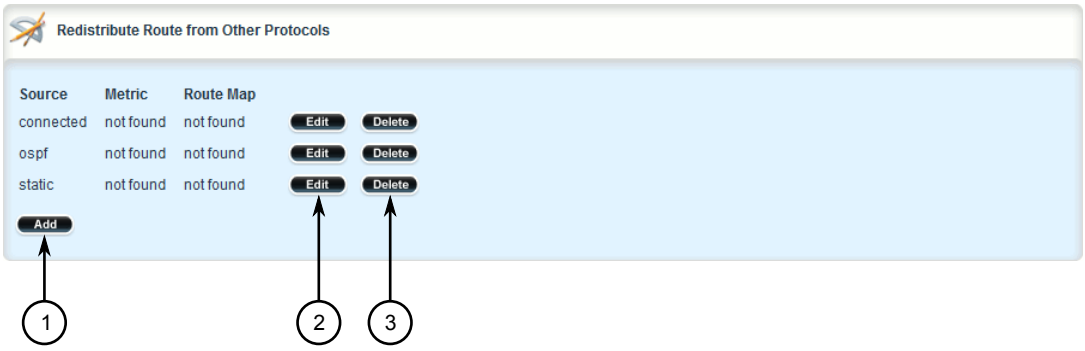


Figure 919: Redistribute Route from Other Protocols Table

1. Add Button **2.** Edit Button **3.** Delete Button

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 13.11.12

Managing Neighbors for IPv4 Address Families

Neighbors are other routers with which to exchange routes. One or more neighbors must be specified in order for VRF to operate.

CONTENTS

Section 13.11.12.1

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.

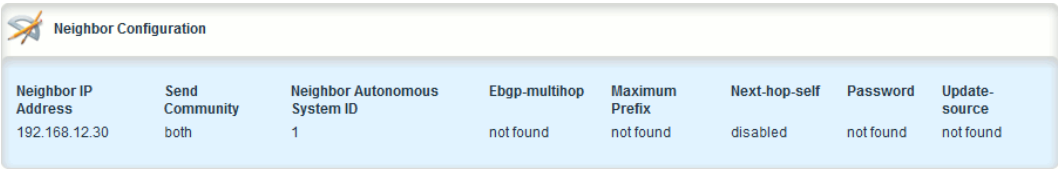


Figure 920: Neighbor Configuration Table

If no neighbors have been configured, add neighbors as needed. For more information, refer to Section 13.11.12.2, "Adding a Neighbor".

Section 13.11.12.2
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.

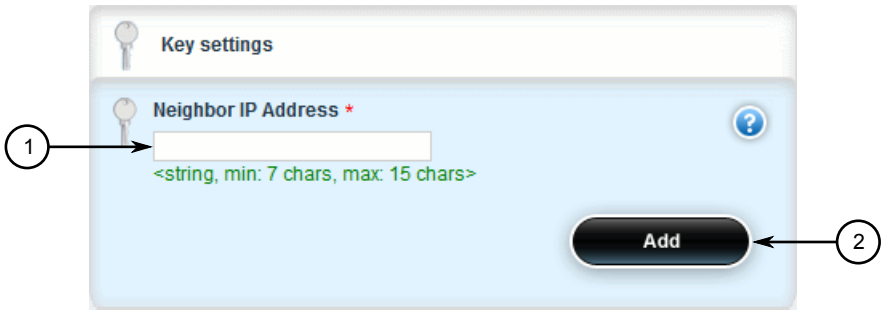


Figure 921: Key Settings Form

1. Neighbor IP Address Box **2.** Add Button

4. Configure the following parameter(s) as required:

Parameter	Description
Neighbor IP Address	**Synopsis:** 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.

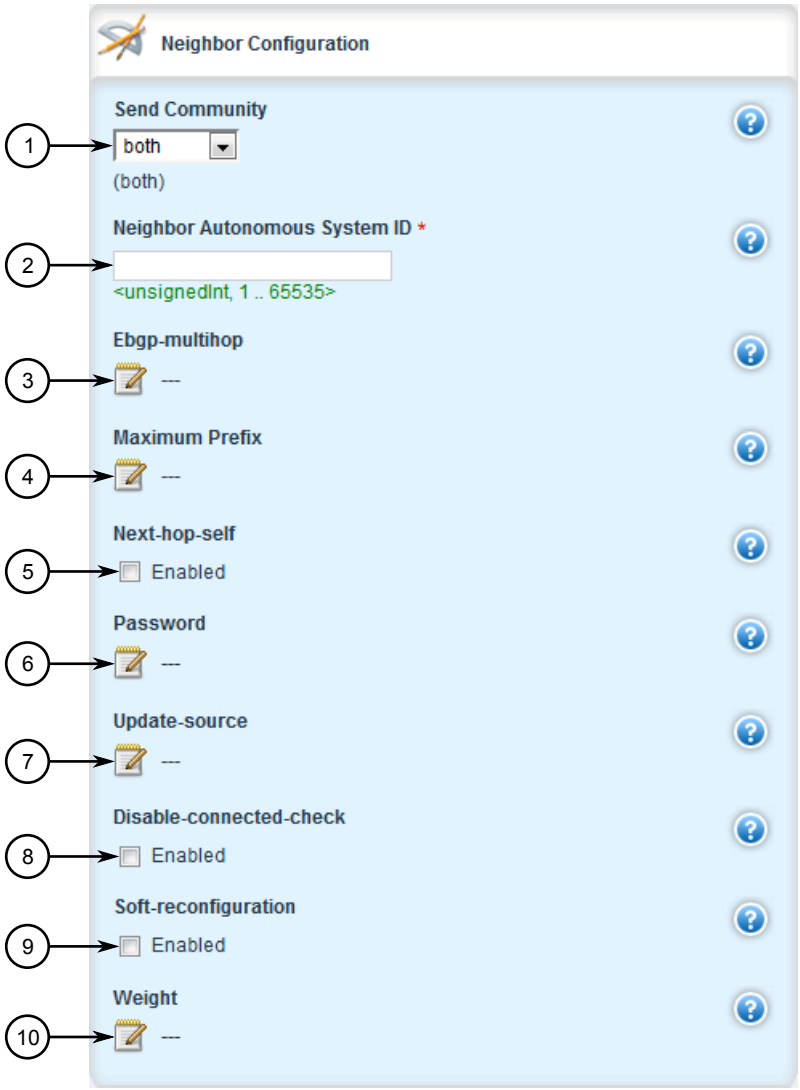


Figure 922: Neighbor Configuration Form

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

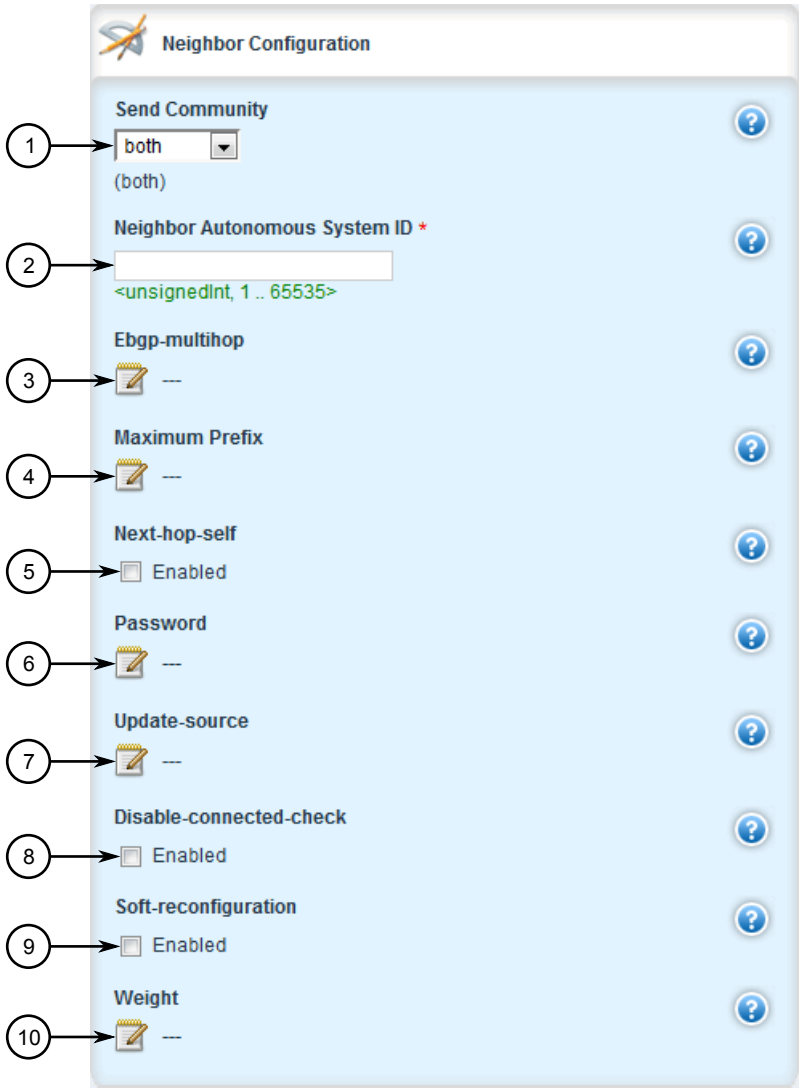


Figure 923: Route Maps Form

1. In List **2.** Out List

6. On the **Neighbor Configuration** form, configure the following parameter(s) as required:

Parameter	Description
Send Community	**Synopsis:** { standard, extended, both, none } **Default:** both Identifies the send Community. Default is both.
Neighbor Autonomous System ID	**Synopsis:** A 32-bit unsigned integer between 1 and 65535 A BGP neighbor. This parameter is mandatory.
ebgp-multihop	**Synopsis:** An 8-bit unsigned integer between 1 and 255

Parameter	Description
	The maximum hop count. This allows EBGP neighbors not on directly connected networks.
Maximum Prefix	**Synopsis:** A 32-bit unsigned integer between 1 and 4294967295 The maximum prefix number accepted from this peer.
next-hop-self	Disables the next hop calculation for this neighbor.
password	**Synopsis:** A string 1 to 1024 characters long Password.
update-source	**Synopsis:** A string 7 to 15 characters long Source IP address of routing updates.
disable-connected-check	Disables connection verification when establishing an eBGP peering session with a single-hop peer that uses a loopback interface.
soft-reconfiguration	Per neighbor soft reconfiguration.
weight	**Synopsis:** A 16-bit unsigned integer The default weight for routes from this neighbor.

7. On the **Route Maps** form, configure the following parameter(s) as required:

Parameter	Description
in	**Synopsis:** A string Apply route map to incoming routes.
out	**Synopsis:** A string Apply route map to outbound routes.

8. Configure the prefix list distribution. For more information, refer to Section 13.11.12.3, "Configuring the Distribution of Prefix Lists".
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 13.11.12.3
Configuring the Distribution of Prefix Lists

To configure the distribution of prefix lists for a neighbor in an IPv4 address family, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Make sure the desired prefix list is configured for the BGP network. For more information, refer to Section 13.8.4.3, "Adding a Prefix List".
3. 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.
4. 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.

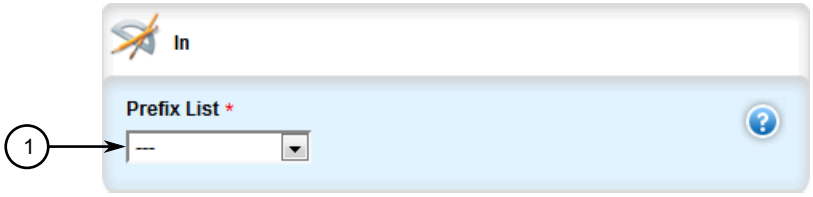


Figure 924: In Form (Example)

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 13.11.12.4, "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 13.11.12.4

Tracking Commands

Network commands can be tracked using event trackers configured under ***global » tracking***. For more information about event trackers, refer to Section 13.5, "Managing Event Trackers".

A network command is activated based on the event tracker's state. The **Apply When** parameter determines when the command is activated. For example, if the **Apply When** parameter is set to **`down`**, the network command becomes active (thereby advertising the network to a router's RIP peers) when the tracked target is unavailable.

To track a command for an IPv4 address family, do the following:

1. 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 13.7.8, "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

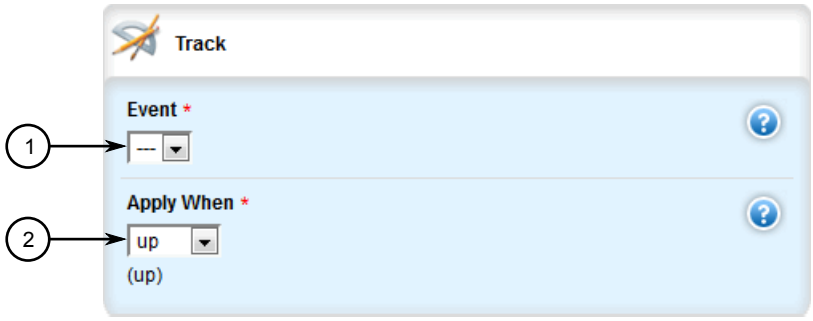


Figure 925: Track Form

1. Event List **2.** Apply When List

5. Configure the following parameter(s) as required:

Parameter	Description
event	**Synopsis:** A string Select to track an event, apply the distribute-prefix-list only when the tracked event goes to UP state. This parameter is mandatory.
apply-when	**Synopsis:** { up, down } **Default:** 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 13.11.12.5
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 926: 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 13.11.13

Managing Static VRF Routes

Routing information can be shared between routers using dynamic routing data or they can be manually configured. Static routes are explicit paths between routers that are manually configured. Static routes are commonly used for stable, often smaller networks whose configurations are not prone to change. They can be used to supplement dynamic routes.

CONTENTS

Section 13.11.13.1

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.

Figure 927: VRF Static Route Table

If no static routes have been configured, add routes as needed. For more information, refer to Section 13.11.13.2, "Adding a Static VRF Route".

Section 13.11.13.2
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.

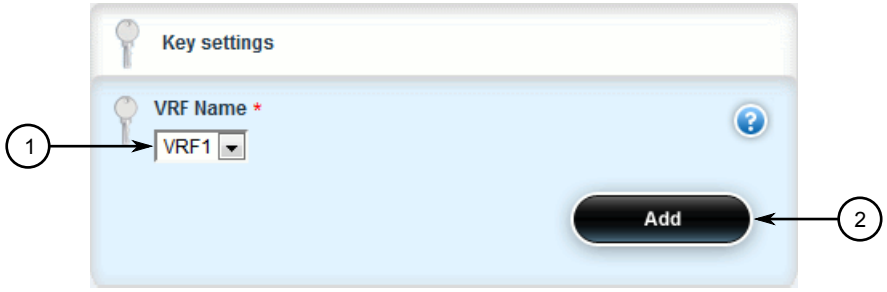


Figure 928: Key Settings Form

1. VRF Name Box **2.** Add Button

3. Configure the following parameter(s) as required:

Parameter	Description
VRF Name	**Synopsis:** A string The VRF name.

4. In the menu, click **ipv4** and then click **<Add route>**. The **Key Settings** form appears.

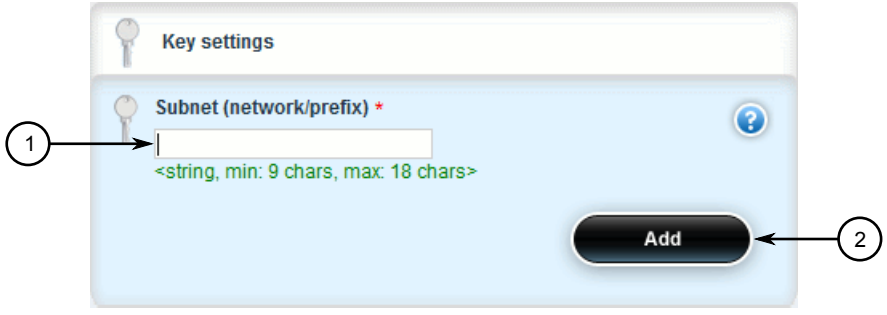


Figure 929: Key Settings Form

1. Subnet (Network/Prefix) Box **2.** Add Button

5. Configure the following parameter(s) as required:

Parameter	Description
Subnet (network/prefix)	**Synopsis:** 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.

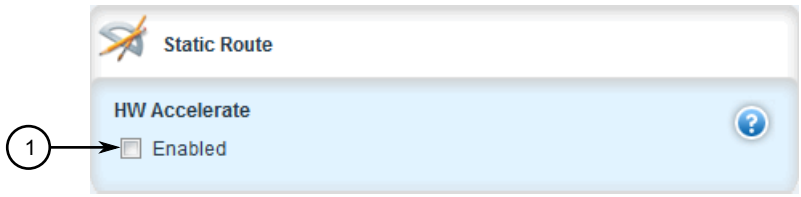


Figure 930: Static Route Form

1. Hardware Accelerate Check Box

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	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 13.11.13.3, "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 13.11.14.2, "Adding a Gateway for a Static VRF Route".
10. If necessary, add interfaces for the static route. For more information, refer to Section 13.11.15.2, "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 13.11.13.3
Configuring a Black Hole Connection for a Static VRF Route

To configure a black hole connection for a static VRF route, do the following:

1. 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.
3. Click the **+** symbol in the menu next to *blackhole*. The **VRF Blackhole Static Route** form appears.

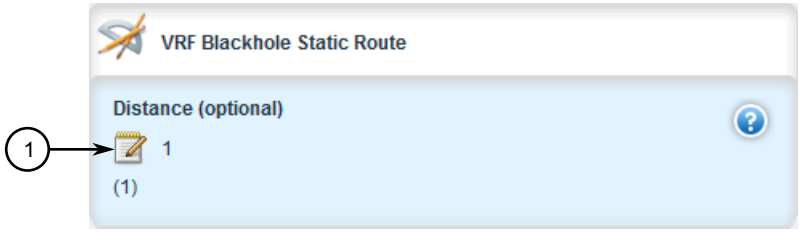


Figure 931: VRF Blackhole Static Route Form

1. Distance Box

4. Configure the following parameter(s) as required:

Parameter	Description
Distance (optional)	**Synopsis:** A 32-bit unsigned integer between 1 and 255 **Default:** 1 The distance for this static route's blackhole. Default is 1.

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 13.11.13.4

Deleting a Static VRF Route

To delete an IPv4 static route configured for a VRF instance, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to ***routing » static » vrf » {vrf} » ipv4***, where *vrf* is the chosen VRF instance. The **VRF Static Route** table appears.

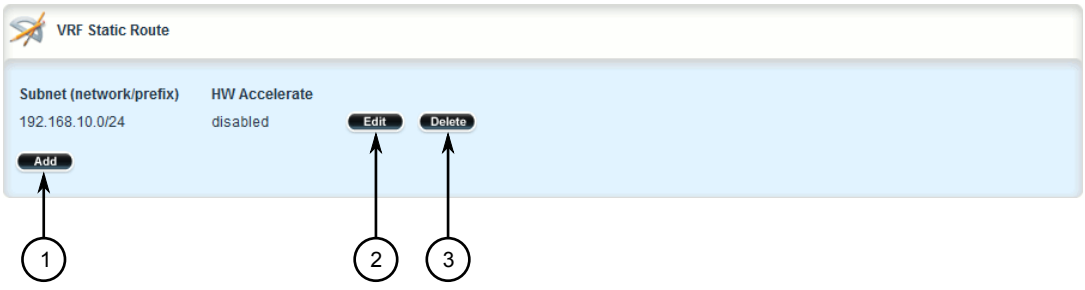


Figure 932: VRF Static Route Table

1. Add Button **2.** Edit Button **3.** Delete Button

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 13.11.14
Managing Gateways for Static VRF Routes

This section describes how to configure and manage gateways for static VRF routes.

CONTENTS

Section 13.11.14.1
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.

Figure 933: VRF Static Route Using Gateway Table

If no gateway addresses have been configured, add addresses as needed. For more information, refer to Section 13.11.14.2, "Adding a Gateway for a Static VRF Route".

Section 13.11.14.2
Adding a Gateway for a Static VRF Route

To add a gateway address for a static VRF route, do the following:

1. 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.

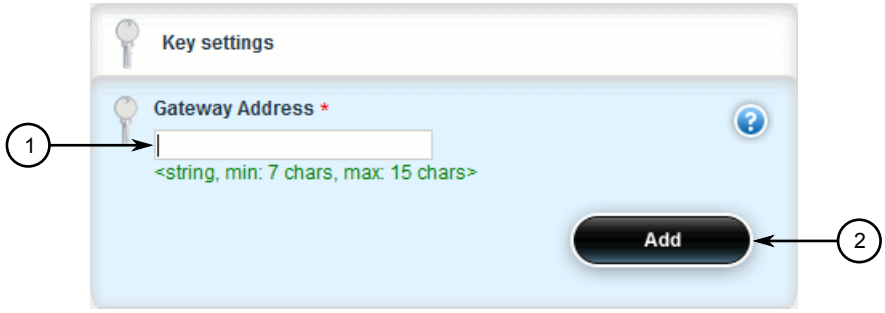


Figure 934: Key Settings Form

1. Gateway Address Box **2.** Add Button

4. Configure the following parameter(s) as required:

Parameter	Description
Gateway Address	**Synopsis:** 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.

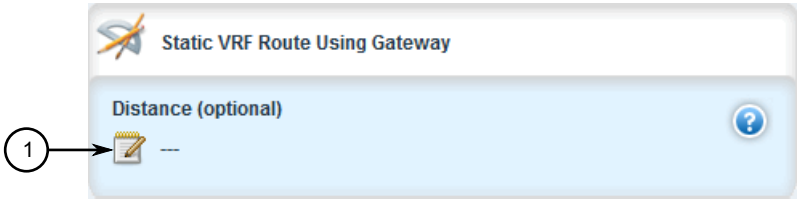


Figure 935: Static VRF Route Using Gateway Form

1. Distance Box

6. Configure the following parameter(s) as required:

Parameter	Description
Distance (optional)	**Synopsis:** A 32-bit unsigned 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 13.11.14.3

Deleting a Gateway for a Static VRF Route

To delete a gateway address assigned to a static VRF route, do the following:

1. 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.

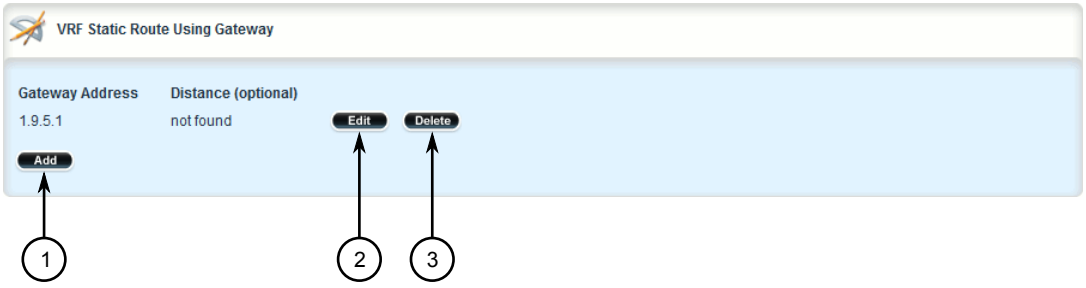


Figure 936: VRF Static Route Using Gateway Table

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 13.11.15

Managing Interfaces for Static VRF Routes

This section describes how to manage interfaces used for static VRF routes.

CONTENTS

Section 13.11.15.1

Viewing a List of Interfaces 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.

Figure 937: VRF Static Route Using Interface Table

If no gateway addresses have been configured, add addresses as needed. For more information, refer to Section 13.11.15.2, "Adding a Gateway for a Static VRF Route".

Section 13.11.15.2
Adding a Gateway for a Static VRF Route

To add an interface for an static VRF route, do the following:

1. 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.

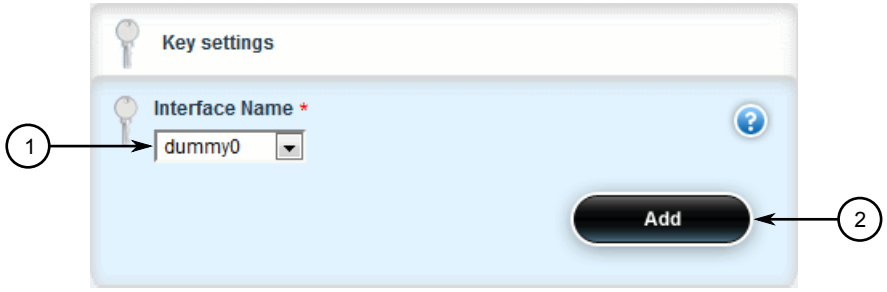


Figure 938: Key Settings Form

1. Interface Name List **2.** Add Button

4. Configure the following parameter(s) as required:

Parameter	Description
Interface Name	**Synopsis:** A string The interface for the static route.

5. Click **Add** to add the interface. The **Static VRF Route Using Interface** form appears.

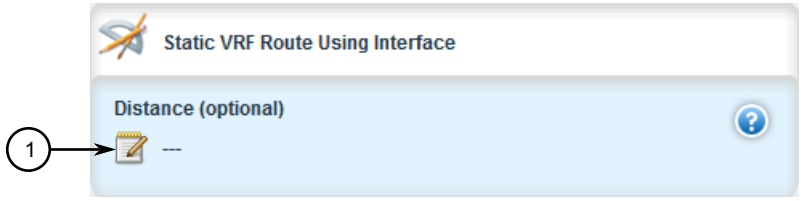


Figure 939: Static VRF Route Using Interface Form

1. Distance Box

6. Configure the following parameter(s) as required:

Parameter	Description
Distance (optional)	**Synopsis:** A 32-bit unsigned 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 13.11.15.3
Deleting a Gateway for a Static VRF Route

To delete an interface assigned to a static VRF route, do the following:

1. 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. The **VRF Static Route Using Interface** table appears.

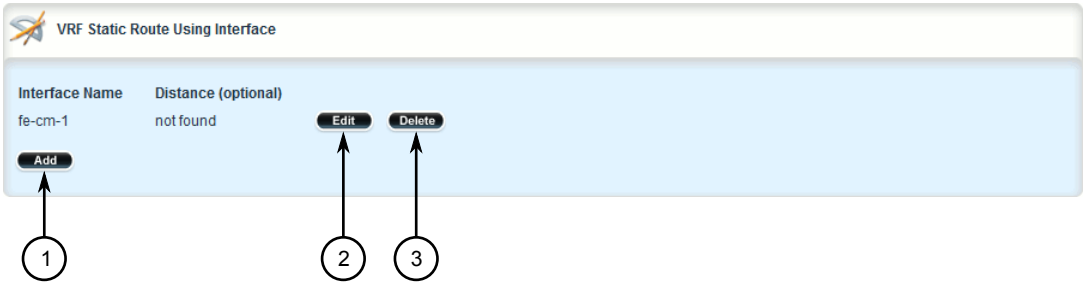


Figure 940: VRF Static Route Using Interface Table

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 13.12
Managing Static Routing

Static routes can be manually added to the routing table when there are no notifications sent by other routers regarding network topology changes.

CONTENTS

Section 13.12.1
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.

Figure 941: Static Route Table

If no static routes have been configured, add routes as needed. For more information, refer to Section 13.12.2, "Adding an IPv4 Static Route" or Section 13.12.3, "Adding an IPv6 Static Route".

Section 13.12.2
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.

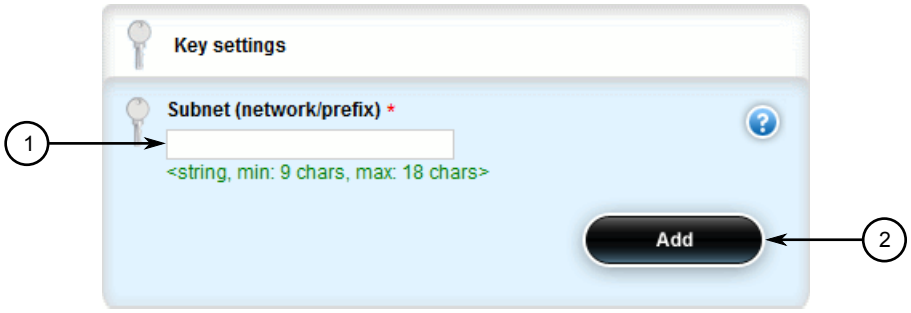


Figure 942: Key Settings Form

1. Subnet (Network/Prefix) Box **2.** Add Button

3. Configure the following parameter(s) as required:

IMPORTANT!
If the route is to be configured as a black hole route, make sure the subnet matches that of another static route. The black hole route will then act as a backup should the other static route go down.

Parameter	Description
Subnet (network/prefix)	**Synopsis:** A string 9 to 18 characters long The subnet (network/mask) of the static route.

4. Click **Add** to add the route. If the device has a Layer 3 switch installed, the **Static Route** form appears.

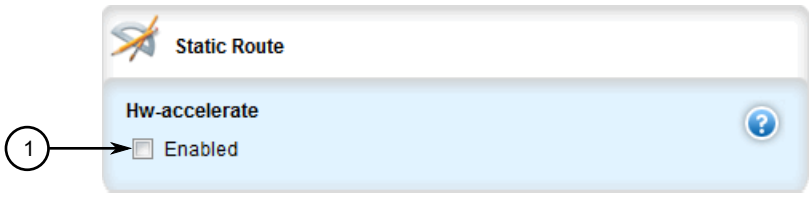


Figure 943: Static Route Form

1. Hardware Accelerate Check Box

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
HW Accelerate	If the static unicast route can be hardware accelerated, this option will be available. For a static unicast route to be accelerated, the ingress and egress interfaces must be switched.

6. [Optional] Configure the route as a black hole route. For more information, refer to Section 13.12.5, "Configuring a Black Hole Connection for an IPv4 Static Route".
7. [Optional] If the static route is not a black hole route, configure either the interface that connects to the next-hop router (if there is a direct connection) or the IP address (gateway) of the next-hop router. Only one can be configured per static route. For more information, refer to either Section 13.12.6.3, "Adding a Gateway for an IPv4 Static Route" or Section 13.12.7.3, "Adding an Interface for an IPv4 Static Route".
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 13.12.3
Adding an IPv6 Static Route

To add an IPv6 static route, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to ***routing » static » ipv6*** and click **<Add route>**. The **Key Settings** form appears.

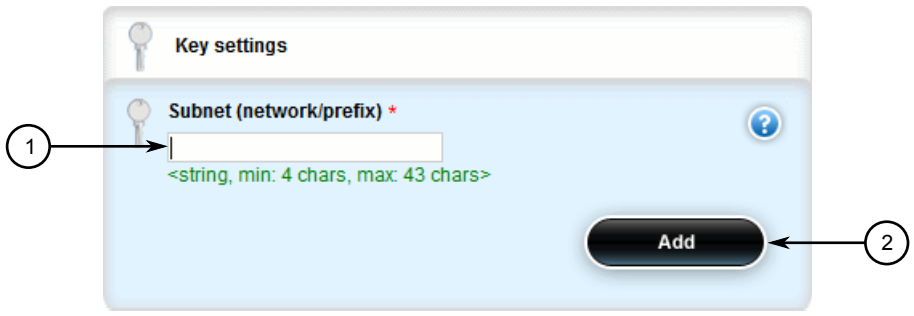


Figure 944: Key Settings Form

1. Subnet (Network/Prefix) Box **2.** Add Button

3. Configure the following parameter(s) as required:

Parameter	Description
Subnet (network/prefix)	**Synopsis:** A string 4 to 43 characters long The subnet (network/mask) of the static route.

4. Click **Add** to add the route.
5. Configure the next hop IP address (gateway) or interface. Only one can be configured per static route. For more information, refer to Section 13.12.6.1, "Configuring Gateways for IPv6 Static Routes" or Section 13.12.7.1, "Configuring Interfaces for IPv6 Static 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 13.12.4
Deleting a Static Route

To delete a static route, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to ***routing » static » {protocol}***, where *{protocol}* is either *IPv4* or *IPv6*. The **Static Route** table appears.

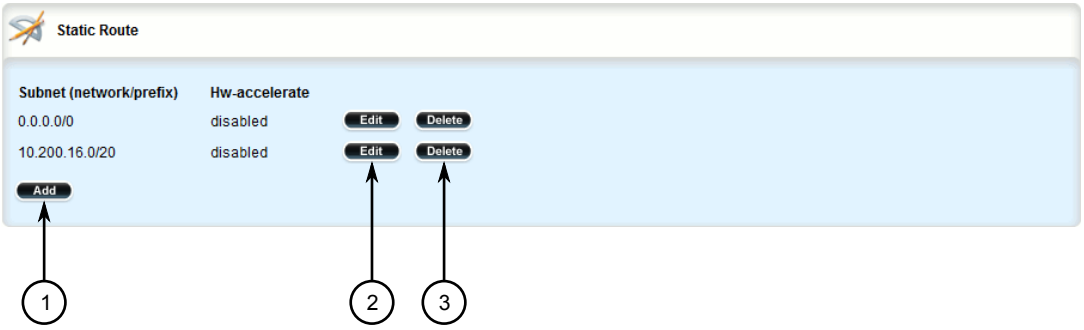


Figure 945: Static Route Table

1. Add Button **2.** Edit Button **3.** Delete Button

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 13.12.5
Configuring a Black Hole Connection for an IPv4 Static Route

To configure a black hole connection for an IPV4 static route, do the following:

1. 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.

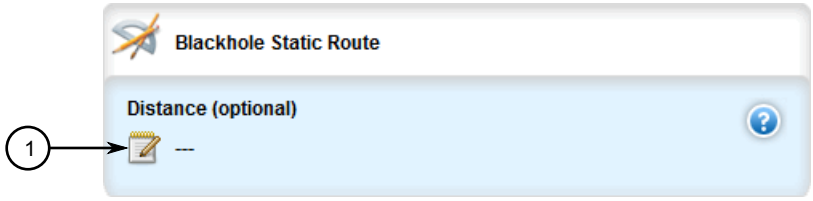


Figure 946: Blackhole Static Route Form

1. Distance Box

4. Configure the following parameter(s) as required:

Parameter	Description
Distance (optional)	**Synopsis:** A 32-bit unsigned integer between 1 and 255 **Default:** 1 The distance for this static route's blackhole. Default is 1.

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 13.12.6

Managing Gateways for Static Routes

If the device is not directly connected to the next-hop router, configure a static route to forward traffic to the next-hop router's IP address. This is referred to as a *gateway*.

In the case of IPv6 static routes, only one gateway can be selected per route.

CONTENTS

Section 13.12.6.1

Configuring Gateways for IPv6 Static Routes

To configure a gateway address 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 *via*. The **Static Route Using Gateway** form appears

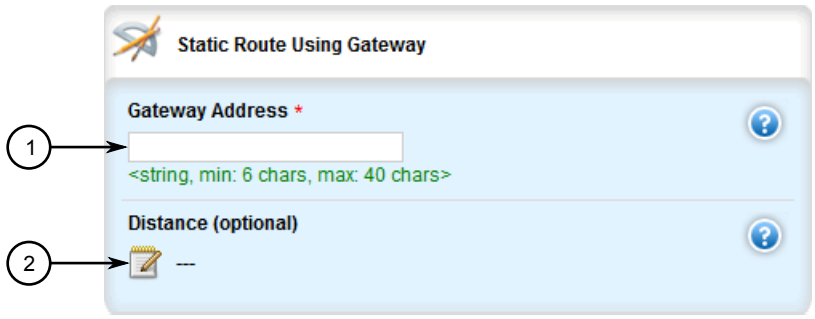


Figure 947: Static Route Using Gateway Form

1. Gateway Address Box **2.** Distance Box

4. Configure the following parameter(s) as required:

Parameter	Description
Gateway Address	**Synopsis:** A string 6 to 40 characters long The gateway for the static route. This parameter is mandatory.
Distance (optional)	**Synopsis:** A 32-bit unsigned 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 13.12.6.2
Viewing a List of Gateways for IPv4 Static Routes

To view a list of gateway addresses assigned to an IPv4 static route, 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.

Figure 948: Static Route Using Gateway Table

If no gateway addresses have been configured, add addresses as needed. For more information, refer to Section 13.12.6.3, “Adding a Gateway for an IPv4 Static Route”.

Section 13.12.6.3

Adding a Gateway for an IPv4 Static Route

To add a gateway address for an IPv4 static route, do the following:

1. 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.
3. Click **<Add via>**. The **Key Settings** form appears.

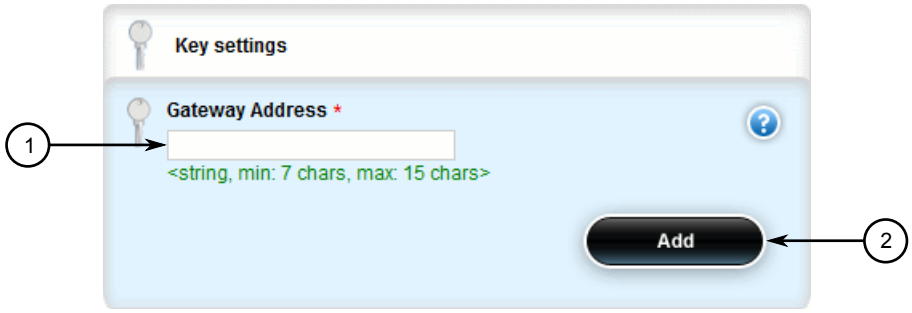


Figure 949: Key Settings Form

1. Gateway Address Box **2.** Add Button

4. Configure the following parameter(s) as required:

Parameter	Description
Gateway Address	**Synopsis:** 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.

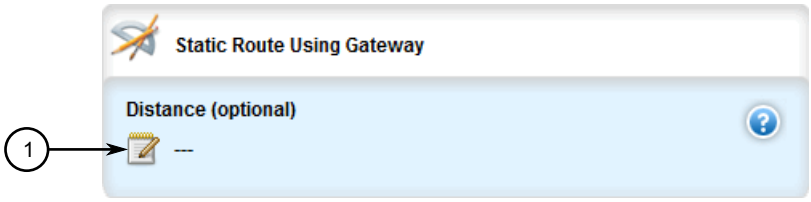


Figure 950: Static Route Using Gateway Form

1. Distance Box

6. Configure the following parameter(s) as required:

Parameter	Description
Distance (optional)	**Synopsis:** A 32-bit unsigned 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 13.12.6.4
Deleting a Gateway for an IPv4 Static Route

To delete a gateway for an IPv4 static route, do the following:

1. 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.

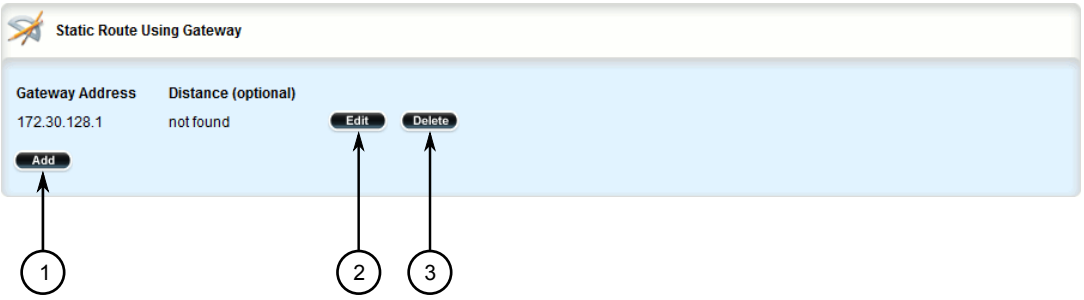


Figure 951: Static Route Using Gateway Table

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 13.12.7
Managing Interfaces for Static Routes

Static routes can be configured to forward packets to an exit interface. Assuming the device is directly connected to a neighboring router, the device will send Address Resolution Protocol (ARP) requests to determines the next hop IP address.

In the case of IPv6 static routes, only one interface can be selected per route.

CONTENTS

Section 13.12.7.1
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

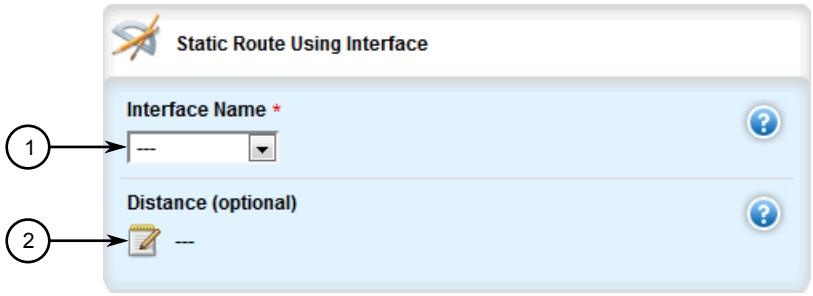


Figure 952: Static Route Using Interface Form

1. Interface Name Box **2.** Distance Box

4. Configure the following parameter(s) as required:

Parameter	Description
Interface Name	**Synopsis:** A string The interface for the static route. This parameter is mandatory.
Distance (optional)	**Synopsis:** A 32-bit unsigned 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 13.12.7.2
Viewing a List of Interfaces for IPv4 Static Routes

To view a list of interfaces assigned to an IPv4 static route, 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.

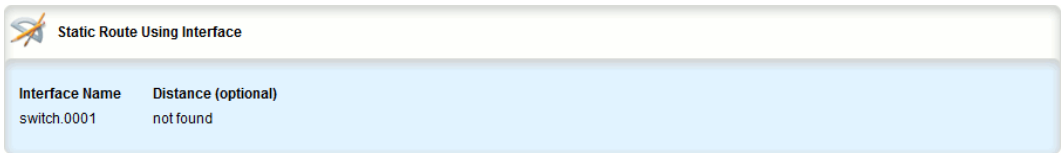


Figure 953: Static Route Using Interface Table

If no interfaces have been configured, add interfaces as needed. For more information, refer to Section 13.12.7.3, "Adding an Interface for an IPv4 Static Route".

Section 13.12.7.3

Adding an Interface for an IPv4 Static Route

To add an interface for an IPv4 static route, do the following:

1. 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.

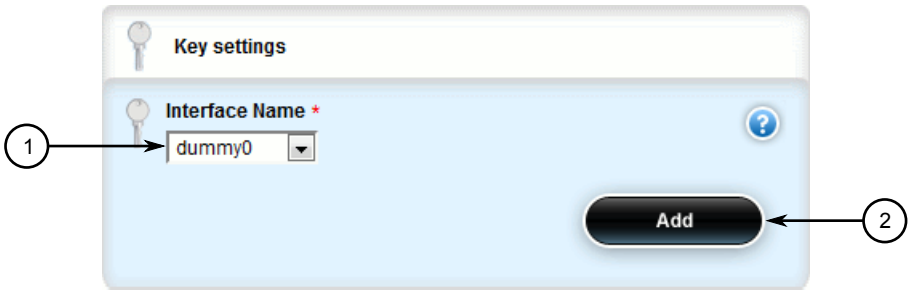


Figure 954: Key Settings Form

1. Interface Name Box **2.** Add Button

4. Configure the following parameter(s) as required:

Parameter	Description
Interface Name	**Synopsis:** A string The interface for the static route.

5. Click **Add** to add the interface. The **Static Route Using Interface** form appears.

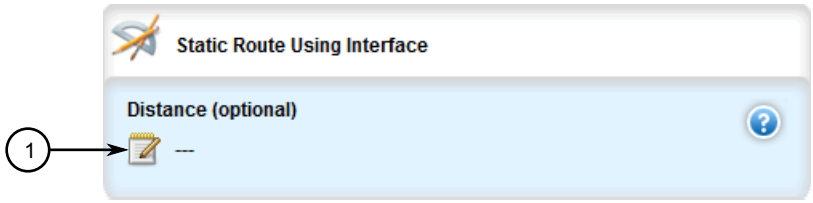


Figure 955: Static Route Using Interface Form

1. Distance Box

6. Configure the following parameter(s) as required:

Parameter	Description
Distance (optional)	**Synopsis:** A 32-bit unsigned 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 13.12.7.4

Deleting an Interface for an IPv4 Static Route

To delete an interface for an IPv4 static route, do the following:

1. 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.

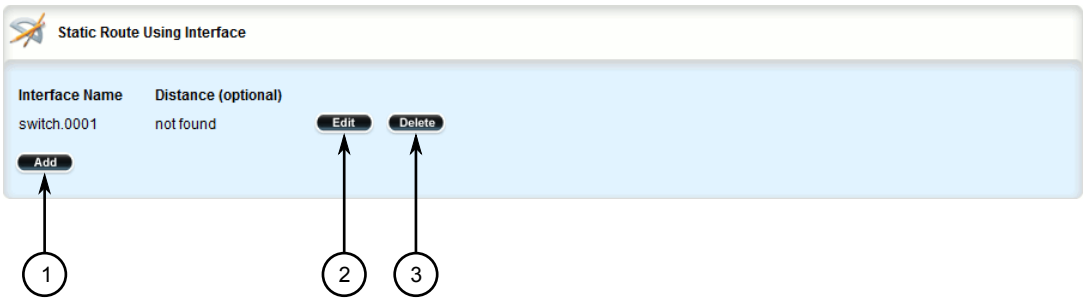


Figure 956: Static Route Using Interface Table

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 13.13
Managing Static Multicast Routing

Static multicast routing allows network designers to control the flow of multicast traffic by manually adding static routes to the routing table.

CONTENTS

Section 13.13.1
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.

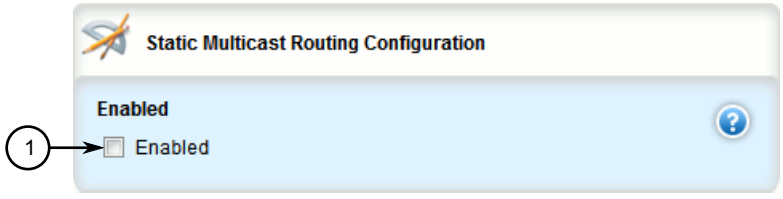


Figure 957: Static Multicast Routing Configuration Form

1. Enabled Check Box

3. Configure the following parameter(s) as required:

Parameter	Description
enabled	Enables static multicast routing 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 13.13.2
Managing Static Multicast Groups

Define a static multicast group for each multicast route. Multiple routes can be configured, as long as the source and multicast IP addresses are unique to the route.

IMPORTANT!
The source IP address for static routes is always a unicast address (e.g. 192.168.0.10), while the destination IP address is always a multicast address (e.g. 225.2.100.1).

CONTENTS

Section 13.13.2.1
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.

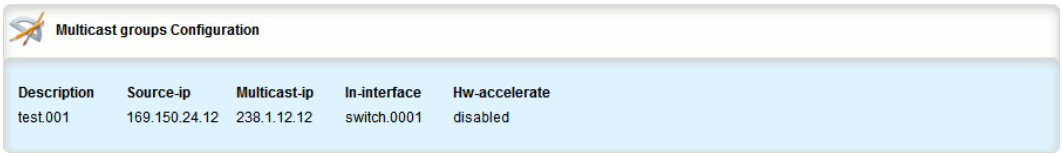


Figure 958: Multicast Groups Configuration Table

If no static multicast groups have been configured, add groups as needed. For more information about adding static multicast groups, refer to Section 13.13.2.2, "Adding a Static Multicast Group".

Section 13.13.2.2
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.

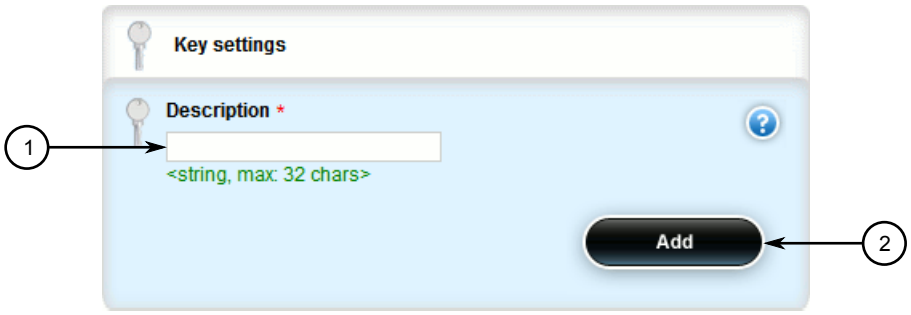


Figure 959: Key Settings Form

1. Description Box **2.** Add Button

3. Configure the following parameter(s) as required:

Parameter	Description
description	**Synopsis:** A string 1 to 32 characters long Describes the multicast group, spaces are not allowed.

4. Click the **Add** button. The **Multicast Group Configuration** form appears.

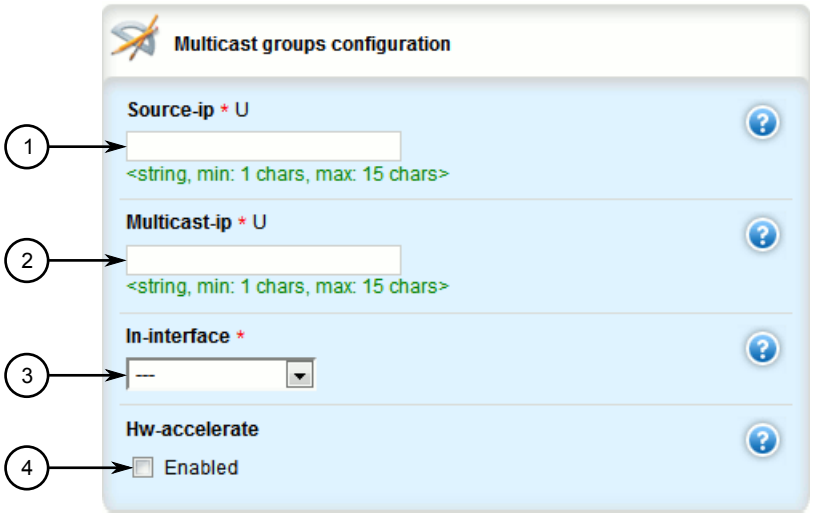


Figure 960: Multicast Group Configuration Form

1. Source-ip Box **2.** Multicast-ip Box **3.** In-interface List **4.** Hw-accelerate Check Box

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	**Synopsis:** A string 7 to 15 characters long or a string 6 to 40 characters long The expected source IP address of the multicast packet, in the format xxx.xxx.xxx.xxx. This address is uniquely paired with the multicast address. You cannot use this IP address to create another multicast routing entry with a different Multicast-IP address. This parameter is mandatory.
Multicast IP	**Synopsis:** A string 7 to 15 characters long or a string 7 to 39 characters long The multicast IP address to be forwarded, in the format xxx.xxx.xxx.xxx The address must be in the range of 224.0.0.0 to 239.255.255.255. This address is uniquely paired with the source IP address. You cannot use this IP address to create another multicast routing entry with a different Source-IP address. This parameter is mandatory.
In Interface	**Synopsis:** A string The interface upon which the multicast packet arrives. This parameter is mandatory.
Hardware Accelerate	If the multicast route can be hardware accelerated, the option will be available. For a multicast route to be accelerated, the ingress and egress interfaces must be switched.

6. Configure out-interfaces. Refer to Section 13.13.3.2, "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 13.13.2.3
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.

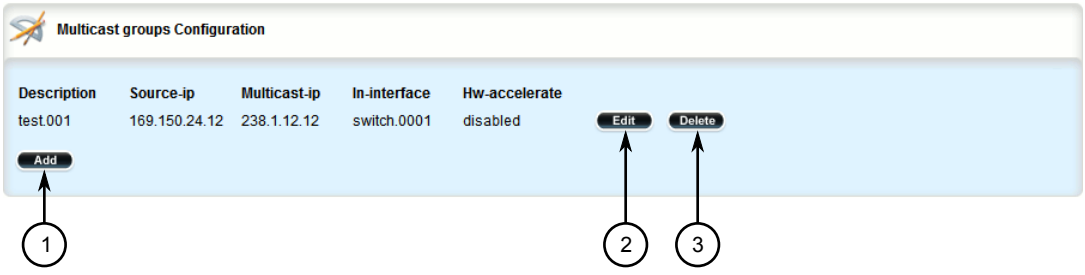


Figure 961: Multicast Groups Configuration Table

1. Add Button **2.** Edit Button **3.** Delete Button

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 13.13.3
Managing Out-Interfaces

An out-interface is the interface to which multicast packets are forwarded. Multiple out-interfaces can be defined for each static multicast group.

CONTENTS

Section 13.13.3.1
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.

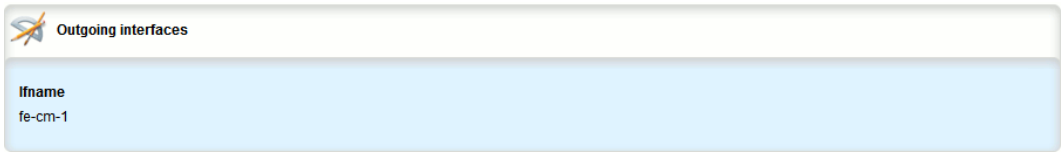


Figure 962: Outgoing Interfaces Table

If no out-interfaces have been configured, add groups as needed. For more information about adding out-interfaces, refer to Section 13.13.3.2, "Adding an Out-Interface".

Section 13.13.3.2
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 963: Key Settings Form

1. Ifname List **2.** Add Button

4. Configure the following parameter(s) as required:

Parameter	Description
Interface Name	**Synopsis:** A string

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 13.13.3.3
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.

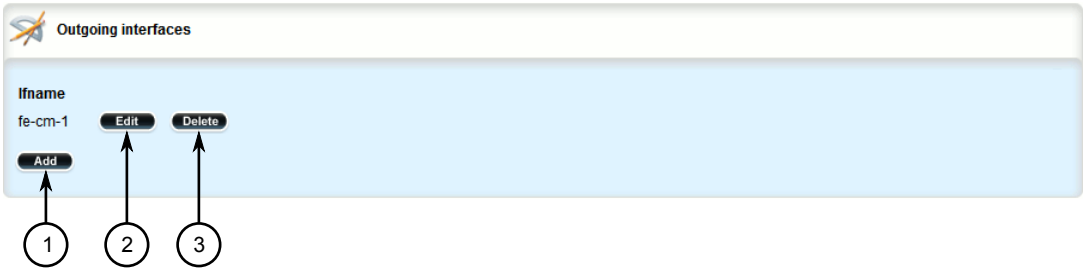


Figure 964: Outgoing Interfaces Table

1. Add Button **2.** Edit Button **3.** Delete Button

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 13.14

Managing Dynamic Multicast Routing

The PIM-SM feature is used for Dynamic Multicast Routing. PIM-SM stands for Protocol Independent Multicast - Sparse Mode. It is a dynamic multicast routing protocol that can dynamically prune and maintain multicast routes. PIM relies on the router's unicast routing table for its capabilities and does not rely on any specific method for learning routes, therefore it is "Protocol Independent".

The following terms are used in PIM-SM:

- **Rendezvous Point**
  The rendezvous point (RP) is a destination in the network (one of the routers), where all multicast traffic is first registered. Whenever a PIM router receives a multicast stream, the source and the multicast address are registered with the rendezvous point.
- **Boot Strap Router**
  A PIM-SM boot strap router (BSR) is a router that announces the location of the rendezvous point to all other PIM routers on the network.
- **Designated Router**
  A designated router (DR) is a router directly attached to a multicast host or device. The router with the highest IP address usually becomes the designated router.
- **Shared Tree**
  The shared tree, also known as the RP-Tree, is a traffic distribution tree which begins from the rendezvous point. The rendezvous point will forward the particular multicast group traffic through this tree whenever there are subscribers for a given multicast flow. Note that the shared tree is on a per-group basis. This means that the shared tree for one group could be different than the shared tree for another on the same network depending on the distribution of the multicast traffic subscribers.
- **Shortest Path Tree**
  The shortest path tree (SPT) is a traffic distribution tree which begins at the source of the multicast traffic or rather the router nearest to the source. The shortest path tree is activated whenever there is a shorter path between the source and the receiver. The shortest path tree can only be triggered by the rendezvous point or the router connected directly to the subscriber.
- **Internet Group Management Protocol**
  Internet Group Management Protocol (IGMP) is the protocol used by hosts and routers to join and leave multicast groups. Routers will send IGMP queries at regular intervals querying whether there are any hosts interested in IP multicast traffic. Whenever an attached host is interested in receiving traffic for a certain group, it will send an IGMP report message expressing its interest. The router will then a) propagate this Join message to another router and b) send the relevant traffic to the segment to which the host is attached.

CONTENTS

Section 13.14.1
PIM-SM Concepts

When a PIM router receives a subscription from a host, e.g. Host A, for particular multicast traffic, the directly attached designated router (DR) sends a PIM join message for this multicast group towards the rendezvous point (RP). The message is sent hop-by-hop and thus any routers encountering the message would register the group and send the message onwards towards the RP. This would create the shared tree (RP-tree). The tree will not be complete, however, until any sources appear.

When a host or device sends multicast traffic destined to the multicast group subscribed by A, the directly attached designated router takes the traffic, encapsulates it with PIM Register headers and unicasts them to the RP. When the RP receives this traffic, it decapsulates the packets and sends the data towards the subscriber through the RP tree. The routers that receive these packets simply pass them on over the RP-Tree until it reaches the subscriber. Note that there may be other subscribers in the network and the path to those subscribers from the RP is also part of the RP Tree.

After the shared tree has been established, the traffic flows from the source to the RP to the receiver. There are two inefficiencies in this process. One, the traffic is encapsulated at the source and decapsulated at the RP, which may be a performance penalty for a high level of traffic. Two, the traffic may be taking a longer path than necessary to reach its receivers.

After the shared tree has been established, the RP may choose to to send a Join message to the source declaring that it only wants traffic for a group (e.g. group G) from the source (e.g. source S). The DR for the source then starts sending the traffic in multicast form (instead of unicast). Without encapsulation, there is little performance overhead other than what is normal for the traffic when routing in general. The RP will continue sending the traffic over the RP-tree after it receives it. This also means that the traffic may reach the RP-tree before it reaches the RP (in the case where the source branches off the RP-tree itself) which will also have the additional benefit of traffic flowing more efficiently towards receivers that are on the same side of the RP-tree as the source.

If the DR to the receiver decided that traffic coming from the RP-tree was using a suboptimal path than if it was received from the source itself, it would issue a source-specific Join message towards the source. This would then make all intermediate routers register the Join message and then traffic would start flowing along that tree. This is the shortest path tree (SP-tree). At this point, the receiver would receive the traffic from both the RP-tree and the SP-tree. After the flow starts from the SP-tree, the DR will drop the packets from the RP-tree and send a prune message for that traffic towards the RP. This will stop the traffic from arriving from the RP. This scenario will most likely only occur when the traffic has to take a detour when arriving from the RP. Otherwise the RP-tree itself is used.

Section 13.14.2
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.

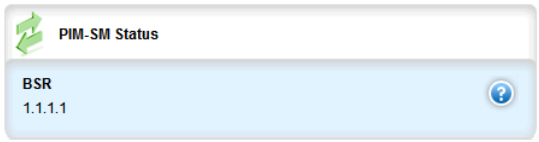


Figure 965: PIM-SM Status Form

2. Navigate to ***routing » status » pim-sm » vinterface***. The **Virtual Interface** table appears displaying the status of the configured devices.

NOTE
*A default rendezvous point with a local address of **169.254.0.1** always appears in the **Virtual Interface** table. This internal rendezvous point is a placeholder to reserve the source-specific multicast address range.*

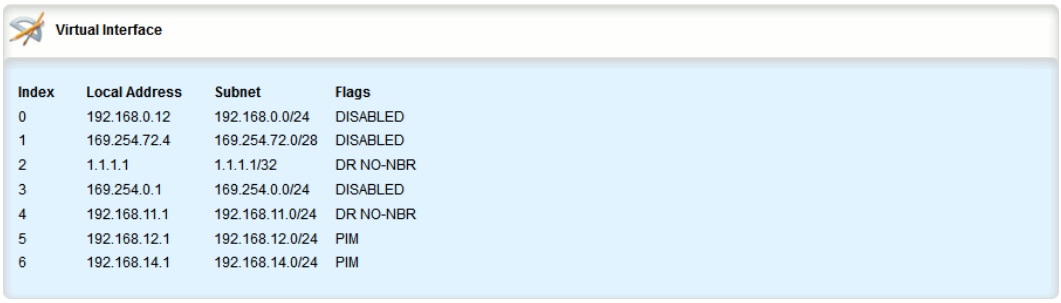


Figure 966: Virtual Interface Table

Parameter	Description
Index	**Synopsis:** A 32-bit unsigned integer Virtual interface index.
Local Address	**Synopsis:** A string 1 to 16 characters long Local address.
Subnet	**Synopsis:** A string 1 to 20 characters long Subnet.
Flags	**Synopsis:** A string 1 to 128 characters long Flags indicates virtual interface information. • DISABLED: The virtual interface is administratively disabled for PIM-SM. • DOWN: This virtual interface is down. • DR: Designated router. • NO-NBR: No neighbor on this virtual interface. • PIM: PIM neighbor. • DVMRP: DVMRP neighbor.

