SIEMENS

RUGGEDCOM ROX II v2.6

User Guide

For RX1500, RX1501, RX1510, RX1511, RX1512

12/2014

RC1155-EN-02

Disclaimer Of Liability

Siemens has verified the contents of this manual 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

ROX™, Rugged Operating System On Linux™, CrossBow™ and ELAN™ are trademarks of Siemens Canada Ltd.. ROS® is a registered trademark of Siemens Canada Ltd..

Linux® is the registered trademark of Linus Torvalds in the U.S. 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® and RUGGEDCOM ROX II are made available under the terms of the GNU General Public License Version 2.0 [http://www.gnu.org/licenses/gpl-2.0.html].

Security Information

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

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

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

Warranty

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

For warranty details, visit www.siemens.com/ruggedcom 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

www.siemens.com/ruggedcom

Table of Contents

Preface

This guide describes the CLI user interface for ROX II v2.6 running on the RUGGEDCOM RX1500 family of products. 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.

Conventions

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

Alerts

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

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

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

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

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

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

CLI Command Syntax

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

Example	Description
`command`	Commands are in bold.

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

Related Documents

Other documents that may be of interest include:

- *RUGGEDCOM RX1500 Installation Guide*
- *RUGGEDCOM RX1500 Data Sheet*
- *RUGGEDCOM Fiber Guide*
- *RUGGEDCOM Wireless Guide*
- *White Paper: Rapid Spanning Tree in Industrial Networks*

System Requirements

Each workstation used to connect to the ROX II Rugged CLI interface must meet the following system requirements:

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

Accessing Documentation

The latest Hardware Installation Guides and Software User Guides for most RUGGEDCOM products are available online at www.siemens.com/ruggedcom.

For any questions about the documentation or for assistance finding a specific document, contact a Siemens sales representative.

Training

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

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

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

For more information about training services and course availability, visit 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, manuals, and much more
  - Submit SRs or check on the status of an existing SR
  - Find and contact a local contact person
  - Ask questions or share knowledge with fellow Siemens customers and the support community
  - And much more...

1 Introduction

Welcome to the RUGGEDCOM ROX II (Rugged Operating System on Linux®) v2.6 User Guide for the RX1500. This document details how to configure the RX1500 via the ROX II Command Line Interface (CLI). ROX II also features a Web interface, which is described in a separate User Guide.

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

The following sections provide more detail about ROX II:

- Section 1.1, “Features and Benefits”
- Section 1.2, “Feature Keys”
- Section 1.3, “Security Recommendations”
- Section 1.4, “Available Services by Port”
- Section 1.5, “User Permissions”

Section 1.1

Features and Benefits

Feature support in 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 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 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. 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. 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. ROX II supports 802.1Q tagged Ethernet frames and VLAN trunks. Port based classification allows legacy devices to be assigned to the correct VLAN. GVRP support is also provided to simplify the configuration of the switches on the VLAN.

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

  SNMP provides a standardized method, for network management stations, to interrogate devices from different vendors. SNMP versions supported by ROX II are v1, v2c and v3. SNMPv3 in particular provides security features (such as authentication, privacy, and access control) not present in earlier SNMP versions. 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 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 ROX II, refer to the *RUGGEDCOM ROX II NETCONF Reference Guide* available on www.siemens.com/ruggedcom.

- **NTP (Network Time Protocol)**

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

- **Port Rate Limiting**

  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. ROX II limits this by filtering broadcast frames with a user-defined threshold.

- **Port Mirroring**

  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**

  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)**

  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**

  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**

  ROX II provides a simple, intuitive user interface for configuration and monitoring via a standard graphical Web browser or via a standard telcom user interface. All system parameters include detailed online help to make setup a breeze. 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 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.

- **Secure Software Upgrade**

  ADD CONTENT

- **USB Mass Storage**

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

  - Configure ROX II from the USB — Configure ROX II to read configuration files and feature keys from the USB Mass Storage drive on startup, rather than any local files saved on the device. This allows for quick, portable configuration of any ROX II device.
  - Upgrade/Downgrade Firmware — Use the USB Mass Storage drive as a portable repository for new or legacy versions of the ROX II firmware.
  - Backup Files — Configure ROX II to backup important information to the USB Mass Storage drive, such as rollbacks, log files, feature keys and configuration files.

  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**

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

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

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

Section 1.2
Feature Keys

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

Three feature keys are currently available: L2STD, L3STD and L3SEC. By default, each new 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 ROX II devices, but a low-level alarm will be generated indicating a hardware mismatch.

Feature keys include the following features:

Feature	Feature Key		
	Layer 2 Standard Edition (L2STD)	Layer 3 Standard Edition (L3STD)	Layer 3 Security Edition (L3SEC)
VLANs (802.1Q)	✓	✓	✓
QoS (802.1p)	✓	✓	✓
MSTP (802.1Q-2005)[a]	✓	✓	✓
RSTP	✓	✓	✓
eRSTP™	✓	✓	✓
SNTP	✓	✓	✓
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 (L2STD)	Layer 3 Standard Edition (L3STD)	Layer 3 Security Edition (L3SEC)
PIM-SM	×	✓	✓
Firewall	×	✓	✓
OSPF	×	✓	✓
BGP	×	✓	✓
RIP v1/v2	×	✓	✓
IS-IS	×	✓	✓
Traffic Prioritization	×	✓	✓
VPN	×	×	✓
IPSec	×	×	✓

[a] *Formerly 802.1s*

For information about installing and viewing the contents of feature keys, refer to Section 3.12, “Managing Feature Keys”.

Section 1.3

Security Recommendations

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

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.

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 and processes (where applicable) before the device is deployed.
- Use strong passwords. Avoid weak passwords such as *password1*, *123456789*, *abcdefgh*, etc. For more information about creating strong passwords, refer to the password requirements in Section 4.10, “Managing Passwords and Passphrases”.
- Make sure passwords are protected and not shared with unauthorized personnel.
- Passwords should not be re-used across different usernames and systems, or after they expire.
- Record passwords in a safe, secure, off-line location for future retrieval should they be misplaced.
- When RADIUS authentication is done remotely, make sure all communications are within the security perimeter or on a secure channel.

- SSL and SSH 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.
- 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.
- 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.
- 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.
- If SNMP is enabled, limit the number of IP addresses that can connect to the device and change the community names. Also configure SNMP to raise a trap upon authentication failures. For more information, refer to Section 5.11, “Managing SNMP”.
- Limit the number of simultaneous Web Server, CLI, SFTP and NETCONF sessions allowed.
- If a firewall is required, configure and start the firewall before connecting the device to a public network. Make sure the firewall is configured to accept connections from a specific domain. For more information, refer to Section 5.17, “Managing Firewalls”
- Configure remote system logging to forward all logs to a central location. For more information, refer to Section 3.8, “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 ROX II device to the Internet is possible. However, the utmost care should be taken to protect the device and the network behind it using secure means such as firewall and IPsec. For more information about configuring firewalls and IPsec, refer to Section 5.17, “Managing Firewalls” and Section 5.28, “Managing IPsec Tunnels”.
- Management of the certificates and keys is the responsibility of the device owner. Before returning the device to Siemens Canada Ltd. for repair, replace the current certificates and keys with temporary *throwaway* certificates and keys that can be destroyed upon the device's return.
- Be aware of any non-secure protocols enabled on the device. While some protocols, such as HTTPS, SSH and 802.1x, are secure, others, such as Telnet and RSTP, were not designed for this purpose. Appropriate safeguards against non-secure protocols should be taken to prevent unauthorized access to the device/network.
- Prevent access to external, untrusted Web pages while accessing the device via a Web browser. This can assist in preventing potential security threats, such as session hijacking.
- Use the latest Web browser version compatible with ROX II to make sure the most secure Transport Layer Security (TLS) versions and ciphers available are employed.
- Make sure the device is fully decommissioned before taking the device out of service. For more information, refer to Section 3.7, “Decommissioning the Device”.
- Configure port security features on access ports to prevent a third-party from launching various attacks that can harm the network or device. For more information, refer to Section 3.17.3, “Configuring Port Security”.

- Periodically audit the device to make sure it complies with these recommendations and/or any internal security policies.

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

> **NOTE**
> *In certain cases, the service might be disabled, but the port can still be open (e.g. TFTP)*

- **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	Open	Yes
NETCONF	TCP/830	Open (if configured with login)	Open	Yes
SFTP	TCP/2222	Open (if configured with login)	Closed	Yes
HTTP	TCP/80	Open (if configured with login)	Open	N/A
NTP	UDP/123	Open (if configured)	Closed	No
SNMP	UDP/161	Open (if configured with login)	Closed	Yes
HTTPS	TCP/443	Open (if configured with login)	Open	Yes
TCP Modbus	TCP/502	Open (if configured)	Closed	No
IPSec IKE	UDP/500	Open (if configured)	Closed	Yes
IPSec NAT-T	UDP/4500	Open (if configured)	Closed	Yes
DNPv3	TCP/20000	Open (if configured)	Closed	No
RawSocket	TCP/configured	Open (if configured)	Closed	No
DHCP Agent	UDP/67	Open (if configured)	Closed	No
DHCP Server	UDP/67 listening, 68 responding	Open (if configured)	Closed	No

Services	Port Number	Port Open	Port Default	Access Authorized
RADIUS	UDP/1812 to send, opens random port to listen	Open (if configured)	Closed	Yes
L2TP	Random Port	Open (if configured)	Closed	Yes

Section 1.5

User Permissions

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

Types of user access:

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

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

Commands/Paths Permitted	Access			Notes
	Administrator	Operator	Guest	
/admin/contact	R/U	R/U	No	
/admin/hostname	R/U	R/U	No	
/admin/location	R/U	R/U	No	
/admin/session-limits	R/U	R/U	No	
/admin/session-security	R/U	R/U	No	
/admin/sftp	R/U	R/U	No	
/admin/time (status)	R	R	No	
/admin/switch-config (status)	R/U	R	No	
/admin/system	R/U	R/U	No	
/admin/sytem-name	R/U	R/U	No	
/admin/timezone	R/U	C/R/U	No	
/admin/clear-all-alarms (action)	E	C/R/U	No	
/admin/backup-files (action)	E/R/U	No	No	
/admin/delete-all-ssh-known-hosts (action)	E	E	No	
/admin/delete-logs (action)	E	No	No	
/admin/delete-ssh-known-host (action)	E	E	No	
/admin/full-configuration-load (action)	E/U	No	No	
/admin/full-configuration-save (action)	E/U	No	No	
/admin/install-files (action)	E/U	No	No	
/admin/reboot (action)	E	E	No	
/admin/restore-factory-defaults (action)	E/U	No	No	
/admin/set-system-clock (action)	E/U	E	No	
/admin/shutdown (action)	E	E	No	
/apps	C/R/U	C/R/U	R	
/chassis/part-list	R/U	R	R	
/chassis/fixed-modules	C/R/U	R/U	R	
/chassis/line-module-list	R/U	R	R	
/chassis/line-modules/line-module	R/U	R/U	R	
/interfaces	R	C/R/U	R	
/interface	C/R/U	R/U	R	
/routing	C/R/U	C/R/U	R	
/routing/dynamic/ospf/interface	C/R/U	R/U	R	
/routing/dynamic/rip/interface	C/R/U	R/U	R	

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

2 Using ROX II

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

- Section 2.1, “Connecting to ROX II”
- Section 2.2, “Default Usernames and Passwords”
- Section 2.3, “Logging In”
- Section 2.4, “Logging Out”
- Section 2.5, “Using Network Utilities”
- Section 2.6, “Using the Command Line Interface”
- Section 2.7, “Configuring the CLI Interface”
- Section 2.8, “Accessing Different Modes”

Section 2.1

Connecting to ROX II

The following describes the various methods for connecting the device:

- Section 2.1.1, “Connecting Directly”
- Section 2.1.2, “Connecting Through the Network”

Section 2.1.1

Connecting Directly

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

Using the RS232 Serial Console Port

To establish a serial connection to the device, do the following:

1. Connect a serial terminal or a computer running terminal emulation software to the RS232 console port on the device.

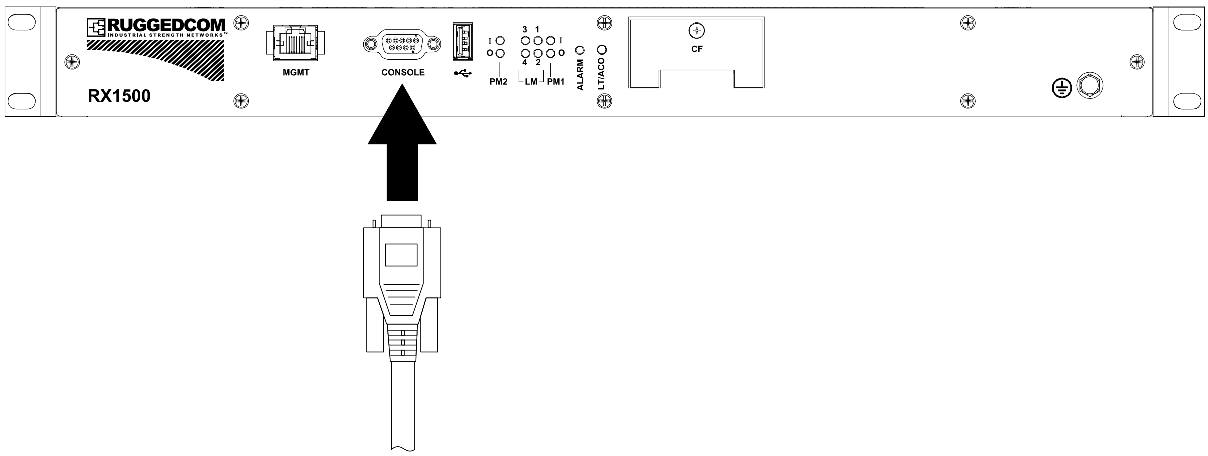

Figure 1: RS232 Console Port

2. Configure the terminal as follows:
   - 57600 bps
   - No parity
   - 8 bits
   - Set terminal type to VT100
   - Disable hardware and software flow control
3. Establish a connection to the device and press any key. The login prompt appears.
4. Log in to ROX II. For more information about logging in to ROX II, refer to Section 2.3, “Logging In”.

Using an Ethernet Port

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

1. Connect a serial terminal or a computer running terminal emulation software to the MGMT port on the device.

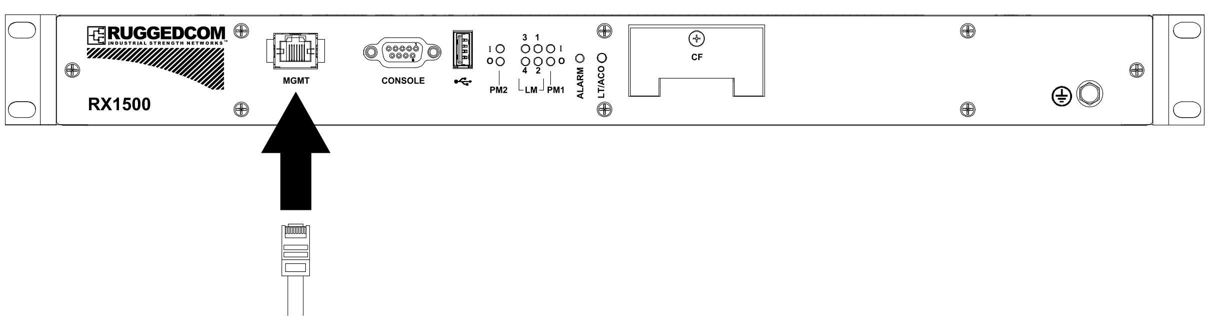

Figure 2: MGMT Port

2. By default, the RUGGEDCOM RX1500 has a different IP address and subnet configured for two types of IP interfaces, both of which are mapped to one or more physical ports:

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

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

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

```
Using username "admin".
admin@192.168.0.2's password:
```

4. Log in to ROX II. For more information about logging in to ROX II, refer to Section 2.3, “Logging In”.

Section 2.1.2

Connecting Through the Network

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

1. On the computer being used to connect to the device, configure the Ethernet port to use an IP address falling within the subnet of the device.

   By default, the RUGGEDCOM RX1500 has a different IP address and subnet configured for two types of IP interfaces, both of which are mapped to one or more physical ports:

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

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

2. Launch the SSH client on the computer and connect to *admin@{ipaddress}*, where *{ipaddress}* is the IP address for the port that is connected to the network.
3. Log in to ROX II. For more information, refer to Section 2.3, “Logging In”.

Section 2.2

Default Usernames and Passwords

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

CAUTION!
Security hazard – risk of unauthorized access and/or exploitation. To prevent unauthorized access to the device, change the default passwords before commissioning the device. For more information, refer to Section 4.10, “Managing Passwords and Passphrases”.

NOTE
A default password does not exist for Maintenance mode.

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

Section 2.3
Logging In

To log in to ROX II, do the following:

1. Connect to the device. For more information about the various methods of connecting to the device, refer Section 2.1, "Connecting to ROX II".
2. Once a connection is established with the device, press **Enter**. The login prompt appears.

   NOTE
   ROX II features three default user accounts: admin, operator and guest. Additional user accounts can be added. For information about adding user accounts, refer to Section 4.9.2, "Adding a User".
3. Type the user name and press **Enter**. The password prompt appears.

   NOTE
   If a unique password/passphrase has not been configured, use the factory default password. For more information, refer to Section 2.2, "Default Usernames and Passwords".
4. Type the password associated with the username and press **Enter**.

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

Section 2.4
Logging Out

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

```
ruggedcom#  exit
```

Section 2.5

Using Network Utilities

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

- Section 2.5.1, “Pinging a Host”
- Section 2.5.2, “Dumping Raw Data to a Terminal or File”
- Section 2.5.3, “Tracing the Route to a Remote Host”
- Section 2.5.4, “Pinging an IPv4 Address Using MPLS Protocols”
- Section 2.5.5, “Tracing the Route of an IPv4 Address Using MPLS Protocols”
- Section 2.5.6, “Tracing Activities on a Serial Port”

Section 2.5.1

Pinging a Host

To ping a host, type:

For Hosts with IPv4 Addresses

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

For Hosts with IPv6 Addresses

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

Where:

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

Section 2.5.2

Dumping Raw Data to a Terminal or File

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

To dump raw data to a terminal or file, type **tcpdump** and configure the following parameters:

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

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

Section 2.5.3

Tracing the Route to a Remote Host

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

For Hosts with IPv4 Addresses

```
traceroute [name | address]
```

For Hosts with IPv6 Addresses

```
traceroute6 [name | address]
```

Where:

- *name* is the name of the remote host
- *address* is the IP address of the remote host

Section 2.5.4

Pinging an IPv4 Address Using MPLS Protocols

To ping an IPv4 address using the MPLS protocols, type:

```
mpls-ping ipaddress/prefix number_of_pings
```

Where:

- *ipaddress/prefix* is the IPv4 address of the MPLS ping
- *number_of_pings* is the number of ping attempts

Section 2.5.5

Tracing the Route of an IPv4 Address Using MPLS Protocols

To trace the route of an IPv4 adress using MPLS protocols, type:

```
mpls-traceroute remoteIPAddr/Pre
```

Where:

- *remoteIPAddr/Pre* is the IPv4 address of the MPLS trace route

Section 2.5.6

Tracing Activities on a Serial Port

To trace activities on a serial port, type:

```
traceserial [port slot port | hex | protocol | tcp-udp]
```

Where:

- `port slot port` defines the port to trace
- `hex` displays the content of serial data in a hex
- `protocol` traces the serial protocol on the serial port
- `tcp-udp` traces TCP-UDP events on the serial port

Section 2.6

Using the Command Line Interface

The following sections describe how use the Command Line Interface (CLI):

- Section 2.6.1, “Accessing Different CLI Modes”
- Section 2.6.2, “Using Command Line Completion”
- Section 2.6.3, “Displaying Available Commands”
- Section 2.6.4, “Editing Commands”
- Section 2.6.5, “Using Output Redirects”
- Section 2.6.6, “Using Regular Expressions”
- Section 2.6.7, “Using CLI Utilities”
- Section 2.6.8, “Specifying a Range”
- Section 2.6.9, “Common Commands”

Section 2.6.1

Accessing Different CLI Modes

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

Mode	Description
Operational Mode	Operational mode is the default mode after a user logs in to the device. It allows users to perform general device management actions and provides troubleshooting and maintenance utilities. It is used for viewing the system status, controlling the CLI environment, monitoring and troubleshooting network connectivity, and launching the Configuration mode.
Configuration Mode	Configuration mode is launched from the Operational Mode. It allows users to change the actual configuration of the device. All changes to the configuration are made on a copy of the active configuration, called the candidate configuration. Changes do not take effect until they are committed.

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

```
ruggedcom#
```

In Configuration mode, the prompt is:

```
ruggedcom(config)#
```

As a user navigates through the configuration data hierarchy, the prompt indicates the user's location in the configuration. For example, after navigating to ***>interface » eth » lm3 » port1***, the CLI prompt will be:

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

Section 2.6.2

Using Command Line Completion

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

NOTE

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

```
who file foo\ bar
```

or

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

NOTE

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

Section 2.6.3

Displaying Available Commands

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

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

```
ruggedcom# ?
Possible completions:
  admin               Configures the general device characteristics
  autowizard       Automatically query for mandatory elements
  clear                 Clear parameter
  commit             Confirm a pending commit
  compare           Compare running configuration to another configuration or a file
  .
  .
  .
  traceserial        Trace serial ports activities
```

```
  who                  Display currently logged on users
  write                 Write configuration
ruggedcom#
```

Section 2.6.4

Editing Commands

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

Moving the Cursor

Command	Description
Ctrl+b or **Left Arrow**	Moves the cursor back one character
Ctrl+f or **Right Arrow**	Moves the cursor forward one character
Esc+b or **Alt+b**	Moves the cursor back one word
Esc+f or **Alt+f**	Moves the cursor forward one word
Ctrl+a or **Home**	Moves the cursor to the beginning of the command line
Ctrl+e or **End**	Moves the cursor to the end of the command line

Deleting Characters

Command	Description
Ctrl+h, **Delete** or **Backspace**	Delete the character before the cursor
Ctrl+d	Delete the character after the cursor
Ctrl+k	Delete all characters from the cursor to the end of the line
Ctrl+u or **Ctrl+x**	Delete the whole line
Ctrl+w, **Esc+Backspace** or **Alt+Backspace**	Delete the whole before the cursor
Esc+d or **Alt+d**	Delete the whole after the cursor

Inserting Recently Deleted Text

Command	Description
Ctrl+y	Inserts the most recently deleted text at the cursor's location

Displaying Previously Entered Commands

Command	Description
Ctrl+p or **Up Arrow**	Shows the previous command in the command history
Ctrl+n or **Down Arrow**	Shows the next command in the command history
Ctrl+r	Reverses the order of commands in the command history
`show` `history`	shows a list of previous commands

Capitalization

Command	Description
Esc+c	Capitalizes the first letter of the word at the cursor's location and sets all other characters to lowercase
Esc+l	Changes the entire word at the cursor's location to lowercase
Esc+u	Changes the entire word at the cursor's location to uppercase

Special Actions

Command	Description
Ctrl+c	Aborts a command or clears the command line
Ctrl+v or **Esc+q**	Treats the next character(s) as character data, not a command
Ctrl+l	Redraws the screen
Ctrl+t	Transposes characters
Esc+m	Enters multi-line mode
Ctrl+d	Exits multi-line mode
Ctrl+z	Exits configuration mode

Inserting Hard Returns

Command	Description
Esc+M	Inserts a hard return

Section 2.6.5

Using Output Redirects

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

```
ruggedcom# show admin | ?
Possible completions:
  append      Append output text to a file
  begin         Begin with the line that matches
  count         Count the number of lines in the output display
  exclude      Exclude lines that match
  include       Include lines that match
  linnum        Enumerate lines in the output
  more          Paginate output
  nomore      Suppress pagination
  notab         Suppress table output
  repeat        Repeat show term with a given interval
  save           Save output text to a file
  select         Select additional columns
  tab             Enforce table output
  until           End with the line that matches
ruggedcom# show admin |
```

Parameter	Description
append	Appends the output text to a specified ASCII text file.

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td></td><td>
For example: running these two terms appends the admin and chassis information to the specified file:
<pre>
ruggedcom# show admin | append foo.txt
ruggedcom# show interface | append foo.txt
ruggedcom#
</pre>
The resulting file contains the results of show interface appended to the results of show admin (lines truncated with ... are shortened for illustrative purposes only):
<pre>
ruggedcom# file show-config foo.txt
admin
 time
  gmtime "Tue Feb 15 07:52:13 2011\n" localtime "Tue Feb 15
 02:52:13 2011\n"
 software-upgrade
  upgrade-progress
   software partition "Partition #1" current version "ROX 2.1.0
 (2010-12-03 17:38)...
 netconf
  statistics
   in sessions 0 in xml parse errs 0 in bad hellos 0 in rpcs 0 in
 bad rpcs 0 in not...
            NETWORK   RSSI   NETWORK   NETWORK
 NETWORK   NETW...
SLOT PORT SUPPORTED IMEI ECIO INDICATOR OPERATOR IN USE
 STATUS   SIM SUPP...
lm2   1   -   -   -   -   -   -   -
       -    -   ...

ruggedcom#
</pre>
</td></tr>
<tr><td>begin</td><td>
Begins the output with the line containing the specified text. Regular expressions can be used with this redirect. For more information about regular expressions, refer to Section 2.6.6, “Using Regular Expressions”.
For example, <code>show admin | begin netconf</code> returns all of the admin information following the <code>netconf</code> line:
<pre>
ruggedcom# show admin | begin netconf
 netconf
  statistics
   in sessions 0 in xml parse errs 0 in bad hellos 0 in rpcs 0 in
 bad rpcs 0 in not...
ruggedcom#
</pre>
</td></tr>
<tr><td>count</td><td>
Displays the number of lines returned by the term.
For example, show admin | count shows the number of lines in the admin information.
<pre>
ruggedcom# show admin | count
Count: 9 lines
ruggedcom#
</pre>
</td></tr>
<tr><td>exclude</td><td>
Excludes lines containing the specified text. Information that is a child of the excluded line is also excluded. Regular expressions can be used with this redirect. For more information about regular expressions, refer to Section 2.6.6, “Using Regular Expressions”.
For example, show admin | exclude netconf shows the admin information, excluding the <code>netconf</code> lines.
<pre>
ruggedcom# show admin | exclude netconf
admin
 time
  gmtime "Tue Feb 15 08:25:27 2011\n" localtime "Tue Feb 15
 03:25:27 2011\n"
</pre>
</td></tr>
</table>

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td></td><td><pre>
 software-upgrade
  upgrade-progress
   software partition "Partition #1" current version "ROX 2.1.0
 (2010-12-03 17:38) ...
  statistics
   in sessions 0 in xml parse errs 0 in bad hellos 0 in rpcs 0 in
 bad rpcs 0 in not...
    supported rpcs 0 out rpc replies 0 out rpc errors 0 out
 notifications 0
ruggedcom#
</pre></td></tr>
<tr><td>include</td><td>Includes lines containing the specified text. Information that is a child of the included line is usually included, but may not be in some cases. Regular expressions can be used with this redirect. For more information about regular expressions, refer to Section 2.6.6, “Using Regular Expressions”.

For example, show admin | include time shows the <code>time</code> lines from the admin information.<pre>
ruggedcom# show admin | include time
 time
  gmtime "Tue Feb 15 08:34:55 2011\n" localtime "Tue Feb 15
 03:34:55 2011\n"
ruggedcom#
</pre></td></tr>
<tr><td>linnum</td><td>Numbers the lines in the output. For example:<pre>
ruggedcom# show admin | linnum
1: admin
2: time
3:   gmtime "Tue Feb 15 08:37:42 2011\n" localtime "Tue Feb 15
 03:37:42 2011\n"
4: software-upgrade
.
.
.
ruggedcom#
</pre></td></tr>
<tr><td>more</td><td>Paginates the output. When the output reaches the screen-length setting, the CLI prompts you to press a key for more. Press Enter to advance line-by-line; press space to advance page-by-page.</td></tr>
<tr><td>nomore</td><td>Suppresses pagination.</td></tr>
<tr><td>notab</td><td>Suppresses table output.

For example, show chassis | begin line-modules shows the following table:<pre>
ruggedcom# show chassis | begin line-modules
 line-modules
  line-module
SLOT DETECTED MODULE
----
lm1   none
lm2   Old V90 Modem
lm3   2x 10/100Tx RJ45
lm4   2x 10/100Tx RJ45
lm5   1x T3/E3
lm6   2x Chan T1/E1

ruggedcom#
</pre>For example, show chassis | begin line-modules | notab suppresses the table formatting:<pre>
ruggedcom# show chassis | begin line-modules | notab
 line-modules
  line-module lm1
</pre></td></tr>
</table>

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td></td><td><pre>
   detected module none
  line-module lm2
   detected module "Old V90 Modem"
  line-module lm3
   detected module "2x 10/100Tx RJ45"
  line-module lm4
   detected module "2x 10/100Tx RJ45"
  line-module lm5
   detected module "1x T3/E3"
  line-module lm6
   detected module "2x Chan T1/E1"
ruggedcom#
</pre></td></tr>
<tr><td>repeat</td><td> Repeats the term at the specified interval. Specify an interval in seconds. The term repeats until you cancel it with Ctrl-C. For example, show admin | repeat 10s repeats the show admin term every 10 seconds. </td></tr>
<tr><td>save</td><td> Saves the output to the specified ASCII text file. For example, show chassis | save foo.txt saves the chassis information to the file <code>foo.txt</code> </td></tr>
<tr><td>select</td><td>This redirect is not yet implemented.</td></tr>
<tr><td>tab</td><td>Enforces table layout for columnar data.</td></tr>
<tr><td>until</td><td> Includes output until a line containing the specified text appears. Regular expressions can be used with this redirect. For more information about regular expressions, refer to Section 2.6.6, “Using Regular Expressions”. For example, show chassis | begin cpu | until status returns the chassis information beginning with <code>cpu</code> and ending with the <code>status</code>: <pre>
ruggedcom# show chassis | begin cpu | until status
 cpu
  slot-cpu
                               CPU   RAM
                         CPU   LOAD RAM   AVAIL
SLOT DETECTED MODULE   LOAD HIGH AVAIL LOW
----
main RX1000 Main Board 13   86   51   50

 status
ruggedcom#
</pre></td></tr>
</table>

Section 2.6.6

Using Regular Expressions

ROX II command line regular expressions are a subset of the regular expressions found in egrep and in the AWK programming language. Regular expressions can be used along with several of the output redirects. For more information about using output redirects, refer to Section 2.6.5, “Using Output Redirects”.

Character	Description	Example
.	Matches any single character (e.g. .100, 100., .100.)	.100 100. .100.
*	Matches zero (0) or more occurrences of a pattern	100*
+	Matches 1 or more occurrences of a pattern	100+

Character	Description	Example
?	Match 0 or 1 occurrences of a pattern	100?
^	Matches the beginning of the line	^100
$	Matches the end of the line	100$
()	Matches only the characters specified	(38a)
[]	Matches any character other than those specified	[^abc]
_ (underscore)	The underscore character has special meanings in an autonomous system path. It matches to: • Each space ( ) and comma (,) • Each AS set delimiter (e.g. *{* and *}*) • Each AS confederation delimiter (e.g. *(* and *)*) • The beginning and end of the line Therefore, the underscore can be used to match AS values.	_100,100_, _100_

For example, to show *chassis* information for line modules 1 and 2 only:

```
ruggedcom# show chassis | include lm[1-2]
lm1   XX     none                           none
lm2   M1_    Old V90 Modem
lm1   none                empty      ----    0D 0hr 0min 0sec  2011-02-13Z  08:35:47Z
lm2   Old V90 Modem       operating  Normal  0D 0hr 0min 0sec  2011-02-13Z  08:35:47Z
lm1   none
lm2   Old V90 Modem
ruggedcom#
```

Section 2.6.7

Using CLI Utilities

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

Parameter	Description
ssh [host | *address/name*] {bind-address | *address*} {cipher-spec | *cipher*} {login | *name*} {port | *number*} {sub-system}	Opens a secure shell on another host. Parameters include: • `host` is the name or IP address of the host. It is mandatory. • `bind-address` is the source address of the connection. Only useful on systems with more than one address. • `cipher-spec` is the cipher specification for encrypting the session. Supported cipher options include aes128-cbc, 3des-cbc, blowfish-cbc, cast128-cbc, arcfour128, arcfour256, arcfour, aes192-cbc, aes256-cbc, aes128-ctr, aes192-ctr and aes256-ctr. • `login` is the users login name on the host. • `port` is the TCP port number to open an SSH session to. • `sub-system` invokes a subsystem on the remote system, such as NETCONF.
telnet {host | *address/name*}	Opens a telnet session to another host. Parameters include: • *host* is the name or IP address of the host

Further documentation for these well-known applications is beyond the scope of this guide, but can be found on the Internet.

Section 2.6.8

Specifying a Range

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

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

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

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

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

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

Section 2.6.9

Common Commands

The following sections describe common commands that can be used in the CLI:

- Section 2.6.9.1, “Basic CLI Commands”
- Section 2.6.9.2, “File Commands”
- Section 2.6.9.3, “Interface and Services Commands”
- Section 2.6.9.4, “Administration Commands”
- Section 2.6.9.5, “Configuration Mode General Commands”

Section 2.6.9.1

Basic CLI Commands

Use the following commands to perform basic CLI functions.

Parameter	Description
exit [level | configuration-mode | no-confirm]	**Default:** level Exits from the current mode. • `level` exits from the current mode. If performed at the top level, this command exits from the configuration mode. • `configuration-mode` exits from configuration mode regardless of mode. • `no-confirm` exits from configuration mode without prompting the user to commit any pending changes.
help *command*	Displays help text for the specified command.

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

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td>logout [logout | sessionid]</td><td>Terminates the specified session. A session can by specified based on its user ID or session ID.</td></tr>
<tr><td>quit</td><td>Logs out of and ends the CLI session.</td></tr>
<tr><td>send [all | admin] message</td><td>Sends a message to all users of the specified type. The message appears in both the CLI and web interface. For example:
<pre>
ruggedcom# send all "Rebooting at midnight!"
 ruggedcom# Message from admin@ruggedcom at 2011-02-15 08:42:49...
 Rebooting at midnight!
 EOF

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

 ruggedcom#
</pre></td></tr>
<tr><td>show [cli | history | jobs | log | logfile]</td><td>Shows selected system information.

<code>cli</code> shows the CLI environment settings. For example:
<pre>
ruggedcom# show cli
 autowizard   true
 complete-on-space   true
 display-level   99999999
 history   100
 ignore-leading-space   true
 output-file   terminal
 paginate   true
 screen-length   65
 screen-width   237
 service prompt config true
 show-defaults   false
 terminal   xterm
 ruggedcom#
</pre>
<code>history</code> displays the CLI command history.
<code>jobs</code> displays currently running background jobs. For example:
<pre>
ruggedcom# show jobs
 JOB COMMAND
 2   monitor start /tmp/saved
 ruggedcom#
</pre>
<code>log</code> and <code>logfile</code> display the selected log file. Use auto completion to view a list of available log files.
</td></tr>
</table>

Parameter	Description
show parser dump *command*	Displays all possible commands starting with the specified command.
show running-config *option*	Displays the current configuration. If an *option* parameter is not specified, the entire configuration will be displayed by default . Use auto completion to see a list of configuration options. Use | and one or more output redirects to restrict the information to be shown.

Section 2.6.9.2

File Commands

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

Parameter	Description

compare file	Compares the running configuration to a file. A **>** character indicates text that is present in the selected file but not in the running configuration. A **<** character indicates text that is present in the running configuration, but not in the selected file. In the following example, the user information is present in the configuration, but not in the selected file:
	`ruggedcom# compare file deleted_users`
	`125,127d124`
	`<  userid jsmith`
	`<   password $1$N1YT8Azl$KcG1E6/r91EXc4mgEEsAW. role administrator`
	`<  !`
	`ruggedcom#`

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

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

Parameter	Description

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

file delete-config *filename*	Deletes a configuration file. After typing the command, press **Tab** to view a list of available files. For example, the following command deletes the `deleted_users` file:
	`ruggedcom# file delete-config deleted_users`
	`ruggedcom#`

file delete-featurekey *filename*	Deletes a feature key file. After typing the command, press **Tab** to view a list of available files. For example, the following command deletes the feature key `1_cmRX1K-12-11-0217.key` file:
	`ruggedcom# file delete-featurekey 1_cmRX1K-12-11-0217.key`
	`ruggedcom#`

file list-config	Lists the configuration files. For example:
	`ruggedcom# file list-config`
	`--help 10.200.20.39  _tmp_confd_cmd.0 archive001 archive002`
	` default_rx1000_config`
	`ruggedcom#`

file list-featurekey	Lists the feature key files. For example:
	`ruggedcom# file list-featurekey`
	`1_cmRX1K-12-11-0015.key`
	`ruggedcom#`

file rename-config *current-filename new-filename*	Renames a configuration file. For example, the following command renames the `test002` file to `production_config`:
	`ruggedcom# file rename-config test002 production_config`
	`ruggedcom#`

file rename-config *current-filename new-filename*	Renames a feature key file. For example, the following command renames the feature key `1_cmRX1K-12-11-0217.key` file to `old_featurekey`:
	`ruggedcom# file rename-featurekey 1_cmRX1K-12-11-0217.key`
	` old_featurekey`
	`ruggedcom#`

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

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td></td><td>

• new-filename is the new filename for the configuration file. To use the current filename, specify the current filename or exclude this parameter from the command.

When prompted, type the password to connect to the remote computer. For example:

<pre>
ruggedcom# file scp-config-from-url jsmith@10.200.20.39:/c:/
ruggedcom/standard_config standard_config
jsmith@10.200.20.39's password:
standard_config.txt   100% 7673
 7.5KB/s   00:00
ruggedcom#
</pre>
</td></tr>
<tr><td>file scp-config-to-url current-filename user@host:/path/new-filename</td><td>

Securely copies a configuration file from the device to a remote computer. The remote computer must have an SCP or SSH (secure shell) service or client installed and running.

To use this command, the user credentials for the remote computer, the IP address or hostname of the remote computer, the directory path to the configuration file on the remote computer, and the configuration file filename must all be known.

Type the command in the following format:

file scp-config-to-url current-filename user@host:/path/new-filename

Where:

• current-filename is the current filename of the configuration file.
• user is a user name with access rights to the remote computer.
• host is the hostname or IP address of the remote computer.
• path path specifies where to save the configuration file on the remote computer.
• new-filename is the new filename for the configuration file. To use the current filename, specify the current filename or exclude this parameter from the command.

When prompted, type the password to connect to the remote computer. For example:

<pre>
ruggedcom# file scp-config-to-url default_config
 jsmith@10.200.20.39:/c:/ruggedcom/default_config
jsmith@10.200.20.39's password:
standard_config.txt   100% 7673
 7.5KB/s   00:00
ruggedcom#
</pre>
</td></tr>
<tr><td>file scp-featurekey-from-url user@host:/path/current-filename new-filename</td><td>

Securely copies a feature key file from a remote computer to the device. The remote computer must have an SCP or SSH (secure shell) service or client installed and running.

To use this command, the user credentials for the remote computer, the IP address or hostname of the remote computer, the directory path to the feature key file on the remote computer, and the feature key file filename must all be known.

Type the command in the following format:

file scp-featurekey-from-url current-filename user@host:/path/new-filename

Where:

• user is a user name with access rights to the remote computer.
• host is the hostname or IP address of the remote computer.
• path path is the path to the feature key file on the remote computer.
• current-filename is the current filename of the feature key file.
• new-filename is the new filename for the feature key file. To use the current filename, specify the current filename or exclude this parameter from the command.

When prompted, type the password to connect to the remote computer. For example:

<pre>
ruggedcom# file scp-featurekey-from-url jsmith@10.200.20.39:/c:/
ruggedcom/1_cmRX1K-12-11-0015.key 1_cmRX1K-12-11-0015.key
jsmith@10.200.20.39's password:
</pre>
</td></tr>
</table>

Parameter	Description

	`1_cmRX1K-12-11-0015.key                              100% 192`
	`0.2KB/s   00:00`
	`ruggedcom#`

file scp-featurekey-to-url *current-filename user@host:/path/new-filename*	Securely copies a feature key file to a remote computer from the device. The remote computer must have an SCP or SSH (secure shell) service or client installed and running.
	To use this command, the user credentials for the remote computer, the IP address or hostname of the remote computer, the directory path to the feature key file on the remote computer, and the feature key file filename must all be known.
	Type the command in the following format:
	file scp-featurekey-to-url *current-filename user@host:/path/new-filename*
	Where:
	• *current-filename* is the current filename of the feature key file.
	• *user* is a user name with access rights to the remote computer.
	• *host* is the hostname or IP address of the remote computer.
	• *path* path specifies where to save the feature key file on the remote computer.
	• *new-filename* is the new filename for the feature key file. To use the current filename, specify the current filename or exclude this parameter from the command.
	When prompted, type the password to connect to the remote computer. For example:
	`ruggedcom# file scp-featurekey-to-url 1_cmRX1K-12-11-0015.key jsmith@10.200.20.39:/c:/ruggedcom/1_cmRX1K-12-11-0015.key`
	`jsmith@10.200.20.39's password:`
	`1_cmRX1K-12-11-0015.key                              100% 192`
	`0.2KB/s   00:00`
	`ruggedcom#`

file scp-log-to-url *current-filename user@host:/path/new-filename*
scp-log-to-url
	Securely copies a log file to a remote computer from the device. The remote computer must have an SCP or SSH (secure shell) service or client installed and running.
	To use this command, the user credentials for the remote computer, the IP address or hostname of the remote computer, the directory path to the log file on the remote computer, and the log file filename must all be known.
	Where:
	• *current-filename* is the current filename of the log file.
	• *user* is a user name with access rights to the remote computer.
	• *host* is the hostname or IP address of the remote computer.
	• *path* path specifies where to save the log file on the remote computer.
	• *new-filename* is the new filename for the log file. To use the current filename, specify the current filename or exclude this parameter from the command.
	When prompted, type the password to connect to the remote computer. For example:
	`ruggedcom# file scp-log-to-url syslog.1 jsmith@10.200.20.39:/c:/ruggedcom/syslog.1`
	`jsmith@10.200.20.39's password:`
	`syslog.1                              100% 12KB  12.4KB/s   00:00`
	
	`ruggedcom#`

file show-config *filename*	Displays the content of a specified file. Use auto completion to display a list of available files. For example:
	`ruggedcom# file show-config added_users.txt`
	`admin system-name "System Name" location Location contact Contact`
	`admin hostname name ruggedcom domain localdomain`
	`admin session-limits max-sessions 50`
	`.`

Parameter	Description

	`.`
	`.`
	`ruggedcom#`

file show-featurekey *filename*	Displays the content of a specified feature key file. Use auto completion to display a list of available feature key files. For example:
	`ruggedcom# file show-featurekey 1_cmRX1K-12-11-0015.key`
	`GPG_FEATUREKEY_LEVEL=1`
	`GPG_FEATUREKEY_CM_SERIALNUMBER=RX1K-12-11-0015`
	`GPG_FEATUREKEY_SIGNATURE=iEYEABECAAYFAk091pAACgkQP2pya`
	`+G5kdZeKACeKdHUB2G1T73Dymq8IjSdYDKAiskAn3abBpCEhfLXxY2ZlVbv`
	`GNwDZow2`
	
	`ruggedcom#`

Section 2.6.9.3

Interface and Services Commands

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

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

Section 2.6.9.4

Administration Commands

Operational mode provides commands for performing device administration tasks.

Parameter	Description
admin acknowledge-all-alarms	Acknowledges all system alarms.
admin clear-all-alarms	Clears all system alarms.
admin delete-all-ssh-known-hosts	Deletes the list of known hosts.

Parameter	Description
admin delete-ssh-known-hosts	Deletes the host entry from the list of known hosts.
admin restore-factory-defaults	Restores the factory default configuration and settings, but does not erase any files you have saved on the device.
admin reboot	Reboots the device.
admin restore-factory-defaults	Restores the factory default configuration and settings, but does not erase any files you have saved on the device.
admin set-system-clock time *YYYY-MM-DD HH:MM:SS*	Sets the date and time on the device. To specify just the date, type the date in the format *YYYY-MM-DD*. To specify just the time, type the time in the format *HH:MM:SS*. To specify both date and time, enclose the string in quotation marks and type the date and time in the format "*YYYY-MM-DD HH:MM:SS*". **NOTE** *When setting the time, specifying seconds seconds (SS) is optional.*
admin shutdown	Shuts down the device. For more information on shutting down the device, refer to Section 3.4, "Shutting Down the Device"
admin software-upgrade decline-upgrade	Cancels (or declines) a recent software upgrade that is waiting for a reboot to the upgraded partition.
admin software-upgrade launch-upgrade	Launches an upgrade in the alternate partition.
admin software-upgrade rollback-reboot	Boots to a previous software release on the alternate partition.
maint-login	**CAUTION!** *Configuration hazard – risk of data loss/corruption. Maintenance mode is provided for troubleshooting purposes and should only be used by Siemens Canada Ltd. technicians. Maintenance mode is provided for troubleshooting purposes and all possible commands are not documented. Misuse of maintenance mode commands can corrupt the operational state of the device and render the device inaccessible.* Logs in to the underlying operating system as the root user. The user must be an administrator and be able to provide the maint-login password.
monitor start *filename*	Starts displaying the specified system log or tracing the specified file. If necessary, the output can be redirected to a file. For information on how to redirect output, refer to Section 2.6.5, "Using Output Redirects". Use auto completion to view a list of available logs and files.
monitor stop *filename*	Stops displaying the specified system log or tracing the specified file. Use auto completion to view a list of available logs and files.
reportstats	Displays an extensive collection of device-specific statistics. If necessary, the output can be redirected to a file. For information on how to redirect output, refer to Section 2.6.5, "Using Output Redirects".
config private	Enters a configuration mode where users can make changes to the system. This is the primary mode for most users who want to make changes to the device/network configuration. It can be accessed by multiple Operator and Admin users.

Parameter	Description
	All changes made during a private configuration session are hidden from other users until they are committed. Each change must be committed before it is applied to the active system. If a user opens an exclusive configuration session during another user's private configuration session, the user in the private configuration session cannot commit their changes until the other user ends their session.
config exclusive	Enters a configuration mode where users can make changes to the system. This mode is similar to the private configuration mode, except all other users are blocked from committing their changes until the user using the exclusive configuration mode exits. Only one Operator or Admin user can use the exclusive configuration mode at a time per device. When committing changes in exclusive configuration mode, use the confirmed option to set a timeout period. Changes will be applied for the set period of time, after which the configuration will be reset to its previous settings. This allows users to test their configuration changes before fully applying them to the active system. For more information about the confirmed option, refer to Section 2.6.9.5, “Configuration Mode General Commands”. **IMPORTANT!** *Always log out of the exclusive configuration mode or exit the transaction. If the session is terminated before a user exits properly, other users logged in to the device will continue to be blocked from making changes until the session timeout period expires.*

Section 2.6.9.5

Configuration Mode General Commands

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

Parameter	Description
abort	Exits the configuration session without saving changes. **NOTE** *In an edit exclusive session, any pending unconfirmed commits will not be cancelled until their timeout periods expire. A new edit exclusive session cannot be opened until the timeout period ends.*
clear	Deletes all configuration changes.
commit no-confirm	Immediately commits the current set of configuration changes. This command will prompt the user to confirm the action. Use the no-confirm parameter to revert the configuration without requiring confirmation.
commit abort	In an edit exclusive session, this command aborts/cancels all confirmed commits.
commit and-quit	Commits all confirmed and unconfirmed changes and exits the configuration mode.
commit check	Validates the current configuration.
commit confirmed *timeout*	Temporarily commits changes for a period of time, allowing users to test the configuration before fully committing the changes. The changes must be committed using a standard **commit** command before the timeout period ends. If changes are not committed before the timeout period ends, they are automatically discarded and the previous settings are restored.

Parameter	Description
	A timeout period can be specified at the end of the command. The default timeout period is 10 minutes. The minimum timout period is 1 minute. For example: `ruggedcom(config-admin)# commit confirmed 2` To cancel a commit before the time elapses and discard the changes, type: **commit** abort To permanently commit the changes before the time elapses, type: **commit**
commit comment *text*	Immediately commits the current set of configuration changes along with a custom comment. The comment will appear next to the commit in a list of pending of commits.
commit label *text*	Immediately commits the current set of configuration changes along with a custom label. In a list of pending commits, the label will appear instead of the auto-generated commit ID.
commit persist-id *text*	Immediately commits the current set of configuration changes and assigns a user-specified ID or flag.
commit save-running *file*	Immediately commits the current set of configuration changes and saves them to the specified file. It does not save the complete running configuration.
copy	Copies a configured element to a new element. For example, the following command copies the userid *admin* to the new userid *wsmith*: `ruggedcom(config)# copy admin users userid admin smith` The new item has all of the attributes of the item from which it is copied. In this example, userid *wsmith* will have the same password and role attributes as the userid *admin*.

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

do	Performs an Operational mode command. For example, the following command performs the Operational mode **ping** command in the Configuration mode session: `ruggedcom(config)# do ping 172.30.134.12`
end	Terminates the configuration session. The system prompts the user to commit uncommitted changes.
exit	Exits from the current mode. Unlike the **end** command, the system does not prompt the user to commit uncommitted changes.
help command	Displays help information for the specified command.
load [merge | override] *filename*	Loads a configuration from an ASCII CLI configuration file. Two parameters are available for the CLI load command: `override` and `merge`. • **Override:** this parameter is for users who have a full configuration file saved and want to load it back on to the device. The full configuration file can be previously created with the CLI **save** command executed from the top level in the configuration tree or with the **admin** `full-configuration-save` command. With the `override` parameter, the entire running configuration is overwritten by the contents of the configuration file. The override option has the following restrictions:

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td></td><td>

- The configuration file must be a *complete* configuration for the device. A *complete* configuration is the entire configuration tree.
- The **load** command must be invoked at the base of the configuration tree.

- **Merge:** this parameter is for users who want to build a template configuration and load it to many devices. The template configuration file can be obtained by using the CLI **save** command. With the `merge` parameter, the contents of the configuration file will be merged with the running configuration. The remaining configurations, which are not included in the configuration file, will remain unchanged.

After loading the configuration, use the **commit** command to commit the changes.</td></tr>
<tr><td>move [after | before | first | last | ipv4]</td><td>Moves an existing IPv4 address to a new position in the list of addresses. The address can be moved to the first or last (default) position in the list, or before or after another address. For example, the following command moves 172.30.137.37/9 before 172.30.137.31/19:

```
ruggedcom(config)# move ip fe-3-1 ipv4 address 172.30.137.37/19
 before 172.30.137.31/19
```
</td></tr>
<tr><td>no</td><td>Negates a command or sets it to its default setting. For example, the following command deletes the IP address 172.30.137.37/19:

```
ruggedcom(config)# no ip fe-3-1 ipv4 address 172.30.137.37/19
```

NOTE

*The **no** command affects only the parameter or setting of the node explicitly specified in the command. When using **no** to negate a parameter or setting that has dependencies, clearing the specific parameter does not clear the related dependencies.*

For example, the following command adds an IPv4 route with a gateway:

```
ruggedcom(config)# routing ipv4 route 192.168.33.0/24 via
 192.168.11.2
```

The following command deletes the gateway, but it does not delete the route:

```
ruggedcom(config)# no routing ipv4 route 192.168.33.0/24
 via 192.168.11.2
```

*The **no** deletes only the explicitly specified parameter or object.*</td></tr>
<tr><td>pwd</td><td>Displays the path to the current node. For example, after navigating to an IPv4 address, the following command displays the path through the command hierarchy to the current node:

```
ruggedcom(config-address-172.30.137.31/19)# pwd
 Current submode path:
 ip fe-3-1 \ ipv4 \ address 172.30.137.31/19
```
</td></tr>
<tr><td>rename</td><td>Changes the value of a parameter. For example, the following command changes the IPv4 address 172.30.137.36/19 to 172.30.137.40/19:

```
ruggedcom(config)# rename ip fe-3-1 ipv4 address 172.30.137.36/19
 172.30.137.40/19
```
</td></tr>
<tr><td>resolved</td><td>Issue this command when conflicts have been resolved. Conflicts are normally discovered when the commit operation is performed. Conflicts typically arise when multiple users edit the same parts of a configuration.</td></tr>
<tr><td>revert no-confirm</td><td>Copies the running configuration into the current configuration. This discards all changes to the current configuration. This command will prompt the user to confirm the action. Use the <code>no-confirm</code> parameter to revert the configuration without requiring confirmation.</td></tr>
</table>

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td>rollback configuration number</td><td>Returns the configuration to a previously committed configuration. The system stores a limited number of old configurations. After reaching the maximum number of old configurations, storing a new configuration deletes the oldest configuration in the list. The most recently committed configuration (the running configuration) appears as item 0 in the list. Select a number from the list and press Enter.

```
ruggedcom(config)# rollback configuration
 Possible completions:
 0      2012-01-08 13:51:46 by admin via cli
 1      2012-01-08 13:50:58 by admin via cli
 2      2012-01-08 12:05:46 by admin via cli
 3      2012-01-08 10:47:42 by admin via cli
 4      2012-01-08 07:49:38 by admin via cli
 5      2012-01-08 07:46:14 by admin via cli

 ruggedcom(config)# rollback configuration
```

After rolling back the configuration, use the commit command to commit the changes.</td></tr>
<tr><td>save filename</td><td>Saves the current configuration, without default values, to an ASCII file. Specify a filename for the file.

Current configuration means the configuration of the user's current level in the configuration data hierarchy. For example, if the user is at the top level, the save command will save the complete/full configuration of the device.

```
ruggedcom(config)# save {full-configuration-filename}
```

If the user is at a level other than the top level, such as the firewall level, the save command will save a partial configuration of the current level.

```
ruggedcom(config)#security firewall
ruggedcom(config-firewall)# save {firewall-configuration-filename}
```

Use this command along with the details command to include default values in the saved configuration file. For example:

```
ruggedcom(config)# save {filename} | details
```
</td></tr>
<tr><td>show</td><td>Shows configuration, history or command line interface parser information. Type show and press Tab to navigate through the items available to display.

This command can also be combined with the details command to display the default configuration values. For example:

```
ruggedcom# show running-config admin session-limits | details
```
</td></tr>
<tr><td>top command</td><td>Exits to the top level of the command hierarchy and, optionally, runs a command.</td></tr>
<tr><td>validate</td><td>Validats the current configuration.</td></tr>
<tr><td>wizard [rox_flash | rox_upgrade]</td><td>Runs the rox_flash or rox_upgrade wizards. For more information, refer to Section 3.10.5.2, “Downgrading Using ROXflash” and Section 3.10.3, “Upgrading the ROX II Software”.</td></tr>
</table>

Section 2.7

Configuring the CLI Interface

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

Parameter	Description
autowizard {true | false}	When enabled, the CLI prompts for required settings when a new identifier is created.
clear history	Clears the CLI history.
display-level	Determines the depth of hierarchical information to display in command results.
history *integer*	Determines the number of items to record in the CLI history.
output-file {*filename* | terminal}	Directs CLI output to the specified ASCII text file, or to the terminal. Output is directed to the specified destination until another destination is set with a subsequent **output-file** command.
paginate {true | false}	Lengthy output is paginated by default. When the output reaches the screen-length setting, the CLI prompts the user to press a key for more output. Press **Enter** to advance line-by-line or press **Space** to advance page-by-page. When disabled, output is not paginated.
screen-length *integer*	Determines the number of lines in a terminal page.
screen-width *integer*	Determines the length of terminal lines.

show-defaults {true | false}	Determines if default values are shown when displaying the configuration. When enabled, default values appear as comments after the configured value. In the following example, the default value for the contact value is shown as a comment following the configured contact string of *wsmith@example.com*:
	`ruggedcom# show running-config admin contact`
	` admin`
	` contact "wsmith@example.com"    ! Contact`
	` !`
	Default values only appear for parameters that have default values. If a parameter does not have a default value, no default appears when **show-defaults** is set to true.

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

Section 2.8
Accessing Different Modes

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

The following sections describe how to access the different modes within ROX II:

- Section 2.8.1, “Accessing BIST Mode”
- Section 2.8.2, “Accessing Service Mode”
- Section 2.8.3, “Accessing Maintenance Mode”

Section 2.8.1

Accessing BIST Mode

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

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

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

NOTE
BIST mode opens port 222.

To access BIST mode normally, do the following:

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

1. Disconnect the device from the network.
2. Connect to ROX II through the RS232 console connection and a terminal application. For more information, refer to Section 2.1.1, “Connecting Directly”.
3. Reboot the device. For more information, refer to Section 3.5, “Rebooting the Device”.
4. As soon as the device starts to boot up, press **ESC**. A list of possible boot modes for each partition appears.

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

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

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

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

 Will reboot after 60 seconds of inactivity
 :
```

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

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

```
BIST:~#
```

7. Type **`help`** to view a list of all available options under BIST.

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

1. Connect to ROX II through the RS232 console connection and a terminal application. For more information, refer to Section 2.1.1, “Connecting Directly”.
2. Cycle power to the device.
3. As the device begins to boot, press **Ctrl+c**. The BIST prompt appears.

```
BIST:~#
```

4. Type **`help`** to view a list of all available options under BIST.

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

1. Set the next boot to normal by typing:

```
nextboot normal
```

2. Reboot the device by typing:

```
reboot
```

3. Connect the device to the network.

Section 2.8.2

Accessing Service Mode

Service mode grants access to the Linux shell.

To access service mode, do the following:

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

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

NOTE
Service mode opens port 222.

1. Connect to ROX II through the RS232 console connection and a terminal application. For more information, refer to Section 2.1.1, "Connecting Directly".
2. Reboot the device. For more information, refer to Section 3.5, "Rebooting the Device".
3. As soon as the device starts to boot up, press **ESC**. A list of possible boot modes for each partition appears.

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

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

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

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

 Will reboot after 60 seconds of inactivity
 :
```

NOTE
In the example above, the text

```
Auto booting [4-0]
```

indicates the active partition is Boot Partition 4.

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

NOTE
If a unique password/passphrase has not been configured, use the factory default password. For more information, refer to Section 2.2, "Default Usernames and Passwords".

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

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

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

 The programs included with the Debian GNU/Linux system are free software;
 the exact distribution terms for each program are described in the
```

```
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
                                                                  8t-eterminal size
now 80x20

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

root@ruggedcom:~#
```

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

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

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

If a RUGGEDCOM APE module is installed, SSH can be permanently disabled. For more information, refer to the RUGGEDCOM APE User Guide.

7. If the device is connected to a network, disable SSH immediately by typing:

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

Section 2.8.3
Accessing Maintenance Mode

Maintenance mode grants access to the Linux shell.

To access maintenance mode, do the following:

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

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

1. In normal mode, type **`maint-login`** and press **Enter**. A password prompt appears.

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

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

   Example:

```
ruggedcom# maint-login
 Password:

 Welcome to ruggedcom Partition2 (Rev ROX 2.4.0 (2013-01-24 18:20)) RX1511 SN R15R-3410-PR061
 22:29:20 up 1 day,  8:42
 Temperature +41.0 C (+105.8 F)  Disk 25%  Memory 43%

 root@ruggedcom:~#
```

3 Device Management

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

> **NOTE**
> *For information about how to configure the device to work with a network, refer to Chapter 5, Setup and Configuration.*

- Section 3.1, "Determining the Product Version"
- Section 3.2, "Viewing Chassis Information and Status"
- Section 3.3, "Viewing the Parts List"
- Section 3.4, "Shutting Down the Device"
- Section 3.5, "Rebooting the Device"
- Section 3.6, "Restoring Factory Defaults"
- Section 3.7, "Decommissioning the Device"
- Section 3.8, "Managing Logs"
- Section 3.9, "Managing the Software Configuration"
- Section 3.10, "Upgrading/Downgrading the ROX II Software"
- Section 3.11, "Managing ROX II Applications"
- Section 3.12, "Managing Feature Keys"
- Section 3.13, "Installing and Backing Up Files"
- Section 3.14, "Managing Fixed Modules"
- Section 3.15, "Managing Line Modules"
- Section 3.16, "Managing Event Trackers"
- Section 3.17, "Managing Switched Ethernet Ports"
- Section 3.18, "Managing Routable Ethernet Ports"
- Section 3.19, "Managing Serial Ports"
- Section 3.20, "Managing Serial Port Protocols"
- Section 3.21, "Managing Ethernet Trunk Interfaces"
- Section 3.22, "Managing Cellular Modem Interfaces"
- Section 3.23, "Managing WAN Interfaces"
- Section 3.24, "Managing Virtual Switches"
- Section 3.25, "Managing a Domain Name System (DNS)"

Section 3.1
Determining the Product Version

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

To view information about the product, do the following:

1. Make sure the CLI is in Operational mode.
2. At the command prompt, type **show chassis** and press **Enter**. Information about the chassis appears.

Example:

```
ruggedcom# show chassis
chassis
chassis-status
model RX1501 software license "Layer 2 Standard Edition" order code ...
hardware
slot-hardware
ORDER
SLOT  FIELD  DETECTED MODULE                                        SERIAL NUMBER
------------------------------------------------------------------------------
pm1   XX     none                                                   none
lm1   XX     none                                                   none
lm2   TC4    T1/E1 w/ 4x RJ48                                       L15R-3333-PR301
lm3   D02    DDS w/ 1x RJ48                                         7
lm4   XX     none                                                   none
lm5   CG01   1000TX w/ 2x RJ45                                      L15R-3109-PR001
lm6   XX     none                                                   none
main  CM04A  RX1501 8 Gigabit Layer 2 w/ 6 LM slots and 1 PM slots  R15R-1310-PR032
```

Section 3.2
Viewing Chassis Information and Status

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

- Section 3.2.1, “Viewing the Slot Hardware”
- Section 3.2.2, “Viewing Module Information”
- Section 3.2.3, “Viewing Flash Card Storage Utilization”
- Section 3.2.4, “Viewing CPU/RAM Utilization”
- Section 3.2.5, “Viewing the Slot Status”
- Section 3.2.6, “Viewing the Slot Sensor Status”
- Section 3.2.7, “Viewing the Power Controller Status”

Section 3.2.1
Viewing the Slot Hardware

To view a list of the hardware installed in each slot, type:

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

A table or list similar to the following example appears:

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

This table or list provides the following information:

Parameter	Description
slot	**Synopsis:** pm1, pm2, main, sm, lm1, lm2, lm3, lm4, lm5, lm6, cm, em, trnk The slot name, as marked on the silkscreen across the top of the chassis.
order-field	The order code of the chassis as derived from the current hardware configuration.
detected-module	The installed module's type specifier.
serial-number	The installed module's unique serial number.

Section 3.2.2

Viewing Module Information

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

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

A table or list similar to the following example appears:

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

This table or list provides the following information:

Parameter	Description
slot	**Synopsis:** pm1, pm2, main, sm, lm1, lm2, lm3, lm4, lm5, lm6, cm, em, trnk The slot name, as marked on the silkscreen across the top of the chassis.
detected-module	The installed module's type specifier.
boot-loader-version	The version of the ROX bootloader software on the installed module.
fpga-version	The version of the ROX FPGA firmware (if any) running on the installed module.

Section 3.2.3

Viewing Flash Card Storage Utilization

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

```
show chassis storage
```

A table or list similar to the following example appears:

```
ruggedcom# show chassis storage | tab
storage
 flash
  storage name                  "Compact Flash"
  total capacity                994896
  current partition             "Partition #1"
  current partition capacity    490496
  secondary partition capacity 490496
  current partition usage       67
```

This table or list provides the following information:

Parameter	Description
storage-name	The type of storage.
total-capacity	The total capacity of the flash storage in KB.
current-partition	The partition ROX is currently running on and booted from.
current-partition-capacity	The capacity of the current partition in KB.
secondary-partition-capacity	The capacity of the secondary partition in KB.
current-partition-usage	The %usage of the current partition.

Section 3.2.4

Viewing CPU/RAM Utilization

To view the CPU/RAM utilization statistics for each module installed in the device, type:

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

A table or list similar to the following example appears:

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

This table or list provides the following information:

Parameter	Description
slot	**Synopsis:** pm1, pm2, main, sm, lm1, lm2, lm3, lm4, lm5, lm6, cm, em, trnk The slot name, as marked on the silkscreen across the top of the chassis.
detected-module	The installed module's type specifier.

Parameter	Description
cpu-load	The CPU load, in percent, on the installed module.
ram-avail	The proportion of memory (RAM) currently unused, in percent, on the installed module.
ram-avail-low	The lowest proportion of unused memory (RAM), in percent, recorded for the installed module since start-up.

Section 3.2.5
Viewing the Slot Status

To view the overall status of each slot, type:

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

A table or list similar to the following example appears:

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

This table or list provides the following information:

Parameter	Description
slot	**Synopsis:** pm1, pm2, main, sm, lm1, lm2, lm3, lm4, lm5, lm6, cm, em, trnk The slot name, as marked on the silkscreen across the top of the chassis.
detected-module	The installed module's type specifier.
state	**Synopsis:** unknown, empty, disabled, resetting, operating, failed, disconnected The current state of the installed module.
status-string	The runtime status of the installed module.
uptime	The total time elapsed since the start-up of the installed module.
start-date	The date on which the installed module was started up.
start-time	The time at which the installed module was started up.

Section 3.2.6

Viewing the Slot Sensor Status

To view information about the slot sensors, type:.

```
show chassis sensors slot-sensors
```

A table or list similar to the following example appears:

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

This table or list provides the following information:

Parameter	Description
slot	**Synopsis:** pm1, pm2, main, sm, lm1, lm2, lm3, lm4, lm5, lm6, cm, em, trnk The slot name, as marked on the silkscreen across the top of the chassis.
detected-module	The installed module's type specifier.
temperature	The temperature, in degrees C, of the installed module. If multiple temperature sensors are present on the board, the maximum reading is reported.
current-supply	The power supply current, in mA, being drawn by the installed module.
voltage-supply	The power supply voltage, in mV, seen by the installed module.

Section 3.2.7

Viewing the Power Controller Status

To view information about the power controller, type:

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

A table or list similar to the following example appears:

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

This table or list provides the following information:

Parameter	Description
pm-slot	**Synopsis:** pm1, pm2 The name of the power module slot as labeled on the chassis.
mov-protection	**Synopsis:** na, working, damaged The state of the MOV protection circuit.

Parameter	Description
pm-temperature	The temperature (Celsius) inside the power module.
pm-current	The current (mA) sourced by the power module.
pm-voltage	The voltage (mV) sourced by the power module.

Section 3.3

Viewing the Parts List

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

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

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

```
ruggedcom# show running-config chassis part-list | tab
MODEL   ORDERFIELD  PARTNUMBER                   PARTNAME
-------------------------------------------------------------------------------
RX1000  24          12-10-0012                   24VDC (9-36VDC) Power Supply
RX1000  48          12-10-0004                   48VDC (36-59VDC) Power Supply
RX1000  CM01        12-01-0099-001               RX1000 Control Module
RX1000  D01         13-01-0007                   DSL card
RX1000  D02         13-01-0008                   DDS Card
RX1000  DS3         13-01-0012                   1x T3/E3
RX1000  FX01        12-11-0007                   2x 100Fx MM ST
RX1000  FX02        12-11-0009                   2x 100Fx MM SC
RX1000  FX03        12-11-0008                   2x 100Fx MM MTRJ
RX1000  FX04        12-11-0006                   2x 100Fx SM ST 20km
RX1000  FX05        12-11-0005                   2x 100Fx SM SC 20km
RX1000  FX06        12-11-0004                   2x 100Fx SM LC 20km
.
.
.
```

Section 3.4

Shutting Down the Device

To shut down the device, type:

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

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

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

```
admin shutdown
```

Section 3.5

Rebooting the Device

To reboot the device, type:

```
admin reboot
```

Section 3.6

Restoring Factory Defaults

To restore the factory defaults for the device, navigate to ***admin » restore-factory-defaults*** and configure the following parameter(s):

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

If necessary, include the following options in the command:

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

Section 3.7

Decommissioning the Device

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

To decommission the device, do the following:

1. Obtain a copy of the 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 *ROX II v2.6 CLI User Guide*Section 2.8.3, "Accessing Maintenance Mode".
3. Delete the current boot password/passphrase by typing:

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

4. Type **exit** and press **Enter**.
5. Log in to ROX II. For more information, refer to Section 2.3, "Logging In".
6. Flash the ROX II firmware obtained in Step 1 to the inactive partition and reboot the device. For more information, refer to Section 3.10.5.2, "Downgrading Using ROXflash".
7. Repeat Step 5 and Step 6 to flash the ROX II firmware obtained in Step 1 to the other partition and reboot the device.
8. Shut down the device. For more information, refer to Section 3.4, "Shutting Down the Device".

Section 3.8
Managing Logs

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 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 3.8.1, "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.

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

- Section 3.8.1, “Viewing Logs”
- Section 3.8.2, “Deleting Logs”
- Section 3.8.3, “Managing Diagnostic Logs”
- Section 3.8.4, “Managing Remote Syslog Servers”
- Section 3.8.5, “Managing Remote Server Selectors”

Section 3.8.1

Viewing Logs

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

> **NOTE**
> *For information about downloading log files from the device, refer to Section 3.13.2, “Backing Up Files”.*

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

```
show log file
```

Where:

- *file* is the log file to view

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

```
show log auth.log
```

A result similar to the following is displayed:

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

Section 3.8.2

Deleting Logs

To delete all logs stored on the device, type:

```
admin delete-logs
```

Section 3.8.3

Managing Diagnostic Logs

Diagnostic logs are available for troubleshooting the device. Various device behaviour 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 ROX II. Only enable diagnostic logging when directed by Siemens.

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

- Section 3.8.3.1, “Enabling/Disabling the Developer's Log”
- Section 3.8.3.2, “Enabling/Disabling the SNMP Log”
- Section 3.8.3.3, “Enabling/Disabling the NETCONF Summary Log”
- Section 3.8.3.4, “Enabling/Disabling the NETCONF Trace Log”
- Section 3.8.3.5, “Enabling/Disabling the XPATH Trace Log”
- Section 3.8.3.6, “Enabling/Disabling the WebUI Trace Log”

Section 3.8.3.1

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 ROX II. Only enable diagnostic logging when directed by Siemens.

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

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

   Enable

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

   Disable

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

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

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

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

Section 3.8.3.2

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 ROX II. Only enable diagnostic logging when directed by Siemens.

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

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

   Enable

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

   Disable

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

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

Section 3.8.3.3

Enabling/Disabling the NETCONF Summary Log

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

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

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

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

   Enable

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

   Disable

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

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

Section 3.8.3.4

Enabling/Disabling the NETCONF Trace Log

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

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

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

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

   Enable

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

   Disable

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

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

Section 3.8.3.5

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 ROX II. Only enable diagnostic logging when directed by Siemens.*

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

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

   Enable

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

   Disable

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

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

Section 3.8.3.6

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 ROX II. Only enable diagnostic logging when directed by Siemens.*

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

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

   Enable

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

   Disable

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

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

Section 3.8.4

Managing Remote Syslog Servers

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

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

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

- Section 3.8.4.1, “Viewing a List of Remote Servers”
- Section 3.8.4.2, “Adding a Remote Server”
- Section 3.8.4.3, “Deleting a Remote Server”

Section 3.8.4.1

Viewing a List of Remote Servers

To view a list of remote servers, type:

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

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

```
ruggedcom# show running-config admin logging server
admin
 logging
  server 172.30.144.254
   enabled
   selector 1
```

```
    no negate
    facility-list [ all ]
   !
  !
 !
!
```

If no remote servers have been configured, add servers as needed. For more information, refer to Section 3.8.4.2, “Adding a Remote Server”.

Section 3.8.4.2
Adding a Remote Server

To add a remote server, do the following:

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

   ```
   admin logging server address
   ```

   Where:

   - *address* is the IP address of the remote server
3. Configure the following parameter(s) as required:

Parameter	Description
enabled	Enables/disables the feed to the remote logging server.

4. Configure one or more selectors for the server. For more information, refer to Section 3.8.5.2, “Adding a Remote Server Selector”.
5. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 3.8.4.3
Deleting a Remote Server

To delete a remote server, do the following:

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

   ```
   no admin logging server address
   ```

   Where:

   - *address* is the IP address of the remote server.
3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 3.8.5
Managing Remote Server Selectors

Remote server selectors filter the information sent to specific servers.

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

- Section 3.8.5.1, “Viewing a List of Remote Server Selectors”
- Section 3.8.5.2, “Adding a Remote Server Selector”
- Section 3.8.5.3, “Deleting a Remote Server Selector”

Section 3.8.5.1
Viewing a List of Remote Server Selectors

To view a list of remote server selectors, type:

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

Where:

- *address* is the IP address of the remote server.

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

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

If no remote server selectors have been configured, add selectors as needed. For more information, refer to Section 3.8.5.2, “Adding a Remote Server Selector”.

Section 3.8.5.2
Adding a Remote Server Selector

To add a remote server selector, do the following:

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

   ```
   admin logging server address selector name
   ```

   Where:

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

Parameter	Description
negate	Excludes messages defined in the *Remote Server Selector* fields from the log. Selecting this option acts as a logical NOT for the selector definition.

Parameter	Description
	For example: Selecting **same**, **debug**, and **mail** in the *Comparison*, *Level*, and *Facility-list* fields includes debug messages from the mail subsystem in the log. Selecting **Negate** *excludes* debug messages from the mail subsystem from the log.
comparison { comparison }	**Synopsis:** same_or_higher, same **Default:** same_or_higher The message severity levels to include in the log: • **same:** includes only messages of the severity level selected in the *Level* field. • **same_or_higher:** includes messages of the severity level selected in the *Level* field, and all messages of higher severity. For example: • Selecting **debug** in the *Level* field and **same** in the *Comparison* field includes only debug messages in the log. • Selecting **debug** in the *Level* field and **same_or_higher** in the *Comparison* field includes debug and all higher severity messages in the log.
level { level }	**Synopsis:** emerg, alert, crit, err, warning, notice, info, debug, none, all **Default:** all The base message severity level to include in the log. **all** includes all messages. **none** excludes all messages. Other levels are listed in order of increasing severity.
facility-list { facility-list }	**Synopsis:** auth, authpriv, cron, daemon, ftp, kern, lpr, mail, news, security, syslog, user, uucp, local0, local1, local2, local3, local4, local5, local6, local7, all **Synopsis:** "facility-list" occurs in an array of at least 1 and at most 8 elements The subsystems generating log messages. Messages from the selected subusystems are included in the log. At least one subsystem must be selected; up to 8 subsystems can be selected.

4. Configure one or more selectors for the server. For more information, refer to Section 3.8.5.2, “Adding a Remote Server Selector”.
5. Type **`commit`** and press **Enter** to save the changes, or type **`revert`** and press **Enter** to abort.

Section 3.8.5.3
Deleting a Remote Server Selector

To delete a remote server selector, do the following:

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

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

Where:

- *address* is the IP address of the remote server
- *name* is the name of the log selector identifier

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

Section 3.9

Managing the Software Configuration

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

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

- Section 3.9.1, "Saving the Configuration"
- Section 3.9.2, "Loading a Configuration"

Section 3.9.1

Saving the Configuration

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

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

Where:

- *filename* is the name of the configuration file

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

1. Make sure the CLI is in Configuration mode.
2. Save the default values by typing:

   ```
   save filename | details
   ```

   Where:

   - *filename* is the name of the configuration file

Section 3.9.2

Loading a Configuration

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

1. Load a configuration file by typing:

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

   Where:

   - *filename* is the name of the configuration file
2. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 3.10

Upgrading/Downgrading the ROX II Software

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

- Section 3.10.1, "Configuring the Upgrade Source"

- Section 3.10.2, “Setting Up an Upgrade Server”
- Section 3.10.3, “Upgrading the ROX II Software”
- Section 3.10.4, “Stopping/Declining a Software Upgrade”
- Section 3.10.5, “Downgrading the ROX II Software”

Section 3.10.1

Configuring the Upgrade Source

Firmware for upgrading or downgrading ROX II can be uploaded from either an upgrade server or a portable USB Mass Storage drive. For information about setting up an upgrade server, refer to Section 3.10.2, “Setting Up an Upgrade Server”.

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

1. Make sure the CLI is in Configuration mode.
2. Configure the following parameter(s) as required:

Parameter	Description
repository-url { repository-url }	The URL for the upgrade server or file system. Supported URIs are http, https and ftp. To upgrade from a USB device, the URL format is 'usb://<usb-device-name>/path-to-repository' and only one single partition is supported.
target-version { target-version }	The target software version. Specify a specific software release in the form of 'rrX.Y.Z' or enter 'current' to upgrade to the latest software release available on the upgrade server.

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

Section 3.10.2

Setting Up an Upgrade Server

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

The upgrade server must meet the following requirements:

- Each device that will be upgraded/downgraded must have access to a host that acts as a Web server or FTP server. The host must also be able to download new software releases from www.siemens.com/ruggedcom.
- The server must have sufficient disk space for at least two full software releases. Each full software release is approximately 75 Mbits, although most upgrades are typically much smaller.
- The server must have sufficient bandwidth. The bandwidth requirements will be based on the number of devices, the size of the upgrade, and when the devices launch an upgrade. The bandwidth is also limited by default for each device to 500 kbps. A modest (e.g. 486 class machine) web server should be able to serve files up to the limit of the network interface bandwidth.
- The server must be able to accept at least as many HTTP, HTTPS or FTP connections as there are devices on the network.
- The server must contain and publish a directory specifically for ROX II software releases. The name of this directory will be specified in the upgrade settings for each device.
- Communication between the server and the device must be along a secure channel, such as IPsec.

- For upgrades via HTTPS, the server's public key must be signed by a trusted Certificate Authority (CA). A list of recognized CA's is available under `/etc/ssl/certs/`

> **NOTE**
> *Each device should be configured to upgrade at different times to minimize impact on the network. A large upgrade (or a low bandwidth limiting value on each device) may cause all the devices to upgrade at the same time.*

The following sections describe how to configure an upgrade server:

- Section 3.10.2.1, “Adding Software Releases to the Upgrade Server”
- Section 3.10.2.2, “Using Microsoft IIS Manager 6.0 or Higher as an Upgrade Server”

Section 3.10.2.1

Adding Software Releases to the Upgrade Server

Software releases are obtained from www.siemens.com/ruggedcom as compressed ZIP files.

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

1. Download the appropriate ROX II software release from www.siemens.com/ruggedcom to the upgrade directory on the upgrade server.

   > **NOTE**
   > *Software release filenames take the form of rrX.Y.Z.zip, where X represents the major release number, Y represents the minor release number, and Z represents the patch release number.*

2. Extract the compressed ZIP file within the directory. The file will extract to a folder that has the same name as the major release (i.e. "rrX"). Subsequence releases will also be extracted to this folder.

Section 3.10.2.2

Using Microsoft IIS Manager 6.0 or Higher as an Upgrade Server

When using Microsoft Internet Information Services (IIS) Manager 6.0 or higher as an upgrade server, a new application/octet-stream MIME type named "*" must be added to the IIS properties. This is required for IIS to consider ROX II upgrade packets as an application/octet-stream, otherwise ROX II upgrades will fail.

To add the new MIME type to the IIS properties, do the following:

1. In the Windows **Start** menu, right-click on **My Computer** and select **Manage**. The **Computer Management** dialog appears.
2. Under **Services and Applications**, locate the **Internet Information Services (IIS) Manager** node. Right-click on your ROX upgrade repository website and select **Properties**. The **Properties** dialog appears.
3. Select the **HTTP Headers** tab and click **MIME Types**. The **MIME Types** dialog appears.
4. Click **New**. The **MIME Type** dialog appears.
5. In the **Extension** field, type **`*`**.
6. In the **MIME type** field, type **`application/octet-stream`**.
7. Click **OK** on the **MIME Type**, **MIME Types**, and **Properties** dialog boxes.

Section 3.10.3

Upgrading the ROX II Software

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

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

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

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

If required, the software upgrade can be stopped/declined at any time before the device is rebooted. For more information about stopping/declining a software upgrade, refer to Section 3.10.4, "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 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.
2. Make sure the source of the software upgrade has been configured. For more information, refer to Section 3.10.1, "Configuring the Upgrade Source".
3. Make sure the CLI is in Configuration mode.
4. Launch the software upgrade wizard by typing:

   ```
   wizard rox_upgrade
   ```

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

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

   ```
   ruggedcom(config)# wizard rox_upgrade
   The upgrade repository url is set to: http://rceng03/debianppc/rr2
   Press <ENTER> to accept this or type a new address to change it:

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

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

   Upgrading system to Partition 2
   ```

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

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

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

Starting download of packages...

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

Installing packages...

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

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

5. If the software upgrade is successful, reboot the device or decline the software upgrade. For more information, refer to Section 3.5, “Rebooting the Device” or Section 3.10.4, “Stopping/Declining a Software Upgrade”.

Section 3.10.4

Stopping/Declining a Software Upgrade

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

> **IMPORTANT!**
> *A software upgrade can only be declined before the device is rebooted. If the software upgrade has already been activated following a reboot, the previous software version installed on the other partition can be activated. For more information, refer to Section 3.10.5.1, “Rolling Back a Software Upgrade”.*

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

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

Section 3.10.5

Downgrading the ROX II Software

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

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

- Section 3.10.5.1, “Rolling Back a Software Upgrade”
- Section 3.10.5.2, “Downgrading Using ROXflash”

Section 3.10.5.1
Rolling Back a Software Upgrade

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

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

```
admin software-upgrade rollback-reboot
```

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

Section 3.10.5.2
Downgrading Using ROXflash

ROXflash is used to flash any previous version of a ROX II software image to the inactive partition. Images are obtained through a Siemens Sales representative.

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

IMPORTANT!
Use ROXflash only to install earlier versions of the ROX II software. Newer software versions should be installed using the software upgrade functions. For more information about upgrading the ROX II software, refer to *Section 3.10.3, "Upgrading the 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 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.
2. Make sure the CLI is in Configuration mode.
3. Launch the ROXflash wizard by typing:

```
wizard rox_flash
```

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

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

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


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

```
Enter url: scp://root:admin@rceng03/debianppc/rr2/image/imagerr2.tar.bz2
Starting download of ROXII image...

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

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

4. If the software downgrade is successful, reboot the device. For more information, refer to Section 3.5, "Rebooting the Device".

Section 3.11

Managing ROX II Applications

ROX II applications are special add-ons that extend the functionality of ROX, such as enhanced support for other ROX products (e.g. CrossBow, eLAN, etc.). They are installed and upgraded the same as the 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 ROX II applications are released as repositories and must be hosted by an upgrade server. For more information about setting up an upgrade server, refer to Section 3.10.2, "Setting Up an Upgrade Server".

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

- Section 3.11.1, "Viewing a List of Installed Applications"
- Section 3.11.2, "Installing an Application"
- Section 3.11.3, "Upgrading an Application"
- Section 3.11.4, "Uninstalling an Application"
- Section 3.11.5, "Managing Application Repositories"

Section 3.11.1

Viewing a List of Installed Applications

To view a list of ROX II applications installed on the device, type:

```
show admin software-upgrade apps installed-apps
```

If applications have been installed, a table or list similar to the following example appears:

```
ruggedcom# show admin software-upgrade apps installed-apps
APP NAME  VERSION
-------------------
crossbow  4.1.2
elan      8.0.2
```

If no applications have been installed, install applications as needed. For more information, refer to Section 3.11.2, "Installing an Application".

Section 3.11.2
Installing an Application

To install an application, do the following:

1. Make sure the CLI is in Configuration mode.
2. Make sure a repository for the application has been configured before installing the application. For more information, refer to Section 3.11.5.3, “Adding a Repository”.
3. Install the application by typing:

```
admin software-upgrade apps install-app app-name name
```

   Where:

   - *name* is the name of the application to install as it appears in the repository configuration. To install more than one application, use a comma seperated list.

Section 3.11.3
Upgrading an Application

To upgrade an application, do the following:

1. Make sure the CLI is in Configuration mode.
2. Install the application by typing:

```
admin software-upgrade apps upgrade-app app-name name
```

   Where:

   - *name* is the name of the application to upgrade as it appears in the repository configuration. To upgrade more than one application, use a comma seperated list.

Section 3.11.4
Uninstalling an Application

To uninstall an application, do the following:

1. Make sure the CLI is in Configuration mode.
2. Install the application by typing:

```
admin software-upgrade apps uninstall-app app-name name
```

   Where:

   - *name* is the name of the application to uninstall as it appears in the repository configuration. To uninstall more than one application, use a comma seperated list.

Section 3.11.5

Managing Application Repositories

Before any ROX II application can be installed or upgraded, a connection to its repository on the upgrade server must be configured.

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

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

- Section 3.11.5.1, “Viewing a List of Repositories”
- Section 3.11.5.2, “Checking the Repository Connection”
- Section 3.11.5.3, “Adding a Repository”
- Section 3.11.5.4, “Deleting a Repository”

Section 3.11.5.1

Viewing a List of Repositories

To view a list of ROX II application repositories, type:

```
show running-config admin software-upgrade apps repository
```

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

```
ruggedcom# show running-config admin software-upgrade apps repository | tab
APP NAME  URL                                             VERSION
-----------------------------------------------------------------
crossbow  http://10.200.20.231/crossbow-repo/debianppc  rs2

 !
!
```

If no repositories have been configured, add repositories as needed. For more information, refer to Section 3.11.5.3, “Adding a Repository”.

Section 3.11.5.2

Checking the Repository Connection

To check the connection with a repository, type:

```
admin software-upgrade apps check-repository-connection app-name name
```

Where:

- *name* is the name of the repository as it appears in the repository configuration. To check the connection with more than one repository, use a comma seperated list.

The connection results are displayed.

Section 3.11.5.3

Adding a Repository

To add an application repository, do the following:

> **NOTE**
> *An application repository must be configured before an application can be installed or upgraded.*

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

   ```
   admin software-upgrade apps repository app-name name
   ```

   Where:

   - *name* is the name of the repository as it appears in the application configuration. Consult the release notes for the appplication.
3. Configure the following parameter(s) as required:

Parameter	Description
url { url }	The URL of the upgrade server hosting the app repository (http, https, and ftp are supported).
version { version }	The version of the app you are installing or upgrading.

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

Section 3.11.5.4

Deleting a Repository

To delete an application repository, do the following:

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

   ```
   no admin software-upgrade apps repository app-name name
   ```

   Where:

   - *name* is the name of the repository as it appears in the application configuration. Consult the release notes for the application.
3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 3.12

Managing Feature Keys

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 ROX II features are only available through the purchase of feature levels. For more information about the available feature levels, refer to the product datasheet for the device available at www.siemens.com/ruggedcom or contact a Siemens Sales representative.*

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

When ordering feature levels, make sure to provide the *main* serial number 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 3.1, "Determining the Product Version".

The following sections describe how to manage feature keys:

- Section 3.12.1, "Viewing the Contents of a Feature Key"
- Section 3.12.2, "Installing Feature Keys"

Section 3.12.1
Viewing the Contents of a Feature Key

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

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

```
file show-featurekey filename
```

Where:

- *filename* is the name of feature key file stored on the device

For example:

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

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

```
ruggedcom# file show-featurekey 1_cmRX1K-12-11-0015.key
GPG_FEATUREKEY_LEVEL=1
GPG_FEATUREKEY_CM_SERIALNUMBER=RX1K-12-11-0015
GPG_FEATUREKEY_SIGNATURE=iEYEABECAAYFAk091pAACgkQP2pya+G5kdZeKACeKdHUB2G1T73Dymq8IjSdYDK
AiskAn3abBpCEhfLXxY2ZlVbvGNwDZow2
ruggedcom#
```

Section 3.12.2
Installing Feature Keys

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

Feature keys can be installed from a host computer or a USB Mass Storage drive.

To install a feature key from a host computer, do the following:

> **NOTE**
> *Before installing a feature key from a host computer, the following information is required:*
> - *The file name of the feature key*
> - *The username and password required to log into the host computer where the feature key is stored*
> - *The hostname or IP address of the computer where the feature key is stored*

1. Make sure the CLI is in Operational mode.
2. Install the feature key by typing:

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

   Where:

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

   For example:

   ```
   file scp-featurekey-from-url wsmith@10.200.10.39:/files/keys/1_cmRX1K-12-11-0015.key
    1_cmRX1K-12-11-0015.key
   ```

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

   ```
    ruggedcom# file scp-featurekey-from-url wsmith@10.200.20.39:/files/keys/
   1_cmRX1K-12-11-0015.key 1_cmRX1K-12-11-0015.key
   wsmith@10.200.20.39's password:
   1_cmRX1K-12-11-0015.key                100%  192     0.2KB/s   00:00
   ```

To install a feature key from a USB Mass Storage drive, do the following:

1. Make sure the CLI is in Operational mode.
2. Install the USB Mass Storage drive in the USB port on the device.
3. Install the feature key by typing:

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

   Where:

   - *path* is the directory path to the feature key file on the USB Mass Storage drive.
   - *current-filename* is the current name of the feature key file.
   - *new-filename* is the new name of the feature key file on the device. This parameter is optional. The current filename will be used if a new filename is not provided.

   For example:

   ```
   file scp-featurekey-from-url usb:/repository/keys/1_cmRX1K-12-11-0015.key 1_cmRX1K-12-11-0015.key
   ```

   The system uploads the feature key file:

```
 ruggedcom# file scp-featurekey-from-url usb:///repository/keys/
1_cmRX1K-12-11-0015.key 1_cmRX1K-12-11-0015.key
1_cmRX1K-12-11-0015.key                100%  192     0.2KB/s   00:00
```

Section 3.13

Installing and Backing Up Files

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

The following sections describe how to install and backup files:

- Section 3.13.1, “Installing Files”
- Section 3.13.2, “Backing Up Files”

Section 3.13.1

Installing Files

To install a file on the device, 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.
2. Make sure the CLI is in Configuration mode.
3. Navigate to ***admin » install-files*** and configure the following parameter(s) as required:

Parameter	Description
file-type { file-type }	**Synopsis:** config, featurekey The file types to be copied.
url { url }	The URL of the ROX file to copy. SCP, SFTP, FTPS, FTP, and HTTP are supported for the file transfer. To install from a USB device, the format is 'usb://path-to-file-on-system' and only one single partition is supported. For the rest of the 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.

Section 3.13.2

Backing Up Files

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

1. If the file's destination is a USB Mass Storage drive, insert the drive in the USB port on the device.
2. Make sure the CLI is in Configuration mode.
3. Navigate to ***admin » backup-files*** and configure the following parameter(s) as required:

Parameter	Description
file-type { file-type }	**Synopsis:** config, featurekey, logfiles, rollbacks The file types to copy.

Parameter	Description
file { file }	The file names to copy.
timestamp	**Default:** false If enabled, a timestamp will be appended to the file name. This option is not applicable to file names that contain '*'.
url { url }	The URL of the ROX file to copy. SCP, SFTP, FTPS, FTP and HTTP are supported for the file transfer. To save to a USB device, the format is 'usb://path-to-file-on-system' and only one single partition is supported. For the rest of the 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.

Section 3.14

Managing Fixed Modules

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

- Section 3.14.1, "Viewing a List of Fixed Module Configurations"
- Section 3.14.2, "Adding a Fixed Module Configuration"
- Section 3.14.3, "Deleting a Fixed Module Configuration"

Section 3.14.1

Viewing a List of Fixed Module Configurations

To view a list of fixed module configurations, type:

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

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

```
ruggedcom# show running-config chassis fixed-modules
  fixed-module cm
   module-type "MX5000 Control Module"
   partnumber  "12-86-0016-H02 12-86-0035-H02"
  !
  fixed-module em
   module-type "Front Panel w/ Interfaces and LEDs"
   partnumber  12-86-0034-001
  !
!
!
```

If no fixed modules have been configured, add fixed module configurations as needed. For more information, refer to Section 3.14.2, "Adding a Fixed Module Configuration".

Section 3.14.2

Adding a Fixed Module Configuration

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

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

```
chassis fixed-modules fixed-module slot
```

   Where:

   - *slot* is the name of the module location
3. Configure the following parameter(s) as required:

Parameter	Description
module-type { module-type }	The module type to be used in this slot.
partnumber { partnumber }	The part number of the module type in this slot.

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

Section 3.14.3
Deleting a Fixed Module Configuration

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

1. Make sure the CLI is in Configuration mode.
2. Delete the configuration for a fixed module by typing:

```
no chassis fixed-modules fixed-module slot
```

   Where:

   - *slot* is the name of the module location
3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 3.15
Managing Line Modules

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

- Section 3.15.1, “Removing a Line Module”
- Section 3.15.2, “Installing a New Line Module”
- Section 3.15.3, “Viewing a List of Line Module Configurations”
- Section 3.15.4, “Configuring a Line Module”
- Section 3.15.5, “Enabling/Disabling Controlled Bypass for M12 Line Modules”

Section 3.15.1
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 3.4, “Shutting Down the Device”.
2. Remove the line module from the device.

Section 3.15.2

Installing a New Line Module

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

1. Make sure the CLI is in Configuration mode.
2. Set the module type to *none* by typing:

   ```
   chassis line-modules line-module slot module-type type
   ```

   Where:

   - *slot* is the name of the module location
   - *type* is the module type
3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.
4. Shut down the device. The device will shutdown for a period of time before rebooting and restarting. The default time-out period is 300 seconds (five minutes). If more time is required to complete the procedure, disconnect power from the device during the time-out period. For more information on how to shutdown the device, refer to Section 3.4, “Shutting Down the Device”.
5. Insert the new line module into the empty slot in the chassis.
6. Reboot the device. For more information, refer to Section 3.5, “Rebooting the Device”.

   After the device is rebooted, the new line module is automatically detected and operational.
7. If the line module is different from the previous module installed in the same slot, add a configuration for the new line module. For more information, refer to Section 3.15.4, “Configuring a Line Module”.

Section 3.15.3

Viewing a List of Line Module Configurations

To view a list of line module configurations, type:

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

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

```
ruggedcom# show running-config chassis line-modules | tab
chassis
line-modules
  line-module
                                                  ADMIN    ADMIN
SLOT  MODULE TYPE                                 ENABLED  BYPASS
-------------------------------------------------------------------
sm    SM 88 Gigabit Layer 3 w/ 2x 10G SFP+ slots  X        -
lm1   4x 10/100/1000TX RJ45                       X        -
lm2   none                                        -        -
lm3   none                                        -        -
```

```
lm4   16x 10/100TX RJ45                          X        -
lm5   16x 10/100TX RJ45                          X        -
lm6   16x 10/100TX RJ45                          X        -

!
!
```

If no line modules have been configured, install line module as needed. For more information, refer to Section 3.15.2, “Installing a New Line Module”.

Section 3.15.4

Configuring a Line Module

To configure a line module, do the following:

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

Parameter	Description
detected-module	The installed module's type specifier.
module-type { module-type }	Sets the module type to be used in this slot.
admin-enabled	Sets the administrative state for a module. Enabling the module powers it on.

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

Section 3.15.5

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.

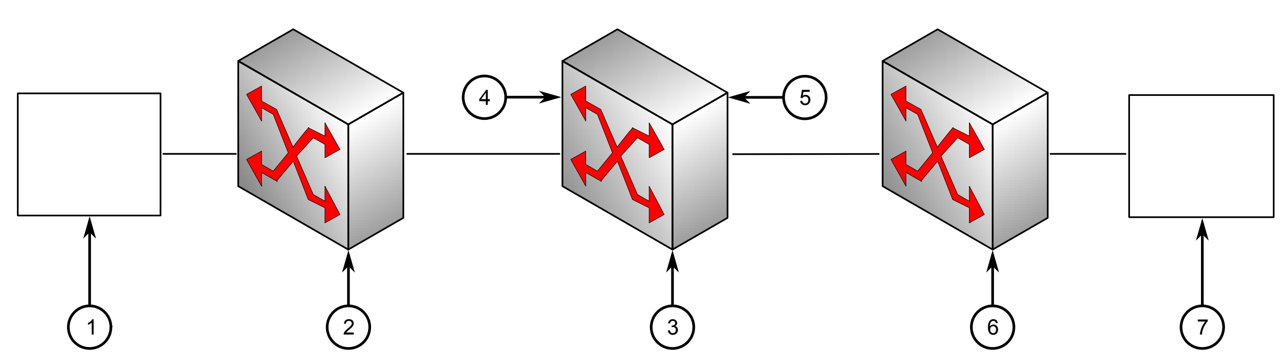

Figure 3: Sample Controlled Bypass Diagram

1. Ethernet Traffic Generator **2.** Router 1 **3.** Defective Router **4.** M12 Line Module Port 1 **5.** M12 Line Module Port 2 **6.** Router 2 **7.** Receiving Traffic

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

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

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

   > **NOTE**
   > *The default status is not bypassed. To view the current status, type:*
   >
   > `show chassis line-modules line-module module bypass`

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

3. Enable or disable controlled bypass by typing:

   ```
   chassis line-modules line-module module bypass admin-bypass
   ```

   Where:

   - *module* is the M12 line module
4. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

> **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 3.16

Managing Event Trackers

Trackers monitor the availability of hosts or devices by periodically transmitting ICMP messages (or pings). Based on the ICMP results, the tracker updates operational data with the status of the host or device as it changes (i.e. between "up " and "down" states). Other parts of the system can then subscribe to the operational data to be notified when changes take place.

Where available, a tracker can allow a user greater flexibility when configuring a feature. For example, advertised or received routes can be filtered or blocked entirely, based on the status of the tracker.

> **NOTE**
> *Trackers only use ICMP messages to ping an IP target. Therefore, it can only provide availability for an IP device, and only up to the IP layer.*

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

- Section 3.16.1, “Viewing a List of Event Trackers”
- Section 3.16.2, “Viewing Event Tracker Statistics”
- Section 3.16.3, “Adding an Event Tracker”
- Section 3.16.4, “Deleting an Event Tracker”

Section 3.16.1

Viewing a List of Event Trackers

To view a list of event trackers, type:

```
show running-config global tracking
```

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

```
ruggedcom# show running-config global tracking
global
 tracking
  event host-in-lan-11
   target   192.168.11.100
   timeout  500
   interval 500
   fall     3
   rise     3
  !
 !
!
```

If no event trackers have been configured, add event trackers as needed. For more information, refer to Section 3.16.3, “Adding an Event Tracker”.

Section 3.16.2

Viewing Event Tracker Statistics

ROX II records statistics for each event tracker.

To view the statistics for an event tracker, type:

```
show global tracking event statistics
```

A list similar to the following example appears:

```
ruggedcom# show global tracking event statistics
                                                    STANDARD
                ECHO      ECHO     MIN  AVERAGE  MAX  DEVIATION
NAME            ATTEMPTS  REPLIES  RTT  RTT      RTT  RTT
-----------------------------------------------------------------
host-in-lan-11  0         0        0.0  0.0      0.0  0.0
```

This list provides the following information:

Parameter	Description
echo-attempts	The number of echo attempts.
echo-replies	The number of echo replies.

Parameter	Description
min-rtt	The minimum of the round trip time (in milliseconds).
average-rtt	The average of the round trip time (in milliseconds).
max-rtt	The maximum of the round trip time (in milliseconds).
standard-deviation-rtt	The standard deviation of the round trip time (in milliseconds).

Section 3.16.3

Adding an Event Tracker

To add an event tracker, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the event tracker by typing:

```
global tracking event name
```

   - *name* is the name of the tracking event

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

Parameter	Description
target { target }	**Synopsis:** The host type represents either an IP address or a DNS domain name. Configures the ping target as an IPv4 address or hostname.domain.
source-ip { source-ip }	**Synopsis:** The ip-address type represents an IP address and is IP version neutral. The format of the textual representations implies the IP version. Sets the source address to a specified IPv4 address.
source-interface { source-interface }	Forces a ping on a selected interface.
timeout { timeout }	Determines how many milliseconds to wait for the ICMP response.
interval { interval }	Determines how many milliseconds to wait before sending another ICMP request.
fall { fall }	The number of times a failure occurs before changing the tracking state from up to down.
rise { rise }	The number of times success occurs before changing the tracking state from down to up.
state	**Synopsis:** up, down **Default:** up The state of the event.