3. Navigate to ***routing » status » pim-sm » rp***. The **Rendezvous Point** table appears displaying the RP server addresses.

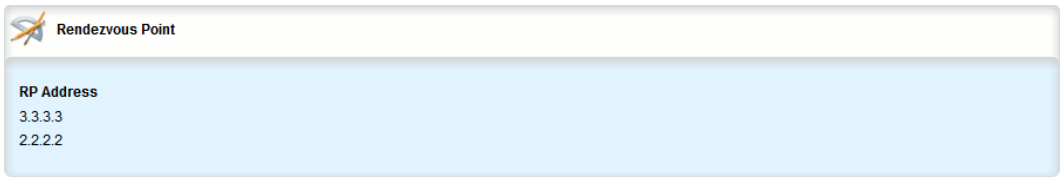


Figure 967: Rendezvous Point Table

Section 13.14.3
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.

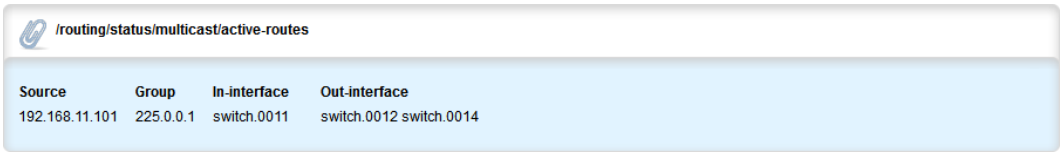


Figure 968: Active Routes Table

Section 13.14.4
Configuring PIM-SM

PIM-SM can be used to establish and dynamically manage the Multicast Routing table.

To configure PIM-SM, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to ***routing » multicast » dynamic » PIM-SM***. The **PIM-SM Configuration** form appears.

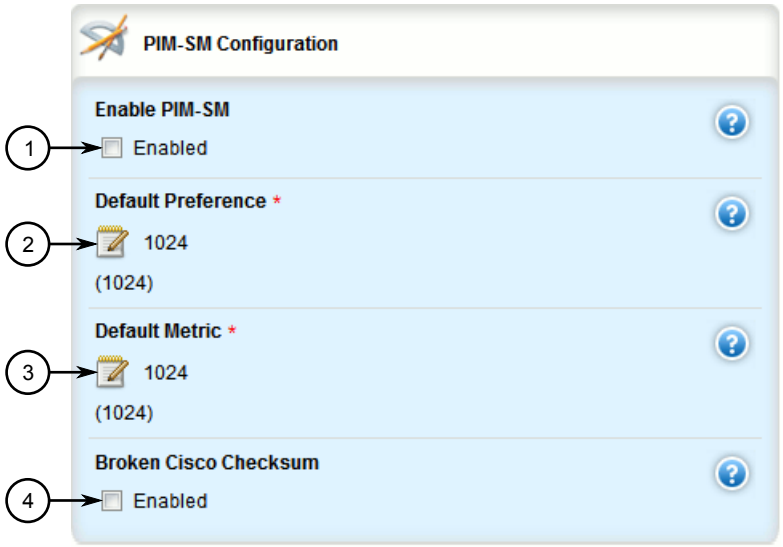


Figure 969: PIM-SM Configuration Form

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	Enable PIM-SM service.
Default Preference	**Synopsis:** A 16-bit unsigned integer equaling 1 or higher **Default:** 1024 Default preference value. Preferences are used by assert elections to determine upstream routers.
Default Metric	**Synopsis:** A 16-bit unsigned integer equaling 1 or higher **Default:** 1024 Default metric value. Metric is the cost of sending data through interface.
Broken Cisco Checksum	If your RP is a cisco and shows many PIM_REGISTER checksum errors from this router, setting this option will help.

4. 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 13.14.5

Setting the Device as a BSR Candidate

To set the device as 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 then click the **+** symbol in the menu next to *bsr-candidate*. The **BSR Candidate** form appears.

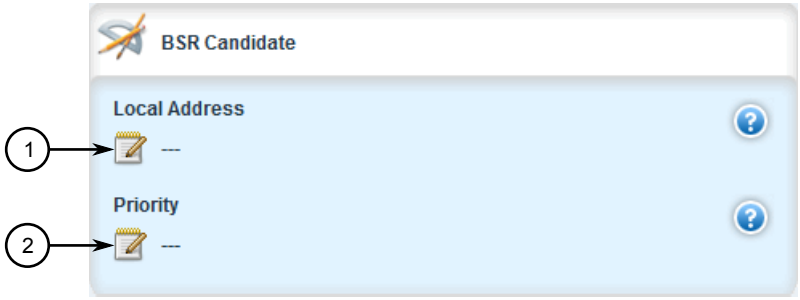


Figure 970: BSR Candidate Form

1. Local Address Box **2.** Priority Box

3. Configure the following parameters as required:

Parameter	Description
Local Address	**Synopsis:** 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	**Synopsis:** An 8-bit unsigned 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 13.14.6

Setting the Device as an RP Candidate

To set the device as 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*** and then click the **+** symbol in the menu. The **RP Candidate** form appears.

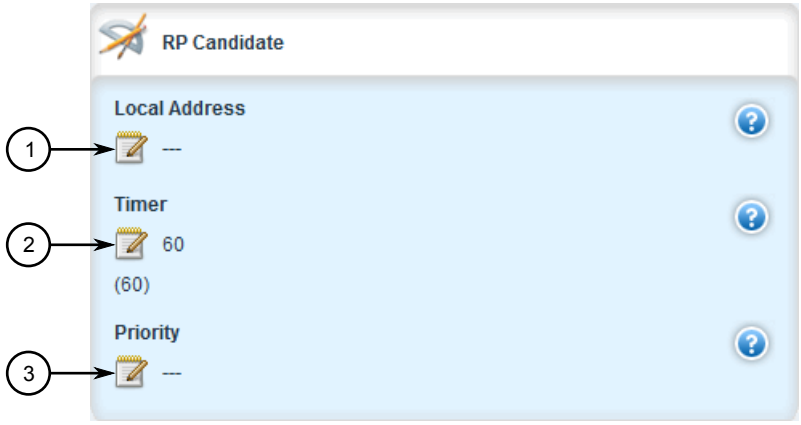


Figure 971: RP Candidate Form

1. Local Address Box **2.** Timer Box **3.** Priority Box

3. Configure the following parameters as required:

Parameter	Description
Local Address	**Synopsis:** 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	**Synopsis:** A 16-bit unsigned integer between 10 and 65535 **Default:** 60 The number of seconds to wait between advertising Cand-RP message.
Priority	**Synopsis:** An 8-bit unsigned integer between 1 and 255 Priority of this CRP, smaller 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 13.14.7
Managing PIM-SM Interfaces

PIM-SM requires at least one interface on which to receive or transmit advertisements. The interface must be non-passive and be assigned an IP address.

CONTENTS

Section 13.14.7.1
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.

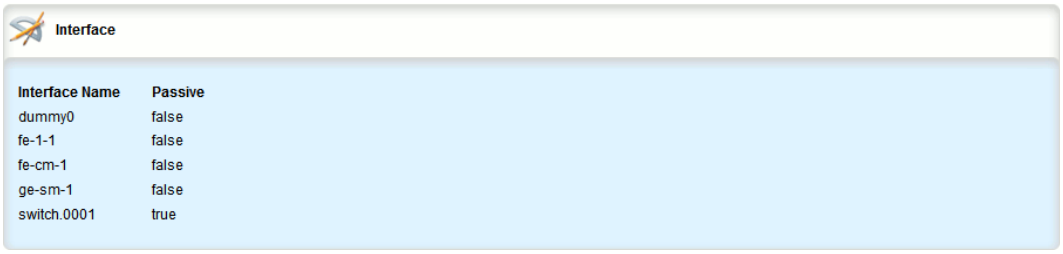


Figure 972: Interface Table

If no PIM-SM interfaces have been configured, enable interfaces as needed. For more information about enabling PIM-SM interfaces, refer to Section 13.14.7.2, "Enabling/Disabling a PIM-SM Interface".

Section 13.14.7.2
Enabling/Disabling a PIM-SM Interface

To enable or disable a PIM-SM interface, do the following:

NOTE
Enabling PIM-SM on an interface also enables IGMPv2 on the interface, wherein the interface with the lowest IP address becomes the IGMP querier and sends periodic query messages every 125 seconds.

1. 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.

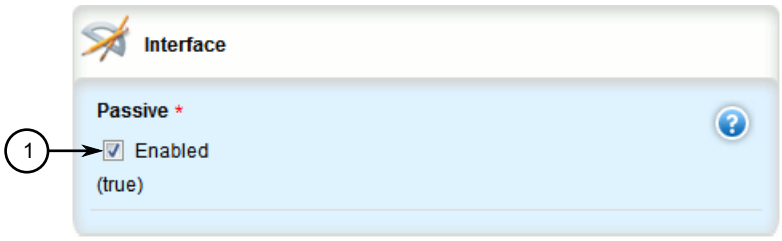


Figure 973: Interface Form

1. Enabled Check Box

4. Configure the following parameter(s) as required:

Parameter	Description
Interface Name	**Synopsis:** A string 1 to 32 characters long Interface name.
Passive	**Synopsis:** { true, false } **Default:** 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. Make sure the chosen interface is assigned an IP address. For more information, refer to Section 7.1, "Managing IP Addresses for Routable Interfaces".
6. For VLAN interfaces only, if IGMP snooping is enabled on the interface, make sure the IGMP query interval is set to 125 seconds. For more information, refer to Section 8.4.3.1, "Configuring IGMP Snooping".

   The same is required for any Layer 2 switches on the network.
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 13.14.8
Managing Static RP Addresses

A commonly used method for locating Rendezvous Points (RPs) is to target them directly by IP address, as opposed to locating them dynamically. Use static IP addresses when there are only a small number of RPs on the network and/or the RP assignment does not change often. It is important though that all static RP addresses be mirrored on all PIM-SM enabled devices in the multicast domain.

CONTENTS

Section 13.14.8.1
Viewing a List of Static RP Addresses

To view a list of static RP addresses, navigate to ***routing » multicast » dynamic » pim-sm » rp-address***. If addresses have been configured, the **RP Address** table appears.

Figure 974: RP Address Table

If no addresses have been configured, add addresses as needed. For more information, refer to Section 13.14.8.2, "Adding a Static RP Address".

Section 13.14.8.2
Adding a Static RP Address

To add 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 then click **<Add dest-address>**. The **Key Settings** form appears.

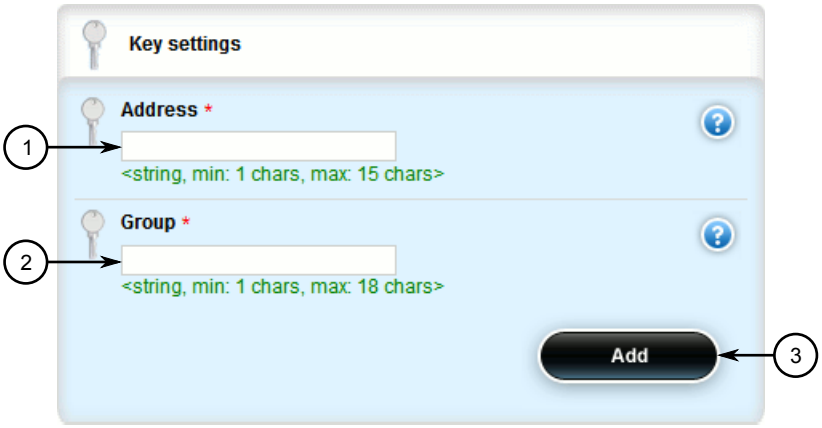


Figure 975: Key Settings Form

1. Address Box **2.** Group Box **3.** Add Button

3. Configure the following parameters as required:

Parameter	Description
Address	**Synopsis:** A string 7 to 15 characters long Static RP (Rendezvous Point) address.
Group	**Synopsis:** A string 9 to 18 characters long The multicast group the RP handles.

4. Click **Add** to add the static RP address. The **RP Address** form appears.

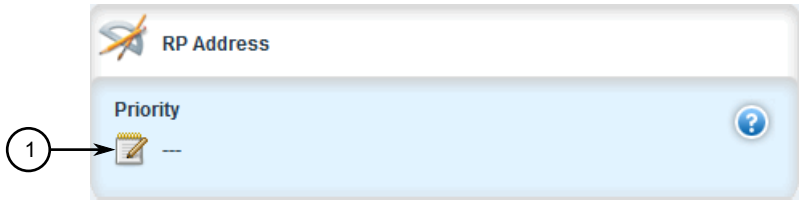


Figure 976: RP Address Form

1. Priority Box

5. Configure the following parameters as required:

Parameter	Description
Priority	**Synopsis:** An 8-bit unsigned integer between 1 and 255 Priority of the RP.

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 13.14.8.3

Deleting a Static RP Address

To delete 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***. The **RP Address** table appears.

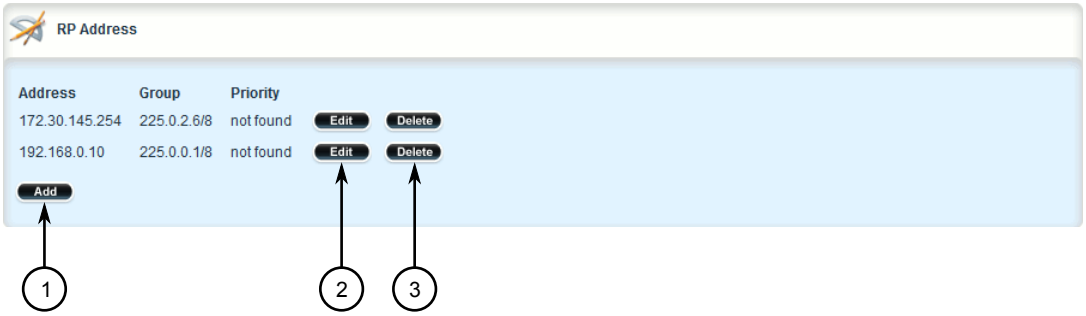


Figure 977: RP Address Table

1. Add Button **2.** Edit Button **3.** Delete Button

3. Click **Delete** next to the chosen RP 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 13.14.9

Managing Multicast Group Prefixes

When nominated to a Rendezvous Point (RP), the device can serve up to 20 groups of multicast devices. The device is associated with a multicast group by defining the prefix for the group's multicast IP address (e.g. 225.1.2.0/24).

CONTENTS

Section 13.14.9.1

Viewing a List of Multicast Group Prefixes

To view a list of multicast group prefixes, navigate to ***routing » multicast » dynamic » pim-sm » group-prefix***. If prefixes have been configured, the **Multicast Group Prefix** table appears.

Figure 978: Multicast Group Prefix Table

If no prefixes have been configured, add prefixes as needed. For more information, refer to Section 13.14.9.2, "Adding a Multicast Group Prefix".

Section 13.14.9.2

Adding a Multicast Group Prefix

To add a multicast group prefix, do the following:

NOTE
A maximum of 20 group prefixes can be defined for PIM-SM.

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to ***routing » multicast » dynamic » pim-sm » group-prefix*** and then click **<Add group-prefix>**. The **Key Settings** form appears.

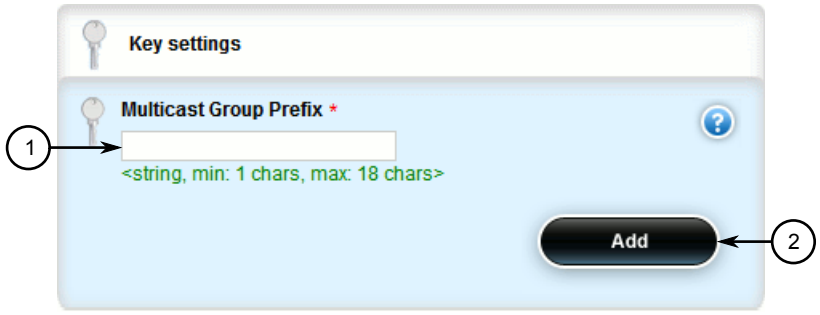


Figure 979: Key Settings Form

1. Multicast Group Prefix Box **2.** Add Button

3. Configure the following parameters as required:

Parameter	Description
Multicast Group Prefix	**Synopsis:** 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 13.14.9.3

Deleting a Multicast Group Prefix

To delete a multicast 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***. The **Multicast Group Prefix** table appears.

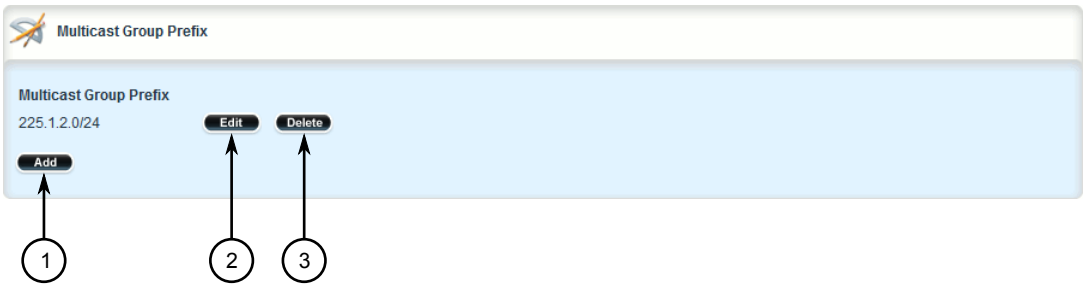


Figure 980: Multicast Group Prefix Table

1. Add Button **2.** Edit Button **3.** Delete Button

3. Click **Delete** next to the chosen prefix.

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.

14 Network Redundancy

This chapter describes protocols and features that allow RUGGEDCOM ROX II to operate with redundancy, protecting the network from crippling service disruptions from single points of failure.

CONTENTS

Section 14.1

Managing VRRP

The Virtual Router Redundancy Protocol (VRRP) is a gateway redundancy protocol. It provides a gateway failover mechanism invisible to hosts and other devices that send traffic through the gateway.

VRRP eliminates a single point of failure associated with statically routed networks by providing automatic failover using alternate routers. The RUGGEDCOM ROX II VRRP daemon (keepalived) is an RFC 5798 [http://tools.ietf.org/html/rfc5798] version 2 and version 3 compliant implementation of VRRP.

NOTE
RFC 5798 defines the standard for VRRP version 3 on IPv4 and IPv6. Only IPv4 is supported in this release of RUGGEDCOM ROX II.

CONTENTS

Section 14.1.1

VRRP Concepts

This section describes some of the concepts important to the implementation of the Virtual Router Redundancy Protocol (VRRP) in RUGGEDCOM ROX II.

CONTENTS

Section 14.1.1.1

Static Routing vs. VRRP

Many network designs employ a statically configured default gateway in the network hosts. A static default gateway is simple to configure, requires little if any overhead to run, and is supported by virtually every IP implementation. When the Dynamic Host Configuration Protocol (DHCP) is employed, hosts may accept a configuration for only a single default gateway.

Unfortunately, this approach creates a single point of failure. Loss of the router supplying the default gateway, or the router's WAN connection, results in isolating the hosts that rely upon the default gateway.

There are a number of ways to provide redundant connections for the hosts. Some hosts can configure alternate gateways while others are intelligent enough to participate in dynamic routing protocols such as the Routing Information Protocol (RIP) or Open Shortest Path First (OSPF) routing protocol. Even when available, these approaches are not always practical due to administrative and operation overhead.

VRRP solves the problem by allowing the establishment of a *virtual router group*, composed of a number of routers that provide one gateway IP. VRRP uses an election protocol to dynamically assign responsibility for the gateway to one of the routers in the group. This router is called the Master.

If the Master (or, optionally, a condition) fails, the alternate (or backup) routers in the group elect a new Master. The new master owns the virtual IP address and issues a gratuitous ARP to inform the network of where the gateway can be reached.

Since the host's default route and MAC address does not change, packet loss at the hosts is limited to the amount of time required to elect a new router.

Section 14.1.1.2

VRRP Terminology

Each physical router running VRRP is known as a VRRP Router. Two or more VRRP Routers can be configured to form a *Virtual Router*. Each VRRP Router may participate in one or more Virtual Routers.

Each Virtual Router has a user-configured Virtual Router Identifier (VRID) and a Virtual IP address or set of IP addresses on the shared LAN. Hosts on the shared LAN are configured to use these addresses as the default gateway.

Each router in the Virtual Router Group has a specific priority, which is a number between 1 and 255. The router with the highest priority (or highest number) is elected the Master, while all other routers are considered Backups.

On RUGGEDCOM RX1500/RX1501/RX1510/RX1511/RX1512 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.

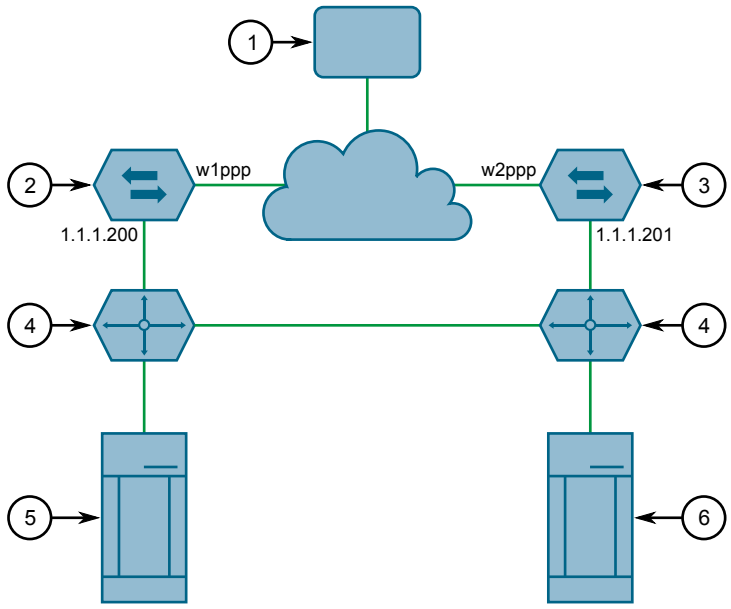


Figure 981: VRRP Example

1. Network **2.** Remote Router 1 **3.** Remote Router 2 **4.** Switch **5.** Host 1 **6.** Host 2

In this example, the remote routers are configured as follows:

Remote Router 1	Remote Router 2
• VRID 10 Gateway IP: 1.1.1.253 • VRID 10 Priority: 100 • VRID 10 Monitor Interface: w1ppp • VRID 11 Gateway IP: 1.1.1.252 • VRID 11 Priority: 50	• VRID 10 Gateway IP: 1.1.1.253 • VRID 10 Priority: 50 • VRID 11 Gateway IP: 1.1.1.252 • VRID 11 Priority: 100 • VRID 11 Monitor Interface: w2ppp

Traffic from host 1 is sent through router 1, and traffic from host 2 is sent through router 2. A failure of either router or their WAN link will be recovered by the other router.

Note that both routers can always be reached by the hosts at their *real* IP addresses.

Two or more VRRP instances can be assigned to be in the same VRRP Group, in which case, they can failover together.

An Example of VRRP Groups

In the next example, both host 1 and host 2 use a gateway of 192.168.3.10. The external side can access the internal side by gateway 192.168.2.10. VRID_20 and VRID_21 are grouped together. Normally, router 1 will provide both an internal and external access gateway, as its priority is higher than those on Router 2. When either the internal or external side of Router 1 becomes inoperative, Router 1 will remove give control of both 192.168.2.10 and 192.168.3.10 gateways to Router 2.

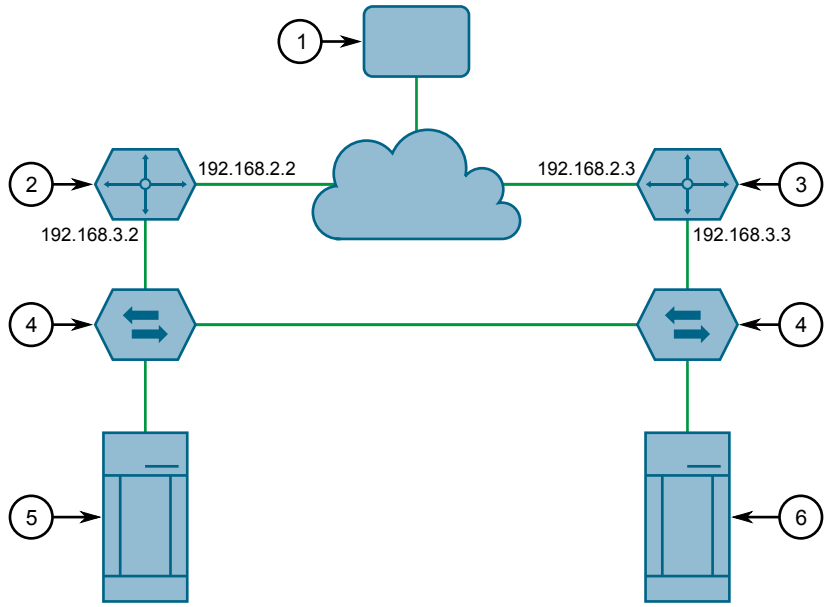


Figure 982: VRRP Group Example

1. Network **2.** Remote Router 1 **3.** Remote Router 2 **4.** Switch **5.** Host 1 **6.** Host 2

In this example, the remote routers are configured as follows:

Remote Router 1	Remote Router 2
• VRID_20 Gateway IP: 192.168.2.10 • VRID_20 Priority: 100 • VRID_21 Gateway IP: 192.168.3.10 • VRID_21 Priority: 100	• VRID_20 Gateway IP: 192.168.2.10 • VRID_20 Priority: 50 • VRID_21 Gateway IP: 192.168.3.10 • VRID_21 Priority: 50

Other VRRP parameters are the Advertisement Interval and Gratuitous ARP Delay. The advertisement interval is the time between which advertisements are sent. A backup router will assume the role of Master three advertisement intervals after the Master fails. If a monitored interface goes down, a Master router will immediately signal an election and allow a Backup router to assume the Master roles.

The router issues a set of gratuitous ARPs when moving between Master and Backup roles. These unsolicited ARPs teach the hosts and switches in the network of the current MAC address and port associated with the gateway. The router will issue a second set of ARPs after the time specified by the Gratuitous ARP delay.

Section 14.1.1.3
Connection Synchronization

When failover occurs, hosts must typically either reconnect manually to the backup firewall, or wait for the connection to automatically reconnect. This can sometimes take several minutes.

When connection synchronization is enabled, stateful connections are maintained when a VRRP master router fails, resulting in a seamless failover to the VRRP backup router. This is done by synchronizing the firewall and NAT states between the master and backup routers.

In the following example, when the master router (R1) fails, the firewall connection and NAT states are initialized automatically for the backup router (R2). The backup router then becomes the new VRRP master.

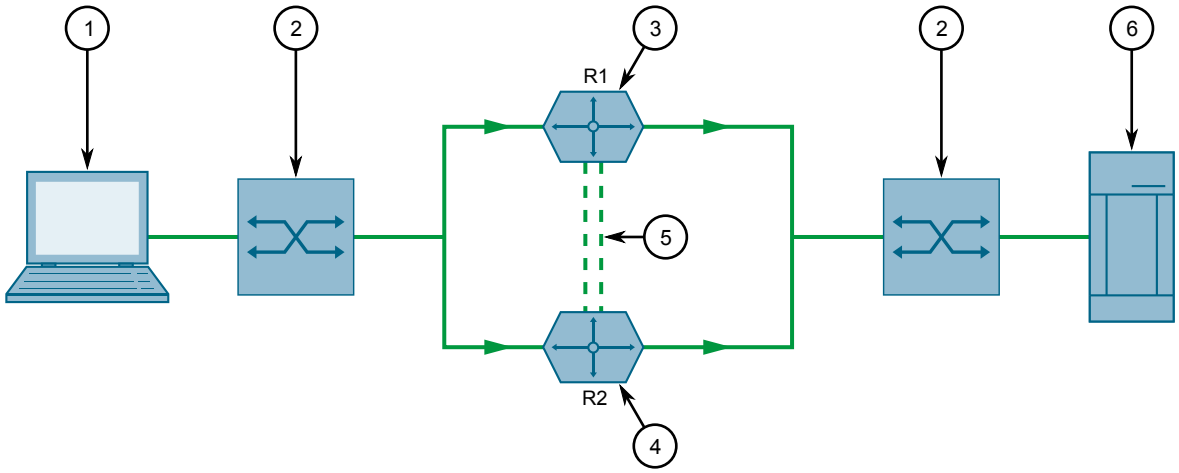


Figure 983: Connection Synchronization Example

1. Host A **2.** Switch **3.** Primary VRRP Firewall and Router (R1) **4.** Backup VRRP Firewall and Router (R2) **5.** Dedicated Links **6.** Host B

Section 14.1.2
Viewing the Status of VRRP

To view the status of VRRP, navigate to ***services » vrrp » status***. The **VRRP Status** form appears.

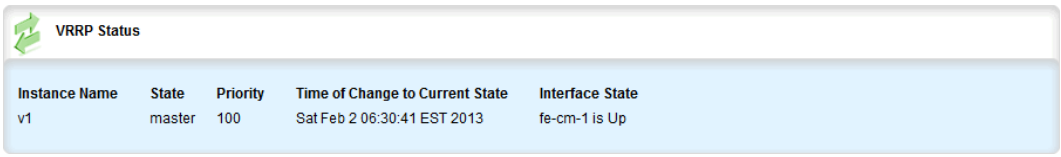


Figure 984: VRRP Status Form

This table provides the following information:

Parameter	Description
Instance Name	**Synopsis:** A string The VRRP instance name.

Parameter	Description
State	**Synopsis:** A string The VRRP instance state. This parameter is mandatory.
Priority	**Synopsis:** A string The VRRP instance priority. This parameter is mandatory.
Time of Change to Current State	**Synopsis:** A string The time of change to the current state. This parameter is mandatory.
Interface State	**Synopsis:** A string The VRRP interface state. This parameter is mandatory.

Section 14.1.3
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.

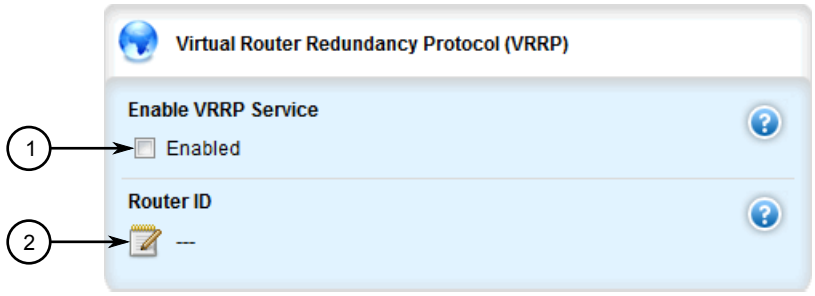


Figure 985: Virtual Router Redundancy Protocol (VRRP) Form

1. Enable VRRP Service Check Box **2.** Router ID Box

3. Configure the following parameter(s) as required:

Parameter	Description
Enable VRRP Service	Enables or disables the VRRP service.
Router ID	**Synopsis:** 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 14.1.4
Managing VRRP Trackers

VRRP trackers monitor the state/condition of a route. When the route is unavailable, VRRP will lower its priority or transition it to a fault state.

NOTE
The decision to increase or decrease the priority of a route must be done in coordination with any backup VRRP Routers since the priority decides whether a router becomes a Master or a Backup. For example, if Router X's priority is 150 and Router Y's priority is 145, Router X's priority must be lowered by 6 to make it a Backup router.

CONTENTS

Section 14.1.4.1
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.

Figure 986: Tracker Table

If no VRRP trackers have been configured, add trackers as needed. For more information, refer to Section 14.1.4.2, "Adding a VRRP Tracker".

Section 14.1.4.2
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 987: Key Settings Form

1. Tracker Name Box **2.** Add Button

3. Configure the following parameter(s) as required:

Parameter	Description
Tracker Name	**Synopsis:** A string 1 to 64 characters long The name of the tracker.

4. Click **Add** to add the tracker. The **Tracker** form appears.

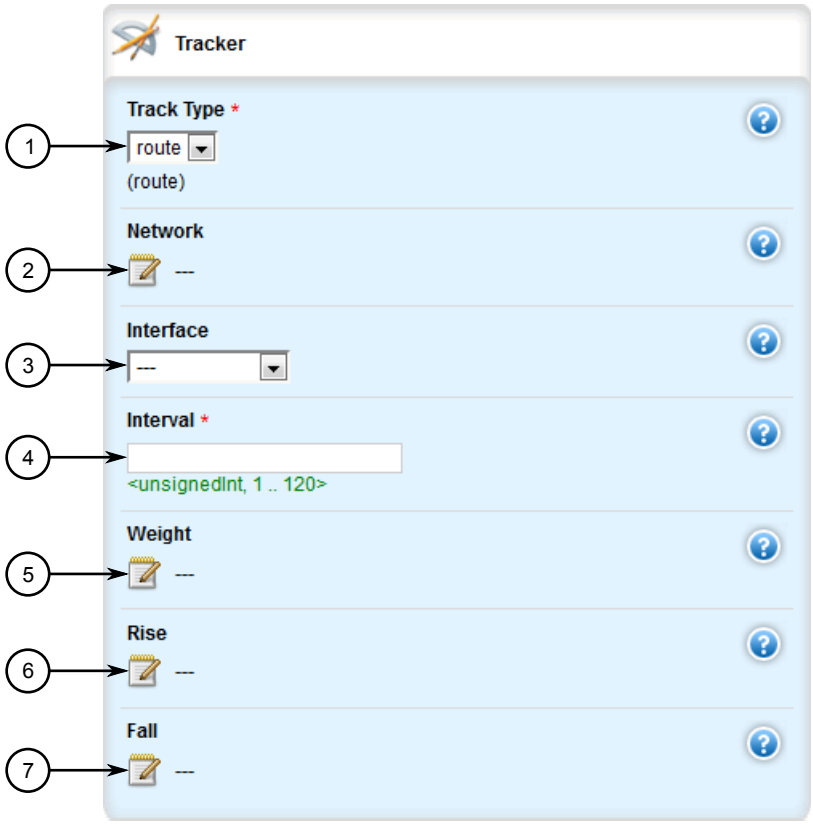


Figure 988: Tracker Form

1. Tracker Type List **2.** Network Box **3.** Interface List **4.** Interval List **5.** Weight Box **6.** Rise Box **7.** Fall Box

5. Configure the following parameter(s) as required:

Parameter	Description
Track Type	**Synopsis:** { route } **Default:** route The type of condition for the tracker to check.
Network	**Synopsis:** A string 9 to 18 characters long The network to track. The tracker checks for a route to this network in the routing table.
Interface	**Synopsis:** A string The interface to the tracked network. The tracker rises only when the route to the monitored network is through this interface.
Interval	**Synopsis:** A 32-bit unsigned integer between 1 and 120 The number of seconds between tracker queries. This parameter is mandatory.
Weight	**Synopsis:** A 32-bit signed integer between -254 and 254 The amount by which to increase or decrease the router's priority. When negative, the priority decreases by this amount when the tracker falls. When positive, the priority increases by this amount when the tracker rises. When not set, the state changes to the fault state when the tracker falls.

Parameter	Description
Rise	**Synopsis:** A 32-bit unsigned integer between 1 and 65535 The number of successful tracker queries before changing the router priority.
Fall	**Synopsis:** A 32-bit unsigned integer between 1 and 65535 The number of unsuccessful tracker queries before changing the router priority.

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 14.1.4.3
Deleting a VRRP Tracker

To delete a VRRP tracker, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to ***services » vrrp » trackers***. The **Tracker** table appears.

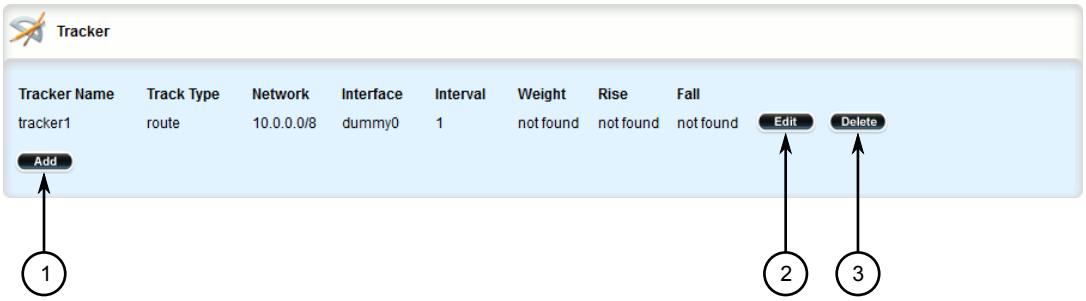


Figure 989: Tracker Table

1. Add Button **2.** Edit Button **3.** Delete Button

3. Click **Delete** next to the chosen tracker.
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 14.1.5
Managing VRRP Groups

Two or more VRRP instances can be assigned to be in the same VRRP Group, in which case, they can failover together.

CONTENTS

Section 14.1.5.1
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.

Figure 990: VRRP Group Table

If no VRRP groups have been configured, add groups as needed. For more information, refer to Section 14.1.5.2, “Adding a VRRP Group”.

Section 14.1.5.2
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.

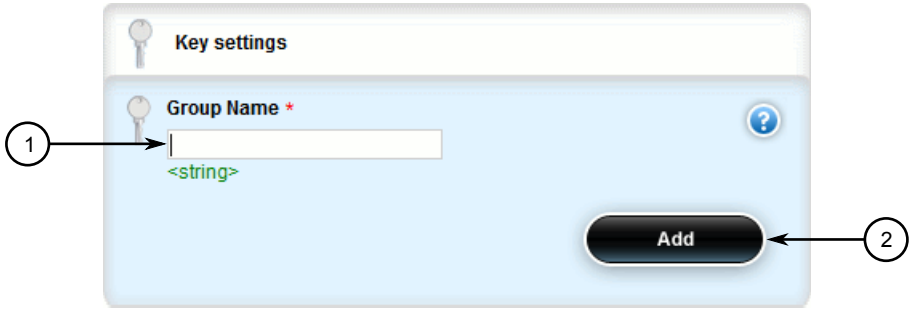


Figure 991: Key Settings Form

1. Group Name Box **2.** Add Button

3. Configure the following parameter(s) as required:

Parameter	Description
Group Name	**Synopsis:** A string 1 to 64 characters long The VRRP group name.

4. Click **Add** to add the group.
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 14.1.5.3
Deleting a VRRP Group

To delete a VRRP group, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to ***services » vrrp » group***. The **VRRP Group** table appears.

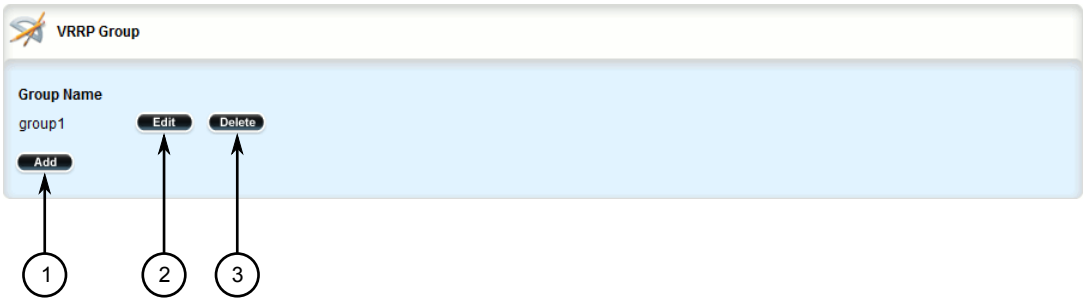


Figure 992: VRRP Group Table

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 14.1.6
Managing VRRP Instances

VRRP instances define the interfaces monitored by VRRP. Two or more instances can be added to the same VRRP group, which allows them to failover together.

CONTENTS

Section 14.1.6.1
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.

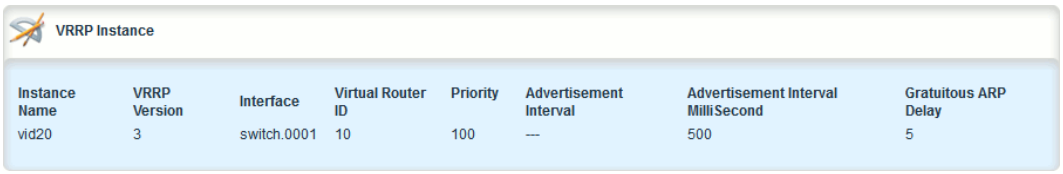


Figure 993: VRRP Instance Table

If no VRRP instances have been configured, add instances as needed. For more information, refer to Section 14.1.6.2, "Adding a VRRP Instance".

Section 14.1.6.2
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 14.1.5.2, "Adding a VRRP Group".
3. Navigate to ***services » vrrp » instance*** and click **<Add instance>**. The **Key Settings** form appears.

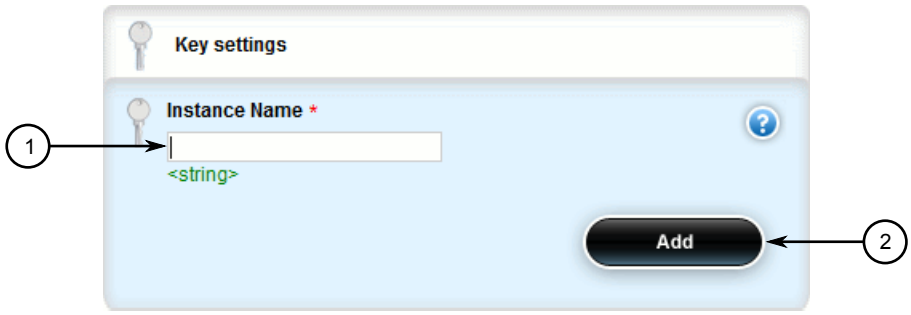


Figure 994: Key Settings Form

1. Instance Name Box **2.** Add Button

4. Configure the following parameter(s) as required:

Parameter	Description
Instance Name	**Synopsis:** 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.

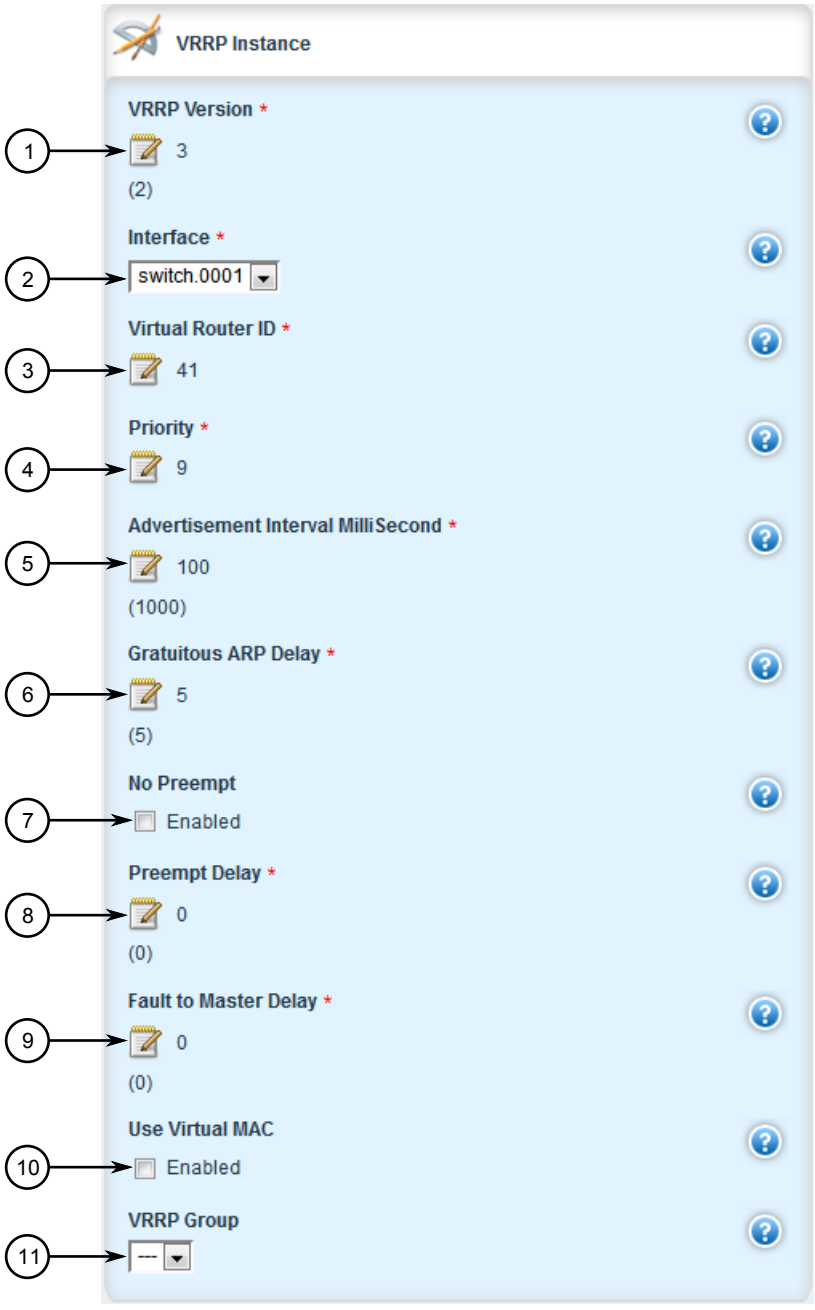


Figure 995: VRRP Instance Form

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	**Synopsis:** An 8-bit unsigned integer between 2 and 3 **Default:** 2 Configure VRRP version for this instance.
Interface	**Synopsis:** A string The interface that will host the VRIP when the router becomes the VRRP Master. This parameter is mandatory.
Virtual Router ID	**Synopsis:** An 8-bit unsigned integer between 1 and 255 The Virtual Router ID. All routers supplying the same VRIP should have the same VRID. This parameter is mandatory.
Priority	**Synopsis:** An 8-bit unsigned integer between 0 and 255 The priority for the VRRP instance. When electing the master, the highest priority wins. The configurable range is 1 to 255. A value of zero (0) is invalid. This parameter is mandatory.
Advertisement Interval	**Synopsis:** An 8-bit unsigned integer between 1 and 255 **Default:** 1 VRRP2 advertisement interval, in seconds.
Advertisement Interval MilliSecond	**Synopsis:** A 32-bit unsigned integer between 20 and 3000 **Default:** 1000 VRRP3 advertisement interval in millisecond, must be multiple of 10.
Gratuitous ARP Delay	**Synopsis:** An 8-bit unsigned integer between 1 and 255 **Default:** 5 Gratuitous ARP delay, in seconds. Sets the delay after the router changes state state before a second set of gratuitous ARPs are sent.
No Preempt	When enabled, a lower priority router maintains its role as master even if this router has a higher priority.
Preempt Delay	**Synopsis:** A 32-bit unsigned integer between 0 and 1000 **Default:** 0 The time, in seconds, after startup until preemption.
Fault to Master Delay	**Synopsis:** A 32-bit unsigned integer between 0 and 1000 **Default:** 0 The delay, in seconds, before a transition from the fault state to the master state occurs, thereby preempting the current master.
Use Virtual MAC	When enabled, the router uses a virtual MAC address for the VRIP interface.
VRRP Group	**Synopsis:** A string Binds this VRRP instance to a VRRP group.

7. Add one or more VRRP monitors. For more information, refer to Section 14.1.7.2, “Adding a VRRP Monitor”.

8. Add one or more track scripts. For more information, refer to Section 14.1.8.2, “Adding a Track Script”.
9. Add one or more virtual IP addresses. For more information, refer to Section 14.1.9.2, “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 14.1.6.3
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 996: 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 14.1.7
Managing VRRP Monitors

A VRRP monitor selects an extra interface to monitor. If the interface becomes unavailable, the router will relinquish control of the gateway IP address to another VRRP Router.

CONTENTS

Section 14.1.7.1
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.

Figure 997: Monitor Interface Table

If no VRRP monitors have been configured, add monitors as needed. For more information, refer to Section 14.1.7.2, "Adding a VRRP Monitor".

Section 14.1.7.2
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.

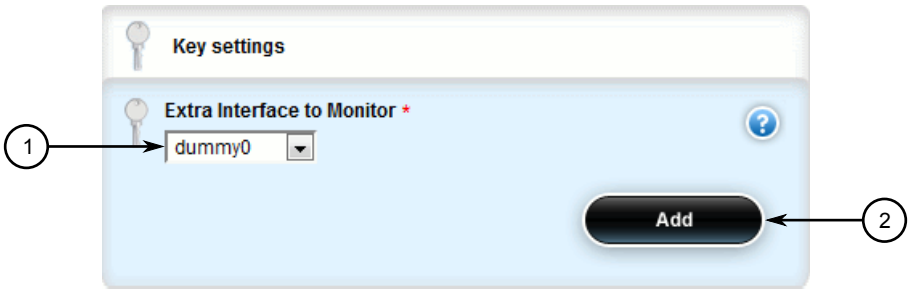


Figure 998: Key Settings Form

1. Extra Interface to Monitor Box **2.** Add Button

4. Configure the following parameter(s) as required:

Parameter	Description
Extra Interface to Monitor	**Synopsis:** A string The name of the interface.

5. Click **Add** to add the monitor. The **Monitor Interface** form appears.

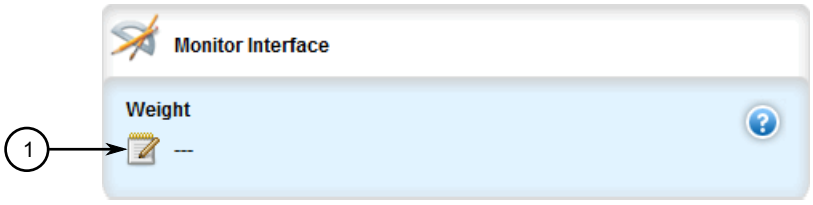


Figure 999: Monitor Interface Form

1. Weight Box

6. Configure the following parameter(s) as required:

Parameter	Description
Weight	**Synopsis:** A 32-bit signed integer between -254 and 254 The amount by which to increase or decrease the router's priority. When negative, the priority decreases by this amount when the interface 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.

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 14.1.7.3
Deleting a VRRP Monitor

To delete 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. The **Monitor Interface** table appears.

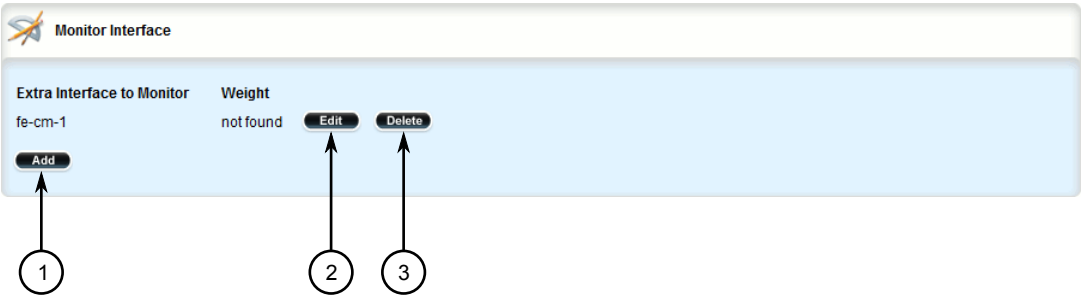


Figure 1000: Monitor Interface Table

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 14.1.8
Managing Track Scripts

Track scripts are used to associate VRRP trackers with VRRP instances.

CONTENTS

Section 14.1.8.1
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.

Figure 1001: Track Script Table

If no VRRP monitors have been configured, add monitors as needed. For more information, refer to Section 14.1.7.2, "Adding a VRRP Monitor".

Section 14.1.8.2
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.

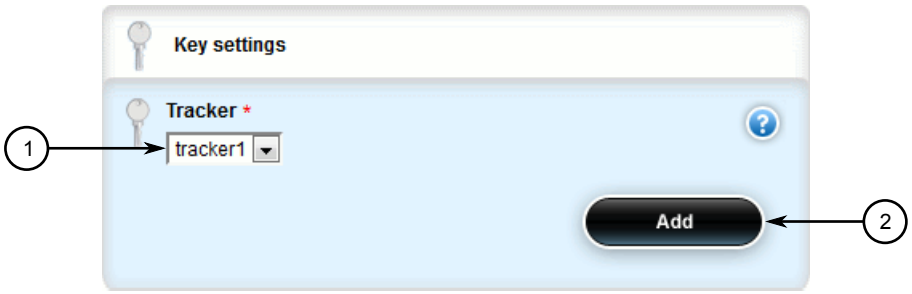


Figure 1002: Key Settings Form

1. Tracker Box **2.** Add Button

4. Configure the following parameter(s) as required:

Parameter	Description
Tracker	**Synopsis:** A string Select a tracker to monitor VRRP instance.

5. Click **Add** to add the track script. The **Track Script** form appears.

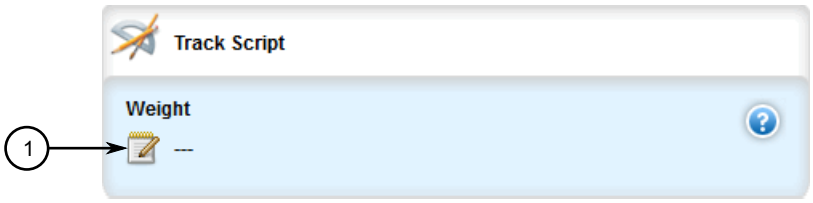


Figure 1003: Track Script Form

1. Weight Box

6. Configure the following parameter(s) as required:

Parameter	Description
Weight	**Synopsis:** A 32-bit signed integer between -254 and 254 This setting overwrites the weight setting in the tracker. If negative, the priority decreases by this amount when the tracker falls. If positive, the priority increases by this amount when the tracker rises. If not set, the weight value in the tracker will be used.

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 14.1.8.3

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.

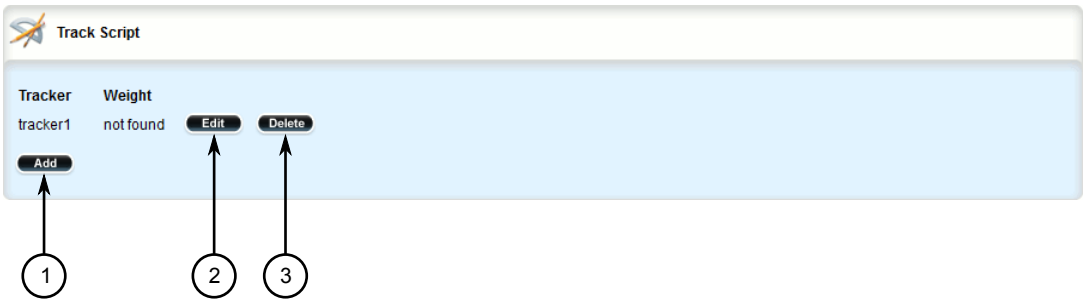


Figure 1004: Track Script Table

1. Add Button **2.** Edit Button **3.** Delete Button

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 14.1.9
Managing Virtual IP Addresses

Virtual IP addresses represent the default gateways used by the hosts on the shared LAN.

CONTENTS

Section 14.1.9.1
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.

Figure 1005: VRIP IP Address Table

If no virtual IP addresses have been configured, add addresses as needed. For more information, refer to Section 14.1.9.2, "Adding a Virtual IP Address".

Section 14.1.9.2
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.

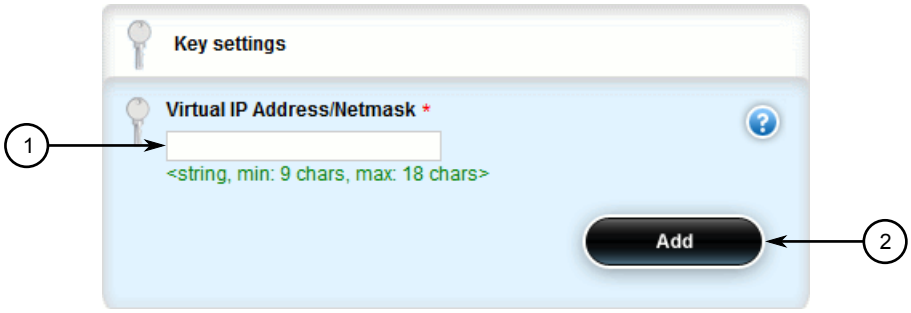


Figure 1006: Key Settings Form

1. Virtual IP Address/Netmask Box **2.** Add Button

4. Configure the following parameter(s) as required:

Parameter	Description
Virtual IP Address/Netmask	**Synopsis:** 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 14.1.9.3
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.

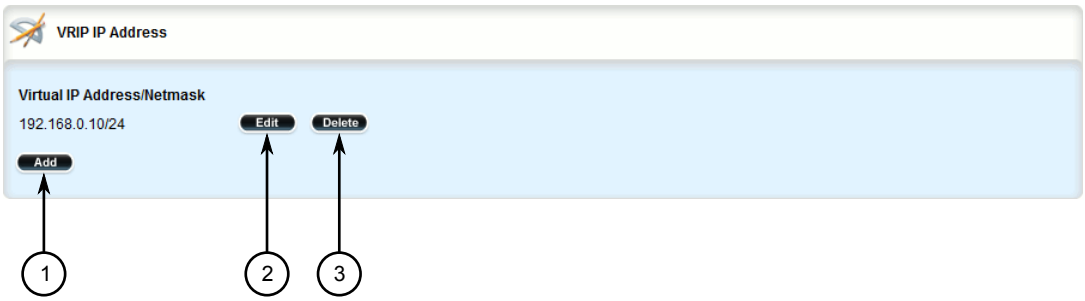


Figure 1007: VRIP IP Address Table

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 14.1.10
Managing Connection Synchronization

This section describes how to configure connection synchronization between two VRRP-enabled routers.

CONTENTS

Section 14.1.10.1
Configuring Connection Synchronization

To configure connection synchronization, do the following for *each* VRRP-enabled device:

IMPORTANT!
Well-formed stateful firewall rules are required. For more information, refer to Section 6.8.1.1, "Stateless vs. Stateful Firewalls".

1. Configure a firewall with stateful firewall rules to control inbound and outbound traffic. For more information, refer to Section 6.8.3, "Adding a Firewall".
2. Make sure the VRRP service is enabled. For more information, refer to Section 14.1.3, "Enabling/Disabling VRRP".
3. Configure VRRP instances and groups. For more information, refer to Section 14.1.6.2, "Adding a VRRP Instance" and Section 14.1.5.2, "Adding a VRRP Group".
4. Define one or more dedicated links for each VRRP group. For more information, refer to Section 14.1.10.4, "Adding a Dedicated Link".
5. Select a link to be the default dedicated link for any VRRP group not assigned a dedicated link. For more information, refer to Section 14.1.10.6, "Selecting a Default Dedicated Link".
6. Enable the configuration synchronization service. For more information, refer to Section 14.1.10.2, "Enabling/Disabling Connection Synchronization".

Once the configuration is complete, verify the status of the service on both devices. For more information, refer to Section 14.1.10.7, "Viewing the Status of Each Dedicated Link".

Section 14.1.10.2
Enabling/Disabling Connection Synchronization

To enable or disable connection synchronization, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to ***services » conn-sync***. The **Connection Sync** form appears.

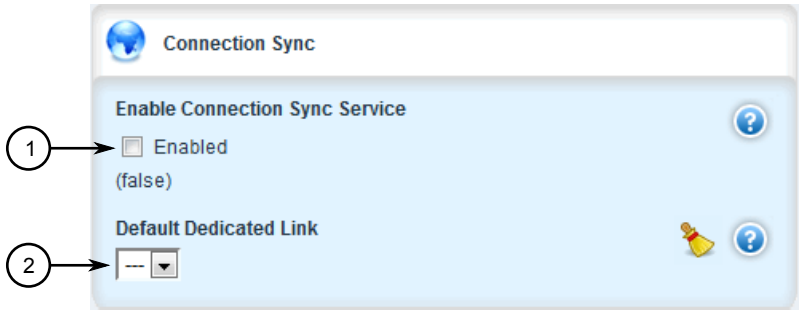


Figure 1008: Connection Sync Form

1. Enabled Check Box **2.** Default Dedicated Link Options

3. Click **Enabled** to enable connection synchronization, or clear **Enabled** 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 14.1.10.3
Viewing a List of Dedicated LInks

To view a list of dedicated links, Navigate to ***services » conn-sync » dedicated-link***. If dedicated links have been configured, the **Dedicated Links** table appears.