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

Section 3.16.4

Deleting an Event Tracker

To delete an event tracker, do the following:

1. Make sure the CLI is in Configuration mode.

2. Delete the event tracker by typing:

```
no global tracking event name
```

   - *name* is the name of the tracking event

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

Section 3.17

Managing Switched Ethernet Ports

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

- Section 3.17.1, “Viewing a List of Switched Ethernet Ports”
- Section 3.17.2, “Configuring a Switched Ethernet Port”
- Section 3.17.3, “Configuring Port Security”
- Section 3.17.4, “Viewing Switched Ethernet Port Statistics”
- Section 3.17.5, “Viewing RMON Port Statistics”
- Section 3.17.6, “Clearing Switched Ethernet Port Statistics”
- Section 3.17.7, “Resetting a Switched Ethernet Port”
- Section 3.17.8, “Testing Switched Ethernet Port Cables”

Section 3.17.1

Viewing a List of Switched Ethernet Ports

To view a list of switched Ethernet ports configured on the device, type:

```
show running-config interface switch
```

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

```
ruggedcom# show running-config interface switch
interface
 switch lm1 1
  auton      on
  speed      auto
  duplex     auto
  switchport
  no flow-control
  no alias
  rate-limiting
   no ingress-limit
   no egress-limit
  !
  port-security
   no shutdown-time
   no admin-shutdown
   dot1x
    no reauth-enable
   !
  !
  lldp
   no notify
  !
```

```
  mcast-filtering
   no gmrp
  !
  cos
   no inspect-tos
  !
  vlan
   pvid 1
   no gvrp-mode
  !
  spanning-tree
   no restricted-role
   no restricted-tcn
  !
 !
.
.
.
```

Section 3.17.2

Configuring a Switched Ethernet Port

To configure a switched Ethernet port, do the following:

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

> **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	**Default:** true

Parameter	Description
	Provides the option to enable or disable this interface. When unchecked(i.e disabled), the interface will prevent all frames from being sent and received on that interface.
auton { auton }	**Synopsis:** on, off Enables or disables IEEE 802.3 auto-negotiation. Enabling auto-negotiation results in speed and duplex being negotiated upon link detection; both end devices must be auto-negotiation compliant for the best possible results.
speed { speed }	**Synopsis:** auto, 1.5M, 2.4M, 10M, 100M, 1G, 10G, 1.776M, 3.072M, 7.2M, 1.2K, 2.4K, 9.6K, 19.2K, 38.4K, 57.6K, 115.2K, 230.4K, 4.8K Speed (in megabits-per-second or gigabits-per-second). If auto-negotiation is enabled, this is the speed capability advertised by the auto-negotiation process. If auto-negotiation is disabled, the port is explicitly forced to this speed mode. AUTO means advertise all supported speed modes.
duplex { duplex }	**Synopsis:** auto, half, full If auto-negotiation is enabled, this is the duplex capability advertised by the auto-negotiation process. If auto-negotiation is disabled, the port is explicitly forced to this duplex mode. AUTO means advertise all supported duplex modes.
link-alarms	**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	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
lfi	Link Fault Indication (LFI) is specifically for FX interfaces.
ip-address-src { ip-address-src }	**Synopsis:** static, dynamic Whether the IP address is static or dynamically assigned via DHCP or BOOTP. Option DYNAMIC is a common case of a dynamically assigned IP address. It switches between BOOTP and DHCP until it gets the response from the relevant server. This must be static for non-management interfaces.
proxyarp	Enables/Disables whether the VLAN will respond to ARP requests for hosts other than itself
mtu { mtu }	**Default:** 1500 Maximum transmission unit (largest packet size allowed for this interface).
alias { alias }	The SNMP alias name of the interface

4. Configuring the rate Limiting settings by configuring the following parameter(s):

Parameter	Description
ingress-limit { ingress-limit }	**Synopsis:** disabled **Default:** 1000 The data rate in kbps at which received frames (of the type described by the ingress frames parameter) will start to be discarded by the switch. The valid range is 62 to 256000 kbps. The default value is 1000 kbps. If not set(cleared), this feature is disabled.
ingress-frames { ingress-frames }	**Synopsis:** broadcast, multicast, mcast-flood-ucast, all **Default:** broadcast This parameter specifies the types of frames to rate-limit on this port. It applies only to received frames:

Parameter	Description
	• BROADCAST : only broadcast frames will be limited. • MULTICAST : all multicast frames (including broadcast) will be limited. • MCAST-FLOOD-UCAST : all multicast frames (including broadcast) will be limited. Unicast will not be limited. • ALL : all frames (both multicast and unicast) will be limited.
egress-limit { egress-limit }	**Synopsis:** disabled, **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. Configure the LLDP settings by configuring the following parameter(s):

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

NOTE
Multicast filtering, CoS and VLAN parameters are only available when the port is in switchport mode.

6. Configure the Multicast filtering settings by configuring the following parameter(s):

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

7. Configure the CoS settings by configuring the following parameter(s):

Parameter	Description
default-priority { default-priority }	**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.

Parameter	Description
	When ToS parsing is enabled the switch will use the differentiated services bits in the TOS field.

8. Configure the VLAN settings by configuring the following parameter(s):

Parameter	Description
pvid { pvid }	The Port VLAN Identifier specifies the VLAN ID associated with untagged (and 802.1p priority tagged) frames received on this port. Frames tagged with a non-zero VLAN ID will always be associated with the VLAN ID retrieved from the frame tag.
type { type }	**Synopsis:** edge, trunk, pvlanedge **Default:** edge How the port determines its membership in VLANs. There are a few types of ports: • EDGE : the port is only a member of one VLAN (its native VLAN specified by the 'PVID' parameter). • PVLAN Edge : the port does not forward traffic to other PVLAN edge ports within the same VLAN. • TRUNK : the port is automatically a member of all configured VLANs. Frames transmitted out of the port on all VLANs except the port's native VLAN will be always tagged. It can also be configured to use GVRP for automatic VLAN configuration.
format { format }	**Synopsis:** untagged, tagged **Default:** untagged Whether frames transmitted out of the port on its native VLAN (specified by the 'PVID' parameter) will be tagged or untagged.
gvrp-mode { gvrp-mode }	**Synopsis:** advertise_only, learn_advertise GVRP (Generic VLAN Registration Protocol) operation on the port. There are several GVRP operation modes: • DISABLED : the port is not capable of any GVRP processing. • ADVERTISE ONLY : the port will declare all VLANs existing in the switch (configured or learned) but will not learn any VLANs. • ADVERTISE and LEARN : the port will declare all VLANs existing in the switch (configured or learned) and can dynamically learn VLANs.

> **NOTE**
> *Once a VLAN ID has been assigned to a switched Ethernet port, a VLAN is created and can be configured in **switch » vlans » all-vlans**.*

9. If the port is in switchport mode, configure the VLAN for the port. For more information, refer to Section 5.35.2, “Configuring VLANs for Switch Ethernet Ports”.
10. Configure the port security settings. For more information, refer to Section 3.17.3, “Configuring Port Security”.
11. Configure the spanning tree settings. For more information, refer to Section 5.34.6, “Configuring STP for Switched Ethernet Ports”.
12. Type `commit` and press **Enter** to save the changes, or type `revert` and press **Enter** to abort.

Section 3.17.3

Configuring Port Security

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

Using IEEE 802.1x authentication, 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, 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
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
ROX II supports both PEAP and EAP-MD5. PEAP is more secure and is recommended over EAP-MD5.

IMPORTANT!
Do not apply port security on core switch connections. Port security is applied at the end of the network to restrict admission to specific devices.

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

1. Make sure the CLI is in Configuration mode.
2. Navigate to ***interface » switch » {interface} » port-security***, where *{interface}* is the name given to the switched Ethernet port.
3. Configure the port security settings by configuring the following parameter(s) as required:

Parameter	Description
security-mode { security-mode }	**Synopsis:** dot1x_mac_auth, dot1x, per_macaddress, off **Default:** off Enables or disables the security feature for the port. The following port access control types are available: • Static MAC address based. With this method, authorized MAC address(es) should be configured in the static MAC address table. If some MAC addresses are not known in advance (or which port they are going to reside behind is unknown), there is still an option to configure the switch to auto-learn a certain number of MAC addresses. • IEEE 802.1X standard authentication. • IEEE 802.1X with MAC Authentication, also known as MAC-Authentication Bypass. With this method, the device can authenticate clients based on the client's MAC address, if IEEE 802.1X authentication times out.
auto-learn { auto-learn }	**Default:** 0 The maximum number of MAC addresses that can be dynamically learned on the port. If there are static addresses configured on the port, the actual number of addresses allowed to be learned is this number minus the number of the static MAC addresses.
shutdown-time { shutdown-time }	How long to shut down an interface if a security violation occurs.
admin-shutdown	Enables/disables administative shutdown if a security violation occurs.

4. Configure the 802.1x settings by configuring the following parameter(s) as required:

Parameter	Description
tx-period { tx-period }	**Default:** 30 IEEE 802.1X PAE (Port Access Entity) parameters
quiet-period { quiet-period }	**Default:** 60

Parameter	Description
	The period of time not to attempt to acquire a supplicant after the authorization session failed.
reauth-enable	Enables or disables periodic reauthentication
reauth-period { reauth-period }	**Default:** 3600 The time between successive reauthentications of the supplicant.
reauth-max { reauth-max }	**Default:** 2 The number of reauthentication attempts that are permitted before the port becomes unauthorized.
supp-timeout { supp-timeout }	**Default:** 30 The time to wait for the supplicant's response to the authentication server's EAP packet.
server-timeout { server-timeout }	**Default:** 30 The time to wait for the authentication server's response to the supplicant's EAP packet.
max-request { max-request }	**Default:** 2 The maximum number of times to retransmit the authentication server's EAP Request packet to the supplicant before the authentication session times out.

5. If IEEE 802.1x standard authentication or IEEE 802.1x with MAC authentication is selected, configure a primary and secondary RADIUS server. For more information, refer to Section 4.8.3, “Configuring RADIUS Authentication for Switched Ethernet Ports”.
6. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 3.17.4
Viewing Switched Ethernet Port Statistics

To view statistics collected for a specific switched Ethernet port, type:

```
show interfaces switch slot port port-stats
```

Where:

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

A table or list similar to the following example appears:

```
ruggedcom# show interfaces switch lm1 1 port-stats
port-stats
 in octets  6820
 out octets 3086
 in pkts    33
 out pkts   18
 error pkts 0
```

This table or list provides the following information:

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

Parameter	Description
in-pkts	The number of received good packets (Unicast+Multicast+Broadcast) and dropped packets.
out-pkts	The number of transmitted good packets.
error-pkts	The number of any type of erroneous packets.

Section 3.17.5

Viewing RMON Port Statistics

To view Remote Network Monitoring (RMON) statistics collected for a specific switched Ethernet port, type:

```
show interfaces switch slot port rmon-stats
```

Where:

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

A table or list similar to the following example appears:

```
ruggedcom# show interfaces switch lm1 1 rmon-stats | tab
rmon-stats
 in octets              10107903
 in pkts                53903
 in bcast pkts          607
 in mcast pkts          42103
 total in octets        10107903
 total in pkts          53903
 out octets             4974162
 out pkts               14356
 drop events            0
 out bcast pkts         0
 out mcast pkts         405
 crc align errors       0
 undersize pkts         0
 oversize pkts          0
 fragments              0
 jabbers                0
 collisions             0
 late collisions        0
 pkts 64 octets         10978
 pkts 65to127 octets    24792
 pkts 128to255 octets   19970
 pkts 256to511 octets   2469
 pkts 512to1023 octets  8410
 pkts 1024to1518 octets 1640
```

This table or list provides the following information:

Parameter	Description
in-octets	The number of octets in received good packets (Unicast+Multicast+Broadcast) and dropped packets.
in-pkts	The number of received good packets (Unicast+Multicast+Broadcast) and dropped packets.
in-bcast-pkts	The number of good broadcast packets received.

Parameter	Description
in-mcast-pkts	The number of good multicast packets received.
total-in-octets	The total number of octets of all received packets. This includes data octets of rejected and local packets which are not forwarded to the switching core for transmission. It should reflect all the data octets received on the line.
total-in-pkts	The number of received packets. This includes rejected, dropped and local packets, as well as packets which are not forwarded to the switching core for transmission. It should reflect all packets received on the line.
out-octets	The number of octets in transmitted good packets.
out-pkts	The number of transmitted good packets.
drop-events	The number of received packets that are dropped due to lack of receive buffers.
out-bcast-pkts	The number of transmitted broadcast packets.
out-mcast-pkts	The number of transmitted multicast packets. This does not include broadcast packets.
crc-align-errors	The number of packets received which meet all the following conditions: . The packet data length is between 64 and 1536 octets inclusive. . The packet has invalid CRC. . A Collision Event has not been detected. . A Late Collision Event has not been detected.
undersize-pkts	The number of received packets which meet all the following conditions: . The packet data length is less than 64 octets. . A Collision Event has not been detected. . A Late Collision Event has not been detected. . The packet has valid CRC.
oversize-pkts	The number of packets received with data length greater than 1536 octets and valid CRC.
fragments	The number of packets received which meet all the following conditions: . The packet data length is less than 64 octets, or it is a packet without SFD and is less than 64 octets in length. . A Collision Event has not been detected. . A Late Collision Event has not been detected. . The packet has invalid CRC.
jabbers	The number of packets which meet all the following conditions: . The packet data length is greater that 1536 octets. . The packet has invalid CRC.
collisions	The number of received packets for which a Collision Event has been detected.
late-collisions	The number of received packets for which a Late Collision Event has been detected.
pkts-64-octets	The number of received and transmitted packets with a size of 64 octets. This includes received and transmitted packets as well as dropped and local received packets. This does not include rejected received packets.
pkts-65to127-octets	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

Parameter	Description
pkts-128to255-octets	The number of received and transmitted packets with a size of 128 to 257 octets. This includes received and transmitted packets as well as dropped and local received packets. This does not include rejected received packets
pkts-256to511-octets	The number of received and transmitted packets with size of 256 to 511 octets. This includes received and transmitted packets as well as dropped and local received packets. This does not include rejected received packets.
pkts-512to1023-octets	The number of received and transmitted packets with size of 512 to 1023 octets. This includes received and transmitted packets as well as dropped and local received packets. This does not include rejected received packets
pkts-1024to1518-octets	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.

Section 3.17.6

Clearing Switched Ethernet Port Statistics

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

```
interfaces switch slot port clear-port-stats
```

Where:

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

Section 3.17.7

Resetting a Switched Ethernet Port

To reset a switched Ethernet port, type:

```
interfaces switch slot port reset-port
```

Where:

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

Section 3.17.8

Testing Switched Ethernet Port Cables

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

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

- Section 3.17.8.1, “Running a Cable Diagnostic Test”
- Section 3.17.8.2, “Viewing Cable Diagnostic Statistics”

- Section 3.17.8.3, “Clearing Cable Diagnostic Statistics”

Section 3.17.8.1
Running a Cable Diagnostic Test

To run a cable diagnostic test on a specific port, type:

IMPORTANT!
When cable diagnostics are performed on a port, any established network link on the port will be dropped and normal network traffic will not be able to pass through either the Port Under Test (PUT) or the Partner Port. When the cable diagnostic test is done, the original network port settings for both the PUT and the Partner Port are restored along with any established link.

```
interfaces switch slot port diagnostics start-cable-test run runs calibration calibration
```

Where:

- *slot* is the name of the module location
- *port* is the port number (or a list of ports, if aggregated in a port trunk) for the module
- *runs* is the total number of times cable diagnostics should be performed on the selected port. When set to 0, cable diagnostics will be performed continuously on the selected port.
- *calibration* is the value used to adjust or calibrate the estimated distance to fault. To calibrate the determine estimated distance to fault, do the following:
  1. Connect an Ethernet cable with a known length (e.g. 50m) to the port that requires calibration. Do not connect the other end of the cable to any link partner.
  2. Run a cable diagnostic test a few times on the port. An OPEN fault should be detected.
  3. Find the average distance to the OPEN fault recorded in the log and compare it to the known length of the cable. The difference can be used as the calibration value.
  4. Enter the calibration value and run the cable diagnostic test a few more times. The distance to the OPEN fault should now be similar to the cable length. Use the distance value to determine the calibration value.

For information about how to view the test results, refer to Section 3.17.8.2, “Viewing Cable Diagnostic Statistics”.

Section 3.17.8.2
Viewing Cable Diagnostic Statistics

To view the statistics collected for a switched Ethernet port after a cable diagnostic test, type:

```
show interfaces switch slot port diagnostics cable-diagnostic-results
```

A list similar to the following example appears:

```
ruggedcom# show interfaces switch lm1 1 diagnostics cable-diagnostic-results
diagnostics cable-diagnostic-results
 running          false
 good             20
 open             0
 short            20
 imped            0
 pass fail total "   10/    0/   10  "
 run count        0
 pass count       0
```

```
 fail count      0
```

This list provides the following information:

Parameter	Description
running	Whether or not a cable test is currently running on this port
good	The number of times GOOD TERMINATION (no fault) is detected on the cable pairs of the selected port.
open	The number of times OPEN is detected on the cable pairs of the selected port.
short	The number of times SHORT is detected on the cable pairs of the selected port.
imped	The number of times IMPEDANCE MISMATCH is detected on the cable pairs of the selected port.
pass-fail-total	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.
run-count	Run Count : The total number of iterations
pass-count	Pass Count
fail-count	Failure Count

Section 3.17.8.3
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 switch can be cleared.

Clearing All Cable Diagnostic Statistics

To clear the statistics, type:

```
switch clear-cable-stats-all
```

Clearing Cable Diagnostic Statistics for a Specific Switch

To clear only the statistics for a specific switch, type:

```
interfaces switch slot port diagnostics clear-cable-stats-port
```

Where:

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

Section 3.18
Managing Routable Ethernet Ports

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

- Section 3.18.1, “Viewing a List of Routable Ethernet Ports”
- Section 3.18.2, “Configuring a Routable Ethernet Port”

Section 3.18.1

Viewing a List of Routable Ethernet Ports

To view a list of routable Ethernet ports, type:

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

A table or list similar to the following example appears:

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

Section 3.18.2

Configuring a Routable Ethernet Port

To configure a routable Ethernet port, do the following:

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

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

Parameter	Description
	Disabling link-alarms will prevent alarms and LinkUp and LinkDown SNMP traps from being sent for that interface. Link alarms may also be controlled for the whole system under admin / alarm-cfg.
ip-address-src { ip-address-src }	**Synopsis:** static, dynamic **Default:** static Determines whether the IP address is static or dynamically assigned via DHCP or BOOTP. The DYNAMIC option is a common case of a dynamically assigned IP address. It switches between BOOTP and DHCP until it gets the response from the relevant server. It must be static for non-management interfaces.
proxyarp	Enables/Disables whether the port will respond to ARP requests for hosts other than itself.
on-demand	This interface is up or down on demand of link fail over.
alias { alias }	The SNMP alias name of the interface

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

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

5. Add a VLAN ID (VID) for the port. For more information, refer to Section 5.35.8.3, “Adding a VLAN ID to a Routable Ethernet Port or Virtual Switch”.
6. Type `commit` and press **Enter** to save the changes, or type `revert` and press **Enter** to abort.

Section 3.19

Managing Serial Ports

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

- Section 3.19.1, “Viewing a List of Serial Ports”
- Section 3.19.2, “Viewing Serial Port Statistics”
- Section 3.19.3, “Viewing Transport Connection Statistics”
- Section 3.19.4, “Viewing DNP Device Table Statistics”
- Section 3.19.5, “Clearing Serial Port Statistics”
- Section 3.19.6, “Configuring a Serial Port”
- Section 3.19.7, “Restarting the Serial Server”
- Section 3.19.8, “Resetting a Serial Port”

Section 3.19.1
Viewing a List of Serial Ports

To view a list of serial ports configured on the device, type:

```
show running-config interface serial
```

A table or list similar to the following example appears:

```
ruggedcom# show running-config interface serial | tab
                            BAUD  DATA         STOP  FLOW     PORT
SLOT  PORT  ENABLED  ALIAS  RATE  BITS  PARITY  BITS  CONTROL  TYPE   PROTOCOL
---------------------------------------------------------------------------------
lm3   1     true     -      9600  8     none    1     none     rs232
lm3   2     true     -      9600  8     none    1     none     rs232
lm3   3     true     -      9600  8     none    1     none     rs232
lm3   4     true     -      9600  8     none    1     none     rs232
lm3   5     true     -      9600  8     none    1     none     rs232
lm3   6     true     -      9600  8     none    1     none     rs232

!
```

Section 3.19.2
Viewing Serial Port Statistics

To view statistics collected for a specific serial port, type:

```
show interfaces serial port
```

A table or list similar to the following example appears:

```
ruggedcom# show interfaces serial port | tab
                                  TX     TX       RX     RX       PACKET  PARITY  FRAMING  OVERRUN
IFNAME   MEDIA  SPEED  PROTOCOL  CHARS  PACKETS  CHARS  PACKETS  ERRORS  ERRORS  ERRORS   ERRORS
-----------------------------------------------------------------------------------------------------
ser-3-1  RS232  9.6K   none      0      0        0      0        0       0       0        0
ser-3-2  RS232  9.6K   none      0      0        0      0        0       0       0        0
ser-3-3  RS232  9.6K   none      0      0        0      0        0       0       0        0
ser-3-4  RS232  9.6K   none      0      0        0      0        0       0       0        0
ser-3-5  RS232  9.6K   none      0      0        0      0        0       0       0        0
ser-3-6  RS232  9.6K   none      0      0        0      0        0       0       0        0
```

This table or list provides the following information:

Parameter	Description
media	The type of port media { RS232 RS422 RS485 }.
speed	**Synopsis:** auto, 1.5M, 2.4M, 10M, 100M, 1G, 10G, 1.776M, 3.072M, 7.2M, 1.2K, 2.4K, 9.6K, 19.2K, 38.4K, 57.6K, 115.2K, 230.4K, 4.8K The speed (in Kilobits-per-second).
protocol	The serial protocol assigned to this port.
tx-chars	The number of bytes transmitted over the serial port.
tx-packets	The number of packets transmitted over the serial port.
rx-chars	The number of bytes received by the serial port.
rx-packets	The number of packets received by the serial port.

Parameter	Description
packet-errors	The number of packet errors on this serial port.
parity-errors	The number of parity errors on this serial port.
framing-errors	The number of framing errors on this serial port.
overrun-errors	The number of overrun errors on this serial port.

Section 3.19.3

Viewing Transport Connection Statistics

To view the statistics collected for all transport connections, type:

```
show interfaces serial transport-connections
```

A table or list similar to the following appears:

```
ruggedcom# show interfaces serial transport-connections | tab
                      REMOTE  LOCAL             RX       TX       TARGET
INDEX  REMOTE IP      PORT    PORT   TRANSPORT  PACKETS  PACKETS  PORT      STATUS
-------------------------------------------------------------------------------------
1      10.200.22.199  15836   20000  TCP        177      0        ser-3-1,  Active
```

These tables or lists provide the following information:

Parameter	Description
remote-ip	The IP address of the remote serial server.
remote-port	The port of the remote serial server.
local-port	The local port for the incoming connection.
transport	The transport protocol (UDP or TCP) for this serial port.
rx-packets	The number of packets received from TCP/UDP.
tx-packets	The number of packets transmitted to TCP/UDP.
target-port	The target serial port.
status	The connection status of the serial port.

Section 3.19.4

Viewing DNP Device Table Statistics

To view the statistics collected for DNP device tables, type:

```
show interfaces serial dnp-device-table
```

A table or list similar to the following appears:

```
ruggedcom# show interfaces serial dnp-device-table | tab
DEVICE                  SERIAL
ADDRESS  REMOTE IP      PORT
---------------------------------
10       -              ser-3-1
```

```
20       10.200.22.199  -
```

This table or list provides the following information:

Parameter	Description
device-address	The DNP device address.
remote-ip	The IP address of the remote host that provides a connection to the this DNP device address.
serial-port	The target serial port.

Section 3.19.5

Clearing Serial Port Statistics

To clear the statistics collected for a specific serial port, type:

```
interfaces serial port name clear-port-stats
```

Where:

- *name* is the name of the serial port

Section 3.19.6

Configuring a Serial Port

To configure a serial port, do the following:

> **IMPORTANT!**
> *Do not enable flow control when Modbus TCP protocol is enabled.*

1. Make sure the CLI is in Configuration mode.
2. Navigate to ***interface » serial » {interface}***, where *{interface}* is the serial port.
3. Configure the following parameter(s) as required:

Parameter	Description
enabled	**Default:** true Provides the option to enable or disable this interface. When unchecked (i.e disabled), the interface will prevent all frames from being sent and received on that interface.
alias { alias }	The SNMP alias name of the interface.
baud-rate { baud-rate }	**Synopsis:** 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200, 230400 **Default:** 9600 The baud rate selection of the serial port.
data-bits { data-bits }	**Default:** 8 The number of data bits.
parity { parity }	**Synopsis:** none, even, odd **Default:** none The parity of the serial port.

Parameter	Description
stop-bits { stop-bits }	**Default:** 1 The number of stop bits of the serial port.
flow-control { flow-control }	**Synopsis:** none, xonxoff **Default:** none The flow control of the serial port.
port-type { port-type }	**Synopsis:** rs232, rs422, rs485 **Default:** rs232 The type of serial port.

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

Section 3.19.7
Restarting the Serial Server

To restart the serial server, type:

```
interfaces serial restart-serserver
```

Section 3.19.8
Resetting a Serial Port

To reset a serial port, type:

```
interfaces serial port name reset
```

Where:

- *`name`* is the name assigned to the port

Section 3.20
Managing Serial Port Protocols

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

- Section 3.20.1, “Raw Socket Concepts”
- Section 3.20.2, “Modbus TCP Concepts”
- Section 3.20.3, “DNP Concepts”
- Section 3.20.4, “Viewing a List of Serial Port Protocols”
- Section 3.20.5, “Adding a Serial Port Protocol”
- Section 3.20.6, “Configuring the DNP Protocol”
- Section 3.20.7, “Configuring the Modbus TCP Protocol”
- Section 3.20.8, “Configuring the Raw Socket Protocol”
- Section 3.20.9, “Deleting a Serial Port Protocol”

- Section 3.20.10, “Managing Device Address Tables”
- Section 3.20.11, “Managing Remote Hosts”

Section 3.20.1
Raw Socket Concepts

The raw socket protocol transports streams of characters from one serial port on the device to a specified remote IP address and port. The raw socket protocol supports TCP and UDP transport.

Broadcast RTU Polling

Broadcast polling allows a single host connected to the device to broadcast a polling stream to a number of remote RTUs.

The host connects through a serial port to the device. Up to 32 TCP remote RTUs may connect to the device's host-end via the network. For UDP transport, the device can send a polling stream to up to 64 remote hosts (RTUs).

Initially, the remote hosts place TCP connections to the device's host-end. The host-end in turn is configured to accept the required number of incoming TCP connections. The host connected to the device then sequentially polls each remote host. When a poll is received, the device forwards (i.e. broadcasts) it to all the remote hosts. All remote hosts will receive the request and the appropriate remote host will issue a reply. The reply is returned to the device, where it is forwarded to the host.

Host And Remote Roles

The raw socket protocol can either initiate or accept a TCP connection for serial encapsulation. It can establish a connection initiated from a remote host, vice versa, or bidirectionally.

Configure the device at the host-end to establish a connection with the remote host when:

- The host-end uses a port redirector that must make the connection
- The host-end is only occasionally activated and will make the connection when it becomes active
- A host-end firewall requires the connection to be made outbound

If the host-end wants to open multiple connections with the remote-ends in order to implement broadcast polling, configure the device to accept connections with the remote-ends.

Configure the device to connect from each side (host or remote) to the other if both sides support this functionality.

Message Packetization

The serial server buffers receive characters into packets in order to improve network efficiency and demarcate messages.

The serial server uses three methods to decide when to packetize and forward the buffered characters to the network:

- packetize on a specific character
- packetize on timeout
- packetize on a full packet

If configured to packetize on a specific character, the serial server will examine each received character, packetize and forward it upon receiving the specific character. The character is usually a <CR> or an <LF> character but may be any ASCII character.

If configured to packetize on a timeout, the serial server will wait for a configurable time after receiving a character before packetizing and forwarding it. If another character arrives during the waiting interval, the timer is restarted. This method allows characters transmitted as part of an entire message to be forwarded to the network in a single packet, when the timer expires after receiving the very last character of the message. This is usually the only packetizer selected when supporting Modbus TCP communications.

Finally, the serial server will always packetize and forward on a full packet, specifically when the number of characters fills its communications buffer (1024 bytes).

Section 3.20.2

Modbus TCP Concepts

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 unconfigured remote host, it will respond to the originator with a special message called an exception (type 10). A type 11 exception is returned by the server if the remote host fails to respond to requests.

Native Modbus TCP polling packages will want to receive these messages. Immediate indication of a failure can accelerate recovery sequences and reduce the need for long timeouts.

Section 3.20.3

DNP Concepts

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

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. ROX II supports DNP3 broadcast messages. DNP broadcast messages received on local serial ports are transmitted to all IP Addresses in the Device Address Table (whether learned or statically configured).

When a DNP broadcast message is received from the IP network, it is transmitted on all local serial ports configured as DNP ports.

Section 3.20.4

Viewing a List of Serial Port Protocols

To view a list of serial port protocols configured on the device, type:

```
show interfaces serial port protocol
```

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

```
ruggedcom# show interfaces serial port protocol
IFNAME   PROTOCOL
-------------------
ser-3-1  none
ser-3-2  none
ser-3-3  none
ser-3-4  none
ser-3-5  none
```

```
ser-3-6  none
```

If no serial port protocols have been configured, add protocols as needed. For more information, refer to Section 3.20.5, “Adding a Serial Port Protocol”.

Section 3.20.5

Adding a Serial Port Protocol

To add a serial port protocol, do the following:

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

   ```
   interface serial slot port protocols protocol
   ```

   Where:

   - *slot* is the name of the module location
   - *port* is the port number (or a list of ports, if aggregated in a port trunk) for the module
   - *protocol* is the protocol type
3. Configure the protocol.
   - For information about configuring a DNP protocol, refer to Section 3.20.6, “Configuring the DNP Protocol”.
   - For information about configuring a Modbus TCP protocol, refer to Section 3.20.7, “Configuring the Modbus TCP Protocol”.
   - For information about configuring a raw socket protocol, refer to Section 3.20.8, “Configuring the Raw Socket Protocol”.
4. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 3.20.6

Configuring the DNP Protocol

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

1. Make sure the CLI is in Configuration mode.
2. Navigate to ***interface » serial » {interface} » protocols » dnp » setdnp***, where *{interface}* is the serial port.
3. Configure the following parameter(s) as required:

Parameter	Description
address-learning { address-learning }	The interface to learn the RTU address from.
aging-timer { aging-timer }	**Default:** 1000 The length of time a learned DNP device in the Device Address Table may go without any DNP communication before it is removed from the table.
max-connection { max-connection }	**Default:** 1 The maximum number of incoming DNP connections.

4. Add a Device Address table. For more information about adding Device Address tables, refer to Section 3.20.10.2, “Adding a Device Address Table”.

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

Section 3.20.7

Configuring the Modbus TCP Protocol

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

1. Make sure the CLI is in Configuration mode.
2. Navigate to ***interface » serial » {interface} » protocols » tcpmodbus » settcpmodbus***, where *{interface}* is the serial port.
3. Configure the following parameter(s) as required:

Parameter	Description
response-timer { response-timer }	**Default:** 100 The maximum time from the last transmitted character of the outgoing poll until the first character of the response. If the RTU does not respond in this time, the poll will have been considered failed.
pack-timer { pack-timer }	**Default:** 1000 The maximum allowable time to wait for a response to a Modbus request to complete once it has started.
turnaround { turnaround }	**Default:** 0 The amount of delay (if any) to insert after the transmissions of Modbus broadcast messages out the serial port.
retransmit { retransmit }	**Default:** 0 The number of times to retransmit the request to the RTU before giving up.
max-connection { max-connection }	**Default:** 1 The maximum number of incoming connections.
local-port { local-port }	**Default:** 502 The alternate local TCP port number. If this field is configured, a single connection (per serial port) may be made to this alternate port number. Note that Modbus TCP uses a default local port number of 502. There is no limit imposed on the number of connections to the default TCP port.
rtu-list { rtu-list }	The ID of the RTU(s) connected to the serial port. Specify multiple RTUs with a space (e.g. 1 2 3 4) or a comma and space (e.g. 1, 2, 3, 4). A strictly comma-separated list (e.g. 1,2,3,4) is not permitted.

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

Section 3.20.8

Configuring the Raw Socket Protocol

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

1. Make sure the CLI is in Configuration mode.
2. Navigate to ***interface » serial » {interface} » protocols » rawsocket***, where *{interface}* is the serial port.
3. Configure the following parameter(s) as required:

Parameter	Description
pack-char { pack-char }	**Synopsis:** off, **Default:** off The numeric value of the ASCII character which will force forwarding of accumulated data to the network.
pack-timer { pack-timer }	**Default:** 1000 The delay from the last received character until when data is forwarded.
pack-size { pack-size }	**Synopsis:** max, **Default:** max The maximum number of bytes received from the serial port to be forwarded.
turnaround { turnaround }	**Default:** 0 The amount of delay (if any) to insert between the transmissions of individual messages out the serial port.
call-direction { call-direction }	**Synopsis:** in, out, both **Default:** out Whether to accept an incoming connection, place an outgoing connection or do both.
max-connection { max-connection }	**Default:** 1 The maximum number of incoming connections to permit when the call direction is incoming.
remote-ip { remote-ip }	The IP address used when placing an outgoing connection.
remote-port { remote-port }	The TCP destination port used in outgoing connections.
local-ip { local-ip }	The IP address used to establish a connection. Leaving it blank allows an incoming connection to any interface.
local-port { local-port }	The local TCP port to use to accept incoming connections.
transport { transport }	**Synopsis:** tcp, udp **Default:** tcp The transport connection protocol (UDP or TCP).

4. If the transport connection protocol is set to UDP, configure one or more remote hosts for the port. For more information about adding a remote host, refer to Section 3.20.11.2, “Adding a Remote Host”.
5. Type **`commit`** and press **Enter** to save the changes, or type **`revert`** and press **Enter** to abort.

Section 3.20.9
Deleting a Serial Port Protocol

To delete a serial port protocol, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the serial port protocol by typing:

```
no interface serial slot port protocols protocol
```

Where:

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

- *protocol* is the protocol type

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

Section 3.20.10

Managing Device Address Tables

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

- Section 3.20.10.1, “Viewing a List of Device Address Tables”
- Section 3.20.10.2, “Adding a Device Address Table”
- Section 3.20.10.3, “Deleting a Device Address Table”

Section 3.20.10.1

Viewing a List of Device Address Tables

To view a list of Device Address tables configured for a serial port using the DNP protocol, type:

```
show running-config interface serial slot/port protocols dnp setdnp device-table
```

Where:

- *slot/port* is the slot name and port number of the serial port

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

```
ruggedcom# show running-config interface serial protocols dnp setdnp device-table
interface
 serial lm3 1
  protocols dnp
   setdnp device-table 12
    remote-ip     172.30.130.2
    remote-device
   !
  !
 !
!
```

If no Device Address tables have been configured, add tables as needed. For more information, refer to Section 3.20.10.2, “Adding a Device Address Table”.

Section 3.20.10.2

Adding a Device Address Table

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

1. Make sure the CLI is in Configuration mode.
2. ```
   interface serial slot port protocols dnp setdnp device-table address
   ```

   Where:

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

- *address* is the local or remote DNP device address. The address may be that of a DNP device connected to a local serial port or one available via the serial port of a remote IP host.

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

Parameter	Description
remote-ip { remote-ip }	The IP address of the remote host that provides a connection to the DNP device with the configured address. Leave this field empty to forward DNP messages that match the configured address to the local serial port.
remote-device	Enables forwarding of DNP messages that match the device address to the remote IP.

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

Section 3.20.10.3
Deleting a Device Address Table

To delete a Device Address table, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the Device Address Table by typing:

```
no interface serial slot port protocols dnp setdnp device-table address
```

Where:

- *slot* is the name of the module location.
- *port* is the port number (or a list of ports, if aggregated in a port trunk) for the module.
- *address* is the local or remote DNP device address. The address may be that of a DNP device connected to a local serial port or one available via the serial port of a remote IP host.

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

Section 3.20.11
Managing Remote Hosts

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

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

- Section 3.20.11.1, “Viewing a List of Remote Hosts”
- Section 3.20.11.2, “Adding a Remote Host”
- Section 3.20.11.3, “Deleting a Remote Host”

Section 3.20.11.1
Viewing a List of Remote Hosts

To view a list of remote hosts configured for a serial port using the raw socket protocol, type:

```
show running-config interface serial protocols rawsocket setrawsocket remote-host
```

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

```
ruggedcom# show running-config interface serial protocols rawsocket setrawsocket remote-host
interface
 serial lm3 1
  protocols rawsocket
   setrawsocket remote-host 172.30.151.11 62011
   !
   setrawsocket remote-host 172.30.151.22 63000
   !
  !
 !
!
```

If no remote hosts have been configured, add hosts as needed. For more information, refer to Section 3.20.11.2, “Adding a Remote Host”.

Section 3.20.11.2

Adding a Remote Host

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

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

   ```
   interface serial slot port protocols rawsocket setrawsocket remote-host address remote-port
   ```

   Where:

   - *slot* is the name of the module location
   - *port* is the port number (or a list of ports, if aggregated in a port trunk) for the module
   - *address* is the IP address for the remote host
   - *remote-port* is the port number for the remote host
3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 3.20.11.3

Deleting a Remote Host

To delete a remote host, do the following:

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

   ```
   no interface serial slot port protocols rawsocket setrawsocket remote-host address remote-port
   ```

   Where:

   - *slot* is the name of the module location
   - *port* is the port number (or a list of ports, if aggregated in a port trunk) for the module
   - *address* is the IP address for the remote host
   - *remote-port* is the port number for the remote host
3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 3.21

Managing Ethernet Trunk Interfaces

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

Section 3.21.1

Viewing a List of Ethernet Trunk Interfaces

To view a list of Ethernet trunk interfaces, type:

```
show running-config interface trunk
```

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

```
ruggedcom# show running-config interface trunks
interface
 trunks 1
  switchport
  no alias
  no mcast-filtering gmrp
  no cos inspect-tos
  vlan pvid 1
  no vlan gvrp-mode
  trunk-ports lm6 1
  !
  trunk-ports lm6 2
  !
  no spanning-tree restricted-role
  no spanning-tree restricted-tcn
 !
!
```

If no Ethernet trunk interfaces have been configured, add trunks as needed. For more information, refer to Section 3.21.2, “Adding an Ethernet Trunk Interface”.

Section 3.21.2

Adding an Ethernet Trunk Interface

To add an Ethernet trunk interface, do the following:

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

   ```
   interface trunks id
   ```

   Where:

   - *id* is the ID given to the trunk
3. Configure the interface by typing the following commands:

Parameter	Description
switchport	The physical port into either Switched mode or a dedicated Routing mode.
on-demand	Bring up this interface on-demand only
ip-address-src { ip-address-src }	**Synopsis:** static, dynamic Whether the IP address is static or dynamically assigned via DHCP or BOOTP. Option DYNAMIC is a common case of a dynamically assigned IP address. It switches between BOOTP and DHCP until it gets the response from the relevant server. This must be static for non-management interfaces.
proxyarp	Enables/Disables whether the VLAN will respond to ARP requests for hosts other than itself
mtu { mtu }	**Default:** 1500 Maximum transmission unit (largest packet size allowed for this interface).
alias { alias }	The SNMP alias name of the interface

4. Configure the multicast filtering settings by typing the following commands:

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

5. Configure the CoS settings by typing the following commands:

Parameter	Description
default-priority { default-priority }	**Default:** 0 The priority of frames received on this port that are not prioritized based on the frame's contents (e.g. priority field in the VLAN tag, DiffServ field in the IP header, prioritized MAC address).
inspect-tos	Enables or disables parsing of the Type-Of-Service (TOS) field in the IP header of the received frames to determine what Class of Service they should be assigned. When TOS parsing is enabled the switch will use the Differentiated Services bits in the TOS field.

6. Configure the VLAN settings by typing the following commands:

Parameter	Description
pvid { pvid }	The Port VLAN Identifier specifies the VLAN ID associated with untagged (and 802.1p priority tagged) frames received on this port. Frames tagged with a non-zero VLAN ID will always be associated with the VLAN ID retrieved from the frame tag.
type { type }	**Synopsis:** edge, trunk, pvlanedge **Default:** edge How the port determines its membership in VLANs. There are the following port types: • EDGE : the port is only a member of one VLAN (its native VLAN specified by the'PVID' parameter).

Parameter	Description
	• PVLAN Edge : the port does not forward traffic to other PVLAN edge ports within the same VLAN. • TRUNK : the port is automatically a member of all configured VLANs. Frames transmitted out of the port on all VLANs except the port's native VLAN will be always tagged. It can also be configured to use GVRP for automatic VLANconfiguration.
format { format }	**Synopsis:** untagged, tagged **Default:** untagged Whether frames transmitted out of the port on its native VLAN(specified by the 'PVID' parameter) will be tagged or untagged.
gvrp-mode { gvrp-mode }	**Synopsis:** advertise_only, learn_advertise GVRP (Generic VLAN Registration Protocol) operation on the port. There are several GVRP operation modes: • DISABLED : the port is not capable of any GVRP processing. • ADVERTISE ONLY : the port will declare all VLANs existing in the switch (configured or learned) but will not learn any VLANs. • ADVERTISE and LEARN : the port will declare all VLANs existing in the switch (configured or learned) and can dynamically learn VLANs.

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

Section 3.21.3
Deleting an Ethernet Trunk Interface

To delete an Ethernet trunk interface, do the following:

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

```
no interface trunks id
```

Where:

• *id* is the ID given to the trunk

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

Section 3.21.4
Managing Ethernet Trunk Ports

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

• Section 3.21.4.1, “Viewing a List of Ethernet Trunk Ports”
• Section 3.21.4.2, “Adding an Ethernet Trunk Port”
• Section 3.21.4.3, “Deleting an Ethernet Trunk Port”

Section 3.21.4.1

Viewing a List of Ethernet Trunk Ports

To view a list of Ethernet trunk interfaces, type:

```
show running-config interface trunks id trunk-ports
```

Where:

- *id* is the ID given to the interface

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

```
ruggedcom# show running-config interface trunks 1 trunk-ports
interface
 trunks 1
  trunk-ports lm1 1
  !
  trunk-ports lm1 2
  !
 !
!
```

If no Ethernet trunk ports have been configured, add ports as needed. For more information, refer to Section 3.21.4.2, “Adding an Ethernet Trunk Port”.

Section 3.21.4.2

Adding an Ethernet Trunk Port

To add an Ethernet trunk port, do the following:

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

   ```
   interface trunks id trunk-ports slot port
   ```

   Where:

   - *id* is the ID given to the trunk
   - *slot* is the name of the module location
   - *port* is the port number (or a list of ports, if aggregated in a port trunk) for the module
3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 3.21.4.3

Deleting an Ethernet Trunk Port

To delete an Ethernet trunk port, do the following:

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

   ```
   no interface trunks id trunk-ports slot port
   ```

   Where:

   - *id* is the ID given to the trunk

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

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

Section 3.22
Managing Cellular Modem Interfaces

The following sections describe how to configure and manage cellular modem interfaces:

- Section 3.22.1, "Viewing a List of Cellular Modem Interfaces"
- Section 3.22.2, "Viewing the Status of a Cellular Modem Interface"
- Section 3.22.3, "Viewing PPP Interface Statistics"
- Section 3.22.4, "Viewing the HSPA Network Status for Cellular Modems"
- Section 3.22.5, "Viewing the CDMA Network Status for Cellular Modems"
- Section 3.22.6, "Configuring a Cellular Modem Interface"
- Section 3.22.7, "Activating a Cellular Modem Account"
- Section 3.22.8, "Resetting the Cellular Modem"
- Section 3.22.9, "Running AT Commands"
- Section 3.22.10, "Connecting as a PPP Client"

Section 3.22.1
Viewing a List of Cellular Modem Interfaces

To view a list of cellular modem interfaces, type:

```
show running-config interface cellmodem
```

A table or list similar to the following example appears:

```
ruggedcom# show running-config interface cellmodem
interface
 cellmodem lm4 1
  enabled
  no alias
  cdma ppp-client
 !
!
```

Section 3.22.2
Viewing the Status of a Cellular Modem Interface

To view the status of a cellular modem interface, type:

```
show interfaces cellmodem slot port profile
```

Where:

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

A table or list similar to the following example appears:

```
ruggedcom# show interfaces cellmodem cel-6-1 cdma
               NETWORK              RSSI       NETWORK   NETWORK  NETWORK  PHONE
IFNAME   TYPE  SUPPORTED  ESN  ECIO  INDICATOR  OPERATOR  IN USE   STATUS   NUMBER
-------------------------------------------------------------------------------------
cel-6-1  cdma                  0     0                             Unknown
```

This table or list provides the following information:

Parameter	Description
state	**Synopsis:** up, down, testing, unknown, dormant, notPresent, lowerLayerDown The port's link status.
media	The type of port media { ***range of values** }. 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.
admin-state	**Synopsis:** up, down, testing, unknown, dormant, notPresent, lowerLayerDown The port's administrative status.

Section 3.22.3

Viewing PPP Interface Statistics

To view the statistics for the PPP interface, type:

```
show interfaces cellmodem ppp-connections
```

A table or list similar to the following example appears:

```
ruggedcom# show interfaces cellmodem ppp-connections
               CONNECTION    LOCAL  REMOTE  TX     RX
IFNAME   TYPE  STATUS        IP     IP      BYTES  BYTES  MTU
----------------------------------------------------------------
cel-4-1  cdma  Disconnected                 0      0      0
```

This table or list provides the following information:

Parameter	Description
connection-status	PPP connection status
local-ip	The IP address assigned to the modem by the remote server
remote-ip	The IP address of the remote server
tx-bytes	The bytes transmitted over the modem
rx-bytes	The bytes received by the modem

Parameter	Description
mtu	MTU (Maximum Transmission Unit) value on the ppp interface

Section 3.22.4
Viewing the HSPA Network Status for Cellular Modems

To view the status of the HSPA GSM network for a cellular modem, type:

```
show interfaces cellmodem slot/port profile profile
```

Where:

- *slot/port* is the slot name and port number for the cellular modem
- *profile* is the profile (e.g. hspa or hspaplus)

A list similar to the following example appears:

```
211# show interfaces cellmodem cel-1-1 hspaplus hspaplus
hspaplus
 network supported GSM,GPRS,EDGE,UMTS,HSDPA/HSUPA,HSPA+
 imei              353567040070824
 radio             on
 rssi indicator    -83
 network operator  "\"KORE\",2"
 network in use    UMTS
 network status    "Registered to Home network"
 sim               89302370200990049282
```

This list provides the following information:

Parameter	Description
network-supported	Wireless technologies supported by the modem
imei	International Mobile Equipment Indentity
radio	The current RF status of cellmodem
rssi-indicator	The Received Signal Strength Indicator in dBm
network-operator	The wireless network operator currently in use
network-in-use	The network technology currently in use by the modem
network-status	The registration status of the modem with the wireless network
sim	The Subscriber Indentity Module number
active-profile	The active profile of cellular connection

Section 3.22.5
Viewing the CDMA Network Status for Cellular Modems

To view the status of the CDMA network for a cellular modem, type:

```
show interfaces cellmodem cdma
```

A list similar to the following example appears:

```
ruggedcom# show interfaces cellmodem cdma
interfaces cellmodem cel-4-1 cdma
 cdma
  network supported "CDMA 1xRTT/EV-DO"
  esn               0x60CFCB3A
  ecio              -11
  rssi indicator    -79
  network operator  Verizon
  network in use    "1xEV-DO, Revision A\n"
  network status    Registered
  phone number      9546496654
```

This list provides the following information:

Parameter	Description
network-supported	Wireless technologies supported by the modem
esn	The Electronic Serial Number of the modem. ESN is only avaible for the CDMA modem.
ecio	The total energy per chip per power density value in dBm
rssi-indicator	The Received Signal Strength Indicator in dBm
network-operator	The wireless network operator currently in use
network-in-use	The network technology currently in use by the modem
network-status	The registration status of the modem with the wireless network
phone-number	The subscriber phone number of the CDMA modem

Section 3.22.6

Configuring a Cellular Modem Interface

To configure a cellular modem interface, do the following:

NOTE

Cellular modems with support for EDVO network technology is backward compatible with CDMA 2G and CDMA 1x RTT networks.

Cellular modems with support for HSPA+ network technology is backward compatible with GSM, GPRS, EDGE, UMTS, HSDPA/HSUPA networks.

1. Make sure the CLI is in Configuration mode.
2. Navigate to ***interface » wan » {interface}***, where *{interface}* is the cellular modem interface.
3. Configure the following parameter(s) as required:

Parameter	Description
enabled	**Default:** false 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.
link-alarms	**Default:** true

Parameter	Description
	Disabling link-alarms will prevent alarms and LinkUp and LinkDown SNMP traps from being sent for that interface. Link alarms may also be controlled for the whole system under admin / alarm-cfg.
alias { alias }	The SNMP alias name of the interface

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

Section 3.22.7

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. The are two account activation methods used by ROX II: OTA (Over-the-Air) and Manual.

The following sections describe the different methods for activating a cellular account:

- Section 3.22.7.1, "Activating a Cellular Modem Account Over-the-Air"
- Section 3.22.7.2, "Activating a Cellular Modem Account Manually"

Section 3.22.7.1

Activating a Cellular Modem Account Over-the-Air

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 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 5.13.1.2, "Adding a CDMA Profile".*

> **NOTE**
> *A typical OTASP dial string begins with *228.*

To configure the OTASP dial string, type:

1. Make sure the CLI is in Configuration mode.
2. Configure the activation data string by typing:

```
interfaces cellmodem slot port profile activation activation-dial-string string
```

Where:

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

- *string* is the activation data string

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

Section 3.22.7.2
Activating a Cellular Modem Account Manually

If the service provider does not support Over the Air Service Provisioning (OTASP), the account must be activated manually.

To manually activate a cellular modem account, do the following:

1. Make sure the CLI is in Configuration mode.
2. Navigate to ***interfaces » cellmodem » {slot/port/profile} » activation***, where *{slot/port/profile}* is the slot name, port number and profile configured for the cellular modem.
3. Configure the following parameter(s) as required:

Parameter	Description
activation-code	The Master Subsidy Lock code provided by the wireless service carrier
phone-number	The Mobile Directory Number provided by the wireless service carrier
mobile-id-number	The Mobile Indentification Number provided by the wireless service carrier
system-id	System Identification Number provided by wireless service carrier
network-id	The Wireless Network ID provided by the wireless service carrier

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

Section 3.22.8
Resetting the Cellular Modem

To reset a cellular modem, type:

```
show interfaces cellmodem slot port profile reset
```

Where:

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

Section 3.22.9
Running AT Commands

To issue AT (Hayes) commands to the cellular modem, type:

```
interfaces cellmodem at command command
```

Where:

- *command* is the AT command

Section 3.22.10
Connecting as a PPP Client

To connect or disconnect from a cellular network as a PPP client, do the following:

1. Make sure the CLI is in Configuration mode.
2. Make sure the cellular modem interface has been configured. For more information, refer to Section 3.22.6, “Configuring a Cellular Modem Interface”.
3. Make sure an appropriate cellular modem profile has been configured. For more information, refer to Section 5.13, “Managing Cellular Modem Profiles”.
4. Make sure an account has been activated with a service provider for the modem type (e.g. HSPA+, Edge or CDMA).
5. Make sure antennas are properly connected to the cellular modem module before initiating the connection.
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 3.22.7, “Activating a Cellular Modem Account”.
8. Verify the network status for the appropriate cellular modem type. For more information refer to Section 3.22.4, “Viewing the HSPA Network Status for Cellular Modems” or Section 3.22.5, “Viewing the CDMA Network Status for Cellular Modems”
9. Navigate to ***interface » cellmodem » {interface} » {hspa/edge/cdma}***, where *{interface}* is the cellular modem.
10. Configure the following parameter(s) as required:

Parameter	Description
connect-to { connect-to }	Selects the gsm profile to connect to wireless network. The gsm profile is configured in /global/cellular/profiles/gsm

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

Section 3.23
Managing WAN Interfaces

The following sections describe how to configure and manage WAN interfaces:

- Section 3.23.1, “Viewing a List of WAN Interfaces”
- Section 3.23.2, “Configuring a WAN Interface”
- Section 3.23.3, “Viewing WAN Statistics”
- Section 3.23.4, “Clearing WAN Statistics”
- Section 3.23.5, “Performing a Loopback Test”
- Section 3.23.6, “Configuring a T1 Line”
- Section 3.23.7, “Configuring an E1 Line”

- Section 3.23.8, “Configuring DDS”
- Section 3.23.9, “Managing Channels”
- Section 3.23.10, “Configuring an HDLC-ETH Connection”
- Section 3.23.11, “Configuring a Multi Link PPP Connection”
- Section 3.23.12, “Configuring a PPP Connection”
- Section 3.23.13, “Configuring a Frame Relay Connection”
- Section 3.23.14, “Managing Data Links for Frame Relay Connections”

Section 3.23.1
Viewing a List of WAN Interfaces

To view a list of WAN interfaces, type:

```
show running-config interface wan
```

A table or list similar to the following example appears:

```
ruggedcom# show running-config interface wan
interface
 wan lm2 1
  enabled
  no alias
  t1 channel 2
   connection ppp nomagic
  !
 !
 wan lm2 2
  no alias
 !
!
```

Section 3.23.2
Configuring a WAN Interface

To configure a WAN interface, do the following:

1. Make sure the CLI is in Configuration mode.
2. Navigate to ***interface » wan » {interface}***, where *{interface}* is the WAN interface.
3. Configure the following parameter(s) as required:

Parameter	Description
{ slot }	**Synopsis:** sm, lm1, lm2, lm3, lm4, lm5, lm6 The name of the module location for the WAN card.
{ port }	The port number on the WAN card.
enabled	**Default:** false Enables this WAN port.
link-alarms	**Default:** true

Parameter	Description
	Disabling link-alarms will prevent alarms and LinkUp and LinkDown SNMP traps from being sent for that interface. Link alarms may also be controlled for the whole system under admin / alarm-cfg.
alias { alias }	The SNMP alias name of the interface

4. Configure a T1 or E1 line. For more information, refer to Section 3.23.6, “Configuring a T1 Line” or Section 3.23.7, “Configuring an E1 Line”.
5. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 3.23.3
Viewing WAN Statistics

To view statistics for the WAN network, type:

```
show interfaces wan t1e1
```

A table or list similar to the following example appears:

```
ruggedcom# show interfaces wan t1e1
interfaces wan t1e1 te1-2-1
 slot        lm2
 port        1
 channelno   2
 state       up
 reliability 255/255
 receive-stats
  frames       227
  bytes        6306
  linkinactive 0
  load         1/255
 transmit-stats
  txframes    217
  txbytes     5733
  txrealigned 0
  load        1/255
 receive-error
  overrun      0
  crcerror     0
  abort        0
  corruption   0
  pcierror     0
  dmaerror     0
.
.
.
```

This table or list provides the following information:

Parameter	Description
slot	**Synopsis:** sm, lm1, lm2, lm3, lm4, lm5, lm6, Line module name of the slot.
port	Port number on the slot.
channelno	Channel number on the port.
state	**Synopsis:** up, down, testing, unknown, dormant, notPresent, lowerLayerDown

Parameter	Description
	Status of the interface.
local	Loacal IP address of the interface.
remote	Peer IP address.
mask	Netmask.
reliability	Reliability of the interface over 5 minutes. It is calculated as an exponential average of the fraction of the total received and transmitted errors and the total packets that are received and transmitted successfully.
create-time	The duration of time since interface is created.
last-status-change	The duration of time since last change of interface status.

For information about clearing the WAN statistics, refer to Section 3.23.4, "Clearing WAN Statistics".

Section 3.23.4
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 statistics for all WAN interfaces, type:

```
interfaces wan clearstatistics all-interfaces
```

To clear statistics for a specific WAN interface, type:

```
interfaces wan clearstatistics [ddsName | t1e1Name | t3e3Name] interface
```

Where:

- *interface* is the WAN interface

Section 3.23.5
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 – 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 – 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 – 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 3.23.2, “Configuring a WAN Interface”.
2. Configure the following parameter(s) as required:

```
interfaces wan loopback duration time nloops loops phsyical-name interface type [digital | line |
remote]
```

Where:

- *time* is the number of seconds required to run the test
- *loops* is the number of loops
- *interface* is the name of the physical interface

The results are displayed when the test is complete.

Section 3.23.6

Configuring a T1 Line

To configure a T1 line for a WAN interface, do the following:

1. Make sure the CLI is in Configuration mode.
2. Navigate to ***interface » wan » {interface} » t1***, where *{interface}* is the WAN interface.
3. Configure the following parameter(s) as required:

Parameter	Description
frame { frame }	**Synopsis:** esf **Default:** esf The frame format.
line-code { line-code }	**Synopsis:** b8zs **Default:** b8zs The line encoding/decoding scheme.
clock { clock }	**Synopsis:** normal, master **Default:** normal Serial clocking mode: master or normal. • master : provide serial clock signal. • normal : accept external clock signal.
lbo { lbo }	**Synopsis:** 0db, 7.5db, 15db, 22.5db, 0-110ft, 110-220ft, 220-330ft, 330-440ft, 440-550ft, 550-660ft **Default:** 0db Line Build Out: tunes the shape of the T1 pulses and adjusts their amplitude depending upon distances and the desired attenuation.

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

Section 3.23.7

Configuring an E1 Line

To configure E1 parameters for a WAN interface, do the following:

1. Make sure the CLI is in Configuration mode.
2. Navigate to ***interface » wan » {interface} » E1***, where *{interface}* is the WAN interface.
3. Configure the following parameter(s) as required:

Parameter	Description
frame { frame }	**Synopsis:** ncrc4, crc4 **Default:** ncrc4 The frame format.
line-code { line-code }	**Synopsis:** hdb3 **Default:** hdb3 A line encoding/decoding scheme.
clock { clock }	**Synopsis:** normal, master **Default:** normal Serial clocking mode: master or normal. • master : provide serial clock signal. • normal : accept external clock signal.

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

Section 3.23.8

Configuring DDS

To configure DDS for a WAN interface, do the following:

1. Make sure the CLI is in Configuration mode.
2. Navigate to ***interface » wan » {interface} » dds » ddsparams***, where *{interface}* is the WAN interface.
3. Configure the following parameter(s) as required:

Parameter	Description
mode { mode }	**Synopsis:** 56k, 64k **Default:** 56k DDS speed mode (kbps).
clock { clock }	**Synopsis:** normal, master **Default:** normal Serial clocking mode: master or normal. • master : provide serial clock signal. • normal : accept external clock signal.

4. Configure a PPP or frame relay connection. For more information, refer to Section 3.23.12, “Configuring a PPP Connection” or Section 3.23.13, “Configuring a Frame Relay Connection”.
5. Type **`commit`** and press **Enter** to save the changes, or type **`revert`** and press **Enter** to abort.

Section 3.23.9

Managing Channels

The following sections describe how to configure and manage channels:

- Section 3.23.9.1, “Viewing a List of Channels”
- Section 3.23.9.2, “Adding a Channel”
- Section 3.23.9.3, “Deleting Channels”

Section 3.23.9.1

Viewing a List of Channels

To view a list of T1 or E1 lines, type:

```
show running-config interface wan slot port protocol channel
```

Where:

- *slot* is the name of the module location
- *port* is the port number (or a list of ports, if aggregated in a port trunk) for the module
- *protocol* is either T1 or E1

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

```
ruggedcom# show running-config interface wan lm2 1 t1 channel
interface
 wan lm2 1
  t1 channel 2
   connection ppp nomagic
  !
 !
!
```

If no channels have been configured, add channels as needed. For more information, refer to Section 3.23.9.2, “Adding a Channel”.

Section 3.23.9.2

Adding a Channel

To configure a channel for a T1/E1 physical interface, do the following:

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

   ```
   interface wan slot port protocol channel number
   ```

   Where:

   - *slot* is the name of the module location
   - *port* is the port number (or a list of ports, if aggregated in a port trunk) for the module
   - *protocol* is either T1 or E1
   - *number* is the channel number
3. Configure the following parameter(s) as required:

Parameter	Description
{ channelnumber }	Channel Number.
ts { ts }	**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.

4. If necessary, configure VLANs for an HDLC-ETH connection. For more information, refer to Section 5.35.6.2, "Adding an HDLC-ETH VLAN".
5. If necessary, configure an MLPPP connection. For more information, refer to Section 3.23.11, "Configuring a Multi Link PPP Connection".
6. If necessary, configure a PPP connection. For more information, refer to Section 3.23.12, "Configuring a PPP Connection".
7. If necessary, configure a frame relay connection. For more information, refer to Section 3.23.13, "Configuring a Frame Relay Connection".
8. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 3.23.9.3
Deleting Channels

To delete a channel configured for a T1/E1 physical interface, do the following:

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

```
no interface wan slot port protocol channel number
```

   Where:

   - *slot* is the name of the module location
   - *port* is the port number (or a list of ports, if aggregated in a port trunk) for the module
   - *protocol* is either T1 or E1
   - *number* is the channel number
3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 3.23.10
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 3.24.2, "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 3.23.6, “Configuring a T1 Line”
- Section 3.23.7, “Configuring an E1 Line”

To configure an HLDC-ETH connection for a T1 or E1 line, do the following:

1. Make sure the CLI is in Configuration mode.
2. Navigate to ***interface » wan » {interface} » {protocol} » channel » {number} » connection » hdlc-eth***, where *{interface}* is the WAN interface, *{parameter}* is either T1 or E1, and *{number}* is the channel number.
3. Configure the following parameter(s) as required:

Parameter	Description
encoding { encoding }	**Synopsis:** nrz **Default:** nrz HDLC encoding type
parity { parity }	**Synopsis:** crc16_ccitt **Default:** crc16_ccitt HDLC parity type
on-demand	This interface is up or down on demand of link fail over.
mtu { mtu }	**Default:** 1500 Maximum transmission unit (largest packet size allowed for this interface).

4. Add one or more VLANs for the HDLC-ETH connection. For more information, refer to Section 5.35.6.2, “Adding an HDLC-ETH VLAN”.
5. Type `commit` and press **Enter** to save the changes, or type `revert` and press **Enter** to abort.

Section 3.23.11

Configuring a Multi Link PPP Connection

To configure a Multi Link Point-to-Point Protocol (MLPPP) connection for a T1 or E1 line, do the following:

1. Make sure the CLI is in Configuration mode.
2. Navigate to ***interface » wan » {interface} » {protocol} » channel » {number}*** , where *{interface}* is the WAN interface, *{parameter}* is either T1 or E1, and *{number}* is the channel number.
3. Configure the following parameter(s) as required:

Parameter	Description
bundle { bundle }	**Default:** 1 The bundle number
on-demand	This interface is up or down on demand of link fail over.
mtu { mtu }	**Default:** 1500 Maximum transmission unit (largest packet size allowed for this interface).

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

Section 3.23.12

Configuring a PPP Connection

To configure a Point-to-Point Protocol (PPP) connection, do the following:

1. Make sure the CLI is in Configuration mode.
2. Depending on the WAN module, navigate to either:
   - **For T1/E1 Lines**

     interface » wan » {interface} » {protocol} » channel » {number} » connection, where *{interface}* is the WAN interface, *{parameter}* is either T1 or E1, and *{number}* is the channel number.
   - **For DDS**

     interface » wan » {interface} » dds » connection, where *{interface}* is the WAN interface, *{parameter}* is either T1 or E1, and *{number}* is the channel number.
3. Configure the following parameter(s) as required:

Parameter	Description
nomagic	**Default:** false Disables the Magic Number. (Valid on RX1000 only)
on-demand	This interface is up or down on demand of link fail over.
mtu { mtu }	**Default:** 1500 Maximum transmission unit (largest packet size allowed for this interface).

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

Section 3.23.13

Configuring a Frame Relay Connection

To configure a frame relay connection for a T1 or E1 line, do the following:

1. Make sure the CLI is in Configuration mode.
2. Depending on the WAN module, navigate to either:
   - **For T1/E1 Lines**

     interface » wan » {interface} » {protocol} » channel » {number} » connection, where *{interface}* is the WAN interface, *{parameter}* is either T1 or E1, and *{number}* is the channel number.
   - **For DDS**

     interface » wan » {interface} » dds » connection, where *{interface}* is the WAN interface, *{parameter}* is either T1 or E1, and *{number}* is the channel number.
3. Configure the following parameter(s) as required:

Parameter	Description
station { station }	**Synopsis:** cpe, switch

Parameter	Description
	Default: cpe The behavior of the frame relay connection, i.e. CPE (Customer Premises Equipment) or as a switch.
signal { signal }	**Synopsis:** ansi, lmi, q933, none **Default:** ansi The frame relay link management protocol used.
t391 { t391 }	**Default:** 10 (Link Integrity Verification polling) Indicates the number of seconds between transmission of in-channel signaling messages. Valid for cpe.
t392 { t392 }	**Default:** 16 (Verification of polling cycle) Indicates the expected number of seconds between reception of in-channel signaling messages transmitted by cpe. Valid for Switch.
n391 { n391 }	**Default:** 6 Defines the frequency of transmission of full status enquiry messages. Valid for CPE.
n392 { n392 }	**Default:** 4 The number of error events (enumerated by n393) for which the channel is declared inactive; valid for either cpe or Switch.
n393 { n393 }	**Default:** 4 The number of error events on the frame relay channel; valid for either cpe or switch.

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

Section 3.23.14

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.

The following sections describe how to configure and manage data links for a Frame Relay connection:

- Section 3.23.14.1, “Viewing a List of Data Links”
- Section 3.23.14.2, “Adding a Data Link”
- Section 3.23.14.3, “Deleting a Data Link”

Section 3.23.14.1

Viewing a List of Data Links

To view a list of data links configured for a frame relay connection, type:

```
show running-config interface wan interface protocol channel number connection framerelay dlci
```

Where:

- *`interface`* is the WAN interface
- *`protocol`* is either T1 or E1

- *number* is the channel number

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

```
ruggedcom# show running-config interface wan lm2 1 t1 channel 1 connection framerelay dlci
interface
wan lm2 1
  t1 channel 1
   connection framerelay dlci 100
    !
   !
!
```

If no data links have been configured, add data links as needed. For more information, refer to Section 3.23.14.2, "Adding a Data Link".

Section 3.23.14.2
Adding a Data Link

To add a data link for a frame relay connection, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the data link by typing:

```
interface wan interface protocol channel number connection framerelay dlci id
```

   Where:

   - *interface* is the WAN interface
   - *protocol* is either T1 or E1
   - *number* is the channel number
   - *id* is the ID of the data link

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

Parameter	Description
on-demand	This interface is up or down on demand of link fail over.
mtu { mtu }	**Default:** 1500 Maximum transmission unit (largest packet size allowed for this interface).

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

Section 3.23.14.3
Deleting a Data Link

To delete a data link for a frame relay connection, do the following:

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

```
no interface wan interface protocol channel number connection framerelay dlci id
```

   Where:

- *interface* is the WAN interface
- *protocol* is either T1 or E1
- *number* is the channel number
- *id* is the ID of the data link

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

Section 3.24

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 packet. In a virtual switch, forwarding is done in a Layer 2 and allows all network traffic, including L2 Multicast (i.e. GOOSE, ISO), IP Multicast, Unicast and Broadcast messages, to travel through the virtual switch tunnel without any modifications.

A virtual swtich can be useful, in particular, for GOOSE messaging when the sender and receiver need to communicate through a routable IP network. Since there is no IP encapsulation for the L2 traffic going through the virtual switch, network latency is minimized for the traffic between end devices.

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

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

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

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

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 VS1, the DHCP configuration must be changed to refer to VS1.

- The virtual switch is implemented in the ROX II software. Therefore, a CPU resource is needed to forward broadcast, multicast and unicast traffic.
- If the router is running as a firewall, the **routeback** parameter under ***firewall » fwconfig » fwinterface*** must be enabled for the virtual switch interface. For more information, refer to Section 5.17.9, “Managing Interfaces”.

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

- Section 3.24.1, “Viewing a List of Virtual Switches”
- Section 3.24.2, “Adding a Virtual Switch”
- Section 3.24.3, “Deleting a Virtual Switch”
- Section 3.24.4, “Managing Virtual Switch Interfaces”
- Section 5.35.7, “Managing VLANs for Virtual Switches”

Section 3.24.1

Viewing a List of Virtual Switches

To view a list of virtual switches, type:

```
show running-config interface virtualswitch
```

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

```
ruggedcom# show running-config interface virtualswitch | tab
                            IP                                       IP
             FORWARD        ADDRESS                                  ADDRESS
ID  ENABLED  DELAY    ALIAS SRC      PROXYARP  NAME              VID SRC      QOS  INGRESS  MARK
---------------------------------------------------------------------------------------------
1   true     15       -     static   -
                                               switch.0100
                                               te1-4-1c01.0100
                                                                 100 static
2   true     15       -     static   -
                                               switch.0200
                                               te1-4-1c01.0200

!
```

If no virtual switches have been configured, add switches as needed. For more information, refer to Section 3.24.2, “Adding a Virtual Switch”.

Section 3.24.2

Adding a Virtual Switch

To add virtual switch, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the virtual switch by typing:

   ```
   interface virtualswitch id
   ```

   Where:

   - *id* is the ID assigned to the virtual switch
3. Configure the following parameter(s) as required:

Parameter	Description
enabled	**Default:** true Enables this interface.
forward-delay { forward-delay }	**Default:** 15 Delay (in seconds) of the listening and learning state before goes to forwarding state.
alias { alias }	The SNMP alias name of the interface
ip-address-src { ip-address-src }	**Synopsis:** static, dynamic **Default:** static Whether the IP address is static or dynamically assigned via DHCP or BOOTP.
proxyarp	Enables/Disables whether the port will respond to ARP requests for hosts other than itself

4. Add interfaces for the virtual switch. For more information, refer to Section 3.24.4.2, “Adding a Virtual Switch Interface”.
5. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 3.24.3
Deleting a Virtual Switch

To delete a virtual switch, do the following:

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

```
no interface virtualswitch id
```

Where:

- *id* is the ID assigned to the virtual switch

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

Section 3.24.4
Managing Virtual Switch Interfaces

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

- Section 3.24.4.1, “Viewing a List of Virtual Switch Interfaces”
- Section 3.24.4.2, “Adding a Virtual Switch Interface”
- Section 3.24.4.3, “Deleting a Virtual Switch Interface”

Section 3.24.4.1
Viewing a List of Virtual Switch Interfaces

To view a list of virtual switch interfaces, type:

```
show running-config interface virtualswitch id interface
```

Where:

- *id* is the ID assigned to the virtual switch

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

```
ruggedcom# show running-config interface virtualswitch 1 interface | tab
NAME
-----------------
switch.0100
te1-4-1c01.0100

 !
!
```

If no virtual switches have been configured, add switches as needed. For more information, refer to Section 3.24.2, “Adding a Virtual Switch”.

Section 3.24.4.2

Adding a Virtual Switch Interface

To add 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.*

1. Make sure the CLI is in Configuration mode.
2. Add the virtual switch by typing:

   ```
   interface virtualswitch id interface name
   ```

   Where:

   - *id* is the ID assigned to the virtual switch
   - *name* is the interface name

   The new interface is now accessible by typing:

   ```
   ip vsid
   ```

3. Assign an IPv4 or IPv6 address to the interface. For more information, refer to Section 5.38.3.2, “Adding an IPv4 Address” or Section 5.38.6.2, “Adding an IPv6 Address”.
4. If necessary, add one or more VLANs to the virtual switch interface. For more information, refer to Section 5.35.7.2, “Adding a Virtual Switch VLAN”.
5. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 3.24.4.3
Deleting a Virtual Switch Interface

To delete a virtual switch interface, do the following:

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

   ```
   no interface virtualswitch id interface name
   ```

   Where:

   - *id* is the ID assigned to the virtual switch
   - *name* is the interface name
3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 3.25
Managing a Domain Name System (DNS)

The following sections describe how to configure and manage a Domain Name Server (DNS):

- Section 3.25.1, "Managing Domain Names"
- Section 3.25.2, "Managing Domain Name Servers"

Section 3.25.1
Managing Domain Names

The DNS service can be configured to use one or more domain names when quering a domain name server. The list of domain names can include the domain in which the router is a member of, and other domains that may be used to search for an unqualified host name (i.e. as though it were local).

The following sections describe how to configure and manage a list of domain names:

- Section 3.25.1.1, "Viewing a List of Domain Names"
- Section 3.25.1.2, "Adding a Domain Name"
- Section 3.25.1.3, "Deleting a Domain Name"

Section 3.25.1.1
Viewing a List of Domain Names

To view a list of domain names, type:

```
show running-config dns search
```

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

```
ruggedcom# show running-config admin dns search
admin
 dns
  search ruggedcom.com
  !
```

```
  !
!
```

If no domain names have been configured, add names as needed. For more information, refer to Section 3.25.1.2, “Adding a Domain Name”.

Section 3.25.1.2
Adding a Domain Name

To add a domain name, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the domain name by typing:

   ```
   admin dns search name
   ```

   Where:

   - *name* is the name of the domain
3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 3.25.1.3
Deleting a Domain Name

To delete a domain name, do the following:

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

   ```
   no admin dns search name
   ```

   Where:

   - *name* is the name of the domain
3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 3.25.2
Managing Domain Name Servers

A hierarchical list of domain name servers can be configured for the DNS service. ROX II will contact each server in the order they are listed when domain names require resolution.

The following sections describe how to configure and manage a list of domain name servers:

- Section 3.25.2.1, “Viewing a List of Domain Name Servers”
- Section 3.25.2.2, “Adding a Domain Name Server”
- Section 3.25.2.3, “Deleting a Domain Name Server”

Section 3.25.2.1
Viewing a List of Domain Name Servers

To view a list of domain name servers, type:

```
show running-config dns server
```

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

```
ruggedcom# show running-config admin dns server
admin
 dns
  server 10.1.1.1
  !
 !
!
```

If no domain name servers have been configured, add servers as needed. For more information, refer to Section 3.25.2.2, “Adding a Domain Name Server”.

Section 3.25.2.2
Adding a Domain Name Server

To add a domain name server, do the following:

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

   ```
   admin dns server address
   ```

   Where:

   - *address* is the IP address of the domain name server.
3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 3.25.2.3
Deleting a Domain Name Server

To delete a domain name server, do the following:

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

   ```
   no admin dns server address
   ```

   Where:

   - *address* is the IP address of the domain name server.
3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

4 System Administration

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

- Section 4.1, “Configuring the System Name and Location”
- Section 4.2, “Configuring the Hostname”
- Section 4.3, “Customizing the Welcome Screen”
- Section 4.4, “Setting the User Authentication Mode”
- Section 4.5, “Setting the Maximum Number of Sessions”
- Section 4.6, “Managing Alarms”
- Section 4.7, “Managing Certificates and Keys”
- Section 4.8, “Managing RADIUS Authentication”
- Section 4.9, “Managing Users”
- Section 4.10, “Managing Passwords and Passphrases”
- Section 4.11, “Scheduling Jobs”

Section 4.1

Configuring the System Name and Location

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

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

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

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

Section 4.2
Configuring the Hostname

To configure the hostname for the device, do the following:

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

Parameter	Description
name { name }	**Default:** ruggedcom The hostname that is the name of this device.
domain { domain }	**Synopsis:** The domain-name type represents a DNS domain name. The name SHOULD be fully qualified whenever possible. Internet domain names are only loosely specified. Section 3.5 of RFC 1034 recommends a syntax (modified in Section 2.1 of RFC 1123). The pattern above is intended to allow for current practice in domain name use, and some possible future expansion. It is designed to hold various types of domain names, including names used for A or AAAA records (host names) and other records, such as SRV records. Note that Internet host names have a stricter syntax (described in RFC 952) than the DNS recommendations in RFCs 1034 and 1123, and that systems that want to store host names in schema nodes using the domain-name type are recommended to adhere to this stricter standard to ensure interoperability. The encoding of DNS names in the DNS protocol is limited to 255 characters. Since the encoding consists of labels prefixed by a length bytes and there is a trailing NULL byte, only 253 characters can appear in the textual dotted notation. The description clause of schema nodes using the domain-name type MUST describe when and how these names are resolved to IP addresses. Note that the resolution of a domain-name value may require to query multiple DNS records (e.g., A for IPv4 and AAAA for IPv6). The order of the resolution process and which DNS record takes precedence can either be defined explicitely or it may depend on the configuration of the resolver. Domain-name values use the US-ASCII encoding. Their canonical format uses lowercase US-ASCII characters. Internationalized domain names MUST be encoded in punycode as described in RFC 3492 **Default:** localdomain The domain for this hostname.

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

Section 4.3
Customizing the Welcome Screen

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

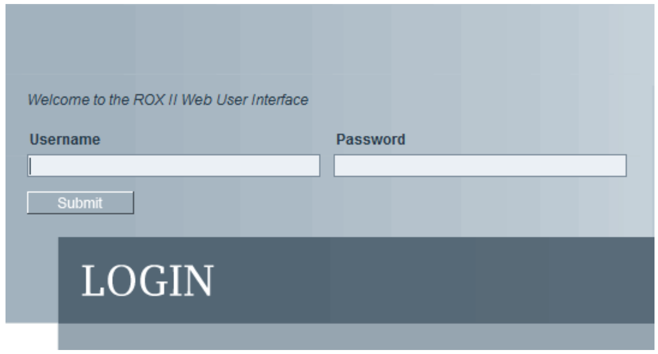

Figure 4: A Customized Welcome Screen

To add a welcome message, do the following:

```
admin authentication banner message
```

Where:

- *message* is the custom welcome message

Section 4.4

Setting the User Authentication Mode

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

To set the authentication mode, type:

```
admin authentication mode [localonly | radius_local | radius_then_local]
```

- 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.

Section 4.5

Setting the Maximum Number of Sessions

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

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

Parameter	Description
max-sessions-total { max-sessions-total }	**Synopsis:** unbounded **Default:** 70

Parameter	Description
	Puts a limit on the total number of concurrent sessions to ROX.

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

Section 4.6

Managing Alarms

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

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

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

Alarm Type	Description
Admin	Admin alarms are for administrative aspects of the device, such as feature-key problems.
Chassis	Chassis alarms are for physical or electrical problems, or similar events of interest. This includes irregular voltages at the power supply or the insertion or removal of a module.
Switch	Switch alarms are for link up/down events on switch interfaces.
Eth	Eth alarms are for fe-cm port related events, such as link up/down events.
WAN	WAN alarms are for T1/E1 and DDS interface related events, such as link up/down events.
Cellmodem	Cellular alarms are for cellular interface related events, such as link up/down events.
Security	Security alarms are for certificate expiry events. This includes warnings 30 days before a certificate is set to expire and when an expired certificate is installed.

The following sections describe how to configure and manage alarms:

- Section 4.6.1, “Viewing a List of Active Alarms”
- Section 4.6.2, “Clearing and Acknowledging Alarms”
- Section 4.6.3, “Configuring an Alarm”

Section 4.6.1

Viewing a List of Active Alarms

To view a list of alarms for a specific alarm type, type:

```
show admin alarms
```

A table or list similar to the following example appears:

```
ruggedcom# show admin alarms | tab
           ALARM  EVENT
```

```
SUBSYSTEM  ID     ID     SEVERITY  DESCRIPTION            DATE TIME                 USER ACTIONS
 ACTUATORS
---------------------------------------------------------------------------------------------
switch     1      1      notice    Link-up on port lm1/8  Wed Feb  6 16:08:44 2013  clear-or-ack  none
```

For information on how to clear or acknowledge an active alarm, refer to Section 4.6.2, “Clearing and Acknowledging Alarms”.

Section 4.6.2

Clearing and Acknowledging Alarms

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

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

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

The following sections describe how to acknowledge and clear alarms:

- Section 4.6.2.1, “Clearing Alarms”
- Section 4.6.2.2, “Acknowledging Alarms”

Section 4.6.2.1

Clearing Alarms

Non-conditional alarms must be cleared by the user. Conditional alarms, when configured, are cleared automatically.

To clear a non-conditional alarm, type:

```
admin alarms active-alarms alarm clear
```

- *`alarm`* is the chosen alarm

Section 4.6.2.2

Acknowledging Alarms

To acknowledge an alarm, type:

```
admin alarms active-alarms alarm acknowledge
```

- *`alarm`* is the chosen alarm

Section 4.6.3

Configuring an Alarm

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

> **NOTE**
> *The `failrelay-enable` and `led-enable` parameters are non-configurable for link up alarms.*

To configure an alarm, do the following:

1. Make sure the CLI is in Configuration mode.
2. Configure the CoS weighting by typing:

   ```
   admin alarms alarm-config type alarm
   ```

   Where:

   - *`type`* is the type of alarm
   - *`alarm`* is the alarm ID
3. Configure the following parameters as required:

   > **NOTE**
   > *Depending on the alarm type, some of the parameters shown are not available.*

Parameter	Description
description { description }	The name of the alarm.
severity { severity }	**Synopsis:** emergency, alert, critical, error, warning, notice, info, debug The severity level can be one of emergency, alert, critical, error, warning, notice, info, and debug. This cannot be changed for some alarms.
admin-enable	If disabled, the alarm is not reported in the active list and does not actuate LED/failrelay.
failrelay-enable	If enabled, this alarm will assert the failrelay.
led-enable	If enabled, the main 'Alarm' LED light will be red when this alarm is asserted. If disabled, the main 'Alarm' LED light is not affected by this alarm.
auto-clear	If enabled, the LED and failrelay will be cleared automatically when condition is met.

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

Section 4.7

Managing Certificates and Keys

The following sections describe how to configure and manage certificates and keys on the device:

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

- Section 4.7.1, “Managing CA Certificates and CRLs”
- Section 4.7.2, “Managing Private Keys”
- Section 4.7.3, “Managing Public Keys”
- Section 4.7.4, “Managing Certificates”

Section 4.7.1

Managing CA Certificates and CRLs

The following sections describe how to configure and manage CA certificates and their associated Certificate Revocation Lists (CRLs) on the device:

- Section 4.7.1.1, “Viewing a List of CA Certificates and CRLs”
- Section 4.7.1.2, “Viewing the Status of a CA Certificate and CRL”
- Section 4.7.1.3, “Adding a CA Certificate and CRL”
- Section 4.7.1.4, “Deleting a CA Certificate and CRL”

Section 4.7.1.1

Viewing a List of CA Certificates and CRLs

To view a list of certificates issued by a Certified Authority (CA) and the Certificate Revocation Lists (CRLs) associated with them, type:

```
show running-config security crypto ca
```

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

```
ruggedcom# show running-config security crypto ca
security
 crypto
  ca ca-cert
   key-cert-sign-certificate "{--contents--}"
  !
 !
!
```

If no certificates have been configured, add certificates as needed. For more information, refer to Section 4.7.1.3, “Adding a CA Certificate and CRL”.

Section 4.7.1.2

Viewing the Status of a CA Certificate and CRL

To view the status of a CA certificate, type:

```
show security crypto ca certificate key-cert-sign-certificate-status
```

Where:

- *certificate* is the name of the certificate

This table or list provides the following information:

Parameter	Description
issuer	
subject	
not-before	**Synopsis:** The date-and-time type is a profile of the ISO 8601 standard for representation of dates and times using the Gregorian calendar. The profile is defined by the date-time production in Section 5.6 of RFC 3339. The date-and-time type is compatible with the dateTime XML schema type with the following notable exceptions: (a) The date-and-time type does not allow negative years. (b) The date-and-time time-offset -00:00 indicates an unknown time zone (see RFC 3339) while -00:00 and +00:00 and Z all represent the same time zone in dateTime. (c) The canonical format (see below) of data-and-time values differs from the canonical format used by the dateTime XML schema type, which requires all times to be in UTC using the time-offset 'Z'. This type is not equivalent to the DateAndTime textual convention of the SMIv2 since RFC 3339 uses a different separator between full-date and full-time and provides higher resolution of time-secfrac. The canonical format for date-and-time values with a known time zone uses a numeric time zone offset that is calculated using the device's configured known offset to UTC time. A change of the device's offset to UTC time will cause date-and-time values to change accordingly. Such changes might happen periodically in case a server follows automatically daylight saving time (DST) time zone offset changes. The canonical format for date-and-time values with an unknown time zone (usually referring to the notion of local time) uses the time-offset -00:00. This certificate is not valid before this date.
not-after	**Synopsis:** The date-and-time type is a profile of the ISO 8601 standard for representation of dates and times using the Gregorian calendar. The profile is defined by the date-time production in Section 5.6 of RFC 3339. The date-and-time type is compatible with the dateTime XML schema type with the following notable exceptions: (a) The date-and-time type does not allow negative years. (b) The date-and-time time-offset -00:00 indicates an unknown time zone (see RFC 3339) while -00:00 and +00:00 and Z all represent the same time zone in dateTime. (c) The canonical format (see below) of data-and-time values differs from the canonical format used by the dateTime XML schema type, which requires all times to be in UTC using the time-offset 'Z'. This type is not equivalent to the DateAndTime textual convention of the SMIv2 since RFC 3339 uses a different separator between full-date and full-time and provides higher resolution of time-secfrac. The canonical format for date-and-time values with a known time zone uses a numeric time zone offset that is calculated using the device's configured known offset to UTC time. A change of the device's offset to UTC time will cause date-and-time values to change accordingly. Such changes might happen periodically in case a server follows automatically daylight saving time (DST) time zone offset changes. The canonical format for date-and-time values with an unknown time zone (usually referring to the notion of local time) uses the time-offset -00:00. This certificate is not valid after this date.

To view the status of a Certificate Revocation List (CRL) that was signed by a separate certificate, type:

```
show security crypto ca certificate crl-sign-certificate-status
```

Where:

- *certificate* is the name of the certificate

This table or list provides the following information:

Parameter	Description
issuer	
subject	
not-before	**Synopsis:** The date-and-time type is a profile of the ISO 8601 standard for representation of dates and times using the Gregorian calendar. The profile is defined by the date-time production in Section 5.6 of RFC 3339. The date-and-time type is compatible with the dateTime XML schema type with the following notable exceptions: (a) The date-and-time type does not allow negative years. (b) The date-and-time time-offset -00:00 indicates an unknown time zone (see RFC 3339) while -00:00 and +00:00 and Z all represent the same

Parameter	Description
	time zone in dateTime. (c) The canonical format (see below) of data-and-time values differs from the canonical format used by the dateTime XML schema type, which requires all times to be in UTC using the time-offset 'Z'. This type is not equivalent to the DateAndTime textual convention of the SMIv2 since RFC 3339 uses a different separator between full-date and full-time and provides higher resolution of time-secfrac. The canonical format for date-and-time values with a known time zone uses a numeric time zone offset that is calculated using the device's configured known offset to UTC time. A change of the device's offset to UTC time will cause date-and-time values to change accordingly. Such changes might happen periodically in case a server follows automatically daylight saving time (DST) time zone offset changes. The canonical format for date-and-time values with an unknown time zone (usually referring to the notion of local time) uses the time-offset -00:00. This certificate is not valid before this date.
not-after	**Synopsis:** The date-and-time type is a profile of the ISO 8601 standard for representation of dates and times using the Gregorian calendar. The profile is defined by the date-time production in Section 5.6 of RFC 3339. The date-and-time type is compatible with the dateTime XML schema type with the following notable exceptions: (a) The date-and-time type does not allow negative years. (b) The date-and-time time-offset -00:00 indicates an unknown time zone (see RFC 3339) while -00:00 and +00:00 and Z all represent the same time zone in dateTime. (c) The canonical format (see below) of data-and-time values differs from the canonical format used by the dateTime XML schema type, which requires all times to be in UTC using the time-offset 'Z'. This type is not equivalent to the DateAndTime textual convention of the SMIv2 since RFC 3339 uses a different separator between full-date and full-time and provides higher resolution of time-secfrac. The canonical format for date-and-time values with a known time zone uses a numeric time zone offset that is calculated using the device's configured known offset to UTC time. A change of the device's offset to UTC time will cause date-and-time values to change accordingly. Such changes might happen periodically in case a server follows automatically daylight saving time (DST) time zone offset changes. The canonical format for date-and-time values with an unknown time zone (usually referring to the notion of local time) uses the time-offset -00:00. This certificate is not valid after this date.

To view the status of a Certificate Revocation List (CRL) that was not signed by a separate certificate, type:

```
show security crypto ca certificate crl-status
```

Where:

- *certificate* is the name of the certificate

This table or list provides the following information:

Parameter	Description
issuer	
this-update	**Synopsis:** The date-and-time type is a profile of the ISO 8601 standard for representation of dates and times using the Gregorian calendar. The profile is defined by the date-time production in Section 5.6 of RFC 3339. The date-and-time type is compatible with the dateTime XML schema type with the following notable exceptions: (a) The date-and-time type does not allow negative years. (b) The date-and-time time-offset -00:00 indicates an unknown time zone (see RFC 3339) while -00:00 and +00:00 and Z all represent the same time zone in dateTime. (c) The canonical format (see below) of data-and-time values differs from the canonical format used by the dateTime XML schema type, which requires all times to be in UTC using the time-offset 'Z'. This type is not equivalent to the DateAndTime textual convention of the SMIv2 since RFC 3339 uses a different separator between full-date and full-time and provides higher resolution of time-secfrac. The canonical format for date-and-time values with a known time zone uses a numeric time zone offset that is calculated using the device's configured known offset to UTC time. A change of the device's offset to UTC time will cause date-and-time values to change accordingly. Such changes might happen periodically in case a server follows automatically daylight saving time (DST) time zone offset changes. The canonical format for date-and-time values with an unknown time zone (usually referring to the notion of local time) uses the time-offset -00:00. This CRL was updated at this date and time.

Parameter	Description
next-update	**Synopsis:** The date-and-time type is a profile of the ISO 8601 standard for representation of dates and times using the Gregorian calendar. The profile is defined by the date-time production in Section 5.6 of RFC 3339. The date-and-time type is compatible with the dateTime XML schema type with the following notable exceptions: (a) The date-and-time type does not allow negative years. (b) The date-and-time time-offset -00:00 indicates an unknown time zone (see RFC 3339) while -00:00 and +00:00 and Z all represent the same time zone in dateTime. (c) The canonical format (see below) of data-and-time values differs from the canonical format used by the dateTime XML schema type, which requires all times to be in UTC using the time-offset 'Z'. This type is not equivalent to the DateAndTime textual convention of the SMIv2 since RFC 3339 uses a different separator between full-date and full-time and provides higher resolution of time-secfrac. The canonical format for date-and-time values with a known time zone uses a numeric time zone offset that is calculated using the device's configured known offset to UTC time. A change of the device's offset to UTC time will cause date-and-time values to change accordingly. Such changes might happen periodically in case a server follows automatically daylight saving time (DST) time zone offset changes. The canonical format for date-and-time values with an unknown time zone (usually referring to the notion of local time) uses the time-offset -00:00. This certificate must be updated by this date and time.

Section 4.7.1.3
Adding a CA Certificate and CRL

To add a certificate issued by a Certified Authority (CA) and its associated Certificate Revocation List (CRL), do the following:

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

1. Enable auto-wizard by typing:

```
autowizard true
```

2. Make sure the CLI is in Configuration mode.

> **NOTE**
> *Before inserting the contents of the certificate, enter multi-line mode by pressing **Esc+m**. Press **Ctrl+d** to exit multi-line mode after the certificate has been added.*

3. Add the CA certificate by typing:

```
security crypto ca certificate key-cert-sign-certificate contents
```

Where:

- *certificate* is the name of the certificate
- *contents* is the contents of the certificate

4. Add the associated Certificate Revocation List (CRL).

> **NOTE**
> *Large CRLs (bigger than 100KB) are not currently supported and may be difficult to add/view in the configuration.*

> **NOTE**
> *Before inserting the contents of the CRL, enter multi-line mode by pressing **Esc+m**. Press **Ctrl+d** to exit multi-line mode after the CRL has been added.*

- If the CRL is signed by a separate certificate, type:

  ```
  security crypto ca certificate crl-sign-certificate contents
  ```

  Where:

  - *certificate* is the name of the certificate
  - *contents* is the contents of the signed CRL

- If the CRL is not signed, type:

  ```
  security crypto ca certificate crl contents
  ```

  Where:

  - *certificate* is the name of the certificate
  - *contents* is the contents of the CRL

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

Section 4.7.1.4

Deleting a CA Certificate and CRL

To delete a certificate issued by a Certified Authority (CA) and its associated Certificate Revocation List (CRL), do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the CA certificate and its associated Certificate Revocation List (CRL) by typing:

   ```
   no security crypto ca certificate
   ```

   Where:

   - *certificate* is the name of the certificate

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

Section 4.7.2

Managing Private Keys

The following sections describe how to configure and manage unsigned private keys on the device:

> **NOTE**
> *Private keys are automatically encrypted using an AES-CFB-128 cipher to protect them from being viewed by unauthorized users.*

- Section 4.7.2.1, “Viewing a List of Private Keys”
- Section 4.7.2.2, “Adding a Private Key”
- Section 4.7.2.3, “Deleting a Private Key”

Section 4.7.2.1

Viewing a List of Private Keys

To view a list of unsigned private keys, type:

```
show running-config security crypto private-key
```

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

```
ruggedcom# show running-config security crypto private-key
security
 crypto
  private-key key
   algorithm rsa
   contents
   "{--contents--}"
  !
 !
!
```

If no private keys have been configured, add keys as needed. For more information, refer to Section 4.7.2.2, “Adding a Private Key”.

Section 4.7.2.2

Adding a Private Key

To add an unsigned private key, do the following:

1. Enable auto-wizard by typing:

```
autowizard true
```

2. Make sure the CLI is in Configuration mode.
3. Add the private key by typing:

```
security crypto private-key name
```

Where:

- *name* is the name of the private key

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

> **NOTE**
> *Before inserting the contents of the key, enter multi-line mode by pressing **Esc+m**. Press **Ctrl+d** to exit multi-line mode after the key has been added.*

Parameter	Description
algorithm { algorithm }	**Synopsis:** rsa, dsa The type of key.
contents { contents }	**Synopsis:** The aes-cfb-128-encrypted-string works exactly like des3-cbc-encrypted-string but AES/128bits in CFB mode is used to encrypt the string. The prefix for encrypted values is '4'. The contents of the unsigned private key.

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

Section 4.7.2.3
Deleting a Private Key

To delete an unsigned private key, do the following:

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

```
no security crypto private-key key name
```

   Where:

   - *name* is the name of the private key
3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 4.7.3
Managing Public Keys

The following sections describe how to configure and manage unsigned public keys on the device:

- Section 4.7.3.1, “Viewing a List of Public Keys”
- Section 4.7.3.2, “Adding a Public Key”
- Section 4.7.3.3, “Deleting a Public Key”

Section 4.7.3.1
Viewing a List of Public Keys

To view a list of unsigned public keys, type:

```
show running-config security crypto public-key
```

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

```
ruggedcom# show running-config security crypto public-key
security
crypto
  public-key ipsec-generated
   algorithm        rsa
   contents         "{--contents--}"
   private-key-name ipsec-generated
  !
!
!
```

If no public keys have been configured, add keys as needed. For more information, refer to Section 4.7.3.2, “Adding a Public Key”.

Section 4.7.3.2
Adding a Public Key

To add an unsigned public key, do the following:

> **NOTE**
> *Do not associate the public key with the private key if the public key belongs to another device.*

1. Make sure the private key associated with the public key has been added. For more information, refer to Section 4.7.2.2, “Adding a Private Key”.
2. Enable auto-wizard by typing:

```
autowizard true
```

3. Make sure the CLI is in Configuration mode.
4. Add the public key by typing:

```
security crypto public-key name
```

Where:

- *name* is the name of the public key

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

> **NOTE**
> *Before inserting the contents of the key, enter multi-line mode by pressing **Esc+m**. Press **Ctrl+d** to exit multi-line mode after the key has been added.*

Parameter	Description
algorithm { algorithm }	**Synopsis:** rsa, dsa The algorithm of the key.
contents { contents }	The contents of the key.
private-key-name { private-key-name }	The private key name associated with this public key.

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

Section 4.7.3.3
Deleting a Public Key

To delete an unsigned public key, do the following:

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

```
no security crypto public-key key name
```

Where:

- *name* is the name of the public key

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

Section 4.7.4

Managing Certificates

The following sections describe how to configure and manage certificates on the device:

- Section 4.7.4.1, "Viewing a List of Certificates"
- Section 4.7.4.2, "Viewing the Status of a Certificate"
- Section 4.7.4.3, "Adding a Certificate"
- Section 4.7.4.4, "Deleting a Certificate"

Section 4.7.4.1

Viewing a List of Certificates

To view a list of certificates, type:

```
show running-config security crypto certificate
```

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

```
ruggedcom# show running-config security crypto certificate
security
 crypto
  certificate cert
   contents         "{--contents--}"
   private-key-name key
   ca-name          ca-cert
  !
 !
!
```

If no certificates have been configured, add certificates as needed. For more information, refer to Section 4.7.4.3, "Adding a Certificate".

Section 4.7.4.2

Viewing the Status of a Certificate

To view the status of a certificate, type:

```
show security crypto certificate certificate status
```

Where:

- *certificate* is the name of the certificate

This table or list provides the following information:

Parameter	Description
issuer	
subject	
not-before	**Synopsis:** The date-and-time type is a profile of the ISO 8601 standard for representation of dates and times using the Gregorian calendar. The profile is defined by the date-time production in Section 5.6 of RFC 3339. The date-and-time type is compatible with the dateTime XML schema type with the following notable exceptions: (a) The date-and-time type does not allow negative years. (b) The date-and-time time-offset -00:00 indicates an

Parameter	Description
	unknown time zone (see RFC 3339) while -00:00 and +00:00 and Z all represent the same time zone in dateTime. (c) The canonical format (see below) of data-and-time values differs from the canonical format used by the dateTime XML schema type, which requires all times to be in UTC using the time-offset 'Z'. This type is not equivalent to the DateAndTime textual convention of the SMIv2 since RFC 3339 uses a different separator between full-date and full-time and provides higher resolution of time-secfrac. The canonical format for date-and-time values with a known time zone uses a numeric time zone offset that is calculated using the device's configured known offset to UTC time. A change of the device's offset to UTC time will cause date-and-time values to change accordingly. Such changes might happen periodically in case a server follows automatically daylight saving time (DST) time zone offset changes. The canonical format for date-and-time values with an unknown time zone (usually referring to the notion of local time) uses the time-offset -00:00. This certificate is not valid before this date.
not-after	**Synopsis:** The date-and-time type is a profile of the ISO 8601 standard for representation of dates and times using the Gregorian calendar. The profile is defined by the date-time production in Section 5.6 of RFC 3339. The date-and-time type is compatible with the dateTime XML schema type with the following notable exceptions: (a) The date-and-time type does not allow negative years. (b) The date-and-time time-offset -00:00 indicates an unknown time zone (see RFC 3339) while -00:00 and +00:00 and Z all represent the same time zone in dateTime. (c) The canonical format (see below) of data-and-time values differs from the canonical format used by the dateTime XML schema type, which requires all times to be in UTC using the time-offset 'Z'. This type is not equivalent to the DateAndTime textual convention of the SMIv2 since RFC 3339 uses a different separator between full-date and full-time and provides higher resolution of time-secfrac. The canonical format for date-and-time values with a known time zone uses a numeric time zone offset that is calculated using the device's configured known offset to UTC time. A change of the device's offset to UTC time will cause date-and-time values to change accordingly. Such changes might happen periodically in case a server follows automatically daylight saving time (DST) time zone offset changes. The canonical format for date-and-time values with an unknown time zone (usually referring to the notion of local time) uses the time-offset -00:00. This certificate is not valid after this date.

Section 4.7.4.3

Adding a Certificate

To add a certificate, do the following:

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

1. Make sure the required CA certificates, public keys and/or private keys have been added to the device.
   - For more information about adding CA Certificates, refer to Section 4.7.1.3, “Adding a CA Certificate and CRL”
   - For more information about adding public keys, refer to Section 4.7.3.2, “Adding a Public Key”
   - For more information about adding private keys, refer to Section 4.7.2.2, “Adding a Private Key”
2. Enable auto-wizard by typing:

```
autowizard true
```

3. Make sure the CLI is in Configuration mode.
4. Add the certificate by typing:

```
autowizard true security crypto certificate certificate
```

Where:

- *certificate* is the name of the certificate.

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

> **NOTE**
> *Before inserting the contents of the certificate, enter multi-line mode by pressing **Esc+m**. Press **Ctrl+d** to exit multi-line mode after the certificate has been added.*

Parameter	Description
contents { contents }	The contents of the certificate.
private-key-name { private-key-name }	The private key associated with this certificate.
ca-name { ca-name }	The optional CA certificate for this certificate.

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

Section 4.7.4.4

Deleting a Certificate

To delete a certificate, do the following:

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

```
no security crypto certificate certificate
```

Where:

- *certificate* is the name of the certificate.

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

Section 4.8

Managing RADIUS Authentication

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

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

> **NOTE**
> *For more information about the RADIUS protocol, refer to RFC 2865 [http://tools.ietf.org/html/rfc2865].*
>
> *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 4.4, "Setting the User Authentication Mode".*

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

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

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

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

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

[a] *EAP-Message is an extension attribute for RADIUS, as defined by RFC 2869.*

Primary and secondary RADIUS servers, typically operating from a common database, can be configured for redundancy. If the first server does not respond to an authentication request, the request will be forwarded to the second server until a positive/negate acknowledgement 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 occurence, source and result are included. For more information about the authentication log file, refer to Section 3.8.1, "Viewing Logs".*

ROX II supports RADIUS authenticaton 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 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, ROX II will not complete the authentication request.

The following sections describe how to configure and manage RADIUS authentication:

- Section 4.8.1, "Configuring RADIUS Authentication for LOGIN Services"
- Section 4.8.2, "Configuring RADIUS Authentication for PPP Services"
- Section 4.8.3, "Configuring RADIUS Authentication for Switched Ethernet Ports"

Section 4.8.1

Configuring RADIUS Authentication for LOGIN Services

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

IMPORTANT!
Passwords are case-sensitive.

1. Make sure the CLI is in Configuration mode.
2. Type the following:

```
admin authentication radius
```

3. Configure the primary or secondary RADIUS server by typing either **primary** or **secondary** and configuring the following parameter(s) as required:

Parameter	Description
address { address }	**Synopsis:** The ip-address type represents an IP address and is IP version neutral. The format of the textual representations implies the IP version. The IP address of the server.
port-udp { port-udp }	**Default:** 1812 The network port of the server.
password { password }	**Synopsis:** The aes-cfb-128-encrypted-string works exactly like des3-cbc-encrypted-string but AES/128bits in CFB mode is used to encrypt the string. The prefix for encrypted values is '4'. The password of the RADIUS server.

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

Section 4.8.2

Configuring RADIUS Authentication for PPP Services

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

> **IMPORTANT!**
> *Passwords are case-sensitive.*

1. Make sure the CLI is in Configuration mode.
2. Type the following:

```
global ppp radius
```

3. Configure the primary or secondary RADIUS server by typing either **primary** or **secondary** and configuring the following parameter(s) as required:

Parameter	Description
address { address }	The IPv4 address of the server.
port-udp { port-udp }	**Default:** 1812
password { password }	**Synopsis:** The aes-cfb-128-encrypted-string works exactly like des3-cbc-encrypted-string but AES/128bits in CFB mode is used to encrypt the string. The prefix for encrypted values is '4'.

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

Section 4.8.3

Configuring RADIUS Authentication for Switched Ethernet Ports

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

> **IMPORTANT!**
> *Passwords are case-sensitive.*

1. Make sure the CLI is in Configuration mode.
2. Type the following:

```
switch port-security radius
```

3. Configure the primary or secondary RADIUS server by typing either **primary** or **secondary** and configuring the following parameter(s) as required:

Parameter	Description
address { address }	The IPv4 address of the server.
port-udp { port-udp }	**Default:** 1812 The IPv4 port of the server.
password { password }	**Synopsis:** The aes-cfb-128-encrypted-string works exactly like des3-cbc-encrypted-string but AES/128bits in CFB mode is used to encrypt the string. The prefix for encrypted values is '4'. The password of the server

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

Section 4.9
Managing Users

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

- Guest
- Operator
- Admin

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

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

CAUTION!
Security hazard – risk of unauthorized access and/or exploitation. To prevent unauthorized access to the device, make sure to change the default passwords for all users before commissioning the device. For more information, refer to Section 4.10.2, “Setting a User Password/Passphrase”.

The following sections describe how to configure and manage users:

- Section 4.9.1, “Viewing a List of Users”
- Section 4.9.2, “Adding a User”
- Section 4.9.3, “Deleting a User”
- Section 4.9.4, “Monitoring Users”

Section 4.9.1
Viewing a List of Users

To view a list of user accounts, type:

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

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

```
ruggedcom# show running-config admin users | tab
admin
 users
  userid
NAME    PASSWORD                            ROLE
```

```
----------------------------------------------------------
admin  $1$LmRO$j7/q/wtlwjfUvbOVrbt4o.      administrator
guest  $1$uGztU0$6b7YS6gqwtrelTzA/2noQ.    guest
oper   $1$eSsFfFMh$NEHgTHsU1T4RRz8sXNV2F1  operator
```

If no user accounts have been configured, add user accounts as needed. For more information, refer to Section 4.9.2, “Adding a User”.

Section 4.9.2
Adding a User

To add a new user account, do the following:

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

```
admin users name name role role
```

   Where:

   - *name* is the name of the user account
   - *role* is the role of the user. The options are `administrator`, `operator`, and `guest`.

3. To set the user password, follow the instructions in Section 4.10.2, “Setting a User Password/Passphrase”.
4. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 4.9.3
Deleting a User

To delete a user account, do the following:

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

```
no admin users name
```

   Where:

   - *name* is the name of the user account.

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

Section 4.9.4
Monitoring Users

Users currently logged in to the device are monitored by ROX II and can be viewed through the CLI. ROX II allows administrators to monitor users, log users out, and broadcast message to all users.

To view a list of users currently logged in to the device, type:

```
who
```

A table or list similar to the following appears:

```
ruggedcom# who
Session User  Context From          Proto Date     Mode
*147    admin cli     192.168.0.200 ssh   11:04:54 operational
 145    admin webui   192.168.0.200 https 10:51:05 operational
```

The following sections describe other actions that can be used to manage users logged in to the device:

- Section 4.9.4.1, “Kicking Users from the Network”
- Section 4.9.4.2, “Sending Messages to Users”

Section 4.9.4.1
Kicking Users from the Network

To log a user out of the device, type:

Type:

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

Where:

- *number* is the session number
- *profile* is the name of the user profile

Section 4.9.4.2
Sending Messages to Users

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

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

Where:

- *profile* is the name of the user profile
- *message* is the message

Section 4.10
Managing Passwords and Passphrases

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

For a list of default passwords, refer to Section 2.2, “Default Usernames 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.

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

NOTE
User authentication can also be verified through a RADIUS server. When enabled for authentication and authorization, the RADIUS server will be used in the absence of any local settings. For more information about configuring a RADIUS server, refer to Section 4.8, "Managing RADIUS Authentication".

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

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

The following sections describe how to configure and manage passwords and passphrases:

- Section 4.10.1, "Configuring Password/Passphrase Complexity Rules"
- Section 4.10.2, "Setting a User Password/Passphrase"
- Section 4.10.3, "Setting the Boot Password/Passphrase"
- Section 4.10.4, "Setting the Maintenance Password/Passphrase"
- Section 4.10.5, "Resetting the Admin Password/Passphrase"
- Section 4.10.6, "Resetting the Boot Password/Passphrase"
- Section 4.10.7, "Resetting the Maintenance Password/Passphrase"

Section 4.10.1

Configuring Password/Passphrase Complexity Rules

Special rules for password/passphrase complexity can be configured. These include setting the password/passphrase length and enabling requirements for special characters.

To configure the password/passphrase complexity rules for all passwords/passphrases, do the following:

NOTE
Password/passphrase complexity rules do not apply to passwords/passphrases previously configured on the device.

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

Parameter	Description
minimum-length { minimum-length }	**Default:** 12 Minimum password length.
maximum-length { maximum-length }	**Default:** 128 Maximum password length.
uppercase-required	**Default:** true

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

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

Section 4.10.2

Setting a User Password/Passphrase

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

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

```
admin users userid profile set-password new-password new-password-passphrase new-password-repeat new-password-passphrase
```

Where:

- *profile* is the user profile (e.g. admin, oper or guest)
- *new-password-passphrase* is the new password/passphrase. Make sure the password/passphrase complies with the password complexity rules configured for this device.

Section 4.10.3

Setting the Boot Password/Passphrase

The boot password/passphrase grants access to BIST mode and service mode, which are only accessible through the Command Line Interface (CLI). For more information about these modes, refer to Section 2.6.1, "Accessing Different CLI Modes".

> **CAUTION!**
> *Security hazard – risk of unauthorized access and/or exploitation. User authentication is not required to access BIST mode. Configure a boot password/passphrase to control initial access to the device.*

> **IMPORTANT!**
> *The boot password/passphrase is only supported by version 2010.09RR16 or later of the uboot binary. For information about determining and/or upgrading the uboot version installed on the device, refer to the application note Upgrading Uboot on ROX Devices available on www.siemens.com/ruggedcom.*

NOTE
To set a blank password/passphrase, type `""` (double quotes).

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

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

NOTE
A passphrase must consist of four separate words and each word must be 4 to 20 characters long.

1. Enable autowizard by typing:

```
autowizard true
```

2. Set the boot password/passphrase by typing:

```
admin authentication set-boot-password new-password new-password-passphrase new-password-repeat
new-password-passphrase old-password old-password-passphrase
```

Where:

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

Section 4.10.4

Setting the Maintenance Password/Passphrase

The maintenance password/passphrase grants access to the maintenance mode, which is only accessible through the Command Line Interface (CLI). For more information about this mode, refer to Section 2.6.1, "Accessing Different CLI Modes".

CAUTION!
Configuration hazard – risk of data corruption. Maintenance mode is provided for troubleshooting purposes and should only be used by Siemens 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.

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

To set the maintenance password, do the following:

NOTE
A passphrase must consist of four separate words and each word must be 4 to 20 characters long.

1. Enable autowizard by typing:

```
autowizard true
```

2. Set the maintenance password/passphrase by typing:

```
admin authentication set-maint-password new-password new-password-passphrase new-password-repeat new-password-passphrase old-password old-password-passphrase
```

Where:

- *new-password-passphrase* is the new password/passphrase. Make sure the password/passphrase complies with the password complexity rules configured for this device.
- *old-password-passphrase* is the old password/passphrase

Section 4.10.5

Resetting the Admin Password/Passphrase

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

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

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

1. Enter service mode. For more information, refer to Section 2.8.2, “Accessing Service Mode”.
2. Type **root** and press **Enter**. The password prompt appears.
3. Type the password/passphrase associated with the root profile and press **Enter**. The default password is *admin*.
4. Type **confd_cli** and press **Enter**.
5. Enable autowizard by typing:

```
autowizard true
```

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

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

7. Reset the admin password/passphrase by typing:

```
admin users userid admin set-password new-password new-password-passphrase new-password-repeat new-password-passphrase
```

Where:

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

8. Reboot the device. For more information, refer to Section 3.5, “Rebooting the Device”.
9. As soon as the device starts to boot up, press **ESC**. A list of possible boot modes for each partition appears.

```
****Boot Partition 4****
```

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

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

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

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

Will reboot after 60 seconds of inactivity
:
```

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

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

Section 4.10.6
Resetting the Boot Password/Passphrase

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

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

1. Log in to maintenance mode. For more information, refer to Section 2.8.3, “Accessing Maintenance Mode”.
2. Delete current boot password/passphrase by typing:

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

3. Type **`exit`** and press **Enter**.
4. Set a new boot password/passphrase. For more information, refer to Section 4.10.3, “Setting the Boot Password/Passphrase”.

Section 4.10.7
Resetting the Maintenance Password/Passphrase

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

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

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

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

1. Make sure the CLI is in Configuration mode.
2. Reset the maintenance password by setting a new password. For more information, refer to Section 4.10.4, "Setting the Maintenance Password/Passphrase".
3. Reboot the device. For more information, refer to Section 3.5, "Rebooting the Device".
4. As soon as the device starts to boot up, press **ESC**. A list of possible boot modes for each partition appears.

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

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

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

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

 Will reboot after 60 seconds of inactivity
 :
```

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

5. Enter the inactive partition by typing the associated target number. For example, if the active partition is Boot Partition 4, type **`6-0`** and press **Enter** to enter Boot Partition 6.
6. Log in to ROX II. For more information about logging in to ROX II, refer to Section 2.3, "Logging In".
7. Repeat Step 1 and Step 5 to reset the password/passphrase on the inactive partition and switch back to the original partition.

Section 4.11

Scheduling Jobs

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

There are two types of scheduled jobs:

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

The following sections describe how to configure and manage scheduled jobs:

- Section 4.11.1, “Viewing a List of Scheduled Jobs”
- Section 4.11.2, “Adding Scheduled Jobs”
- Section 4.11.3, “Deleting a Scheduled Job”

Section 4.11.1

Viewing a List of Scheduled Jobs

To view a list of scheduled jobs, type:

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

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

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

If no jobs have been configured, add jobs as needed. For more information, refer to Section 4.11.2, “Adding Scheduled Jobs”.

Section 4.11.2

Adding Scheduled Jobs

To add a scheduled job, do the following:

1. Make sure the CLI is in Configuration mode.
2. Configure the following parameter(s) as required:

Parameter	Description
{ scheduler-job-name }	The name of the scheduled job. The name can be up to 64 characters in length.
job-type { job-type }	**Synopsis:** configchange, periodic

Parameter	Description
	Default: periodic Determines when to launch the scheduled job: • periodic: The job launches at a set date and time. • configchange: The job launches when the configuration changes.
job-minute { job-minute }	**Default:** 0 For periodic jobs, sets the minutes portion of the job launch time. Valid values are in the range of 0 to 59. If no value is set, the scheduler uses the default value of 0 and launches the job every hour on the the hour. • To specify a single value, enter the value in the field. For example, to launch the job 10 minutes past the hour, enter 10. • To specify a list of values, enter the values as a comma-separated list. For example, to launch the job at 15, 30, and 45 minutes past the hour, enter 15,30,45. • To specify a range of values, enter the range as comma-separated values. For example, to launch the job every minute between 30 and 45 minutes past the hour, enter 30-45. This parameter is not required for configchange jobs.
job-hour { job-hour }	For periodic jobs, sets the hour portion of the job launch time, in the 24-hour clock format. Valid values are in the range of 0 to 23. If no value is set, the job launches every hour at the time set in the Minute field. • To specify a single value, enter the value in the field. For example, to launch the job at 5:00 pm, enter 17. • To specify a list of values, enter the values as a comma-separated list. For example, to launch the job at 9:00 am, 12:00 pm, and 5:00 pm, enter 9,12,17. • To specify a range of values, enter the range as comma-separated values. For example, to launch the job every hour between 9:00 am and 5:00 pm, enter 9-17. This parameter is not required for configchange jobs.
job-day-month { job-day-month }	For periodic jobs, sets the day of the month on which to run the scheduled job. Valid values are in the range of 1 to 31. If no value is set, the job launches every day. • To specify a single value, enter the value in the field. For example, to launch the job on the tenth day of the month, enter 10. • To specify a list of values, enter the values as a comma-separated list. For example, to launch the job on the first, fifteenth, and thirtieth days of the month, enter 10,15,30. • To specify a range of values, enter the range as comma-separated values. For example, to launch the job on days one through fifteen, enter 1-15. This parameter is not required for configchange jobs.
job-month { job-month }	For periodic jobs, sets the month in which to run the scheduled job. Valid values are in the rage of 1 to 12. If no value is set, the job launches every day. • To specify a single value, enter the value in the field. For example, to set the month to February, enter 2. • To specify a list of values, enter the values as a comma-separated list. For example, to set the months to January, June, and December, enter 1,6,12. • To specify a range of values, enter the range as comma-separated values. For example, to set the months to January through June, enter 1-6. This parameter is not required for configchange jobs.
job-day-week { job-day-week }	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.

Parameter	Description
	This parameter is not required for configchange jobs.
job-command { job-command }	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.

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

Section 4.11.3

Deleting a Scheduled Job

To delete a scheduled Job, do the following:

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

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

Where:

- *`name`* is the name of the scheduled job

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

5 Setup and Configuration

This chapter describes how to setup and configure the device for use on a network using the various features available in ROX II. It describes the following tasks:

- Section 5.1, “Configuring a Basic Network”
- Section 5.2, “Configuring ICMP Control”
- Section 5.3, “Enabling and Configuring CLI Sessions”
- Section 5.4, “Enabling and Configuring SFTP Sessions”
- Section 5.5, “Enabling Configuring WWW Interface Sessions”
- Section 5.6, “Enabling/Disabling Brute Force Attack Protection”
- Section 5.7, “Viewing the Status of IPv4 Routes”
- Section 5.8, “Viewing the Status of IPv6 Routes”
- Section 5.9, “Viewing the Memory Statistics”
- Section 5.10, “Managing NETCONF”
- Section 5.11, “Managing SNMP”
- Section 5.12, “Managing Time Synchronization Functions”
- Section 5.13, “Managing Cellular Modem Profiles”
- Section 5.14, “Managing the DHCP Relay Agent”
- Section 5.15, “Managing the DHCP Server”
- Section 5.16, “Managing Port Mirroring”
- Section 5.17, “Managing Firewalls”
- Section 5.18, “Managing IS-IS”
- Section 5.19, “Managing BGP”
- Section 5.20, “Managing RIP”
- Section 5.21, “Managing OSPF”
- Section 5.22, “Managing Static Routing”
- Section 5.23, “Managing Static Multicast Routing”
- Section 5.24, “Managing Dynamic Multicast Routing”
- Section 5.25, “Managing Multicast Filtering”
- Section 5.26, “Managing VRRP”
- Section 5.27, “Managing Link Failover Protection”
- Section 5.28, “Managing IPsec Tunnels”
- Section 5.29, “Managing Layer 2 Tunnels”
- Section 5.30, “Managing Generic Routing Encapsulation Tunnels”
- Section 5.31, “Managing Layer 3 Switching”
- Section 5.32, “Managing Classes of Service”

- Section 5.33, “Managing MAC Addresses”
- Section 5.34, “Managing Spanning Tree Protocol”
- Section 5.35, “Managing VLANs”
- Section 5.36, “Managing Network Discovery and LLDP”
- Section 5.37, “Managing Traffic Control”
- Section 5.38, “Managing IP Addresses for Routable Interfaces”
- Section 5.39, “Managing MPLS”

Section 5.1

Configuring a Basic Network

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 you have one or more Ethernet line modules installed. It is created implicitly, as all switched ports have a default PVID of 1.

The following table lists the default IP addresses.

Table: Default IP Addresses

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

The following sections describe how to configure a basic network:

- Section 5.1.1, “Configuring a Basic IPv4 Network”
- Section 5.1.2, “Configuring a Basic IPv6 Network”

Section 5.1.1

Configuring a Basic IPv4 Network

To configure a basic IPv4 network, do the following:

1. Connect a computer to the Fast Ethernet (fe-cm-1) port on the router.
2. Configure the computer to be on the same subnet as the port.
3. Configure the computer to use the IP address of the Fast Ethernet port as the default gateway.
4. Connect one of the switched ports from any available line module to a switch that is connected to a LAN.
5. Make sure the computer connected to the switch is on the same subnet as the switch.
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 the computers connected to the switch can be pinged by the computer connectedto the router.

Section 5.1.2
Configuring a Basic IPv6 Network

To configure a basic IPv6 network, do the following:

1. Connect a computer to the Fast Ethernet port (fe-cm-1) of the device and configure the computer to be on the same subnet as the port.
2. Configure an IPv6 address and default gateway for the computer (e.g. FDD1:9AEF:3DE4::1/24 and FDD1:9AEF:3DE4::2).
3. Configure the fe-cm-1 and switch.0001 interfaces on the device with IPv6 addresses.
4. Connect one of the switched ports from any available line module to an IPv6 capable network.
5. Configure the computers on the IPv6 network to be on the same IP subnet as switch.0001 and configure the default gateway address.
6. Enable IPv6 Neighbor Discovery. For more information, refer to Section 5.38.4, “Configuring IPv6 Neighbor Discovery”.
7. Verify the computers connected to switch.001 can be seen by the computer connected to fe-cm-1.

Section 5.2
Configuring ICMP Control

To configure how ROX II manages ICMP redirect messages, do the following:

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

Parameter	Description
ignore-icmp-all	**Default:** false Ignores all ICMP echo requests sent to it.
ignore-icmp-broadcast	**Default:** true Ignores all ICMP ECHO and TIMESTAMP requests sent to it via broadcast/multicast.
tcp-syn-cookies	**Default:** false Sends out syncookies when the syn backlog queue of a socket overflows. This is to prevent against the common 'SYN flood attack'.
send-icmp-redirect	**Default:** true Sends the ICMP redirect.

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

Section 5.3
Enabling and Configuring CLI Sessions

To enable and configure CLI sessions, do the following:

1. Make sure the CLI is in Configuration mode.

2. Navigate to ***admin » cli*** and configure the following parameter(s) as required:

Parameter	Description
enabled	**Default:** true Provides the ability to configure the device via CLI over ssh and serial console.
listen-ip { listen-ip }	**Synopsis:** The ip-address type represents an IP address and is IP version neutral. The format of the textual representations implies the IP version. **Default:** 0.0.0.0 The IP Address the CLI will listen on for CLI requests.
port { port }	**Synopsis:** The port-number type represents a 16-bit port number of an Internet transport layer protocol such as UDP, TCP, DCCP, or SCTP. Port numbers are assigned by IANA. A current list of all assignments is available from <http://www.iana.org/>. Note that the port number value zero is reserved by IANA. In situations where the value zero does not make sense, it can be excluded by subtyping the port-number type. In the value set and its semantics, this type is equivalent to the InetPortNumber textual convention of the SMIv2. **Default:** 22 The port on which the CLI listens for CLI requests.
extra-ip-ports { extra-ip-ports }	**Synopsis:** "extra-ip-ports" occurs in an unbounded array The CLI will also listen on these IP Addresses. For port values, add ':#' to set the non-default port value. (ie. xxx.xxx.xxx.xxx:19343 [::] [::]:16000). If using the default address, do not specify another listen address with the same port.
max-sessions { max-sessions }	**Synopsis:** unbounded **Default:** 10 The maximum number of concurrent CLI sessions.
idle-timeout { idle-timeout }	**Default:** PT30M The maximum time before an idle CLI session is terminated. The default time is 30 minutes, or PT30M. A timeout period of 1 year, 1 month, 2 hours and 30 seconds would be translated as P1Y1MT2H30S. The countdown will not begin if the system is waiting for notifications or if commits are pending. Changes will not take effect until the next CLI session.
greeting { greeting }	**Default:** Welcome to Rugged CLI Sets the greeting presented when the user logs in to the CLI. The string must be enclosed in quotation marks.

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

Section 5.4
Enabling and Configuring SFTP Sessions

To enable and configure SFTP sessions, do the following:

1. Make sure the CLI is in Configuration mode.
2. Configure the following parameter(s) as required:

Parameter	Description
enabled	**Default:** false Enables/Disables the SFTP user interface.

Parameter	Description
listen-ip { listen-ip }	**Synopsis:** The ip-address type represents an IP address and is IP version neutral. The format of the textual representations implies the IP version. **Default:** 0.0.0.0 The IP Address the SFTP will listen on for SFTP requests.
port { port }	**Synopsis:** The port-number type represents a 16-bit port number of an Internet transport layer protocol such as UDP, TCP, DCCP, or SCTP. Port numbers are assigned by IANA. A current list of all assignments is available from <http://www.iana.org/>. Note that the port number value zero is reserved by IANA. In situations where the value zero does not make sense, it can be excluded by subtyping the port-number type. In the value set and its semantics, this type is equivalent to the InetPortNumber textual convention of the SMIv2. **Default:** 2222 The port the SFTP will listen on for SFTP requests.
extra-ip-ports { extra-ip-ports }	**Synopsis:** "extra-ip-ports" occurs in an unbounded array 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.
max-sessions { max-sessions }	**Synopsis:** unbounded **Default:** 10 This parameter is not supported and any value is ignored by the system.

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

Section 5.5

Enabling Configuring WWW Interface Sessions

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

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

Parameter	Description
enabled	**Default:** true Provides the ability to configure WebUI features on the device.
listen-ip { listen-ip }	**Synopsis:** The ip-address type represents an IP address and is IP version neutral. The format of the textual representations implies the IP version. **Default:** 0.0.0.0 The IP Address the CLI will listen on for WebUI requests.
port { port }	**Synopsis:** The port-number type represents a 16-bit port number of an Internet transport layer protocol such as UDP, TCP, DCCP, or SCTP. Port numbers are assigned by IANA. A current list of all assignments is available from <http://www.iana.org/>. Note that the port number value zero is reserved by IANA. In situations where the value zero does not make sense, it can be excluded by subtyping the port-number type. In the value set and its semantics, this type is equivalent to the InetPortNumber textual convention of the SMIv2. **Default:** 443 The port on which the WebUI listens for WebUI requests.
extra-ip-ports { extra-ip-ports }	**Synopsis:** "extra-ip-ports" occurs in an unbounded array

Parameter	Description
	The WebUI will also listen on these IP Addresses. For port values, add ':#' to set non-default port value. (ie. xxx.xxx.xxx.xxx:19343 [::] [::]:16000). If using the default address, do not specify another listen address with the same port.
max-sessions { max-sessions }	**Synopsis:** unbounded **Default:** 20 The maximum number of concurrent WebUI sessions
idle-timeout { idle-timeout }	**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	**Default:** true Redirects traffic from port 80 to port 443. If disabled, port 80 will be closed.
client-certificate-verification { client-certificate-verification }	**Synopsis:** none, peer, fail-if-no-peer-cert **Default:** none Client certificate verifaction level Level of verification the server does on client certificates • none - It does not do any verification. • peer - The server will ask the client for a client-certificate but not fail if the client does not supply a client-certificate. • fail-if-no-peer-cert - The server requires the client to supply a client certificate.

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

Section 5.6

Enabling/Disabling Brute Force Attack Protection

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

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

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

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

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

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

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

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

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

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

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

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

NOTE
For information about how to view auth.log, refer to Section 3.8.1, “Viewing Logs”.

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

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

   ```
   security bruteforce enabled
   ```

   Or disable the BFA protection mechanism by typing:

   ```
   no security bruteforce enabled
   ```

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

Section 5.7
Viewing the Status of IPv4 Routes

To view the status of the IPv4 routes configured on the device, type:

NOTE
It is possible to create a route on a locally connected broadcast network (i.e. without a gateway) without also bringing up a corresponding IP address on that interface. For example, it would be possible to add 192.168.1.0/24 to switch.0001, which has an IP address of 10.0.1.1 but no corresponding alias address on the 192.168.1.0/24 subnet.

```
show routing status ipv4routes
```

If IPv4 routes have been configured, a table or list similar to the following example appears:

```
ruggedcom# show routing status ipv4routes
DESTINATION     GATEWAY  INTERFACE    TYPE    WEIGHT  METRIC
--------------------------------------------------------------
192.168.0.0/24           switch.0001  kernel
```

This table/list provides the following information:

Parameter	Description
destination	The network/prefix.
gateway	The gateway address.
interface	The interface name.
type	The route type.
weight	The route weight.
metric	The route metric value.

If no IPv4 routes have been configured, add routes as needed. For more information, refer to Section 5.38.3.2, “Adding an IPv4 Address”.

Section 5.8

Viewing the Status of IPv6 Routes

To view the status of the IPv6 routes configured on the device, type:

```
show routing status ipv6routes
```

If IPv6 routes have been configured, a table or list similar to the following example appears:

```
ruggedcom# show routing status ipv6routes
DESTINATION  GATEWAY  INTERFACE    TYPE    WEIGHT  METRIC
------------------------------------------------------------
fe80::/64             switch       kernel          256
fe80::/64             dp1          kernel          256
fe80::/64             vrf_lo       kernel          256
fe80::/64             switch.0001  kernel          256
fe80::/64             fe-cm-1      kernel          256
fe80::/64             switch.4094  kernel          256
ff00::/8              switch                       256
ff00::/8              dp1                          256
ff00::/8              vrf_lo                       256
ff00::/8              switch.0001                  256
ff00::/8              fe-cm-1                      256
ff00::/8              switch.4094                  256
```

This table/list provides the following information:

Parameter	Description
destination	The network/prefix.
gateway	The gateway address.
interface	The interface name.
type	The route type.
weight	The route weight.
metric	The metric value.

If no IPv6 routes have been configured, add routes as needed. For more information, refer to Section 5.22.3, “Adding an IPv6 Static Route”.

Section 5.9

Viewing the Memory Statistics

To view statistics related to the Core, RIP, OSPF and BGP daemons, type:

```
show routing status memory
```

A list similar to the following example appears:

```
ruggedcom# show routing status memory
routing status memory
 zebra
  total 405504
  used  359424
  free  46080
 rip
  total 0
  used  0
  free  0
 ospf
  total 0
  used  0
  free  0
 bgp
  total 0
  used  0
  free  0
```

This list provides the following information:

Parameter	Description
total	The total heap allocated (in bytes).
used	The number of used ordinary blocks (in bytes).
free	The number of free ordinary blocks (in bytes).

Section 5.10

Managing NETCONF

The Network Configuration Protocol (NETCONF) is a network configuration protocol developed by the Internet Engineering Task Force (IETF). NETCONF provides functions to download, upload, change, and delete the configuration data on network devices. 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 ROX II NETCONF Reference Guide.

The following sections describe how to configure and manage NETCONF:

- Section 5.10.1, “Enabling and Configuring NETCONF Sessions”
- Section 5.10.2, “Viewing NETCONF Statistics”

Section 5.10.1

Enabling and Configuring NETCONF Sessions

To enable and configure NETCONF sessions, do the following:

1. Make sure the CLI is in Configuration mode.

   CAUTION!
   Security hazard – risk of unauthorized access/exploitation. Configure an idle timeout period for NETCONF to prevent unauthorized access (e.g. a user leaves their station unprotected) or denial of access (e.g. a guest user blocks an admin user by opening the maximum number of NETCONF sessions).

   IMPORTANT!
   Before configuring an idle timeout on a device managed by RUGGEDCOM NMS, make sure NMS is configured to support a timeout period for NETCONF sessions.

2. Navigate to ***admin » netconf*** and configure the following parameter(s) as required:

Parameter	Description
enabled	**Default:** true Provides the ability to configure NETCONF features on the device.
listen-ip { listen-ip }	**Synopsis:** The ip-address type represents an IP address and is IP version neutral. The format of the textual representations implies the IP version. **Default:** 0.0.0.0 The IP Address the CLI will listen on for NETCONF requests.
port { port }	**Synopsis:** The port-number type represents a 16-bit port number of an Internet transport layer protocol such as UDP, TCP, DCCP, or SCTP. Port numbers are assigned by IANA. A current list of all assignments is available from <http://www.iana.org/>. Note that the port number value zero is reserved by IANA. In situations where the value zero does not make sense, it can be excluded by subtyping the port-number type. In the value set and its semantics, this type is equivalent to the InetPortNumber textual convention of the SMIv2. **Default:** 830 The port on which NETCONF listens for NETCONF requests.
extra-ip-ports { extra-ip-ports }	**Synopsis:** "extra-ip-ports" occurs in an unbounded array 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.
max-sessions { max-sessions }	**Synopsis:** unbounded **Default:** 10 The maximum number of concurrent NETCONF sessions.
idle-timeout { idle-timeout }	**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.

Parameter	Description
in-bad-hellos	The total number of sessions silently dropped because an invalid 'hello' message was received. This includes hello messages with a 'session-id' attribute, bad namespace, and bad capability declarations.
in-sessions	The total number of NETCONF sessions started towards the NETCONF peer. inSessions - inBadHellos = 'The number of correctly started NETCONF sessions.'
dropped-sessions	The total number of NETCONF sessions dropped. inSessions - inBadHellos = 'The number of correctly started NETCONF sessions.'
in-rpcs	The total number of RPC requests received.
in-bad-rpcs	The total number of RPCs which were parsed correctly, but couldn't be serviced because they contained non-conformant XML.
out-rpc-errors	The total number of 'rpc-reply' messages with 'rpc-error' sent.
out-notifications	The total number of 'notification' messages sent.

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

Section 5.10.2

Viewing NETCONF Statistics

To view NETCONF related statistics, type:

```
show admin netconf
```

A table or list similar to the following example appears:

```
ruggedcom# show admin netconf
netconf
 statistics
  in bad hellos     0
  in sessions       0
  dropped sessions  0
  in rpcs           0
  in bad rpcs       0
  out rpc errors    0
  out notifications 0
```

This table or list provides the following information:

Parameter	Description
in-bad-hellos	The total number of sessions silently dropped because an invalid 'hello' message was received. This includes hello messages with a 'session-id' attribute, bad namespace, and bad capability declarations.
in-sessions	The total number of NETCONF sessions started towards the NETCONF peer.

Parameter	Description
	inSessions - inBadHellos = 'The number of correctly started NETCONF sessions.'
dropped-sessions	The total number of NETCONF sessions dropped. inSessions - inBadHellos = 'The number of correctly started NETCONF sessions.'
in-rpcs	The total number of RPC requests received.
in-bad-rpcs	The total number of RPCs which were parsed correctly, but couldn't be serviced because they contained non-conformant XML.
out-rpc-errors	The total number of 'rpc-reply' messages with 'rpc-error' sent.
out-notifications	The total number of 'notification' messages sent.

Section 5.11

Managing SNMP

The Simple Network Management Protocol (SNMP) is used by network management systems and the devices they manage. It is used to report alarm conditions and other events that occur on the devices it manages.

In addition to SNMPv1 and SNMPv2, ROX II also supports SNMPv3, which offers the following features:

- Provides the ability to send a notification of an event via *traps*. Traps are unacknowledged UDP messages and may be lost in transit.
- Provides the ability to notify via *informs*. Informs simply add acknowledgment to the trap process, resending the trap if it is not acknowledged in a timely fashion.
- Encrypts all data transmitted by scrambling the contents of each packet to prevent it from being seen by an unauthorized source. The AES CFB 128 and DES3 encryption protocols are supported.
- Authenticates all messages to verify they are from a valid source.
- Verifies the integrity of each message by making sure each packet has not been tampered with in-transit.

SNMPv3 also provides security models and security levels. A security model is an authentication strategy that is set up for a user and the group in which the user resides. A security level is a permitted level of security within a security model. A combination of a security model and security level will determine which security mechanism is employed when handling an SNMP packet.

Before configuring SNMP, note the following:

- each user belongs to a group
- a group defines the access policy for a set of users
- an access policy defines what SNMP objects can be accessed for: reading, writing and creating notifications
- a group determines the list of notifications its users can receive
- a group also defines the security model and security level for its users

The following sections describe how to configure and manage SNMP:

- Section 5.11.1, “MIB Files and SNMP Traps”
- Section 5.11.2, “Enabling and Configuring SNMP Sessions”
- Section 5.11.3, “Viewing Statistics for SNMP”
- Section 5.11.4, “Discovering SNMP Engine IDs”

- Section 5.11.5, “Managing SNMP Communities”
- Section 5.11.6, “Managing SNMP Target Addresses”
- Section 5.11.7, “Managing SNMP Users”
- Section 5.11.8, “Managing SNMP Security Model Mapping”
- Section 5.11.9, “Managing SNMP Group Access”

Section 5.11.1

MIB Files and SNMP Traps

The current MIB files supported by ROX II can be downloaded from the www.siemens.com/ruggedcom.

> **NOTE**
> *SNMP traps are not configurable in ROX II.*

The MIB files support the following SNMP traps:

Table: 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

Standard	MIB	Trap and Description
		and transitioned into some other state (but not into the notPresent state). This other state is indicated by the included value of ifOperStatus.
		linkDown A linkDown trap signifies that the SNMP entity, acting in an agent role, has detected that the ifOperStatus object for one of its communication links is about to enter the down state from some other state (but not from the notPresent state). This other state is indicated by the included value of ifOperStatus.
RuggedCom	RUGGEDCOM-TRAPS-MIB	**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 5.11.2

Enabling and Configuring SNMP Sessions

To enable and configure SNMP sessions, do the following:

1. Make sure the CLI is in Configuration mode.
2. Configure the following parameter(s) as required:

Parameter	Description
enabled	**Default:** false Provides the ability to configure SNMP features on the device.
listen-ip { listen-ip }	**Synopsis:** The ip-address type represents an IP address and is IP version neutral. The format of the textual representations implies the IP version. **Default:** 0.0.0.0

Parameter	Description
	The IP Address the SNMP agent will listen on for SNMP requests.
port { port }	**Synopsis:** The port-number type represents a 16-bit port number of an Internet transport layer protocol such as UDP, TCP, DCCP, or SCTP. Port numbers are assigned by IANA. A current list of all assignments is available from <http://www.iana.org/>. Note that the port number value zero is reserved by IANA. In situations where the value zero does not make sense, it can be excluded by subtyping the port-number type. In the value set and its semantics, this type is equivalent to the InetPortNumber textual convention of the SMIv2. **Default:** 161 The port the SNMP agent will listen on for SNMP requests.
extra-ip-ports { extra-ip-ports }	**Synopsis:** "extra-ip-ports" occurs in an unbounded array 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.
max-sessions { max-sessions }	**Synopsis:** unbounded **Default:** 30 The maximum number of concurrent SNMP sessions.
snmp-engine-id { snmp-engine-id }	**Synopsis:** A list of colon-separated hexa-decimal octets e.g. '4F:4C:41:71'. The statement tailf:value-length can be used to restrict the number of octets. Note that using the 'length' restriction limits the number of characters in the lexical representation. 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 { source-ip }	**Synopsis:** The ip-address type represents an IP address and is IP version neutral. The format of the textual representations implies the IP version. If set, all traffic/traps originating from this device shall use the configured IP Address for the Source IP.
auth-failure-trap-notify { auth-failure-trap-notify }	**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.
authen-traps-enabled	**Default:** false Enables authentication traps to be sent from the SNMP agent.
dscp { dscp }	**Synopsis:** The dscp type represents a Differentiated Services Code-Point that may be used for marking packets in a traffic stream. In the value set and its semantics, this type is equivalent to the Dscp textual convention of the SMIv2. **Default:** 0 Support for setting the Differentiated Services Code Point (6 bits) for traffic originating from the SNMP agent.

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

Section 5.11.3

Viewing Statistics for SNMP

To view the statistics collected for SNMP, type:

```
show admin snmp statistics
```

If statistics are available, a table or list similar to the following example appears:

```
ruggedcom# show admin snmp statistics
statistics
 unsupported sec levels 1
 not in time windows    1
 unknown user names     1
 unknown engine ids     4
 wrong digests          1
 decryption errors      1
```

This table or list provides the following information:

Parameter	Description
unsupported-sec-levels	**Synopsis:** The counter32 type represents a non-negative integer that monotonically increases until it reaches a maximum value of 2^32-1 (4294967295 decimal), when it wraps around and starts increasing again from zero. Counters have no defined 'initial' value, and thus, a single value of a counter has (in general) no information content. Discontinuities in the monotonically increasing value normally occur at re-initialization of the management system, and at other times as specified in the description of a schema node using this type. If such other times can occur, for example, the creation of a schema node of type counter32 at times other than re-initialization, then a corresponding schema node should be defined, with an appropriate type, to indicate the last discontinuity. The counter32 type should not be used for configuration schema nodes. A default statement SHOULD NOT be used in combination with the type counter32. In the value set and its semantics, this type is equivalent to the Counter32 type of the SMIv2. The total number of packets received by the SNMP engine which were dropped because they requested a securityLevel that was unknown to the SNMP engine or otherwise unavailable.
not-in-time-windows	**Synopsis:** The counter32 type represents a non-negative integer that monotonically increases until it reaches a maximum value of 2^32-1 (4294967295 decimal), when it wraps around and starts increasing again from zero. Counters have no defined 'initial' value, and thus, a single value of a counter has (in general) no information content. Discontinuities in the monotonically increasing value normally occur at re-initialization of the management system, and at other times as specified in the description of a schema node using this type. If such other times can occur, for example, the creation of a schema node of type counter32 at times other than re-initialization, then a corresponding schema node should be defined, with an appropriate type, to indicate the last discontinuity. The counter32 type should not be used for configuration schema nodes. A default statement SHOULD NOT be used in combination with the type counter32. In the value set and its semantics, this type is equivalent to the Counter32 type of the SMIv2. The total number of packets received by the SNMP engine which were dropped because they appeared outside of the authoritative SNMP engine's window.
unknown-user-names	**Synopsis:** The counter32 type represents a non-negative integer that monotonically increases until it reaches a maximum value of 2^32-1 (4294967295 decimal), when it wraps around and starts increasing again from zero. Counters have no defined 'initial' value, and thus, a single value of a counter has (in general) no information content. Discontinuities in the monotonically increasing value normally occur at re-initialization of the management system, and at other times as specified in the description of a schema node using this type. If such other times can occur, for example, the creation of a schema node of type counter32 at times other than re-initialization, then a corresponding schema node should be defined, with an appropriate type, to indicate the last discontinuity. The counter32 type should not be used for configuration schema nodes. A default statement SHOULD NOT be

Parameter	Description
	used in combination with the type counter32. In the value set and its semantics, this type is equivalent to the Counter32 type of the SMIv2. The total number of packets received by the SNMP engine which were dropped because they referenced a user that was not known to the SNMP engine.
unknown-engine-ids	**Synopsis:** The counter32 type represents a non-negative integer that monotonically increases until it reaches a maximum value of 2^32-1 (4294967295 decimal), when it wraps around and starts increasing again from zero. Counters have no defined 'initial' value, and thus, a single value of a counter has (in general) no information content. Discontinuities in the monotonically increasing value normally occur at re-initialization of the management system, and at other times as specified in the description of a schema node using this type. If such other times can occur, for example, the creation of a schema node of type counter32 at times other than re-initialization, then a corresponding schema node should be defined, with an appropriate type, to indicate the last discontinuity. The counter32 type should not be used for configuration schema nodes. A default statement SHOULD NOT be used in combination with the type counter32. In the value set and its semantics, this type is equivalent to the Counter32 type of the SMIv2. The total number of packets received by the SNMP engine which were dropped because they referenced an snmpEngineID that was not known to the SNMP engine.
wrong-digests	**Synopsis:** The counter32 type represents a non-negative integer that monotonically increases until it reaches a maximum value of 2^32-1 (4294967295 decimal), when it wraps around and starts increasing again from zero. Counters have no defined 'initial' value, and thus, a single value of a counter has (in general) no information content. Discontinuities in the monotonically increasing value normally occur at re-initialization of the management system, and at other times as specified in the description of a schema node using this type. If such other times can occur, for example, the creation of a schema node of type counter32 at times other than re-initialization, then a corresponding schema node should be defined, with an appropriate type, to indicate the last discontinuity. The counter32 type should not be used for configuration schema nodes. A default statement SHOULD NOT be used in combination with the type counter32. In the value set and its semantics, this type is equivalent to the Counter32 type of the SMIv2. The total number of packets received by the SNMP engine which were dropped because they did not contain the expected digest value.
decryption-errors	**Synopsis:** The counter32 type represents a non-negative integer that monotonically increases until it reaches a maximum value of 2^32-1 (4294967295 decimal), when it wraps around and starts increasing again from zero. Counters have no defined 'initial' value, and thus, a single value of a counter has (in general) no information content. Discontinuities in the monotonically increasing value normally occur at re-initialization of the management system, and at other times as specified in the description of a schema node using this type. If such other times can occur, for example, the creation of a schema node of type counter32 at times other than re-initialization, then a corresponding schema node should be defined, with an appropriate type, to indicate the last discontinuity. The counter32 type should not be used for configuration schema nodes. A default statement SHOULD NOT be used in combination with the type counter32. In the value set and its semantics, this type is equivalent to the Counter32 type of the SMIv2. The total number of packets received by the SNMP engine which were dropped because they could not be decrypted.

Section 5.11.4

Discovering SNMP Engine IDs

To discover an SNMP engine ID on a device, type:

```
admin snmp snmp-discover
```

Section 5.11.5

Managing SNMP Communities

The following sections describe how to configure and manage SNMP communities:

- Section 5.11.5.1, “Viewing a List of SNMP Communities”
- Section 5.11.5.2, “Adding an SNMP Community”
- Section 5.11.5.3, “Deleting an SNMP Community”

Section 5.11.5.1

Viewing a List of SNMP Communities

To view a list of SNMP communities configured on the device, type:

```
show running-config admin snmp snmp-community name
```

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

```
ruggedcom# show running-config admin snmp snmp-community | tab
COMMUNITY  USER
NAME       NAME
------------------
private    oper
public     guest

 !
!
```

By default, private and public communities are pre-configured. If additional communities are required, add them as needed. For more information, refer to Section 5.11.5.2, “Adding an SNMP Community”.

Section 5.11.5.2

Adding an SNMP Community

To add an SNMP community, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the SNMP community by typing:

   ```
   admin snmp snmp-community name
   ```

   Where:

   - *name* is the name of the community
3. Configure the following parameter(s) as required:

Parameter	Description
{ community-name }	The SNMP community name.
user-name { user-name }	The SNMP community security name.

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

Section 5.11.5.3
Deleting an SNMP Community

To delete an SNMP community, do the following:

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

```
no admin snmp snmp-community name
```

Where:

- *name* is the name of the community

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

Section 5.11.6
Managing SNMP Target Addresses

The following sections describe how to configure and manage SNMP target addresses:

- Section 5.11.6.1, “Viewing a List of SNMP Target Addresses”
- Section 5.11.6.2, “Adding an SNMP Target Address”
- Section 5.11.6.3, “Deleting an SNMP Target Address”

Section 5.11.6.1
Viewing a List of SNMP Target Addresses

To view a list of SNMP target addresses configured on the device, type:

```
show running-config admin snmp snmp-target-address
```

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

```
ruggedcom# show running-config admin snmp snmp-target-address | tab
                             TARGET         TRAP  SECURITY  USER   SECURITY
TARGET NAME          ENABLED  ADDRESS        PORT  MODEL     NAME   LEVEL
--------------------------------------------------------------------------------
127.0.0.1 v1         true     127.0.0.1      162   v1        oper   noAuthNoPriv
127.0.0.1 v2         true     127.0.0.1      162   v2c       oper   noAuthNoPriv
127.0.0.1 v3.guest   true     127.0.0.1      162   v3        admin  noAuthNoPriv
127.0.0.1 v3.inform  true     127.0.0.1      162   v3        admin  authPriv
127.0.0.1 v3.trap    true     127.0.0.1      162   v3        admin  authNoPriv
target               true     192.168.0.111  162   v2c       admin  noAuthNoPriv

 !
!
```

If no SNMP target addresses have been configured, add target addresses as needed. For more information, refer to Section 5.11.6.2, “Adding an SNMP Target Address”.

Section 5.11.6.2

Adding an SNMP Target Address

To add an SNMP target adress, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the SNMP target address by typing:

```
admin snmp snmp-target-address target-name
```

Where:

- *target-name* is a descriptive name for the target (e.g. *Corportate NMS*)

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

Parameter	Description
{ target-name }	A descriptive name for the target (ie. 'Corportate NMS').
enabled	**Default:** true Enables/disables this specific target.
target-address { target-address }	**Synopsis:** The ip-address type represents an IP address and is IP version neutral. The format of the textual representations implies the IP version. An IPv4 or IPv6 address for the remote target.
trap-port { trap-port }	**Synopsis:** The port-number type represents a 16-bit port number of an Internet transport layer protocol such as UDP, TCP, DCCP, or SCTP. Port numbers are assigned by IANA. A current list of all assignments is available from <http://www.iana.org/>. Note that the port number value zero is reserved by IANA. In situations where the value zero does not make sense, it can be excluded by subtyping the port-number type. In the value set and its semantics, this type is equivalent to the InetPortNumber textual convention of the SMIv2. **Default:** 162 The UDP Port for the remote target to receive traps on.
security-model { security-model }	**Synopsis:** v1, v2c, v3 **Default:** v2c The SNMP security model to use: SNMPv1, SNMPv2c, or USM/SNMPv3.
user-name { user-name }	The user name to be used in communications with this target.
security-level { 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 { control-community }	Restricts incoming SNMP requests from the IPv4 or IPv6 address associated with this community.
tag-list { tag-list }	**Default:** snmpv2_trap Selects the type of trap communications to be sent to this target.
inform-timeout { inform-timeout }	**Default:** 6000 The timeout used for reliable inform transmissions (seconds*100).
inform-retries { inform-retries }	**Default:** 3 The number of retries used for reliable inform transmissions.

Parameter	Description
target-engine-id { target-engine-id }	**Synopsis:** A list of colon-separated hexa-decimal octets e.g. '4F:4C:41:71'. The statement tailf:value-length can be used to restrict the number of octets. Note that using the 'length' restriction limits the number of characters in the lexical representation. **Default:** Empty string The target's SNMP local engine ID. This field may be left blank.

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

Section 5.11.6.3
Deleting an SNMP Target Address

To delete an SNMP target address, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the SNMP target address by typing:

```
no admin snmp snmp-target-address target-name
```

Where:

- *`target-name`* is a descriptive name for the target (e.g. *Corportate NMS*)

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

Section 5.11.7
Managing SNMP Users

The following sections describe how to configure and manage SNMP users:

- Section 5.11.7.1, “Viewing a List of SNMP Users”
- Section 5.11.7.2, “Adding an SNMP User”
- Section 5.11.7.3, “Deleting an SNMP User”

Section 5.11.7.1
Viewing a List of SNMP Users

To view a list of SNMP users configured on the device, type:

```
show running-config admin snmp snmp-user
```

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

```
ruggedcom# show running-config admin snmp snmp-user | tab
                                  USER   AUTH
USER ENGINE ID                    NAME   PROTOCOL  AUTH KEY
--------------------------------------------------------------------------------
80:00:3a:9c:03:00:0a:dc:ff:9a:00  oper   sha1      $4$kNxlPIYMx2xJhYYI0d4IDw==
80:00:3a:9c:03:00:0a:dc:ff:9a:00  admin  none      -
80:00:3a:9c:03:00:0a:dc:ff:9a:00  guest  md5       $4$kNxlPIYMx2xJhYYI0d4IDw==

 !
!
```

If no SNMP users have been configured, add users as needed. For more information, refer to Section 5.11.7.2, “Adding an SNMP User”.

Section 5.11.7.2
Adding an SNMP User

To add an SNMP user, do the following:

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

```
admin snmp snmp-user id name
```

   Where:

   - *id* is the ID for the user
   - *name* is the name of the user

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

Parameter	Description
{ user-engine-id }	**Synopsis:** A list of colon-separated hexa-decimal octets e.g. '4F:4C:41:71'. The statement tailf:value-length can be used to restrict the number of octets. Note that using the 'length' restriction limits the number of characters in the lexical representation. 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 }	The user for the SNMP key. Select a user name from the list.
auth-protocol { auth-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.
auth-key { auth-key }	**Synopsis:** The aes-cfb-128-encrypted-string works exactly like des3-cbc-encrypted-string but AES/128bits in CFB mode is used to encrypt the string. The prefix for encrypted values is '4'. A free-text password in the format `$0$<your password>`. passphrase must be minimum 8 characters long
privacy-protocol { 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 { privacy-key }	**Synopsis:** The aes-cfb-128-encrypted-string works exactly like des3-cbc-encrypted-string but AES/128bits in CFB mode is used to encrypt the string. The prefix for encrypted values is '4'. A free-text password in the format `$0$<your password>`. passphrase must be minimum 8 characters long

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

Section 5.11.7.3
Deleting an SNMP User

To delete an SNMP user, do the following:

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

```
no admin snmp snmp-user id name
```

   Where:

   - *id* is the ID for the user
   - *name* is the name of the user

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

Section 5.11.8
Managing SNMP Security Model Mapping

The following sections describe how to configure and manage SNMP security models:

- Section 5.11.8.1, "Viewing a List of SNMP Security Models"
- Section 5.11.8.2, "Adding an SNMP Security Model"
- Section 5.11.8.3, "Deleting an SNMP Security Model"

Section 5.11.8.1
Viewing a List of SNMP Security Models

To view a list of SNMP security models configured on the device, type:

```
show running-config admin snmp snmp-security-to-group
```

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

```
ruggedcom# show running-config admin snmp snmp-security-to-group | tab
SECURITY  USER
MODEL     NAME   GROUP
-----------------------------
v1        oper   all-rights
v1        guest  all-rights
v2c       oper   all-rights
v2c       admin  testgroup
v2c       guest  all-rights
v3        admin  initial

 !
!
```

If no SNMP security models have been configured, add security models as needed. For more information, refer to Section 5.11.8.2, "Adding an SNMP Security Model".

Section 5.11.8.2
Adding an SNMP Security Model

To add an SNMP security model, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the SNMP security model by typing:

```
admin snmp snmp-security-to-group model name
```

   Where:
   - *model* is the security model
   - *name* is the name of the user
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 }	The security name (a ROX user name) for the SNMP group.
group { group }	**Default:** all-rights The name of the SNMP group.

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

Section 5.11.8.3
Deleting an SNMP Security Model

To delete an SNMP security model, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the SNMP security model by typing:

```
no admin snmp snmp-security-to-group model name
```

   Where:
   - *model* is the security model
   - *name* is the name of the user
3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.11.9
Managing SNMP Group Access

The following sections describe how to configure and manage SNMP group access:

- Section 5.11.9.1, “Viewing a List of SNMP Groups”
- Section 5.11.9.2, “Adding an SNMP Group”
- Section 5.11.9.3, “Deleting an SNMP Group”

Section 5.11.9.1
Viewing a List of SNMP Groups

To view a list of SNMP groups configured on the device, type:

```
show running-config admin snmp snmp-access
```

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

```
ruggedcom# show running-config admin snmp snmp-access | tab
            SECURITY  SECURITY      READ VIEW   WRITE VIEW  NOTIFY
GROUP       MODEL     LEVEL         NAME        NAME        VIEW NAME
------------------------------------------------------------------------
initial     any       noAuthNoPriv  all-of-mib  all-of-mib  all-of-mib
initial     any       authNoPriv    all-of-mib  all-of-mib  all-of-mib
initial     any       authPriv      all-of-mib  all-of-mib  all-of-mib
testgroup   v2c       noAuthNoPriv  all-of-mib  all-of-mib  all-of-mib
all-rights  any       noAuthNoPriv  all-of-mib  all-of-mib  all-of-mib

 !
!
```

If no SNMP groups have been configured, add groups as needed. For more information, refer to Section 5.11.9.2, “Adding an SNMP Group”.

Section 5.11.9.2
Adding an SNMP Group

To add an SNMP group, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the SNMP group by typing:

```
admin snmp snmp-access group model level
```

Where:

- *group* is the name of the group
- *model* is the security model for the group
- *level* is the security level for the group

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

Parameter	Description
{ group }	The name of the SNMP group.
{ security-model }	**Synopsis:** any, v1, v2c, v3 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.
read-view-name { read-view-name }	**Synopsis:** no-view, v1-mib, restricted, all-of-mib **Default:** all-of-mib

Parameter	Description
	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 { 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 { 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.

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

Section 5.11.9.3

Deleting an SNMP Group

To delete an SNMP group, do the following:

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

```
no admin snmp snmp-access group model level
```

Where:

- *`group`* is the name of the group
- *`model`* is the security model for the group
- *`level`* is the security level for the group

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

Section 5.12

Managing Time Synchronization Functions

ROX II uses version 4 of the Network Time Protocol (NTP) to synchronize the internal clock with a time source.

> **NOTE**
> *For more information about version 4 of NTP, refer to RFC 5905 [http://tools.ietf.org/html/rfc5905].*

NTP is a fault-tolerant protocol that allows an NTP daemon to automatically select the best of several available reference clocks to synchronize with. Multiple candidates can be combined to minimize the accumulated error. The NTP daemon can also detect and avoid reference clocks that are temporarily or permanently advertising the wrong time.

The NTP daemon achieves synchronization by making small and frequent changes to the internal clock. It operates in a *client-server* mode, which allows it to synchronize the internal clock with NTP servers and act as an NTP server for peer devices.

If multiple NTP servers are available to choose from, the NTP daemon will synchronize with the server that has the lowest stratum. The stratum is a rating of the server compared to the server with the reference clock. The reference clock itself appears at stratum 0. A server synchronized with a stratum *n* server will be running at stratum *n+1*.

NTP hosts with a lower stratum are typically configured as NTP servers, while NTP hosts with higher stratums are configured at the same stratum as their peers. If each NTP server fails, a configured peer will help in providing the NTP time. It is recommended that at least one server and one peer be configured.

The NTP daemon knows which NTP servers and peers to use in three ways:

- The daemon is configured manually with list of servers to poll
- The daemon is configured manually with a list of peers to send to
- NTP servers issue advertisements to the daemon on broadcast or multicast address

NOTE
If a firewall is enabled, make sure UDP port 123 is open to send (if the router is an NTP client) or receive (if the router is an NTP server).

NTP uses UDP/IP packets for data transfer, as UDP offers fast connections and response times, and transfers them through UDP port 123.

The following sections describe how to configure and manage time synchronization functions:

- Section 5.12.1, “Configuring the Time Synchronization Settings”
- Section 5.12.2, “Configuring the System Time and Date”
- Section 5.12.3, “Configuring the System Time Zone”
- Section 5.12.4, “Configuring the Local Time Settings”
- Section 5.12.5, “Configuring NTP Multicast Clients”
- Section 5.12.6, “Configuring NTP Broadcast Clients”
- Section 5.12.7, “Enabling/Disabling the NTP Service”
- Section 5.12.8, “Viewing the NTP Service Status”
- Section 5.12.9, “Viewing the Status of Reference Clocks”
- Section 5.12.10, “Monitoring Subscribers”
- Section 5.12.11, “Managing NTP Servers”
- Section 5.12.12, “Managing NTP Broadcast/Multicast Addresses”
- Section 5.12.13, “Managing Server Keys”
- Section 5.12.14, “Managing Server Restrictions”

Section 5.12.1

Configuring the Time Synchronization Settings

To configure the time synchronization settings, do the following:

1. Configure the system time and date. For more information, refer to Section 5.12.2, “Configuring the System Time and Date”.
2. Configure the system time zone. For more information, refer to Section 5.12.3, “Configuring the System Time Zone”.

3. Configure the local time settings. For more information, refer to Section 5.12.4, “Configuring the Local Time Settings”.
4. If multicast addresses will be configured for the NTP server, configure the NTP multicast client. For more information, refer to Section 5.12.5, “Configuring NTP Multicast Clients”.
5. If broadcast addresses will be configured for the NTP server, configure the NTP broadcast client. For more information, refer to Section 5.12.6, “Configuring NTP Broadcast Clients”.
6. Add remote NTP servers. For more information, refer to Section 5.12.11.2, “Adding an NTP Server”.
7. Add broadcast/mutlicast addresses for the NTP server. For more information, refer to Section 5.12.12.2, “Adding a Broadcast/Multicast Address”.
8. If required, add server authentication keys. For more information, refer to Section 5.12.13.2, “Adding a Server Key”.
9. Add restrictions for the remote NTP servers. For more information, refer to Section 5.12.14.2, “Adding a Server Restriction”.
10. Enable the NTP service. For more information, refer to Section 5.12.7, “Enabling/Disabling the NTP Service”.
11. View the status of the NTP service. For more information, refer to Section 5.12.8, “Viewing the NTP Service Status”.

Section 5.12.2
Configuring the System Time and Date

To configure the system time and date, do the following:

1. Make sure the CLI is in Configuration mode.
2. Set the system time and date by typing:

```
admin set-system-clock time time-date
```

   Where:

   - *time-date* is the date time in the format YYYY-MM-DD HH:MM:SS

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

Section 5.12.3
Configuring the System Time Zone

To configure the system time zone, do the following:

1. Make sure the CLI is in Configuration mode.
2. Set the system time zone by typing:

   > **NOTE**
   > *The Etc/GMT time zones conform to the POSIX style and have their signs reversed from common usage. In POSIX style, zones west of Greenwich Mean Time (GMT) have a positive sign, while zones east of GMT have a negative sign.*

```
admin timezone category category zone zone
```

   Where:

- *category* is the time zone category
- *zone* is the time zone

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

Section 5.12.4

Configuring the Local Time Settings

The local time settings configure the local clock on the device as the NTP time source.

To configure the local NTP time settings, do the following:

1. Make sure the CLI is in Configuration mode.
2. Enable and configure the local NTP time settings by typing:

```
services ntp local-clock enable stratum number
```

Where:

- *number* is the stratum number of the local clock

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

Section 5.12.5

Configuring NTP Multicast Clients

The NTP multicast client enables the NTP server to receive advertisements from other NTP servers.

To configure the NTP multicast client, do the following:

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

Parameter	Description
enabled	Enables the multicast message mode.
address { address }	**Synopsis:** The host type represents either an IP address or a DNS domain name. **Default:** 224.0.1.1 The multicast address on which the NTP client listens for NTP messages.

3. Add a multicast address for a known NTP server. For more information, refer to Section 5.12.12.2, “Adding a Broadcast/Multicast Address”.
4. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.12.6

Configuring NTP Broadcast Clients

The NTP broadcast client enables the NTP server to receive advertisements from other NTP servers and send advertisements of its own.

To configure the NTP broadcast client, do the following:

1. Make sure the CLI is in Configuration mode.
2. Enable NTP broadcast clients by typing:

```
services ntp broadcastclient enable
```

3. Add a broadcast address for a known NTP server. For more information, refer to Section 5.12.12.2, "Adding a Broadcast/Multicast Address".
4. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.12.7
Enabling/Disabling the NTP Service

To enable/disable the NTP service, do the following:

1. Make sure the CLI is in Configuration mode.
2. Enable the NTP service by typing:

```
services ntp enable
```

Disable the NTP service by typing:

```
no services ntp enable
```

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

Section 5.12.8
Viewing the NTP Service Status

To view the status of the NTP service, do the following:

1. Make sure the NTP service is enabled. For more information, refer to Section 5.12.7, "Enabling/Disabling the NTP Service".
2. Display the NTP service status by typing:

```
services ntp ntp-status
```

A table similar to the following example appears:

```
ruggedcom# services ntp ntp-status
 ntp-status
   remote           refid      st t when poll reach   delay   offset  jitter
 ==============================================================================
 *142.3.100.2     .GPS.            1 u  937 1024  377   38.104   -0.273   0.802
  172.30.149.45   .INIT.          16 u    - 1024    0    0.000    0.000   0.000
 +206.186.255.226 128.138.140.44   2 u  413 1024  377   58.578    0.143  27.963
 x206.186.255.227 CHU_AUDIO(1)     3 u  927 1024  377   58.034  10846.0  30.289
 +209.87.233.53   209.87.233.52    2 u  449 1024  377   27.060   -1.132   3.153
```

This table provides the following information:

Parameter	Description
ntp-status	Use this action to get the current NTP running status.

A character before an address is referred to as a tally code. Tally codes indicate the fate of the peer in the clock selection process. The following describes the meaning of each tally code:

Tally Code	Description
blank	A blank tally code indicates the peer has been discarded either because it is unreachable, it is synchronized to the same server (synch loop) or the synchronization distance is too far.
x	This tally code indicates the peer has been discarded because its clock is not correct. This is referred to as a *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 5.12.9

Viewing the Status of Reference Clocks

To view the status of reference clocks, type:

```
show services ntp status
```

A table similar to the following example appears:

```
ruggedcom# show services ntp status reference-clock
                                   REFERENCE           ADDRESS
ADDRESS           STATE            ID         STRATUM  TYPE     WHEN  POLL  REACH  DELAY  OFFSET
 JITTER
-----------------------------------------------------------------------------------------------------------
127.127.1.0       System peer      .LOCL.     10       1        2     64    377    0.000  0.000   0.000
206.186.255.227   Not synchronized .INIT.     16       -        -     1024  0      0.000  0.000   0.000
206.186.255.226   Not synchronized .INIT.     16       -        -     1024  0      0.000  0.000   0.000
142.3.100.2       Not synchronized .INIT.     16       -        -     1024  0      0.000  0.000   0.000
```

This table provides the following information:

Parameter	Description
address	The IP address of the reference clock.
state	The state of the clock.
reference-id	The identification of the reference clock.
stratum	The stratum number of the reference clock.
address-type	The address type of the remote machine.
when	The number of seconds since the last poll of the reference clock.
poll	The polling interval in seconds.

Parameter	Description
reach	An 8-bit left-rotating register. Any 1 bit means that a time packet was received.
delay	The time delay (in milliseconds) to communicate with the reference clock.
offset	The offset (in milliseconds) between our time and that of the reference clock.
jitter	The observed jitter (in milliseconds).

Section 5.12.10

Monitoring Subscribers

ROX II monitors the subscriptions of up to 600 hosts (e.g. clients, servers and peers) that are connected to the NTP server.

To view the list of subscriber hosts, type:

```
show services ntp status monitor-list
```

If hosts are detected, a table or list similar to the following example appears:

```
ruggedcom# show services ntp status monitor-list | tab
                     AVERAGE   LAST
 REMOTE        PORT  COUNT  MODE  VERSION  RESTRICT                             INTERVAL  INTERVAL
 ---------------------------------------------------------------------------------------------------
 192.168.0.1   123   2      3     4        [ nomodify nopeer noquery notrap ]   447       887
 192.168.0.2   123   1      3     4        [ nomodify nopeer noquery notrap ]   885       885
 192.168.0.3   123   1      3     4        [ nomodify nopeer noquery notrap ]   883       883
 192.168.0.4   123   1      3     4        [ nomodify nopeer noquery notrap ]   881       881
 192.168.1.1   123   1      3     4        [ nomodify nopeer noquery notrap ]   862       862
 192.168.1.3   123   1      3     4        [ nomodify nopeer noquery notrap ]   854       854
 192.168.1.8   123   1      3     4        [ nomodify nopeer noquery notrap ]   850       850
 192.168.2.1   123   1      4     4        [ nomodify nopeer noquery notrap ]   837       837
 192.168.2.4   123   1      4     4        [ nomodify nopeer noquery notrap ]   834       834
 192.168.2.10  123   1      4     4        [ nomodify nopeer noquery notrap ]   830       830
 192.168.3.3   123   1      1     4        [ nomodify nopeer noquery notrap ]   823       823
 192.168.3.7   123   1      1     4        [ nomodify nopeer noquery notrap ]   816       816
 192.168.3.9   123   1      1     4        [ nomodify nopeer noquery notrap ]   813       813
```

The table/list provides the following information:

Parameter	Description
remote	Remote address.
port	UDP port number.
count	Number of packets received.
mode	Mode of last packet.
version	Version of last packet.
restrict	**Synopsis:** ignore, kod, limited, lowpriotrap, nomodify, nopeer, noquery, noserve, notrap, notrust, ntpport, version **Synopsis:** "restrict" occurs in an unbounded array Restrict flags.
average-interval	Average interval (in seconds) between packets from this address.

Parameter	Description
last-interval	Interval (in seconds) between the receipt of the most recent packet from this address and the completion of the retrieval of the status.

Section 5.12.11

Managing NTP Servers

ROX II can periodically refer to a remote NTP server to correct any accumulated drift in the onboard clock. ROX II can also serve time via SNTP (Simple Network Time Protocol) to hosts that request it.

NTP servers can be added with or without authentication keys. To associate an authentication key with an NTP server, first define a server key. For information about adding server keys, refer to Section 5.12.13.2, “Adding a Server Key”.

The following sections describe how to configure and manage NTP servers:

- Section 5.12.11.1, “Viewing a List of NTP Servers”
- Section 5.12.11.2, “Adding an NTP Server”
- Section 5.12.11.3, “Deleting an NTP Server”

Section 5.12.11.1

Viewing a List of NTP Servers

To view a list of NTP servers configured on the device, type:

```
show running-config services ntp server
```

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

```
ruggedcom# show running-config services ntp server | tab
                                                          NTP
NAME              ENABLED  PEER  MINPOLL  MAXPOLL  IBURST  VERSION  PREFER  KEY
--------------------------------------------------------------------------------
142.3.100.2       X        -     6        10       -       -        X       -
206.186.255.226   X        -     6        10       -       -        -       -
206.186.255.227   X        -     6        10       -       -        -       -

!
!
```

If no servers have been configured, add servers as needed. For more information, refer to Section 5.12.11.2, “Adding an NTP Server”.

Section 5.12.11.2

Adding an NTP Server

To configure an NTP server on the device, do the following:

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

Parameter	Description
{ name }	**Synopsis:** The host type represents either an IP address or a DNS domain name. The Internet address of the remote NTP server to be monitored.
enabled	Turns on the NTP interface to this server.
peer	Allows you to enter and edit peers. Peers are NTP servers of the same stratum as the router, and are useful when contact is lost with the hosts in the NTP servers menu.
minpoll { minpoll }	**Default:** 6 **Prerequisite:** minpoll must be less than or equal to maxpoll The minimum poll interval for NTP messages, in seconds as a power of two.
maxpoll { maxpoll }	**Default:** 10 **Prerequisite:** minpoll must be less than or equal to maxpoll The maximum poll interval for NTP messages, in seconds as a power of two.
iburst	When the server is unreachable and at each poll interval, a burst of eight packets is sent instead of one.
ntp-version { ntp-version }	The version of the NTP protocol used to communicate with this host. Change this only if it is known that the host requires a version other than 4.
prefer	Marks this server as preferred.
key { key }	An authentication key associated with this host.

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

Section 5.12.11.3
Deleting an NTP Server

To delete an NTP server configured on the device, do the following:

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

```
no services ntp server IP Address
```

Where:

- *IP Address* is the internal address of the remote NTP server.

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

Section 5.12.12
Managing NTP Broadcast/Multicast Addresses

When broadcast or multicast addresses for known NTP servers are configured, the NTP daemon monitors advertisements from each address and chooses the server with the lowest stratum to use as the NTP host. This is opposed to manually configuring a list of servers or peers.

The following sections describe how to configure and manage broadcast and multicast addresses for an NTP server:

- Section 5.12.12.1, “Viewing a List of Broadcast/Multicast Addresses”

- Section 5.12.12.2, “Adding a Broadcast/Multicast Address”
- Section 5.12.12.3, “Deleting a Broadcast/Multicast Address”

Section 5.12.12.1
Viewing a List of Broadcast/Multicast Addresses

To view a list of broadcast/multicast addresses, type:

```
show running-config services ntp broadcast
```

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

```
ruggedcom# show running-config services ntp broadcast
services
 ntp
  broadcast 224.0.0.1
   no enabled
   key 1
   no ntp-version
  !
 !
!
```

If no broadcast/multicast addresses have been configured, add addresses as needed. For more information, refer to Section 5.12.12.2, “Adding a Broadcast/Multicast Address”.

Section 5.12.12.2
Adding a Broadcast/Multicast Address

To add a broadcast/multicast address for an NTP server, do the following:

> **IMPORTANT!**
> *It is strongly recommended to enable NTP authentication, unless all hosts on the network are trusted.*

1. Make sure a server key has been configured with the broadcast/multicast setting to enable NTP authentication. For more information, refer to Section 5.12.13.2, “Adding a Server Key”.
2. Make sure the CLI is in Configuration mode.
3. Add the address by typing:

   > **IMPORTANT!**
   > *The broadcast/multicast address must be the same as the address for the NTP multicast client.*

   ```
   services ntp broadcast address
   ```

   Where:

   - *address* is the broadcast or multicast address
4. Configure the following parameter(s) as required:

Parameter	Description
enabled	Enables sending broadcast or multicast NTP messages to this address.

Parameter	Description
key { key }	Authentication key.
ntp-version { ntp-version }	The version of the NTP protocol used to communicate with this host. Change this only if it is known that the host requires a version other than 4.
ttl { ttl }	**Default:** 1 Time to live.

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

Section 5.12.12.3
Deleting a Broadcast/Multicast Address

To delete a broadcast/multicast address for an NTP server, do the following:

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

```
no services ntp broadcast address
```

   Where:

   • *address* is the broadcast or multicast address

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

Section 5.12.13
Managing Server Keys

Server keys are used to authenticate NTP communications and prevent tampering with NTP timestamps. When using authentication, both the local and remote servers must share the same key and key identifier. Packets sent to and received from the server/peer include authentication fields encrpyted using the key.

The following sections describe how to configure and manage server keys:

• Section 5.12.13.1, “Viewing a List of Server Keys”
• Section 5.12.13.2, “Adding a Server Key”
• Section 5.12.13.3, “Deleting a Server Key”

Section 5.12.13.1
Viewing a List of Server Keys

To view a list of server keys, type:

```
show running-config services ntp key
```

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

```
ruggedcom# show running-config services ntp key
services
 ntp
  key 1
```

```
    value   $4$87sRT/Z+sxs9hYYI0d4IDw==
    trusted
   !
  !
 !
```

If no server keys have been configured, add keys as needed. For more information, refer to Section 5.12.13.2, "Adding a Server Key".

Section 5.12.13.2

Adding a Server Key

To add a server key, do the following:

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

```
services ntp key id
```

   Where:

   - *id* is the ID assigned to the key
3. Configure the following parameter(s) as required:

Parameter	Description
value { value }	**Synopsis:** The aes-cfb-128-encrypted-string works exactly like des3-cbc-encrypted-string but AES/128bits in CFB mode is used to encrypt the string. The prefix for encrypted values is '4'. The key.
trusted	Mark this key as trusted for the purposes of authenticating peers with symmetric key cryptography. The authentication procedures require that both the local and remote servers share the same key and key identifier.

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

Section 5.12.13.3

Deleting a Server Key

To delete a server key, do the following:

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

```
no services ntp key id
```

   Where:

   - *id* is the ID assigned to the key
3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.12.14
Managing Server Restrictions

Server restrictions control access to the NTP servers.

The following sections describe how to configure and manage NTP server restrictions:

- Section 5.12.14.1, "Viewing a List of Server Restrictions"
- Section 5.12.14.2, "Adding a Server Restriction"
- Section 5.12.14.3, "Deleting a Server Restriction"

Section 5.12.14.1
Viewing a List of Server Restrictions

To view a list of NTP server restrictions, type:

```
show running-config services ntp restrict
```

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

```
ruggedcom# show running-config services ntp restrict | tab
NAME       MASK     FLAGS
---------------------------
127.0.0.1  default  -

 !
!
```

If no server restrictions have been configured, add restrictions as needed. For more information, refer to Section 5.12.14.2, "Adding a Server Restriction".

Section 5.12.14.2
Adding a Server Restriction

To add an NTP server restriction, do the following:

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

   ```
   services ntp restrict address mask
   ```

   Where:

   - *address* is the IP address to match. The address can be a host or network IP address, or a valid host DNS name.
   - *mask* is the mask used to match the address. A value of 255.255.255.255 indicates the address is treated as the address of an individual host.
3. Configure the following parameter(s) as required:

   CAUTION!
   Security hazard – risk of unauthorized access and/or exploitation. It is recommended to restrict queries via ntpdc and ntpq, unless the queries come from a localhost, or to disable this feature entirely if not required. This prevents DDoS (Distributed Denial of Service) reflection/amplification

attacks. To set this restriction, configure the following flags: `kod`, `nomodify`, `nopeer`, `noquery` *and* `notrap`.

Parameter	Description
flags { flags }	**Synopsis:** ignore, kod, limited, lowpriotrap, nomodify, nopeer, noquery, noserve, notrap, notrust, ntpport, version **Synopsis:** "flags" occurs in an unbounded array Flags restrict access to NTP services. An entry with no flags allows free access to the NTP server. • Version: Denies packets that do not match the current NTP version. • ntpport: Matches only if the source port in the packet is the standard NTP UDP port (123). • notrust: Denies service unless the packet is cryptographically authenticated. • notrap: Declines to to provide mode 6 control message trap service to matching hosts. • noserve: Denies all packets except ntpq(8) and ntpdc(8) queries. • noquery: Denies ntpq(8) and ntpdc(8) queries. • nopeer: Denies packets which result in mobilizing a new association. • nomodify: Denies ntpq(8) and ntpdc(8) queries attempting to modify the state of the server; queries returning information are permitted. • lowpriotrap: Declares traps set by matching hosts to be low priority. • limited: Denies service if the packet spacing violates the lower limits specified in the NTP discard setting. • kod: Sends a Kiss-o'-Death (KoD) packet when an access violation occurs. • ignore: Denies all packets.

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

Section 5.12.14.3
Deleting a Server Restriction

To delete an NTP server restriction, do the following:

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

```
no services ntp restrict address mask
```

Where:

- *address* is the IP address to match. The address can be a host or network IP address, or a valid host DNS name.
- *mask* is the mask used to match the address. A value of 255.255.255.255 indicates the address is treated as the address of an individual host.

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

Section 5.13
Managing Cellular Modem Profiles

The following sections describe how to configure and manage cellular modem profiles:

- Section 5.13.1, “Managing CDMA Profiles”

- Section 5.13.2, “Managing GSM Profiles”

Section 5.13.1
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 3.22.5, “Viewing the CDMA Network Status for Cellular Modems”.

The following sections describe how to configure and manage CDMA profiles:

- Section 5.13.1.1, “Viewing a List of CDMA Profiles”
- Section 5.13.1.2, “Adding a CDMA Profile”
- Section 5.13.1.3, “Deleting a CDMA Profile”

Section 5.13.1.1
Viewing a List of CDMA Profiles

To view a list of CDMA profiles, type:

```
show running-config global cellular profiles cdma
```

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

```
ruggedcom# show running-config global cellular profiles cdma | tab
                USE                        DIAL     DISCONNECT   FAILOVER
          DIAL  PEER                       ON       IDLE         ON
NAME      STRING DNS   USERNAME  PASSWORD  DEMAND   TIMEOUT      DEMAND    MTU
--------------------------------------------------------------------------------
gsm-cdma  #777    -     N/A       N/A       -        0            -         1500

!
```

If no CDMA profiles have been configured, add profiles as needed. For more information, refer to Section 5.13.1.2, “Adding a CDMA Profile”.

Section 5.13.1.2
Adding a CDMA Profile

To add a CDMA profile for the celullar modem interface, do the following:

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

   ```
   global cellular profiles cdma name
   ```

   Where:

   - *name* is the name of the profile
3. Configure the cellular network by typing the following commands:

Parameter	Description
dial-string { dial-string }	**Default:** #777 The dial string to connect to the wireless provider.

4. Configure the CDMA PPP settings by typing the following commands:

Parameter	Description
use-peer-dns	Enables the DNS server entries that the PPP server recommends. Enables this option unless you provide your own name servers.
username { username }	**Default:** N/A The user ID to connect to the remote server.
password { password }	**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. **Prerequisite:** If dial-on-demand is configured, Failover on Demand cannot be configured.
disconnect-idle-timeout { disconnect-idle-timeout }	**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. **Prerequisite:** If link failover on-demand is configured, Dial on Demand cannot be configured.
mtu { mtu }	**Default:** 1500 MTU (Maximum Transmission Unit) value on a PPP interface.

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

Section 5.13.1.3

Deleting a CDMA Profile

To delete a CDMA Profile, do the following:

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

```
no global cellular profiles cdma name
```

   Where:

   - *`name`* is the name of the profile

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

Section 5.13.2

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 3.22.4, "Viewing the HSPA Network Status for Cellular Modems".

The following sections describe how to configure and manage GSM profiles:

- Section 5.13.2.1, "Viewing a List of GSM Profiles"
- Section 5.13.2.2, "Adding a GSM Profile"
- Section 5.13.2.3, "Deleting a GSM Profile"

Section 5.13.2.1

Viewing a List of GSM Profiles

To view a list of GSM profiles, type:

```
show running-config global cellular profiles gsm
```

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

```
ruggedcom# show running-config global cellular profiles gsm | tab
                            USE                    DIAL    DISCONNECT  FAILOVER
                    DIAL    PEER                   ON      IDLE        ON
NAME      APN     STRING    DNS   USERNAME  PASSWORD  DEMAND  TIMEOUT     DEMAND    MTU
------------------------------------------------------------------------------------------
hspa-gsm  Rogers  *99***1#  -     N/A       N/A       -       0           -         1500

!
```

If no GSM profiles have been configured, add profiles as needed. For more information, refer to Section 5.13.2.2, "Adding a GSM Profile".

Section 5.13.2.2

Adding a GSM Profile

To add a GSM profile for the celullar modem interface, do the following:

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

   ```
   global cellular profiles gsm name
   ```

   Where:

   - *name* is the name of the profile
3. Configure the cellular network by typing the following commands:

Parameter	Description
apn { apn }	The name of the wireless network access point.
dial-string { dial-string }	**Default:** *99***1# The dial string given by the wireless provider to connect to the access point name.

Parameter	Description
sim { sim }	**Default:** 1 Specify SIM index to be used by this profile

4. Configure the GSM PPP settings by typing the following commands:

Parameter	Description
use-peer-dns	Enables the DNS server entries that the PPP server recommends. Enables this option unless you provide your own name servers.
username { username }	**Default:** N/A The user ID to connect to the remote server.
password { password }	**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. **Prerequisite:** If dial-on-demand is configured, Failover on Demand cannot be configured.
disconnect-idle-timeout { disconnect-idle-timeout }	**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. **Prerequisite:** If link failover on-demand is configured, Dial on Demand cannot be configured.
mtu { mtu }	**Default:** 1500 MTU (Maximum Transmission Unit) value on a PPP interface.

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

Section 5.13.2.3
Deleting a GSM Profile

To delete a GSM Profile, do the following:

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

```
no global cellular profiles gsm name
```

Where:

- *name* is the name of the profile

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

Section 5.14

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 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.

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, ROX II forwards the request to each of the configured DHCP servers. When a reply is received from a server, ROX II forwards the reply back to the originating client.

> **NOTE**
> *While DHCP Relay and DHCP Server may both be configured to run concurrently, they may not be configured to run on the same network interface.*

To configure the DHCP relay agent, do the following:

- Section 5.14.1, "Configuring the DHCP Relay Agent"
- Section 5.14.2, "Viewing a List of DHCP Client Ports"
- Section 5.14.3, "Adding DHCP Client Ports"
- Section 5.14.4, "Deleting a DHCP Client Port"

Section 5.14.1

Configuring the DHCP Relay Agent

To configure the DHCP relay agent, do the following:

1. Make sure the CLI is in Configuration mode.
2. Configure the following parameter(s) as required:

Parameter	Description
dhcp-server-address { dhcp-server-address }	**Synopsis:** The ipv4-address type represents an IPv4 address in dotted-quad notation. The IPv4 address may include a zone index, separated by a % sign. The zone index is used to disambiguate identical address values. For link-local addresses, the zone index will typically be the interface index number or the name of an interface. If the zone index is not present, the default zone of the device will be used. The canonical format for the zone index is the numerical format The IP address of the DHCP server to which DHCP queries will be forwarded from this relay agent.

3. Add client ports. For more information, refer to Section 5.14.3, “Adding DHCP Client Ports”.
4. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.14.2
Viewing a List of DHCP Client Ports

To view a list of DHCP relay agent client ports, type:

```
show running-config switch dhcp-relay-agent dhcp-client-ports
```

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

```
ruggedcom# show running-config switch dhcp-relay-agent dhcp-client-ports
switch dhcp-relay-agent
 dhcp-client-ports lm1 1
 !
!
```

If no client ports have been configured, add client ports as needed. For more information, refer to Section 5.14.3, “Adding DHCP Client Ports”.

Section 5.14.3
Adding DHCP Client Ports

To add a client port for the DHCP relay agent, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the client port by typing:

   ```
   switch dhcp-relay-agent  dhcp-client-ports slot port
   ```

   Where:

   - *slot* is the name of the module location.
   - *port* is the port number (or a list of ports, if aggregated in a port trunk) for the module.
3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.14.4
Deleting a DHCP Client Port

To delete a client port for the DHCP relay agent, do the following:

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

```
no switch dhcp-relay-agent  dhcp-client-ports slot port
```

   Where:

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

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

Section 5.15
Managing the DHCP Server

Dynamic Host Configuration Protocol (DHCP) is a method for centrally and consistently managing IP addresses and settings for clients, offering a variety of assignment methods. IP addresses can be assigned based on the Ethernet MAC address of a client either sequentially or by using port identification provided by a DHCP relay agent device.

The information that is assigned to addresses in DHCP is organized to deal with clients at the interface, subnet, pool, shared network, host-group and host levels.

The following sections describe how to configure and manage the DHCP server:

- Section 5.15.1, “Configuring the DHCP Server”
- Section 5.15.2, “Enabling/Disabling the DHCP Server”
- Section 5.15.3, “Enabling/Disabling the DHCP Relay Support”
- Section 5.15.4, “Viewing a List of Active Leases”
- Section 5.15.5, “Managing DHCP Listen Interfaces”
- Section 5.15.6, “Managing Shared Networks”
- Section 5.15.7, “Managing Subnets”
- Section 5.15.8, “Managing Custom Client Options for Subnets”
- Section 5.15.9, “Managing Hosts”
- Section 5.15.10, “Managing Custom Host Client Configurations”
- Section 5.15.11, “Managing Host Groups”
- Section 5.15.12, “Managing Custom Host Group Client Configurations”
- Section 5.15.13, “Managing IP Pools”
- Section 5.15.14, “Managing IP Ranges for Subnets”
- Section 5.15.15, “Managing IP Ranges for IP Pools”
- Section 5.15.16, “Managing Option 82 Classes for IP Pools”

Section 5.15.1
Configuring the DHCP Server

To configure the DHCP server, do the following:

1. Enable the DHCP Server. For more information, refer to Section 5.15.2, "Enabling/Disabling the DHCP Server".
2. Add and configure DHCP listen interfaces. For more information, refer to Section 5.15.5.2, "Adding a DHCP Listen Interface".
3. Add and configure shared networks. For more information, refer to Section 5.15.6.2, "Adding a Shared Network".

> **NOTE**
> *At least one shared network must be available before a subnet is added.*

4. Add and configure subnets. For more information, refer to Section 5.15.7.2, "Adding a Subnet".
5. Add and configure hosts. For more information, refer to Section 5.15.9.2, "Adding a Host".
6. Add and configure host-groups. For more information, refer to Section 5.15.11.2, "Adding a Host Group".

Section 5.15.2
Enabling/Disabling the DHCP Server

To enable or disable the DHCP server, do the following:

1. Make sure the CLI is in Configuration mode.
2. Enable or disable the DHCP server by typing:

```
services dhcpserver enabled
```

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

Section 5.15.3
Enabling/Disabling the DHCP Relay Support

If DHCP relay (or Option 82) clients are used on the same subnet as the DHCP server, some clients will try to renew a lease immediately after receiving it by requesting a renewal directly from the DHCP server. Because the DHCP server is configured by default to only provide the lease through a relay agent configured with the current Option 82 fields, the server sends the client a NAK protocol message to disallow the lease. Enabling Option 82 disables the NAK protocol message so that the renewal request sent from the DHCP relay agent (which the DHCP server accepts since it has the correct Option 82 fields added) is the only message for which the client receives a reply.

> **NOTE**
> *Option 82 support should only be enabled If the DHCP server and clients are on the same subnet.*

NOTE
The meaning of most Option 82 fields is determined by the DHCP relay client. To determine which values are required by the client for special options, refer to the client documentation.

NOTE
DHCP relay support can also be enabled on an individual subnet. For more information, refer to *Section 5.15.7.3, "Configuring Subnet Options".*

To enable or disable DHCP relay support on the DHCP server, do the following:

1. Make sure the CLI is in Configuration mode.
2. Enable or disable DHCP relay support by typing:

```
services dhcpserver options option82
```

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

Section 5.15.4
Viewing a List of Active Leases

ROX II can generate a list of active leases. The list includes the start and end times, hardware Ethernet address, and client hostname for each lease.

To view a list of active leases, do the following:

```
services dhcpserver show-active-leases
```

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

```
ruggedcom# services dhcpserver show-active-leases
dhcpActionResult
lease 192.168.0.9 {
  starts 2 2012/11/13 20:35:47;
  ends 2 2012/11/13 20:45:47;
  hardware Ethernet 00:01:c0:0c:8b:a4;
  client-hostname "ape2-PC";
}

lease 192.168.0.11 {
  starts 2 2012/11/13 20:38:37;
  ends 2 2012/11/13 20:48:37;
  hardware Ethernet 00:01:c0:0b:b7:70;
}

lease 192.168.0.8 {
  starts 2 2012/11/13 20:38:47;
  ends 2 2012/11/13 20:48:47;
  hardware Ethernet 00:01:c0:0c:8b:a3;
  client-hostname "ape2-PC";
}

lease 192.168.0.22 {
  starts 2 2012/11/13 20:36:14;
  ends 2 2012/11/13 20:46:14;
  hardware Ethernet 00:01:c0:0b:b7:71;
}
```

Section 5.15.5

Managing DHCP Listen Interfaces

DHCP listen interfaces specify the IP interface to which the client sends a request.

The following sections describe how to manage DHCP listen interfaces:

- Section 5.15.5.1, "Viewing a List of DHCP Listen Interfaces"
- Section 5.15.5.2, "Adding a DHCP Listen Interface"
- Section 5.15.5.3, "Deleting a DHCP Listen Interface"

Section 5.15.5.1

Viewing a List of DHCP Listen Interfaces

To view a list of DHCP listen interfaces, type:

```
show running-config services dhcpserver interface
```

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

```
ruggedcom# show running-config services dhcpserver interface | tab
NAME
-------------
switch.0001

 !
!
```

If no DHCP listen interfaces have been configured, add interfaces as needed. For more information, refer to Section 5.15.5.2, "Adding a DHCP Listen Interface".

Section 5.15.5.2

Adding a DHCP Listen Interface

To add a DHCP listen interface, do the following:

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

   ```
   services dhcpserver interface name
   ```

   Where:

   - *name* is the name of the interface
3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.15.5.3

Deleting a DHCP Listen Interface

To delete a DHCP listen interface, do the following:

1. Make sure the CLI is in Configuration mode.

2. Delete the interface by typing:

```
no services dhcpserver interface name
```

Where:

- *name* is the name of the interface

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

Section 5.15.6

Managing Shared Networks

Shared networks are used when multiple subnets should be served by a single physical port. This applies both when using a DHCP relay agent connected to the port with additional subnets behind the relay agent, or when multiple virtual networks exist on one physical interface. Each subnet then gets its own subnet definition inside the shared network rather than at the top level. Shared networks contain subnets, groups and hosts.

The following sections describe how to configure and manage shared networks on a DHCP server:

- Section 5.15.6.1, “Viewing a List of Shared Networks”
- Section 5.15.6.2, “Adding a Shared Network”
- Section 5.15.6.3, “Configuring Shared Network Options”
- Section 5.15.6.4, “Configuring a Shared Network Client”
- Section 5.15.6.5, “Customizing Shared Network Clients”
- Section 5.15.6.6, “Deleting a Shared Network”

Section 5.15.6.1

Viewing a List of Shared Networks

To view a list of shared networks, type:

```
show running-config services dhcpserver shared-network
```

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

```
ruggedcom# show running-config services dhcpserver shared-network
services
 dhcpserver
  shared-network Shared
   options client
    no hostname
    no subnetmask
    no default-route
    no broadcast
    no domain
    no dns-server
    no static-route
    no nis server
    no nis domain
   !
  !
 !
!
```

If no shared networks have been configured, add shared networks as needed. For more information, refer to Section 5.15.6.2, “Adding a Shared Network”.

Section 5.15.6.2
Adding a Shared Network

To add a shared network to the DHCP server, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the shared network by typing:

```
services dhcpserver shared-network name
```

   Where:

   - *name* is the name of the shared network
3. Configure options for the shared network. For more information, refer to Section 5.15.6.3, “Configuring Shared Network Options”.
4. Configure the client for the shared network. For more information, refer to Section 5.15.6.4, “Configuring a Shared Network Client”.
5. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.15.6.3
Configuring Shared Network Options

To configure options for a shared network on the DHCP server, do the following:

> **NOTE**
> *Options set at the shared network level override options set at the DHCP server level.*

1. Make sure the CLI is in Configuration mode.
2. Configure the following parameter(s) as required:

Parameter	Description
unknown-client { unknown-client }	**Synopsis:** allow, deny, ignore The action to take for previously unregistered clients.
authorize-server	Enables/disables the server's authorization on this client. If enabled, the server will send deny messages to the client that is trying to renew the lease, which the server knows the client shouldn't have.
option82	Enables/disables the NAK of option 82 clients for this subnet.
default { default }	**Default:** 600 The minimum leased time in seconds that the server offers to the client.
maximum { maximum }	**Default:** 7200 The maximum leased time in seconds that the server offers to the clients.

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

Section 5.15.6.4

Configuring a Shared Network Client

To configure the client for a shared network on the DHCP server, do the following:

1. Make sure the CLI is in Configuration mode.
2. Configure the following parameter(s) as required:

Parameter	Description
hostname { hostname }	The unique name to refer to the host within a DHCP configuration.
subnetmask { subnetmask }	Subnet mask
default-route { default-route }	The default route that the server offers to the client when it issues the lease to the client.
broadcast { broadcast }	The broadcast address that the server offers to the client when it issues the lease to the client.
domain { domain }	The domain name that the server offers to the client when it issues the lease to the client.
dns-server { dns-server }	The domain name server that the server offers to the client when it issues the lease to the client.
static-route { static-route }	The static route that the DHCP server offers to the client when it issues the lease to the client.
server { server }	The NIS server address that the DHCP server offers to the client when it issues the lease to the client.
domain { domain }	The NIS domain name that the DHCP server offers to the client when it issues the lease to the client.
scope { scope }	**Default:** netbios The NetBIOS scope that the DHCP server offers to the client when it issues the lease to the client.
nameserver { nameserver }	**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.

3. If custom options are required for the shared network client, refer to Section 5.15.6.5, "Customizing Shared Network Clients".
4. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.15.6.5

Customizing Shared Network Clients

Custom DHCP options can be set for a shared network client.

To add a custom DHCP option to a shared network client, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the custom DHCP option by typing:

```
services dhcpserver shared-network name options client custom number value
```

Where:

- *name* is the name of the shared network
- *number* is the number assigned to the client
- *value* is the value of the custom option

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

Section 5.15.6.6
Deleting a Shared Network

To delete a shared network, do the following:

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

```
no services dhcpserver shared-network name
```

Where:

- *name* is the name of the shared network

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

Section 5.15.7
Managing Subnets

Subnets control settings for each subnet that DHCP serves. A subnet can include a range of IP addresses to give clients. Subnets contain groups, pools and hosts. Only one subnet can contain dynamic IP address ranges without any access restrictions on any given physical port, since DHCP doesn't know which subnet a client should belong to when the request is received.

The following sections describe how to configure and manage subnets on a DHCP server:

- Section 5.15.7.1, “Viewing a List of Subnets”
- Section 5.15.7.2, “Adding a Subnet”
- Section 5.15.7.3, “Configuring Subnet Options”
- Section 5.15.7.4, “Configuring a Subnet Client”
- Section 5.15.7.5, “Deleting a Subnet”

Section 5.15.7.1
Viewing a List of Subnets

To view a list of subnets, type:

```
show running-config services dhcpserver subnet
```

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

```
ruggedcom# show running-config services dhcpserver subnet network-ip | tab
NAME  NETWORK IP
-----------------------
SUB1  192.168.0.0/27
```

```
SUB2  192.168.0.32/27

  !
 !
```

If no subnets have been configured, add subnets as needed. For more information, refer to Section 5.15.7.2, "Adding a Subnet".

Section 5.15.7.2
Adding a Subnet

To add a subnet to the DHCP server, do the following:

> **NOTE**
> *Make sure a shared network is configured before adding a new subnet. For information about configuring a shared network, refer to Section 5.15.6.2, "Adding a Shared Network".*

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

```
services dhcpserver subnet name
```

   Where:

   - *name* is the name of the subnet
3. Configure the following parameter(s) as required:

Parameter	Description
network-ip { network-ip }	The network IP address for this subnet.
shared-network { shared-network }	The shared-network that this subnet belongs to.

4. Configure the options for the subnet. For more information, refer to Section 5.15.7.3, "Configuring Subnet Options"
5. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.15.7.3
Configuring Subnet Options

To configure options for a subnet, do the following:

> **NOTE**
> *Options set at the subnet level override options set at the DHCP server level.*

1. Make sure the CLI is in Configuration mode.
2. Navigate to ***services » dhcpserver » subnet » {name} » options***, where *{name}* is the name of the subnet.
3. Configure the following parameter(s) as required:

Parameter	Description
unknown-client { unknown-client }	**Synopsis:** allow, deny, ignore

Parameter	Description
	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.
default { default }	**Default:** 600 The minimum leased time in seconds that the server offers to the client.
maximum { maximum }	**Default:** 7200 The maximum leased time in seconds that the server offers to the clients.

4. Configure the client for the subnet. For more information, refer to Section 5.15.7.4, “Configuring a Subnet Client”
5. Configure one or more IP pools to the subnet. For more information, refer to Section 5.15.13.2, “Adding an IP Pool”
6. Configure one or more IP ranges to the subnet. For more information, refer to Section 5.15.14.2, “Adding an IP Range to a DHCP Subnet”
7. Type **`commit`** and press **Enter** to save the changes, or type **`revert`** and press **Enter** to abort.

Section 5.15.7.4
Configuring a Subnet Client

To configure a client for a subnet, do the following:

1. Make sure the CLI is in Configuration mode.
2. Navigate to ***services » dhcpserver » subnet » {name} » options » client***, where *{name}* is the name of the subnet.
3. Configure the following parameter(s) as required:

Parameter	Description
hostname { hostname }	The unique name to refer to the host within a DHCP configuration.
subnetmask { subnetmask }	Subnet mask
default-route { default-route }	The default route that the server offers to the client when it issues the lease to the client.
broadcast { broadcast }	The broadcast address that the server offers to the client when it issues the lease to the client.
domain { domain }	The domain name that the server offers to the client when it issues the lease to the client.
dns-server { dns-server }	The domain name server that the server offers to the client when it issues the lease to the client.
static-route { static-route }	The static route that the DHCP server offers to the client when it issues the lease to the client.
server { server }	The NIS server address that the DHCP server offers to the client when it issues the lease to the client.

Parameter	Description
domain { domain }	The NIS domain name that the DHCP server offers to the client when it issues the lease to the client.
scope { scope }	**Default:** netbios The NetBIOS scope that the DHCP server offers to the client when it issues the lease to the client.
nameserver { nameserver }	**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.

4. If custom options are required for the subnet client, refer to Section 5.15.8.2, "Adding a Custom Client Option".
5. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.15.7.5
Deleting a Subnet

To delete a subnet, do the following:

1. Make sure the CLI is in Configuration mode.
2. Configure the following parameter(s) as required:

```
no services dhcpserver subnet name
```

   Where:

   - *name* is the name of the subnet
3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.15.8
Managing Custom Client Options for Subnets

The following sections describe how to configure and manage custom client options for a DHCP subnet:

- Section 5.15.8.1, "Viewing a List of Custom Client Options"
- Section 5.15.8.2, "Adding a Custom Client Option"
- Section 5.15.8.3, "Deleting a Custom Client Option"

Section 5.15.8.1
Viewing a List of Custom Client Options

To view a list of custom client options configured for a DHCP subnet, type:

```
no services dhcpserver subnet name options client custom
```

Where:

- *name* is the name of the subnet

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

```
ruggedcom# show running-config services dhcpserver shared-network Shared options client custom
services
 dhcpserver
  shared-network Shared
   options client
    custom 22 2
    !
    custom 23 1
    !
   !
  !
 !
!
```

If no custom client options have been configured, add options as needed. For more information, refer to Section 5.15.8.2, “Adding a Custom Client Option”.

Section 5.15.8.2
Adding a Custom Client Option

To add a custom client option to a DHCP subnet, do the following:

> **NOTE**
> *The number of the option (defined by the Internet Assigned Numbers Authority or IANA) and its allowed value must be known before this custom option can be configured. For more information about DHCP options, refer to RFC 2132 [http://tools.ietf.org/html/rfc2132].*

1. Make sure the CLI is in Configuration mode.
2. Add the custom client option by typing:

   ```
   services dhcpserver subnet name options client custom number value
   ```

   Where:

   - *name* is the name of the subnet
   - *number* is the number defined by the Internet Assigned Numbers Authority (iANA) for the custom client option
   - *value* is the value of the custom client option
3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.15.8.3
Deleting a Custom Client Option

To delete a custom client option for a DHCP subnet, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the custom client option by typing:

   ```
   no services dhcpserver subnet name options client custom number value
   ```

   Where:

   - *name* is the name of the subnet

- *number* is the number defined by the Internet Assigned Numbers Authority (iANA) for the custom client option
- *value* is the value of the custom client option

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

Section 5.15.9

Managing Hosts

Host entries assign settings to a specific client based on its Ethernet MAC address.

The following sections describe how to configure and manage hosts on a DHCP server:

- Section 5.15.9.1, "Viewing a List of Hosts"
- Section 5.15.9.2, "Adding a Host"
- Section 5.15.9.3, "Configuring Host Options"
- Section 5.15.9.4, "Configuring a Host Client"
- Section 5.15.9.5, "Deleting Hosts"

Section 5.15.9.1

Viewing a List of Hosts

To view a list of hosts on the DHCP server, type:

```
show running-config services dhcpserver host
```

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

```
ruggedcom# show running-config services dhcpserver host APE-LM1-INT
services
 dhcpserver
  host APE-LM1-INT
   options
    hardware mac 00:01:C0:0B:B7:71
    fixed-ip       192.168.0.60
    unknown-client allow
    subnet         SUB2
    client
     hostname APE-LM1-INT
     no subnetmask
     no default-route
     no broadcast
     no domain
     no dns-server
     no static-route
     no nis server
     no nis domain
    !
   !
  !
 !
!
```

If no hosts have been configured, add hosts as needed. For more information, refer to Section 5.15.9.2, "Adding a Host".

Section 5.15.9.2
Adding a Host

To add a host to the DHCP server, do the following:

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

```
services dhcpserver host name
```

Where:

- *name* is the name of the host

3. Configure options for the host. For more information, refer to Section 5.15.9.3, “Configuring Host Options”.
4. Configure the client for the host. For more information, refer to Section 5.15.9.4, “Configuring a Host Client”.
5. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.15.9.3
Configuring Host Options

To configure options for a host on the DHCP server, do the following:

> **NOTE**
> *Options set at the host level override options set at the DHCP server level.*

1. Make sure the CLI is in Configuration mode.
2. Configure the following parameter(s) as required:

Parameter	Description
type { type }	**Synopsis:** fddi, token-ring, ethernet **Default:** ethernet The type of network hardware used by the client, associated with the host entry.
mac { mac }	The physical network address of the client. Note that this corresponds to the hardware type; for example, the MAC address for the ethernet.

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

Section 5.15.9.4
Configuring a Host Client

To configure a client for a host on the DHCP Server, do the following:

1. Make sure the CLI is in Configuration mode.
2. Navigate to ***services » dhcpserver » hosts » {host} » options » client***, where *{host}* is the name of the host.
3. Configure the following parameter(s) as required:

Parameter	Description
hostname { hostname }	The unique name to refer to the host within a DHCP configuration.
subnetmask { subnetmask }	Subnet mask
default-route { default-route }	The default route that the server offers to the client when it issues the lease to the client.
broadcast { broadcast }	The broadcast address that the server offers to the client when it issues the lease to the client.
domain { domain }	The domain name that the server offers to the client when it issues the lease to the client.
dns-server { dns-server }	The domain name server that the server offers to the client when it issues the lease to the client.
static-route { static-route }	The static route that the DHCP server offers to the client when it issues the lease to the client.
server { server }	The NIS server address that the DHCP server offers to the client when it issues the lease to the client.
domain { domain }	The NIS domain name that the DHCP server offers to the client when it issues the lease to the client.
scope { scope }	**Default:** netbios The NetBIOS scope that the DHCP server offers to the client when it issues the lease to the client.
nameserver { nameserver }	**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.

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

Section 5.15.9.5
Deleting Hosts

To delete a host, do the following:

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