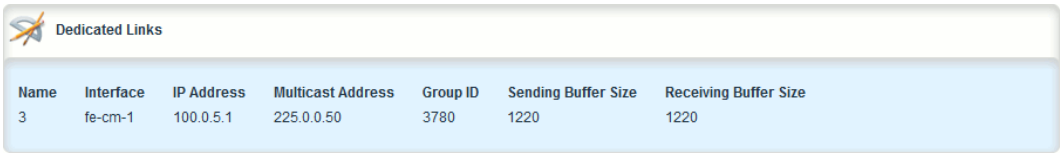


Figure 1009: Dedicated Links Table

If no dedicated links have been configured, add dedicated links as needed. For more information, refer to Section 14.1.10.4, "Adding a Dedicated Link".

Section 14.1.10.4
Adding a Dedicated Link

To add a dedicated link, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.

   NOTE
   RUGGEDCOM ROX II supports up to four dedicated links.

2. Navigate to ***services » conn-sync » dedicated-link*** and click **<Add dedicated-link>**. The **Key Settings** form appears.

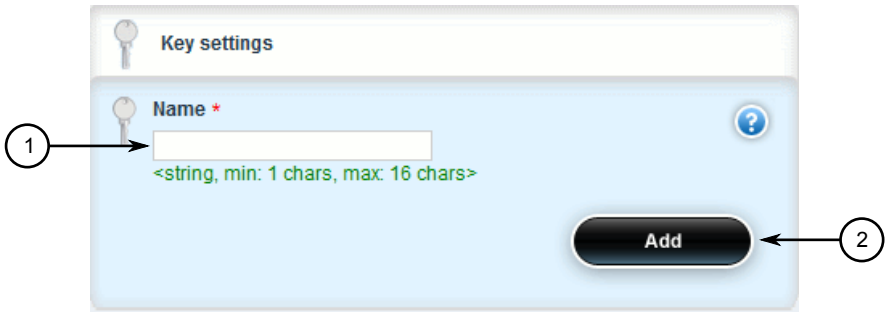


Figure 1010: Key Settings Form

1. Name Box **2.** Add Button

3. Configure the following parameter(s) as required:

Parameter	Description
Name	**Synopsis:** A string 1 to 16 characters long Dedicated link name.

4. Click **Add**. The **Dedicated Link** form appears.

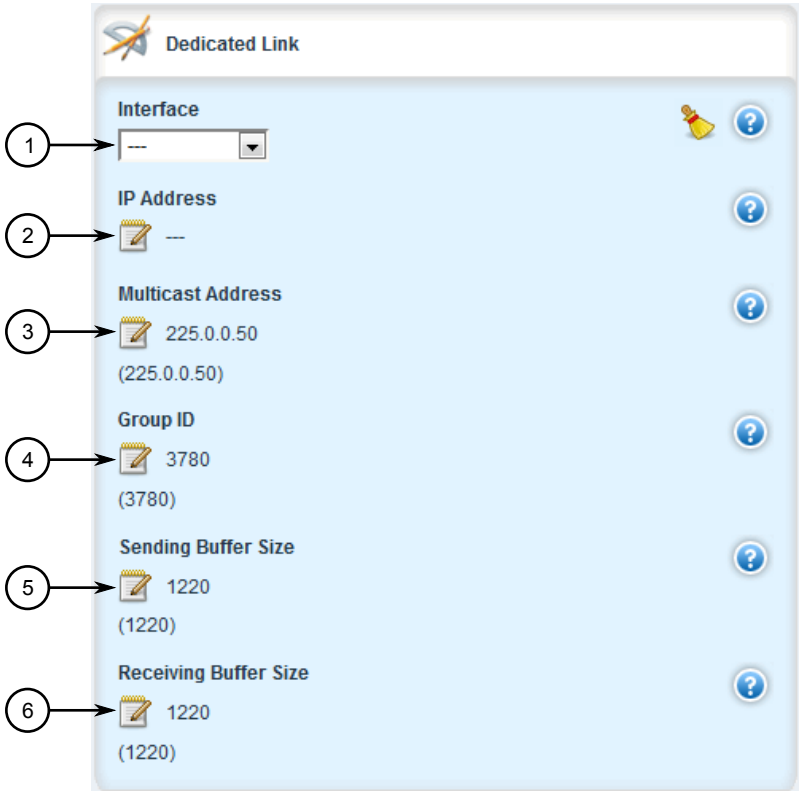


Figure 1011: Dedicated Link Form

1. Interface Options **2.** IP Address Box **3.** Multicast Address Box **4.** Group ID Box **5.** Sending Buffer Size Box **6.** Receiving Buffer Size Box

5. Configure the following parameter(s) as required:

Parameter	Description
interface	**Synopsis:** A string The interface name of the dedicated link.
IP Address	**Synopsis:** A string 7 to 15 characters long or a string 6 to 40 characters long The IPv4 or IPv6 address of the dedicated link interface.
Multicast Address	**Synopsis:** A string 7 to 15 characters long or a string 7 to 39 characters long **Default:** 225.0.0.50 The destination IPv4 or IPv6 multicast address of the dedicated link.
Group ID	**Synopsis:** A 16-bit unsigned integer between 1 and 65535 **Default:** 3780

Parameter	Description
	The multicast group ID of the cluster.
Sending Buffer Size	**Synopsis:** A 32-bit unsigned integer between 64 and 2560 **Default:** 1220 The sending socket buffer size in kB.
Receiving Buffer Size	**Synopsis:** A 32-bit unsigned integer between 64 and 2560 **Default:** 1220 The receiving socket buffer size in kB.

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 14.1.10.5
Deleting a Dedicated Link

To delete a dedicated link, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to ***services » conn-sync » dedicated-link***. The **Dedicated Links** table appears.

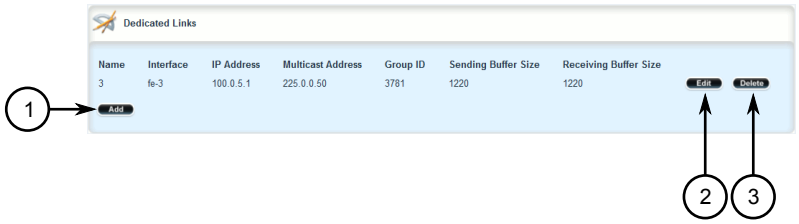


Figure 1012: Dedicated Links Table

1. Add Button **2.** Edit Button **3.** Delete Button

3. Click **Delete** next to the chosen dedicated link.
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 14.1.10.6
Selecting a Default Dedicated Link

To select a default a dedicated link, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to ***services » conn-sync***. The **Connection Sync** form appears.

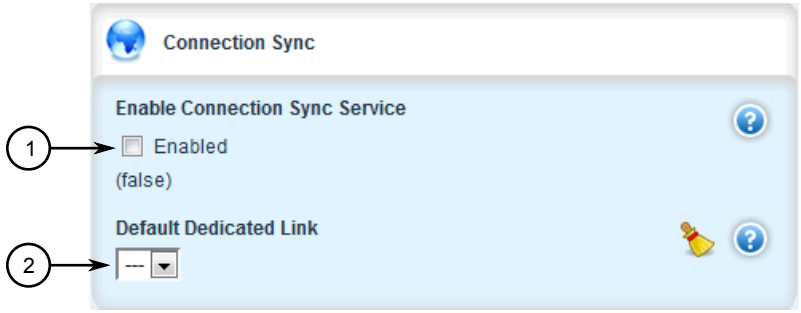


Figure 1013: Connection Sync Form

1. Enabled Check Box **2.** Default Dedicated Link Options

3. Configure the following parameter(s) as required:

Parameter	Description
Default Dedicated Link	**Synopsis:** A string The default dedicated link.

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 14.1.10.7

Viewing the Status of Each Dedicated Link

To view the status of all dedicated links, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to ***services » conn-sync » status***. The **Dedicated Link Status** table appears.

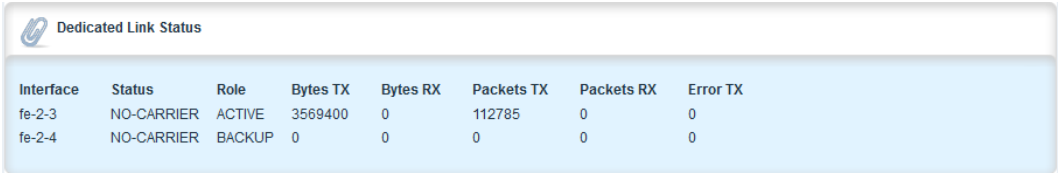


Figure 1014: Dedicated Links Status Table

This table provides the following information:

Parameter	Description
Interface	**Synopsis:** A string The conn-sync dedicated link interface name.
Status	**Synopsis:** A string

Parameter	Description
	The conn-sync dedicated link status.
Role	**Synopsis:** A string The conn-sync dedicated link role.
Bytes TX	**Synopsis:** A 64-bit unsigned integer The number of bytes sent on conn-sync dedicated link.
Bytes RX	**Synopsis:** A 64-bit unsigned integer The number of bytes received on conn-sync dedicated link.
Packets TX	**Synopsis:** A 64-bit unsigned integer The number of packets sent on conn-sync dedicated link.
Packets RX	**Synopsis:** A 64-bit unsigned integer The number of packets received on conn-sync dedicated link.
Error TX	**Synopsis:** A 64-bit unsigned integer The number of errors sent on conn-sync dedicated link.
Error RX	**Synopsis:** A 64-bit unsigned integer The number of errors received on conn-sync dedicated link.

Section 14.2

Managing Link Failover Protection

Link failover provides an easily configurable means of raising a backup link upon the failure of a designated main link. The main and backup links can be Ethernet, Cellular Modem, T1/E1, or DDS.

Link failover can back up to multiple remote locations, managing multiple main-to-backup link relationships. When the backup link is a modem, many profiles of dialed numbers can exist, each serving as a distinct backup link.

Link failover can back up a permanent, high-speed WAN link to a permanent, low-speed WAN link. Use this function when OSPF cannot be employed, such as on public links.

Link failover can also be used to migrate the default route from the main link to the backup link.

The time after a main link failure to backup link startup, and the time after a main link recovery to backup link stoppage, are configurable. The link failover function also provides failover status information and a test of the failover settings.

CONTENTS

Section 14.2.1
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.

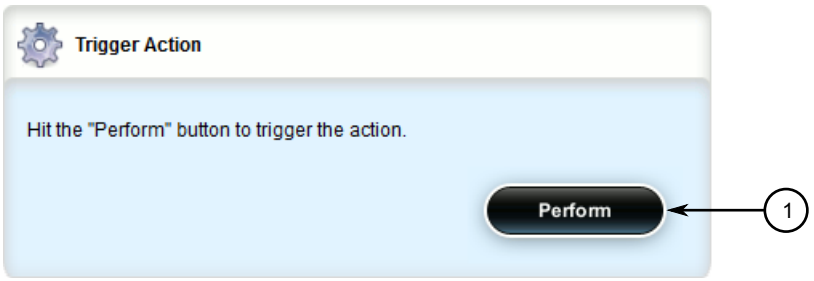


Figure 1015: Trigger Action Form

1. Perform Button

3. Click **Perform**. The **Link Failover Logs** form appears.

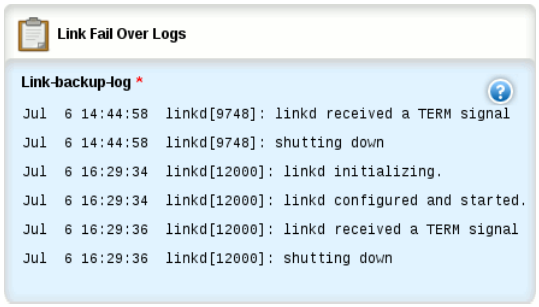


Figure 1016: Link Fail Over Logs Form

Section 14.2.2
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.

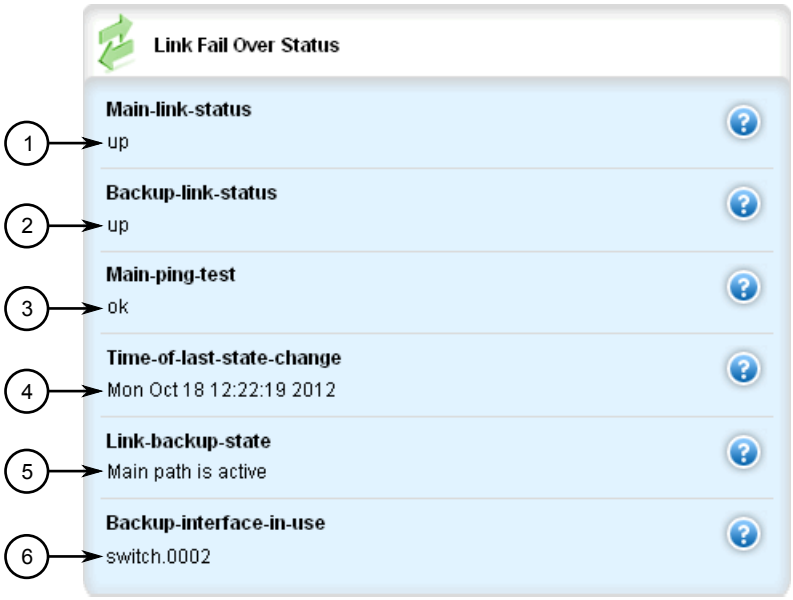


Figure 1017: Link Fail Over Status Form

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	**Synopsis:** A string The main link status.
Backup Link Status	**Synopsis:** A string The backup link status.
Main Ping Test	**Synopsis:** A string The results of pinging the target using the main interface.
Time Of Last State Change	**Synopsis:** A string The time of the last state change.
Link Backup State	**Synopsis:** A string The backup link state.
Backup Interface In Use	**Synopsis:** A string The name of the backup interface that is being used.

Section 14.2.3
Managing Link Failover Parameters

This section describes how to manage parameter settings for link failover.

CONTENTS

Section 14.2.3.1
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.

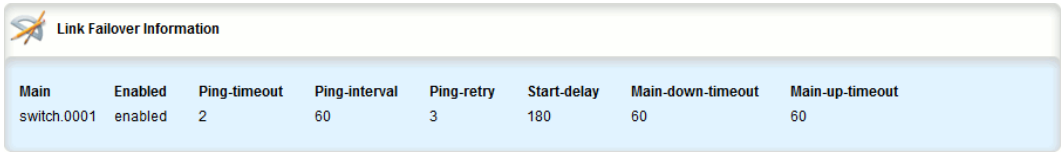


Figure 1018: Link Failover Information Table

If no parameters have been configured, add parameters as needed. For more information, refer to Section 14.2.3.2, "Adding a Link Failover Parameter".

Section 14.2.3.2
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 1019: 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.

Figure 1020: 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	Enables this link backup.
Ping Timeout	**Synopsis:** A 32-bit signed integer between 1 and 65536 **Default:** 2 The time interval, in seconds, before immediately retrying a ping.
Ping Interval	**Synopsis:** A 32-bit signed integer between 0 and 65536 **Default:** 60 The time interval, in seconds, between ping tests.
Ping Retry	**Synopsis:** A 32-bit signed integer between 0 and 65536 **Default:** 3 The number of ping retries before constructing a path failure.
Start Delay	**Synopsis:** A 32-bit signed integer between 0 and 65536

Parameter	Description
	Default: 180 The delay time, in seconds, when first starting link failover.
Main Down Timeout	**Synopsis:** A 32-bit signed integer between 0 and 65536 **Default:** 60 The delay time, in seconds, that the main trunk is down before starting the backup trunk.
Main Up Timeout	**Synopsis:** A 32-bit signed integer between 0 and 65536 **Default:** 60 The delay time, in seconds, to confirm that the main trunk is up (returned to service) before stopping the backup trunk.

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 14.2.3.3
Deleting a Link Failover Parameter

To delete a link failover parameter, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to ***services » link-failover***. The **Link Failover Information** table appears.

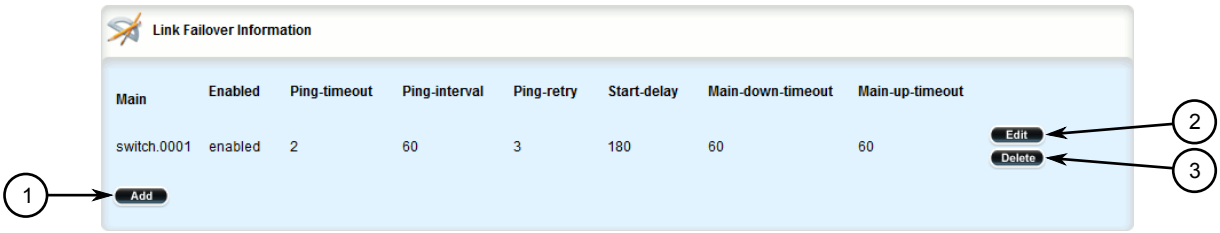


Figure 1021: Link Failover Information Table

1. Add Button **2.** Edit Button **3.** Delete Button

3. Click **Delete** next to the chosen parameter.
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 14.2.4

Managing Link Failover Backup Interfaces

A backup interface is the interface to which link failover switches when the main interface is determined to be down. You can add up to three backup interfaces to each link failover configuration.

CONTENTS

Section 14.2.4.1

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.

Figure 1022: Backup Information Table

If no backup interfaces have been configured, add backup interfaces as needed. For more information, refer to Section 14.2.4.2, "Adding a Link Failover Backup Interface".

Section 14.2.4.2

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 8.1.2, "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.

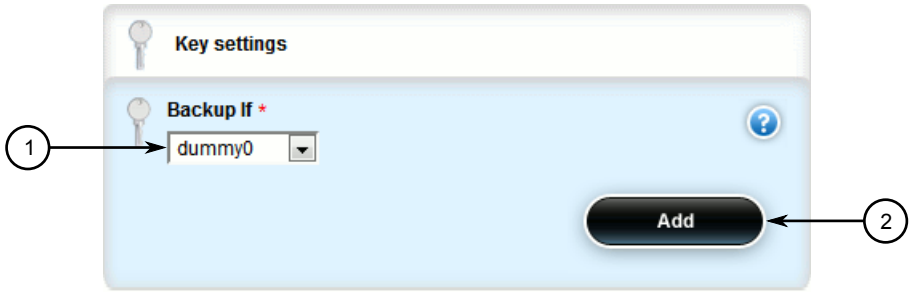


Figure 1023: Key Settings Form

1. Backup Interface List **2.** Add Button

4. Configure the following parameter(s) as required:

Parameter	Description
backupIf	**Synopsis:** A string The interface used to back up the main interface.

5. Click **Add**. The **Backup Settings** form appears.

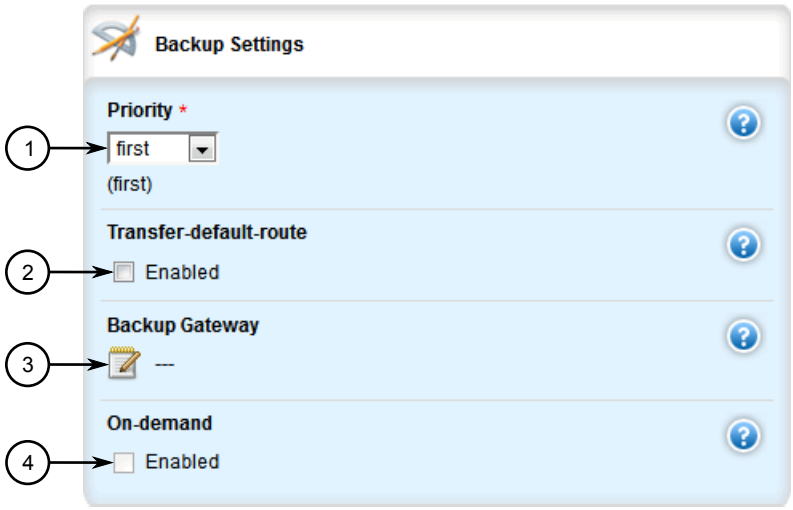


Figure 1024: Backup Settings Form

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	**Synopsis:** { third, second, first } **Default:** first The priority which is applied to the backup interface when switching.
Transfer Default Route	The transfer default gateway on the switching main and backup interface. The default route on the device must have a *distance* greater than one.
Backup Gateway	**Synopsis:** A string 1 to 15 characters long The IP address of the backup gateway.
On Demand	**Synopsis:** { true, false } Displays the status of the interface's On-demand option. When enabled, link failover can set the interface to up or down as needed. The interface is down until needed by link failover. When disabled, link failover cannot set the interface to up or down. By default, the interface is always up.

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 14.2.4.3
Deleting a Link Failover Backup Interface

To delete a link failover backup interface, do the following:

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. The **Backup Information** table appears.

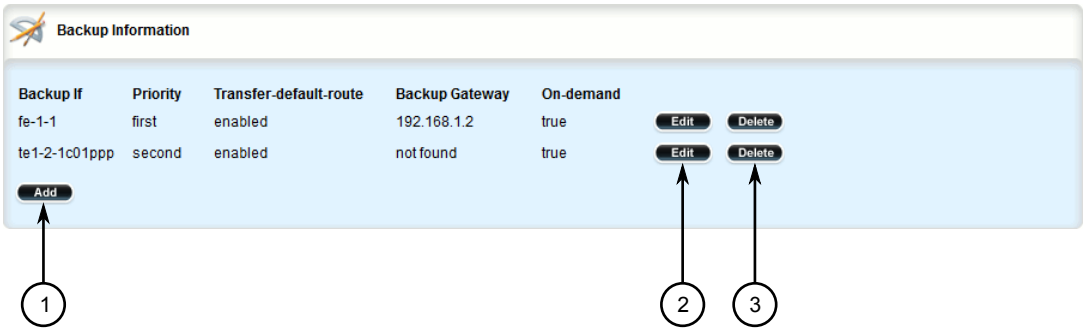


Figure 1025: Backup Information Table

1. Add Button **2.** Edit Button **3.** Delete Button

3. Click **Delete** next to the chosen backup 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 14.2.5
Managing Link Failover Ping Targets

A link failover ping target is an IP address that link failover pings to determine if the main link is down. The address can be a dedicated host or a dummy address on a router. Up to three link failover ping targets can be added to each link failover configuration.

CONTENTS

Section 14.2.5.1
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.

Figure 1026: Targets IP Addresses Table

If no ping targets have been configured, add targets as needed. For more information, refer to Section 14.2.5.2, "Adding a Link Failover Ping Target".

Section 14.2.5.2
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.

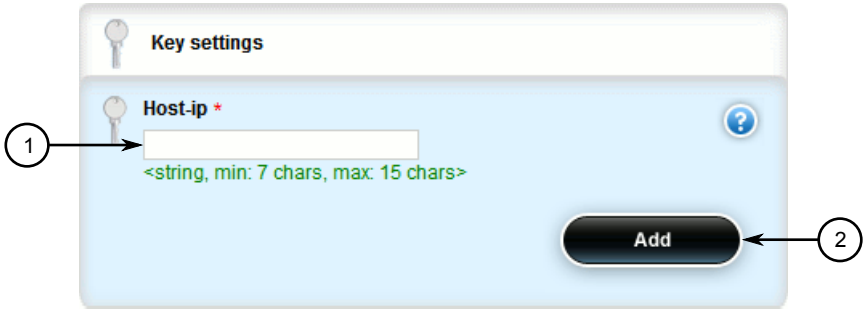


Figure 1027: Key Settings Form

1. Host IP Box **2.** Add Button

4. Configure the following parameter(s) as required:

Parameter	Description
Host IP	**Synopsis:** 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 14.2.5.3
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.

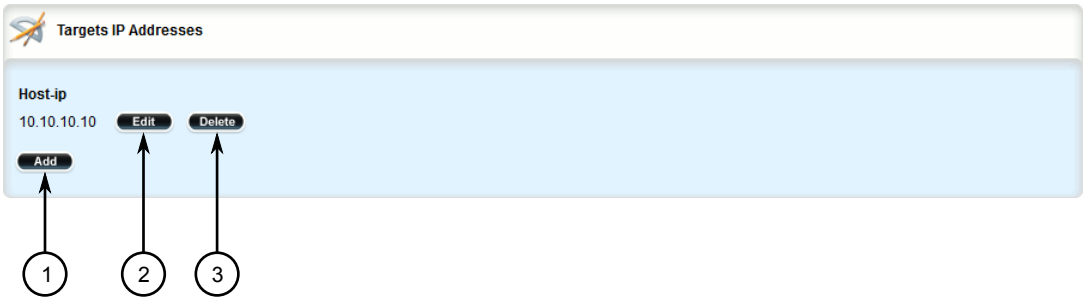


Figure 1028: Targets IP Addresses Table

1. Add Button **2.** Edit Button **3.** Delete Button

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 14.2.6

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 14.2.2, "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 14.2.7, "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.

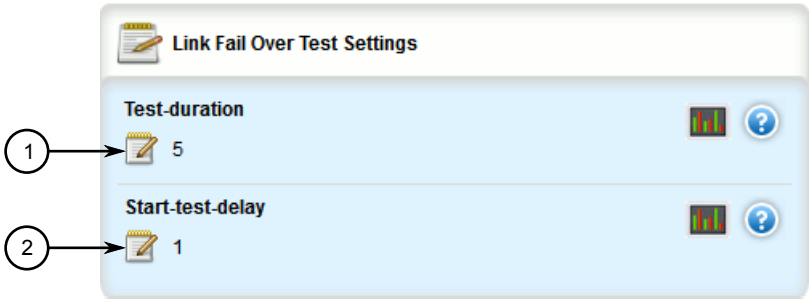


Figure 1029: Link Failover Test Settings Form

1. Test Duration Box **2.** Start Test Delay Box

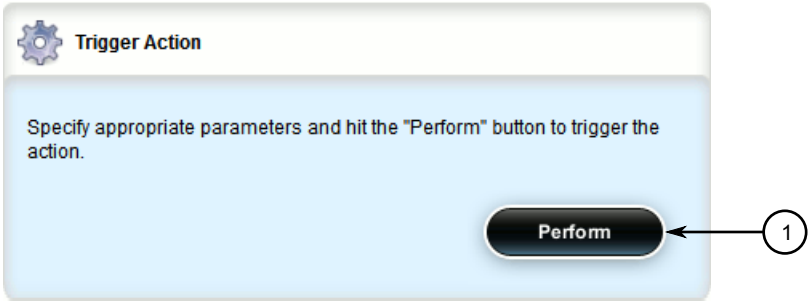


Figure 1030: Trigger Action Form

1. Perform Button

2. Configure the following parameter(s) as required:

Parameter	Description
Test Duration	**Synopsis:** A 32-bit signed integer between 1 and 65536 **Default:** 5 The amount of time (in minutes) to run before restoring service to the main trunk.
Start Test Delay	**Synopsis:** A 32-bit signed integer between 1 and 65536 **Default:** 1 The amount of waiting time (in minutes) before running the test.

3. On the **Trigger Action** form, click **Perform** to begin the test.

Section 14.2.7

Canceling a Link Failover Test

To cancel a link failover test, do the following:

1. 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.

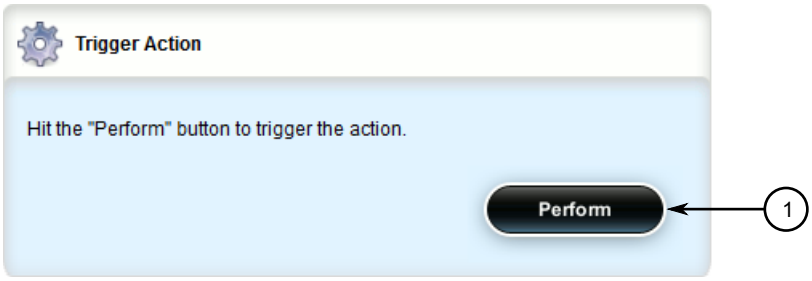


Figure 1031: Trigger Action Form

1. Perform Button

2. Click **Perform** to cancel the test.

Section 14.3

Managing Spanning Tree Protocol

This section describes how to manage the Spanning Tree Protocol (STP).

CONTENTS

Section 14.3.1

RSTP Operation

The IEEE 802.1D Spanning Tree Protocol (STP) was developed to enable the construction of robust networks that incorporate redundancy while pruning the active topology of the network to prevent loops. While STP is effective, it requires that frame transfer halt after a link outage until all bridges in the network are guaranteed to be aware of the new topology. Using the values recommended by IEEE 802.1D, this period lasts 30 seconds.

The Rapid Spanning Tree Protocol (RSTP), first introduced by IEEE 802.1w and significantly improved in IEEE 802.12D-2004, was a further evolution of the IEEE 802.1D Spanning Tree Protocol. It replaced the settling period

with an active handshake between bridges that guarantees the rapid propagation of topology information throughout the network.

CONTENTS

Section 14.3.1.1

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.

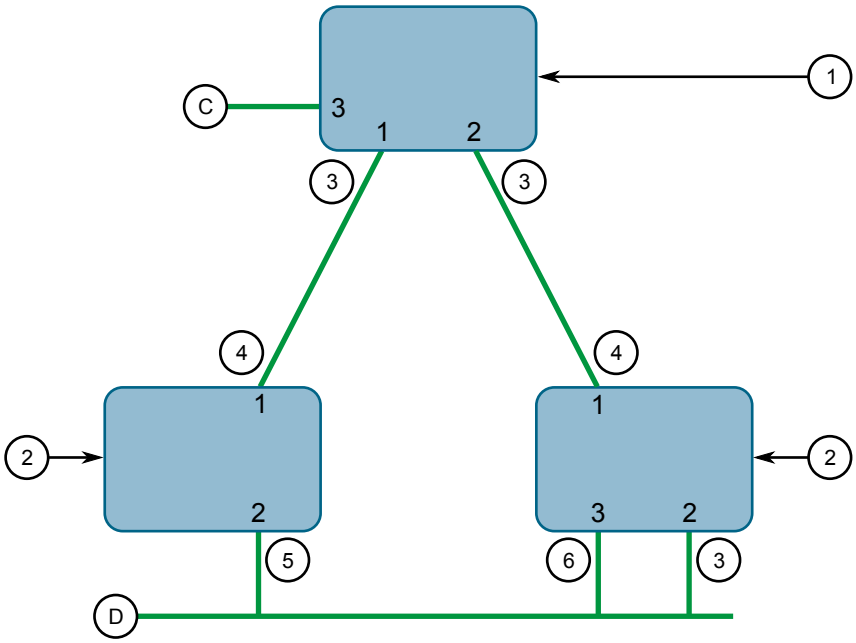


Figure 1032: Bridge and Port Roles

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 14.3.1.2
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 14.3.1.3
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 14.3.1.4
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 14.3.1.5
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 14.3.1.6
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 14.3.1.7
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 14.3.2
RSTP Applications

This section describes various applications of RSTP.

CONTENTS

Section 14.3.2.1

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 1033 would leave all the ports of bridges 555 through 888 connected to the network.

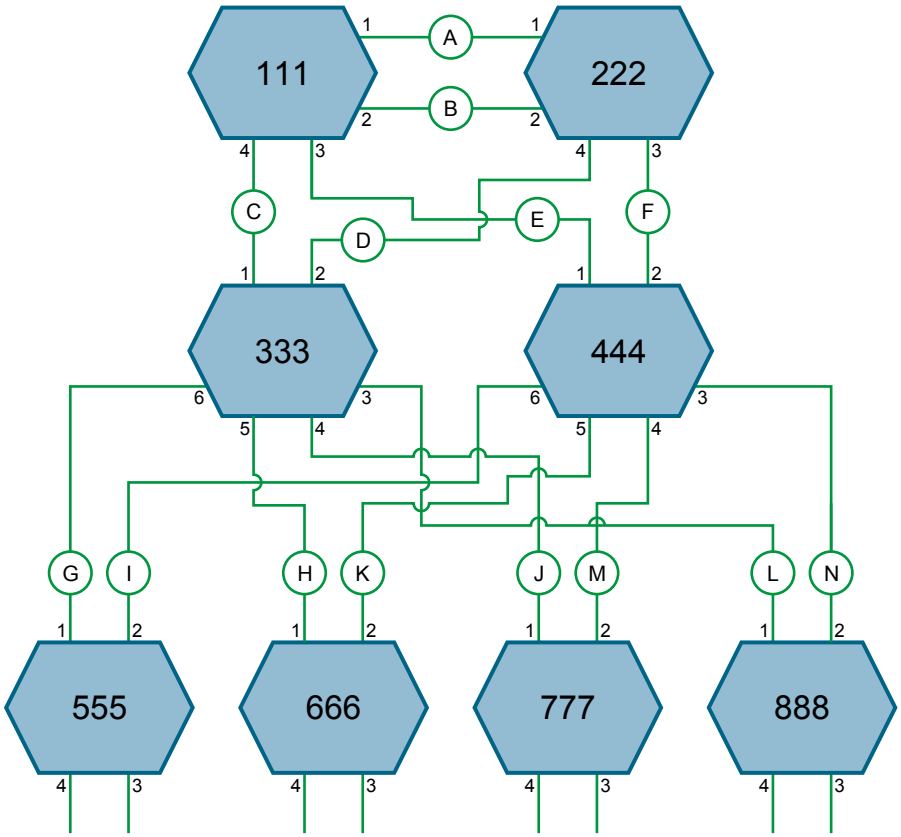


Figure 1033: Example - Structured Wiring Configuration

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 14.3.2.2

RSTP in Ring Backbone Configurations

RSTP may be used in ring backbone configurations where rapid recovery from link failure is required. In normal operation, RSTP will block traffic on one of the links. For an example, refer to link H in Figure 1034. In the event of a failure on link D, bridge 444 will unblock link H and bridge 333 will communicate with the network through link F.

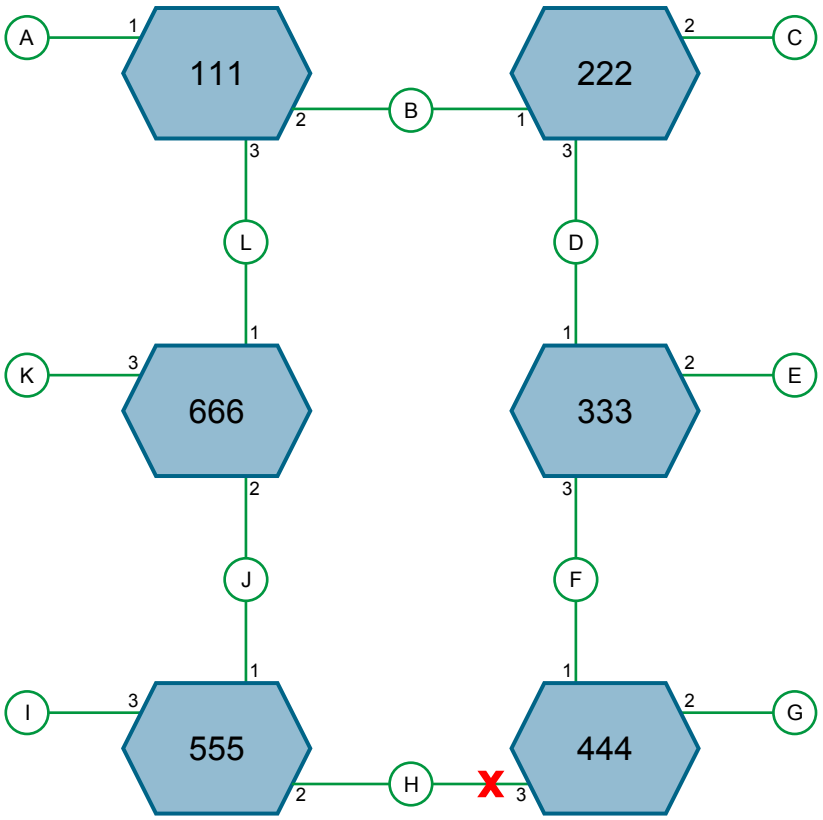


Figure 1034: Example - Ring Backbone Configuration

To design a ring backbone configuration with RSTP, do the following:

1. **Select the design parameters for the network.**

   What are the requirements for robustness and network fail-over/recovery times? Typically, ring backbones are chosen to provide cost effective but robust network designs.

2. **Identify required legacy support and ports with half-duplex/shared media restrictions.**

   These bridges should not be used if network fail-over/recovery times are to be minimized.

3. **Identify edge ports.**

   Ports that connect to host computers, IEDs and controllers may be set to edge ports in order to guarantee rapid transitioning to forwarding as well as to reduce the number of topology change notifications in the network.

4. **Choose the root bridge.**

   The root bridge can be selected to equalize either the number of bridges, number of stations or amount of traffic on either of its legs. It is important to realize that the ring will always be broken in one spot and that traffic always flows through the root.

5. **Assign bridge priorities to the ring.**

   For more information, refer to the RUGGEDCOM White Paper *Performance of the RSTP in Ring Network Topologies* available on https://www.siemens.com/ruggedcom.

6. **Decide upon a port cost calculation strategy.**

   It is recommended to use the auto-negotiated cost style, unless it is necessary for the network design to change the auto-negotiated cost style. Select whether the STP or RSTP cost style should be used. Make sure to configure the same cost style on all devices on the network.

7. **Disable RSTP Fast Root Failover option.**

   This is a proprietary feature of Siemens. In RUGGEDCOM ROX II, the RSTP Fast Root Failover option is enabled by default. It is recommended to disable this feature when operating in a Ring network.

8. Implement the network and test under load.

Section 14.3.2.3
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.

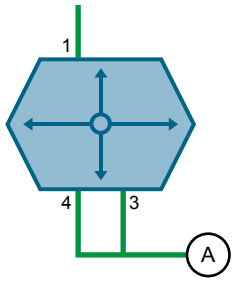


Figure 1035: Example - Port Redundancy

Section 14.3.3
MSTP Operation

The Multiple Spanning Tree (MST) algorithm and protocol provide greater control and flexibility than RSTP and legacy STP. MSTP (Multiple Spanning Tree Protocol) is an extension of RSTP, whereby multiple spanning trees may be maintained on the same bridged network. Data traffic is allocated to one or several spanning trees by mapping one or more VLANs to different Multiple Spanning Tree Instances (MSTIs).

The sophistication and utility of the MSTP implementation on a given bridged network is proportional to the amount of planning and design invested in configuring MSTP.

If MSTP is activated on some or all of the bridges in a network with no additional configuration, the result will be a fully and simply connected network. At best though, the result will be the same as a network using only RSTP. Taking full advantage of the features offered by MSTP requires a potentially large number of configuration variables to be derived from an analysis of data traffic on the bridged network, and from requirements for load sharing, redundancy, and path optimization. Once these parameters have all been derived, it is also critical they are consistently applied and managed across all bridges in an MST region.

By design, MSTP processing time is proportional to the number of active STP instances. This means MSTP will likely be significantly slower than RSTP. Therefore, for mission critical applications, RSTP should be considered a better network redundancy solution than MSTP.

CONTENTS

Section 14.3.3.1

MSTP Regions and Interoperability

In addition to supporting multiple spanning trees in a network of MSTP-capable bridges, MSTP is capable of interoperating with bridges that support only RSTP or legacy STP, without requiring any special configuration.

An MST region may be defined as the set of interconnected bridges whose MST Region Identification is identical. The interface between MSTP bridges and non-MSTP bridges, or between MSTP bridges with different MST Region Identification information, becomes part of an MST Region boundary.

Bridges outside an MST region will see the entire region as though it were a single (R)STP bridge, with the internal detail of the MST region being hidden from the rest of the bridged network. In support of this, MSTP maintains separate *hop counters* for spanning tree information exchanged at the MST region boundary versus information propagated inside the region. For information received at the MST region boundary, the (R)STP Message Age is incremented only once. Inside the region, a separate Remaining Hop Count is maintained, one for each spanning tree instance. The external Message Age parameter is referred to the (R)STP Maximum Age Time, whereas the internal Remaining Hop Counts are compared to an MST region-wide Maximum Hops parameter.

» MSTI

An MSTI (Multiple Spanning Tree Instance) is one of sixteen independent spanning tree instances that may be defined in an MST region (not including the IST). An MSTI is created by mapping a set of VLANs to a given MSTI ID. The same mapping must be configured on all bridges that are intended to be part of the MSTI. Moreover, all VLAN-to-MSTI mappings must be identical for all bridges in an MST region.

RUGGEDCOM ROX II supports 16 MSTIs in addition to the IST.

Each MSTI has a topology that is independent of others. Data traffic originating from the same source and bound to the same destination, but on different VLANs on different MSTIs, may therefore travel a different path across the network.

» IST

An MST region always defines an IST (Internal Spanning Tree). The IST spans the entire MST region, and carries all data traffic that is not specifically allocated (by VLAN) to a specific MSTI. The IST is always computed and is defined to be MSTI zero.

The IST is also the extension inside the MST region of the CIST

CST

The CST (Common Spanning Tree) spans the entire bridged network, including MST regions and any connected STP or RSTP bridges. An MST region is seen by the CST as an individual bridge, with a single cost associated with its traversal.

CIST

The CIST (Common and Internal Spanning Tree) is the union of the CST and the ISTs in all MST regions. The CIST therefore spans the entire bridged network, reaching into each MST region via the latter's IST to reach every bridge on the network.

Section 14.3.3.2

MSTP Bridge and Port Roles

MSTP supports the following bridge and port roles:

Bridge Roles

Role	Description
CIST Root	The CIST Root is the elected root bridge of the CIST (Common and Internal Spanning Tree), which spans all connected STP and RSTP bridges and MSTP regions.
CIST Regional Root	The root bridge of the IST within an MSTP region. The CIST Regional Root is the bridge within an MSTP region with the lowest cost path to the CIST Root. Note that the CIST Regional Root will be at the boundary of an MSTP region. Note also that it is possible for the CIST Regional Root to be the CIST Root.
MSTI Regional Root	The root bridge for an MSTI within an MSTP region. A root bridge is independently elected for each MSTI in an MSTP region.

Port Roles

Each port on an MSTP bridge may have more than one CIST role depending on the number and topology of spanning tree instances defined on the port.

Role	Description
CIST Port Roles	• The Root Port provides the minimum cost path from the bridge to the CIST Root via the CIST Regional Root. If the bridge itself happens to be the CIST Regional Root, the Root Port is also the Master Port for all MSTIs, and provides the minimum cost path to a CIST Root located outside the region. • A Designated Port provides the minimum cost path from an attached LAN, via the bridge to the CIST Regional Root. • Alternate and Backup Ports function the same as they do in RSTP, but relative to the CIST Regional Root.
MSTI Port Roles	For each MSTI on a bridge: • The Root Port provides the minimum cost path from the bridge to the MSTI Regional Root, if the bridge itself is not the MSTI Regional Root. • A Designated Port provides the minimum cost path from an attached LAN, via the bridge to the MSTI Regional Root. • Alternate and Backup Ports function the same as they do in RSTP, but relative to the MSTI Regional Root.

Role	Description
	The Master Port, which is unique in an MSTP region, is the CIST Root Port of the CIST Regional Root, and provides the minimum cost path to the CIST Root for all MSTIs.
Boundary Ports	A Boundary Port is a port on a bridge in an MSTP region that connects to either: a bridge belonging to a different MSTP region, or a bridge supporting only RSTP or legacy STP. A Boundary Port blocks or forwards all VLANs from all MSTIs and the CIST alike. A Boundary Port may be: • The CIST Root Port of the CIST Regional Root (and therefore also the MSTI Master Port). • A CIST Designated Port, CIST Alternate/Backup Port, or Disabled. At the MSTP region boundary, the MSTI Port Role is the same as the CIST Port Role. A Boundary Port connected to an STP bridge will send only STP BPDUs. One connected to an RSTP bridge need not refrain from sending MSTP BPDUs. This is made possible by the fact that the MSTP carries the CIST Regional Root Identifier in the field that RSTP parses as the Designated Bridge Identifier.

Section 14.3.3.3
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 14.3.3.4

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 14.3.4, "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 14.3.6.3, "Adding a Multiple Spanning Tree Instance".
3. Create static VLANs and map them to the MSTIs. For more information, refer to Section 8.5.5.2, "Adding a Static VLAN".
4. Configure individual MSTI for each switched Ethernet port and/or Ethernet trunk interface that will transmit/receive MST BPDU (Bridge Protocol Data Unit) traffic. For more information, refer to Section 14.3.7, "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 14.3.4, "Configuring STP Globally".

Section 14.3.4

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.

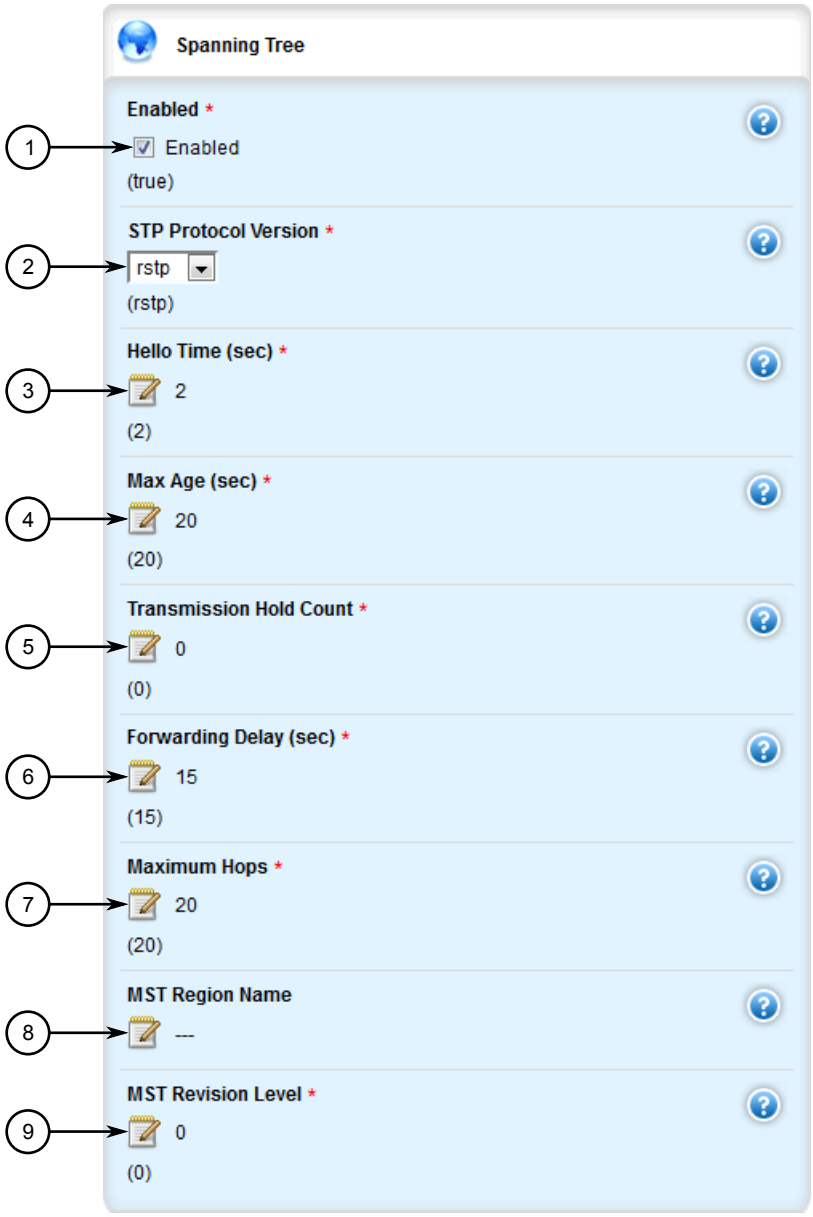


Figure 1036: Spanning Tree Form

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

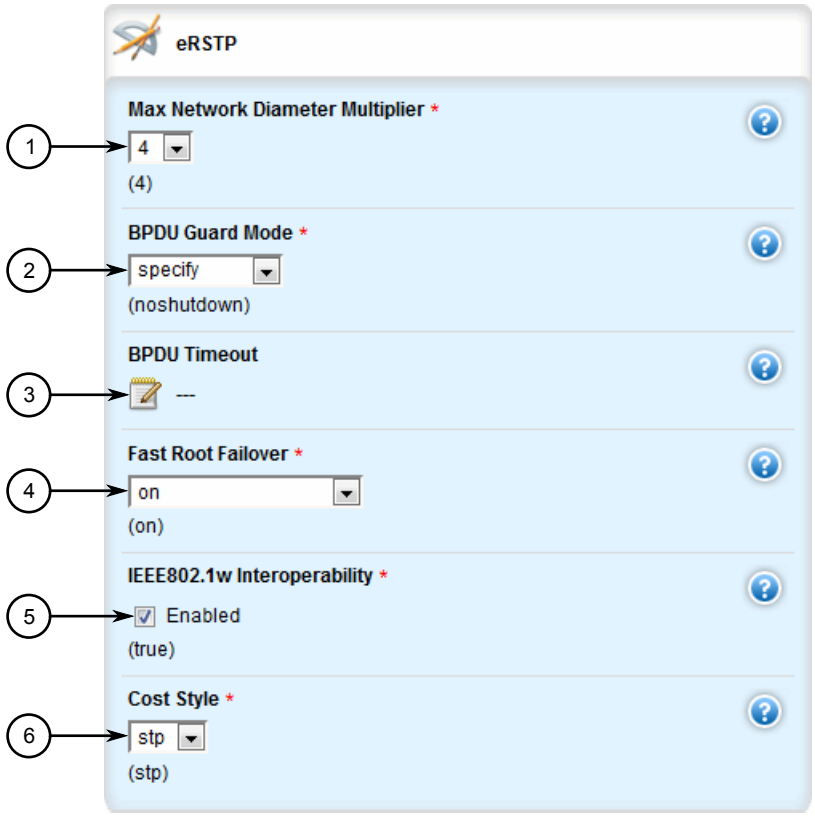


Figure 1037: eRSTP Form

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

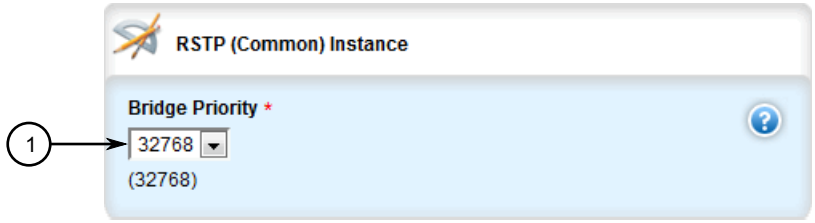


Figure 1038: RSTP (Common) Instance Form

1. Bridge Priority List

3. On the **Spanning Tree** form, configure the following parameters as required:

Parameter	Description
Enabled	**Synopsis:** { true, false } **Default:** true Enables STP/RSTP/MSTP for the bridge globally. Note that STP/RSTP/MSTP is enabled on a port when it is enabled globally and along with enabling per port setting.

Parameter	Description
STP Protocol Version	**Synopsis:** { stp, rstp, mstp } **Default:** rstp The version (either only STP or Rapid STP or Multiple STP) of the Spanning Tree Protocol (STP) to support.
Hello Time (sec)	**Synopsis:** A 32-bit unsigned integer between 1 and 10 **Default:** 2 The time between configuration messages issued by the root bridge. Shorter hello times result in faster detection of topology changes at the expense of moderate increases in STP traffic. (Relationship : maxAgeTime >= 2 * (helloTime + 1.0 seconds))
Max Age (sec)	**Synopsis:** A 32-bit unsigned integer between 6 and 40 **Default:** 20 The time for which a configuration message remains valid after being issued by the root bridge. Configure this parameter with care when many tiers of bridges exist, or slow speed links (such as those used in WANs) are part of the network. (Relationship : maxAgeTime >= 2 * (helloTime + 1.0 seconds))
Transmission Hold Count	**Synopsis:** A 32-bit unsigned integer between 0 and 100 **Default:** 0 The maximum number of configuration messages on each port that may be sent in a special event, such as recovering from a failure or bringing up a new link. After the maximum number of messages is reached, Rapid Spanning Tree Protocol (RSTP) will be limited to one message per second. Larger values allow the network to recover from failed links more quickly. If RSTP is being used in a ring architecture, the transmit count should be larger than the number of switches in the ring. If a number is not defined, the value is considered unlimited.
Forwarding Delay (sec)	**Synopsis:** A 32-bit unsigned integer between 4 and 30 **Default:** 15 The amount of time a bridge spends learning MAC addresses on a rising port before beginning to forward traffic. Lower values allow the port to reach the forwarding state more quickly, but at the expense of flooding unlearned addresses to all ports.
Maximum Hops	**Synopsis:** A 32-bit unsigned integer between 6 and 40 **Default:** 20 The maximum possible bridge diameter inside a Multiple Spanning Tree (MST) region. MST BPDUs propagating inside an MST region carry a time-to-live parameter decremented by every switch that propagates the BPDU. If the maximum number of hops inside the region exceeds the configured maximum, the BPDUs may be discarded due to their time-to-live information. This parameter is only applicable to Multiple Spanning Tree Protocol (MSTP) configurations.
MST Region Name	**Synopsis:** A string 1 to 32 characters long The name of the MST region. All devices in the same MST region must have the same region name configured
MST Revision Level	**Synopsis:** A 32-bit unsigned integer between 0 and 65535 **Default:** 0 The revision level for the MST configuration. Typically, all devices in the same MST region are configured with the same revision level. However, different revision levels can be used to create sub-regions under the same region name.

4. On the **eRSTP** form, configure the following parameters as required:

Parameter	Description
Max Network Diameter Multiplier	**Synopsis:** { 1, 4 } **Default:** 4 The Max Network Diameter as a multiplier of the MaxAgeTime value.

Parameter	Description
BPDU Guard Mode	**Synopsis:** { specify, noshutdown, untilreset } **Default:** noshutdown The Rapid Spanning Tree Protocol (RSTP) standard does not address network security. RSTP must process every received Bridge Protocol Data Unit (BPDU) and take an appropriate action. This opens a way for an attacker to influence RSTP topology by injecting RSTP BPDUs into the network. BPDU Guard is a feature that protects the network from BPDUs received by a port where RSTP-capable devices are not expected to be attached. If a BPDU is received by a port for which the 'Edge' parameter is set to 'TRUE' or RSTP is disabled, the port will be shut down for the time period specified by this parameter. • NO SHUTDOWN: BPDU Guard is disabled. • UNTIL RESET: The port will remain shut down until the port reset command is issued by the user. • SPECIFY: A timeout period is specified for the port using the BPDU Timeout parameter.
BPDU Timeout	**Synopsis:** A 32-bit unsigned integer between 1 and 86400 The time for which a port is shutdown. Only applicable when BPDU Guard Mode is set to *specify*.
Fast Root Failover	**Synopsis:** { on, off, on-with-standard-root } **Default:** on The Fast Root Failover algorithm. Options include: • Off: The Fast Root Failover algorithm is disabled. As such, a root switch failure may result in excessive connectivity recovery time in a mesh network. • On: Fast Root Failover is enabled and the most robust algorithm is used, which restores network connectivity quickly in case of root bridge failure in a mesh network. • On with standard root: Fast Root Failover is enabled but a relaxed algorithm is used, allowing the use of a standard switch in the root role.
IEEE802.1w Interoperability	**Synopsis:** { true, false } **Default:** true Enables/disables IEEE 802.1w Interoperability
Cost Style	**Synopsis:** { stp, rstp } **Default:** stp The style of link costs to employ. STP uses 16-bit path costs based upon 1x10E9/link speed (4 for 1Gbps, 19 for 100 Mbps and 100 for 10 Mbps) whereas RSTP uses 32-bit costs based upon 2x10E13/link speed (20,000 for 1Gbps, 200,000 for 100 Mbps and 2,000,000 for 10 Mbps). Note that RSTP link costs are used only when the bridge version support is set to allow RSTP and the port does not migrate to the Spanning Tree Protocol (STP).

5. On the **RSTP (Common) Instance** form, configure the following parameters as required:

Parameter	Description
Bridge Priority	**Synopsis:** { 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440 } **Default:** 32768 The priority assigned to the RSTP/Common Bridge Instance.

6. If necessary, add Multiple Spanning Tree Instances (MSTI). For more information, refer to Section 14.3.6.3, "Adding a Multiple Spanning Tree Instance".
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 14.3.5

Configuring STP for Switched Ethernet Ports and Ethernet Trunk Interfaces

To configure the Spanning Tree Protocol (STP) for a switched Ethernet port, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to:
   - **For switched Ethernet ports:**
     interface » switch » {interface} » spanning-tree, where *{interface}* is the name given to the switched Ethernet port.
   - **For Ethernet trunk interfaces:**
     interface » trunks » {id} » spanning-tree, where *{id}* is the ID given to the interface.

   The **Spanning Tree** form appears.

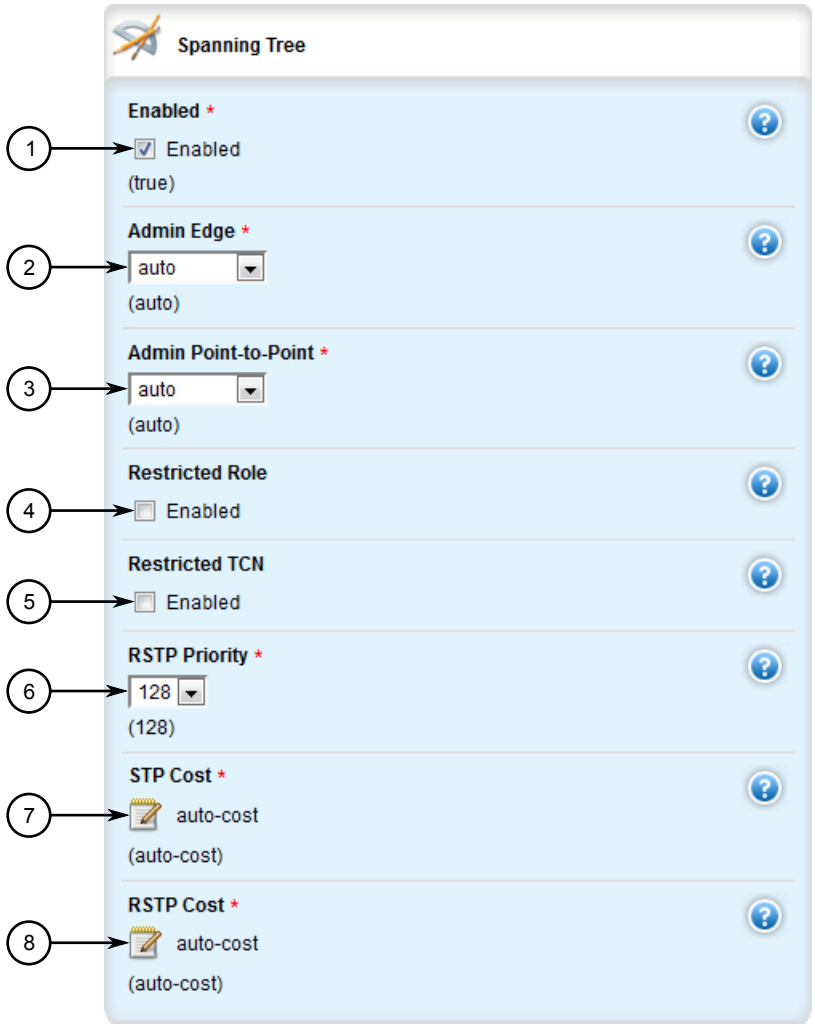


Figure 1039: Spanning Tree Form

1. Enabled Check Box **2.** Admin Edge List **3.** Admin Point-to-Point List **4.** Restricted Role Check Box **5.** Restricted TCN Check Box **6.** RSTP Priority List **7.** STP Cost Box **8.** RSTP Cost Box

3. Configure the following parameters as required:

Parameter	Description
Enabled	**Synopsis:** { true, false } **Default:** true Enables/disables STP/RSTP on the interface.
Admin Edge	**Synopsis:** { forceTrue, forceFalse, auto } **Default:** auto Edge ports are ports that do not participate in the spanning tree, but still send configuration messages. Edge ports transition directly to frame forwarding without any listening and learning delays. The MAC tables of edge ports do not need to be flushed when topology changes occur in the STP network. Unlike an STP-disabled port, accidentally connecting an edge port to another port in the spanning tree will result in

Parameter	Description
	a detectable loop. The *Edgeness* of the port will be switched off and the standard RSTP rules will apply (until the next link outage).
Admin Point-to-Point	**Synopsis:** { forceTrue, forceFalse, auto } **Default:** auto RSTP uses a peer-to-peer protocol that provides for rapid transitioning on point-to-point links. This protocol is automatically turned off in situations where multiple STP bridges communicate over a shared (non point-to-point) LAN. The bridge will automatically take point-to-point to be true when the link is found to be operating in full-duplex mode. The point-to-point parameter allows this behavior or overrides it, forcing point-to-point to be true or false. Force the parameter true when the port operates a point-to-point link but cannot run the link in full-duplex mode. Force the parameter false when the port operates the link in full-duplex mode, but is still not point-to-point (e.g. a full-duplex link to an unmanaged bridge that concentrates two other STP bridges).
Restricted Role	If enabled, causes the port not to be selected as the root port for the CIST or any MSTI, even though it has the best spanning tree priority vector. This parameter should be FALSE by default.
Restricted TCN	If TRUE, causes the port not to propagate received topology change notifications and topology changes to other ports. This parameter should be FALSE by default. If set, it can cause a temporary loss of connectivity after changes in a spanning tree's active topology as a result of persistent, incorrectly learned station location information.
RSTP Priority	**Synopsis:** { 0, 16, 32, 64, 96, 112, 128, 144, 160, 176, 192, 208, 224, 240 } **Default:** 128 The STP port priority. Ports of the same cost that attach to a common LAN will select the port to be used based upon the port priority.
STP Cost	**Synopsis:** { auto-cost } or a 32-bit unsigned integer between 0 and 65535 **Default:** auto-cost The cost to use in cost calculations, when the cost style parameter is set to STP in the bridge RSTP parameters configuration. Setting the cost manually provides the ability to preferentially select specific ports to carry traffic over others. Leave this field set to 'auto' to use the standard STP port costs as negotiated (four for 1Gbps, 19 for 100 Mbps links and 100 for 10 Mbps links). For MSTP, this parameter applies to both external and internal path cost.
RSTP Cost	**Synopsis:** { auto-cost } or a 32-bit unsigned integer between 0 and 2147483647 **Default:** auto-cost The cost to use in cost calculations, when the cost style parameter is set to RSTP in the bridge RSTP parameters configuration. Setting the cost manually provides the ability to preferentially select specific ports to carry traffic over others. Leave this field set to 'auto' to use the standard RSTP port costs as negotiated (20,000 for 1Gbps, 200,000 for 100 Mbps links and 2,000,000 for 10 Mbps links). For MSTP, this parameter applies to both external and internal path costs.