```
no services dhcpserver host name
```

Where:

- *`name`* is the name of the host

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

Section 5.15.10
Managing Custom Host Client Configurations

Custom configuration settings can be set for each host client.

The following sections describe how to configure and manage custom host client configurations on a DHCP server:

- Section 5.15.10.1, “Viewing a List of Custom Host Client Configurations”
- Section 5.15.10.2, “Adding Custom Host Client Configurations”
- Section 5.15.10.3, “Deleting Custom Host Client Configurations”

Section 5.15.10.1
Viewing a List of Custom Host Client Configurations

To view a list of custom configurations for host clients on the DHCP server, type:

```
show running-config services dhcpserver host options client custom
```

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

```
ruggedcom# show running-config services dhcpserver host options client custom
services
 dhcpserver
  host 157
   options
    client
     custom 120 500
     !
    !
   !
  !
 !
!
```

If no custom configurations have been configured for the host client, add custom configurations as needed. For more information, refer to Section 5.15.10.2, “Adding Custom Host Client Configurations”.

Section 5.15.10.2
Adding Custom Host Client Configurations

To add a custom configuration to a host client on the DHCP server, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the custom configuration by typing:

   ```
   services dhcpserver host host options client custom number value
   ```

   Where:

   - *host* is the name of the host
   - *number* is the number assigned to the host
   - *value* is the value of the custom option
3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.15.10.3

Deleting Custom Host Client Configurations

To delete a custom configuration for a host client on the DHCP server, do the following:

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

```
no services dhcpserver host host options client custom number value
```

   Where:

   - *host* is the name of the host
   - *number* is the number assigned to the host
   - *value* is the value of the custom option

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

Section 5.15.11

Managing Host Groups

Host-groups allow identical settings to be created for a group of hosts, making it easier to manage changes to the settings for all the hosts contained within the group. Host-groups contain hosts.

The following sections describe how to configure and manage host groups on a DHCP server:

- Section 5.15.11.1, “Viewing a List of Host Groups”
- Section 5.15.11.2, “Adding a Host Group”
- Section 5.15.11.3, “Configuring Host Group Options”
- Section 5.15.11.4, “Configuring a Host Group Client”
- Section 5.15.11.5, “Deleting a Host Group”

Section 5.15.11.1

Viewing a List of Host Groups

To view a list of host groups, type:

```
show running-config services dhcpserver host-groups
```

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

```
ruggedcom# show running-config services dhcpserver host-groups
services
 dhcpserver
  host-groups "Local Group"
   options
    client
     no hostname
     no subnetmask
     no default-route
     no broadcast
     no domain
     no dns-server
     no static-route
```

```
     no nis server
     no nis domain
    !
   !
  !
 !
!
```

If no host groups have been configured, add host groups as needed. For more information, refer to Section 5.15.11.2, “Adding a Host Group”.

Section 5.15.11.2

Adding a Host Group

To add a host group to the DHCP server, do the following:

1. Make sure the CLI is in Configuration mode.
2. Configure the following parameter(s) as required:

Parameter	Description
{ name }	The description of the host groups.

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

Section 5.15.11.3

Configuring Host Group Options

To configure options for a host group on the DHCP server, do the following:

> **NOTE**
> *Options set at the host group level override options set at the DHCP server level.*

1. Make sure the CLI is in Configuration mode.
2. Navigate to ***services » dhcpserver » host-groups » {host} » options***, where *{host}* is the name of the host group.
3. Configure the following parameter(s) as required:

Parameter	Description
unknown-client { unknown-client }	**Synopsis:** allow, deny, ignore **Default:** allow The action to take for previously unregistered clients.
shared-network { shared-network }	The shared network that this host group belongs to.
subnet { subnet }	The subnet that this host group belongs to.
default { default }	**Default:** 600 The minimum leased time in seconds that the server offers to the client.
maximum { maximum }	**Default:** 7200 The maximum leased time in seconds that the server offers to the clients.

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

Section 5.15.11.4
Configuring a Host Group Client

To configure a client for a host on the DHCP Server, do the following:

1. Make sure the CLI is in Configuration mode.
2. Navigate to ***services » dhcpserver » host-groups » {host} » options » client***, where *{host}* is the name of the host group.
3. Configure the following parameter(s) as required:

Parameter	Description
hostname { hostname }	The unique name to refer to the host within a DHCP configuration.
subnetmask { subnetmask }	Subnet mask
default-route { default-route }	The default route that the server offers to the client when it issues the lease to the client.
broadcast { broadcast }	The broadcast address that the server offers to the client when it issues the lease to the client.
domain { domain }	The domain name that the server offers to the client when it issues the lease to the client.
dns-server { dns-server }	The domain name server that the server offers to the client when it issues the lease to the client.
static-route { static-route }	The static route that the DHCP server offers to the client when it issues the lease to the client.
server { server }	The NIS server address that the DHCP server offers to the client when it issues the lease to the client.
domain { domain }	The NIS domain name that the DHCP server offers to the client when it issues the lease to the client.
scope { scope }	**Default:** netbios The NetBIOS scope that the DHCP server offers to the client when it issues the lease to the client.
nameserver { nameserver }	**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.

4. If custom configuration settings are required for the host group client, refer to Section 5.15.12, “Managing Custom Host Group Client Configurations”.
5. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.15.11.5
Deleting a Host Group

To delete a host group, do the following:

1. Make sure the CLI is in Configuration mode.

2. Delete the host group by typing:

   ```
   no services dhcpserver host-groups name
   ```

   Where:

   - *name* is the name of the host group

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

Section 5.15.12

Managing Custom Host Group Client Configurations

Custom configuration settings can be set for each host group client.

The following sections describe how to configure and manage custom host group client configurations on a DHCP server:

- Section 5.15.12.1, “Viewing a List of Custom Host Group Client Configurations”
- Section 5.15.12.2, “Adding Custom Host Group Client Configurations”
- Section 5.15.12.3, “Deleting Custom Host Group Client Configurations”

Section 5.15.12.1

Viewing a List of Custom Host Group Client Configurations

To view a list of custom configurations for host group clients on the DHCP server, type:

```
show running-config services dhcpserver host-groups options client custom
```

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

```
ruggedcom# show running-config services dhcpserver host-groups
services
 dhcpserver
  host-groups APE-LM-INT-NIC
   options
    subnet SUB2
    client
     hostname      SUB3
     subnetmask    255.255.255.224
     default-route 192.168.0.33
     no broadcast
     no domain
     no dns-server
     no static-route
     no nis server
     no nis domain
    !
   !
  !
 !
!
```

If no custom configurations have been configured for the host group client, add custom configurations as needed. For more information, refer to Section 5.15.10.2, “Adding Custom Host Client Configurations”.

Section 5.15.12.2
Adding Custom Host Group Client Configurations

To add a custom configuration to a host group client on the DHCP server, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the custom configuration by typing:

```
services dhcpserver host-groups host options client custom number value
```

   Where:

   - *host* is the name of the host group
   - *number* is the number assigned to the host group
   - *value* is the value of the custom option
3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.15.12.3
Deleting Custom Host Group Client Configurations

To delete a custom configuration for a host group client on the DHCP server, do the following:

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

```
no services dhcpserver host-groups host options client custom number value
```

   Where:

   - *host* is the name of the host group
   - *number* is the number assigned to the host group
   - *value* is the value of the custom option
3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.15.13
Managing IP Pools

The following sections describe how to configure and manage IP pools for DHCP subnets:

- Section 5.15.13.1, “Viewing a List of IP Pools”
- Section 5.15.13.2, “Adding an IP Pool”
- Section 5.15.13.3, “Deleting an IP Pool”

Section 5.15.13.1
Viewing a List of IP Pools

To view a list of IP pools configured for a DHCP subnet, type:

```
show running-config services dhcpserver subnet name options ippool
```

Where:

- *name* is the name of the subnet

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

```
ruggedcom# show running-config services dhcpserver subnet Local options ippool
services
 dhcpserver
  subnet Local
   options
    ippool pool1
     no unknown-client
     iprange 172.0.0.0
      end 172.0.0.1
     !
     option82 class1
      remote-id  00:00:00:01:03:01
      circuit-id 00:00:00:01:01:01
     !
    !
   !
  !
 !
!
```

If no IP pools have been configured, add pools as needed. For more information, refer to Section 5.15.13.2, “Adding an IP Pool”.

Section 5.15.13.2
Adding an IP Pool

To add an IP pool to a DHCP subnet, do the following:

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

```
services dhcpserver subnet name options ippool description
```

   Where:

   - *name* is the name of the subnet
   - *description* is the name of the IP pool

3. Configure the leased time settings by configuring the following parameter(s):

Parameter	Description
default { default }	**Default:** 600 The minimum leased time in seconds that the server offers to the client.
maximum { maximum }	**Default:** 7200 The maximum leased time in seconds that the server offers to the clients.

4. Configure the client and failover settings by configuring the following parameter(s):

Parameter	Description
default { default }	**Default:** 600 The minimum leased time in seconds that the server offers to the client.

Parameter	Description
maximum { maximum }	**Default:** 7200 The maximum leased time in seconds that the server offers to the clients.

5. Add one or more IP ranges for the pool. For more information, refer to Section 5.15.15.2, “Adding an IP Range to an IP Pool”.
6. Add one or more Option82 classes to the pool. For more information, refer to Section 5.15.16.2, “Adding an Option 82 Class to an IP Pool”.
7. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.15.13.3
Deleting an IP Pool

To delete an IP pool, do the following:

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

```
no services dhcpserver subnet name options ippool description
```

Where:

- *name* is the name of the subnet
- *description* is the name of the IP pool

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

Section 5.15.14
Managing IP Ranges for Subnets

The following sections describe how to configure and manage IP ranges for DHCP subnets:

- Section 5.15.14.1, “Viewing a List of IP Ranges for Subnets”
- Section 5.15.14.2, “Adding an IP Range to a DHCP Subnet”
- Section 5.15.14.3, “Deleting an IP Range From a Subnet”

Section 5.15.14.1
Viewing a List of IP Ranges for Subnets

To view a list of IP ranges configured for a DHCP subnet, type:

```
show running-config services dhcpserver subnet name options iprange
```

Where:

- *name* is the name of the subnet

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

```
ruggedcom# show running-config services dhcpserver subnet Local options iprange
services
```

```
dhcpserver
  subnet Local
   options
    iprange 172.30.144.251
     end 172.30.144.254
    !
   !
  !
 !
!
```

If no IP ranges have been configured, add ranges as needed. For more information, refer to Section 5.15.14.2, “Adding an IP Range to a DHCP Subnet”.

Section 5.15.14.2
Adding an IP Range to a DHCP Subnet

To add an IP range to a DHCP subnet, do the following:

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

   ```
   services dhcpserver subnet name options iprange start end end
   ```

   Where:

   - *name* is the name of the subnet
   - *start* is the starting IP address pool the server uses to offer to the client
   - *end* is the ending IP address pool the server uses to offer to the client
3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.15.14.3
Deleting an IP Range From a Subnet

To delete an IP range from a DHCP subnet, do the following:

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

   ```
   no dhcpserver subnet name options iprange start end end
   ```

   Where:

   - *name* is the name of the subnet
   - *start* is the starting IP address pool the server uses to offer to the client
   - *end* is the ending IP address pool the server uses to offer to the client
3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.15.15

Managing IP Ranges for IP Pools

The following sections describe how to configure and manage IP ranges for IP pools:

- Section 5.15.15.1, “Viewing a List of IP Ranges for IP Pools”
- Section 5.15.15.2, “Adding an IP Range to an IP Pool”
- Section 5.15.15.3, “Deleting an IP Range From an IP Pool”

Section 5.15.15.1

Viewing a List of IP Ranges for IP Pools

To view a list of IP ranges configured for an IP pool, type:

```
show running-config services dhcpserver subnet name options ippool description iprange
```

Where:

- *name* is the name of the subnet
- *description* is the name of the IP pool

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

```
ruggedcom# show running-config services dhcpserver subnet Local options ippool pool1 iprange
services
 dhcpserver
  subnet Local
   options
    ippool pool1
     iprange 172.0.0.0
      end 172.0.0.1
     !
    !
   !
  !
 !
!
```

If no IP ranges have been configured, add ranges as needed. For more information, refer to Section 5.15.15.2, “Adding an IP Range to an IP Pool”.

Section 5.15.15.2

Adding an IP Range to an IP Pool

To add an IP range to an IP pool, do the following:

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

   ```
   services dhcpserver subnet name options ippool description iprange start end end
   ```

   Where:

   - *name* is the name of the subnet
   - *description* is the name of the IP pool

   - *start* is the starting IP address pool the server uses to offer to the client
   - *end* is the ending IP address pool the server uses to offer to the client
3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.15.15.3
Deleting an IP Range From an IP Pool

To delete an IP range from an IP Pool, do the following:

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

```
no services dhcpserver subnet name options ippool description iprange start end end
```

   Where:
   - *name* is the name of the subnet
   - *description* is the name of the IP pool
   - *start* is the starting IP address pool the server uses to offer to the client
   - *end* is the ending IP address pool the server uses to offer to the client
3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.15.16
Managing Option 82 Classes for IP Pools

The following sections describe how to configure and manage Option82 classes for IP pools:

- Section 5.15.16.1, “Viewing a List of Option 82 Classes for IP Pools”
- Section 5.15.16.2, “Adding an Option 82 Class to an IP Pool”
- Section 5.15.16.3, “Deleting an Option 82 Class From an IP Pool”

Section 5.15.16.1
Viewing a List of Option 82 Classes for IP Pools

To view a list of Option 82 classes configured for an IP pool, type:

```
show running-config services dhcpserver subnet name options ippool description option82
```

Where:

- *name* is the name of the subnet
- *description* is the name of the IP pool

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

```
ruggedcom# show running-config services dhcpserver subnet Local options ippool pool1 option82
services
 dhcpserver
  subnet Local
```

```
   options
    ippool pool1
     option82 class1
      remote-id  00:00:00:01:03:01
      circuit-id 00:00:00:01:01:01
     !
    !
   !
  !
 !
!
```

If no Option 82 classes have been configured, add classes as needed. For more information, refer to Section 5.15.16.2, “Adding an Option 82 Class to an IP Pool”.

Section 5.15.16.2

Adding an Option 82 Class to an IP Pool

To add an Option 82 class to an IP pool, do the following:

> **NOTE**
> *The format for the* `circuit-id` *value is 00:00:00:{vlan}:{slot}:{port}. If the remote host is connected to LM3/1 on VLAN 1, the ID would be 00:00:00:01:03:01.*

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

   ```
   services dhcpserver subnet name options ippool description option82 class
   ```

   Where:

   - *name* is the name of the subnet
   - *description* is the name of the IP pool
   - *class* is the name of the Option82 class
3. Configure the following parameter(s) as required:

Parameter	Description
remote-id { remote-id }	Specifies the information relating to the remote host end of the circuit.
circuit-id { circuit-id }	Specifies the local information to which circuit the request came in on.

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

Section 5.15.16.3

Deleting an Option 82 Class From an IP Pool

To delete an Option 82 class from an IP Pool, do the following:

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

   ```
   no services dhcpserver subnet name options ippool description option82 class
   ```

   Where:

- *name* is the name of the subnet
- *description* is the name of the IP pool
- *class* is the name of the Option82 class

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

Section 5.16

Managing Port Mirroring

Port mirroring is a troubleshooting tool that copies, or mirrors, all traffic received or transmitted on a designated port to another mirror port. If a protocol analyzer were attached to the target port, the traffic stream of valid frames on any source port is made available for analysis.

Select a target port that has a higher speed than the source port. Mirroring a 100 Mbps port onto a 10 Mbps port may result in an improperly mirrored stream.

Frames will be dropped if the full-duplex rate of frames on the source port exceeds the transmission speed of the target port. Since both transmitted and received frames on the source port are mirrored to the target port, frames will be discarded if the sum traffic exceeds the target port's transmission rate. This problem reaches its extreme in the case where traffic on a 100 Mbps full-duplex port is mirrored onto a 10 Mbps half-duplex port.

Invalid frames received on the source port will not be mirrored. These include CRC errors, oversized and undersized packets, fragments, jabbers, collisions, late collisions and dropped events).

NOTE

Port mirroring has the following limitations:

- *The target port may sometimes incorrectly show the VLAN tagged/untagged format of the mirrored frames.*
- *Network management frames (such as RSTP, GVRP, etc.) may not be mirrored.*
- *Switch management frames generated by the switch (such as Telnet, HTTP, SNMP, etc.) may not be mirrored.*

The following sections describe how to configure and manage port mirroring:

- Section 5.16.1, "Configuring Port Mirroring"
- Section 5.16.2, "Managing Egress Source Ports"
- Section 5.16.3, "Managing Ingress Source Ports"

Section 5.16.1

Configuring Port Mirroring

To configure port mirroring, do the following:

1. Make sure the CLI is in Configuration mode.
2. Navigate to ***switch » port-mirroring***.
3. Configure the port mirroring settings by configuring the following parameter(s) as required:

Parameter	Description
target-slot { target-slot }	**Synopsis:** sm, lm1, lm2, lm3, lm4, lm5, lm6 The slot where a monitoring device should be connected.
target-port { target-port }	The port where a monitoring device should be connected.
enabled	Enabling port mirroring causes all frames received and/or transmitted by the source port to be transmitted out of the target port.

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

Section 5.16.2

Managing Egress Source Ports

The following sections describe how to configure and manage egress source ports for port mirroring:

- Section 5.16.2.1, "Viewing a List of Egress Source Ports"
- Section 5.16.2.2, "Adding an Egress Source Port"
- Section 5.16.2.3, "Deleting an Egress Source Port"

Section 5.16.2.1

Viewing a List of Egress Source Ports

To view a list of egress source port for port mirroring, type:

```
show running-config switch port-mirroring egress-src
```

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

```
ruggedcom# show running-config switch port-mirroring egress-src
switch port-mirroring
 egress-src lm1 1
  !
!
```

If no egress source ports have been configured, add egress source ports as needed. For more information, refer to Section 5.16.2.2, "Adding an Egress Source Port".

Section 5.16.2.2

Adding an Egress Source Port

To add an egress source port for port mirroring, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the egress source port by typing:

```
switch port-mirroring egress-src slot port
```

Where:

- *`slot`* is the name of the module location

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

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

Section 5.16.2.3
Deleting an Egress Source Port

To delete an egress source port for port mirroring, do the following:

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

```
no switch port-mirroring egress-src slot port
```

Where:

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

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

Section 5.16.3
Managing Ingress Source Ports

The following sections describe how to configure and manage ingress source ports for port mirroring:

- Section 5.16.3.1, “Viewing a List of Ingress Source Ports”
- Section 5.16.3.2, “Adding an Ingress Source Port”
- Section 5.16.3.3, “Deleting an Ingress Source Port”

Section 5.16.3.1
Viewing a List of Ingress Source Ports

To view a list of ingress source port for port mirroring, type:

```
show running-config switch port-mirroring ingress-src
```

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

```
ruggedcom# show running-config switch port-mirroring ingress-src
switch port-mirroring
 ingress-src lm1 2
 !
!
```

If no ingress source ports have been configured, add ingress source ports as needed. For more information, refer to Section 5.16.3.2, “Adding an Ingress Source Port”.

Section 5.16.3.2

Adding an Ingress Source Port

To add an ingress source port for port mirroring, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the ingress source port by typing:

```
switch port-mirroring ingress-src slot port
```

   Where:

   - *slot* is the name of the module location
   - *port* is the port number (or a list of ports, if aggregated in a port trunk) for the module
3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.16.3.3

Deleting an Ingress Source Port

To delete an ingress source port for port mirroring, do the following:

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

```
no switch port-mirroring ingress-src slot port
```

   Where:

   - *slot* is the name of the module location
   - *port* is the port number (or a list of ports, if aggregated in a port trunk) for the module
3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.17

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 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 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 rule for the TCP and UDP protocols is applied.*

> . *The router sees both TCP and UDP traffic that qualifies for NAT.*
>
> . *The rule is then modified to allow only UDP.*
>
> . *The router will still see TCP packets (i.e. retransmission packets).*
>
> *If required, reboot the router to flush all existing connection streams.*

ROX II employs a stateful firewall system known as netfilter, a subsystem of the Linux kernel that provides the ability to examine IP packets on a per-session basis.

For more information about firewalls, refer to Section 5.17.1, "Firewall Concepts".

The following sections describe how to configure and manage a firewall:

- Section 5.17.2, "Viewing a List of Firewalls"
- Section 5.17.3, "Adding a Firewall"
- Section 5.17.4, "Deleting a Firewall"
- Section 5.17.5, "Working with Multiple Firewall Configurations"
- Section 5.17.9, "Managing Interfaces"
- Section 5.17.8, "Managing Zones"
- Section 5.17.11, "Managing Policies"
- Section 5.17.12, "Managing Network Address Translation Settings"
- Section 5.17.13, "Managing Masquerade and SNAT Settings"
- Section 5.17.10, "Managing Hosts"
- Section 5.17.14, "Managing Rules"
- Section 5.17.6, "Configuring the Firewall for a VPN"
- Section 5.17.7, "Configuring the Firewall for a VPN in a DMZ"
- Section 5.17.15, "Validating a Firewall Configuration"
- Section 5.17.16, "Enabling/Disabling a Firewall"

Section 5.17.1
Firewall Concepts

The following sections describe some of the concepts important to the implementation of firewalls in ROX II:

- Section 5.17.1.1, "Stateless vs. Stateful Firewalls"
- Section 5.17.1.2, "Linux netfilter"
- Section 5.17.1.3, "Network Address Translation"
- Section 5.17.1.4, "Port Forwarding"
- Section 5.17.1.5, "Protecting Against a SYN Flood Attack"

Section 5.17.1.1
Stateless vs. Stateful Firewalls

There are two types of firewalls: stateless and stateful.

Stateless or static firewalls make decisions about traffic without regard to traffic history. They simply open a path for the traffic type based on a TCP or UDP port number. Stateless firewalls are relatively simple, easily handling web and e-mail traffic. However, stateless firewalls have some disadvantages. All paths opened in the firewall are always open, and connections are not opened or closed based on outside criteria. Static IP filters offer no form of authentication.

Stateful or session-based firewalls add considerably more complexity to the firewalling process. They track the state of each connection, look at and test each packet (connection tracking), and recognize and manage as a whole traffic from a particular protocol that is on connected sets of TCP/UDP ports.

Section 5.17.1.2
Linux netfilter

Netfilter, a subsystem of the Linux kernel, is a stateful firewall that provides the ability to examine IP packets on a per-session basis.

Netfilter uses rulesets, which are collections of packet classification rules that determine the outcome of the examination of a specific packet. The rules are defined by iptables, a generic table structure syntax and utility program for the configuration and control of netfilter.

ROX implements an IP firewall using a structured user interface to configure iptables rules and netfilter rulesets.

Section 5.17.1.3
Network Address Translation

Network Address Translation (NAT) enables a LAN to use one set of IP addresses for internal traffic and a second set for external traffic. The netfilter NAT function makes all necessary IP address translations as traffic passes between the Intranet and the Internet. NAT is often referred to in Linux as IP Masquerading.

NAT itself provides a type of firewall by hiding internal IP addresses. More importantly, NAT enables a network to use more internal IP addresses. Since they are only used internally, there is no possibility of conflict with IP addresses used by other organizations. Typically, an internal network is configured to use one or more of the reserved address blocks described in RFC1918.

Table: RFC1918 Reserved IP Address Blocks

IP Network/Mask	Address Range
10.0.0.0/8	10.0.0.0 – 10.255.255.255
172.16.0.0/12	172.16.0.0 – 172.31.255.255
192.168.0.0/16	192.168.0.0 – 192.168.255.255

When a packet from a host on the internal network reaches the NAT gateway, its source address and source TCP/UDP port number are recorded. The address and port number is translated to the public IP address and an unused port number on the public interface. When the Internet host replies to the internal host's packet, it is addressed to the NAT gateway's external IP address at the translation port number. The NAT gateway searches its tables and makes the opposite changes it made to the outgoing packet. NAT then forwards the reply packet to the internal host.

Translation of ICMP packets happens in a similar fashion, but without the source port modification.

NAT can be used in static and dynamic modes. Static NAT (SNAT) masks the private IP addresses by translating each internal address to a unique external address. Dynamic NAT translates all internal addresses to one or more external addresses.

Section 5.17.1.4
Port Forwarding

Port forwarding, also known as redirection, allows traffic coming from the Internet to be sent to a host behind the NAT gateway.

Previous examples have described the NAT process when connections are made from the intranet to the Internet. In those examples, addresses and ports were unambiguous.

When connections are attempted from the Internet to the intranet, the NAT gateway will have multiple hosts on the intranet that could accept the connection. It needs additional information to identify the specific host to accept the connection.

Suppose that two hosts, 192.168.1.10 and 192.168.1.20 are located behind a NAT gateway having a public interface of 213.18.101.62. When a connection request for http port 80 arrives at 213.18.101.62, the NAT gateway could forward the request to either of the hosts (or could accept it itself). Port forwarding configuration could be used to redirect the requests to port 80 to the first host.

Port forwarding can also remap port numbers. The second host may also need to answer http requests. As connections to port 80 are directed to the first host, another port number (such as 8080) can be dedicated to the second host. As requests arrive at the gateway for port 8080, the gateway remaps the port number to 80 and forwards the request to the second host.

Port forwarding also takes the source address into account. Another way to solve the above problem could be to dedicate two hosts 200.0.0.1 and 200.0.0.2 and have the NAT gateway forward requests on port 80 from 200.0.0.1 to 192.168.1.10 and from 200.0.0.2 to 192.168.1.20.

Section 5.17.1.5
Protecting Against a SYN Flood Attack

ROX II responds to SYN packets according to the TCP standard by replying with a SYN-ACK packet for open ports and an RST packet for closed ports. If the device is flooded by a high frequency of SYN packets, the port being flooded may become unresponsive.

To prevent SYN flood attacks on closed ports, set the firewall to block all traffic to closed ports. This prevents SYN packets from reaching the kernel.

Siemens also recommends setting the listen ports to include IP addresses on separate interfaces. For example, set the device to listen to an IP address on switch.0001 and fe-cm-1. This will make sure that one port is accessible if the other is flooded.

Section 5.17.2
Viewing a List of Firewalls

To view a list of firewalls, type:

```
show running-config security firewall fwconfig
```

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

```
ruggedcom# show running-config security firewall fwconfig
security
 firewall
  fwconfig firewall1
  !
  fwconfig firewall2
```

```
   !
  !
!
```

If no firewalls have been configured, add firewalls as needed. For more information, refer to Section 5.17.3, “Adding a Firewall”.

Section 5.17.3
Adding a Firewall

To add a new firewall, do the following:

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

   ```
   security firewall fwconfig firewall
   ```

   Where:

   - *firewall* is the name of the firewall
3. Configure the following parameter(s) as required:

Parameter	Description
description { description }	An optional description string.

4. Add interfaces associated with the firewall. For more information about adding interfaces, refer to Section 5.17.9.2, “Adding an Interface”.
5. Add network zones for the firewall. Make sure a zone with the type **firewall** exists. For more information about adding network zones, refer to Section 5.17.8.2, “Adding a Zone”.
6. Associate an interface with each zone. For more information about associating interfaces with zones, refer to Section 5.17.9.3, “Associating an Interface with a Zone”.
7. Set the default policies for traffic control between zones. Make sure the policies are as restrictive as possible. For more information about configuring policies, refer to Section 5.17.11, “Managing Policies”.
8. Configure the network address translation (NAT), masquerading or static network address translation (SNAT) settings. For more information about configuring NAT settings, refer to Section 5.17.12, “Managing Network Address Translation Settings”. For more information about configuring masquerading and/or SNAT settings, refer to Section 5.17.13, “Managing Masquerade and SNAT Settings”.
9. If hosts on the network must accept sessions from the Internet, configure the firewall to support Destination Network Address Translation (DNAT). For more information about configuring hosts, refer to Section 5.17.10, “Managing Hosts”.
10. If required, configure rules that override the default policies. For more information about configuring rules, refer to Section 5.17.14, “Managing Rules”.
11. If required, configure support for a VPN. For more information, refer to:
    - Section 5.17.6, “Configuring the Firewall for a VPN”
    - Section 5.17.7, “Configuring the Firewall for a VPN in a DMZ”
12. Validate the configuration. For more information about validating a firewall configuration, refer to Section 5.17.15, “Validating a Firewall Configuration”.
13. Enable the firewall. For more information, refer to Section 5.17.16, “Enabling/Disabling a Firewall”.

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

Section 5.17.4
Deleting a Firewall

To delete a firewall, do the following:

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

```
no security firewall fwconfig firewall
```

   Where:

   - *firewall* is the name of the firewall
3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.17.5
Working with Multiple Firewall Configurations

ROX II allows users to create multiple firewall configurations and work with one configuration while another is active.

To set one configuration as the working configuration and another as the active configuration, do the following:

1. Make sure the CLI is in Configuration mode.
2. Specify the work configuration by typing:

```
security firewall work-config name
```

   Where:

   - *name* is the name of a firewall configuration
3. Specify the active configuration by typing:

```
security firewall active-config name
```

   Where:

   - *name* is the name of a firewall configuration
4. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.17.6
Configuring the Firewall for a VPN

To configure the firewall for a policy-based VPN, do the following:

1. Make sure a basic firewall has been configured. For more information about configuring a firewall, refer to Section 5.17.3, "Adding a Firewall".
2. Make sure zones for local, network and VPN traffic have been configured. For more information about managing zones, refer to Section 5.17.8, "Managing Zones".

3. Make sure a zone called *Any* exists and is of the type IPsec . For more information about managing zones, refer to Section 5.17.8, “Managing Zones”.
4. Configure the interface that carries the encrypted IPsec traffic. Make sure it is associated with the *Any* zone, as it will be carrying traffic for all zones. For more information about associating interfaces with zones, refer to Section 5.17.9.3, “Associating an Interface with a Zone”.
5. Configure a host for the interface that carries the encrypted IPsec traffic. Make sure the VPN zone is associated with the interface. If VPN tunnels to multiple remote sites are required, make sure host entry exists for each or collapse them into a single subnet. For more information about configuring hosts, refer to Section 5.17.10, “Managing Hosts”.
6. Configure a second host for the interface that carries the encrypted IPsec traffic. Make sure the interface is associated with the network zone and specify a wider subnet mask, such as 0.0.0.0/0. For more information about configuring hosts, refer to Section 5.17.10, “Managing Hosts”.

NOTE
The VPN host must be specified before the network host so the more specific VPN zone subnet can be inspected first.

Table: Example

Host	Interface	Subnet	IPsec Zone
vpn	W1ppp	192.168.1.0/24	Yes
net	W1ppp	0.0.0.0/0	No

7. Configure rules with the following parameter settings for the UDP, Authentication Header (AH) and Encapsulation Security Payload (ESP) protocols:

NOTE
The IPsec protocol operates on UDP port 500, using protocols Authentication Header (AH) and Encapsulation Security Payload (ESP) protocols. The firewall must be configured to accept this traffic in order to allow the IPsec protocol.

Table: Example

Action	Source-Zone	Destination-Zone	Protocol	Dest-Port
Accept	net	fw	ah	—
Accept	net	fw	esp	—
Accept	net	fw	udp	500

For more information about configuring rules, refer to Section 5.17.14, “Managing Rules”.

8. Configure the following rule to allow traffic from openswan, the IPsec daemon, to enter the firewall:

NOTE
IPsec traffic arriving at the firewall is directed to openswan, the IPsec daemon. Openswan decrypts the traffic and then forwards it back to the firewall on the same interface that originally received it. A rule is required to allow traffic to enter the firewall from this interface.

Table: Example

Action	Source-Zone	Destination-Zone	Protocol	Dest-Port
Accept	vpn	loc	—	—

For more information about configuring rules, refer to Section 5.17.14, “Managing Rules”.

Section 5.17.7

Configuring the Firewall for a VPN in a DMZ

When the firewall needs to pass VPN traffic through to another device, such as a VPN device in a Demilitarized Zone (DMZ), then a DMZ zone and special rules are required.

To configure the firewall for a VPN in a DMZ, do the following:

1. Make sure a basic firewall has been configured. For more information about configuring a firewall, refer to Section 5.17.3, “Adding a Firewall”.
2. Make sure a zone called *dmz* exists. For more information about managing zones, refer to Section 5.17.8, “Managing Zones”.
3. Configure rules with the following parameter settings for the UDP, Authentication Header (AH) and Encapsulation Security Payload (ESP) protocols:

> **NOTE**
> *The IPsec protocol operations on UDP port 500, using protocols Authentication Header (AH) and Encapsulation Security Payload (ESP) protocols. The firewall must be configured to accept this traffic in order to allow the IPsec protocol.*

Table: Example

Action	Source-Zone	Destination-Zone	Protocol	Dest-Port
Accept	Net	dmz	Ah	—
Accept	Net	dmz	Esp	—
Accept	Net	dmz	UDP	500
Accept	dmz	Net	Ah	—
Accept	dmz	Net	Esp	—
Accept	dmz	Net	Udp	500

For more information about configuring rules, refer to Section 5.17.14, “Managing Rules”.

Section 5.17.8

Managing Zones

A network zone is a collection of interfaces for which forwarding decisions are made. Common zones include:

Table: Example

Zone	Description
Net	The Internet
Loc	The local network
DMZ	Demilitarized zone

Zone	Description
Fw	The firewall itself
Vpn1	IPsec connections on w1ppp
Vpn2	IPsec connections on w2ppp

New zones may be defined as needed. For example, if each Ethernet interface is part of the local network zone, disabling traffic from the Internet zone to the local network zone would disable traffic to all Ethernet interfaces. If access to the Internet is required for some Ethernet interfaces, but not others, a new zone may be required for those interfaces.

The following sections describe how to configure and manage zones for a firewall:

- Section 5.17.8.1, “Viewing a List of Zones”
- Section 5.17.8.2, “Adding a Zone”
- Section 5.17.8.3, “Deleting a Zone”

Section 5.17.8.1
Viewing a List of Zones

To view a list of zones, type:

```
show running-config security firewall fwconfig firewall fwzone
```

Where:

- *firewall* is the name of the firewall

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

```
ruggedcom# show running-config security firewall fwconfig fwzone
security
 firewall
  fwconfig firewall
   fwzone fw
    type        firewall
    description FirewallZone
   !
   fwzone man
    description IPv4Zone
   !
  !
 !
!
```

If no zones have been configured, add zones as needed. For more information, refer to Section 5.17.8.2, “Adding a Zone”.

Section 5.17.8.2
Adding a Zone

To add a new zone for a firewall, do the following:

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

```
security firewall fwconfig firewall fwzone zone
```

Where:

- *firewall* is the name of the firewall
- *zone* is the name of the zone

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

Parameter	Description
type { type }	**Synopsis:** ipv4, ipsec, firewall **Default:** ipv4 Zone types are firewall, IPv4 or IPSsec
description { description }	(Optional) The description string for this zone

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

Section 5.17.8.3

Deleting a Zone

To delete a zone, do the following:

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

```
no security firewall fwconfig firewall fwzone name
```

Where:

- *firewall* is the name of the firewall
- *name* is the name of the zone

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

Section 5.17.9

Managing Interfaces

Firewall interfaces are the LAN and WAN interfaces available to the router. Each interface must be placed in a network zone. If an interface supports more than one subnet, it must be placed in zone *undefined-zone* and use the zone hosts setup to define a zone for each subnet on the interface.

Table: Example

Interface	Zone
Switch.0001	Loc
Switch.0002	Loc
Switch.0003	Any
Switch.0004	DMZ
W1ppp	net

The following sections describe how to configure and manage zones for a firewall:

- Section 5.17.9.1, "Viewing a List of Interfaces"
- Section 5.17.9.2, "Adding an Interface"
- Section 5.17.9.3, "Associating an Interface with a Zone"
- Section 5.17.9.4, "Configuring a Broadcast Address"
- Section 5.17.9.5, "Deleting an Interface"

Section 5.17.9.1
Viewing a List of Interfaces

To view a list of interfaces, type:

```
show running-config security firewall fwconfig firewall fwinterface
```

Where:

- *firewall* is the name of the firewall

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

```
ruggedcom# show running-config security firewall fwconfig fwinterface
security
 firewall
  fwconfig firewall
   fwinterface fe-cm-1
    zone man
    description Interface
   !
  !
 !
!
```

If no interfaces have been configured, add interfaces as needed. For more information, refer to Section 5.17.9.2, "Adding an Interface".

Section 5.17.9.2
Adding an Interface

To configure an interface for a firewall, do the following:

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

   ```
   security firewall fwconfig firewall fwinterface name
   ```

   Where:

   - *firewall* is the name of the firewall
   - *name* is the name of the interface
3. Configure the interface settings by typing the following commands:

Parameter	Description
description { description }	(Optional) The description string for this interface

4. Configure the interface options by typing the following commands:

Parameter	Description
arp_filter	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	Allows traffic on this interface to be routed back out that same interface.
tcpflags	Illegal combinations of TCP flags dropped and logged at info level.
dhcp	Allows DHCP datagrams to enter and leave the interface.
norfc1918	Not currently implemented
routefilter	Enables route filtering.
proxyarp	Enables proxy ARP.
maclist	Not currently implemented
nosmurfs	Packets with a broadcast address as the source are dropped and logged at info level.
logmartians	Enables logging of packets with impossible source addresses.

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

Section 5.17.9.3

Associating an Interface with a Zone

To associate an interface with a pre-defined zone or mark the assocated zone as undefined, do the following:

1. Make sure the CLI is in Configuration mode.
2. Navigate to ***security » firewall » fwconfig » fwconfig » {firewall} » fwinterface{interface} » zone***, where *{firewall}* is the name of the firewall and *{interface}* is the name of the interface.
3. Configure the following parameter(s) as required:

Parameter	Description
predefined-zone { predefined-zone }	A pre-defined zone
undefined-zone	This is used in conjunction with hosts definitions.

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

Section 5.17.9.4

Configuring a Broadcast Address

To configure a broadcast address for an interface, do the following:

1. Make sure the CLI is in Configuration mode.

2. Navigate to ***security » firewall » fwconfig » fwconfig » {firewall} » fwinterface{interface} » broadcast-addr***, where *{firewall}* is the name of the firewall and *{interface}* is the name of the interface.
3. Configure the following parameter(s) as required:

Parameter	Description
ipv4-address { ipv4-address }	An IPv4 address for a broadcast address.
detect	Automatic detection of the broadcast address(es).
none	The default.

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

Section 5.17.9.5
Deleting an Interface

To delete an interface, do the following:

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

```
no security firewall fwconfig firewall fwinterface name
```

Where:

- `firewall` is the name of the firewall
- `name` is the name of the interface

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

Section 5.17.10
Managing Hosts

Hosts are used to assign zones to individual hosts or subnets (if the interface supports multiple subnets). This allows the firewall to receive a packet and then redirect it to the same device that received it. This is functionality is useful for VPN setups to handle the VPN traffic separately from the other traffic on the interface which carries the VPN traffic.

Table: Example

Zone	Interface	IP Address or Network
Local	Switch.0003	10.0.0.0/8
Guests	Switch.0003	192.168.0.0/24

The following sections describe how to configure and manage hosts for a firewall:

- Section 5.17.10.1, “Viewing a List of Hosts”
- Section 5.17.10.2, “Adding a Host”
- Section 5.17.10.3, “Deleting a Host”

Section 5.17.10.1
Viewing a List of Hosts

To view a list of hosts, type:

```
show running-config security firewall fwconfig firewall fwhost
```

Where:

- *firewall* is the name of the firewall

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

```
ruggedcom# show running-config security firewall fwconfig firewall1 fwhost
security
 firewall
  fwconfig firewall1
   fwhost host1
    zone      man
    interface fe-cm-1
    no ipaddress
    no description
   !
  !
 !
!
```

If no hosts have been configured, add hosts as needed. For more information, refer to Section 5.17.10.2, “Adding a Host”.

Section 5.17.10.2
Adding a Host

To add a new host for a firewall, do the following:

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

```
security firewall fwconfig firewall fwhost name
```

Where:

- *firewall* is the name of the firewall
- *name* is the name of the host

3. Configure the host options by typing the following commands:

Parameter	Description
ipsec	**Default:** false

4. Configure the main host by typing the following commands:

Parameter	Description
zone { zone }	A pre-defined zone
interface { interface }	A pre-defined interface to which optional IPs and/or networks can be added.
ipaddress { ipaddress }	(Optional) Additional IP addresses or networks - comma separated.

Parameter	Description
description { description }	(Optional) The description string for this host.

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

Section 5.17.10.3
Deleting a Host

To delete a host, do the following:

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

```
no security firewall fwconfig firewall fwhost name
```

   Where:
   - *firewall* is the name of the firewall
   - *name* is the name of the host
3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.17.11
Managing Policies

Policies define the default actions for establishing a connection between different firewall zones. Each policy consists of a source zone, a destination zone and an action to be performed when a connection request is received.

The following example illustrates the policies for establishing connections between a local network and the Internet.

Table: Example

Policy	Source Zone	Destination Zone	Action
1	Loc	Net	ACCEPT
2	Net	All	DROP
3	All	All	REJECT

Each policy controls the connection between the source and destination zones. The first policy accepts all connection requests from the local network to the Internet. The second policy drops or ignores all connection requests from the Internet to any device on the network. The third policy rejects all other connection requests and sends a TCP RST or an ICMP destination-unreachable packet to the client.

The order of the policies is important. If the last policy in the example above were to be the first policy, the firewall would reject all connection requests.

NOTE
The source and destination zones must be configured before a policy can be created. For more information about zones, refer to *Section 5.17.8, "Managing Zones".*

> **NOTE**
> *Policies for specific hosts or types of traffic can be overridden by rules. For more information about rules, refer to Section 5.17.14, “Managing Rules”.*

The following sections describe how to configure and manage policies for a firewall:

- Section 5.17.11.1, “Viewing a List of Policies”
- Section 5.17.11.2, “Adding a Policy”
- Section 5.17.11.3, “Configuring the Source Zone”
- Section 5.17.11.4, “Configuring the Destination Zone”
- Section 5.17.11.5, “Deleting a Policy”

Section 5.17.11.1
Viewing a List of Policies

To view a list of policies, type:

```
show running-config security firewall fwconfig firewall fwpolicy
```

Where:

- *firewall* is the name of the firewall

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

```
ruggedcom# show running-config security firewall fwconfig firewall1 fwpolicy
security
 firewall
  fwconfig firewall1
   fwpolicy p1
    description Policy
   !
  !
 !
!
```

If no policies have been configured, add policies as needed. For more information, refer to Section 5.17.11.2, “Adding a Policy”.

Section 5.17.11.2
Adding a Policy

To configure a policy for the firewall, do the following:

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

   ```
   security firewall fwconfig firewall fwpolicy policy
   ```

   Where:

   - *firewall* is the name of the firewall
   - *policy* is the name of the policy
3. Configure the following parameter(s) as required:

Parameter	Description
policy { policy }	**Synopsis:** accept, drop, reject, continue **Default:** reject A default action for connection establishment between different zones.
log-level { log-level }	**Synopsis:** none, debug, info, notice, warning, error, critical, alert, emergency **Default:** none (Optional) Determines whether or not logging will take place and at which logging level.
description { description }	(Optional) The description string for this policy.

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

Section 5.17.11.3

Configuring the Source Zone

To configure the source zone for a firewall policy, do the following:

1. Make sure the CLI is in Configuration mode.
2. Navigate to ***security » firewall » fwconfig » {firewall} » fwpolicy{policy} » source-zone***, where *{firewall}* is the name of the firewall and *{policy}* is the name of the policy.
3. Configure the following parameter(s) as required:

   Default: all

Parameter	Description
predefined-zone { predefined-zone }	
all	

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

Section 5.17.11.4

Configuring the Destination Zone

To configure the destination zone for a firewall policy, do the following:

1. Make sure the CLI is in Configuration mode.
2. Configure the following parameter(s) as required:

Parameter	Description
predefined-zone { predefined-zone }	
all	

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

Section 5.17.11.5
Deleting a Policy

To delete a policy, do the following:

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

```
no security firewall fwconfig firewall fwpolicy policy
```

   Where:

   - *firewall* is the name of the firewall
   - *policy* is the name of the policy
3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.17.12
Managing Network Address Translation Settings

Network address translation entries can be used to set up a one-to-one correspondence between an external address on the firewall and the RFC1918 address of a host behind the firewall. This is often set up to allow connections to an internal server from outside the network.

> **NOTE**
> *Destination Network Address Translation (DNAT) can be setup by configuring the destination zone in a rule. For more information on rules, refer to* *Section 5.17.14, "Managing Rules".*

The following sections describe how to configure and manage network address translation settings for a firewall:

- Section 5.17.12.1, "Viewing a List of NAT Settings"
- Section 5.17.12.2, "Adding a NAT Setting"
- Section 5.17.12.3, "Deleting a NAT Setting"

Section 5.17.12.1
Viewing a List of NAT Settings

To view a list of NAT settings, type:

```
show running-config security firewall firewall fwnat
```

Where:

- *firewall* is the name of the firewall

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

```
ruggedcom# show running-config security firewall fwconfig firewall1 fwnat
security
 firewall
  fwconfig firewall1
   fwnat n1
    external-addr 172.30.150.10
    interface     fe-cm-1
    internal-addr 192.168.1.100
```

```
    no description
   !
   fwnat fwmasq
    external-addr 172.30.159.5
    interface     fe-cm-1
    internal-addr 193.168.1.1
    no description
   !
  !
 !
!
```

If no NAT settings have been configured, add NAT settings as needed. For more information, refer to Section 5.17.12.2, “Adding a NAT Setting”.

Section 5.17.12.2

Adding a NAT Setting

To configure a Network Address Translation (NAT) entry, do the following:

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

   ```
   security firewall fwconfig firewall fwnat name
   ```

   Where:

   - *firewall* is the name of the firewall
   - *name* is the name of the network address translation entry
3. Configure the following parameter(s) as required:

Parameter	Description
external-addr { external-addr }	**Synopsis:** The ipv4-address type represents an IPv4 address in dotted-quad notation. The IPv4 address may include a zone index, separated by a % sign. The zone index is used to disambiguate identical address values. For link-local addresses, the zone index will typically be the interface index number or the name of an interface. If the zone index is not present, the default zone of the device will be used. The canonical format for the zone index is the numerical format The external IP Address. The address must not be a DNS name. External IP addresses must be manually added to the interface.
interface { interface }	An interface that has an external IP address.
ipalias	Create IP Alias for NAT rule.
internal-addr { internal-addr }	**Synopsis:** The ipv4-address type represents an IPv4 address in dotted-quad notation. The IPv4 address may include a zone index, separated by a % sign. The zone index is used to disambiguate identical address values. For link-local addresses, the zone index will typically be the interface index number or the name of an interface. If the zone index is not present, the default zone of the device will be used. The canonical format for the zone index is the numerical format The internal IP address. The address must not be a DNS Name.
limit-interface	Translation only effective from the defined interface.
local	Translation effective from the firewall system.
description { description }	(Optional) The description string for this NAT entry.

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

Section 5.17.12.3
Deleting a NAT Setting

To delete a network address translation entry, do the following:

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

```
no security firewall fwconfig firewall fwnat name
```

   Where:

   - *firewall* is the name of the firewall
   - *name* is the name of the network address translation entry

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

Section 5.17.13
Managing Masquerade and SNAT Settings

Masquerading and Source Network Address Translation (SNAT) are forms of dynamic Network Address Translation (NAT). Both hide a subnetwork behind a single public IP address.

Masquerading is used when the ISP provides a dynamic IP address. SNAT is used when the ISP provides a static IP address.

The following sections describe how to configure and manage masquerade and SNAT settings for a firewall:

- Section 5.17.13.1, “Viewing a List of Masquerade and SNAT Settings”
- Section 5.17.13.2, “Adding Masquerade or SNAT Settings”
- Section 5.17.13.3, “Deleting a Masquerade or SNAT Setting”

Section 5.17.13.1
Viewing a List of Masquerade and SNAT Settings

To view a list of masquerade and SNAT settings, type:

```
show running-config security firewall fwconfig firewall fwmasq
```

Where:

- *firewall* is the name of the firewall

If masquerade and SNAT settings have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config security firewall fwconfig firewall2 fwmasq
security
 firewall
  fwconfig firewall2
   fwmasq SNAT
    out-interface fe-cm-1
    no out-interface-specifics
    source-hosts  192.168.1.0/24
```

```
     address       172.30.15.10
     no description
    !
    fwmasq Masq
     out-interface fe-cm-1
     no out-interface-specifics
     source-hosts  192.168.0.0/24
     no address
     no description
    !
   !
  !
 !
```

If no masquerade or SNAT settings have been configured, add masquerade or SNAT settings as needed. For more information, refer to Section 5.17.13.2, “Adding Masquerade or SNAT Settings”.

Section 5.17.13.2
Adding Masquerade or SNAT Settings

To add rules for masquerading or SNAT, do the following:

> **NOTE**
> *Masquerading requires that the IP address being used to masquerade must belong to the router. When configuring the SNAT address under masquerading, the SNAT address must be one of the IP addresses on the outbound interface.*

1. Make sure the CLI is in Configuration mode.
2. Add the masquerade or SNAT setting by typing:

   ```
   security firewall fwconfig firewall fwmasq name
   ```

   Where:

   - *firewall* is the name of the firewall
   - *name* is the name of the masquerade or SNAT setting
3. Configure the following parameter(s) as required:

Parameter	Description
out-interface { out-interface }	An outgoing interface list - usually the internet interface.
out-interface-specifics { out-interface-specifics }	(Optional) An outgoing interface list - specific IP destinations for the out-interface.
ipalias	Create IP Alias for NAT rule.
source-hosts { source-hosts }	Subnet range or comma-separated list of hosts (IPs)
address { address }	(Optional) By specifying an address here, SNAT will be used and this will be the source address.
description { description }	(Optional) The description string for this masq entry.

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

Section 5.17.13.3
Deleting a Masquerade or SNAT Setting

To delete a masquerade or SNAT setting, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the masquerade or SNAT setting by typing:

   ```
   no security firewall fwconfig firewall fwmasq name
   ```

   Where:

   - *firewall* is the name of the firewall
   - *name* is the name of the masquerade or SNAT setting
3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.17.14
Managing Rules

Rules establish exceptions to the default firewall policies for certain types of traffic, sources or destinations. Each rule defines specific criteria. If an incoming packet matches that criteria, the default policy is overridden and the action defined by the rule is applied.