4. If necessary, add Multiple Spanning Tree Instances (MSTI). For more information, refer to Section 14.3.6.3, "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 14.3.6

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.

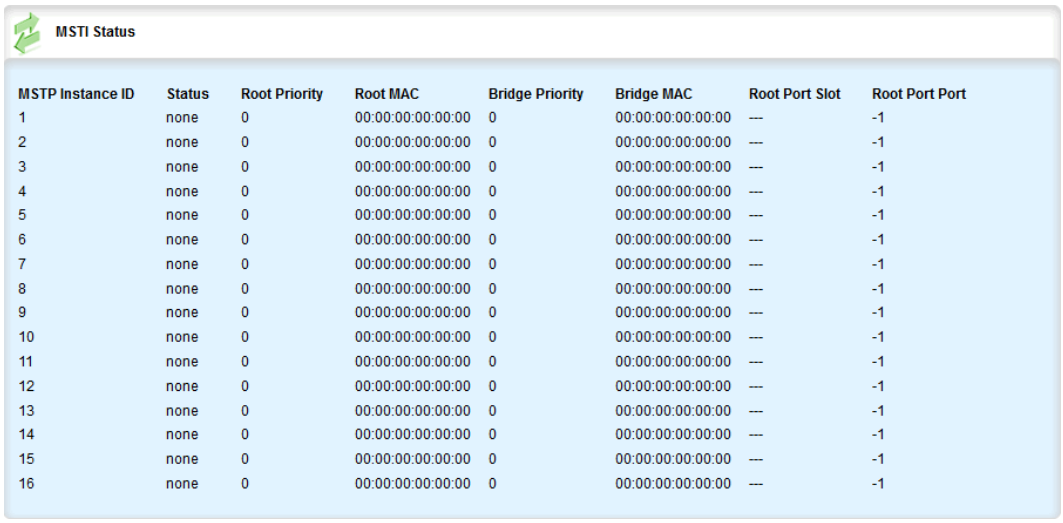
For more information about MSTP, refer to Section 14.3.3, "MSTP Operation".

CONTENTS

Section 14.3.6.1

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 1040: MSTI Status Table

This table provides the following information:

Parameter	Description
MSTP Instance ID	**Synopsis:** A 32-bit signed integer between 1 and 16

Parameter	Description
	The bridge identifier of this bridge.
status	**Synopsis:** { none, designatedBridge, notDesignatedForAnyLAN, rootBridge } The spanning tree status of the bridge. The status may be root or designated. This field may show text saying 'not designated for any LAN' if the bridge is not the designated bridge for any of its ports. This parameter is mandatory.
Root Priority	**Synopsis:** A 32-bit signed integer The bridge identifier of the root bridge. This parameter is mandatory.
Root MAC	**Synopsis:** A string 17 characters long The bridge identifier of the root bridge. This parameter is mandatory.
Bridge Priority	**Synopsis:** A 32-bit signed integer The bridge identifier of this bridge. This parameter is mandatory.
Bridge MAC	**Synopsis:** A string 17 characters long The bridge identifier of this bridge. This parameter is mandatory.
Root Port Slot	**Synopsis:** { { --- }{ sm, lm1, lm2, lm3, lm4, lm5, lm6, swport, eth, serport, celport, wlanport }{ trnk } } If the bridge is designated, this is the slot containing the port that provides connectivity towards the root bridge of the network. This parameter is mandatory.
Root Port Port	**Synopsis:** A 32-bit signed integer If the bridge is designated, this is the port of the slot that provides connectivity towards the root bridge of the network. This parameter is mandatory.
Root Path Cost	**Synopsis:** A 32-bit unsigned integer The total cost of the path to the root bridge composed of the sum of the costs of each link in the path. If custom costs have not been configured, 1Gbps ports will contribute a cost of four, 100 Mbps ports will contribute 19 and 10 Mbps ports will contribute 100. For the Common and Internal Spanning Tree (CIST) instance of the Multiple Spanning Tree Protocol (MSTP), this is an external root path cost, which is the cost of the path from the Internal Spanning Tree (IST) root (i.e. regional root) bridge to the Common Spanning Tree (CST) root (i.e. network "global" root) bridge. This parameter is mandatory.
Total Topology Changes	**Synopsis:** A 32-bit unsigned integer A count of topology changes in the network, as detected on this bridge through link failures or as signaled from other bridges. Excessively high or rapidly increasing counts signal network problems. This parameter is mandatory.

Section 14.3.6.2
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.

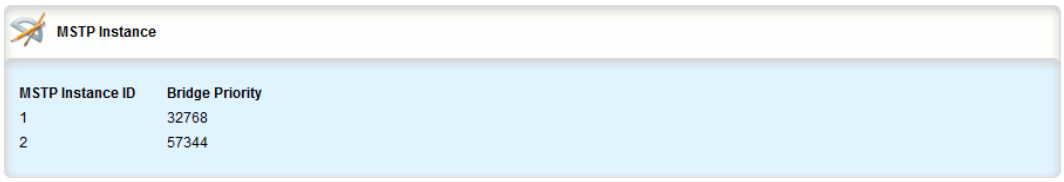


Figure 1041: MSTP Instance Table

If no MSTIs have been configured, add instances as needed. For more information, refer to Section 14.3.6.3, "Adding a Multiple Spanning Tree Instance".

Section 14.3.6.3
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.

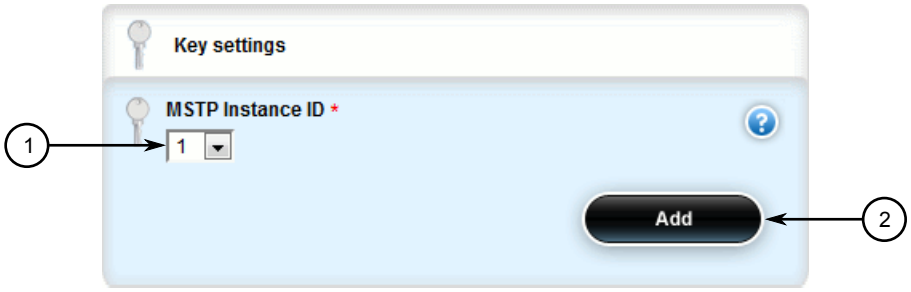


Figure 1042: Key Settings Form

1. MSTP Instance ID List **2.** Add Button

3. Configure the following parameter(s) as required:

Parameter	Description
MSTP Instance ID	**Synopsis:** A string 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.

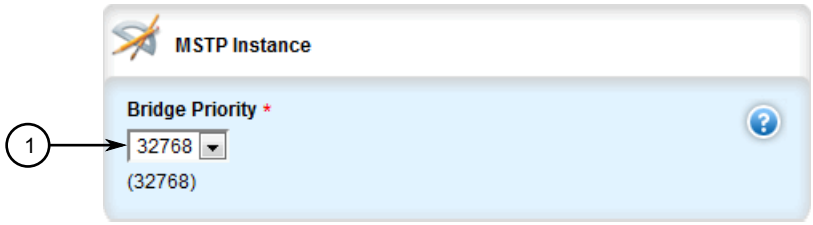


Figure 1043: MSTP Instance Form

1. Bridge Priority List

5. Configure the following parameter(s) as required:

Parameter	Description
Bridge Priority	**Synopsis:** { 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440 } **Default:** 32768 Bridge priority provides a way to control the topology of the Spanning Tree Protocol (STP) connected network. The desired root and designated bridges can be configured for a particular topology. The bridge with the lowest priority will become the root. In the event of a failure of the root bridge, the bridge with the next lowest priority will then become the root. Designated bridges that (for redundancy purposes) service a common Local Area Network (LAN) also use priority to determine which bridge is active. In this way, careful selection of bridge priorities can establish the path of traffic flows in normal and abnormal conditions.

6. Map one or more static VLANs and map them to the MSTI. For more information, refer to Section 8.5.5.2, "Adding a Static VLAN".
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 14.3.6.4
Deleting a Multiple Spanning Tree Instance

To delete a Multiple Spanning Tree Instance (MSTI), do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to ***switch » spanning-tree » mstp-instance***. The **MSTP Instance** table appears.

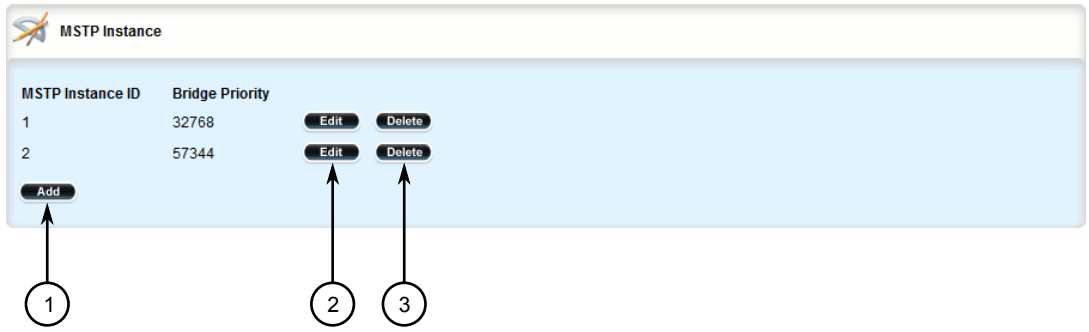


Figure 1044: MSTP Instance Table

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 14.3.7

Managing Multiple Spanning Tree Instances Per-Port

This section describes how to configure and manage Multiple Spanning Tree Instances (MSTIs) for individual ports.

CONTENTS

Section 14.3.7.1

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.:

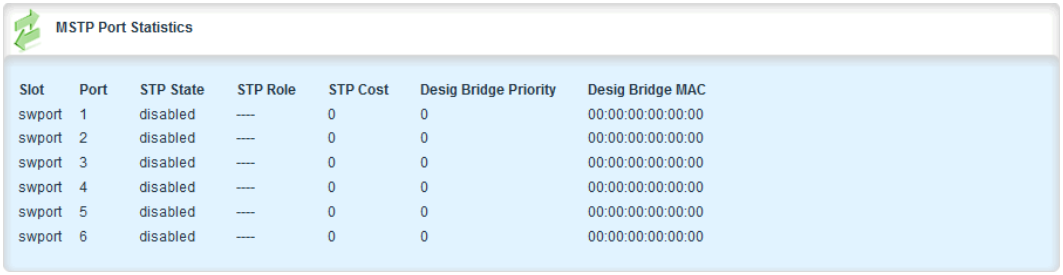


Figure 1045: MSTP Port Statistics Table

This table provides the following information:

Parameter	Description
Slot	**Synopsis:** { { sm, lm1, lm2, lm3, lm4, lm5, lm6, swport, eth, serport, celport, wlanport } { trnk } } The slot of the module that contains this port.
Port	**Synopsis:** A 32-bit signed integer between 1 and 16 The port number as seen on the front plate silkscreen of the module.
STP State	**Synopsis:** { disabled, blocking, listening, learning, forwarding, linkDown, discarding } The status of this interface in the spanning tree: • Disabled: The Spanning Tree Protocol (STP) is disabled on this port. • Link Down: STP is enabled on this port but the link is down. • Discarding: The link is not used in the STP topology but is standing by. • Learning: The port is learning MAC addresses in order to prevent flooding when it begins forwarding traffic. • Forwarding: The port is forwarding traffic. This parameter is mandatory.
STP Role	**Synopsis:** { ----, root, designated, alternate, backup, master } The role of this port in the spanning tree: • Designated: The port is designated for (i.e. carries traffic towards the root for) the Local Area Network (LAN) it is connected to. • Root: The single port on the bridge, which provides connectivity towards the root bridge. • Backup: The port is attached to a LAN that is serviced by another port on the bridge. It is not used but is standing by. • Alternate: The port is attached to a bridge that provides connectivity to the root bridge. It is not used but is standing by. • Master: Only exists in Multiple Spanning Tree Protocol (MSTP). The port is a Multiple Spanning Tree (MST) region boundary port and the single port on the bridge, which provides connectivity for the Multiple Spanning Tree Instance towards the Common Spanning Tree (CST) root bridge (i.e. this port is the root port for the Common Spanning Tree Instance). This parameter is mandatory.
STP Cost	**Synopsis:** A 32-bit unsigned integer The total cost of the path to the root bridge composed of the sum of the costs of each link in the path. If custom costs have not been configured, 1Gbps ports will contribute a cost of four, 100 Mbps ports will contribute 19 and 10 Mbps ports will contribute 100. For the Common and Internal Spanning Tree (CIST) instance of Multiple Spanning Tree Protocol (MSTP), this is an external root path cost, which is the cost of the path from the Internal Spanning Tree (IST) root (i.e. regional root) bridge to the Common Spanning Tree (CST) root (i.e. network "global" root) bridge.

Parameter	Description
	This parameter is mandatory.
Desig Bridge Priority	**Synopsis:** A 32-bit signed integer The bridge identifier of this bridge. This parameter is mandatory.
Desig Bridge MAC	**Synopsis:** A string 17 characters long The bridge identifier of this bridge. This parameter is mandatory.

Section 14.3.7.2
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.

Figure 1046: MSTI Configuration Table

If no MSTIs have been configured, add them as needed. For more information, refer to Section 14.3.7.3, "Adding a Port-Specific Multiple Spanning Tree Instance".

Section 14.3.7.3
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.

3. Click **<Add msti>** in the menu. The **Key Settings** form appears.

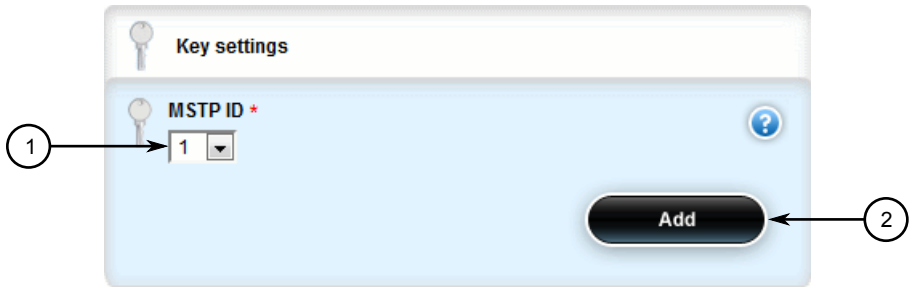


Figure 1047: Key Settings Form

1. MSTP ID List **2.** Add Button

4. Configure the following parameter(s) as required:

Parameter	Description
MSTP ID	**Synopsis:** A string MSTP Instance Identifier

5. 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.

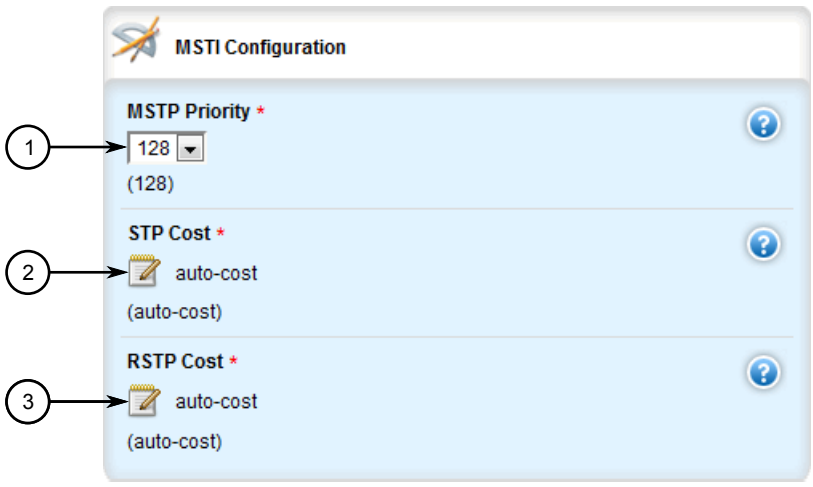


Figure 1048: MSTI Configuration Form

1. MSTP Priority List **2.** STP Cost List **3.** RSTP Cost List

6. Configure the following parameter(s) as required:

Parameter	Description
MSTP Priority	**Synopsis:** { 0, 16, 32, 64, 96, 112, 128, 144, 160, 176, 192, 208, 224, 240 } **Default:** 128 The STP port priority. Ports of the same cost that attach to a common LAN will select the port to be used based upon the port priority.
STP Cost	**Synopsis:** { auto-cost } or a 32-bit unsigned integer between 0 and 65535 **Default:** auto-cost The cost to use in cost calculations, when the cost style parameter is set to STP in the bridge RSTP parameter configuration. Setting the cost manually provides the ability to preferentially select specific ports to carry traffic over others. Leave this field set to 'auto' to use the standard STP port costs as negotiated (four for 1Gbps, 19 for 100 Mbps links and 100 for 10 Mbps links). For MSTP, this parameter applies to both external and internal path costs.
RSTP Cost	**Synopsis:** { auto-cost } or a 32-bit unsigned integer between 0 and 2147483647 **Default:** auto-cost The cost to use in cost calculations, when the cost style parameter is set to RSTP in the bridge RSTP parameter configuration. Setting the cost manually provides the ability to preferentially select specific ports to carry traffic over others. Leave this field set to 'auto' to use the standard RSTP port costs as negotiated (20,000 for 1Gbps, 200,000 for 100 Mbps links and 2,000,000 for 10 Mbps links). For MSTP, this parameter applies to both external and internal path costs.

7. Map one or more static VLANs and map them to the MSTI. For more information, refer to Section 8.5.5.2, "Adding a Static VLAN".
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 14.3.7.4

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.

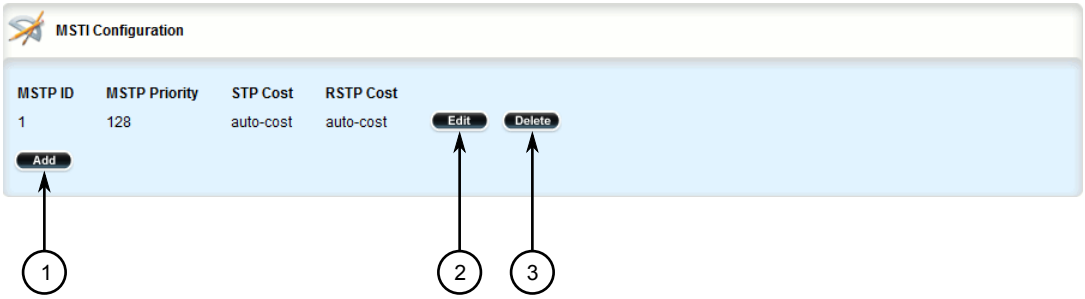


Figure 1049: MSTI Configuration Table

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 14.3.8

Viewing the Status of RSTP

To view the status of the RSTP network, navigate to ***switch » spanning-tree***. The **RSTP Status** form appears.

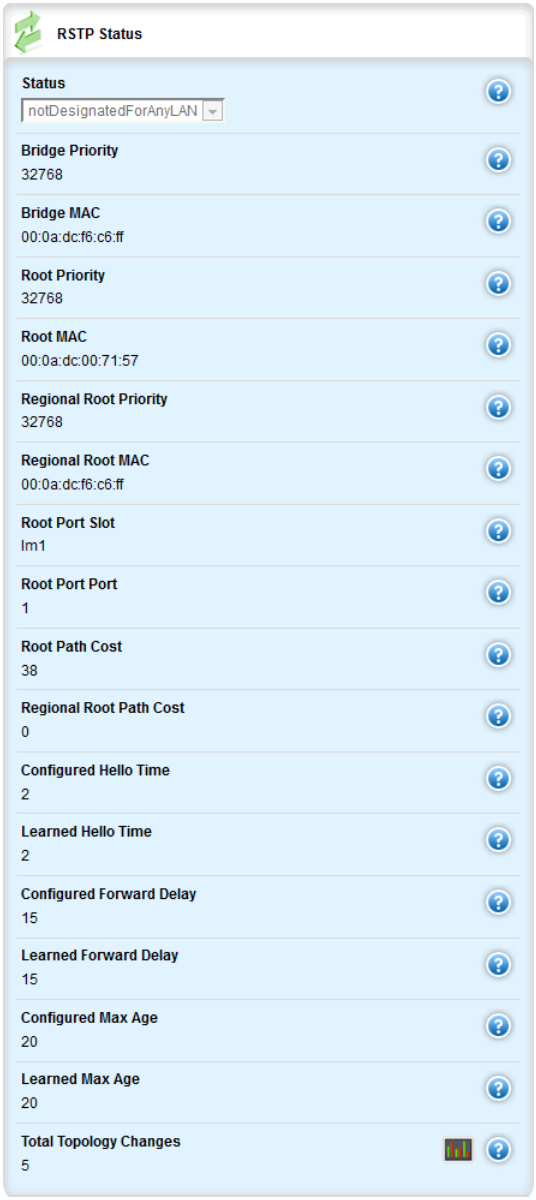


Figure 1050: RSTP Status Form

This form provides the following information:

Parameter	Description
Status	**Synopsis:** { none, designatedBridge, notDesignatedForAnyLAN, rootBridge } The spanning tree status of the bridge. The status may be root or designated. This field may show text saying 'not designated for any LAN' if the bridge is not the designated bridge for any of its ports. This parameter is mandatory.
Bridge Priority	**Synopsis:** A 32-bit signed integer The bridge identifier of this bridge. This parameter is mandatory.

Parameter	Description
Bridge MAC	**Synopsis:** A string 17 characters long The bridge identifier of this bridge. This parameter is mandatory.
Root Priority	**Synopsis:** A 32-bit signed integer The ports to which the multicast group traffic is forwarded. This parameter is mandatory.
Root MAC	**Synopsis:** A string 17 characters long The ports to which the multicast group traffic is forwarded. This parameter is mandatory.
Regional Root Priority	**Synopsis:** A 32-bit signed integer The bridge identifier of the Internal Spanning Tree (IST) regional root bridge for the Multiple Spanning Tree (MST) region this device belongs to. This parameter is mandatory.
Regional Root MAC	**Synopsis:** A string 17 characters long The bridge identifier of the Internal Spanning Tree (IST) regional root bridge for the Multiple Spanning Tree (MST) region this device belongs to. This parameter is mandatory.
Root Port Slot	**Synopsis:** { { --- }{ sm, lm1, lm2, lm3, lm4, lm5, lm6, swport, eth, serport, celport, wlanport }{ trnk } } If the bridge is designated, this is the slot containing the port that provides connectivity towards the root bridge of the network. This parameter is mandatory.
Root Port Port	**Synopsis:** A 32-bit signed integer If the bridge is designated, this is the port of the slot that provides connectivity towards the root bridge of the network. This parameter is mandatory.
Root Path Cost	**Synopsis:** A 32-bit unsigned integer The total cost of the path to the root bridge, composed of the sum of the costs of each link in the path. If custom costs have not been configured. 1Gbps ports will contribute a cost of four, 100 Mbps ports will contribute 19 and 10 Mbps ports will contribute 100. For the Common and Internal Spanning Tree (CIST) instance of the Multiple Spanning Tree Protocol (MSTP), this is an external root path cost, which is the cost of the path from the Internal Spanning Tree (IST) root (i.e. regional root) bridge to the Common Spanning Tree (CST) root (i.e. network "global" root) bridge. This parameter is mandatory.
Regional Root Path Cost	**Synopsis:** A 32-bit unsigned integer For the Common and Internal Spanning Tree (CIST) instance of the Multiple Spanning Tree Protocol (MSTP), this is the cost of the path to the Internal Spanning Tree (IST) root (i.e. regional root) bridge This parameter is mandatory.
Configured Hello Time	**Synopsis:** A 32-bit signed integer The configured hello time from the Bridge RSTP Parameters menu. This parameter is mandatory.
Learned Hello Time	**Synopsis:** A 32-bit signed integer The actual hello time provided by the root bridge as learned in configuration messages. This time is used in designated bridges.

Parameter	Description
	This parameter is mandatory.
Configured Forward Delay	**Synopsis:** A 32-bit signed integer The configured forward delay time from the Bridge RSTP Parameters menu. This parameter is mandatory.
Learned Forward Delay	**Synopsis:** A 32-bit signed integer The actual forward delay time provided by the root bridge as learned in configuration messages. This time is used in designated bridges. This parameter is mandatory.
Configured Max Age	**Synopsis:** A 32-bit signed integer The configured maximum age time from the Bridge RSTP Parameters menu. This parameter is mandatory.
Learned Max Age	**Synopsis:** A 32-bit signed integer The actual maximum age time provided by the root bridge as learned in configuration messages. This time is used in designated bridges. This parameter is mandatory.
Total Topology Changes	**Synopsis:** A 32-bit unsigned integer A count of topology changes in the network, as detected on this bridge through link failures or as signaled from other bridges. Excessively high or rapidly increasing counts signal network problems. This parameter is mandatory.

Section 14.3.9

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.

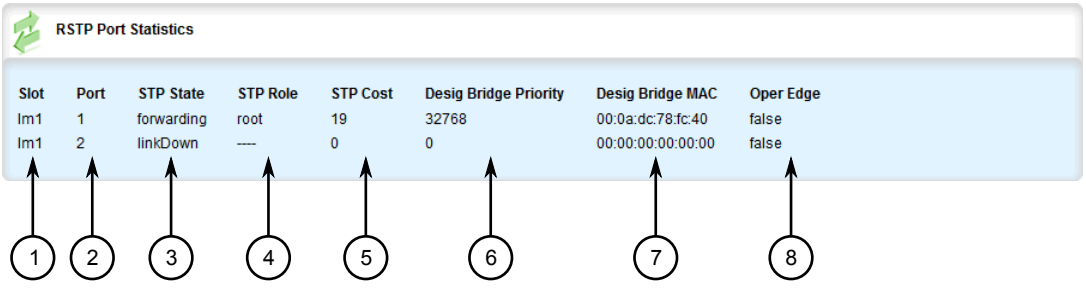


Figure 1051: RSTP Port Statistics Form

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	**Synopsis:** { { sm, lm1, lm2, lm3, lm4, lm5, lm6, swport, eth, serport, celport, wlanport } { trnk } }

Parameter	Description
	The slot of the module that contains this port.
Port	**Synopsis:** A 32-bit signed integer between 1 and 16 The port number as seen on the front plate silkscreen of the module.
STP State	**Synopsis:** { disabled, blocking, listening, learning, forwarding, linkDown, discarding } Describes the status of this interface in the spanning tree: • Disabled: Spanning Tree Protocol (STP) is disabled on this port. • Link Down: STP is enabled on this port but the link is down. • Discarding: The link is not used in the STP topology but is standing by. • Learning: The port is learning MAC addresses in order to prevent flooding when it begins forwarding traffic. • Forwarding : The port is forwarding traffic. This parameter is mandatory.
STP Role	**Synopsis:** { ----, root, designated, alternate, backup, master } The role of this port in the spanning tree: • Designated: The port is designated for (i.e. carries traffic towards the root for) the Local Area Network (LAN) it is connected to. • Root: The single port on the bridge, which provides connectivity towards the root bridge. • Backup: The port is attached to a LAN that is serviced by another port on the bridge. It is not used but is standing by. • Alternate: The port is attached to a bridge that provides connectivity to the root bridge. It is not used but is standing by. • Master: Only exists in Multiple Spanning Tree Protocol (MSTP). The port is a Multiple Spanning Tree (MST) region boundary port and the single port on the bridge, which provides connectivity for the Multiple Spanning Tree Instance (MSTI) towards the Common Spanning Tree (CST) root bridge (i.e. this port is the root port for the Common Spanning Tree Instance). This parameter is mandatory.
STP Cost	**Synopsis:** A 32-bit unsigned integer The cost offered by this port. If the Bridge RSTP Parameters Cost Style is set to STP, 1Gbps ports will contribute a cost of four, 100 Mbps ports will contribute 19 and 10 Mbps ports contribute 100. If the Cost Style is set to RSTP, 1Gbps will contribute 20,000, 100 Mbps ports will contribute a cost of 200,000 and 10 Mbps ports contribute a cost of 2,000,000. Note that even if the Cost style is set to RSTP, a port that migrates to STP will have its cost limited to a maximum of 65535. This parameter is mandatory.
Desig Bridge Priority	**Synopsis:** A 32-bit signed integer between 0 and 65535 Provided on the root ports of the designated bridges, the bridge identifier of the bridge this port is connected to. This parameter is mandatory.
Desig Bridge MAC	**Synopsis:** A string 17 characters long Provided on the root ports of the designated bridges, the bridge identifier of the bridge this port is connected to. This parameter is mandatory.
Oper Edge	**Synopsis:** { true, false } Whether or not the port is operating as an edge port. This parameter is mandatory.
RX RSTs	**Synopsis:** A 32-bit unsigned integer The number of Rapid Spanning Tree Protocol (RSTP) configuration messages received on this port.

Parameter	Description
	This parameter is mandatory.
TX RSTs	**Synopsis:** A 32-bit unsigned integer The number of Rapid Spanning Tree Protocol (RSTP) configuration messages transmitted on this port. This parameter is mandatory.
RX Configs	**Synopsis:** A 32-bit unsigned integer The number of Spanning Tree Protocol (STP) configuration messages received on this port. This parameter is mandatory.
TX Configs	**Synopsis:** A 32-bit unsigned integer The number of Spanning Tree Protocol (STP) configuration messages transmitted on this port. This parameter is mandatory.
RX TCNs	**Synopsis:** A 32-bit unsigned integer The number of configuration change notification messages received on this port. Excessively high or rapidly increasing counts signal network problems. This parameter is mandatory.
TX TCNs	**Synopsis:** A 32-bit unsigned integer The number of configuration messages transmitted from this port. This parameter is mandatory.

Section 14.3.10
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.

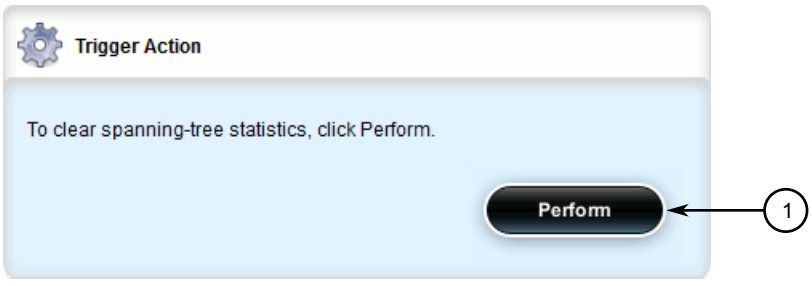


Figure 1052: Trigger Action Form

1. Perform Button

2. Click **Perform**.

15 Network Discovery and Management

RUGGEDCOM ROX II supports the following protocols for automatic network discovery, monitoring and device management:

- **Link Layer Device Protocol (LLDP)**
  Use LLDP to broadcast the device's network capabilities and configuration to other devices on the network, as well as receive broadcasts from other devices.
- **Simple Network Management Protocol (SNMP)**
  Use SNMP to notify select users or groups of certain events that happen during the operation of the device, such as changes to network topology, link state, spanning tree root, etc.
- **Network Configuration Protocol (NETCONF)**
  Use NETCONF to remotely download, upload, change, and delete configuration data on the device.

CONTENTS

Section 15.1

Managing LLDP

RUGGEDCOM ROX II supports the Link Layer Discovery Protocol (LLDP), a Layer 2 protocol for automated network discovery.

LLDP is an IEEE standard protocol (IEEE 802.11AB) that allows a networked device to advertise its own basic networking capabilities and configuration. It can simplify the troubleshooting of complex networks and can be used by Network Management Systems (NMS) to obtain and monitor detailed information about a network’s topology. LLDP data are made available via SNMP (through support of LLDP-MIB).

LLDP allows a networked device to discover its neighbors across connected network links using a standard mechanism. Devices that support LLDP are able to advertise information about themselves, including their capabilities, configuration, interconnections, and identifying information.

LLDP agent operation is typically implemented as two modules: the LLDP transmit module and LLDP receive module. The LLDP transmit module, when enabled, sends the local device’s information at regular intervals, in 802.1AB standard format. Whenever the transmit module is disabled, it transmits an LLDPDU (LLDP data unit) with a time-to-live (TTL) TLV containing *0* in the information field. This enables remote devices to remove the information associated with the local device in their databases. The LLDP receive module, when enabled, receives information about remote devices and updates its LLDP database of remote systems. When new or updated information is received, the receive module initiates a timer for the valid duration indicated by the TTL TLV in the

received LLDPDU. A remote system's information is removed from the database when an LLDPDU is received from it with TTL TLV containing *0* in its information field.

CAUTION!
Security hazard – risk of unauthorized access and/or exploitation. LLDP is not secure by definition. Avoid enabling LLDP on devices connected to external networks. Siemens recommends using LLDP only in secure environments operating within a security perimeter.

NOTE
LLDP is implemented to keep a record of only one device per Ethernet port. Therefore, if there are multiple devices sending LLDP information to a switch port on which LLDP is enabled, information about the neighbor on that port will change constantly.

CONTENTS

Section 15.1.1
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.

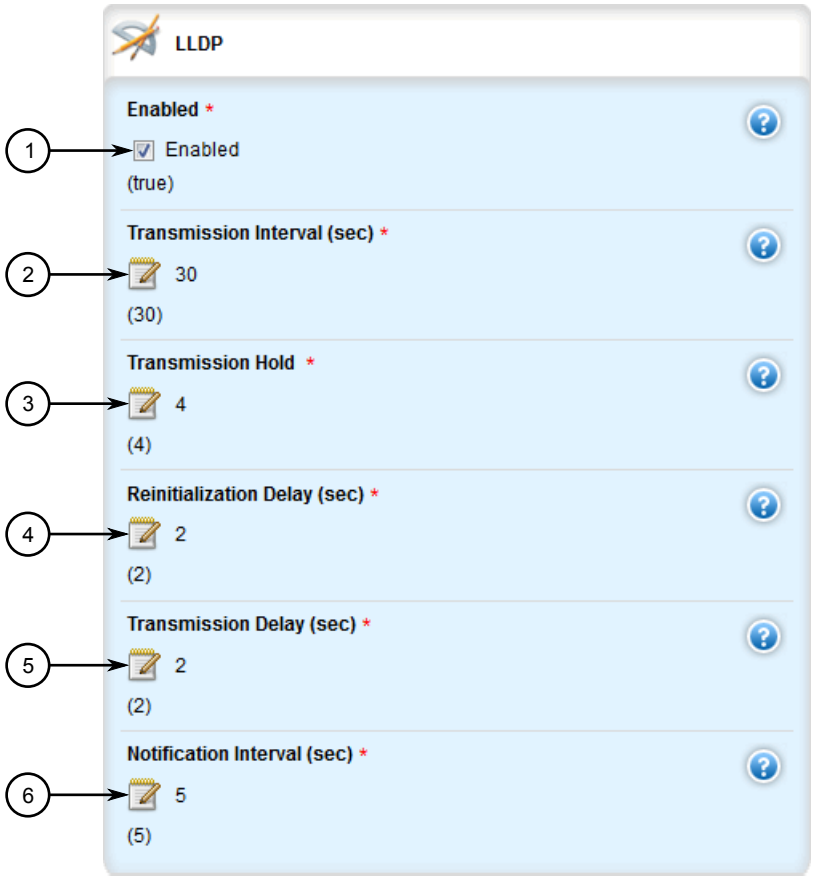


Figure 1053: LLDP Form

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	**Synopsis:** { true, false } **Default:** 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)	**Synopsis:** A 32-bit signed integer between 5 and 32768 **Default:** 30 The interval at which Link Layer Discovery Protocol (LLDP) frames are transmitted on behalf of this LLDP agent.
Transmission Hold	**Synopsis:** A 32-bit signed integer between 2 and 10 **Default:** 4 The multiplier of the Tx Interval parameter that determines the actual time-to-live (TTL) value used in an LLDPDU. The actual TTL value can be expressed by the following formula: TTL = MIN(65535, (Tx Interval * Tx Hold))
Reinitialization Delay (sec)	**Synopsis:** A 32-bit signed integer between 1 and 10

Parameter	Description
	Default: 2 The delay in seconds from when the value of the Admin Status parameter of a particular port becomes 'Disbled' until re-initialization will be attempted.
Transmission Delay (sec)	**Synopsis:** A 32-bit signed integer between 1 and 8192 **Default:** 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 * Tx Interval)
Notification Interval (sec)	**Synopsis:** A 32-bit signed integer between 5 and 3600 **Default:** 5 Controls transmission of LLDP traps. The agent must not generate more than one trap in an indicated period.

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 15.1.2

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 1054: LLDP Global Statistics Form

1. Inserts **2.** Deletes **3.** Drops **4.** Ageouts **5.** Time Stamp of Last Change

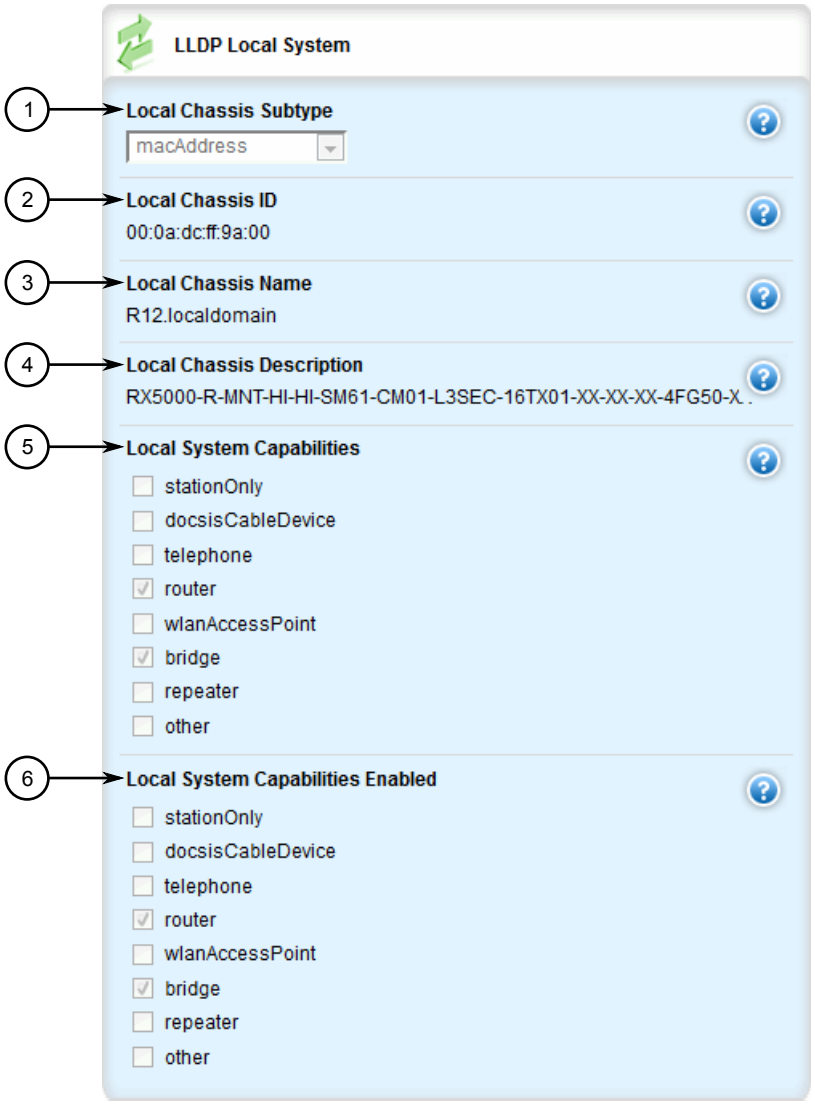


Figure 1055: LLDP Local System Form

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	**Synopsis:** A 32-bit unsigned integer between 0 and 4294967295 The number of times an entry was inserted into the LLDP Neighbor Information Table. This parameter is mandatory.
Deletes	**Synopsis:** A 32-bit unsigned integer between 0 and 4294967295 The number of times an entry was deleted from the LLDP Neighbor Information Table. This parameter is mandatory.
Drops	**Synopsis:** A 32-bit unsigned 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. This parameter is mandatory.
Ageouts	**Synopsis:** A 32-bit unsigned integer between 0 and 4294967295 The number of all TLVs discarded. This parameter is mandatory.
Time Stamp of Last Change	**Synopsis:** A string The duration of time between power-on and when this information was received. This parameter is mandatory.

The **LLDP Local System** form displays the following information:

Parameter	Description
Local Chassis Subtype	**Synopsis:** { chassisComponent, interfaceAlias, portComponent, macAddress, networkAddress, interfaceName, local } local-chassis-subtype This parameter is mandatory.
Local Chassis ID	**Synopsis:** A string 17 characters long local-chassis-id This parameter is mandatory.
Local Chassis Name	**Synopsis:** A string 1 to 255 characters long local-system-name This parameter is mandatory.
Local Chassis Description	**Synopsis:** A string 1 to 255 characters long local-system-desc This parameter is mandatory.
Local System Capabilities	**Synopsis:** { other, repeater, bridge, wlanAccessPoint, router, telephone, docsisCableDevice, stationOnly } local-system-caps This parameter is mandatory.
Local System Capabilities Enabled	**Synopsis:** { other, repeater, bridge, wlanAccessPoint, router, telephone, docsisCableDevice, stationOnly } local-system-caps-enabled This parameter is mandatory.

Section 15.1.3

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.

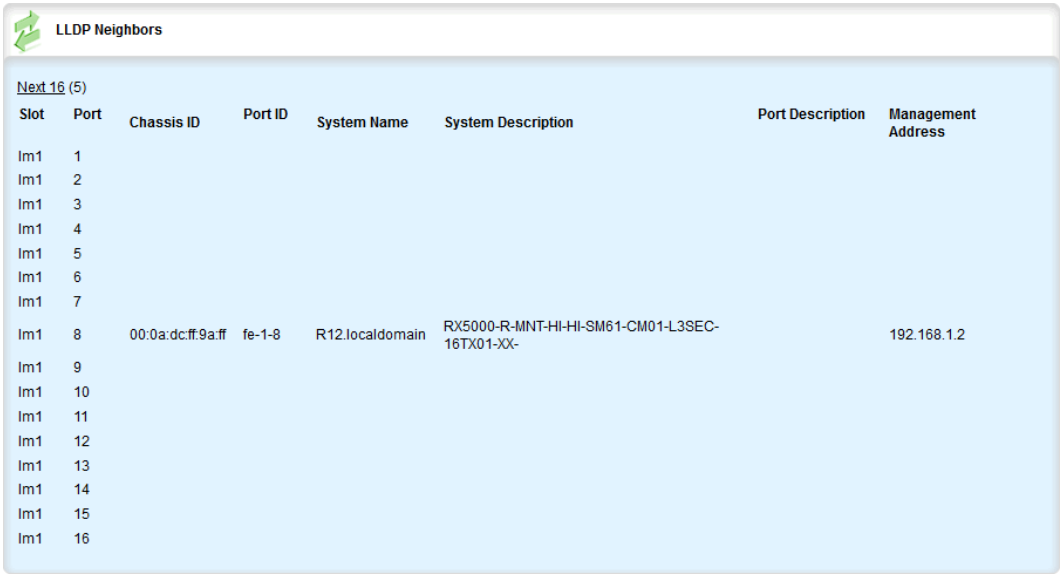


Figure 1056: LLDP Neighbors Form

This table displays the following information:

Parameter	Description
slot	**Synopsis:** { { --- }{ pm1, pm2, main }{ sm, lm1, lm2, lm3, lm4, lm5, lm6, swport, eth, serport, celport, wlanport }{ cm, em }{ trnk } } The slot of the module that contains this port.
Port	**Synopsis:** A 32-bit signed integer between 1 and 16 The port number as seen on the front plate silkscreen of the module.
Chassis ID	**Synopsis:** A string 17 characters long The Chassis ID information received from a remote Link Layer Discovery Protocol (LLDP) agent.
Port ID	**Synopsis:** A string 17 characters long The port ID (MAC) information received from a remote Link Layer Discovery Protocol (LLDP) agent.
System Name	**Synopsis:** A string 1 to 255 characters long The system name information received from a remote Link Layer Discovery Protocol (LLDP) agent
System Description	**Synopsis:** A string 1 to 255 characters long The system descriptor information received from a remote Link Layer Discovery Protocol (LLDP) agent.
Port Description	**Synopsis:** A string 1 to 255 characters long The port description information received from a remote Link Layer Discovery Protocol (LLDP) agent.
Management Address	**Synopsis:** A string 31 characters long The management address received from a remote Link Layer Discovery Protocol (LLDP) agent.
Management Address Interface ID	**Synopsis:** A 32-bit signed integer

Parameter	Description
	The Management Address Interface ID received from a remote Link Layer Discovery Protocol (LLDP) agent.
System Capabilities	**Synopsis:** { other, repeater, bridge, wlanAccessPoint, router, telephone, docsisCableDevice, stationOnly } The system capabilities that are advertised for the remote device.
System Capabilities Enabled	**Synopsis:** { other, repeater, bridge, wlanAccessPoint, router, telephone, docsisCableDevice, stationOnly } Enables/disables the System Capabilities feature.
Chassis Subtype	**Synopsis:** { chassisComponent, interfaceAlias, portComponent, macAddress, networkAddress, interfaceName, local } The chassis subtype information received from a remote Link Layer Discovery Protocol (LLDP) agent.
Port Subtype	**Synopsis:** { interfaceAlias, portComponent, macAddress, networkAddress, interfaceName, agentCircuitId, local } The port subtype information received from a remote Link Layer Discovery Protocol (LLDP) agent.
Management Address Subtype	**Synopsis:** { other, ipV4, ipV6, nsap, hdlc, bbn1822, all802, e163, e164, f69, x121, ipx, appleTalk, decnetIV, banyanVines, e164withNsap, dns, distinguishedName, asNumber, xtpOverIpv4, xtpOverIpv6, xtpNativeModeXTP, fibreChannelWWPN, fibreChannelWWNN, gwid, afi, reserved } The management address subtype received from a remote Link Layer Discovery Protocol (LLDP) agent.
Management Address Interface Subtype	**Synopsis:** { unknown, ifIndex, systemPortNumber } The management address interface subtype received from a remote Link Layer Discovery Protocol (LLDP) agent.
Time Stamp of Last Change	**Synopsis:** A string The duration of time between power-on and when this information was received.

Section 15.1.4
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.

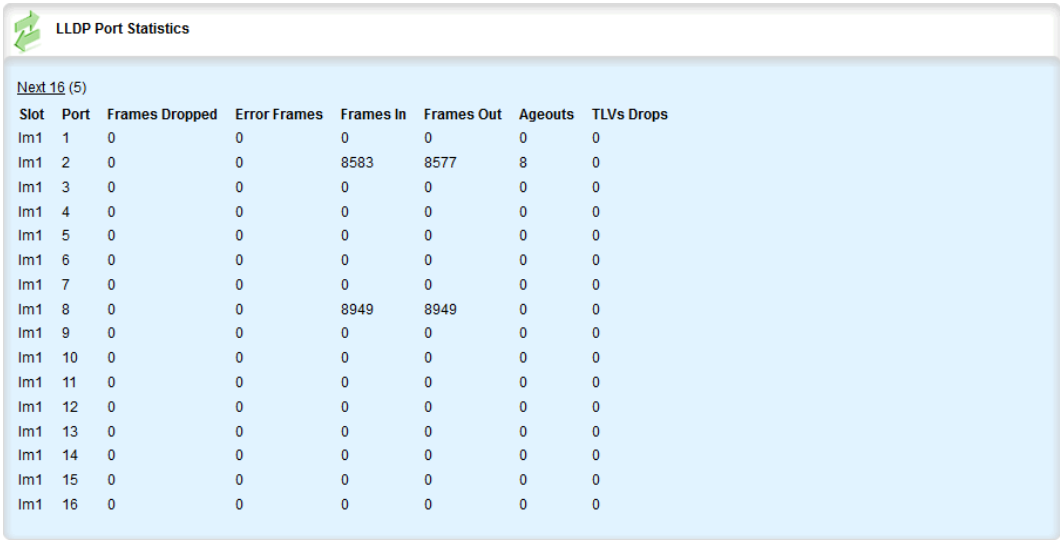


Figure 1057: LLDP Port Statistics Form

This table displays the following information:

Parameter	Description
slot	**Synopsis:** { { --- }{ pm1, pm2, main }{ sm, lm1, lm2, lm3, lm4, lm5, lm6, swport, eth, serport, celport, wlanport }{ cm, em }{ trnk } } The slot of the module that contains this port.
Port	**Synopsis:** A 32-bit signed integer between 1 and 16 The port number as seen on the front plate silkscreen of the module.
Frames Dropped	**Synopsis:** A 32-bit unsigned integer between 0 and 4294967295 A counter of all Link Layer Discovery Protocol (LLDP) frames discarded. This parameter is mandatory.
Error Frames	**Synopsis:** A 32-bit unsigned integer between 0 and 4294967295 A counter of all Link Layer Discovery Protocol Units (LLDPUs) received with detectable errors. This parameter is mandatory.
Frames In	**Synopsis:** A 32-bit unsigned integer between 0 and 4294967295 A counter of all Link Layer Discovery Protocol Units (LLDPUs) received. This parameter is mandatory.
Frames Out	**Synopsis:** A 32-bit unsigned integer between 0 and 4294967295 A counter of all Link Layer Discovery Protocol Units (LLDPUs) transmitted. This parameter is mandatory.
Ageouts	**Synopsis:** A 32-bit unsigned 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 This parameter is mandatory.
TLVs Drops	**Synopsis:** A 32-bit unsigned integer between 0 and 4294967295 A counter of all TLVs discarded This parameter is mandatory.

Parameter	Description
TLVs Unknown	**Synopsis:** A 32-bit unsigned 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 This parameter is mandatory.

Section 15.2

Managing SNMP

The Simple Network Management Protocol (SNMP) is used by network management systems and the devices they manage. It is used to report alarm conditions and other events that occur on the devices it manages.

In addition to SNMPv1 and SNMPv2, RUGGEDCOM ROX II also supports SNMPv3, which offers the following features:

- Provides the ability to send a notification of an event via *traps*. Traps are unacknowledged UDP messages and may be lost in transit.
- Provides the ability to notify via *informs*. Informs simply add acknowledgment to the trap process, resending the trap if it is not acknowledged in a timely fashion.
- Encrypts all data transmitted by scrambling the contents of each packet to prevent it from being seen by an unauthorized source. The AES CFB 128 and DES3 encryption protocols are supported.
- Authenticates all messages to verify they are from a valid source.
- Verifies the integrity of each message by making sure each packet has not been tampered with in-transit.

SNMPv3 also provides security models and security levels. A security model is an authentication strategy that is set up for a user and the group in which the user resides. A security level is a permitted level of security within a security model. A combination of a security model and security level will determine which security mechanism is employed when handling an SNMP packet.

Before configuring SNMP, note the following:

- each user belongs to a group
- a group defines the access policy for a set of users
- an access policy defines what SNMP objects can be accessed for: reading, writing and creating notifications
- a group determines the list of notifications its users can receive
- a group also defines the security model and security level for its users

CONTENTS

- Section 15.2.9, “Managing SNMP Group Access”

Section 15.2.1

MIB Files and SNMP Traps

The current MIB files supported by RUGGEDCOM ROX II can be downloaded from the https://www.siemens.com/ruggedcom.

NOTE
SNMP traps are not configurable in RUGGEDCOM ROX II.

The MIB files support the following SNMP traps:

Standard	MIB	Trap and Description
RFC 3418	SNMPv2-MIB	**authenticationFailure** An authenticationFailure trap signifies that the SNMP entity has received a protocol message that is not properly authenticated. While all implementations of SNMP entities MAY be capable of generating this trap, the snmpEnableAuthenTraps object indicates whether this trap will be generated.
		coldStart A coldStart trap signifies that the SNMP entity, supporting a notification originator application, is reinitializing itself and that its configuration may have been altered.
		warmStart A warmStart trap signifies that the SNMP entity, supporting a notification originator application, is reinitializing itself such that its configuration is unaltered.
RFC 4188	BRIDGE-MIB	**newRoot** The newRoot trap indicates that the sending agent has become the new root of the Spanning Tree. The trap is sent by a bridge soon after its election as the new root (e.g. upon expiration of the Topology Change Timer) immediately subsequent to its election. Implementation of this trap is optional.
		topologyChange A topologyChange trap is sent by a bridge when any of its configured ports transitions from the Learning state to the Forwarding state, or from the Forwarding state to the Blocking state. The trap is not sent if a newRoot trap is sent for the same transition. Implementation of this trap is optional.
IEEE Std 802.1AB-2005	LLDP-MIB	**lldpRemTablesChange** An lldpRemTablesChange notification is sent when the value of lldpStatsRemTableLastChangeTime changes. It can be utilized by a Network Management System (NMS) to trigger LLDP remote systems table maintenance polls. Note that transmission of lldpRemTablesChange notifications are throttled by the agent, as specified by the lldpNotificationInterval object.
RFC 1229, 2863, 2233, 1573	IF-MIB	**linkUp** A linkUp trap signifies that the SNMP entity, acting in an agent role, has detected that the ifOperStatus object for one of its communication links left the down state and transitioned into some other state (but not into the notPresent state). This other state is indicated by the included value of ifOperStatus.
		linkDown A linkDown trap signifies that the SNMP entity, acting in an agent role, has detected that the ifOperStatus object for one of its communication links is about

Standard	MIB	Trap and Description
		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	**trapGenericTrap** The main subtree for RUGGEDCOM generic traps. Used for *User Authentication Events* only.
		trapPowerSupplyTrap The main subtree for the RUGGEDCOM power supply trap.
		trapSwUpgradeTrap The main subtree for the RUGGEDCOM software upgrade trap.
		trapCfgChangeTrap The main subtree for the RUGGEDCOM configuration change trap.
		trapFanBankTrap The main subtree for the RUGGEDCOM fan bank trap.
		trapHotswapModuleStateChangeTrap The main subtree for the RUGGEDCOM fan hot-swap module state change trap.
RFC 3895	DS1-MIB	**ds1LineStatusChange** A ds1LineStatusChange trap is sent when the status of a dsx1Line instance changes. The value of the trap is the value of one or more of the following instances: • **dsx1RcvFarEndLOF** – Far end Loss of Frames (i.e. yellow alarm or RAI) • **dsx1RcvAIS** – Far end sending AIS • **dsx1LossOfFrame** – Near end Loss of Frame (i.e. red alarm) • **dsx1LossofSignal** – Near end Loss of Signal • **dsx1OtherFailure** – Out of Frame • **dsx1NoAlarm**

Section 15.2.2
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.

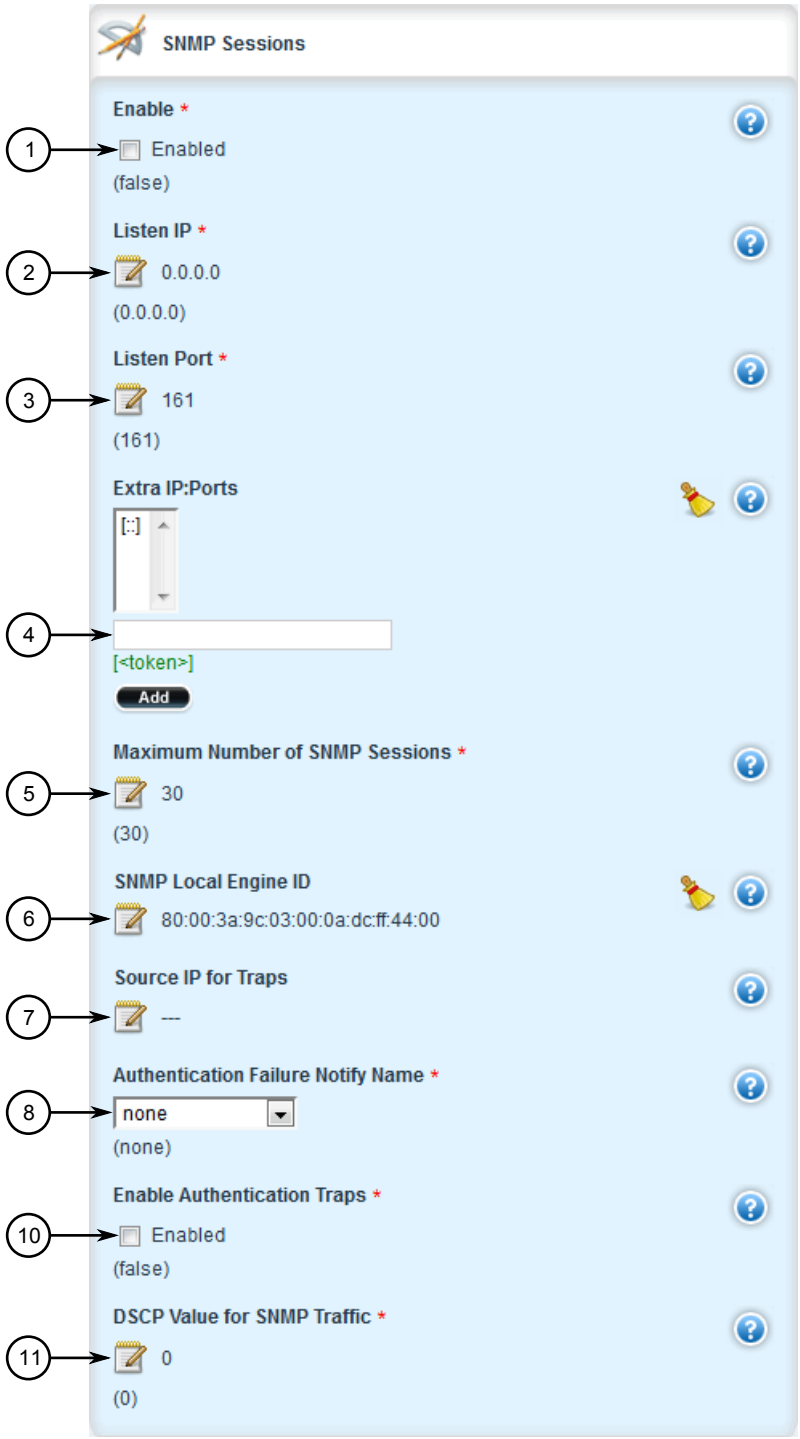


Figure 1058: SNMP Sessions

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):

IMPORTANT!
To generate all SNMP traffic for a specific interface, make sure the IP address for the desired interface is set for both the `Listen IP` *and* `Source IP for Traps` *parameters.*

Parameter	Description
Enable	**Synopsis:** { true, false } **Default:** false Provides the ability to configure SNMP features on the device.
Listen IP	**Synopsis:** A string **Default:** 0.0.0.0 The IP Address the SNMP agent will listen on for SNMP requests.
Listen Port	**Synopsis:** A 16-bit unsigned integer between 0 and 65535 **Default:** 161 The port the SNMP agent will listen on for SNMP requests.
Extra IP:Ports	**Synopsis:** A string 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.
Maximum Number of SNMP Sessions	**Synopsis:** a 32-bit unsigned integer **Default:** 30 The maximum number of concurrent SNMP sessions.
SNMP Local Engine ID	**Synopsis:** A string 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.
Source IP for Traps	**Synopsis:** A string If set, all traffic/traps originating from this device shall use the configured IP Address for the Source IP.
Authentication Failure Notify Name	**Synopsis:** { none, snmpv1_trap, snmpv2_trap, snmpv2_inform, snmpv3_trap, snmpv3_inform } **Default:** none 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.
Enable Authentication Traps	**Synopsis:** { true, false } **Default:** false Enables authentication traps to be sent from the SNMP agent.
DSCP Value for SNMP Traffic	**Synopsis:** An 8-bit unsigned integer between 0 and 63 **Default:** 0 Support for setting the Differentiated Services Code Point (6 bits) for traffic originating from the SNMP agent.

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 15.2.3

Viewing Statistics for SNMP

To view the statistics collected for SNMP, navigate to ***admin » snmp***. The **SNMP USM** form appears.

Figure 1059: SNMP USM Form

This table provides the following information:

Parameter	Description
Unsupported Security Levels	**Synopsis:** A 32-bit unsigned integer 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. This parameter is mandatory.
Not In Time Windows	**Synopsis:** A 32-bit unsigned integer The total number of packets received by the SNMP engine which were dropped because they appeared outside of the authoritative SNMP engine's window. This parameter is mandatory.
Unknown User Names	**Synopsis:** A 32-bit unsigned integer 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. This parameter is mandatory.
Unknown Engine IDs	**Synopsis:** A 32-bit unsigned integer 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. This parameter is mandatory.
Wrong Digests	**Synopsis:** A 32-bit unsigned integer The total number of packets received by the SNMP engine which were dropped because they did not contain the expected digest value. This parameter is mandatory.
Decryption Errors	**Synopsis:** A 32-bit unsigned integer The total number of packets received by the SNMP engine which were dropped because they could not be decrypted. This parameter is mandatory.

Section 15.2.4

Discovering SNMP Engine IDs

To discover an ID of a remote SNMP protocol engine, 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.

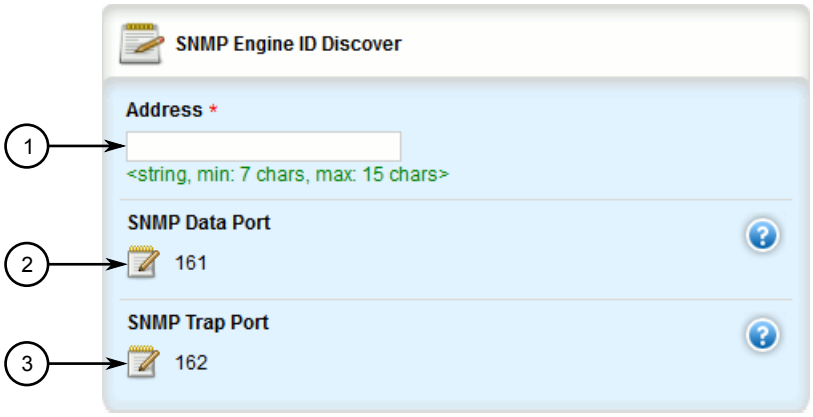


Figure 1060: SNMP Engine ID Discover Form

1. Address Box **2.** SNMP Data Port Box **3.** SNMP Trap Port Box

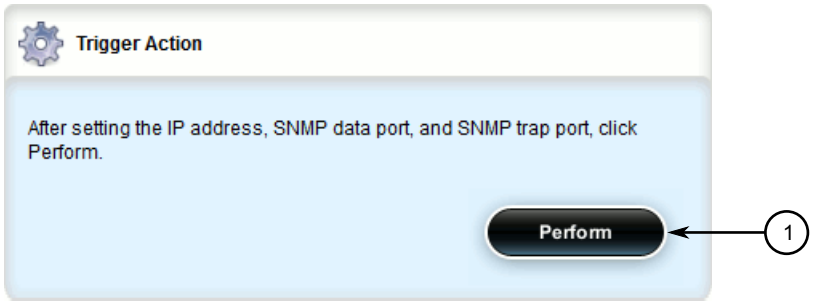


Figure 1061: Trigger Action Form

1. Perform Button

2. On the **SNMP Engine ID Discover Form** form, configure the following parameter(s) as required:

Parameter	Description
address	**Synopsis:** A string 7 to 15 characters long This parameter is mandatory.
SNMP Data Port	**Synopsis:** A 32-bit signed integer between 0 and 65535 **Default:** 161 The SNMP data port the device listens on (if any).
SNMP Trap Port	**Synopsis:** A 32-bit signed integer between 0 and 65535 **Default:** 162

Parameter	Description
	The SNMP trap port the device listens on (if any).

3. On the **Trigger Action** form, click **Perform**.

Once discovered, the ID is displayed. For example:

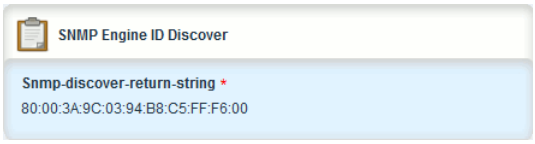


Figure 1062: Engine ID Discovered (Example)

1. Perform Button

Section 15.2.5

Managing SNMP Communities

This section describes how to manage SNMP communities.

CONTENTS

Section 15.2.5.1

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.

Figure 1063: 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 15.2.5.2, "Adding an SNMP Community".

Section 15.2.5.2
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.

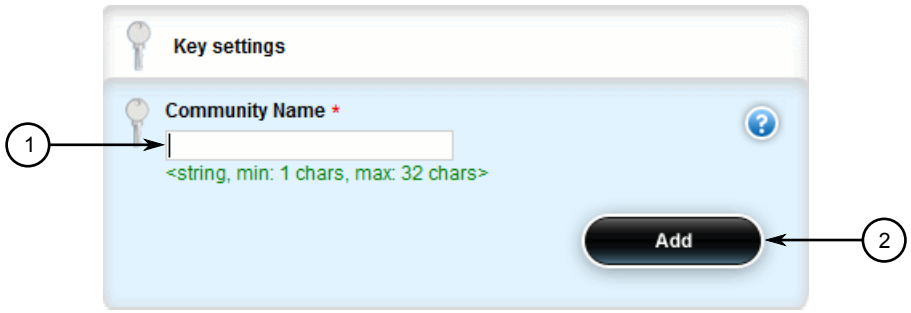


Figure 1064: Key Settings Form

1. Community Name Box **2.** Add Button

3. Configure the following parameter(s) as required:

Parameter	Description
Community Name	**Synopsis:** A string 1 to 32 characters long The SNMP community name.

4. Click **Add** to create the community. The **SNMPv1/v2c Community Configuration** form appears.

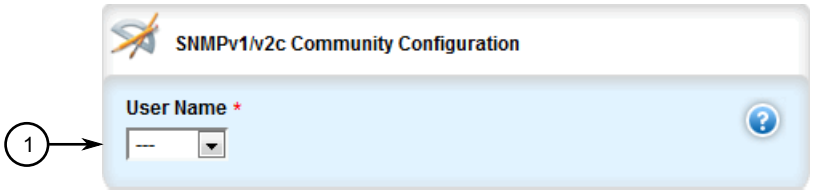


Figure 1065: SNMPv1/v2c Community Configuration Form

1. User Name List

5. Configure the following parameter(s) as required:

Parameter	Description
User Name	**Synopsis:** A string The SNMP community security name. This parameter is mandatory.

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 15.2.5.3
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.

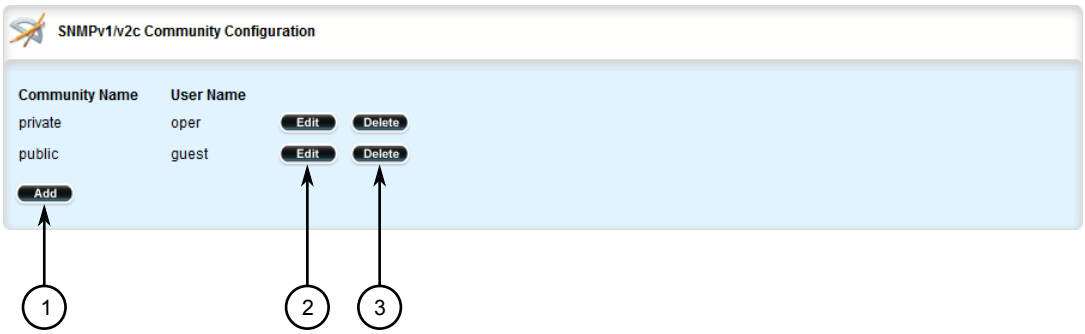


Figure 1066: SNMPv1/v2c Community Configuration Table

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 15.2.6
Managing SNMP Target Addresses

This section describes how to manage SNMP target addresses.

CONTENTS

Section 15.2.6.1
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.

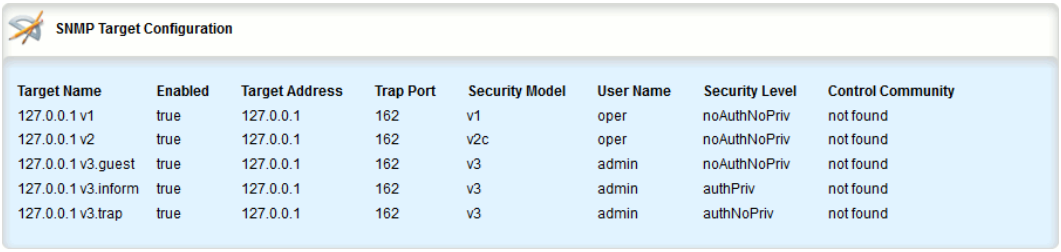


Figure 1067: SNMPv3 Target Configuration Table

If no SNMP target addresses have been configured, add target addresses as needed. For more information, refer to Section 15.2.6.2, "Adding an SNMP Target Address".

Section 15.2.6.2
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.

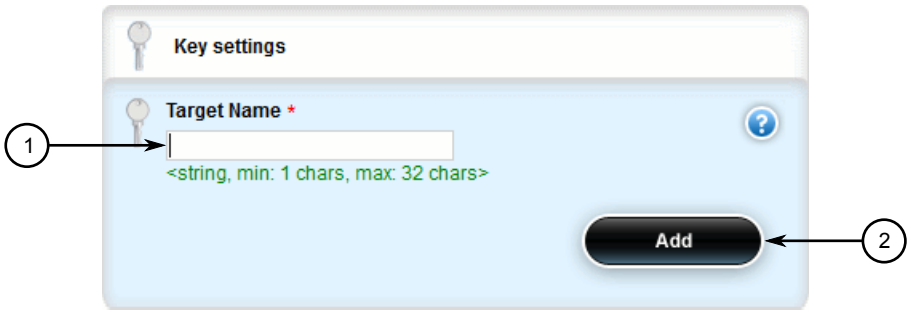


Figure 1068: Key Settings Form

1. Target Name Box **2.** Add Button

3. Configure the following parameter(s) as required:

Parameter	Description
Target Name	**Synopsis:** 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.

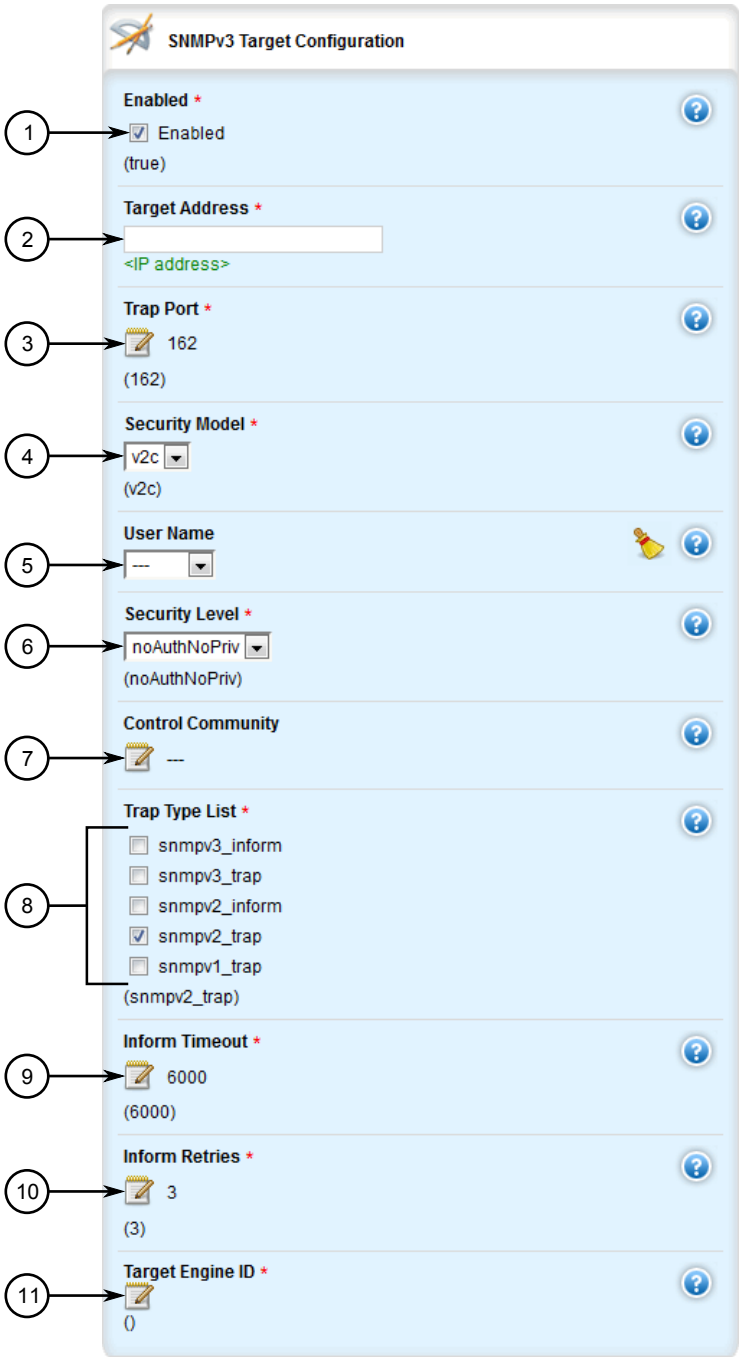


Figure 1069: SNMPv3 Target Configuration Form

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	**Synopsis:** { true, false } **Default:** true Enables/disables this specific target.
Target Address	**Synopsis:** A string An IPv4 or IPv6 address for the remote target. This parameter is mandatory.
Trap Port	**Synopsis:** A 16-bit unsigned integer between 0 and 65535 **Default:** 162 The UDP Port for the remote target to receive traps on.
Security Model	**Synopsis:** { v1, v2c, v3 } **Default:** v2c The SNMP security model to use: SNMPv1, SNMPv2c, or USM/SNMPv3.
User Name	**Synopsis:** A string The user name to be used in communications with this target. This parameter is mandatory.
Security Level	**Synopsis:** { noAuthNoPriv, authNoPriv, authPriv } **Default:** noAuthNoPriv The SNMP security level: • authPriv: Communication with authentication and privacy. • authNoPriv: Communication with authentication and without privacy. • noAuthnoPriv: Communication without authentication and privacy.
Control Community	**Synopsis:** A string 1 to 32 characters long Restricts incoming SNMP requests from the IPv4 or IPv6 address associated with this community.
Trap Type List	**Synopsis:** { snmpv1_trap, snmpv2_trap, snmpv2_inform, snmpv3_trap, snmpv3_inform } **Default:** snmpv2_trap Selects the type of trap communications to be sent to this target. **NOTE** *Multiple options can be selected.*
Inform Timeout	**Synopsis:** A 32-bit signed integer between 0 and 2147483647 **Default:** 6000 The timeout used for reliable inform transmissions (seconds*100).
Inform Retries	**Synopsis:** A 32-bit signed integer between 0 and 255 **Default:** 3 The number of retries used for reliable inform transmissions.
Target Engine ID	**Synopsis:** A string The target's SNMP local engine ID. This field may be left blank.

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 15.2.6.3
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.

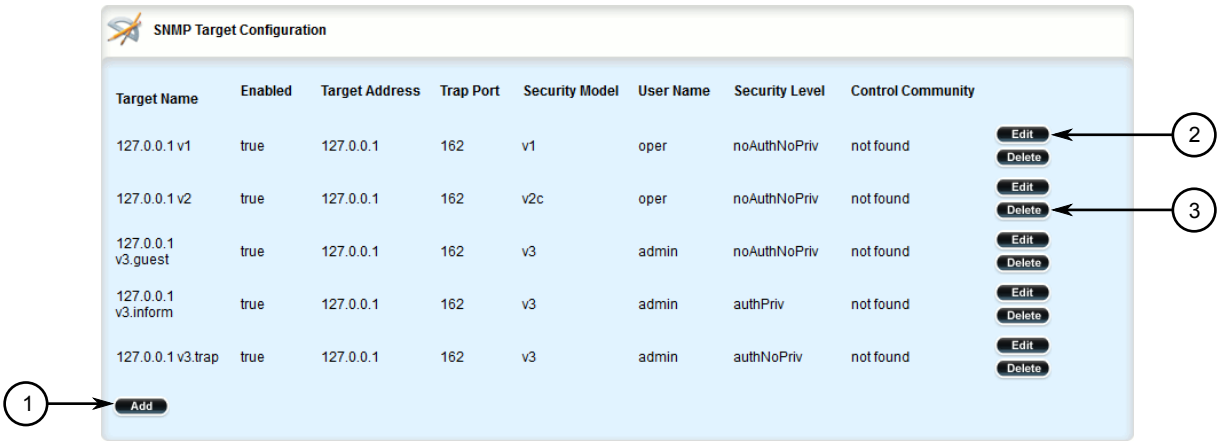


Figure 1070: SNMPv3 Target Configuration Table

1. Add Button **2.** Edit Button **3.** Delete Button

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 15.2.7
Managing SNMP Users

This section describes how to manage SNMP users.

CONTENTS

Section 15.2.7.1
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.

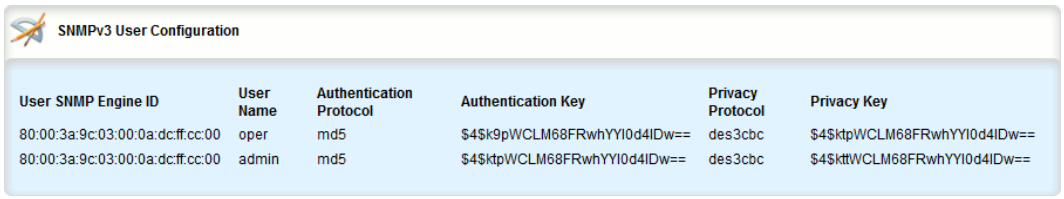


Figure 1071: SNMP User Configuration Table

If no SNMP users have been configured, add users as needed. For more information, refer to Section 15.2.7.2, "Adding an SNMP User".

Section 15.2.7.2
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.

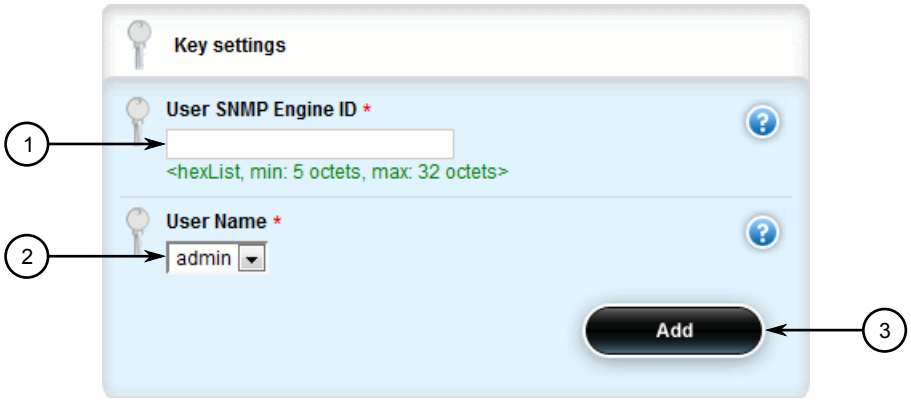


Figure 1072: Key Settings Form

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	**Synopsis:** A string The administratively-unique identifier for the SNMP engine; a value in the format 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	**Synopsis:** A string 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.

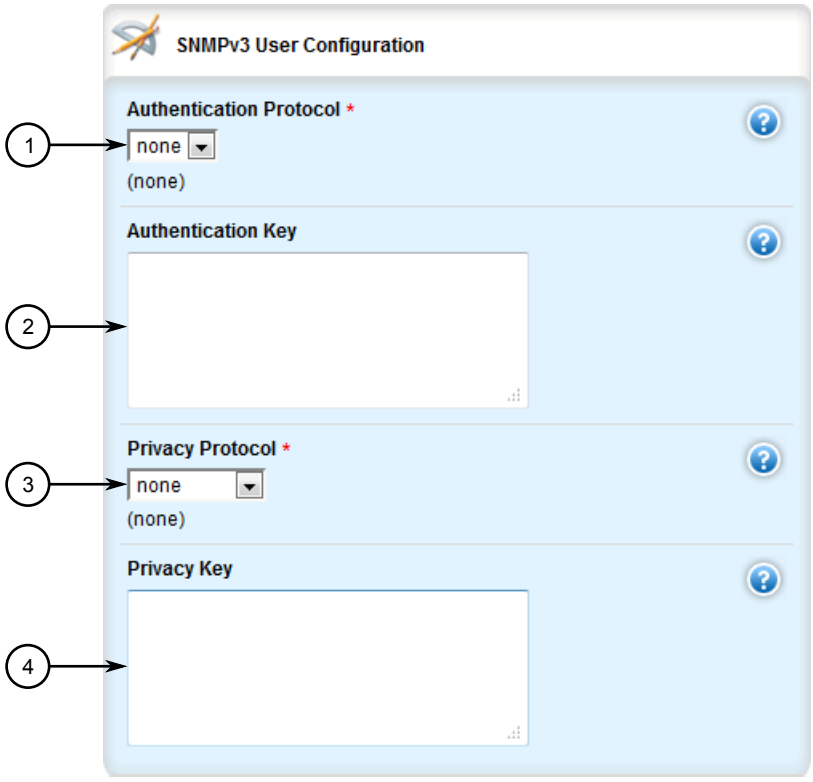


Figure 1073: SNMPv3 User Configuration Form

1. Authentication Protocol List **2.** Authentication Key Box **3.** Privacy Protocol List **4.** Privacy Key Box

CAUTION!
Security hazard – risk of unauthorized access and/or exploitation. Use only strong passwords when configuring SNMP users that consist of at least:

- *One lower case character*
- *One upper case character*
- *One number*
- *One special character (i.e. !@#$%^&*()_+-={}[];:',<.>/?\|`~)*

Avoid weak passwords (e.g. ***password1****,* ***123456789****,* ***abcdefgh****) or repeated characters (e.g.* ***abcabc****).*

5. Configure the following parameter(s) as required:

Parameter	Description
Authentication Protocol	**Synopsis:** { none, md5, sha1 } **Default:** none The authentication protocol providing data integrity and authentication for SNMP exchanges between the user and the SNMP engine.
Authentication Key	**Synopsis:** A string The authentication passphrase. The passphrase must be 8 characters long at minimum.

Parameter	Description
Privacy Protocol	**Synopsis:** { none, des3cbc, aescfb128 } **Default:** none The symmetric privacy protocol providing data encryption and decryption for SNMP exchanges between the user and the SNMP engine.
Privacy Key	**Synopsis:** A string The privacy passphrase. The passphrase must be 8 characters long at minimum.

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 15.2.7.3
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.

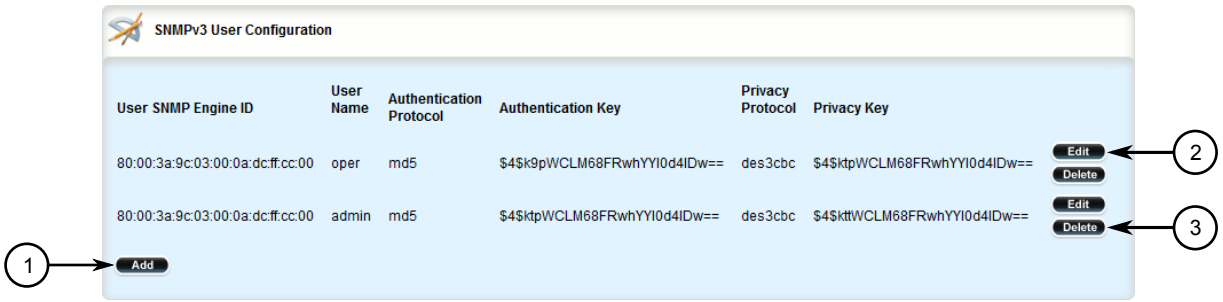


Figure 1074: SNMPv3 User Configuration Table

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 15.2.8
Managing SNMP Security Model Mapping

This section describes how to manage the mapping of SNMP security models.

CONTENTS

Section 15.2.8.1
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.

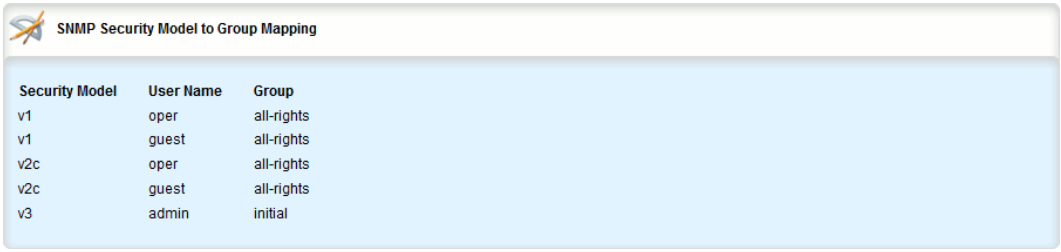


Figure 1075: SNMP Security Model to Group Mapping Table

If no SNMP security models have been configured, add security models as needed. For more information, refer to Section 15.2.8.2, "Adding an SNMP Security Model".

Section 15.2.8.2
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.

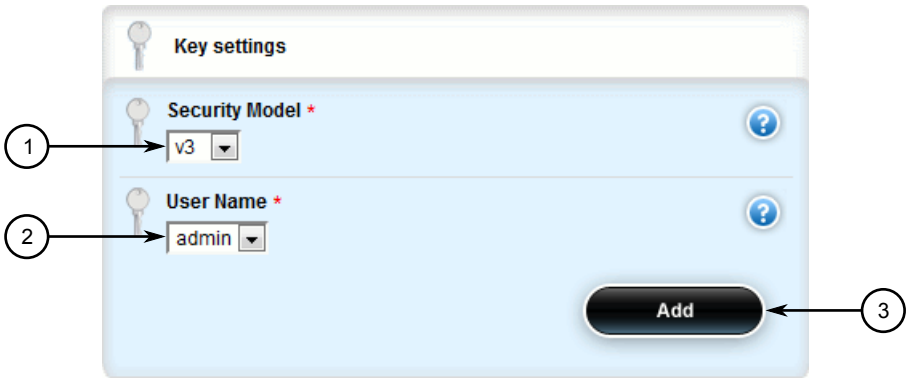


Figure 1076: Key Settings Form

1. Security Model List **2.** User Name List **3.** Add Button

3. Configure the following parameter(s) as required:

Parameter	Description
Security Model	**Synopsis:** { v1, v2c, v3 } The SNMP security model to use: SNMPv1, SNMPv2c, or USM/SNMPv3.
User Name	**Synopsis:** A string 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.

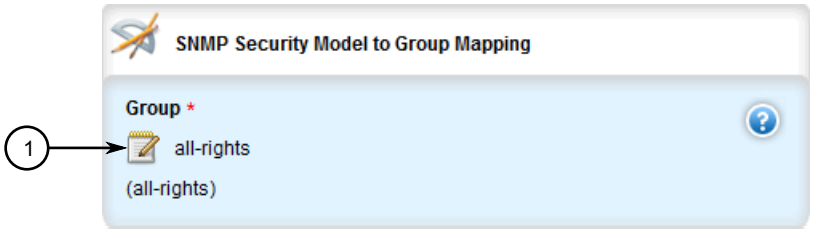


Figure 1077: SNMP Security Model to Group Mapping Form

1. Group Box

5. Configure the following parameter(s) as required:

Parameter	Description
Group	**Synopsis:** A string 1 to 32 characters long **Default:** 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 15.2.8.3

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.

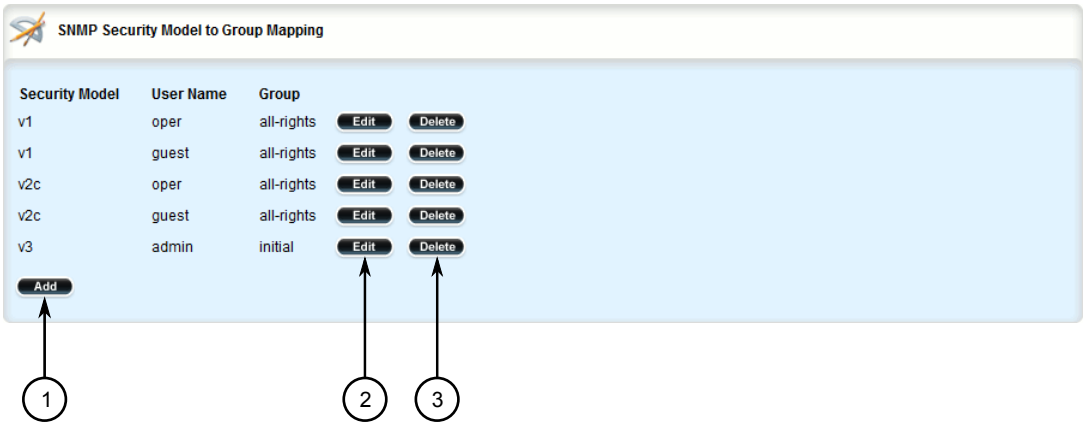


Figure 1078: SNMP Security Model to Group Mapping Table

1. Add Button **2.** Edit Button **3.** Delete Button

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 15.2.9

Managing SNMP Group Access

This section describes how to manage access for SNMP groups.

CONTENTS

Section 15.2.9.1

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.

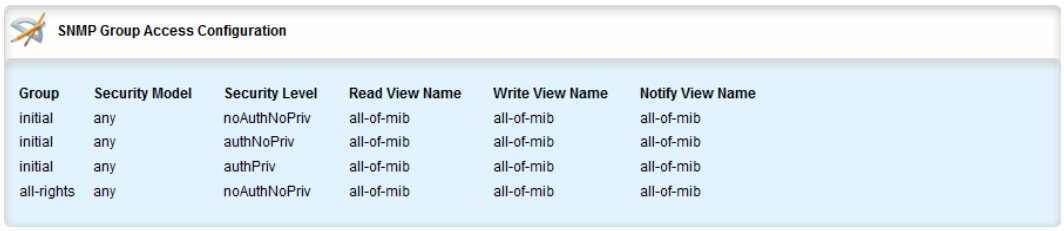


Figure 1079: SNMP Group Access Configuration Table

If no SNMP groups have been configured, add groups as needed. For more information, refer to Section 15.2.9.2, "Adding an SNMP Group".

Section 15.2.9.2
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.

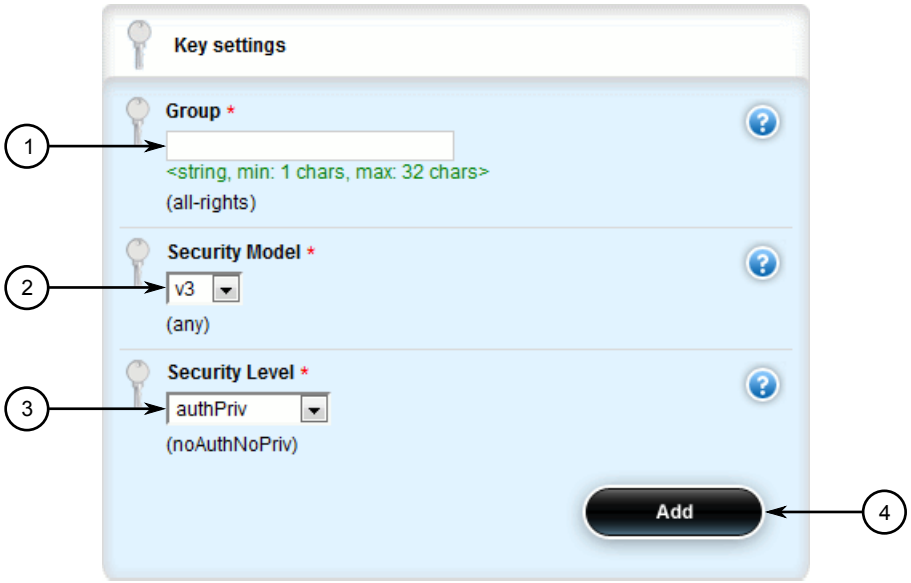


Figure 1080: Key Settings Form

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	**Synopsis:** A string 1 to 32 characters long The name of the SNMP group.
Security Model	**Synopsis:** { any, v1, v2c, v3 }

Parameter	Description
	The SNMP security model to use: SNMPv1, SNMPv2c, or USM/SNMPv3.
Security Level	**Synopsis:** { noAuthNoPriv, authNoPriv, authPriv } The SNMP security level: • authPriv: Communication with authentication and privacy. • authNoPriv: Communication with authentication and without privacy. • noAuthnoPriv: Communication without authentication and privacy.

4. Click **Add** to create the protocol. The **SNMP Group Access Configuration** form appears.

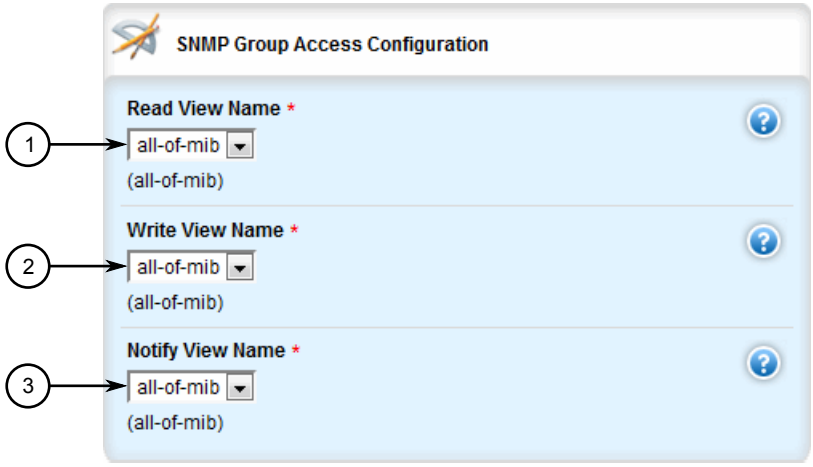


Figure 1081: SNMP Group Access Configuration Form

1. Read View Name List **2.** Write View Name List **3.** Notify View Name List

5. Configure the following parameter(s) as required:

Parameter	Description
Read View Name	**Synopsis:** { no-view, v1-mib, restricted, all-of-mib } **Default:** 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	**Synopsis:** { no-view, v1-mib, restricted, all-of-mib } **Default:** 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	**Synopsis:** { no-view, v1-mib, restricted, all-of-mib } **Default:** 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 15.2.9.3
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.

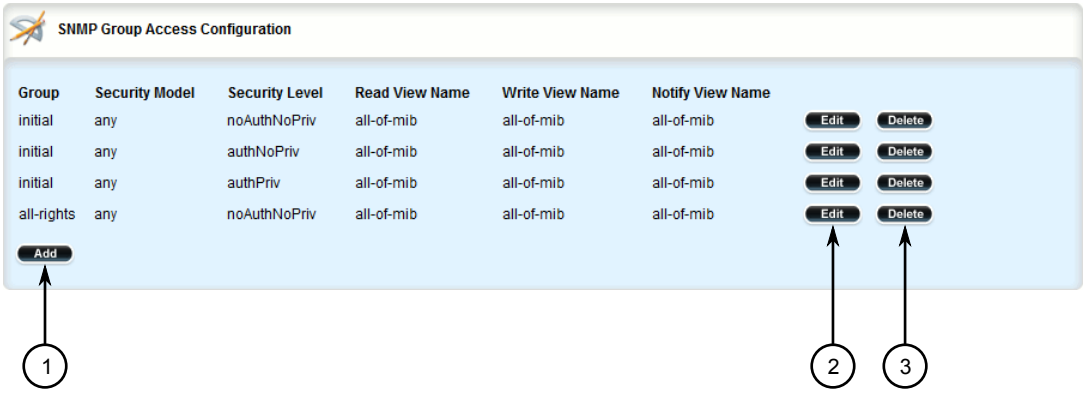


Figure 1082: SNMP Group Access Configuration Table

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 15.3
Managing NETCONF

The Network Configuration Protocol (NETCONF) is a network configuration protocol developed by the Internet Engineering Task Force (IETF). NETCONF provides functions to download, upload, change, and delete the configuration data on network devices. RUGGEDCOM ROX II devices also support the ability to collect data and perform direct actions on the device, such as rebooting the device, clearing statistics, and restarting services.

NOTE
For more information about NETCONF and its use, refer to the NETCONF Reference Guide for RUGGEDCOM ROX II v2.12.

CONTENTS

Section 15.3.1

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.

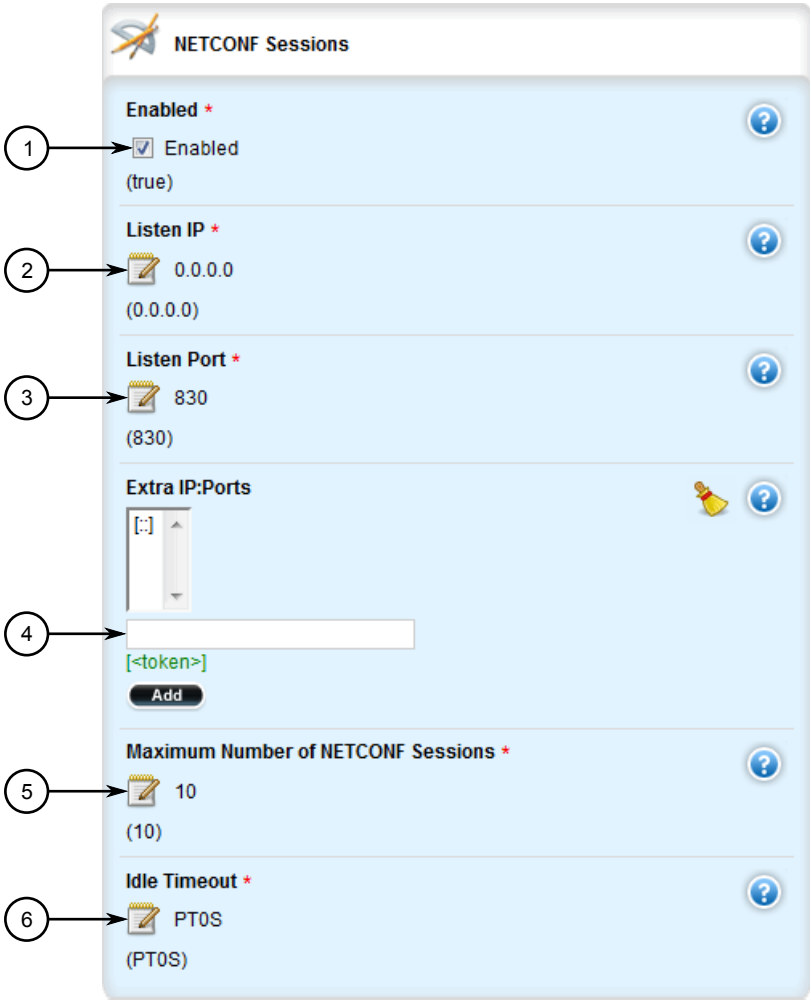


Figure 1083: NETCONF Sessions

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	**Synopsis:** { true, false } **Default:** true Provides the ability to configure NETCONF features on the device.
Listen IP	**Synopsis:** A string **Default:** 0.0.0.0 The IP Address the CLI will listen on for NETCONF requests.
Listen Port	**Synopsis:** A 16-bit unsigned integer between 0 and 65535 **Default:** 830 The port on which NETCONF listens for NETCONF requests.
Extra IP:Ports	**Synopsis:** 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: • nnn.nnn.nnn.nnn:port represents an IPv4 address followed by a colon and port number. For example, 192.168.10.12:19343 • 0.0.0.0 represents the default IPv4 address and default port number. This is the default configuration. • [::]:port represents an IPv6 address followed by a colon and port number. For example, [fe80::5eff:35ff]:16000 • If using the default address, do not specify another listen address with the same port.
Maximum Number of NETCONF Sessions	**Synopsis:** a 32-bit unsigned integer **Default:** 10 The maximum number of concurrent NETCONF sessions.
Idle Timeout	**Synopsis:** A string **Default:** 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.

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. [Optional] Enable the NETCONF summary log (saved under `/var/log/netconf.log`) to record all NETCONF protocol transactions. For more information, refer to Section 4.10.4.3, "Enabling/Disabling the NETCONF Summary Log".
7. [Optional] Enable the NETCONF trace log (saved under `/var/log/netconf-trace.log`) to record the text of each NETCONF XML message received by and sent by the device. For more information, refer to Section 4.10.4.4, "Enabling/Disabling the NETCONF Trace Log".

Section 15.3.2

Viewing NETCONF Statistics

To view NETCONF related statistics, navigate to ***admin » netconf***. The **NETCONF State/Statistics** form appears.

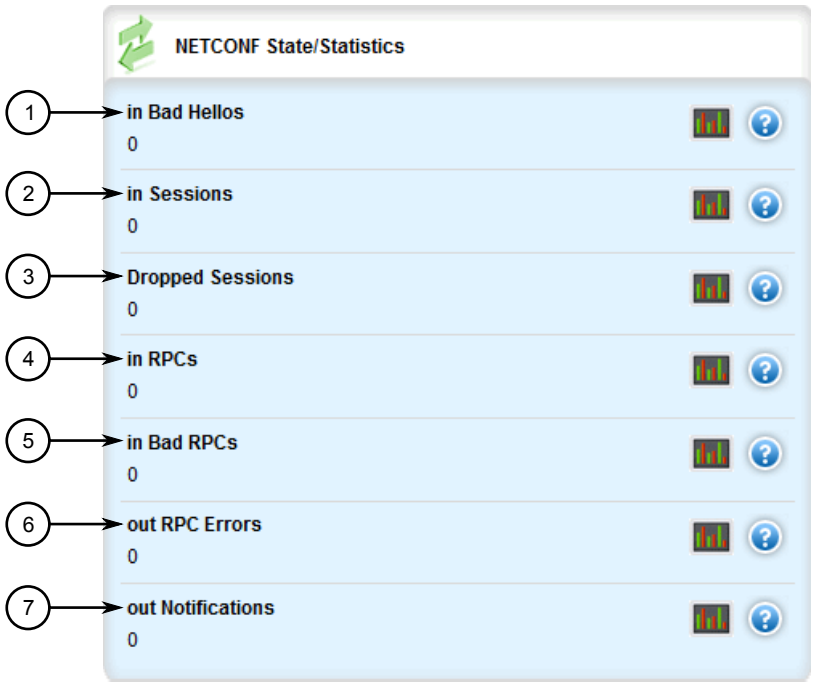


Figure 1084: NETCONF State/StatisticsForm

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	**Synopsis:** A 32-bit unsigned integer 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. This parameter is mandatory.
In Sessions	**Synopsis:** A 32-bit unsigned integer The total number of NETCONF sessions started towards the NETCONF peer. inSessions - inBadHellos = 'The number of correctly started NETCONF sessions.' This parameter is mandatory.
Dropped Sessions	**Synopsis:** A 32-bit unsigned integer The total number of NETCONF sessions dropped. inSessions - inBadHellos = 'The number of correctly started NETCONF sessions.' This parameter is mandatory.
In RPCs	**Synopsis:** A 32-bit unsigned integer The total number of RPC requests received. This parameter is mandatory.

Parameter	Description
In Bad RPCs	**Synopsis:** A 32-bit unsigned integer The total number of RPCs which were parsed correctly, but couldn't be serviced because they contained non-conformant XML. This parameter is mandatory.
Out RPC Errors	**Synopsis:** A 32-bit unsigned integer The total number of 'rpc-reply' messages with 'rpc-error' sent. This parameter is mandatory.
Out Notifications	**Synopsis:** A 32-bit unsigned integer The total number of 'notification' messages sent. This parameter is mandatory.

16 Traffic Control and Classification

Use the traffic control and classification subsystems to control the flow of data packets to connected network interfaces. RUGGEDCOM ROX II also features tools for traffic analysis and characterization.

CONTENTS

Section 16.1

Managing Port Mirroring

Port mirroring is a troubleshooting tool that copies, or mirrors, all traffic received or transmitted on a designated port to another mirror port. If a protocol analyzer were attached to the target port, the traffic stream of valid frames on any source port is made available for analysis.

Select a target port that has a higher speed than the source port. Mirroring a 100 Mbps port onto a 10 Mbps port may result in an improperly mirrored stream.

Frames will be dropped if the full-duplex rate of frames on the source port exceeds the transmission speed of the target port. Since both transmitted and received frames on the source port are mirrored to the target port, frames will be discarded if the sum traffic exceeds the target port’s transmission rate. This problem reaches its extreme in the case where traffic on a 100 Mbps full-duplex port is mirrored onto a 10 Mbps half-duplex port.

Invalid frames received on the source port will not be mirrored. These include CRC errors, oversized and undersized packets, fragments, jabbers, collisions, late collisions and dropped events).

NOTE

Port mirroring has the following limitations:

- *The target port may sometimes incorrectly show the VLAN tagged/untagged format of the mirrored frames.*
- *Network management frames (such as RSTP, GVRP, etc.) may not be mirrored.*
- *Switch management frames generated by the switch (such as Telnet, HTTP, SNMP, etc.) may not be mirrored.*

CONTENTS

- Section 16.1.3, "Managing Ingress Source Ports"

Section 16.1.1
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.

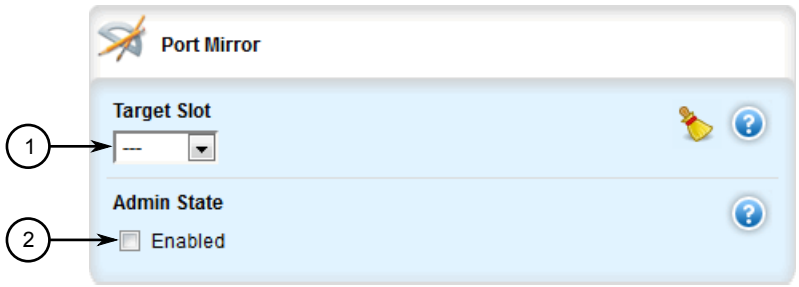


Figure 1085: Port Mirror Form

1. Target Slot List **2.** Admin State Check Box

3. Configure the following parameter(s) as required:

Parameter	Description
Target Slot	**Synopsis:** A string The slot where a monitoring device should be connected.
Target Port	**Synopsis:** A string The port where a monitoring device should be connected.
Admin State	Enabling port mirroring causes all frames received and/or transmitted by the source port to be transmitted out of the target port.

4. Add egress and ingress source ports. For more information, refer to Section 16.1.2.2, "Adding an Egress Source Port" and Section 16.1.3.2, "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 16.1.2
Managing Egress Source Ports

This section describes how to configure and manage egress source ports for port mirroring.

CONTENTS

Section 16.1.2.1
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.

Figure 1086: Egress Source Ports Table

If no egress source ports have been configured, add egress source ports as needed. For more information, refer to Section 16.1.2.2, "Adding an Egress Source Port".

Section 16.1.2.2
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.

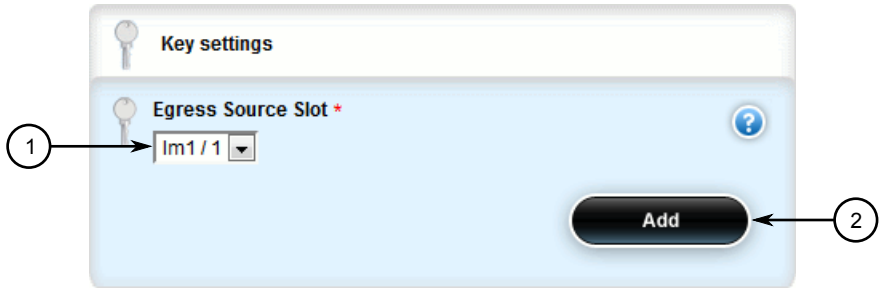


Figure 1087: Key Settings Form

1. Egress Source Slot List **2.** Add Button

3. Configure the following parameter(s) as required:

Parameter	Description
Egress Source Slot	**Synopsis:** A string The name of the module location provided on the silkscreen across the top of the device.
Egress Source Port	**Synopsis:** A string The selected ports on the module installed in the indicated slot.

4. Click **Add** to create the new egress 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 16.1.2.3
Deleting an Egress Source Port

To delete 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***. The **Egress Source Ports** table appears.

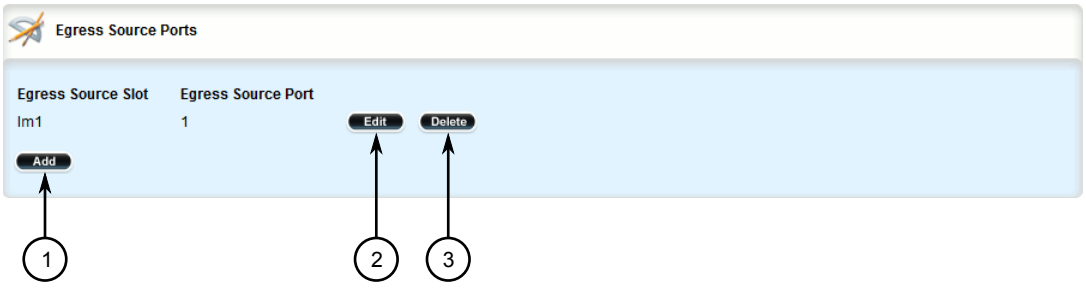


Figure 1088: Egress Source Ports Table

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 16.1.3
Managing Ingress Source Ports

This section describes how to configure and manage egress source ports for port mirroring.

CONTENTS

Section 16.1.3.1
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.

Figure 1089: Ingress Source Ports Table

If no ingress source ports have been configured, add ingress source ports as needed. For more information, refer to Section 16.1.3.2, "Adding an Ingress Source Port".

Section 16.1.3.2
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.

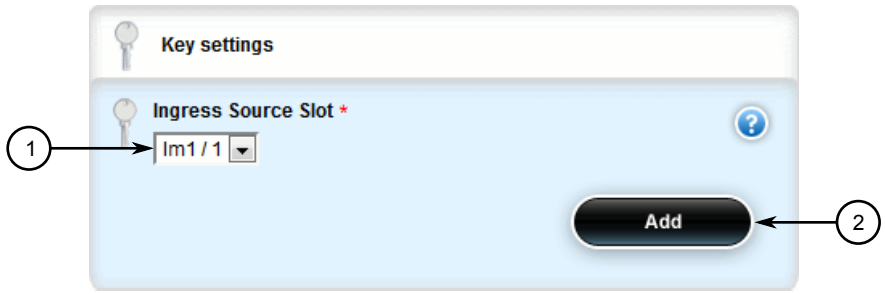


Figure 1090: Key Settings Form

1. Ingress Source Slot List **2.** Add Button

3. Configure the following parameter(s) as required:

Parameter	Description
Ingress Source Slot	**Synopsis:** A string The name of the module location provided on the silkscreen across the top of the device.
Ingress Source Port	**Synopsis:** A string The selected ports on the module installed in the indicated slot.

4. Click **Add** to create the new 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 16.1.3.3

Deleting an Ingress Source Port

To delete 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***. The **Ingress Source Ports** table appears.

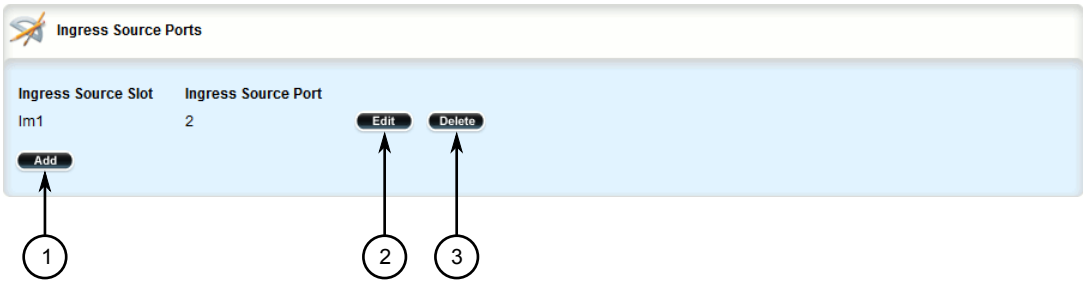


Figure 1091: Ingress Source Ports Table

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 16.2
Managing Traffic Control

Traffic control is a firewall subsystem that manages the amount of bandwidth for each network interface that different types of traffic are permitted to use. For a traffic control configuration to work, a firewall must be configured.

NOTE
For more information about firewalls, refer to Section 6.8, "Managing Firewalls".

RUGGEDCOM ROX II allows up to four different firewall configurations, enabling users to quickly change between configurations. Users can quickly assess different configurations without needing to save and reload any part of the configuration. In contrast, there is only one traffic control configuration.

When enabled, a traffic control configuration is used with the current firewall configuration. A current firewall configuration is defined as one that is specified in either work-config and/or active-config. It does not have to be enabled to be validated.

NOTE
Traffic control is not available for Ethernet traffic on any line module when Layer 3 hardware acceleration is enabled. It is intended to be used only on WAN interfaces.

CONTENTS

Section 16.2.1
Enabling and Configuring Traffic Control

Traffic control functions are divided into two modes:

- **Basic Mode**
  Basic mode offers a limited set of options and parameters. Use this mode to set the outgoing bandwidth for an interface, the interface priority (high, medium or low), and some simple traffic control characteristics. Basic traffic shaping affects traffic identified by protocol, port number, address and interface. Note that some of these options are mutually exclusive. Refer to the information given for each option.

  In basic mode, a packet is categorized based on the contents of its Type of Service (ToS) field if it does not match any of the defined classes.

- **Advanced Mode**
  In advanced mode, each interface to be managed is assigned a total bandwidth for incoming and outgoing traffic. Classes are then defined for each interface, each with its own minimum assured bandwidth and a maximum permitted bandwidth. The combined minimum of the classes on an interface must be no more than the total outbound bandwidth specified for the interface. Each class is also assigned a priority, and any bandwidth left over after each class has received its minimum allocation (if needed) will be allocated to the lowest priority class up until it reaches its maximum bandwidth, after which the next priority is allocated more bandwidth. When the specified total bandwidth for the interface is reached, no further packets are sent, and any further packets may be dropped if the interface queues are full.

  Packets are assigned to classes on the outbound interface based on either a mark assigned to the packet, or the Type of Service (ToS) field in the IP header. If the ToS field matches a defined class, the packet is allocated to that class. Otherwise, it is allocated to any class that matches the mark assigned to the packet. If no class matches the mark, the packet is assigned to the default class.

  Marks are assigned to packets by traffic control rules that are based on a number of parameters, such as IP address, port number, protocol, packet length, and more.

The two modes cannot be accessed simultaneously. Only the mode that is currently configured can be accessed.

To enable and configure traffic control, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to ***qos » traffic-control***. The **Traffic Control Configuration** form appears.

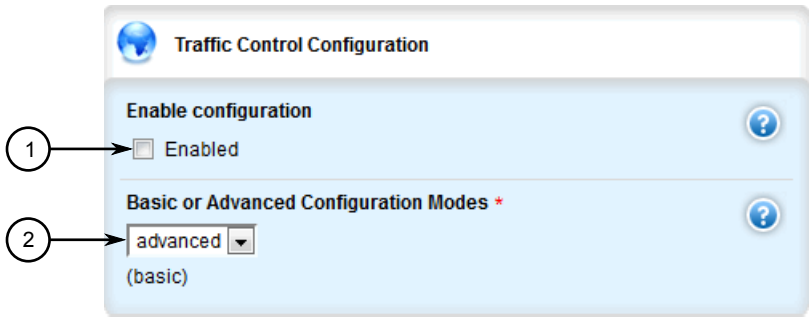


Figure 1092: Traffic Control Configuration Form

1. Enable Configuration Box **2.** Basic or Advanced Configuration Modes List

3. Configure the following parameter(s) as required:

Parameter	Description
Enable configuration	Enables/disables traffic control (TC) for the current firewall configuration. The current firewall configuration is the one that is committed. When an active configuration is committed to the system, then an **enabled** TC configuration will be included. When a work configuration is committed, the **enabled** TC configuration will be included in the work configuration. **A TC configuration needs a firewall configuration to operate**.

Parameter	Description
Basic or Advanced Configuration Modes	**Synopsis:** { basic, advanced } **Default:** basic 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 16.2.2.2, "Adding a Traffic Control Interface".
   b. Add traffic control priorities. For more information, refer to Section 16.2.3.2, "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 16.2.4.2, "Adding a Traffic Control Class".
   b. Add traffic control devices. For more information, refer to Section 16.2.5.2, "Adding a Traffic Control Device".
   c. Add traffic control rules. For more information, refer to Section 16.2.6.2, "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 16.2.2
Managing Traffic Control Interfaces

Traffic control interfaces define interfaces used for traffic shaping, mainly for outbound bandwidth and the outgoing device.

NOTE
Traffic control interfaces can only be configured in basic mode. For more information about setting the traffic control mode, refer to Section 16.2.1, "Enabling and Configuring Traffic Control".

CONTENTS

Section 16.2.2.1
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.

Figure 1093: Basic Traffic Control Interfaces Table

If no interfaces have been configured, add interfaces as needed. For more information, refer to Section 16.2.2.2, "Adding a Traffic Control Interface".

Section 16.2.2.2
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.

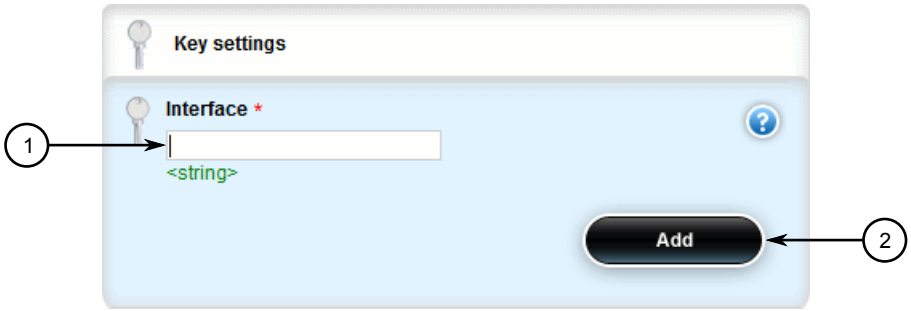


Figure 1094: Key Settings Form

1. Interface Box **2.** Add Button

3. Configure the following parameter(s) as required:

Parameter	Description
interface	**Synopsis:** 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 interface. The **Interface to Apply Traffic Control** form appears.

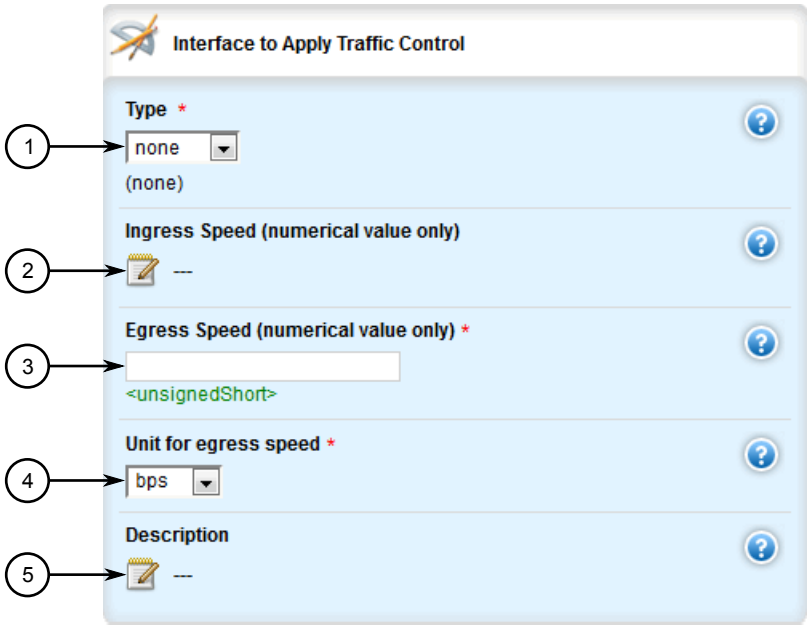


Figure 1095: Interface to Apply Traffic Control Form

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	**Synopsis:** { ipv4, ipv6, ipv4ipv6 } **Default:** ipv4 Internet protocol type - use both when no addresses are used, otherwise define IPv4 and IPv6 rules for each type of addresses used.
Type	**Synopsis:** { internal, external, none } **Default:** none (optional) 'external' (facing toward the Internet) or 'internal' (facing toward a local network). 'external' causes the traffic generated by each unique source IP address to be treated as a single flow. 'internal' causes the traffic generated by each unique destination IP address to be treated as a single flow. Internal interfaces seldom benefit from simple traffic shaping.
Ingress Speed (numerical value only)	**Synopsis:** A 16-bit unsigned integer (optional) The incoming bandwidth of this interface. If incoming traffic exceeds the given rate, received packets are dropped randomly. When unspecified, maximum speed is assumed. Specify only the number here. The unit (kilobits, megabits) is specified in the in-unit.
Unit for Ingress Speed	**Synopsis:** { none, kilobits, megabits } **Default:** none The unit for inbandwidth, per second.
Egress Speed (numerical value only)	**Synopsis:** A 16-bit unsigned integer The outgoing bandwidth for this interface. Specify only the number here. The unit (kilobits, megabits) is specified in the out-unit. This parameter is mandatory.

Parameter	Description
Unit for Egress Speed	**Synopsis:** { kilobits, megabits } **Default:** megabits The unit for outgoing bandwidth, per second.
Description	**Synopsis:** A string 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 16.2.2.3
Deleting a Traffic Control Interface

To delete a 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***. The **Basic Traffic Control Interfaces** table appears.

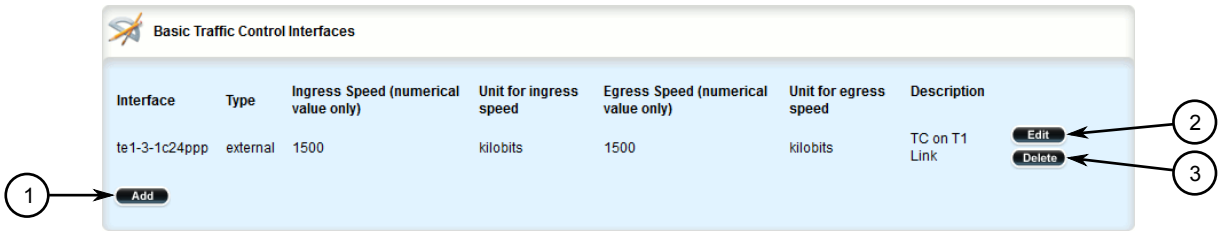


Figure 1096: Basic Traffic Control Interfaces Table

1. Add Button **2.** Edit Button **3.** Delete Button

3. Click **Delete** next to the chosen traffic control 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 16.2.3
Managing Traffic Control Priorities

Traffic control priorities define priorities used for traffic shaping.

NOTE
Traffic control priorities can only be configured in basic mode. For more information about setting the traffic control mode, refer to Section 16.2.1, "Enabling and Configuring Traffic Control".

CONTENTS

Section 16.2.3.1
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.

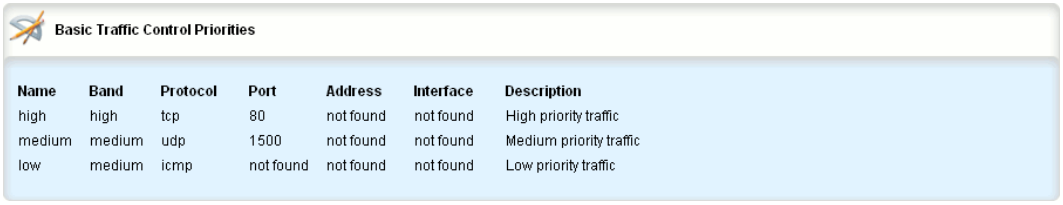


Figure 1097: Basic Traffic Control Priorities Table

If no priorities have been configured, add priorities as needed. For more information, refer to Section 16.2.3.2, "Adding a Traffic Control Priority".

Section 16.2.3.2
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.

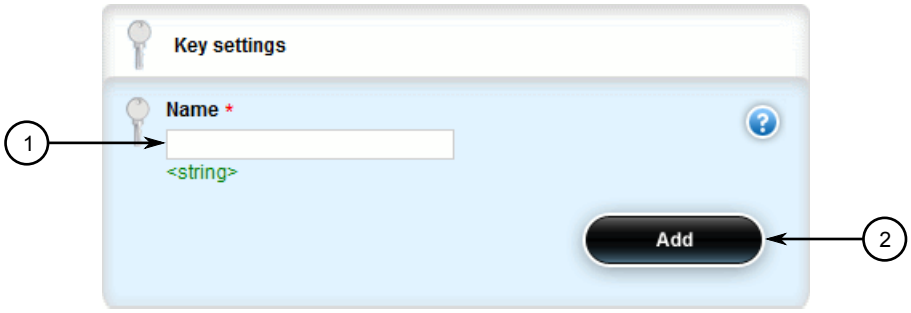


Figure 1098: Key Settings Form

1. Name Box **2.** Add Button

3. Configure the following parameter(s) as required:

Parameter	Description
name	**Synopsis:** A string A distinct name for this configuration entry. This parameter is mandatory.

4. Click **Add** to create the new traffic control priority. The **Basic Traffic Control Priorities** form appears.

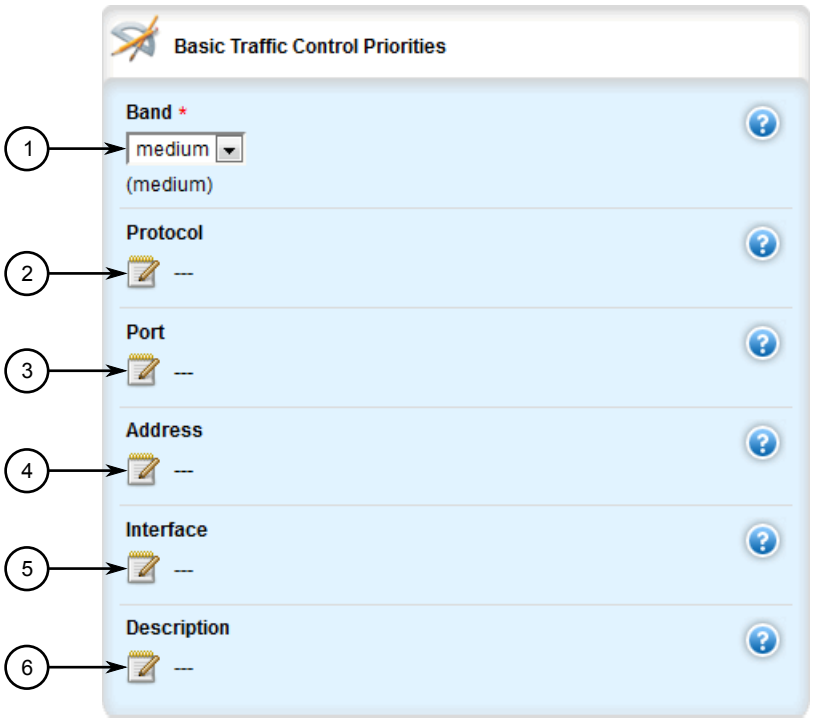


Figure 1099: Basic Traffic Control Priorities Form

1. Band List **2.** Protocol Box **3.** Port Box **4.** Address Box **5.** Interface Box **6.** Description Box

5. Configure the following parameter(s) as required:

Parameter	Description
iptype	**Synopsis:** { ipv4, ipv6, ipv4ipv6 } **Default:** ipv4 Internet protocol type - use both when no addresses are used, otherwise define IPv4 and IPv6 rules for each type of addresses used.
band	**Synopsis:** { high, medium, low } **Default:** medium Priority (band) : high, medium, low... **High band includes:** Minimize Delay (md) (0x10), md + Minimize Monetary Cost (mmc) (0x12), md + Maximize Reliability (mr) (0x14), mmc+md+mr (0x16). **Medium band includes:** Normal Service (0x0), mr (0x04), mmc +mr (0x06), md + Maximize Throughput (mt) (0x18), mmc+mt+md (0x1a), mr+mt+md (0x1c), mmc+mr+mt+md (0x1e). **Low band includes:** mmc (0x02), mt (0x08), mmc+mt (0x0a), mr+mt (0x0c), mmc+mr+mt (0x0e).
protocol	**Synopsis:** { tcp, udp, icmp, all } or a string (choice) A targeted protocol.
port	**Synopsis:** A string (choice) Source port - can be specified **only if** protocol is TCP, UDP, DCCP, SCTP or UDPlite
address	**Synopsis:** A string (choice) The source address. This can be specified **only if** the protocol, port and interface are not defined.
interface	**Synopsis:** A string 1 to 15 characters long (choice) The source interface. This can be specified **only if** the protocol, port and address are not defined. Lowercase alphanumerical as well as '.' and '-' characters are allowed.
description	**Synopsis:** A string (optional) A description for this 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 16.2.3.3
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.

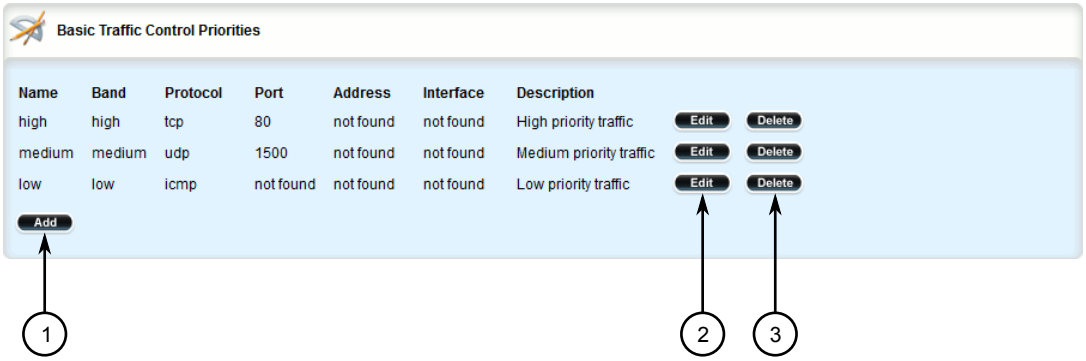


Figure 1100: Basic Traffic Control Priorities Table

1. Add Button **2.** Edit Button **3.** Delete Button

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 16.2.4

Managing Traffic Control Classes

Traffic control classes define classes for traffic shaping. Optionally, they can also define parameters for Type of Service (ToS), which is an eight-bit field in the IPv4 header. Traffic control can inspect the ToS value of an incoming IP frame and classify traffic to provide preferential service in the outgoing queue. Traffic classification is done based on the ToS value and the ToS options defined for each traffic control class and traffic control rule. IP Traffic matching with the ToS options takes precedence over the mark rules.

NOTE
One traffic control class must be added for each network interface.

NOTE
Type of Service (ToS) is defined by the Internet Engineering Task Force (IETF). For more information about ToS, refer to RFC 1349 [http://tools.ietf.org/html/rfc1349].

CONTENTS

Section 16.2.4.1
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.

Figure 1101: Advanced Traffic Control Classes Table

If no classes have been configured, add classes as needed. For more information, refer to Section 16.2.4.2, "Adding a Traffic Control Class".

Section 16.2.4.2
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.

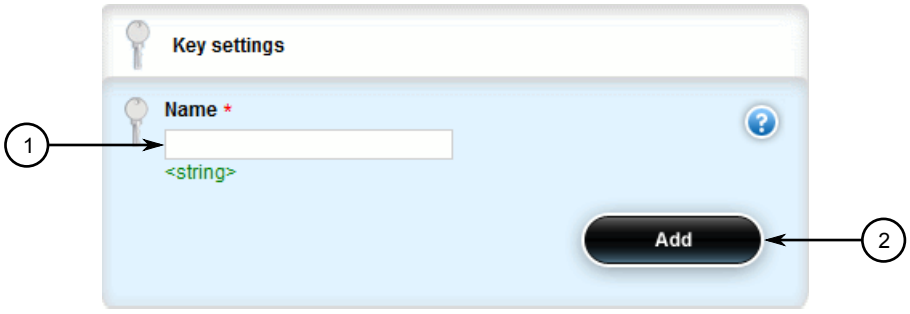


Figure 1102: Key Settings Form

1. Name Box **2.** Add Button

3. Configure the following parameter(s) as required:

Parameter	Description
name	**Synopsis:** A string The name for this TC class entry. This parameter is mandatory.

4. Click **Add** to create the new class. The **Class Options** and **Advanced Traffic Control Classes** forms appear.

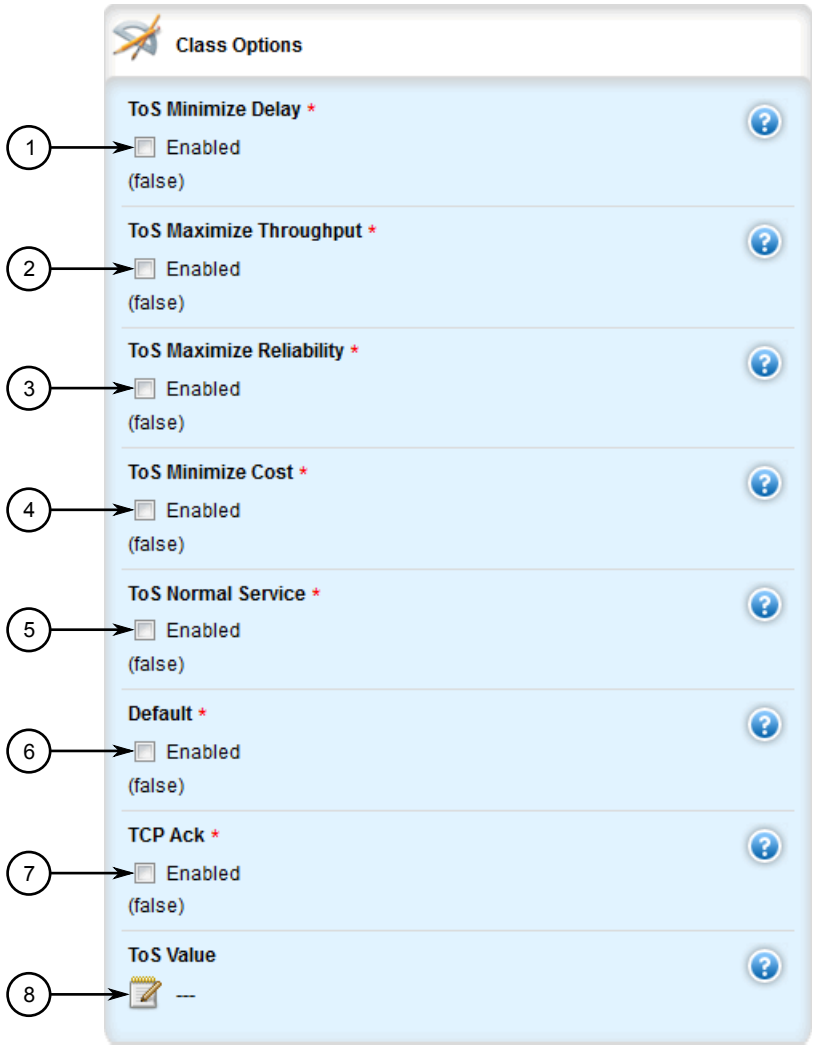


Figure 1103: Class Options Form

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

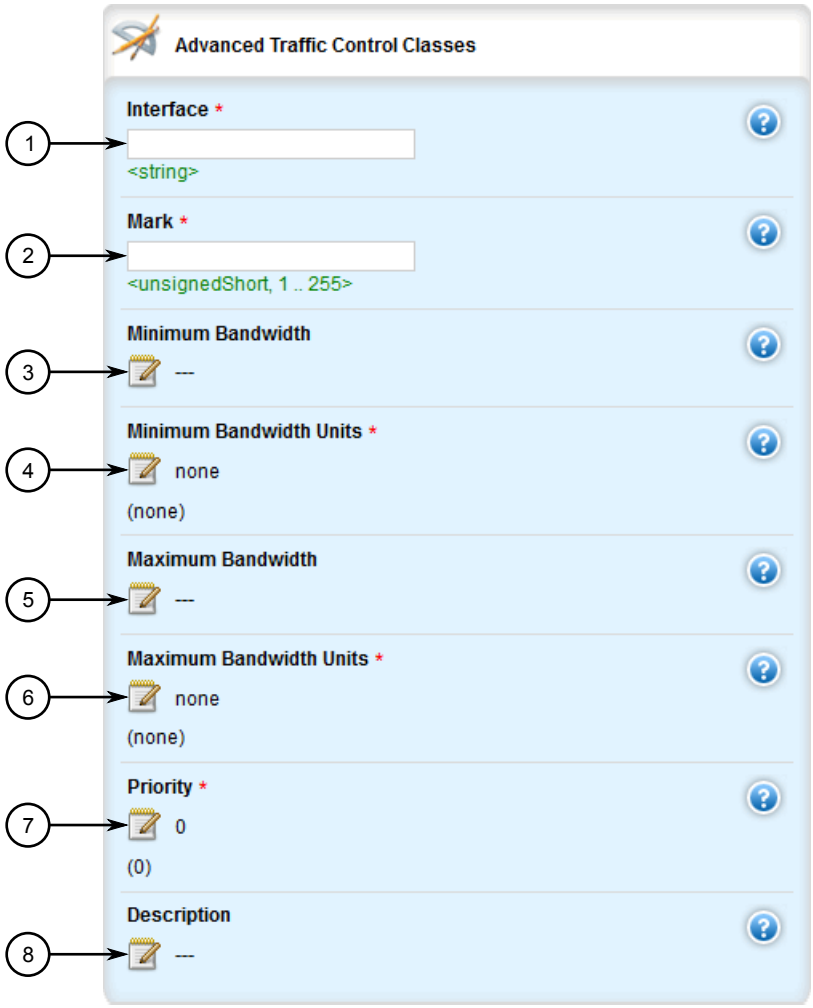


Figure 1104: Advanced Traffic Control Classes Form

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	**Synopsis:** { true, false } **Default:** false Value/mask encoding: 0x10/0x10
ToS Maximize Throughput	**Synopsis:** { true, false } **Default:** false Value/mask encoding: 0x08/0x08
ToS Maximize Reliability	**Synopsis:** { true, false } **Default:** false Value/mask encoding: 0x04/0x04
ToS Minimize Cost	**Synopsis:** { true, false }

Parameter	Description
	Default: false Value/mask encoding: 0x02/0x02
ToS Normal Service	**Synopsis:** { true, false } **Default:** false Value/mask encoding: 0x00/0x1e
default	**Synopsis:** { true, false } **Default:** false **One default class** per interface **must** be defined.
TCP ACK	**Synopsis:** { true, false } **Default:** false All TCP ACK packets into this class. This option should be specified only once per interface.
ToS Value	**Synopsis:** 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	**Synopsis:** { ipv4, ipv6, ipv4ipv6 } **Default:** ipv4 Internet protocol type - use both when no addresses are used, otherwise define IPv4 and IPv6 rules for each type of addresses used.
interface	**Synopsis:** A string The interface to which this class applies. Each interface must be listed only once. Lowercase alphanumerical as well as '.' and '-' characters are allowed. This parameter is mandatory.
mark	**Synopsis:** A 16-bit unsigned integer between 1 and 255 A mark that identifies traffic belonging to this class. This is a unique integer between 1-255. Each class must have its own unique mark. This parameter is mandatory.
Minimum Bandwidth	**Synopsis:** A string The minimum bandwidth this class should have when the traffic load rises. This can be either a numeric value or a calculated expression based on the bandwidth of the interface. A fixed numerical value must only be a number - its unit is specified in Minbw-unit. A calculated expression is based on a fraction of the 'full' bandwidth, such as: • 'full/3' for a third of the bandwidth and • 'full*9/10' for nine tenths of the bandwidth. In such a case, do not specify any minbw-unit. This parameter is mandatory.
Minimum Bandwidth Units	**Synopsis:** { none, kilobits, megabits } **Default:** none (per second) Only if the minimum bandwidth is a single numerical value
Maximum Bandwidth	**Synopsis:** A string The maximum bandwidth this class is allowed to use when the link is idle. This can be either a numeric value or a calculated expression based on the bandwidth of the

Parameter	Description
	interface. A fixed numerical value must only be a number - its unit is specified in Maxbw-unit. A calculated expression is based on a fraction of the 'full' bandwidth, such as: • 'full/3' for a third of the bandwidth and • 'full*9/10' for nine tenths of the bandwidth. In such a case, do not specify any maxbw-unit. This parameter is mandatory.
Maximum Bandwidth Units	**Synopsis:** { none, kilobits, megabits } **Default:** none (per second) only if max-bandwidth is a **single numerical value**
priority	**Synopsis:** A 16-bit unsigned integer between 0 and 7 **Default:** 0 The priority in which classes will be serviced. Higher priority classes will experience less delay since they are serviced first. Priority values are serviced in ascending order (e.g. 0 is higher priority than 1. Minimum: 7).
description	**Synopsis:** A string A description for this configuration item.

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 16.2.4.3
Deleting a Traffic Control Class

To delete a 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***. The **Advanced Traffic Control Classes** table appears.

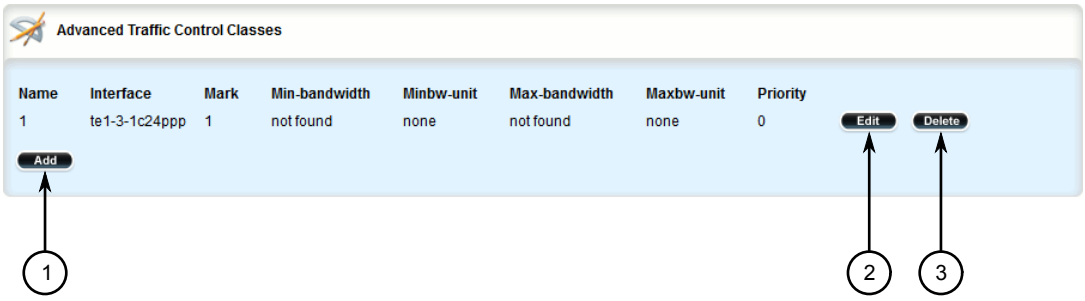


Figure 1105: Advanced Traffic Control Classes Table

1. Add Button **2.** Edit Button **3.** Delete Button

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 16.2.5
Managing Traffic Control Devices

Traffic control devices define devices used for traffic shaping.

NOTE
Traffic control devices can only be configured in advanced mode. For more information about setting the traffic control mode, refer to Section 16.2.1, "Enabling and Configuring Traffic Control".

CONTENTS

Section 16.2.5.1
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.

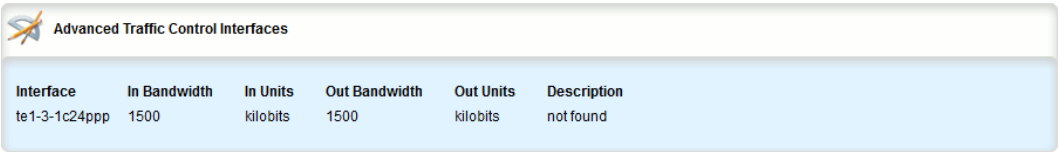


Figure 1106: Advanced Traffic Control Interfaces Table

If no devices have been configured, add devices as needed. For more information, refer to Section 16.2.5.2, "Adding a Traffic Control Device".

Section 16.2.5.2
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.

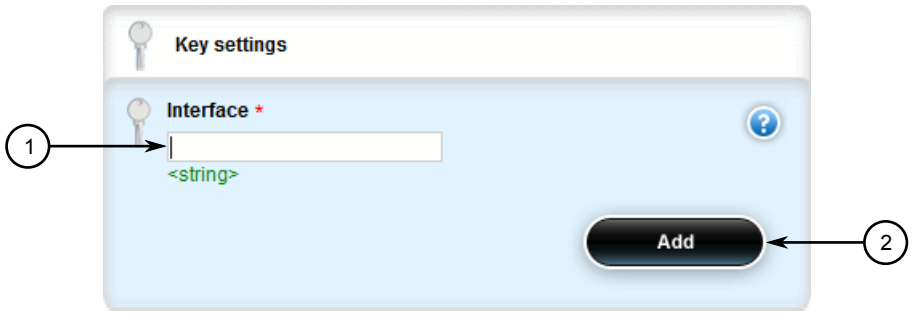


Figure 1107: Key Settings Form

1. Interface Box **2.** Add Button

3. Configure the following parameter(s) as required:

Parameter	Description
interface	**Synopsis:** 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.

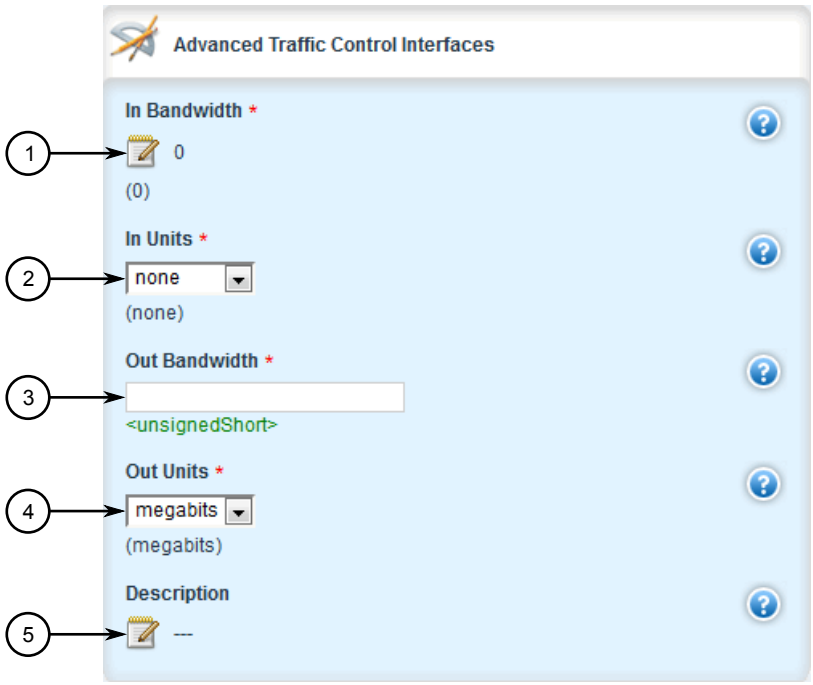


Figure 1108: Advanced Traffic Control Interfaces Form

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	**Synopsis:** { ipv4, ipv6, ipv4ipv6 } **Default:** ipv4 Internet protocol type - use both when no addresses are used, otherwise define IPv4 and IPv6 rules for each type of addresses used.
In Bandwidth	**Synopsis:** A 16-bit unsigned integer **Default:** 0 Incoming bandwidth. Default: 0 = ignore ingress. Defines the maximum traffic allowed for this interface in total. If the rate is exceeded, the packets are dropped.
In Units	**Synopsis:** { none, kilobits, megabits } **Default:** none Unit for inbandwidth, per second.
Out Bandwidth	**Synopsis:** A 16-bit unsigned integer Maximum outgoing bandwidth... This is the maximum speed that can be handled. Additional packets will be dropped. This is the bandwidth that can be refrred-to as 'full' when defining classes. This parameter is mandatory.
Out Units	**Synopsis:** { kilobits, megabits } **Default:** megabits Unit for outgoing bandwidth, per second.
description	**Synopsis:** A string 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 16.2.5.3
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.

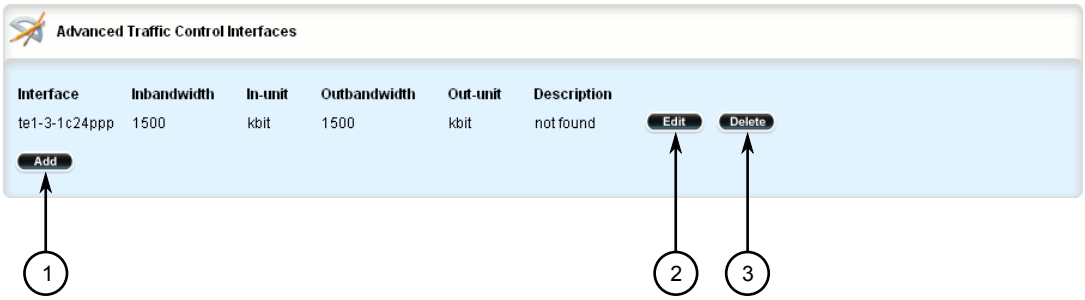


Figure 1109: Advanced Traffic Control Interfaces Table

1. Add Button **2.** Edit Button **3.** Delete Button

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 16.2.6

Managing Traffic Control Rules

Traffic control rules define rules for packet marking.

NOTE
Traffic control rules can only be configured in advanced mode. For more information about setting the traffic control mode, refer to Section 16.2.1, "Enabling and Configuring Traffic Control".

CONTENTS

Section 16.2.6.1

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.

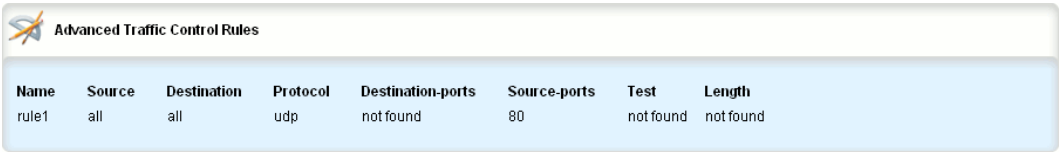


Figure 1110: Advanced Traffic Control Rules Table

If no rules have been configured, add rules as needed. For more information, refer to Section 16.2.6.2, "Adding a Traffic Control Rule".

Section 16.2.6.2

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.

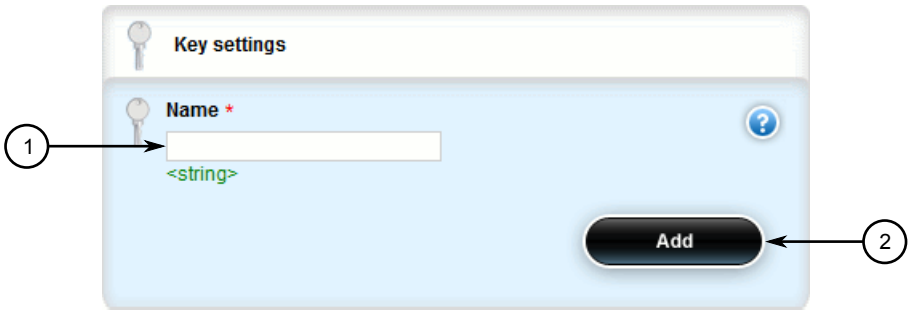


Figure 1111: Key Settings Form

1. Name Box **2.** Add Button

3. Configure the following parameter(s) as required:

Parameter	Description
name	**Synopsis:** A string A distinct name for this rule.

4. Click **Add** to create the new traffic control rule. The **Advanced Traffic Control Rules** form appears.

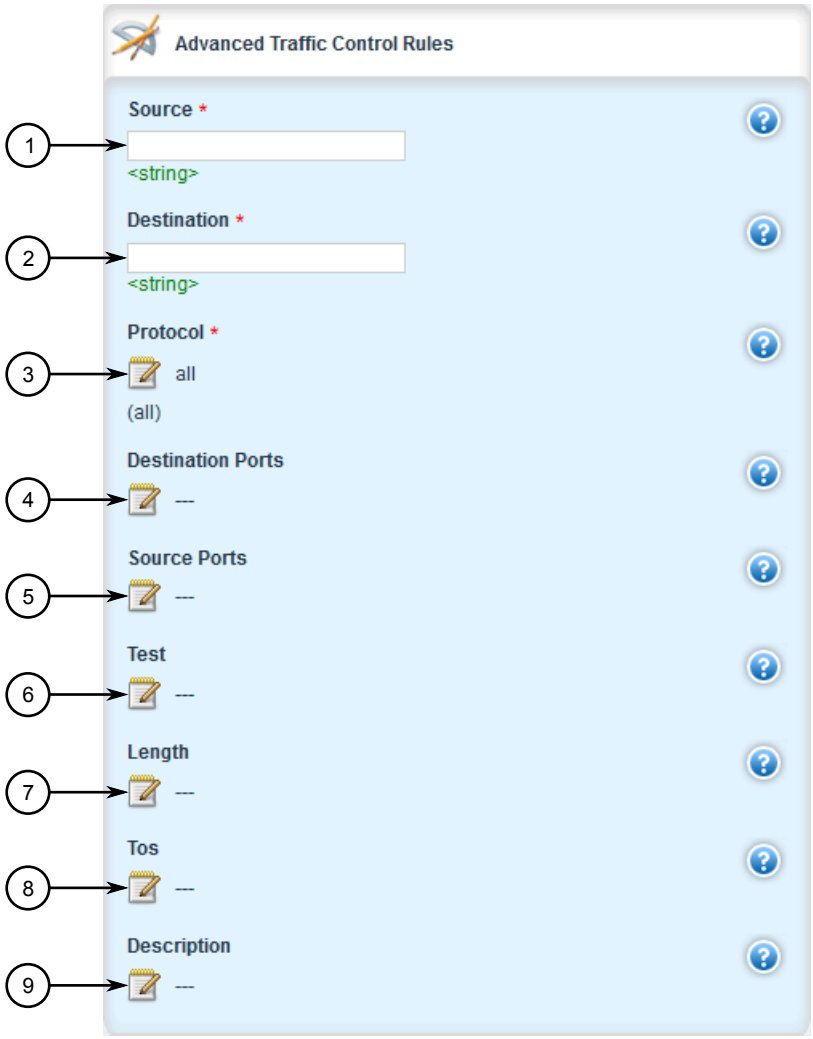


Figure 1112: Advanced Traffic Control Rules Form

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	**Synopsis:** { ipv4, ipv6, ipv4ipv6 } **Default:** ipv4 Internet protocol type - use both when no addresses are used, otherwise define IPv4 and IPv6 rules for each type of addresses used.
source	**Synopsis:** A string IF name, comma-separated list of hosts or IPs, MAC addresses, or 'all'. When using MAC addresses, use '~' as prefix and '-' as separator. Ex.: ~00-1a-6b-4a-72-34,~00-1a-6b-4a-71-42 This parameter is mandatory.
destination	**Synopsis:** A string

Parameter	Description
	IF name, comma-separated list of hosts or IPs, or 'all'. This parameter is mandatory.
protocol	**Synopsis:** { tcp, udp, icmp, all } or a string **Default:** all The protocol to match.
Destination Ports	**Synopsis:** A string (Optional) A comma-separated list of port names, port numbers or port ranges.
Source Ports	**Synopsis:** A string (Optional) A comma- separated list of port names, port numbers or port ranges.
test	**Synopsis:** A string (Optional) Defines a test on the existing packet or connection mark. The default is a packet mark. For testing a connection mark, add ':C' at the end of the test value. Ex.: Test if the packet mark is not zero: **!0** Test if the connection mark is not zero: **!0:C**
length	**Synopsis:** A string (Optional) Matches the length of a packet against a specific value or range of values... Greater than and lesser than, as well as ranges are supported in the form of min:max. Ex.: Equal to 64 **64** Greater or equal to 65 **65:** Lesser or equal to 65 **:65** In-between 64 and 768 **64:768**
tos	**Synopsis:** { minimize-delay, maximize-throughput, maximize-reliability, minimize-cost, normal-service } or a string (Optional) Type of Service . A pre-defined ToS value or a numerical value. The numerical value is hexadecimal. Ex.: 0x38
description	**Synopsis:** A string A description for this configuration item.

NOTE
Only one QoS mark is allowed for each traffic control rule.

6. Configure the rules for a QoS mark. For more information, refer to Section 16.2.6.3, "Configuring QoS Marking".
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 16.2.6.3
Configuring QoS Marking

Quality of Service (QoS) marking applies a mark to important data packets that should receive preferential treatment as they travel through the network. Only one QoS mark is allowed for each traffic control rule. Options include:

- **Set:** Determines whether the packet or the connection is assigned the QoS mark.
- **Modify:** Changes the QoS mark value using an AND or OR argument.
- **Save/Restore:** Replaces the connection's QoS mark value with an assigned value.
- **Continue:** If the packet matches, no more traffic control rules are checked and the packet is automatically forwarded to the specified chain.
- **DSCP Marking:** Determines whether the packet is assigned the DSCP mark.

To configure the QoS mark for a traffic control rule, do the following:

Configuring a Set Mark

1. 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.

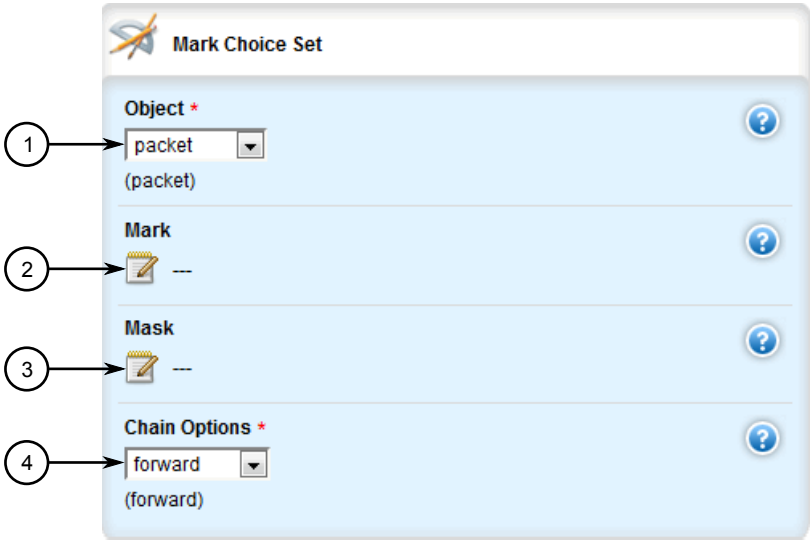


Figure 1113: Mark Choice Set Form

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	**Synopsis:** { packet, connection } **Default:** packet Sets the mark on either a packet or a connection.
mark	**Synopsis:** A string A mark that corresponds to a class mark (decimal value).
mask	**Synopsis:** A string (optional) A mask to determine which mark bits will be set.
Chain Options	**Synopsis:** { forward, postrouting, prerouting } **Default:** 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.

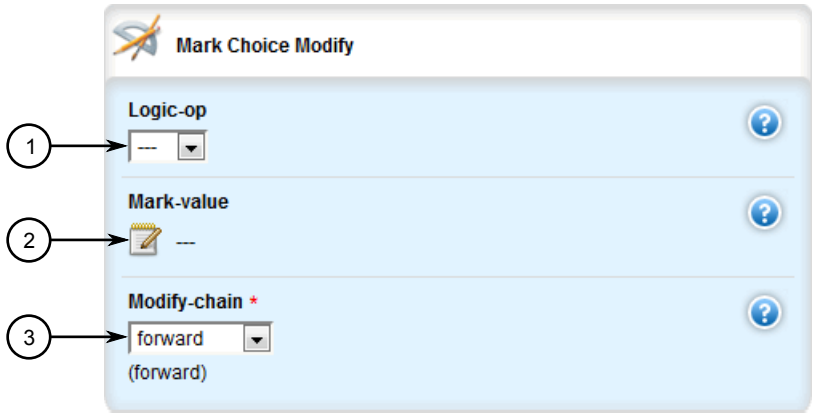


Figure 1114: Mark Choice Modify Form

1. Logic Operation List **2.** Mark Value Box **3.** Modify Chain List

2. Configure the following parameter(s) as required:

Parameter	Description
Logic Options	**Synopsis:** { and, or } A logical operation to perform on the current mark: AND/OR.
Mark Value	**Synopsis:** A string A mark to perform the operation with (decimal value).
Modify Chain	**Synopsis:** { forward, postrouting, prerouting }

Parameter	Description
	Default: 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.

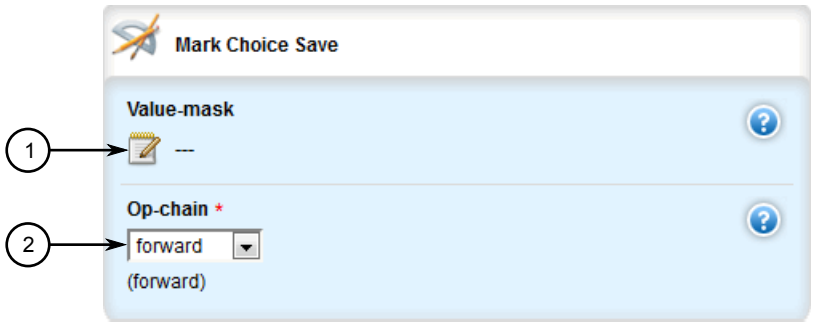


Figure 1115: Mark Choice Save Form

1. Value Mask Box **2.** Operation Chain List

2. Configure the following parameter(s) as required:

Parameter	Description
Value Mask	**Synopsis:** A string Mask to process the mark with
Option Chain	**Synopsis:** { forward, prerouting } **Default:** 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.

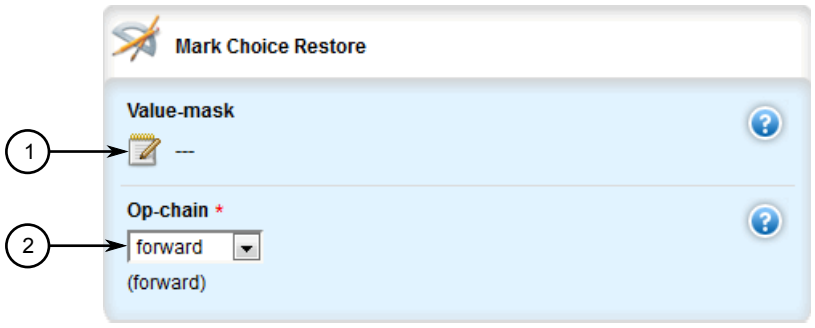


Figure 1116: Mark Choice Restore Form

1. Value Mask Box **2.** Operation Chain List

2. Configure the following parameter(s) as required:

Parameter	Description
Value Mask	**Synopsis:** A string A mask to process the mark with.
Option Chain	**Synopsis:** { forward, prerouting } **Default:** 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.

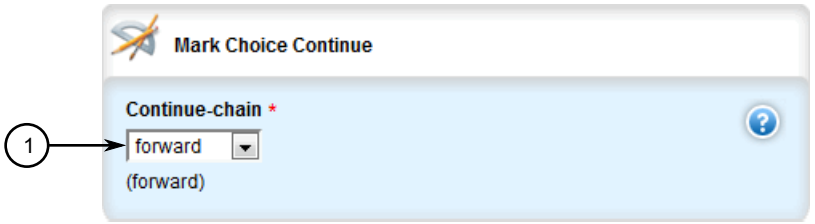


Figure 1117: Mark Choice Continue Form

1. Continue Chain List

2. Configure the following parameter(s) as required:

Parameter	Description
Continue Chain	**Synopsis:** { forward, prerouting } **Default:** 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.

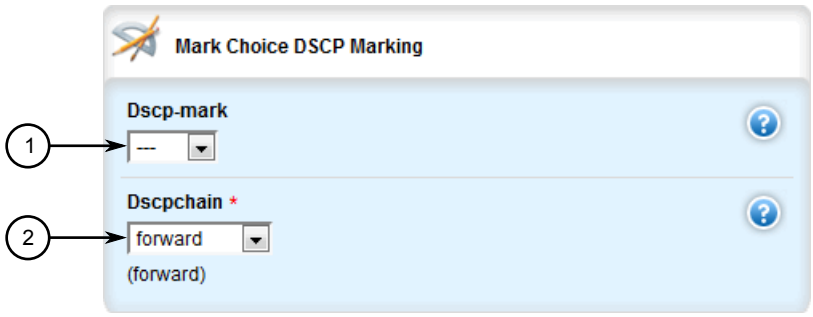


Figure 1118: Mark Choice DSCP Marking Form

1. DSCP Mark List **2.** DSCP Chain List

2. Configure the following parameter(s) as required:

Parameter	Description
DSCP Mark	**Synopsis:** { BE, AF11, AF12, AF13, AF21, AF22, AF23, AF31, AF32, AF33, AF41, AF42, AF43, CS1, CS2, CS3, CS4, CS5, CS6, CS7, EF } A DSCP class value chosen amongst the given list.
dscpchain	**Synopsis:** { forward, postrouting, prerouting } **Default:** 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 16.2.6.4

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.

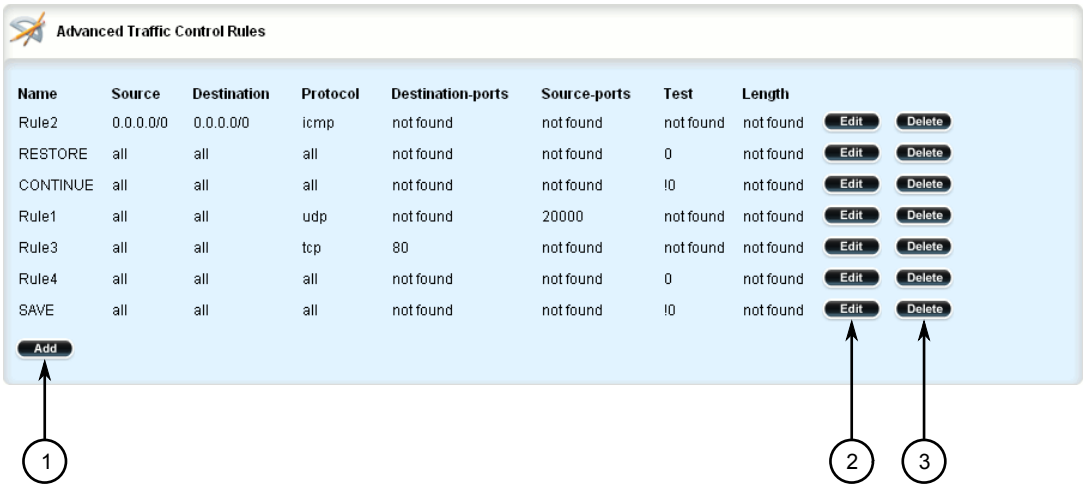


Figure 1119: Advanced Traffic Control Rules Table

1. Add Button **2.** Edit Button **3.** Delete Button

3. Click **Delete** next to the chosen traffic control 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 16.2.7

Managing QoS Mapping for VLANs

Quality of Service (QoS) mapping is used to map QoS traffic. It assigns a traffic control mark to incoming IP traffic based on the priority value of a tagged frame. The incoming traffic is then classified and placed in the priority queues according to the traffic control rules specified for the marked rule. In addition, traffic control can assign the same priority or a different priority value when a frame needs to be egressed with a VLAN tag through a traffic control interface.

QoS maps can be configured for VLAN connections on routable Ethernet ports and virtual switches.

CONTENTS

Section 16.2.7.1

Viewing a List of QoS Maps for VLANs

To view a list of QoS maps for a VLAN connection, navigate to either:

- **For Switched Ethernet Ports**
  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.
- **For WAN Interfaces**
  interface » wan » {interface} » {protocol} » vlan » {vlan-id}, where:
  - *{interface}* is the WAN interface
  - *{protocol}* is either T1 or E1
  - *{id}* is the ID of the virtual switch
  - *{vlan-id}* is the VLAN ID

If QoS maps have been configured, the **QoS Map Settings** table appears.

Figure 1120: QoS Map Settings Table

If no QoS maps have been configured, add maps as needed. For more information, refer to Section 16.2.7.2, "Adding a QoS Map".

Section 16.2.7.2
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 12.2.2, "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.
   - **For WAN Interfaces**
     interface » wan » {interface} » {protocol} » vlan » {vlan-id} » qosmap, where:

- *{interface}* is the WAN interface
- *{protocol}* is either T1 or E1
- *{id}* is the ID of the virtual switch
- *{vlan-id}* is the VLAN ID

4. Click **<Add qosmap>**. The **Key Settings** form appears.

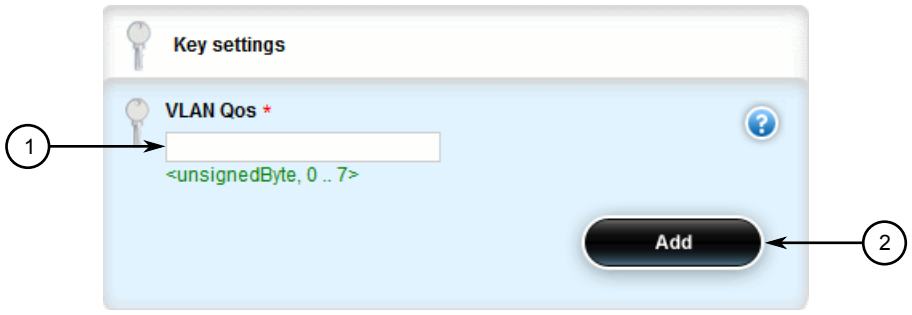


Figure 1121: Key Settings Form

1. VLAN QoS Box **2.** Add Button

5. Configure the following parameter(s) as required:

Parameter	Description
VLAN QoS	**Synopsis:** An 8-bit unsigned 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.

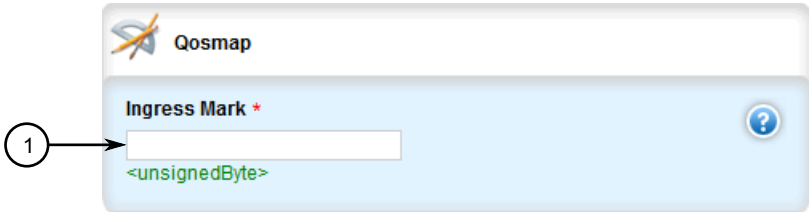


Figure 1122: Qosmap Form

1. Ingress Mark Box

7. Configure the following parameter(s) as required:

Parameter	Description
Ingress Mark	**Synopsis:** An 8-bit unsigned integer between 0 and 255 Map the ingress to a mark. This parameter is mandatory.

8. Add an egress mark for the QoS map. For more information, refer to Section 16.2.8.2, "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 16.2.7.3
Deleting a QoS Map

To delete a QoS map for a VLAN connection, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to either:
   - **For Switched Ethernet Ports**
     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.
   - **For WAN Interfaces**
     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.

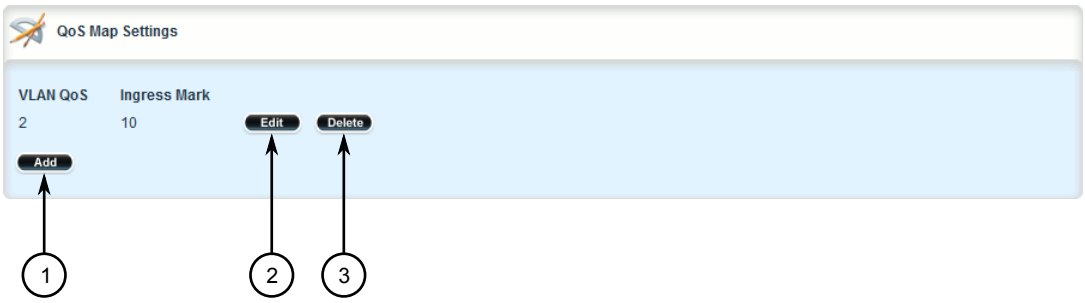


Figure 1123: QoS Map Settings Table

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 16.2.8

Managing Egress Markers for QoS Maps

Egress markers for QoS maps are used to assign priority to traffic that shares the same mark as one of the egress marks configured for the device.

CONTENTS

Section 16.2.8.1

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
- **For WAN Interfaces**
  interface » wan » {interface} » {protocol} » vlan » {vlan-id} » qosmap » {priority} » egress, where:
  - *{interface}* is the WAN interface
  - *{protocol}* is either T1 or E1
  - *{id}* is the ID of the virtual switch
  - *{vlan-id}* is the VLAN ID
  - *{priority}* is the priority assigned to the QoS map

If egress marks have been configured, the **Egress Marks Settings** table appears.

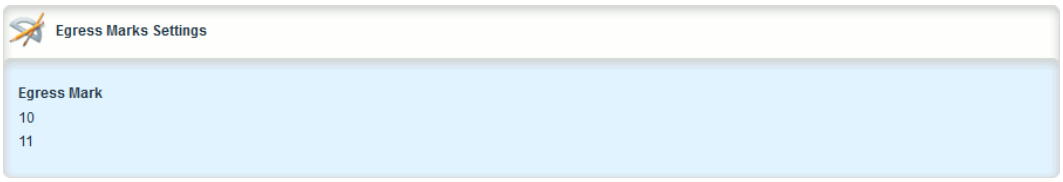


Figure 1124: Egress Marks Settings Table

If no egress marks have been configured, add egress marks as needed. For more information, refer to Section 16.2.8.2, "Adding an Egress Mark".

Section 16.2.8.2
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
   - **For WAN Interfaces**
     interface » wan » {interface} » {protocol} » vlan » {vlan-id} » qosmap » {priority} » egress, where:
     - *{interface}* is the WAN interface
     - *{protocol}* is either T1 or E1
     - *{id}* is the ID of the virtual switch
     - *{vlan-id}* is the VLAN ID
     - *{priority}* is the priority assigned to the QoS map
3. Click **<Add egress>**. The **Key Settings** form appears.

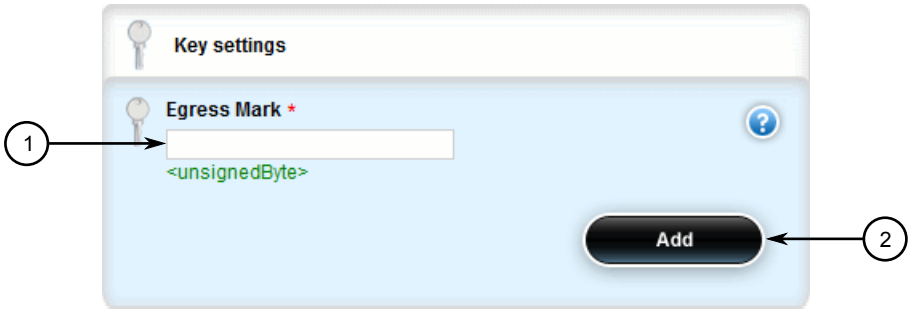


Figure 1125: Key Settings Form

1. Egress Mark Box **2.** Add Button

4. Configure the following parameter(s) as required:

Parameter	Description
Egress Mark	**Synopsis:** An 8-bit unsigned 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 16.2.8.3
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

- **For WAN Interfaces**
  interface » wan » {interface} » {protocol} » vlan » {vlan-id} » qosmap » {priority} » egress, where:
  - *{interface}* is the WAN interface
  - *{protocol}* is either T1 or E1
  - *{id}* is the ID of the virtual switch
  - *{vlan-id}* is the VLAN ID
  - *{priority}* is the priority assigned to the QoS map

The **Egress Marks Settings** table appears.

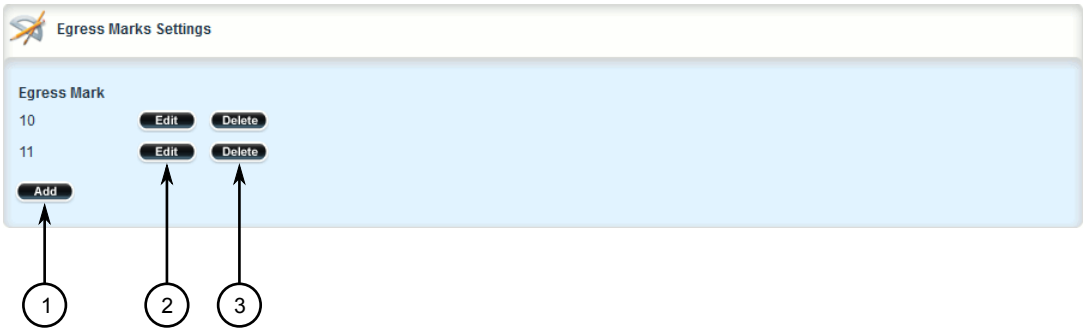


Figure 1126: Egress Marks Settings Table

1. Add Button **2.** Edit Button **3.** Delete Button

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 16.2.9
Viewing QoS Statistics

RUGGEDCOM ROX II provides statistics for traffic going through each class that has been configured. Packets are assigned to classes on the outbound interface based on rules. If a packet matches the specified criteria, it is considered to be a member of the class and is forwarded to that class. If the packet does not match any rule, it is forwarded to the default class.

For more information about traffic control classes, refer to Section 16.2.4, "Managing Traffic Control Classes".

NOTE
Statistics are only available when traffic control is enabled in advanced mode. For more information about enabling traffic control, refer to Section 16.2.1, "Enabling and Configuring Traffic Control".

To view the QoS statistics, navigate to ***qos » statistics***. The **QoS Statistics** table appears.

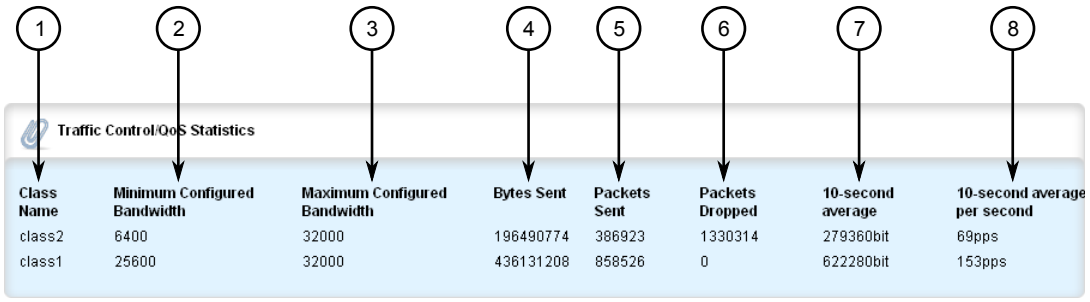


Figure 1127: QoS Statistics Table

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	**Synopsis:** A string
Minimum Configured Bandwidth	**Synopsis:** A string The minimum guaranteed bandwidth. This is based on the device's defined characteristics.
Maximum Configured Bandwidth	**Synopsis:** A string The maximum guaranteed bandwidth in absence of any higher prioritized traffic. This is based on the device's defined characteristics.
Bytes Sent	**Synopsis:** A string The number of bytes that were sent through this class.
Packets Sent	**Synopsis:** A string The number of packets that were sent through this class.
Packets Dropped	**Synopsis:** A string The number of packets that were dropped in this class.
10-Second Average	**Synopsis:** A string Based on a 10-second average.
10-Second Average: Packets per Second	**Synopsis:** A string Based on a 10-second average.

Section 16.3

Managing Classes of Service

Classes of Service (CoS) provides the ability to expedite the transmission of certain frames and port traffic over others. The CoS of a frame can be set to Normal, Medium, High or Critical. By default, RUGGEDCOM ROX II enforces Normal CoS for all traffic.

IMPORTANT!
Use the highest supported CoS with caution, as it is always used by the switch for handling network management traffic, such as RSTP BPDUs.

If this CoS is used for regular network traffic, upon traffic bursts, it may result in the loss of some network management frames, which in turn may result in the loss of connectivity over the network.

The process of controlling traffic based on CoS occurs over two phases:

- **Inspection Phase**
  In the inspection phase, the CoS priority of a received frame is determined from:
  - A specific CoS based upon the source and destination MAC address (as set in the Static MAC Address Table)
  - The priority field in 802.1Q tags
  - The Differentiated Services Code Point (DSCP) component of the Type Of Service (TOS) field, if the frame is IP
  - The default CoS for the port

  Each frame's CoS will be determined once the first examined parameter is found in the frame.

  Received frames are first examined to determine if their destination or source MAC address is found in the Static MAC Address Table. If they are, the CoS configured for the static MAC address is used. If neither destination or source MAC address is in the Static MAC Address Table, the frame is then examined for 802.1Q tags and the priority field is mapped to a CoS. If a tag is not present, the frame is examined to determine if it is an IP frame. If the frame is IP and inspecting TOS is enabled, the CoS is determined from the DSCP field. If the frame is not IP or inspecting TOS is disabled, the default CoS for the port is used.

  After inspection, the frame is forwarded to the egress port for transmission.
- **Forwarding Phase**
  Once the CoS of the frame is determined, the frame is forwarded to the egress port, where it is collected into one of the priority queues according to the assigned CoS.

  CoS weighting selects the degree of preferential treatment that is attached to different priority queues. The ratio of the number of higher CoS to lower CoS frames transmitted can be configured. If desired, the user can configure lower CoS frames to be transmitted only after all higher CoS frames have been serviced.

CONTENTS

Section 16.3.1
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.

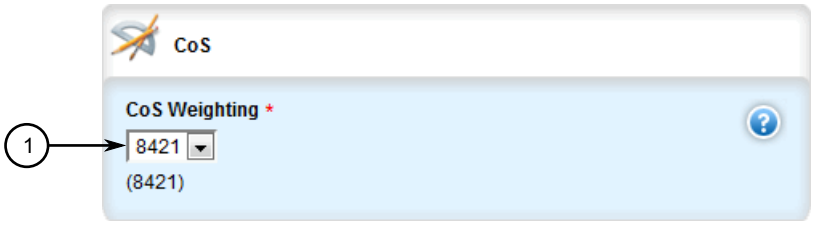


Figure 1128: CoS Form

1. CoS Weighting List

3. Configure the following parameters as required:

Parameter	Description
CoS Weighting	**Synopsis:** { 8421, strict } **Default:** 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 16.3.2.2, "Adding a Priority-to-CoS Mapping Entry" or Section 16.3.3.2, "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 16.3.2
Managing Priority-to-CoS Mapping

Assigning CoS to different IEEE 802.1p priority values in the frame is done by defining priority-to-CoS mapping table entries.

CONTENTS

Section 16.3.2.1
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.

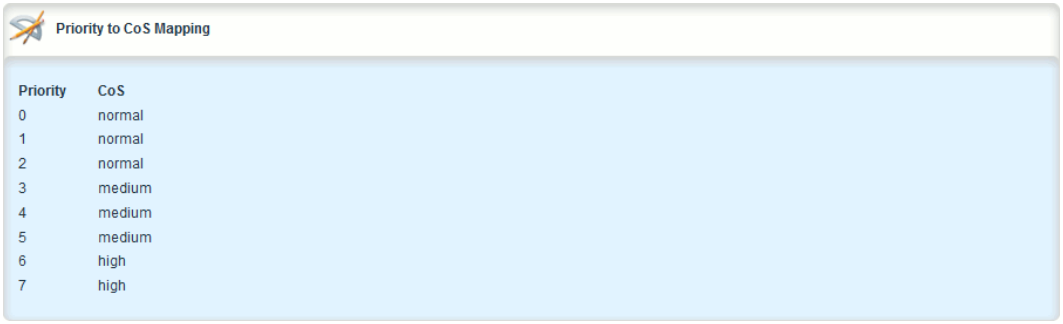


Figure 1129: Priority to CoS Mapping Table

If no entries have been configured, add entries as needed. For more information, refer to Section 16.3.2.2, "Adding a Priority-to-CoS Mapping Entry".

Section 16.3.2.2
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.

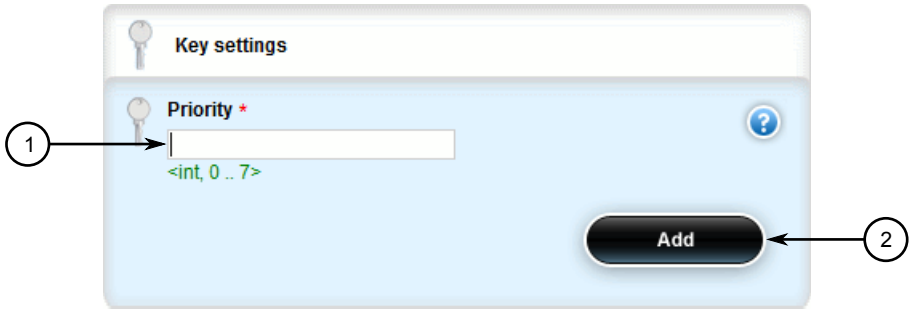


Figure 1130: Key Settings Form

1. Priority Box **2.** Add Button

3. Configure the following parameter(s) as required:

Parameter	Description
Priority	**Synopsis:** A 32-bit signed integer between 0 and 7 The value of the IEEE 802.1p priority.

4. Click **Add** to add the priority. The **Priority to CoS Mapping** form appears.

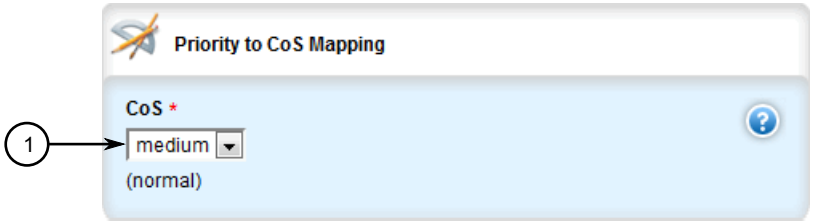


Figure 1131: Priority to CoS Mapping Form

1. CoS List

5. 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	**Synopsis:** { N/A, normal, medium, high, crit } **Default:** normal The Class of Service (CoS) assigned to received tagged frames with the specified IEEE 802.1p priority value.

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 16.3.2.3
Deleting a Priority-to-CoS Mapping Entry

To delete a priority-to-CoS mapping entry, do the following:

NOTE
Deleting an entry sets the CoS to Normal.

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to ***switch » class-of-service » priority-to-cos***. The **Priority to CoS Mapping** table appears.

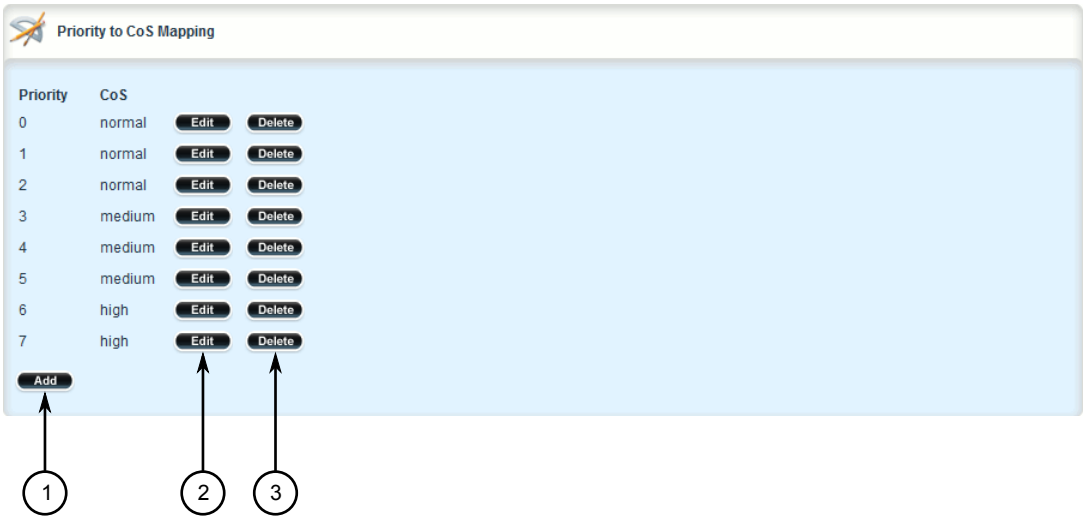


Figure 1132: Priority to CoS Mapping Table

1. Add Button **2.** Edit Button **3.** Delete Button

3. Click **Delete** next to the chosen 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 16.3.3

Managing DSCP-to-CoS Mapping

Assigning CoS to different values of the Differentiated Services Code Point (DSCP) field in the IP header of received packets is done by defining DSCP-to-CoS mapping table entries.

CONTENTS

Section 16.3.3.1

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.

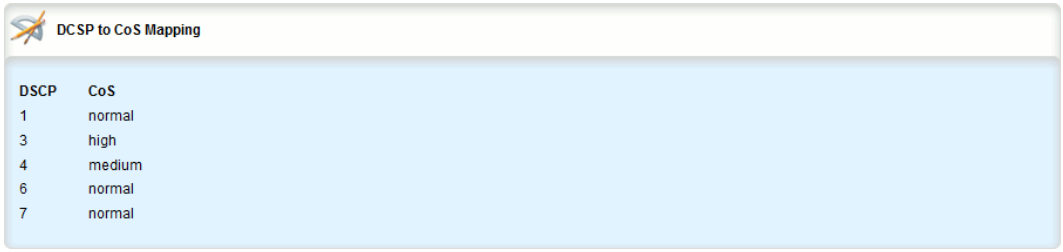


Figure 1133: DSCP to CoS Mapping Table

If no entries have been configured, add entries as needed. For more information, refer to Section 16.3.3.2, "Adding a DSCP-to-CoS Mapping Entry".

Section 16.3.3.2
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.

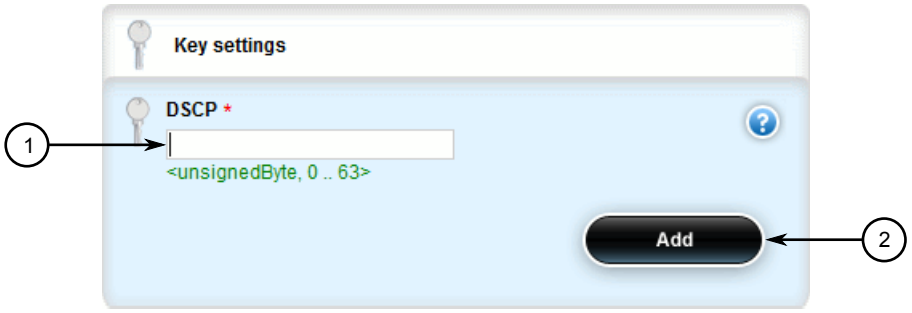


Figure 1134: Key Settings Form

1. DSCP Box **2.** Add Button

3. Configure the following parameter(s) as required:

Parameter	Description
DSCP	**Synopsis:** An 8-bit unsigned 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.

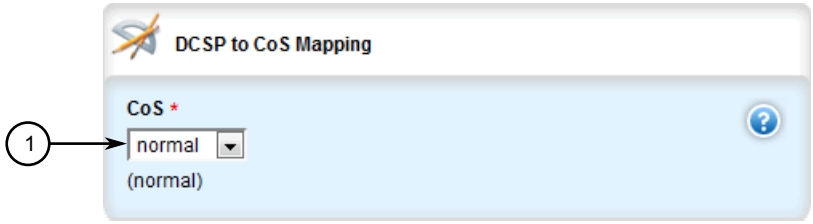


Figure 1135: DSCP to CoS Mapping Form

1. CoS List

5. Configure the following parameter(s) as required:

Parameter	Description
CoS	**Synopsis:** { N/A, normal, medium, high, crit } **Default:** normal The Class of Service (CoS) assigned to the received frames with the specified DSCP.

6. Configure the CoS parameters on select switched Ethernet ports and/or trunk interfaces as needed. For more information, refer to Section 8.1.2, "Configuring a Switched Ethernet Port" and/or Section 8.2.2, "Adding an Ethernet Trunk Interface".
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 16.3.3.3

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.

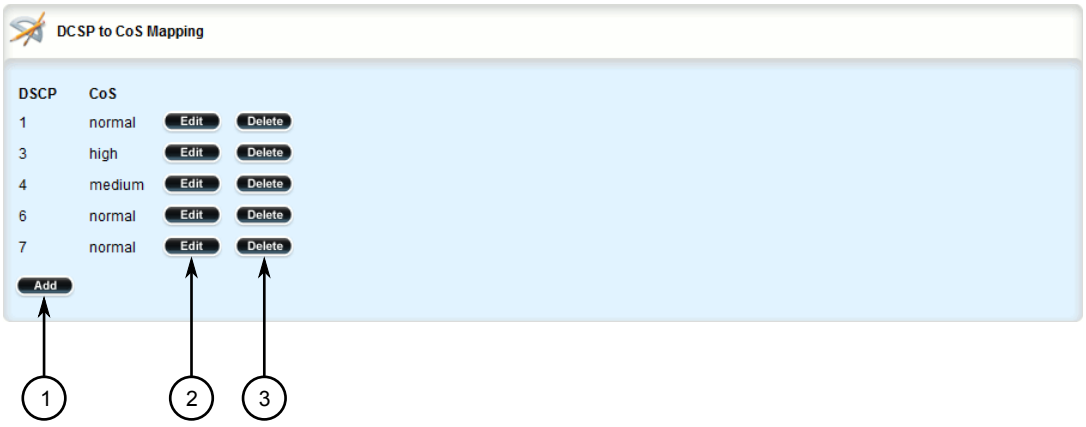


Figure 1136: DSCP to CoS Mapping Table

1. Add Button **2.** Edit Button **3.** Delete Button

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 16.4

Managing NetFlow Data Export

RUGGEDCOM ROX II supports the collection and forwarding of flow records to NetFlow-enabled servers, or NetFlow Collectors.

IMPORTANT!

NetFlow requires additional memory and CPU resources, which may affect device performance when network traffic is high. When enabled, general performance should be monitored to make sure traffic is processed optimally. If needed, NetFlow's resource requirements can be minimized by reducing the NetFlow cache. For more information, refer to Section 16.4.5, "Controlling the NetFlow Cache".

CONTENTS

Section 16.4.1

Understanding NetFlow Data Export

NetFlow is a traffic analysis tool developed by Cisco that allows network operators to characterize traffic flows across their networks. It provides information that allows operators to identify security vulnerabilities, assess network productivity and resource utilization, determine the causes of congestion, and more.

A basic NetFlow monitoring setup consists of the following components

- **Flow Exporter**
  The exporter aggregates data packets into flows, which are forwarded to one or more flow collectors.
- **Flow Collector**
  The collector receives, stores and pre-processes flow data received from one or more flow exporters.
- **Flow Analyzer**
  The flow analyzer queries one or more flow collectors for flow data and then analyzes the data with a focus on intrusion detection and traffic profiling.

RUGGEDCOM ROX II acts as a *flow exporter*, collecting data from ingress (incoming) and/or egress (outgoing) packets and then forwarding them as flow records to one or more collectors.

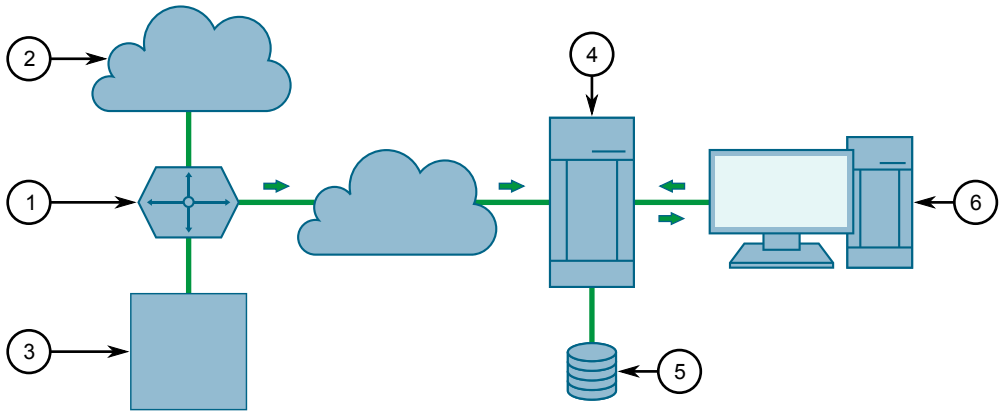


Figure 1137: NetFlow

1. NetFlow Exporter (RUGGEDCOM ROX II) **2.** WAN **3.** LAN **4.** NetFlow Collector **5.** Flow Storage **6.** Analysis Console

NOTE
RUGGEDCOM ROX II supports NetFlow version 5.

CONTENTS

Section 16.4.1.1
Flow Records

A flow record, as defined by the Cisco standard, is a unidirectional sequence of packets that share the same:

- Ingress interface
- Source and destination IP address
- IP protocol
- Source and destination port for TCP and UDP
- Type of Service (ToS)

Each flow record is exported using the User Datagram Protocol (UDP), which requires each packet to include the IP address of the target NetFlow collector and its designated UDP port.

A flow record is considered ready to export when either of the following conditions are met:

- The flow has been inactive (e.g. no new packets) for a specific period of time
- The flow has been active for longer than allowed by the configuration
- A TCP flag indicates the flow has been terminated

RUGGEDCOM ROX II includes user-configurable timers for inactive and active flows.

NOTE
RUGGEDCOM ROX II does not retain a record of flows sent. Therefore, any NetFlow packets dropped due to congestion or packet corruption will be lost permanently.

Section 16.4.2
Configuring NetFlow Data Export

To configure the device to send flows to a NetFlow collector, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.

   IMPORTANT!
   NetFlow does not support Layer 3 switching functions. Layer 3 switching must be disabled before NetFlow is enabled.

2. Make sure Layer 3 switching is disabled by setting the following parameters under ***switch » layer3-switching*** to `disabled`:

   - *`Unicast Mode`*
   - *`Multicast Mode`*

   For more information, refer to Section 9.2, "Configuring Layer 3 Switching".
3. Enable the NetFlow service. For more information, refer to Section 16.4.3, "Enabling/Disabling NetFlow".
4. [Optional] Set the engine ID that is assigned to each flow record. For more information, refer to Section 16.4.4, "Setting the NetFlow Engine ID".
5. [Optional] Set the maximum number of active flows tracked by the device. This can help improve performance in some scenarios. For more information, refer to Section 16.4.5, "Controlling the NetFlow Cache".

6. [Optional] Control how RUGGEDCOM ROX II manages active and inactive flows. For more information, refer to Section 16.4.6, "Controlling Active/Inactive Flows".
7. Define one or more interfaces from which to monitor traffic. For more information, refer to Section 16.4.7.2, "Adding a NetFlow Interface".
8. Define one or more NetFlow collectors to which RUGGEDCOM ROX II can send flows. For more information, refer to Section 16.4.8.2, "Adding a NetFlow Collector".

Section 16.4.3

Enabling/Disabling NetFlow

To enable or disable NetFlow, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to ***services » netflow***. The **NetFlow** form appears.

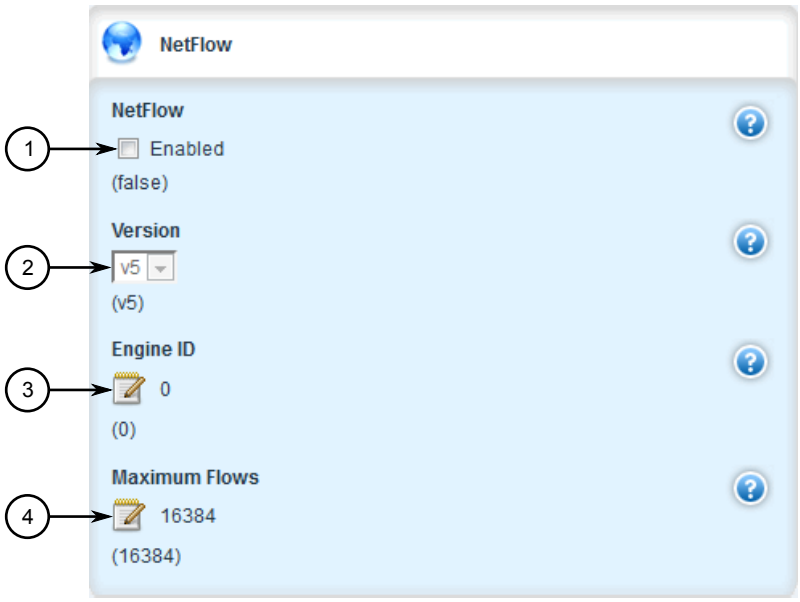


Figure 1138: NetFlow Form

1. NetFlow Check Box **2.** Engine ID Box **3.** Maximum Flows

3. Under **NetFlow**, do one of the following:
   - Select **Enabled** to enable NetFlow
   - Clear **Enabled** to disable NetFlow
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 16.4.4
Setting the NetFlow Engine ID

An engine ID can be assigned to flow records to uniquely link them to the device from which they were sent. This can be useful information to network analysts wishing to further categorize NetFlow data by device, region, etc.

The engine ID is defined in the header of the data export.

To set an engine ID for the device, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to ***services » netflow***. The **NetFlow** form appears.

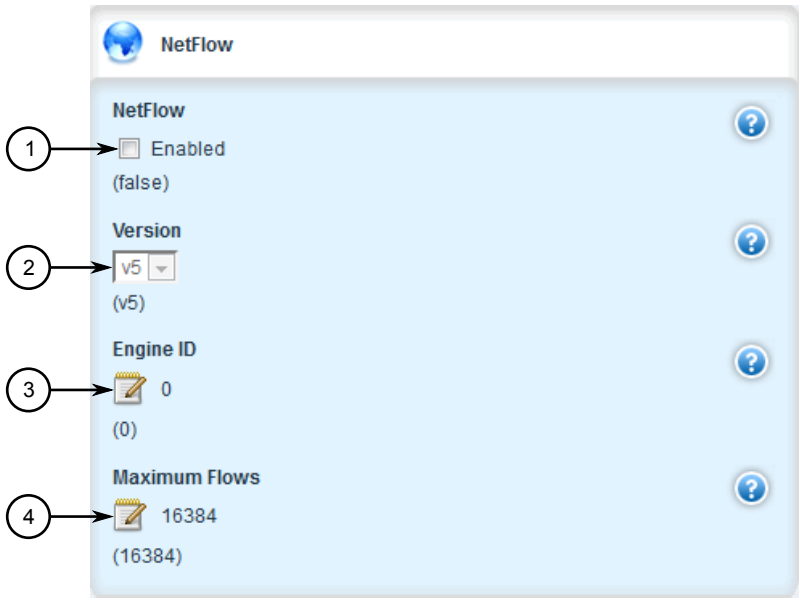


Figure 1139: NetFlow Form

1. NetFlow Check Box **2.** Engine ID Box **3.** Maximum Flows

3. Under **Engine ID**, enter a number.
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 16.4.5
Controlling the NetFlow Cache

NetFlow consumes memory and CPU resources during operation, which may affect the performance of the device during times of high traffic. To reduce NetFlow's effect on performance, consider reducing the number of active flows tracked by NetFlow. This will reduce the cache and free resources for other processes.

To control the NetFlow cache, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.

2. Navigate to ***services » netflow***. The **NetFlow** form appears.

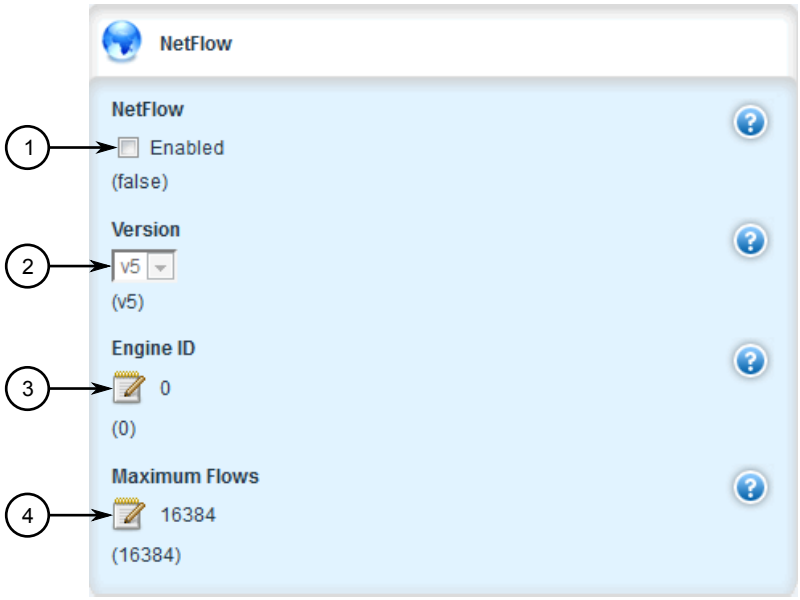


Figure 1140: NetFlow Form

1. NetFlow Check Box **2.** Engine ID Box **3.** Maximum Flows

3. Configure the following parameter:

Parameter	Description
Maximum Flows	**Synopsis:** A 16-bit unsigned integer **Default:** 16384 The maximum number of active flows tracked by NetFlow.

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 16.4.6

Controlling Active/Inactive Flows

NetFlow considers a flow to be ready for export when it has been inactive for a specific period of time or the flow has been active (long lived) for too long. By default, a flow is considered inactive if no new packets have been received for 15 seconds. An active flow is considered ready if it has received packets for longer than 30 minutes. Both durations can be adjusted to reduce or increase either the size of the NetFlow packets and/or the speed at which they are delivered.

To control how RUGGEDCOM ROX II manages active and inactive flows, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to ***services » netflow***. The **Timeouts** form appears.

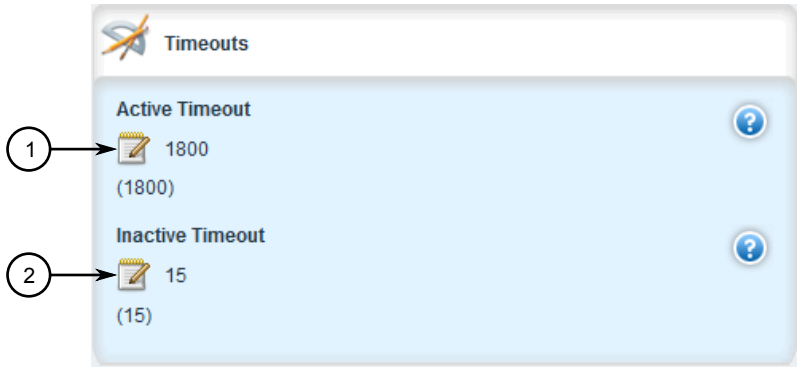


Figure 1141: Timeouts Form

1. Active Timeout Box **2.** Inactive Timeout Box

3. Configure the following parameters:

Parameter	Description
Active Timeout	**Synopsis:** A 32-bit signed integer equaling 1 or higher **Default:** 1800 The time in seconds (s) an active flow remains active.
Inactive Timeout	**Synopsis:** A 32-bit signed integer equaling 1 or higher **Default:** 15 The time in seconds (s) an inactive flow remains in the cache before it is deleted.

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 16.4.7

Managing NetFlow Interfaces

RUGGEDCOM ROX II requires an interface from which to collect NetFlow data, but can be configured to monitor multiple interfaces if needed. Each interface can be configured to monitor packets entering (ingress) and/or exiting (egress).

IMPORTANT!
RUGGEDCOM ROX II does not support Netflow data collection on hardware-accelerated interfaces.

CONTENTS

Section 16.4.7.1
Viewing a List of NetFlow Interfaces

To view a list of interfaces configured to monitor traffic for NetFlow, navigate to ***services » netflow » interface***. The **Interface** table appears.

Figure 1142: Interface Table

If no interfaces have been configured, add interfaces as needed. For more information, refer to Section 16.4.7.2, "Adding a NetFlow Interface".

Section 16.4.7.2
Adding a NetFlow Interface

To add a NetFlow interface, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to ***services » netflow » interface*** and then click **<Add interface>**. The **Key Settings** form appears.

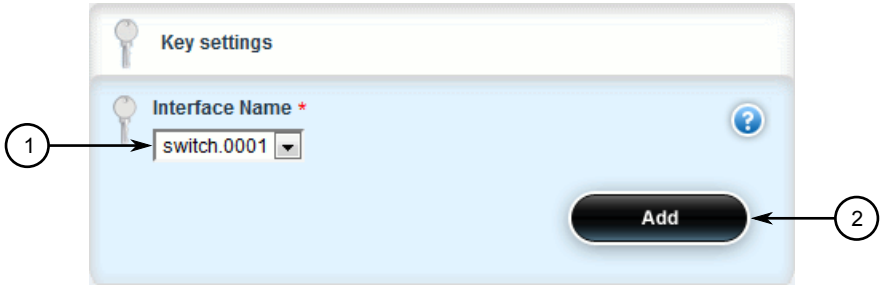


Figure 1143: Key Settings Form

1. Interface Name List **2.** Add Button

3. Under **Interface Name**, select the desired interface and then click **Add**. The **Interface** form appears.

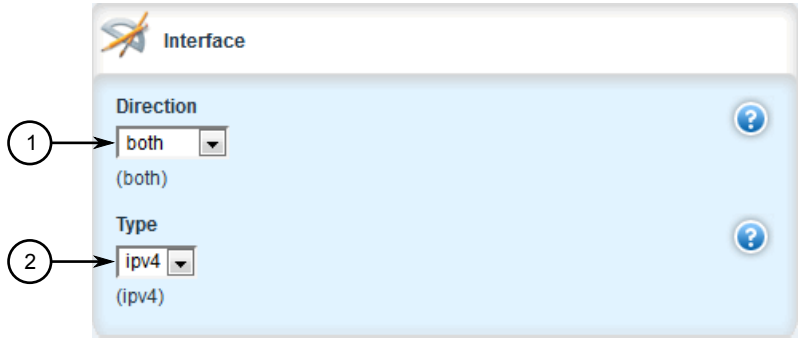


Figure 1144: Interface Form

1. Direction List

4. Under **Direction**, select the direction of traffic to be monitored. Options include:
   - `ingress` – Only traffic entering through the interface is monitored
   - `egress` – Only traffic exiting through the interface is monitored
   - `both` – All traffic traversing the interface is monitored
5. 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 16.4.7.3

Deleting a NetFlow Interface

To delete a NetFlow interface, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to ***services » netflow » interface***. The **Interface** table appears.

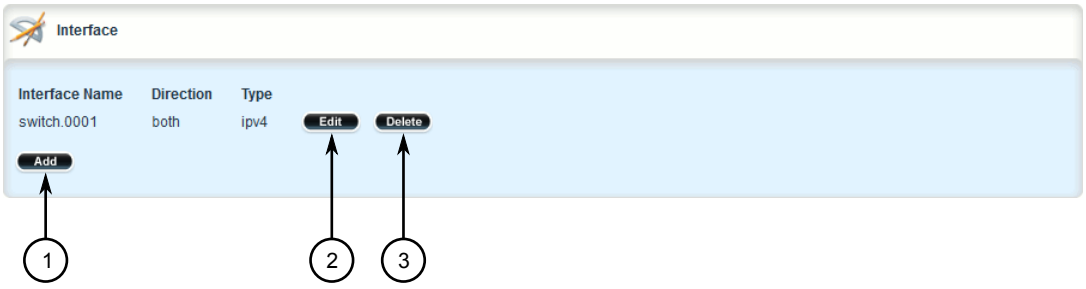


Figure 1145: Interface Table

1. Add Button **2.** Edit Button **3.** Delete Button

3. Click **Delete** next to the desired NetFlow 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 16.4.8
Managing NetFlow Collectors

RUGGEDCOM ROX II can be configured to forward flows to up to four NetFlow collectors.

CONTENTS

Section 16.4.8.1
Viewing a List of NetFlow Collectors

To view a list of NetFlow collectors the device can send flows, navigate to ***services » netflow » collector***. The **Collector** table appears.

Figure 1146: Collector Table

If no collectors have been configured, add collectors as needed. For more information, refer to Section 16.4.8.2, "Adding a NetFlow Collector".

Section 16.4.8.2
Adding a NetFlow Collector

To define a NetFlow collector to which RUGGEDCOM ROX II will send flows, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to ***services » netflow » collector*** and then click **<Add collector>**. The **Key Settings** form appears.

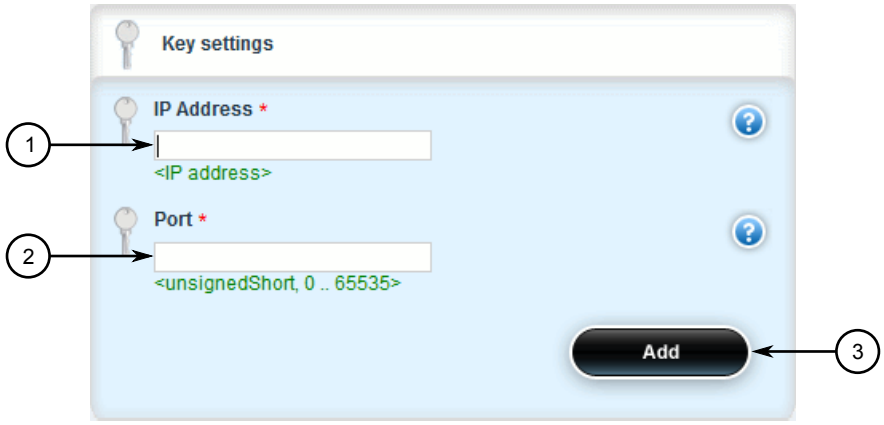


Figure 1147: Key Settings Form

1. IP Address Box **2.** Port Box **3.** Add Button

3. Configure the following parameters:

NOTE
A single server can host multiple NetFlow collectors, each monitoring a specific UDP port.

Parameter	Description
IP Address	**Synopsis:** A string The IP address of the NetFlow collector.
Port	**Synopsis:** A 16-bit unsigned integer between 0 and 65535 The UDP port used by the NetFlow Collector to receive messages.

4. Click **Add**.
5. [Optional] Enable the collector so RUGGEDCOM ROX II can forward NetFlow packets to it. For more information, refer to Section 16.4.8.3, "Enabling/Disabling a NetFlow Collector".
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 16.4.8.3
Enabling/Disabling a NetFlow Collector

To enable or disable a NetFlow collector defined in RUGGEDCOM ROX II, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to ***services » netflow » collector » {collector}***, where **{collector}** is the desired NetFlow collector. The **Collector** form appears.

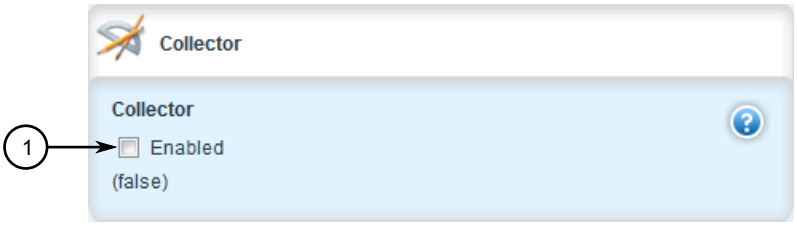


Figure 1148: Collector Form

1. Collector Check Box

3. Under **Collector**, do one for the following:
   - Select **Enabled** to enable the collector
   - Clear **Enabled** to disable the collector
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 16.4.8.4

Deleting a NetFlow Collector

To delete a NetFlow collector, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to ***services » netflow » collector***. The **Collector** table appears.

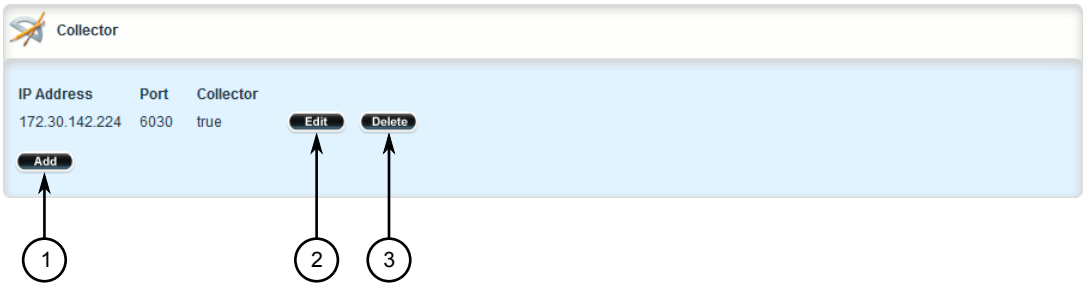


Figure 1149: Collector Table

1. Add Button **2.** Edit Button **3.** Delete Button

3. Click **Delete** next to the desired NetFlow collector.
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 16.4.9

Viewing the Status of NetFlow

To view the status of NetFlow, navigate to ***services » netflow » status***. The **Flow Status** and **Aggregated Throughput Status** forms appear.

Flow Status

The **Flow Status** form lists the number of active flows.

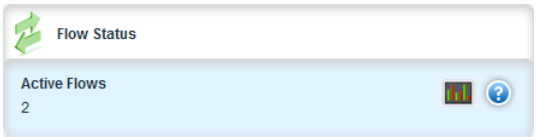


Figure 1150: Flow Status Table

Parameter	Description
Active Flows	**Synopsis:** A 32-bit signed integer The total number of active flows.

Aggregated Throughput Status

The **Aggregated Throughput Status** form provides real-time information about all flows distributed to NetFlow collectors.

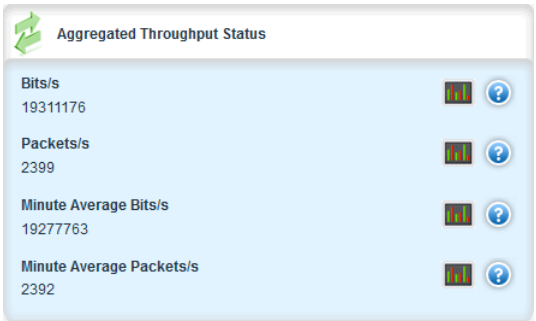


Figure 1151: Flow Status Table

Parameter	Description
Bits/s	**Synopsis:** A 32-bit unsigned integer The current rate in bits/s.
Packets/s	**Synopsis:** A 32-bit unsigned integer The current rate in packets/s.
Minute Average Bits/s	**Synopsis:** A 32-bit unsigned integer The average rate in bits/s over a minute.
Minute Average Packets/s	**Synopsis:** A 32-bit unsigned integer

Parameter	Description
	The average rate in packets/s over a minute.

Section 16.4.10

Example: Exporting Flows to Multiple Collectors

This example describes how to configure RUGGEDCOM ROX II to forward NetFlow data to two NetFlow collectors.

In the following topology, the NetFlow exporter (RUGGEDCOM ROX II) is collecting data on packets traversing two interfaces. Packets sharing the same characteristics (i.e. source, destination, port, etc.) are placed into flows. When each flow is either deemed inactive, has exceeded the active timer, or is flagged as terminated, the exporter forwards the flow to the specified collectors.

IMPORTANT!
The values shown are specific to the provided topology. Actual values can vary based on the user's configuration.

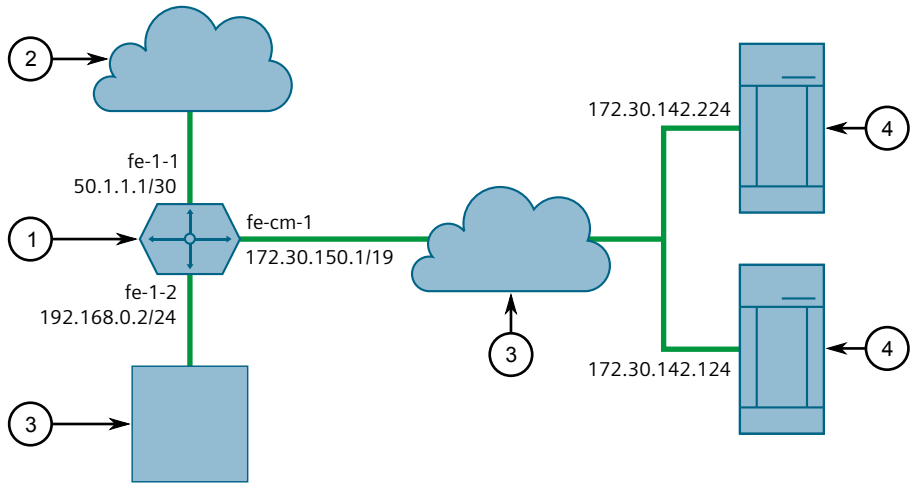


Figure 1152: Topology – Exporting Data to Multiple Collectors

1. NetFlow Exporter (RUGGEDCOM ROX II) **2.** WAN **3.** LAN **4.** NetFlow Collector

» Configuration

To configure RUGGEDCOM ROX II to export NetFlow packets to two NetFlow collectors, do the following:

1. Make sure Layer 3 switching is disabled by setting the following parameters under ***switch » layer3-switching*** to `disabled`:
   - *`Unicast Mode`*
   - *`Multicast Mode`*

   For more information, refer to Section 9.2, "Configuring Layer 3 Switching".
2. Enable NetFlow. For more information, refer to Section 16.4.3, "Enabling/Disabling NetFlow".

3. Define two NetFlow collectors and make sure they are both enabled. For more information, refer to Section 16.4.8.2, "Adding a NetFlow Collector".
4. Define the interface that will be monitored by NetFlow. For more information, refer to Section 16.4.7.2, "Adding a NetFlow Interface".
5. Send traffic to the interface monitored by RUGGEDCOM ROX II.
6. Verify the NetFlow collectors are receiving flows from the device.

Final Configuration Example

```
services
 netflow
  enabled
  engine-id 10
  timeouts active-timeout 1800
  timeouts inactive-timeout 15
  collector 172.30.142.124 2
   enabled
  !
  collector 172.30.142.224 1
   enabled
  !
  interface fe-1-1
  !
 !
!
```

17 Time Services

RUGGEDCOM ROX II offers the following time-keeping and time synchronization features:

- Local hardware time keeping and time zone management
- NTP (Network Time Protocol) client and server

CONTENTS

Section 17.1

Configuring the Time Synchronization Settings

To configure the time synchronization settings, do the following:

1. Configure the system time and date. For more information, refer to Section 17.2, "Configuring the System Time and Date".
2. Configure the system time zone. For more information, refer to Section 17.3, "Configuring the System Time Zone".
3. Configure the local time settings. For more information, refer to Section 17.4, "Configuring the Local Time Settings".
4. If multicast addresses will be configured for the NTP server, enable and configure the NTP multicast client. For more information, refer to Section 17.9.1, "Enabling and Configuring NTP Multicast Clients".
5. If broadcast addresses will be configured for the NTP server, enable and configure the NTP broadcast client. For more information, refer to Section 17.9.2, "Enabling and Configuring NTP Broadcast Clients".
6. Add remote NTP servers. For more information, refer to Section 17.8.3, "Adding an NTP Server".
7. Add broadcast/mutlicast addresses for the NTP server. For more information, refer to Section 17.9.3.2, "Adding a Broadcast/Multicast Address".
8. If required, add server authentication keys. For more information, refer to Section 17.8.5.2, "Adding a Server Key".

9. Add restrictions for the remote NTP servers. For more information, refer to Section 17.8.6.2, "Adding a Server Restriction".
10. Enable and configure the NTP service. For more information, refer to Section 17.5, "Enabling and Configuring the NTP Service".
11. View the status of the NTP service. For more information, refer to Section 17.6, "Viewing the NTP Service Status".

Section 17.2

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.

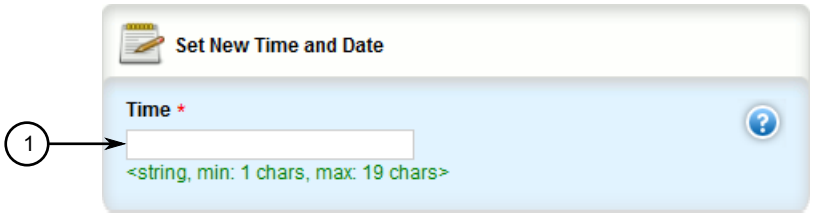


Figure 1153: Set New Time and Date Form

1. Time Box

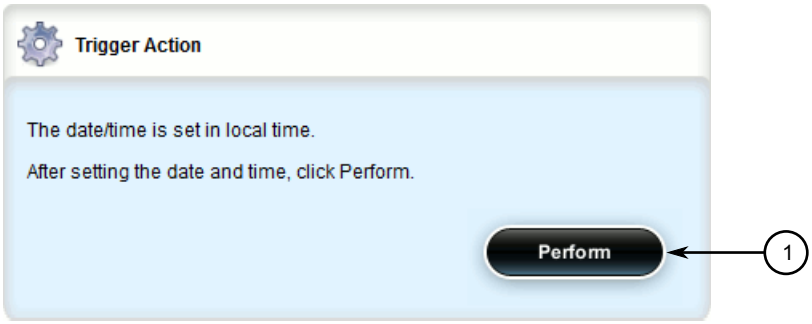


Figure 1154: Trigger Action Form

1. Perform Button

3. On the **Set New Time and Date** form, configure the following parameter(s) as required:

Parameter	Description
time	**Synopsis:** A string 1 to 19 characters long Enter the date and time in the format YYYY-MM-DD HH:MM:SS.

Parameter	Description
	This parameter is mandatory.

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 17.3
Configuring the System Time Zone

To configure the system time zone, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to ***admin***. The **Timezone** form appears.

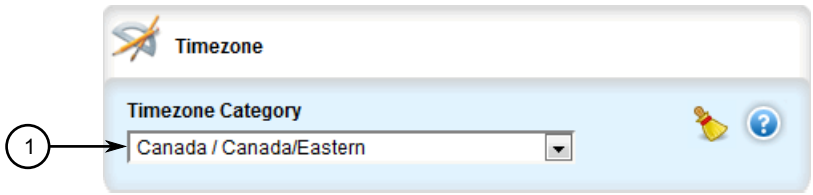


Figure 1155: Timezone Form

1. Timezone Category Box

3. Configure the following parameter(s) as required:

Parameter	Description
Timezone Category	**Synopsis:** A string The time zone in which the device resides. Note that UTC/GMT time zones conform to the POSIX style and have their signs reversed from common usage. In POSIX style, zones west of the GMT zone have a negative sign, while zones east of the GMT zone have a positive sign.

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 17.4
Configuring the Local Time Settings

The local time settings configure the local clock on the device as the NTP time source.

To configure the local NTP time settings, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to ***services » time » ntp***. The **Local Time Settings** form appears.

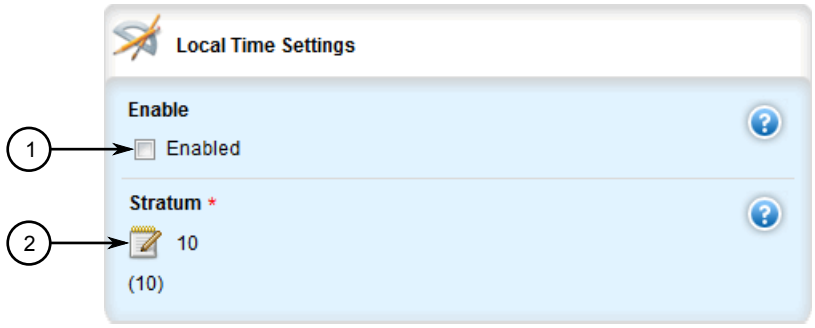


Figure 1156: Local Time Settings Form

1. Enable Check Box **2.** Stratum Box

3. Configure the following parameter(s) as required:

Parameter	Description
Enable	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	**Synopsis:** An 8-bit unsigned integer between 0 and 15 **Default:** 10 The stratum number of the local clock.

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 17.5

Enabling and Configuring the NTP Service

To enable and configure the NTP service, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to ***services » time » ntp***. The **Network Time Protocol (NTP)** form appears.

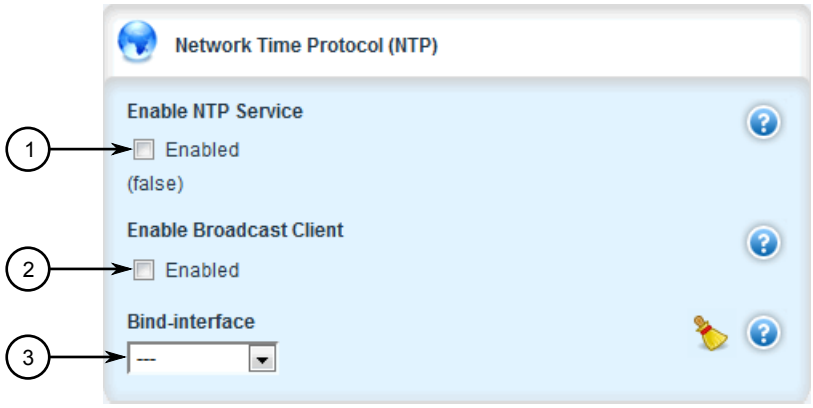


Figure 1157: Network Time Protocol (NTP) Form

1. Enable NTP Service Check Box **2.** Enable Broadcast Client Check Box

3. Configure the following parameters as required:

> **NOTE**
> *RUGGEDCOM ROX II supports both IPv4 and IPv6 addresses.*

Parameter	Description
Enable NTP Service	**Synopsis:** { true, false } **Default:** false Enables NTP service.
Bind Interface	**Synopsis:** A string Sets the IP address for the selected interface as the source IP address for outgoing NTP messages. Make sure an IP address is first assigned to the selected interface. The dummy0 interface should be used, unless required otherwise.

4. Select the **Enable NTP Service** check box to enable the NTP service, or clear the check box to disable the service.
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 17.6
Viewing the NTP Service Status

To view the status of the NTP service, do the following:

1. Make sure the NTP service is enabled. For more information, refer to Section 17.5, "Enabling and Configuring the NTP Service".
2. Navigate to ***services » time » ntp*** and click **ntp-status** in the menu. The **Trigger Action** form appears.

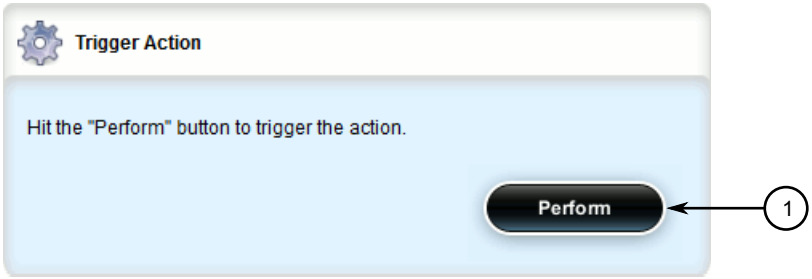


Figure 1158: Trigger Action Form

1. Perform Button

3. Click **Perform**. The **NTP Service Status** form appears.

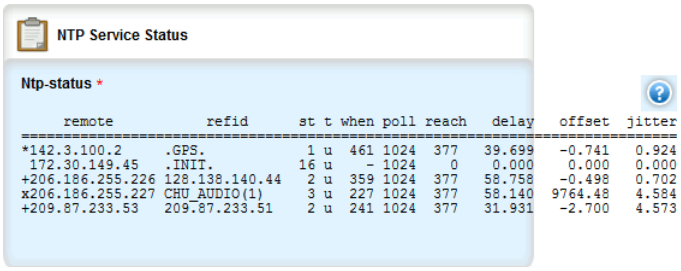


Figure 1159: NTP Service Status Form

This form provides the following information:

Parameter	Description
Remote IP	**Synopsis:** A string 1 to 40 characters long Remote address.
RefId	**Synopsis:** A string 1 to 40 characters long The identification of the reference clock.
Stratum	**Synopsis:** A string 1 to 32 characters long The stratum number of the reference clock.
Address type	**Synopsis:** A string 1 to 32 characters long The address type of the remote machine.
When	**Synopsis:** A string 1 to 32 characters long The number of seconds since the last poll of the reference clock.
Poll	**Synopsis:** A string 1 to 32 characters long The polling interval in seconds.
Reach	**Synopsis:** A string 1 to 32 characters long An 8-bit left-rotating register. Any 1 bit means that a time packet was received.
Delay	**Synopsis:** A string 1 to 32 characters long The time delay (in milliseconds) to communicate with the reference clock.

Parameter	Description
Offset	**Synopsis:** A string 1 to 32 characters long The offset (in milliseconds) between our time and that of the reference clock.
Jitter	**Synopsis:** A string 1 to 32 characters long The observed jitter (in milliseconds).

A character before an address is referred to as a tally code. Tally codes indicate the fate of the peer in the clock selection process. The following describes the meaning of each tally code:

Tally Code	Description
blank	A blank tally code indicates the peer has been discarded either because it is unreachable, it is synchronized to the same server (synch loop) or the synchronization distance is too far.
x	This tally code indicates the peer has been discarded because its clock is not correct. This is referred to as a *falseticker*.
.	This tally code indicates the peer has been discarded because its synchronization distance is too poor to be considered a candidate.
-	This tally code indicates the peer has been discarded because its offset is too a significant compared to the other peers. This is referred to as an *outlier*.
+	This tally code indicates the peer is considered a candidate.
#	This tally code indicates the peer is considered a candidate, but it is not among the top six sorted by synchronization distance. If the association is short-lived, it may be demobilized to conserve resources.
*	This tally code indicates the peer is the system peer.
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 17.7

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.

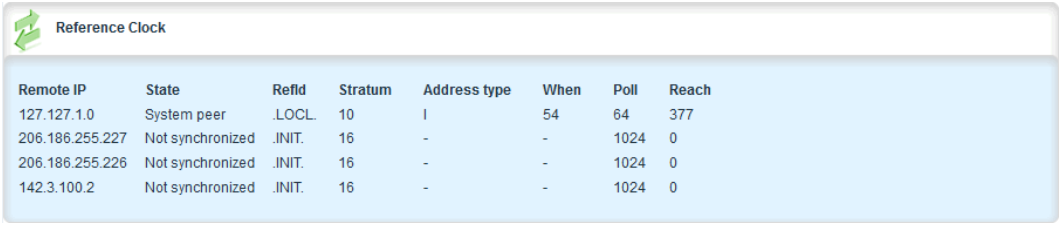


Figure 1160: Reference Clock Table

This table provides the following information:

Parameter	Description
Remote IP	**Synopsis:** A string 1 to 40 characters long The IP address of the reference clock.

Parameter	Description
State	**Synopsis:** A string 1 to 32 characters long The state of the clock.
RefId	**Synopsis:** A string 1 to 40 characters long The identification of the reference clock.
Stratum	**Synopsis:** A string 1 to 32 characters long The stratum number of the reference clock.
Address type	**Synopsis:** A string 1 to 32 characters long The address type of the remote machine.
When	**Synopsis:** A string 1 to 32 characters long The number of seconds since the last poll of the reference clock.
Poll	**Synopsis:** A string 1 to 32 characters long The polling interval in seconds.
Reach	**Synopsis:** A string 1 to 32 characters long An 8-bit left-rotating register. Any 1 bit means that a time packet was received.
Delay	**Synopsis:** A string 1 to 32 characters long The time delay (in milliseconds) to communicate with the reference clock.
Offset	**Synopsis:** A string 1 to 32 characters long The offset (in milliseconds) between our time and that of the reference clock.
Jitter	**Synopsis:** A string 1 to 32 characters long The observed jitter (in milliseconds).

Section 17.8

Managing NTP Servers

RUGGEDCOM ROX II can periodically refer to a remote NTP server to correct any accumulated drift in the onboard clock. RUGGEDCOM ROX II can also serve time via SNTP (Simple Network Time Protocol) to hosts that request it.

NTP servers can be added with or without authentication keys. To associate an authentication key with an NTP server, first define a server key. For information about adding server keys, refer to Section 17.8.5.2, "Adding a Server Key".

CONTENTS

Section 17.8.1
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.

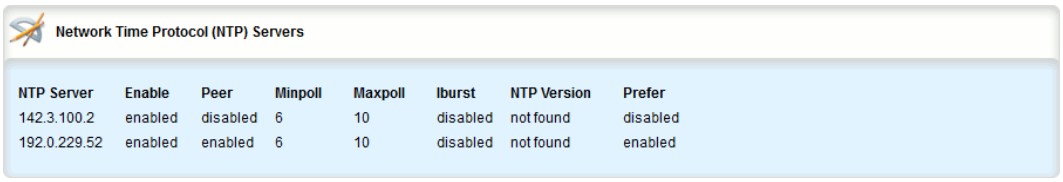


Figure 1161: Network Time Protocol (NTP) Servers Table

If no servers have been configured, add servers as needed. For more information, refer to Section 17.8.3, "Adding an NTP Server".

Section 17.8.2
Monitoring Subscribers

RUGGEDCOM ROX II monitors the subscriptions of up to 600 hosts (e.g. clients, servers and peers) that are connected to the NTP server. 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 v2.12 User Guide*.

Section 17.8.3
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. [Optional] If the communications with the server are to be authenticated, add a server authentication key or make sure the required key has been configured. For more information, refer to Section 17.8.5, "Managing Server Keys".
3. Navigate to ***services » time » ntp » server*** and click **<Add server>**. The **Key Settings** form appears.

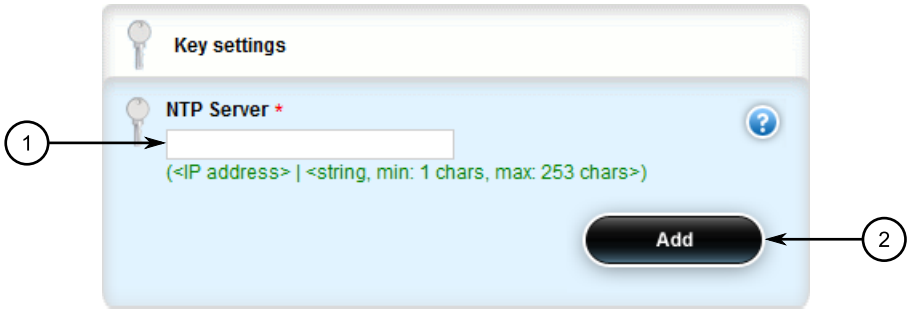


Figure 1162: Key Settings Form

1. NTP Server Box **2.** Add Button

4. Configure the following parameter(s) as required:

NOTE
RUGGEDCOM ROX II supports both IPv4 and IPv6 addresses.

Parameter	Description
NTP Server	**Synopsis:** A string 1 to 253 characters long The Internet address of the remote NTP server to be monitored.

5. Click **Add** to create the server configuration. The **Network Time Protocol (NTP) Servers** form appears.

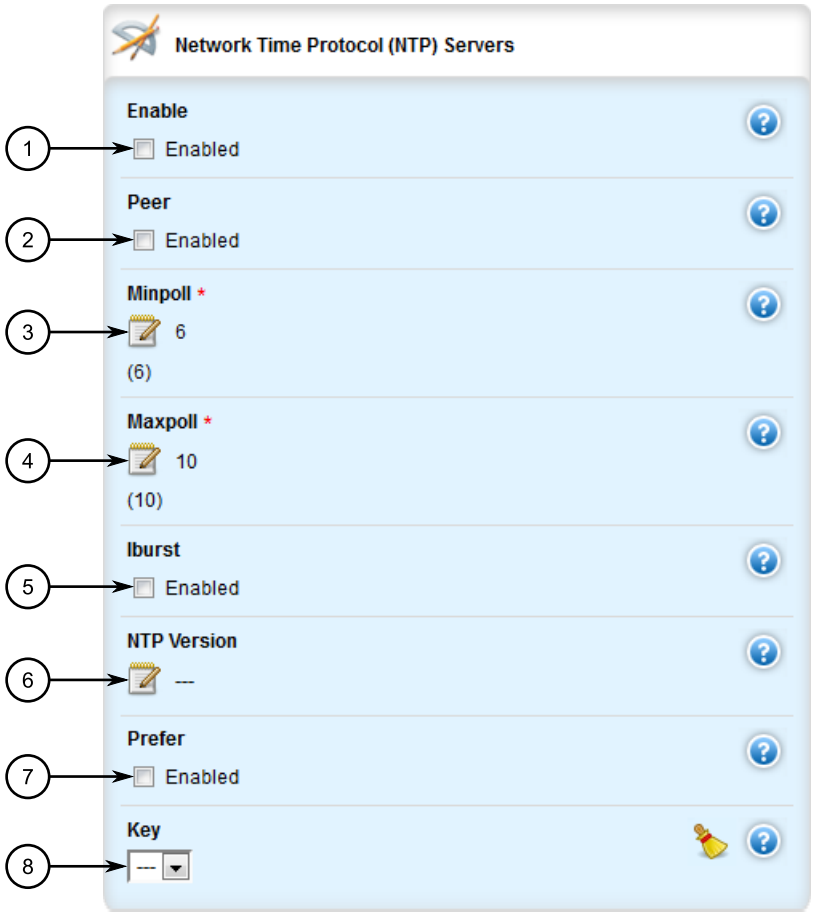


Figure 1163: Network Time Protocol (NTP) Servers Form

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

6. Configure the following parameter(s) as required:

Parameter	Description
Enable	Turns on the NTP interface to this server.
Peer	Allows you to enter and edit peers. Peers are NTP servers of the same stratum as the router, and are useful when contact is lost with the hosts in the NTP servers menu.
Minpoll	**Synopsis:** An 8-bit unsigned integer between 4 and 17 **Default:** 6 The minimum poll interval for NTP messages, in seconds as a power of two.
Maxpoll	**Synopsis:** An 8-bit unsigned integer between 4 and 17 **Default:** 10 The maximum poll interval for NTP messages, in seconds as a power of two.
Iburst	When the server is unreachable and at each poll interval, a burst of eight packets is sent instead of one.
NTP Version	**Synopsis:** A 32-bit signed integer between 1 and 4

Parameter	Description
	The version of the NTP protocol used to communicate with this host. Change this only if it is known that the host requires a version other than 4.
Prefer	Marks this server as preferred.
Key	**Synopsis:** A string An authentication key associated with this host.

7. [Optional] Set restrictions to control which NTP services can be accessed on the server. For more information, refer to Section 17.8.6.2, "Adding a Server Restriction".
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 17.8.4
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.

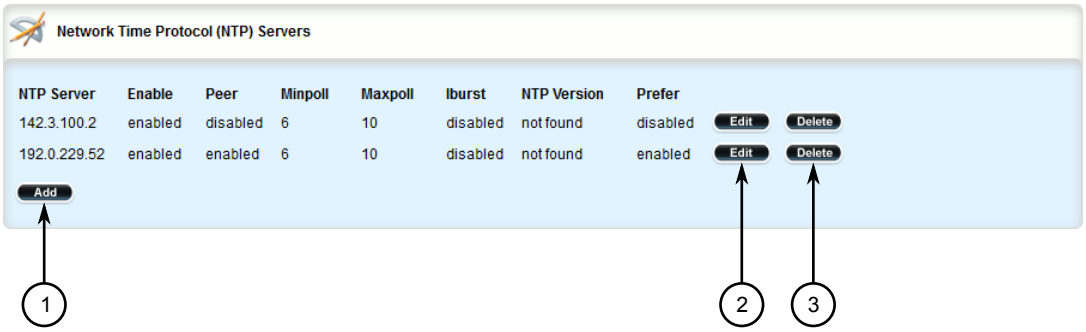


Figure 1164: Network Time Protocol (NTP) Servers Table

1. Add Button **2.** Edit Button **3.** Delete Button

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 17.8.5

Managing Server Keys

Server keys are used to authenticate NTP communications and prevent tampering with NTP timestamps. When using authentication, both the local and remote servers must share the same key and key identifier. Packets sent to and received from the server/peer include authentication fields encrypted using the key.

CONTENTS

Section 17.8.5.1

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.

Figure 1165: Server Keys Table

If no server keys have been configured, add keys as needed. For more information, refer to Section 17.8.5.2, "Adding a Server Key".

Section 17.8.5.2

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.

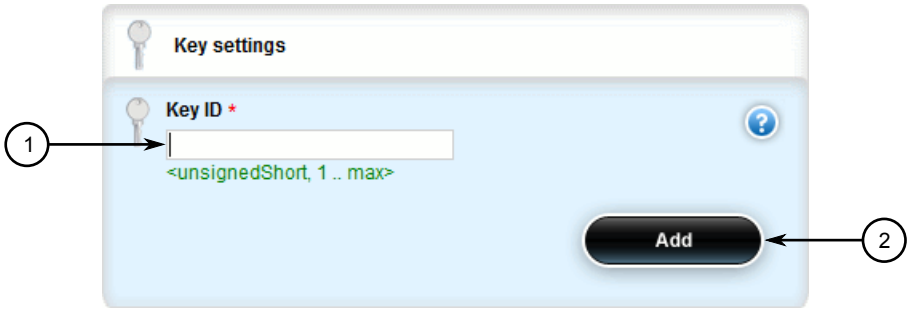


Figure 1166: Key Settings Form

1. Key ID Box **2.** Add Button

3. Configure the following parameter(s) as required:

Parameter	Description
Key ID	**Synopsis:** A 16-bit unsigned integer equaling 1 or higher The name of the key.

4. Click **Add** to create the new key. The **Server Keys** form appears.

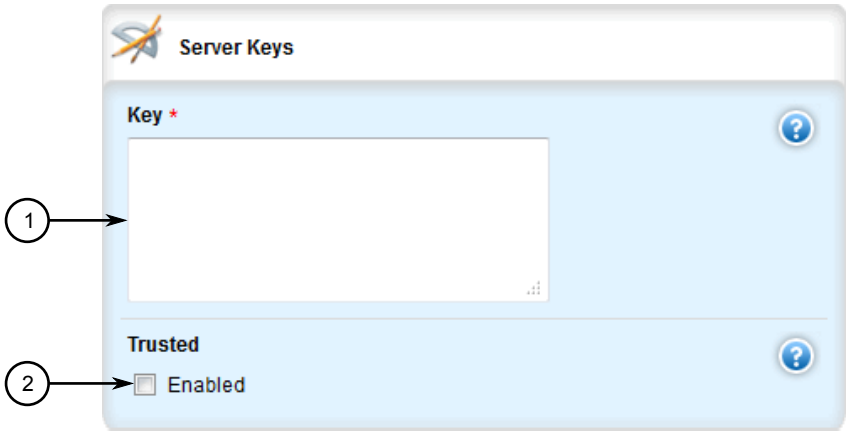


Figure 1167: Server Keys Form

1. Key Box **2.** Trusted Check Box

5. Configure the following parameter(s) as required:

Parameter	Description
Key	**Synopsis:** A string 1 to 1024 characters long The key. This parameter is mandatory.
Trusted	Mark this key as trusted for the purposes of authenticating peers with symmetric key cryptography. The authentication procedures require that both the local and remote servers share the same key and key identifier.

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 17.8.5.3
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.

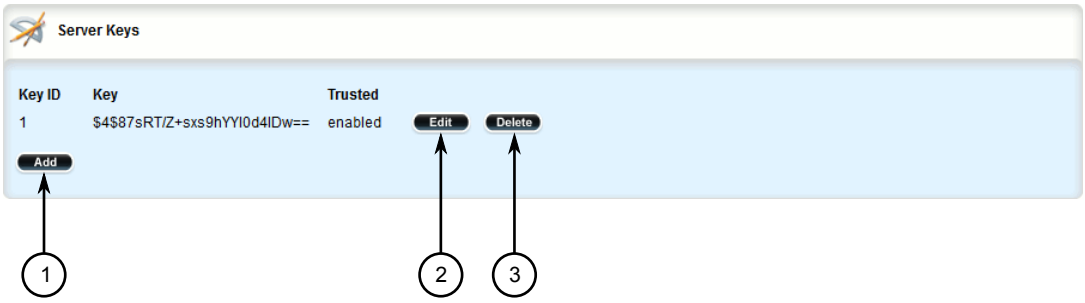


Figure 1168: Server Keys Table

1. Add Button **2.** Edit Button **3.** Delete Button

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 17.8.6
Managing Server Restrictions

Server restrictions control access to the NTP servers.

CONTENTS

Section 17.8.6.1
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.

Figure 1169: Server Restrictions Table

If no server restrictions have been configured, add restrictions as needed. For more information, refer to Section 17.8.6.2, "Adding a Server Restriction".

Section 17.8.6.2
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.

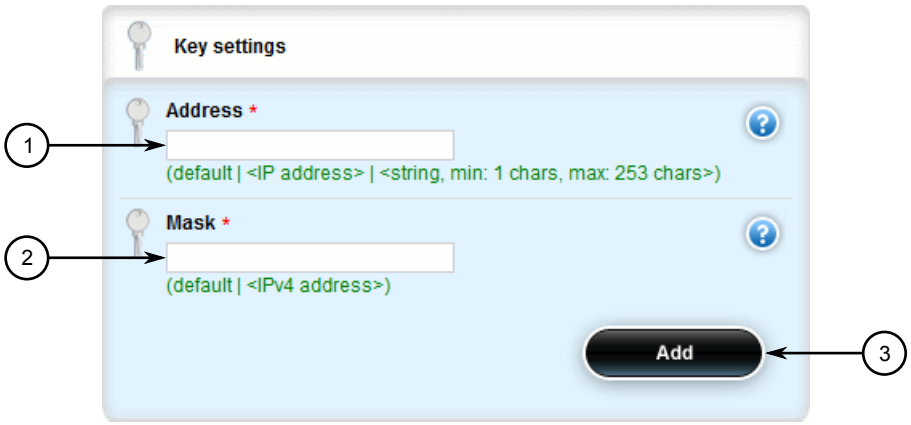


Figure 1170: Key Settings Form

1. Address Box **2.** Mask Box **3.** Add Button

3. Configure the following parameter(s) as required:

Parameter	Description
Address	**Synopsis:** { default } or a string 1 to 253 characters long The address to match. The address can be a host or network IP address or a valid host DNS name.
Mask	**Synopsis:** { default } or a string

Parameter	Description
	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 1171: 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 ntpdc and ntpq, unless the queries come from a local host, or to disable this feature entirely if not required. This prevents DDoS (Distributed Denial of Service) reflection/amplification attacks. Configure the following flags to the restrict default entry: `kod`, `nomodify`, `nopeer`, `noquery` *and* `notrap`.

Parameter	Description
Flags	**Synopsis:** { ignore, kod, limited, lowpriotrap, nomodify, nopeer, noquery, noserve, notrap, notrust, ntpport, version } Flags restrict access to NTP services. An entry with no flags allows free access to the NTP server. • Version: Denies packets that do not match the current NTP version. • ntpport: Matches only if the source port in the packet is the standard NTP UDP port (123). • notrust: Denies service unless the packet is cryptographically authenticated. • notrap: Declines to to provide mode 6 control message trap service to matching hosts. • noserve: Denies all packets except ntpq(8) and ntpdc(8) queries. • noquery: Denies ntpq(8) and ntpdc(8) queries. • nopeer: Denies packets which result in mobilizing a new association. • nomodify: Denies ntpq(8) and ntpdc(8) queries attempting to modify the state of the server; queries returning information are permitted. • lowpriotrap: Declares traps set by matching hosts to be low priority. • limited: Denies service if the packet spacing violates the lower limits specified in the NTP discard setting. • kod: Sends a Kiss-o'-Death (KoD) packet when an access violation occurs. • ignore: Denies all packets.

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 17.8.6.3
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.

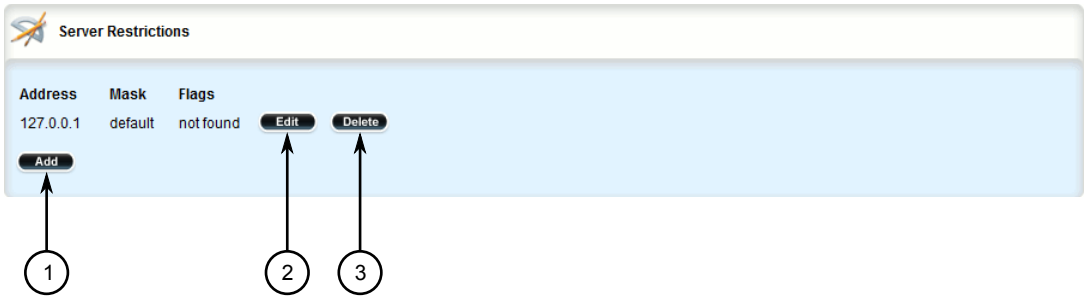


Figure 1172: Server Restrictions Table

1. Add Button **2.** Edit Button **3.** Delete Button

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 17.9
Managing NTP Broadcast/Multicast Clients

Set the device to NTP broadcast or multicast client mode if the NTP server issues regular time-of-day advertisements.

CONTENTS

Section 17.9.1
Enabling and Configuring NTP Multicast Clients

The NTP multicast client enables the NTP server to receive advertisements from other NTP servers.

To enable and configure the NTP multicast client, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to ***services » time » ntp***. The **NTP Multicast Clients** form appears.

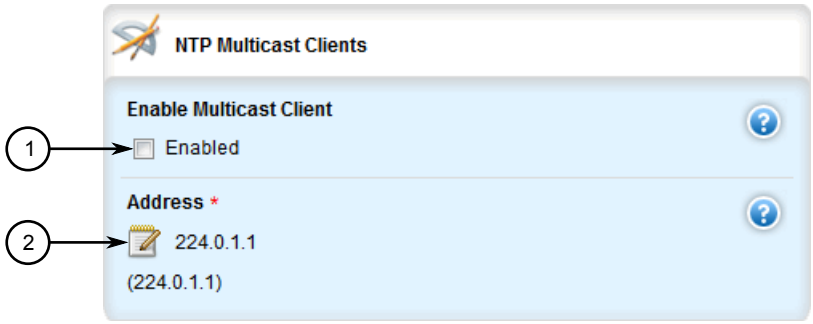


Figure 1173: NTP Multicast Clients Form

1. Enable Mutlicast Client Check Box **2.** Address Box

3. Configure the following parameter(s) as required:

Parameter	Description
Enable Multicast Client	Enables the multicast message mode.
Address	**Synopsis:** A string 1 to 253 characters long **Default:** 224.0.1.1 The multicast address on which the NTP client listens for NTP messages.

4. Add a multicast address for a known NTP server. For more information, refer to Section 17.9.3.2, “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 17.9.2
Enabling and Configuring NTP Broadcast Clients

The NTP broadcast client enables the NTP server to receive advertisements from other NTP servers and send advertisements of its own.

To enable and configure the NTP broadcast client, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to ***services » time » ntp***. The **Network Time Protocol (NTP)** form appears.

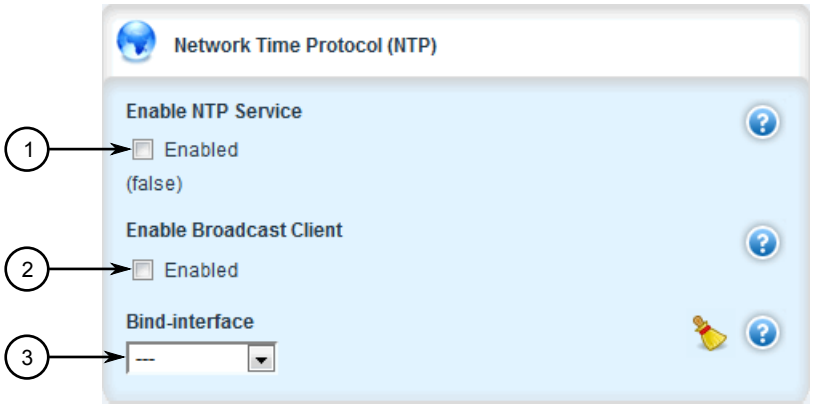


Figure 1174: Network Time Protocol (NTP) Form

1. Enable NTP Service Check Box **2.** Enable Broadcast Client Check Box **3.** Bind Interface List

3. Configure the following parameters as required:

Parameter	Description
Enable Broadcast Client	Enables/disables the broadcast client.

4. Add a broadcast address for a known NTP server. For more information, refer to Section 17.9.3.2, "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 17.9.3

Managing NTP Broadcast/Multicast Addresses

When broadcast or multicast addresses for known NTP servers are configured, the NTP daemon monitors advertisements from each address and chooses the server with the lowest stratum to use as the NTP host. This is opposed to manually configuring a list of servers or peers.

CONTENTS

Section 17.9.3.1

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.

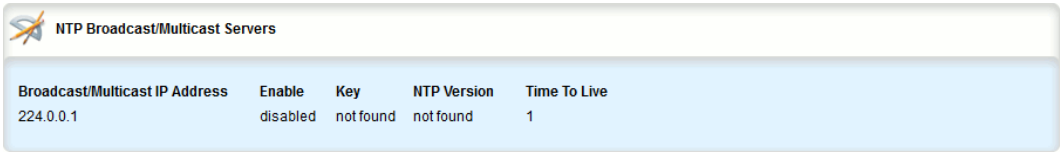


Figure 1175: NTP Broadcast/Multicast Servers Table

If no broadcast/multicast addresses have been configured, add addresses as needed. For more information, refer to Section 17.9.3.2, "Adding a Broadcast/Multicast Address".

Section 17.9.3.2
Adding a Broadcast/Multicast Address

To add a broadcast/multicast address for an NTP server, do the following:

IMPORTANT!
It is strongly recommended to enable NTP authentication, unless all hosts on the network are trusted.

1. 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 17.8.5.2, "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 1176: 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	**Synopsis:** 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.

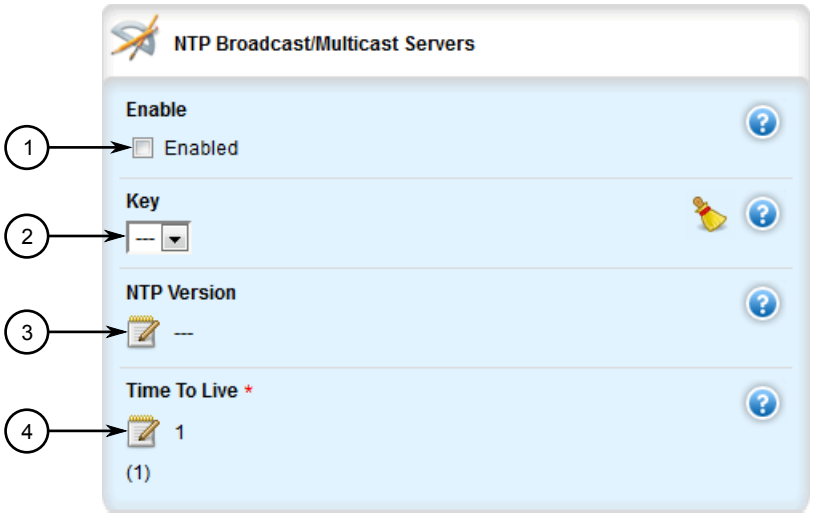


Figure 1177: NTP Broadcast/Multicast Servers Form

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	Enables sending broadcast or multicast NTP messages to this address.
Key	**Synopsis:** A string Authentication key.
NTP Version	**Synopsis:** A 32-bit signed integer between 1 and 4 The version of the NTP protocol used to communicate with this host. Change this only if it is known that the host requires a version other than 4.
Time To Live	**Synopsis:** An 8-bit unsigned integer between 1 and 127 **Default:** 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 17.9.3.3
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.

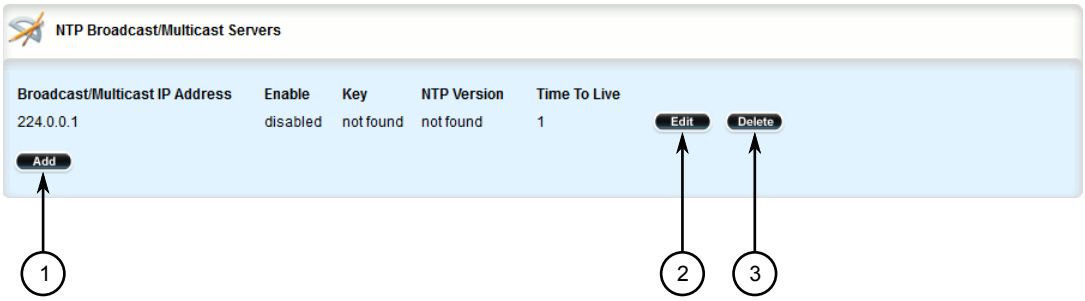


Figure 1178: NTP Broadcast/Multicast Servers Table

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.

18 Applications

Applications are special add-ons that extend the functionality of RUGGEDCOM ROX II, such as enhanced support for other RUGGEDCOM products (e.g. RUGGEDCOM CROSSBOW). They are installed and upgraded the same as the RUGGEDCOM ROX II operating system, in that they are first installed on the inactive partition and are only activated after a reboot. This makes it possible to decline or undo the installation if the application creates undesirable results. The currently active partition is also unaffected when an application is being installed or upgraded.

All RUGGEDCOM ROX II applications are released as repositories and must be hosted by an upgrade server. For more information about setting up an upgrade server, refer to Section 4.12.2, "Setting Up an Upgrade Server".

CONTENTS

Section 18.1

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.

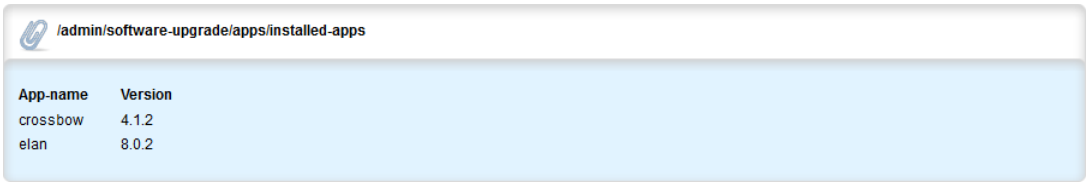


Figure 1179: Installed Apps Table

If no applications have been installed, install applications as needed. For more information, refer to Section 18.2, "Installing an Application".

Section 18.2
Installing an Application

To install an application, do the following:

1. 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 18.5.3, "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.

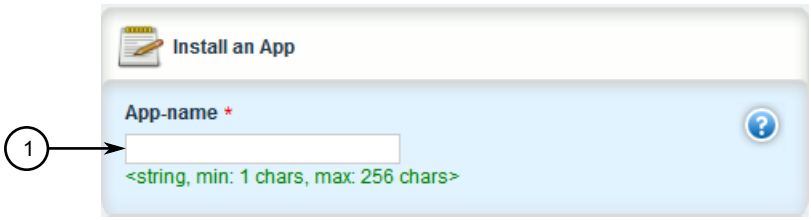


Figure 1180: Install App Form

1. App Name Box

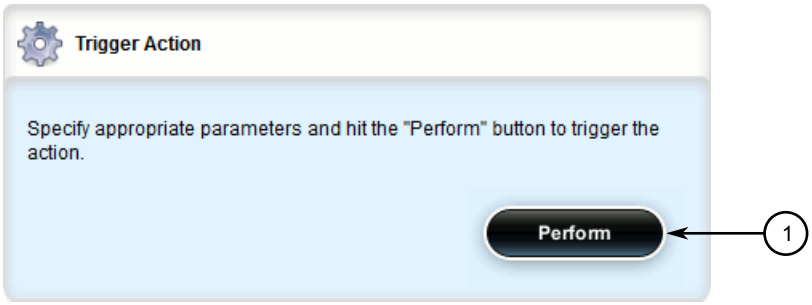


Figure 1181: Trigger Action Form

1. Perform Button

4. On the **Install Apps** form, configure the following parameters:

Parameter	Description
App Name	**Synopsis:** A string 1 to 256 characters long 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. This parameter is mandatory.

5. On the **Trigger Action** form, click **Perform**.

Section 18.3

Upgrading an Application

To upgrade an application, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to ***admin » software-upgrade » apps*** and click **upgrade-app** in the menu. The **Upgrade an App** and **Trigger Action** forms appear.

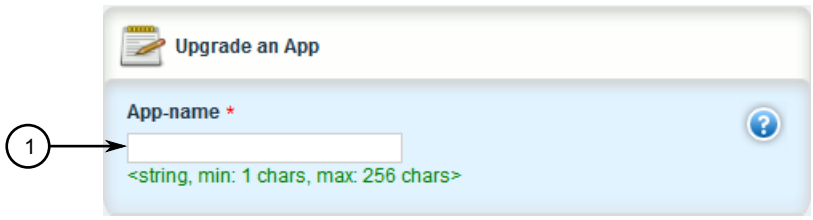


Figure 1182: Upgrade an App Form

1. App Name Box

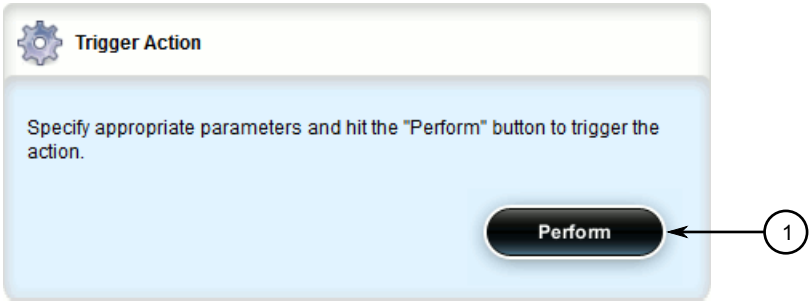


Figure 1183: Trigger Action Form

1. Perform Button

3. On the **Upgrade Apps** form, configure the following parameters:

Parameter	Description
App Name	**Synopsis:** 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. This parameter is mandatory.

4. On the **Trigger Action** form, click **Perform**.

Section 18.4

Uninstalling an Application

To uninstall an application, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to ***admin » software-upgrade » apps*** and click **uninstall-app** in the menu. The **Uninstall Apps** and **Trigger Action** forms appear.

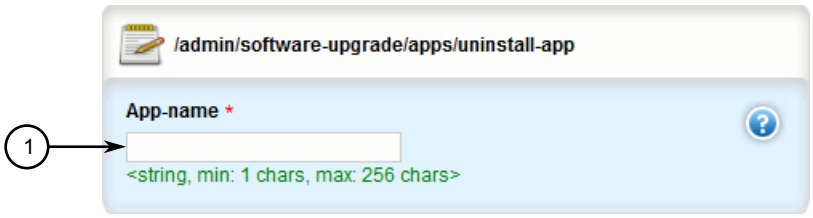


Figure 1184: Uninstall Apps Form

1. App Name Box

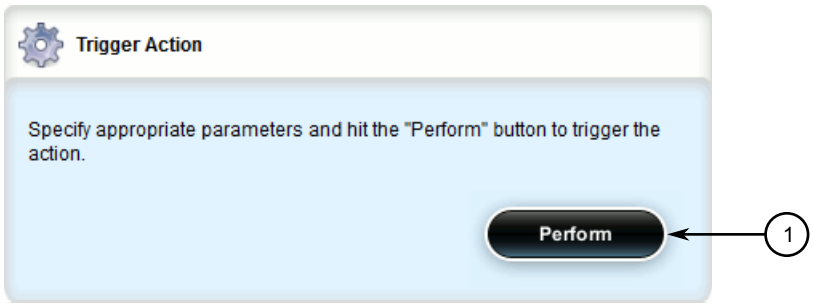


Figure 1185: Trigger Action Form

1. Perform Button

3. On the **Uninstall Apps** form, configure the following parameters:

Parameter	Description
App Name	**Synopsis:** A string 1 to 256 characters long 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. This parameter is mandatory.

4. On the **Trigger Action** form, click **Perform**.

Section 18.5
Managing Application Repositories

Before any RUGGEDCOM ROX II application can be installed or upgraded, a connection to its repository on the upgrade server must be configured.

CONTENTS

Section 18.5.1
Viewing a List of Repositories

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.

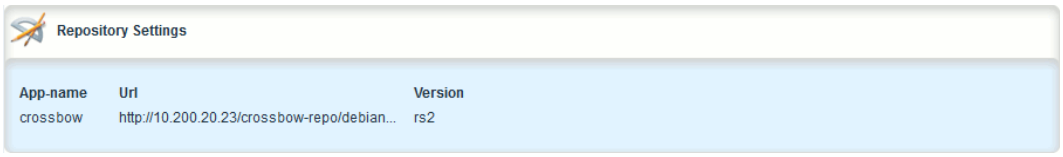


Figure 1186: Repository Settings Table

If no repositories have been configured, add repositories as needed. For more information, refer to Section 18.5.3, "Adding a Repository".

Section 18.5.2
Checking the Repository Connection

To check the connection with a repository, 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.

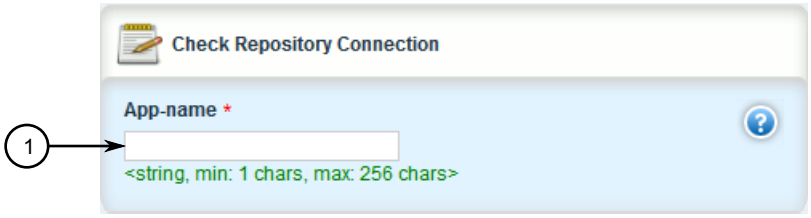


Figure 1187: Check Repository Connection Form

1. App Name Box

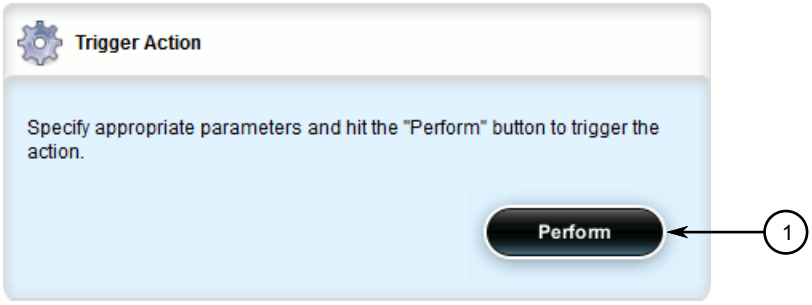


Figure 1188: Trigger Action Form

1. Perform Button

2. On the **Check Repository Connection** form, configure the following parameters:

Parameter	Description
App Name	**Synopsis:** A string 1 to 256 characters long 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. This parameter is mandatory.

3. On the **Trigger Action** form, click **Perform**. The connection results are displayed.

Section 18.5.3

Adding a Repository

To add an application repository, do the following:

NOTE
An application repository must be configured before an application can be installed or upgraded.

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to ***admin » software-upgrade » apps » repository*** and click **<Add repository>**. The **Key Settings** form appears.

Figure 1189: Key Settings Form

1. App Name Box **2.** Add Button

3. Configure the following parameter(s) as required:

Parameter	Description
App Name	**Synopsis:** 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.

4. Click **Add** to create the repository connection. The **Repository** form appears.

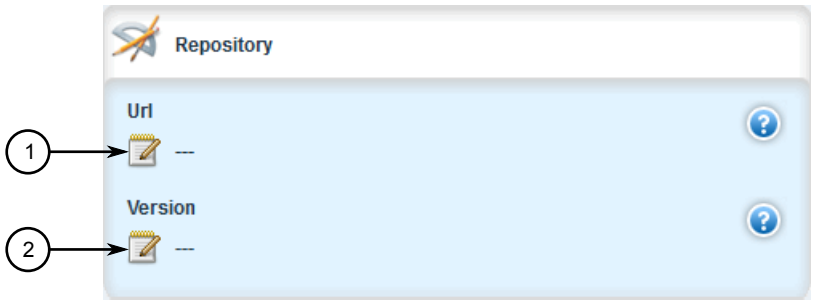


Figure 1190: Repository Form

1. URL Box **2.** Version Box

5. Configure the following parameter(s) as required:

Parameter	Description
url	**Synopsis:** A string 1 to 1024 characters long The URL of the upgrade server hosting the app repository (http, https, and ftp are supported).
version	**Synopsis:** 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 18.5.4

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.

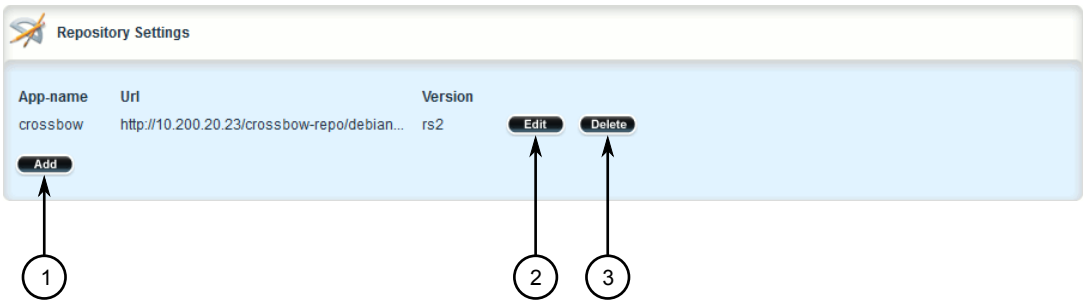


Figure 1191: Repository Settings Table

1. Add Button **2.** Edit Button **3.** Delete Button

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 18.6

Managing the RUGGEDCOM CROSSBOW Application

CROSSBOW is part of the RUGGEDCOM family of communications products. It was developed to address the need to interactively and securely access remote field devices to perform maintenance, configuration, and data retrieval functions.

CROSSBOW allows a device maintenance application on a client PC to communicate with its associated devices remotely, as if the user's PC was directly connected to the end device.

The RUGGEDCOM CROSSBOW application enables a RUGGEDCOM ROX II device to launch a device maintenance application at the facility level. This is referred to as a Station Access Controller or SAC. A SAC is a local version of the primary CROSSBOW Server, which is located at a remote site. During normal operation, communications occur as usual between the remote CROSSBOW Server (the enterprise server) and the devices within the facility. However, if network connectivity is lost, or if the network speed makes it impractical for an on-site operator to use the enterprise server connection, a user can launch CROSSBOW Client from within the facility, connect to the SAC, and restore access to all of the facility's devices using their usual RUGGEDCOM CROSSBOW interface.

Operations initiated via the SAC are logged and can be uploaded to the enterprise server database after the network connection is restored. The SAC appears as a device in the Device View in the main RUGGEDCOM CROSSBOW database.

NOTE
For more information about RUGGEDCOM CROSSBOW, refer to the technical documentation provided with the product.

CONTENTS

Section 18.6.1

Enabling/Disabling CROSSBOW

To enable or disable communication with a RUGGEDCOM CROSSBOW system, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to ***apps » crossbow***. The **CROSSBOW** form appears.

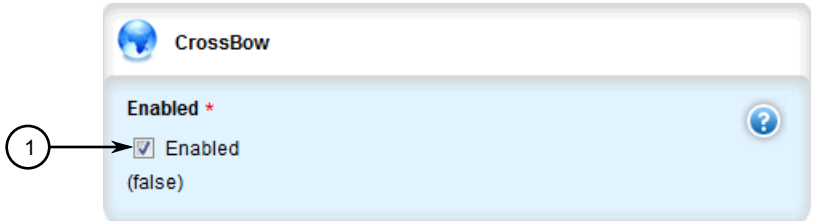


Figure 1192: CROSSBOW Form

1. Enabled Check Box

3. Configure the following parameter(s) as required:

Parameter	Description
enabled	**Synopsis:** { true, false } **Default:** false Enables crossbow.

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 18.6.2

Configuring the Client Connection

To configure the client connection for RUGGEDCOM CROSSBOW, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to ***apps » crossbow » client-connection***. The **Client Connection Info** form appears.

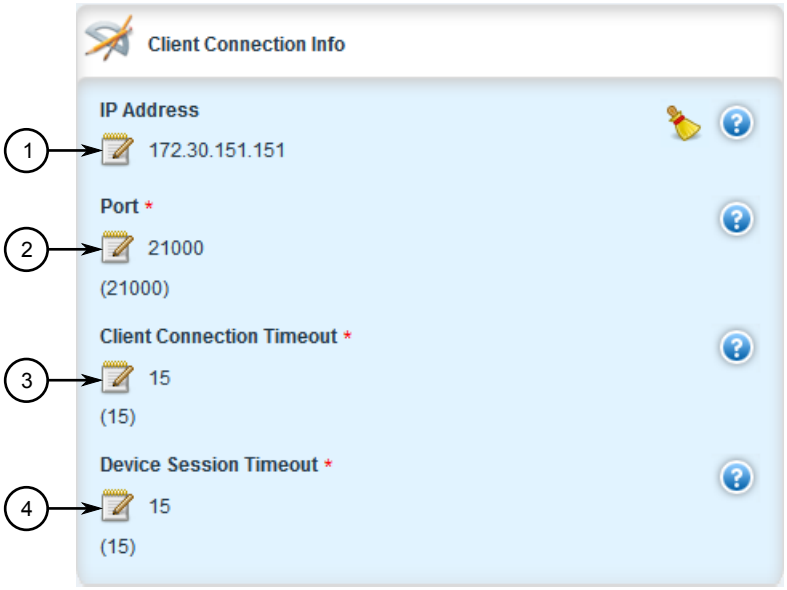


Figure 1193: Client Connection Info Form

1. IP Address Box **2.** Port Box **3.** Client Connection Timeout Box **4.** Device Sessions Timeout Box

3. Configure the following parameter(s) as required:

Parameter	Description
ipaddr	**Synopsis:** A string 7 to 15 characters long or a string 6 to 40 characters long The IP address to which a client will connect to the Station Access Controller (SAC).
port	**Synopsis:** A 16-bit unsigned integer between 0 and 65535 **Default:** 21000 The TCP port to which a client will connect to the Station Access Controller (SAC).
ClientConnectionTimeout	**Synopsis:** A 32-bit unsigned integer **Default:** 15 The Client Connection Timeout in minutes (set to 0 for no timeout).
DeviceSessionTimeout	**Synopsis:** A 32-bit unsigned integer **Default:** 15 The Device Session Timeout in minutes (set to 0 for no timeout).

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 18.6.3

Configuring CROSSBOW Certificates and Private Keys

To configure a certificate and and private key for RUGGEDCOM CROSSBOW, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Add a certificate. For more information, refer to Section 6.7.7.3, "Adding a Certificate".
3. Add a private key. For more information, refer to Section 6.7.5.2, "Adding a Private Key".
4. Navigate to ***apps » CROSSBOW » certificate***. The **Certificates Info** forms appear.

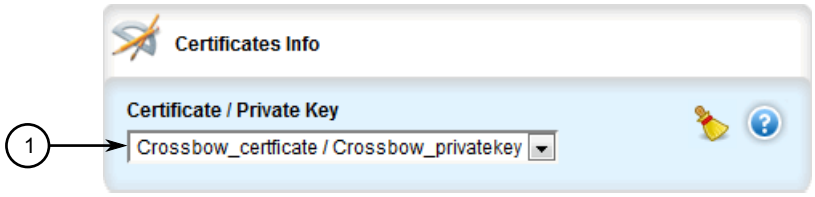


Figure 1194: Certificates Info Form

1. Certificate/Private Key List

5. Configure the following parameters as required:

Parameter	Description
cert	**Synopsis:** A string The certificate name and associated private key.
cert-private-key	**Synopsis:** A string The private key associated with certificate.

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 18.6.4

Managing SAC Connections

This section describes how to configure and manage Station Access Controller (SAC) connections for RUGGEDCOM CROSSBOW.

CONTENTS

Section 18.6.4.1
Viewing a List of SAC Connections

To view a list of SAC connections, navigate to ***apps » crossbow » sac-connection***. If SAC connections have been configured, the **SAC Connection List** table appears.

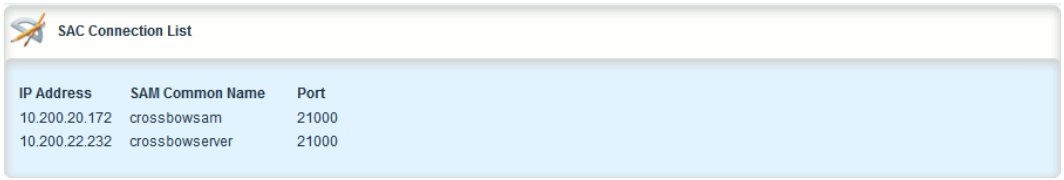


Figure 1195: SAC Connection List Table

If no SAC connections have been configured, add connections as needed. For more information, refer to Section 18.6.4.2, "Adding a SAC Connection".

Section 18.6.4.2
Adding a SAC Connection

To add a SAC connection, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to ***apps » crossbow » sac-connection » Add connection-list***. The **Key Settings** form appears.

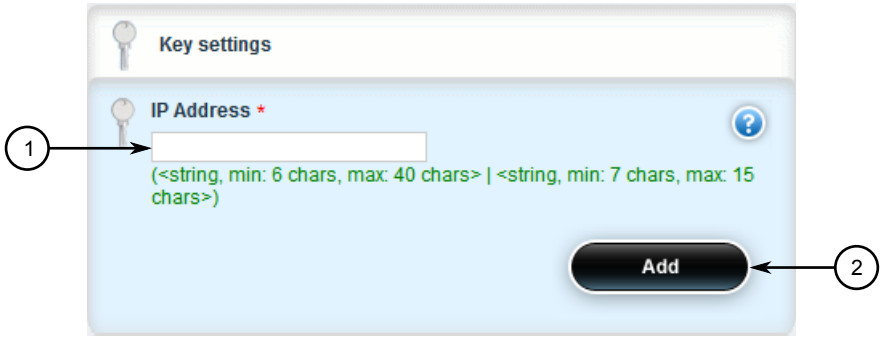


Figure 1196: Key Settings Form

1. IP Address Box

3. Configure the following parameter(s) as required:

Parameter	Description
sam-ipaddr	**Synopsis:** A string 7 to 15 characters long or a string 6 to 40 characters long The IP address of Secure Access Manager (SAM - parent of SAC) to which the Station Access Controller (SAC) will connect.

4. Click **Add** to add the connection. The **SAC Connection List** form appears.

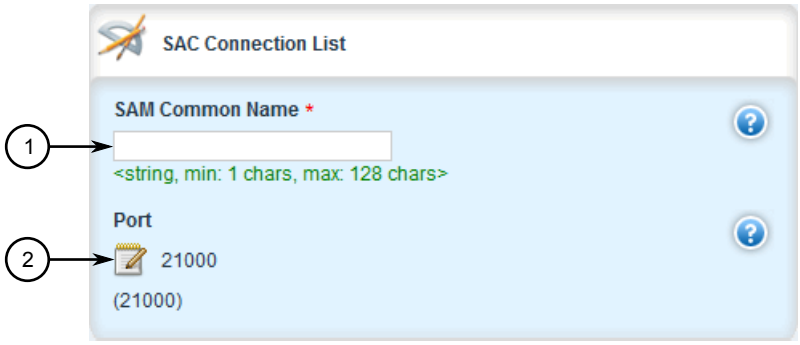


Figure 1197: SAC Connection List Form

1. SAM Common Name Box **2.** Port Box

5. Configure the following parameter(s) as required:

Parameter	Description
sam-ipaddr	**Synopsis:** A string 7 to 15 characters long or a string 6 to 40 characters long The IP address of Secure Access Manager (SAM - parent of SAC) to which the Station Access Controller (SAC) will connect.
sam-name	**Synopsis:** A string 1 to 128 characters long The common name in the certificate that the Secure Access Manager (SAM - parent of SAC) will present when mutually authenticating with the Station Access Controller (SAC). This parameter is mandatory.
sam-port	**Synopsis:** A 16-bit unsigned integer between 0 and 65535 **Default:** 21000 The TCP port of SAM (parent of SAC) to which SAC (Station Access Controller) will connect.

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 18.6.4.3
Deleting a SAC Connection

To delete a SAC connection, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to ***apps » crossbow » sac-connection***. The **SAC Connection List** table appears.

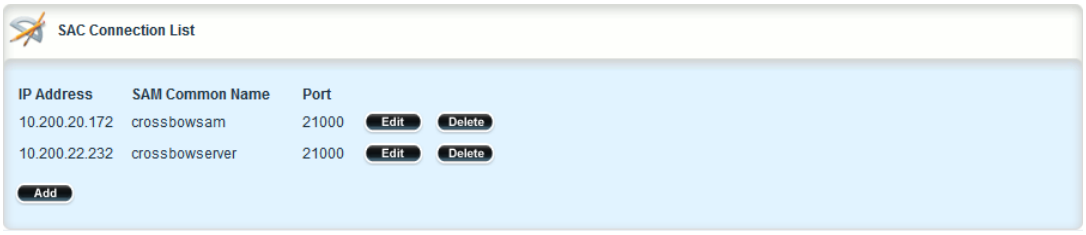


Figure 1198: SAC Connection List Table

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 18.6.5

Managing CROSSBOW CA Certificate Lists

This section describes how to configure CA (Certified Authority) certificates for the RUGGEDCOM CROSSBOW application.

CONTENTS

Section 18.6.5.1

Viewing a List of RUGGEDCOM CROSSBOW Certificate Lists

To view a list of CA certificate lists configured for the RUGGEDCOM CROSSBOW application, navigate to ***apps » crossbow » certificate » ca-cert-list***. If CA certificate lists have been configured, the **CA Certificate List** table appears.

Figure 1199: CA Certificate List Table

If no CA certificate lists have been configured, add lists as needed. For more information, refer to Section 18.6.5.2, "Adding a CA Certificate List".

Section 18.6.5.2
Adding a CA Certificate List

To add a CA certificate list for the RUGGEDCOM CROSSBOW application, do the following:

1. Make sure the required CA (Certified Authority) certificate has been added to the device. For more information, refer to Section 6.7.4.3, "Adding a CA Certificate and CRL".
2. Change the mode to **Edit Private** or **Edit Exclusive**.
3. Navigate to ***apps » crossbow » certificate » ca-cert-list*** and click **<Add ca-cert-list>**. The **Key Settings** form appears.

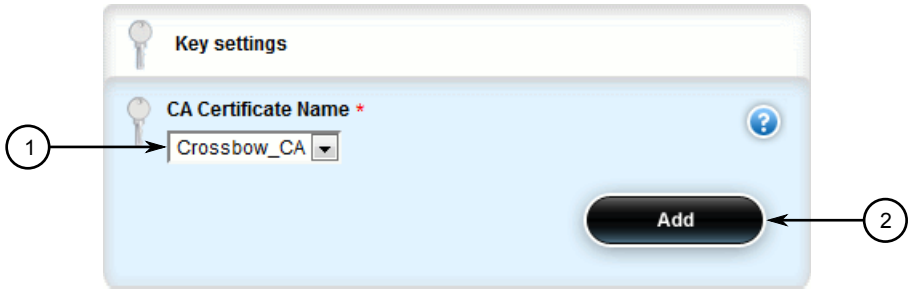


Figure 1200: Key Settings Form

1. CA Certificate Name **2.** Add Button

4. Configure the following parameter(s) as required:

Parameter	Description
name	**Synopsis:** A string The Certificate Authority (CA) certificate name.

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 18.6.5.3
Deleting a CA Certificate List

To delete a CA certificate list for the RUGGEDCOM CROSSBOW application, do the following:

1. Change the mode to **Edit Private** or **Edit Exclusive**.
2. Navigate to ***apps » crossbow » certificate » ca-cert-list***. The **CA Certificate List** table appears.

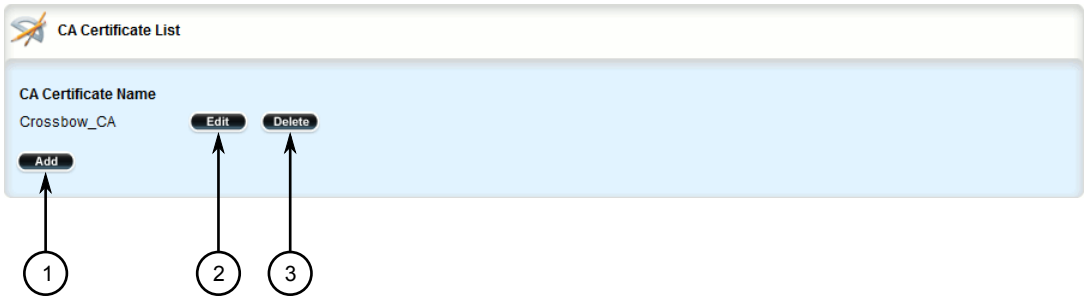


Figure 1201: CA Certificate List Table

1. Add Button **2.** Edit Button **3.** Delete Button

3. Click **Delete** next to the chosen CA certificate 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 18.6.6
Viewing the Status of RUGGEDCOM CROSSBOW

To view the status of RUGGEDCOM CROSSBOW, navigate to ***apps » crossbow » status***. The **Status** form appears.

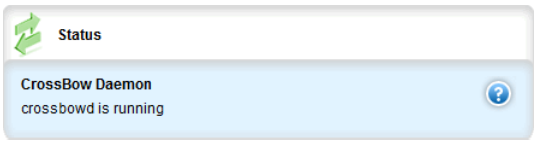


Figure 1202: Status Form

Section 18.6.7
Viewing the RUGGEDCOM CROSSBOW Log

To view the RUGGEDCOM CROSSBOW log , do the following:

1. Navigate to ***apps » crossbow » status*** and click **log** in the menu. The **Trigger Action** form appears.

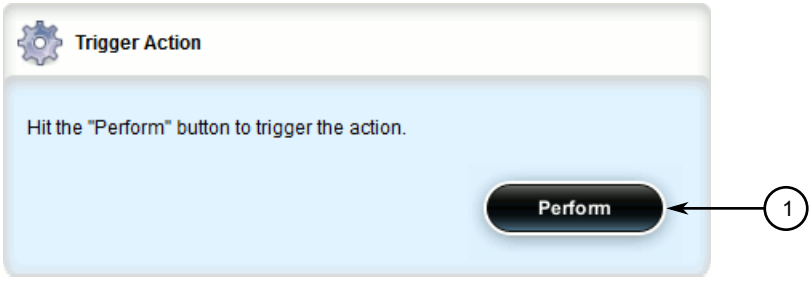


Figure 1203: Trigger Action Form

1. Perform Button

2. Click **Perform**. The **Log** form appears.

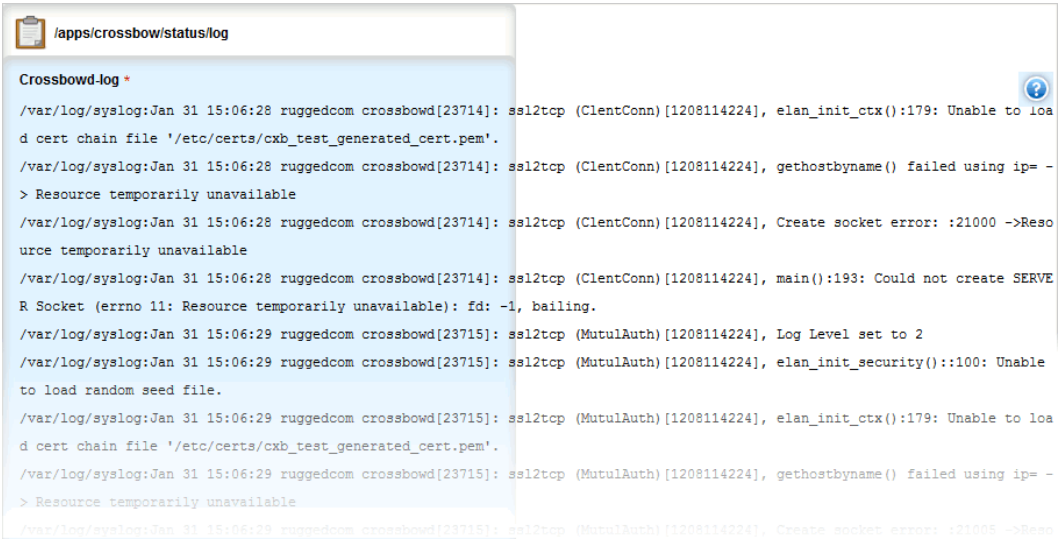


Figure 1204: Log Form

19 Troubleshooting

This chapter describes troubleshooting steps for common issues that may be encountered when using RUGGEDCOM ROX II or designing a network. It describes the following tasks:

IMPORTANT!
For further assistance, contact Siemens Customer Support.

NOTE
For a description of pre-configured alarms, refer to Section 5.7.1, "Pre-Configured Alarms".

CONTENTS

Section 19.1

Feature Keys

The following describes common problems related to feature keys.

Problem	Solution
A file-based feature key does not match the hardware	Each file-based feature key is licensed to a particular device. When transferring a feature key from one device to another, such as when configuring a backup unit to replace a malfunctioning device, the device will detect a hardware mismatch with the key and trigger an alarm. Do not transfer file-based feature keys between devices. Contact a Siemens Canada Ltd sales representative to order a feature key matching the serial numbers of the hardware in the destination device.

Section 19.2

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.	A possible cause of intermittent operation is that of a *duplex mismatch*. If one end of the link is fixed to full-duplex and the peer auto-negotiates, the auto-negotiating end falls back to half-duplex operation. At lower traffic volumes, the link may display few if any errors. As the traffic volume rises, the fixed negotiation side will begin to experience dropped packets while the auto-negotiating side will experience collisions. Ultimately, as traffic loads approach 100%, the link will become entirely unusable. The ping command with flood options is a useful tool for testing commissioned links. The command **`ping`** `192.168.0.1 500 2` can be used to issue 500 pings each separated by two milliseconds to the next switch. If the link used is of high quality, then no pings should be lost and the average round trip time should be small.
Links are inaccessible, even when using the Link Fault Indication (LFI) protection feature.	Make sure LFI is not enabled on the peer as well. If both sides of the link have LFI enabled, then both sides will withhold link signal generation from each other.

Section 19.3
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.	Is the port used to connect the router included in the Router Ports list? To determine whether the multicast stream is being delivered to the router, view the statistics collected for switched Ethernet ports. For more information, refer to Section 8.1.3, "Viewing Switched Ethernet Port Statistics". Verify the traffic count transmitted to the router is the same as the traffic count received from the multicasting source.
The video stream at an end station is of poor quality.	Video serving is a resource-intensive application. Because it uses isochronous workload, data must be fed at a prescribed rate or end users will see glitches in the video. Networks that carry data from the server to the client must be engineered to handle this heavy, isochronous workload. Video streams can consume large amounts of bandwidth. Features and capacity of both server and network (including routers, bridges, switches and interfaces) impact the streams. Do not exceed 60% of the maximum interface bandwidth. For example, if using a 10 Mbps Ethernet, run a single multicasting source at no more than 6 Mbps, or two sources at 3 Mbps. It is important to consider these ports in the network design, as router ports will carry the traffic of all multicast groups. **IMPORTANT!** *Multicasting will introduce latency in all traffic on the network. Plan the network carefully in order to account for capacity and latency concerns.*
Multicast streams of some groups are not forwarded properly. Some segments without subscribers receive the traffic, while some segments with subscribers do not.	Make sure different multicast groups do not have multicast IP addresses that map to the same multicast MAC address. The switch forwarding operation is MAC address-based and will not work properly for several groups mapping to the same MAC address.
Computers on the switch issue join requests, but do not receive multicast streams from a router.	Is the multicast route running IGMP version 2? It must run IGMP version 2 in order for IGMP Snooping to operate properly.

Problem	Solution
Unable to connect or disconnect some switch ports, and multicast goes everywhere. Is IGMP broken?	IGMP is not broken. This may in fact be proper switch behavior. When the switch detects a change in the network topology through RSTP, it acts to avoid loss of multicast traffic. If configured to do so, it starts forwarding all multicast traffic to all ports that are not RSTP Edge ports (because they may potentially link to routers). This may result in some undesired flooding of multicast traffic, which will stop after a few minutes. However, it guarantees that all devices interested in the traffic will keep receiving it without interruption. The same behavior will be observed when the switch resets or when IGMP Snooping is being disabled for the VLAN.

Section 19.4
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.	If one of the switches appears to flip the root from one port to another, the problem may be one of traffic prioritization. For more information refer to The network becomes unstable when a specific application is started. Another possible cause of intermittent operation is that of an auto-negotiation mismatch. If one end of the link is fixed to full-duplex mode and the peer auto-negotiates, the auto-negotiating end will fall back to half-duplex operation. At lower traffic, the volumes the link may display few if any errors. As the traffic volume rises, the fixed negotiation side will begin to experience dropped packets while the auto-negotiating side will experience collisions. Ultimately, as traffic loads approach 100%, the link will become entirely unusable. At this point, RSTP will not be able to transmit configuration messages over the link and the spanning tree topology will break down. If an alternate trunk exists, RSTP will activate it in the place of the congested port. Since activation of the alternate port often relieves the congested port of its traffic, the congested port will once again become reliable. RSTP will promptly enter it back into service, beginning the cycle once again. The root port will flip back and forth between two ports on the switch.
A computer or device is connected to a switch. After the switch is reset, it takes a long time for it to come up.	Is it possible that the RSTP edge setting for this port is set to false? If Edge is set to false, the bridge will make the port go through two forward delay times before the port can send or receive frames. If Edge is set to true, the bridge will transition the port directly to forwarding upon link up. Another possible explanation is that some links in the network run in half-duplex mode. RSTP uses a peer-to-peer protocol called Proposal-Agreement to ensure transitioning in the event of a link failure. This protocol requires full-duplex operation. When RSTP detects a non-full duplex port, it cannot rely on Proposal-Agreement protocol and must make the port transition the slow (i.e. STP) way. If possible, configure the port for full-duplex operation. Otherwise, configure the port's point-to-point setting to true. Either one will allow the Proposal-Agreement protocol to be used.
When the switch is tested by deliberately breaking a link, it takes a long time before devices beyond the switch can be polled.	Is it possible that some ports participating in the topology have been configured to STP mode or that the port's point-to-point parameter is set to false? STP and multi-point ports converge slowly after failures occur.

Problem	Solution
	Is it possible that the port has migrated to STP? If the port is connected to the LAN segment by shared media and STP bridges are connected to that media, then convergence after link failure will be slow. Delays on the order of tens or hundreds of milliseconds can result in circumstances where the link broken is the sole link to the root bridge and the secondary root bridge is poorly chosen. The worst of all possible designs occurs when the secondary root bridge is located at the farthest edge of the network from the root. In this case, a configuration message will have to propagate out to the edge and then back in order to reestablish the topology.
The network is composed of a ring of bridges, of which two (connected to each other) are managed and the rest are unmanaged. Why does the RSTP protocol work quickly when a link is broken between the managed bridges, but not in the unmanaged bridge part of the ring?	A properly operating unmanaged bridge is transparent to STP configuration messages. The managed bridges will exchange configuration messages through the unmanaged bridge part of the ring as if it is non-existent. When a link in the unmanaged part of the ring fails however, the managed bridges will only be able to detect the failure through timing out of hello messages. Full connectivity will require three hello times plus two forwarding times to be restored.
The network becomes unstable when a specific application is started. The network returns to normal when the application is stopped.	RSTP sends its configuration messages using the highest possible priority level. If CoS is configured to allow traffic flows at the highest priority level and these traffic flows burst continuously to 100% of the line bandwidth, STP may be disrupted. It is therefore advised not to use the highest CoS.
When a new port is brought up, the root moves on to that port instead of the port it should move to or stay on.	Is it possible that the port cost is incorrectly programmed or that auto-negotiation derives an undesired value? Inspect the port and path costs with each port active as root.
An IED/controller does not work with the device.	Certain low CPU bandwidth controllers have been found to behave less than perfectly when they receive unexpected traffic. Try disabling STP for the port. If the controller fails around the time of a link outage, there is the remote possibility that frame disordering or duplication may be the cause of the problem. Try setting the root port of the failing controller's bridge to STP.
Polls to other devices are occasionally lost.	Review the network statistics to determine whether the root bridge is receiving TCNs around the time of observed frame loss. It may be possible there are problems with intermittent links in the network.
The root is receiving a number of TCNs. Where are they coming from?	Examine the RSTP port statistics to determine the port from which the TCNs are arriving. Sign-on to the switch at the other end of the link attached to that port. Repeat this step until the switch generating the TCNs is found (i.e. the switch that is itself not receiving a large number of TCNs). Determine the problem at that switch.

Section 19.5
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 *edge* and leave the native VLAN set to 1. This is the default configuration for the switch.
Two VLANs were created and a number of ports were made members of them. Now some of the devices in one VLAN need to send messages to devices in the other VLAN.	If the devices need to communicate at the physical address layer, they must be members of the same VLAN. If they can communicate in a Layer 3 fashion (i.e. using a protocol such as IP or IPX), use a router. The router will treat each VLAN as a separate interface, which will have its own associated IP address space.

Section 19.6

Firmware Updates

The following describes common errors and possible solutions related to firmware updates. If further assistance is needed, contact Siemens Customer Support.

Error Message	Solution
unknown firmware image file	The firmware image is not valid for the modem installed in the device, or the firmware download is accidentally interrupted. Check the connectivity between the device and the remote server. Make sure the connectivity is reliable.
mis-matched carrier	The new firmware is not targeted to the modem currently installed in the device. Check the firmware file name in the version information file. Make sure the file name has PRI ID of modem installed in the device. Manually download the firmware to the device, then execute qmi-firware-update command to determine what carrier the firmware is targeting. See command and option in (*).
url connection/downloading failure	The device is not able to reach the remote host server based on the URL configuration. Or, the version information file or firmware file is not found on the remote server. Check the URL configuration, and make sure the remote server is reachable. Check the path of the URL configuration. Make sure the new firmware file is in the correct location in the remote server.
invalid firmware information	The version information file name or firmware file name does not exist in server. Check the existence of the version information file name and firmware file name in remote server.
Unspecified error.	Check the syslog for more details.