The following sections describe how to configure and manage rules for a firewall:

- Section 5.17.14.1, “Viewing a List of Rules”
- Section 5.17.14.2, “Adding a Rule”
- Section 5.17.14.3, “Configuring the Source Zone”
- Section 5.17.14.4, “Configuring the Destination Zone”
- Section 5.17.14.5, “Deleting Rules”

Section 5.17.14.1
Viewing a List of Rules

To view a list of rules, type:

```
show running-config security firewall fwconfig firewall fwrule
```

Where:

- *firewall* is the name of the firewall

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

```
ruggedcom# show running-config security firewall fwconfig firewall1 fwrule
security
 firewall
  fwconfig firewall1
   fwrule Rule1
    action accept
    source-zone man
    destination-zone man
    no description
   !
```

```
   fwrule Rule2
    action accept
    source-zone man
    destination-zone man
    no description
   !
  !
 !
!
```

If no rules have been configured, add rules as needed. For more information, refer to Section 5.17.14.2, “Adding a Rule”.

Section 5.17.14.2
Adding a Rule

To configure a rule for a firewall, do the following:

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

```
security firewall fwconfig firewall fwrule rule
```

Where:

- *firewall* is the name of the firewall
- *rule* is the name of the rule

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

> **NOTE**
> *When applying new rules, previous traffic seen by the router might still be considered as having valid connections by the connection tracking table. For instance:*
>
> . *A rule for the TCP and UDP protocols is applied.*
>
> . *The router sees both TCP and UDP traffic that qualifies for NAT.*
>
> . *The rule is then modified to allow only UDP.*
>
> . *The router will still see TCP packets (i.e. retransmission packets).*
>
> *If required, reboot the router to flush all existing connection streams.*

Parameter	Description
action { action }	**Synopsis:** accept, drop, reject, continue, redirect, dnat-, dnat **Default:** reject The final action to take on incoming packets matching this rule.
source-zone-hosts { source-zone-hosts }	(Optional) Add comma-separated host IPs to a predefined source-zone.
destination-zone-hosts { destination-zone-hosts }	(Optional) Add comma-separated host IPs to the destination-zone - may include :port for DNAT or REDIRECT.
log-level { log-level }	**Synopsis:** none, debug, info, notice, warning, error, critical, alert, emergency **Default:** none (Optional) Determines whether or not logging will take place and at which logging level.
protocol { protocol }	**Synopsis:** tcp, udp, icmp, all **Default:** all

Parameter	Description
	The protocol to match for this rule.
source-ports { source-ports }	**Default:** none (Optional) The TCP/UDP port(s) the connection originated from. Default: all ports. Add a single port or a list of comma-separated ports
destination-ports { destination-ports }	**Default:** none (Optional) The TCP/UDP port(s) the connection is destined for. Default: all ports. Add a single port or a list of comma-separated ports
original-destination { original-destination }	**Synopsis:** None **Default:** none (Optional) The destination IP address in the connection request as it was received by the firewall.
description { description }	(Optional) The description string for this rule.

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

Section 5.17.14.3
Configuring the Source Zone

To configure the source zone for a firewall rule, do the following:

1. Make sure the CLI is in Configuration mode.
2. Navigate to ***security » firewall » fwconfig » {firewall} » fwrule{rule} » source-zone***, where *{firewall}* is the name of the firewall and *{rule}* is the name of the rule.
3. Configure the following parameter(s) as required:

Parameter	Description
predefined-zone { predefined-zone }	A predefined zone
other { other }	Type a custom definition - this can be a comma-separated list of zones.
all	All zones

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

Section 5.17.14.4
Configuring the Destination Zone

To configure the destination zone for a firewall rule, do the following:

1. Make sure the CLI is in Configuration mode.
2. Configure the following parameter(s) as required:

Parameter	Description
predefined-zone { predefined-zone }	A pre-defined zone
other { other }	An undefined zone (string).

Parameter	Description
all	All zones

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

Section 5.17.14.5
Deleting Rules

To delete a rule, do the following:

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

```
no security firewall fwconfig firewall fwrule rule
```

Where:

- *firewall* is the name of the firewall
- *rule* is the name of the rule

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

Section 5.17.15
Validating a Firewall Configuration

To validate a firewall configuration, do the following:

1. Make sure the CLI is in Configuration mode.
2. Set the firewall as the working configuration by typing:

```
security firewall work-config name
```

Where:

- *name* is the name of the firewall configuration

3. Type **commit** and press **Enter** to save the changes. The system validates the firewall configuration and displays the results.

Section 5.17.16
Enabling/Disabling a Firewall

To enable or disable the firewall, do the following:

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

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

```
security firewall enable
```

Or disable the firewall by using the *no* version of the command:

```
no security firewall enable
```

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

Section 5.18

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]).

IS-IS is an Interior Gateway Protocol (IGP) meant to exchange information between 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.

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, 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 inter-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 intra-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.

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)

Before enabling IS-IS, note the following advantages and disadvantages:

IS-IS Advantages

- runs natively on the OSI network layer
- can support both IPv4 and IPv6 networks due to it's independence from IP addressing
- IS-IS concept of areas is simpler to understand and implement
- IS-IS updates grouped together and sent as one LSP, rather than several small LSAs as with OSPF
- better scalability than OSPF due to a leaner daemon with less overhead
- gaining popularity among service providers
- integrates with MPLS
- protects from *spoofing* and Denial of Service (DoS) attacks due to use of the data link layer

IS-IS 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

NOTE
In complex legacy networks, RIP, OSPF, BGP and IS-IS may all be active on the same router at the same time. Typically, however, only one dynamic routing protocol is employed at one time.

The following sections describe how to configure the IS-IS routing protocol:

- Section 5.18.2, “Viewing the Status of Neighbors”
- Section 5.18.3, “Viewing the Status of the Link-State Database”
- Section 5.18.1, “Configuring IS-IS”
- Section 5.18.4, “Managing Area Tags”
- Section 5.18.5, “Managing Interfaces”
- Section 5.18.6, “Managing LSP Generation”
- Section 5.18.7, “Managing SPF Calculations”
- Section 5.18.8, “Managing the Lifetime of LSPs”
- Section 5.18.9, “Managing LSP Refresh Intervals”
- Section 5.18.10, “Managing Network Entity Titles (NETs)”
- Section 5.18.11, “Managing Redistribution Metrics”

Section 5.18.1

Configuring IS-IS

To configure dynamic routing with IS-IS, do the following:

1. Make sure the CLI is in Configuration mode.
2. Enable IS-IS by typing:

```
routing isis enabled
```

3. Associate the device with one or more areas in the IS-IS network by defining area tags. For more information, refer to Section 5.18.4, “Managing Area Tags”.
4. Configure one or more interfaces on which to perform IS-IS routing. For more information, refer to Section 5.18.5, “Managing Interfaces”.
5. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Example

The following illustrates how to configure an IS-IS network that includes all circuit types. In this example, R1 is a Level-1 router that needs to forward traffic to Level-2 routers. R2 and R3 are configured to be Level-1-2 routers to facilitate the connection with routers R4 and R5, which are Level-2-only routers. Each router is configured to have a non-passive interface, use point-to-point network communication, and be in the same area.

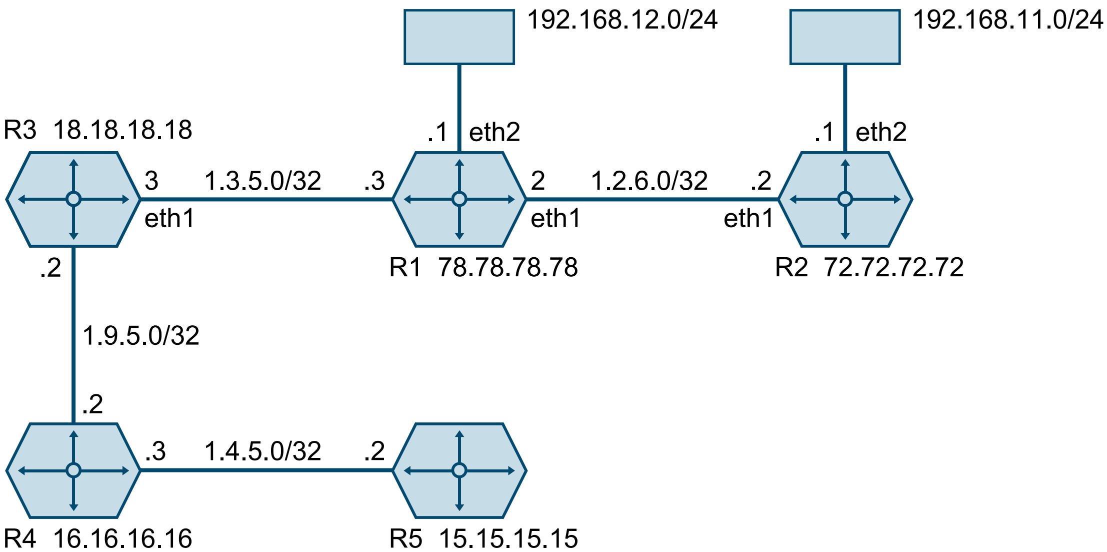

Figure 5: Multi-Level IS-IS Configuration

Section 5.18.2

Viewing the Status of Neighbors

To view the status of neighboring devices on an IS-IS network, do the following:

1. Make sure IS-IS is configured. For more information, refer to Section 5.18.1, “Configuring IS-IS”.
2. View the status by typing:

```
routing status isis isis-neighbors-status
```

If IS-IS routes have been configured, a table similar to the following example appears:

```
ruggedcom# routing status isis isis-neighbors-status
isis-neighbors-status
Area area1:

  System Id            Interface    L  State         Holdtime  SNPA

  Spirent-             switch.0012 3  Up            24        2020.2020.2020
```

Section 5.18.3
Viewing the Status of the Link-State Database

To view the basic status of the link-state database for the IS-IS network, do the following:

1. Make sure IS-IS is configured. For more information, refer to Section 5.18.1, “Configuring IS-IS”.
2. Display the basic status by typing:

```
routing status isis isis-database-status
```

Or display a more detailed status by typing:

```
routing status isis isis-database-detail-status
```

If IS-IS routes have been configured, a list similar to the following example appears:

```
ruggedcom# routing status isis isis-database-status
isis-database-status
Area area1:

IS-IS Level-1 link-state database:

LSP ID                  PduLen  SeqNumber   Chksum  Holdtime  ATT/P/OL

R1.00-00             *      75  0x00000015  0xe43a    1129    0/0/0

    1 LSPs



IS-IS Level-2 link-state database:

LSP ID                  PduLen  SeqNumber   Chksum  Holdtime  ATT/P/OL

Spirent-.00-00             121  0x0000000f  0xd5e6     871    0/0/0

R1.00-00             *      75  0x00000015  0xe636    1031    0/0/0

Spirent-right.00-00       1465  0x0000000f  0x3d65     871    0/0/0

Spirent-right.00-01        295  0x0000000f  0x6a0d     872    0/0/0

Spirent-right.00-00       1465  0x0000000f  0x4638     872    0/0/0

Spirent-right.00-01        287  0x0000000f  0x54d0     872    0/0/0

Spirent-right.00-00       1462  0x0000000f  0x6528     872    0/0/0

Spirent-right.00-01        269  0x0000000f  0x7e8a     872    0/0/0

Spirent-right.00-00       1463  0x0000000f  0x99a0     872    0/0/0

Spirent-right.00-01        261  0x0000000f  0xb0d2     872    0/0/0

Spirent-right.00-00       1460  0x0000000f  0x80c6     872    0/0/0

Spirent-right.00-01        253  0x0000000f  0x97fb     872    0/0/0

Spirent-right.00-00       1460  0x0000000f  0x1137     872    0/0/0

Spirent-right.00-01        237  0x0000000f  0x0db7     872    0/0/0

    14 LSPs
```

Section 5.18.4
Managing Area Tags

An IS-IS area is a grouping of inter-connected (or neighboring) IS-IS configured routers. As opposed to OSPF, where an Area Border Router (ABR) can exist in two areas at once, IS-IS routers reside only in one area. It is the link between routers in two different areas that forms the border. This is because an IS-IS router has only one Network Service Access Point (NSAP) address.

A single router can be configured to act as a Level-1, Level-2 or Level-1-2 router in one or more areas.

Routers are associated with areas by area tags, which define the routing type, metric, and authentication/authorization rules.

The following sections describe how to configure and manage area tags for IS-IS:

- Section 5.18.4.1, “Viewing a List of Area Tags”
- Section 5.18.4.2, “Adding an Area Tag”
- Section 5.18.4.3, “Deleting an Area Tag”

Section 5.18.4.1
Viewing a List of Area Tags

To view a list of area tags configured for dynamic IS-IS routes, type:

```
show running-config routing isis area
```

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

```
ruggedcom# show running-config routing isis area
routing isis
 area Area_1
  is-type                level-1-2
  metric-style           narrow
  area-authorization     md5
  area-password          admin
  area-authentication    validate
  domain-authorization   md5
  domain-password        admin
  domain-authentication validate
  net 49.0001.1921.6800.1001.00
  !
  redistribute bgp
   is-type     level-1-2
   metric-type internal
   metric      10
  !
  lsp-gen-interval is-type level-1-only
   interval 60
  !
  lsp-refresh-interval is-type level-1-2
   interval 20
  !
  max-lsp-lifetime is-type level-2-only
   interval 10
  !
  spf-interval is-type level-1-2
   interval 5
  !
 !
!
```

If no area tags have been configured, add area tags as needed. For more information, refer to Section 5.18.4.2, "Adding an Area Tag".

Section 5.18.4.2
Adding an Area Tag

To add an area tag for dynamic IS-IS routes, do the following:

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

```
routing isis area name
```

   Where:

   - *name* is the unique name for a routing process that belongs to a specific router.
3. Configure the following parameter(s) as required:

Parameter	Description
is-type { is-type }	**Synopsis:** level-1-only, level-2-only, level-1-2 The IS type for this area: level-1-only, level-2-only or level-1-2. Level-1 routers have neighbors only on the same area. Level-2-only (backbone) can have neighbors on different areas. Level-1-2 can have neighbors on any areas. Default is level-1-2.
metric-style { metric-style }	**Synopsis:** narrow, transition, wide **Default:** wide The metric style Type length Value (TLV) for this area: narrow, transition or wide. Default is wide.
area-authorization { area-authorization }	**Synopsis:** clear, md5 **Default:** clear The authorization type for the area password. Default is clear.
area-password { area-password }	The area password to be used for transmission of level-1 LSPs.
area-authentication { area-authentication }	**Synopsis:** send-only, validate **Default:** send-only The authentication option to be used with the area password on SNP PDUs. Default is send-only.
domain-authorization { domain-authorization }	**Synopsis:** clear, md5 **Default:** clear The authorization type for the domain password. Default is clear.
domain-password { domain-password }	The domain password to be used for transmission of level-2 LSPs.
domain-authentication { domain-authentication }	**Synopsis:** send-only, validate **Default:** send-only The authentication option to be used with the domain password on SNP PDUs. Default is send-only.

4. Add one or more Network Entity Titles (NETs). For more information, refer to Section 5.18.10, "Managing Network Entity Titles (NETs)"
5. If necessary, configure intervals for the generation of Link-State Packets (LSPs). The default is 30 seconds. For more information, refer to Section 5.18.6, "Managing LSP Generation".

6. If necessary, configure refresh intervals for Link-State Packets (LSPs). The default is 900 seconds. For more information, refer to Section 5.18.9, “Managing LSP Refresh Intervals”.
7. If necessary, configure the minimum interval between consecutive SPF calculations. The default is 1 second. For more information, refer to Section 5.18.7, “Managing SPF Calculations”.
8. If necessary, configure how long LSPs can reside in the device's Link State Database (LSDB) before they are refreshed. The default is 1200 seconds. For more information, refer to Section 5.18.8, “Managing the Lifetime of LSPs”.
9. If necessary, define rules for redistributing static, RIP, BGP or OSPF routes. For more information, refer to Section 5.18.11, “Managing Redistribution Metrics”
10. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.18.4.3
Deleting an Area Tag

To delete an area tag for dynamic IS-IS routes, do the following:

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

```
no routing isis area name
```

   Where:

   - *name* is the unique name for a routing process that belongs to a specific router.
3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.18.5
Managing Interfaces

IS-IS transmits hello packets and Link-State Packets (LSPs) through IS-IS enabled interfaces.

> **NOTE**
> *IS-IS is only supported on Ethernet and WAN (HDLC-ETH) interfaces.*

The following sections describe how to configure and manage interfaces for IS-IS:

- Section 5.18.5.1, “Viewing a List of Interfaces”
- Section 5.18.5.2, “Configuring an Interface”

Section 5.18.5.1
Viewing a List of Interfaces

To view a list of interfaces for dynamic IS-IS routes, type:

```
show running-config routing isis interface
```

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

```
ruggedcom# show running-config routing isis interface | tab
             IPV4                   POINT
             AREA                   TO              CIRCUIT   CIRCUIT                   CSNP       HELLO
 HELLO       PSNP
IFNAME       TAG      CIRCUIT TYPE  POINT  PASSIVE  PASSWORD  AUTHORIZATION  METRIC   INTERVAL   INTERVAL
 MULTIPLIER  INTERVAL
-----------------------------------------------------------------------------------------------------------
fe-cm-1      Area_1   level-1-2     true   true     admin     md5            10       10         3
 10          2
switch.0001  Area_2   level-1-only  false  true     admin     clear          10       10         3
 10          2

!
```

Interfaces are added automatically when a VLAN is created. For more information about creating a VLAN, refer to Section 5.35, “Managing VLANs”.

Section 5.18.5.2

Configuring an Interface

By default, two interfaces are already configured for IS-IS: fe-cm-01 and switch.0001.

To configure optional parameters for these and any other interfaces that have been added for IS-IS, do the following:

1. Make sure the CLI is in Configuration mode.
2. Navigate to the interface by typing:

```
routing isis interface name
```

Where:

- *name* is the name of the interface. If the desired interface is not available, it must be created as a VLAN. For more information about creating a VLAN, refer to Section 5.35, “Managing VLANs”.

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

Parameter	Description
ipv4-area-tag { ipv4-area-tag }	Name of Area Tag to be used for IS-IS over IPv4.
circuit-type { circuit-type }	**Synopsis:** level-1-only, level-2-only, level-1-2 The IS-IS Circuit Type. Level-1 routers have neighbors only on the same area. Level-2 (backbone) can have neighbors on different areas. Level-1-2 can have neighbors on any areas. Default is level-1-2.
point-to-point	**Default:** false Enable or disable point-to-point network communication
passive	**Default:** true Whether an interface is active or passive. Passive interfaces do not send packets to other routers and are not part of an IS-IS area.
circuit-password { circuit-password }	The value to be used as a transmit password in IIH PDUs transmitted by this Intermediate System.
circuit-authorization { circuit-authorization }	**Synopsis:** clear, md5 **Default:** clear The authorization type ot be associated with the transmit password in IIH PDUs transmitted by this Intermediate System.

Parameter	Description
metric { metric }	**Default:** 10 Metric assigned to the link, used to calculate the cost of the route. Value ranges from 1 to 16777214. Default is 10.
csnp-interval { csnp-interval }	**Default:** 10 CSNP interval in seconds, ranging from 1 to 600. Default is 10.
hello-interval { hello-interval }	**Default:** 3 Hello interval in seconds, ranging from 1 to 600. Default is 3.
hello-multiplier { hello-multiplier }	**Default:** 10 Multiplier for Hello holding time. Value ranges from 2 to 100. Default is 10.
psnp-interval { psnp-interval }	**Default:** 2 PSNP interval in seconds, ranging from 1 to 120. Default is 2.

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

Section 5.18.6

Managing LSP Generation

IS-IS generates new Link-State Packets (LSPs) every 30 seconds by default. However, the interval can be configured anywhere between 1 and 120 seconds.

Since the introduction of a new LSP causes other routers in the area to recalculate routes, it is recommended to increase the interval to decrease flooding during periods of network instability, so as to reduce the load on other routers in the area.

The following sections describe how to configure and manage generation intervals for LSPs:

- Section 5.18.6.1, “Viewing a List of LSP Generation Intervals”
- Section 5.18.6.2, “Adding an LSP Generation Interval”
- Section 5.18.6.3, “Deleting an LSP Generation Interval”

Section 5.18.6.1

Viewing a List of LSP Generation Intervals

To view a list of LSP generation intervals configured for an IS-IS area, type:

```
show running-config routing isis area name lsp-gen-interval
```

Where:

- *name* is the unique name for a routing process that belongs to a specific router.

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

```
ruggedcom# show running-config routing isis area Area_1 lsp-gen-interval | tab
ISTYPE        INTERVAL
------------------------
level-1-only  60

 !
!
```

If no intervals have been configured, add intervals as needed. For more information, refer to Section 5.18.6.2, “Adding an LSP Generation Interval”.

Section 5.18.6.2
Adding an LSP Generation Interval

To add an LSP generation interval to an IS-IS area, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add a new interval by typing:

```
routing isis area name lsp-gen-interval is-type [level-1-2 | level-1-only | level-2-only] interval
seconds
```

   Where:

   - *name* is the unique name for a routing process that belongs to a specific router.
   - *level* is the IS type.
   - *seconds* is the minimum interval in seconds, ranging from 1 to 120. The default value is 30.
3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.18.6.3
Deleting an LSP Generation Interval

To delete an LSP generation interval for an IS-IS area, do the following:

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

```
no routing isis area name lsp-gen-interval is-type [level-1-2 | level-1-only | level-2-only]
interval seconds
```

   Where:

   - *name* is the unique name for a routing process that belongs to a specific router.
   - *level* is the IS type.
   - *seconds* is the minimum interval in seconds, ranging from 1 to 120. The default value is 30.
3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.18.7
Managing SPF Calculations

IS-IS uses the Shortest Path First (SPF) algorithm to determine the best routes to every known destination in the network. When the network topology (not external links) changes, a partial recalculation is required.

IS-IS can be configured to perform the SPF calculation every 1 to 120 seconds. By default, IS-IS performs the SPF calculation every second. which could potentially be processor intensive, depending on the size of the area and how often the topology changes.

The following sections describe how to configure and manage SPF calculations for IS-IS areas:

- Section 5.18.7.1, “Viewing a List of SPF Calculation Intervals”
- Section 5.18.7.2, “Adding an SPF Calculation Interval”
- Section 5.18.7.3, “Deleting an SPF Calculation Interval”

Section 5.18.7.1
Viewing a List of SPF Calculation Intervals

To view a list of SPF calculation intervals configured for an IS-IS area, type:

```
show running-config routing isis area name spf-interval
```

Where:

- *name* is the unique name for a routing process that belongs to a specific router.

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

```
ruggedcom# show running-config routing isis area Area_1 spf-interval | tab
ISTYPE        INTERVAL
------------------------
level-1-only  60

 !
!
```

If no intervals have been configured, add intervals as needed. For more information, refer to Section 5.18.7.2, “Adding an SPF Calculation Interval”.

Section 5.18.7.2
Adding an SPF Calculation Interval

To add an SPF calculation interval to an IS-IS area, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add a new interval by typing:

   ```
   routing isis area name spf-interval is-type [level-1-2 | level-1-only | level-2-only] interval
   seconds
   ```

   Where:

   - *name* is the unique name for a routing process that belongs to a specific router.
   - *level* is the IS type.
   - *seconds* is the minimum interval in seconds, ranging from 1 to 120. The default value is 30.
3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.18.7.3
Deleting an SPF Calculation Interval

To delete an SPF calculation interval for an IS-IS area, do the following:

1. Make sure the CLI is in Configuration mode.

2. Delete the LDP interface by typing:

```
no routing isis area name spf-interval is-type [level-1-2 | level-1-only | level-2-only] interval
seconds
```

Where:

- *name* is the unique name for a routing process that belongs to a specific router.
- *level* is the IS type.
- *seconds* is the minimum interval in seconds, ranging from 1 to 120. The default value is 30.

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

Section 5.18.8

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.

The following sections describe how to configure and manage LSP lifetime intervals for LSPs:

> **NOTE**
> *For information about configuring the refresh interval for an LSP, refer to Section 5.18.9, “Managing LSP Refresh Intervals”.*

- Section 5.18.8.1, “Viewing a List of LSP Lifetime Intervals”
- Section 5.18.8.2, “Adding an LSP Lifetime Interval”
- Section 5.18.8.3, “Deleting an LSP Lifetime Interval”

Section 5.18.8.1

Viewing a List of LSP Lifetime Intervals

To view a list of LSP lifetime intervals configured for an IS-IS area, type:

```
show running-config routing isis area name max-lsp-lifetime
```

Where:

- *name* is the unique name for a routing process that belongs to a specific router.

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

```
ruggedcom# show running-config routing isis area Area_1 max-lsp-lifetime | tab
ISTYPE        INTERVAL
------------------------
level-1-only  60

 !
!
```

If no intervals have been configured, add intervals as needed. For more information, refer to Section 5.18.8.2, “Adding an LSP Lifetime Interval”.

Section 5.18.8.2

Adding an LSP Lifetime Interval

To add an LSP lifetime interval to an IS-IS area, do the following:

> **IMPORTANT!**
> *The LSP lifetime interval must be 300 seconds higher than the LSP refresh interval. For more information about LSP refresh intervals, refer to Section 5.18.9, "Managing LSP Refresh Intervals".*

1. Make sure the CLI is in Configuration mode.
2. Add a new interval by typing:

```
routing isis area name max-lsp-lifetime is-type [level-1-2 | level-1-only | level-2-only] interval
seconds
```

   Where:
   - *name* is the unique name for a routing process that belongs to a specific router.
   - *level* is the IS type.
   - *seconds* is the minimum interval in seconds, ranging from 1 to 120. The default value is 30.
3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.18.8.3

Deleting an LSP Lifetime Interval

To delete an LSP lifetime interval for an IS-IS area, do the following:

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

```
no routing isis area name max-lsp-lifetime is-type [level-1-2 | level-1-only | level-2-only]
interval seconds
```

   Where:
   - *name* is the unique name for a routing process that belongs to a specific router.
   - *level* is the IS type.
   - *seconds* is the minimum interval in seconds, ranging from 1 to 120. The default value is 30.
3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.18.9

Managing LSP Refresh Intervals

IS-IS retains Link-State Packets (LSP) in the Link-State Database (LSDB) for only a short period of time unless they are refreshed. By default, LSPs are retained in the LSDB for 1200 seconds (this is referred to as the *lifetime* of the LSP) and are refreshed every 900 seconds.

The refresh interval is configurable for each area and routing type in the IS-IS network.

The following sections describe how to configure and manage refresh intervals for LSPs:

> **NOTE**
> *For information about configuring the lifetime of an LSP, refer to Section 5.18.8, “Managing the Lifetime of LSPs”.*

- Section 5.18.9.1, “Viewing a List of LSP Refresh Intervals”
- Section 5.18.9.2, “Adding an LSP Refresh Interval”
- Section 5.18.9.3, “Deleting an LSP Refresh Interval”

Section 5.18.9.1
Viewing a List of LSP Refresh Intervals

To view a list of LSP refresh intervals configured for an IS-IS area, type:

```
show running-config routing isis area name lsp-refresh-interval
```

Where:

- *name* is the unique name for a routing process that belongs to a specific router.

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

```
ruggedcom# show running-config routing isis area Area_1 lsp-refresh-interval | tab
ISTYPE        INTERVAL
------------------------
level-1-only  60

 !
!
```

If no intervals have been configured, add intervals as needed. For more information, refer to Section 5.18.9.2, “Adding an LSP Refresh Interval”.

Section 5.18.9.2
Adding an LSP Refresh Interval

To add an LSP refresh interval to an IS-IS area, do the following:

> **IMPORTANT!**
> *The LSP refresh interval must be 300 seconds less than the LSP lifetime interval. For more information about LSP refresh intervals, refer to Section 5.18.8, “Managing the Lifetime of LSPs”.*

1. Make sure the CLI is in Configuration mode.
2. Add a new interval by typing:

   ```
   routing isis area name lsp-refresh-interval is-type [level-1-2 | level-1-only | level-2-only]
   interval seconds
   ```

   Where:

   - *name* is the unique name for a routing process that belongs to a specific router.
   - *level* is the IS type.
   - *seconds* is the minimum interval in seconds, ranging from 1 to 120. The default value is 30.
3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.18.9.3
Deleting an LSP Refresh Interval

To delete an LSP refresh interval for an IS-IS area, do the following:

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

```
no routing isis area name lsp-refresh-interval is-type [level-1-2 | level-1-only | level-2-only]
interval seconds
```

   Where:

   - *name* is the unique name for a routing process that belongs to a specific router.
   - *level* is the IS type.
   - *seconds* is the minimum interval in seconds, ranging from 1 to 120. The default value is 30.
3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.18.10
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.

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.*

The following sections describe how to configure and manage NETs for IS-IS areas:

- Section 5.18.10.1, “Viewing a List of NETs”
- Section 5.18.10.2, “Adding a NET”
- Section 5.18.10.3, “Deleting a NET”

Section 5.18.10.1
Viewing a List of NETs

To view a list of areas configured for dynamic IS-IS routes, type:

```
show running-config routing isis area name net
```

Where:

- *name* is the unique name for a routing process that belongs to a specific router.

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

```
ruggedcom# show running-config routing isis area Area_1 net | tab
NET TITLE
---------------------------
49.0001.1921.6800.1001.00

 !
!
```

If no NETs have been configured, add NETs as needed. For more information, refer to Section 5.18.10.2, “Adding a NET”.

Section 5.18.10.2
Adding a NET

To add a Network Entity Title (NET) for an IS-IS area, do the following:

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

   ```
   routing isis area name net title
   ```

   Where:

   - *name* is the unique name for a routing process that belongs to a specific router.
   - *title* is the NET for the router, consisting of a two-octet area ID, a three-octet system ID and a one-octet selector. For example: 0001.1921.6800.1001.00
3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.18.10.3
Deleting a NET

To delete a Network Entity Title (NET) for an IS-IS area, do the following:

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

   ```
   no routing isis area name net title
   ```

   Where:

   - *name* is the unique name for a routing process that belongs to a specific router.
   - *title* is the NET for the router, consisting of a two-octet area ID, a three-octet system ID and a one-octet selector. For example: 0001.1921.6800.1001.00

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

Section 5.18.11
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 understand by the protocol.

There are two types of metrics: internal and external. Both types can be assigned a value between 0 and 63. However, to prevent external metrics from competing with internal metrics, 64 is automatically added to any external metric. This puts external metrics in the range of 64 to 128, even though the metric value defined is only in the range of 0 to 63.

There is no default metric for IS-IS. A metric should be defined for each routing protocol, otherwise a metric value of zero (0) is automatically applied.

The following sections describe how to configure and manage redistribution metrics for IS-IS:

- Section 5.18.11.1, “Viewing a List of Redistribution Metrics”
- Section 5.18.11.2, “Adding a Redistribution Metric”
- Section 5.18.11.3, “Deleting a Redistribution Metric”

Section 5.18.11.1
Viewing a List of Redistribution Metrics

To view a list of redistribution metrics defined for an IS-IS area, type:

```
show running-config routing isis area name redistribute
```

Where:

- *name* is the unique name for a routing process that belongs to a specific router.

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

```
ruggedcom# show running-config routing isis area Area_1 redistribute | tab
                   METRIC
SOURCE  IS TYPE    TYPE      METRIC
-------------------------------------
bgp     level-1-2  internal  10

 !
!
```

If no redistribution metrics have been configured, add metrics as needed. For more information, refer to Section 5.18.11.2, “Adding a Redistribution Metric”.

Section 5.18.11.2

Adding a Redistribution Metric

To add a redistribution metric for an IS-IS area, do the following:

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

```
routing isis area name redistribute source
```

   Where:

   - *name* is the unique name for a routing process that belongs to a specific router.
   - *source* is the protocol transmitting packets over the IS-IS route. Options include bgp, connected, kernel, ospf, rip, and static.

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

Parameter	Description
is-type { is-type }	**Synopsis:** level-1-only, level-2-only, level-1-2 IS type of the IS-IS information, specified as level-1-only, level-2-only or level-1-2. If not provided, uses IS type from area.
metric-type { metric-type }	**Synopsis:** internal, external **Default:** external The IS-IS metric type for redistributed routes. Default is external
metric { metric }	The metric for redistributed routes.

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

Section 5.18.11.3

Deleting a Redistribution Metric

To delete a redistribution metric for an IS-IS area, do the following:

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

```
no routing isis area name redistribute source
```

   Where:

   - *name* is the unique name for a routing process that belongs to a specific router.
   - *source* is the protocol transmitting packets over the IS-IS route. Options include bgp, connected, kernel, ospf, rip, and static.

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

Section 5.19

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.

The following sections describe how to configure and manage BGP:

- Section 5.19.1, “Configuring BGP”
- Section 5.19.2, “Viewing the Status of Dynamic BGP Routes”
- Section 5.19.3, “Managing Route Maps”
- Section 5.19.4, “Managing Prepended and Excluded Autonomous System Paths”
- Section 5.19.5, “Managing Prefix Lists and Entries”
- Section 5.19.6, “Managing Autonomous System Paths and Entries”
- Section 5.19.7, “Managing Neighbors”
- Section 5.19.8, “Managing Networks”
- Section 5.19.9, “Managing Aggregate Addresses”
- Section 5.19.10, “Managing Aggregate Address Options”
- Section 5.19.11, “Managing Redistribution Metrics”

Section 5.19.1

Configuring BGP

To configure dynamic routing with BGP, do the following:

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

Parameter	Description
enabled	Enables BGP.
as-id { as-id }	Autonomous System ID.
always-compare-med	Always comparing MED from different neighbors.
default-local-preference { default-local-preference }	**Default:** 100 Default local preference value.
deterministic-med	Pick the best-MED path among paths advertised from neighboring AS.

Parameter	Description
router-id { router-id }	Router ID for BGP.
external { external }	Distance value for external routes. **Prerequisite:** external, internal and local must all be empty or all be configured.
internal { internal }	Distance value for internal routes. **Prerequisite:** external, internal and local must all be empty or all be configured.
local { local }	Distance value for local routes. **Prerequisite:** external, internal and local must all be empty or all be configured.

3. Configure autonomous system path filters. For more information, refer to Section 5.19.6.3, “Adding an Autonomous System Path Filter”.
4. Configure prefix list filters. For more information, refer to Section 5.19.5.3, “Adding a Prefix List”.
5. Configure route map filters. For more information, refer to Section 5.19.3.3, “Adding a Route Map Filter”.
6. Configure a network. For more information, refer to Section 5.19.8.2, “Adding a Network”.
7. Configure IP addresses for neighbors. For more information, refer to Section 5.19.7.2, “Adding a Neighbor”.
8. Configure aggregate addresses. For more information, refer to Section 5.19.9.2, “Adding an Aggregate Address”.
9. Configure redistribution metrics. For more information, refer to Section 5.19.11.2, “Adding a Redistribution Metric”.
10. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.19.2

Viewing the Status of Dynamic BGP Routes

To view the status of the dynamic BGP routes configured on the device, type:

```
show routing status bgp route
```

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

```
ruggedcom# show routing status bgp route | tab
                                                       LOCAL                AS
NETWORK       ADDRESS      SELECTED  INTERNAL  METRIC  PREFERENCE  WEIGHT  PATH  ORIGIN
-----------------------------------------------------------------------------------------
192.168.1.0
              192.168.1.2  true      true      0       100         0             IGP
192.168.6.0
              2.0.0.1      true      false     0                   0       200   IGP
192.168.12.0
              192.168.1.2  true      true      0       100         0             IGP
192.168.13.0
              0.0.0.0      true      false     0                   32768         IGP
```

The list provides the following information:

Parameter	Description
network	Network.
next-hop	Next-hop address.

Parameter	Description
selected	Selected next-hop for this route.
internal	Internal route.
metric	Metric value.
local-preference	Local preference.
weight	Weight.
as-path	Path.
origin	Origin.

To view the status of the dynamic BGP neighbor configured on the device, type:

```
show routing status bgp neighbor
```

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

```
ruggedcom# show routing status bgp neighbor | tab
                                                                   PREFIX
                              LOCAL                AS
ID           VERSION  AS    MSGRCVD  MSGSENT  UPTIME    STATE        RECEIVED  NETWORK        NEXT HOP
  SELECTED  INTERNAL  METRIC  PREFERENCE  WEIGHT  PATH  ORIGIN
------------------------------------------------------------------------------------------------------------------
13.13.13.2  4        2122  982      984      16:18:04  Established  2
                                                                             13.13.13.0/30  13.13.13.1
  true      false     0                  32768         IGP
                                                                             192.168.12.0   13.13.13.1
  true      false     2                  32768         Unspecified
```

The list provides the following information:

Parameter	Description
id	Neighbor address.
version	BGP version.
as	Remote AS number.
msgrcvd	Number of received BGP messages.
msgsent	Number of sent BGP messages.
uptime	Peer up time.
state	Connection state with this neighbor.
prefix-received	Number of prefixes (networks) received from this neighbor.

Parameter	Description
network	Network.
next-hop	Next-hop address.
selected	Selected next-hop for this route.
internal	Internal route.
metric	Metric value.
local-preference	Local preference.

Parameter	Description
weight	Weight.
as-path	Path.
origin	Origin.

If no dynamic BGP routes have been configured, configure BGP and add routes as needed. For more information about configuring BGP, refer to Section 5.19.1, “Configuring BGP”.

Section 5.19.3

Managing Route Maps

Route maps are sequential statements used to filter routes that meet the defined criteria. If a route meets the criteria of the applied route map, it can either be excluded from the routing table or prevented from being redistributed.

Each route map requires a sequence number (e.g. 10, 20, 30, etc.), which allows for multiple route maps to be run in sequence until a match is found. It is recommended to create sequence numbers in intervals of 10, in case a new route map is required later between two existing route maps.

The following sections describe how to configure and manage route maps for BGP:

- Section 5.19.3.1, “Viewing a List of Route Map Filters”
- Section 5.19.3.2, “Viewing a List of Route Map Filter Entries”
- Section 5.19.3.3, “Adding a Route Map Filter”
- Section 5.19.3.4, “Adding a Route Map Filter Entry”
- Section 5.19.3.5, “Deleting a Routing Map Filter”
- Section 5.19.3.6, “Deleting a Routing Map Filter Entry”
- Section 5.19.3.7, “Configuring Match Rules”
- Section 5.19.3.8, “Configuring a Set”

Section 5.19.3.1

Viewing a List of Route Map Filters

To view a list of route map filters for either dynamic BGP routes, type:

```
show running-config routing bgp filter route-map
```

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

```
ruggedcom# show running-config routing bgp filter route-map | tab
                        ON
                        MATCH  AS     PREFIX  PREFIX  PREFIX                                LOCAL
                  NEXT          ORIGINATOR
TAG   SEQ  ACTION  CALL  GOTO   PATH  LIST    LIST    LIST    METRIC  PEER  ORIGIN  AS  IP  PREFERENCE
 OPERATION  VALUE  HOP   ORIGIN  ID           WEIGHT
---------------------------------------------------------------------------------------------
map
     10   permit  -     -      -     -       -       -       -       -     -       -   -   -
 -          -      -     -       -           -
```

```
!
```

If no filters have been configured, add filters as needed. For more information, refer to Section 5.19.6.3, “Adding an Autonomous System Path Filter”.

Section 5.19.3.2
Viewing a List of Route Map Filter Entries

To view a list of entries for a route map filter for either BGP, type:

```
show running-config routing bgp filter route-map tag entry
```

Where:

- *tag* is the tag for the route map filter

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

```
ruggedcom# show running-config routing bgp filter route-map map entry | tab
                   ON
                   MATCH  AS     PREFIX  PREFIX  PREFIX                                LOCAL
             NEXT          ORIGINATOR
SEQ  ACTION  CALL  GOTO   PATH  LIST    LIST    LIST    METRIC  PEER  ORIGIN  AS  IP  PREFERENCE
 OPERATION  VALUE  HOP   ORIGIN  ID          WEIGHT  AS
---------------------------------------------------------------------------------------------
10   permit  -     -      -     -       -       -       -       -     -       -   -   -           -
      -      -     -       -           -

 !
!
```

If no filters have been configured, add filters as needed. For more information, refer to Section 5.19.6.3, “Adding an Autonomous System Path Filter”.

Section 5.19.3.3
Adding a Route Map Filter

To add a route map filter for dynamic BGP routes, do the following:

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

   ```
   routing bgp filter route-map tag
   ```

   Where:

   - *tag* is the tag for the route map filter
3. Add one or more entries. For more information, refer to Section 5.19.3.4, “Adding a Route Map Filter Entry”.
4. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.19.3.4
Adding a Route Map Filter Entry

To add an entry for an route map filter, do the following:

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

```
routing bgp filter route-map tag entry number
```

   Where:

   - *tag* is the tag for the route map filter
   - *number* is the sequence number for the entry
3. Configure the following parameter(s) as required:

Parameter	Description
action { action }	**Synopsis:** deny, permit **Default:** permit Action.
call { call }	Jump to another route-map after match+set.
on-match-goto { on-match-goto }	Go to this entry on match.

4. Configure the match rules for the route map filter. For more information, refer to Section 5.19.3.7, “Configuring Match Rules”.
5. Configure a set for the route map filter. For more information, refer to Section 5.19.3.8, “Configuring a Set”.
6. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.19.3.5
Deleting a Routing Map Filter

To delete a route map filter for dynamic BGP routes, do the following:

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

```
no routing bgp filter route-map tag
```

   Where:

   - *tag* is the tag for the route map filter
3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.19.3.6
Deleting a Routing Map Filter Entry

To delete an entry for a route map filter, do the following:

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

```
no routing bgp filter route-map tag entry number
```

   Where:

   - *tag* is the tag for the route map filter

- *number* is the sequence number for the entry

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

Section 5.19.3.7
Configuring Match Rules

To configure match rules for a route map filter entry, do the following:

1. Make sure the CLI is in Configuration mode.
2. Navigate to ***routing » bgp » filter » route-map » {tag} » entry » {number} » match***, where *{tag}* is the tag for the route map filter and *{number}* is the sequence number for the entry.
3. Configure the following parameters as required:

Parameter	Description
as-path { as-path }	Match the BGP AS path filter.
metric { metric }	Match the route metric.
peer { peer }	This parameter is not supported and any value is ignored by the system.s
origin { origin }	**Synopsis:** egp, igp, incomplete Match the BGP origin code.
prefix-list { prefix-list }	The prefix list name.
prefix-list { prefix-list }	The prefix list name.
prefix-list { prefix-list }	The prefix list name.

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

Section 5.19.3.8
Configuring a Set

To configure matched rules for a route map filter entry, do the following:

1. Make sure the CLI is in Configuration mode.
2. Navigate to ***routing » bgp » filter » route-map » {tag} » entry » {number} » set***, where *{tag}* is the tag for the route map filter and *{number}* is the sequence number for the entry.
3. Configure the following parameters as required:

Parameter	Description
local-preference { local-preference }	Local preference.
next-hop { next-hop }	**Synopsis:** peer The next hop address (xxx.xxx.xxx.xxx/xx or peer to use peer address).
origin { origin }	**Synopsis:** egp, igp, incomplete The origin code.
originator-id { originator-id }	This parameter is not supported and any value is ignored by the system.

Parameter	Description
weight { weight }	Weight.
as { as }	AS number. **Prerequisite:** as must be empty when ip is not configured.
ip { ip }	IP address of aggregator. **Prerequisite:** ip must be empty when as is not configured.
operation { operation }	**Synopsis:** set, add, sub Set , add or subtract the metric value. **Prerequisite:** Operation must be empty when value is not configured.
value { value }	Value. **Prerequisite:** value must be empty when operation is not configured.

4. Add pre-pended and/or excluded autonomous system paths. For more information, refer to Section 5.19.4.3, “Adding a Prepended Autonomous System Path Filter” and/or Section 5.19.4.4, “Adding an Excluded Autonomous System Path filter”.
5. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.19.4
Managing Prepended and Excluded Autonomous System Paths

The following sections describe how to configure and manage prepended and excluded autonomous system paths:

- Section 5.19.4.1, “Viewing a List of Prepended Autonomous System Path Filters”
- Section 5.19.4.2, “Viewing a List of Excluded Autonomous System Paths”
- Section 5.19.4.3, “Adding a Prepended Autonomous System Path Filter”
- Section 5.19.4.4, “Adding an Excluded Autonomous System Path filter”
- Section 5.19.4.5, “Deleting a Prepended Autonomous System Path Filter”
- Section 5.19.4.6, “Deleting an Excluded Autonomous System Path Filter”

Section 5.19.4.1
Viewing a List of Prepended Autonomous System Path Filters

To view a list of prepended autonomous system path filters configured for a BGP route map entry, type:

```
show running-config routing bgp filter route-map name entry number set as-path prepend
```

Where:

- *name* is the name of the route map
- *number* is the entry number

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

```
ruggedcom# show running-config routing bgp filter route-map route entry 10 set as-path prepend
```

```
routing bgp
 filter route-map route
  entry 10
   set as-path prepend 120
   !
  !
 !
!
```

If no prepended autonomous system path filters have been configured, add filters as needed. For more information, refer to Section 5.19.4.3, “Adding a Prepended Autonomous System Path Filter”.

Section 5.19.4.2
Viewing a List of Excluded Autonomous System Paths

To view a list of excluded autonomous system path filters configured for a BGP route map entry, type:

```
show running-config routing bgp filter route-map name entry number set as-path exclude
```

Where:

- *name* is the name of the route map
- *number* is the entry number

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

```
ruggedcom# show running-config routing bgp filter route-map route entry 10 set as-path exclude
routing bgp
 filter route-map route
  entry 10
   set as-path exclude 110
   !
  !
 !
!
```

If no excluded autonomous system path filters have been configured, add filters as needed. For more information, refer to Section 5.19.4.4, “Adding an Excluded Autonomous System Path filter”.

Section 5.19.4.3
Adding a Prepended Autonomous System Path Filter

To add a prepended autonomous system path filter to a BGP route map entry, do the following:

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

   ```
   routing bgp filter route-map name entry number set as-path prepend path
   ```

   Where:

   - *name* is the name of the route map
   - *number* is the entry number
   - *path* is the number for the autonomous system path
3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.19.4.4

Adding an Excluded Autonomous System Path filter

To add an excluded autonomous system path filter to a BGP route map entry, do the following:

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

```
routing bgp filter route-map name entry number set as-path exclude path
```

   Where:
   - *name* is the name of the route map
   - *number* is the entry number
   - *path* is the number for the autonomous system path
3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.19.4.5

Deleting a Prepended Autonomous System Path Filter

To delete a prepended autonomous system path filter from a BGP route map entry, do the following:

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

```
no routing bgp filter route-map name entry number set as-path prepend path
```

   Where:
   - *name* is the name of the route map
   - *number* is the entry number
   - *path* is the number for the autonomous system path
3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.19.4.6

Deleting an Excluded Autonomous System Path Filter

To delete an excluded autonomous system path filter from a BGP route map entry, do the following:

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

```
no routing bgp filter route-map name entry number set as-path exclude path
```

   Where:
   - *name* is the name of the route map
   - *number* is the entry number
   - *path* is the number for the autonomous system path
3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.19.5
Managing Prefix Lists and Entries

Neighbors can be associated with prefix lists, which allow the BGP daemon to filter incoming or outgoing routes based on the *allow* and *deny* entries in the prefix list.

The following sections describe how to configure and manage prefix lists and entries for dynamic BGP routes:

Section 5.19.5.1
Viewing a List of Prefix Lists

To view a list of prefix lists for dynamic BGP routes, type:

```
routing bgp filter prefix-list
```

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

```
ruggedcom# show running-config routing bgp filter prefix-list | tab
NAME                  DESCBGPTION  SEQ  ACTION  SUBNET           LE  GE
-----------------------------------------------------------------------
list-permit-lan-22    -
                                   100  permit  192.168.33.0/24  -   -
list-withdraw-lan-11  -
                                   100  permit  192.168.33.0/24  -   -
                                   200  permit  192.168.33.0/24  32  -

!
```

If no prefix lists have been configured, add lists as needed. For more information, refer to Section 5.19.5.3, “Adding a Prefix List”.

Section 5.19.5.2
Viewing a List of Prefix Entries

To view a list of entries for dynamic BGP, OSPF, or BGP prefix lists, type:

```
routing bgp filter prefix-list name entry
```

Where:

- *name* is the name of the prefix list

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

```
ruggedcom# show running-config routing bgp filter prefix-list test entry | tab
SEQ  ACTION  SUBNET           LE  GE
---------------------------------------------
5    permit  192.168.40.0/24  32  -
```

```
6    deny    192.168.5.21/32     -   -
 !
!
```

If no entries have been configured, add entries as needed. For more information, refer to Section 5.19.5.4, “Adding a Prefix Entry”.

Section 5.19.5.3
Adding a Prefix List

To add a prefix list for dynamic BGP routes, do the following:

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

   ```
   routing bgp filter prefix-list name
   ```

   Where:

   - *name* is the name of the prefix list
3. Configure the following parameter(s) as required:

Parameter	Description
description { description }	The description of the prefix list.

4. Add prefix entries as needed. For more information, refer to Section 5.19.5.4, “Adding a Prefix Entry”.
5. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.19.5.4
Adding a Prefix Entry

To add an entry for a dynamic BGP prefix list, do the following:

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

   ```
   routing bgp filter prefix-list name entry number
   ```

   Where:

   - *name* is the name of the prefix list
   - *number* is the sequence number for the entry
3. Configure the following parameter(s) as required:

Parameter	Description
action { action }	**Synopsis:** deny, permit **Default:** permit Action.
subnet { subnet }	Network (xxx.xxx.xxx.xxx/xx).

Parameter	Description
le { le }	The maximum prefix length to match ipaddress within subnet.
ge { ge }	The minimum prefix length to match ipaddress within subnet.

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

Section 5.19.5.5
Deleting a Prefix List

To delete a prefix list for dynamic BGP routes, do the following:

1. Make sure the CLI is in Configuration mode.

> **NOTE**
> *Deleting a prefix list removes all associate prefix entries as well.*

2. Delete the list by typing:

```
no routing bgp filter prefix-list name
```

Where:

- *name* is the name of the prefix list

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

Section 5.19.5.6
Deleting a Prefix Entry

To delete an entry for a dynamic BGP prefix list, do the following:

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

```
no routing bgp filter prefix-list name entry number
```

Where:

- *name* is the name of the prefix list
- *number* is the sequence number for the entry

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

Section 5.19.6
Managing Autonomous System Paths and Entries

The following sections describe how to configure and manage autonomous system paths and entries for dynamic BGP routes:

- Section 5.19.6.1, “Viewing a List of Autonomous System Paths”
- Section 5.19.6.2, “Viewing a List of Autonomous System Path Entries”

- Section 5.19.6.3, “Adding an Autonomous System Path Filter”
- Section 5.19.6.4, “Adding an Autonomous System Path Filter Entry”
- Section 5.19.6.5, “Deleting an Autonomous System Path”
- Section 5.19.6.6, “Deleting an Autonomous System Path Filter Entry”

Section 5.19.6.1
Viewing a List of Autonomous System Paths

To view a list of autonomous system path filters for dynamic BGP routes, type:

```
show running-config routing bgp filter as-path
```

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

```
ruggedcom# show running-config routing bgp filter as-path | tab
NAME              ACTION  MATCH
---------------------------------
filter-allow-120
                  permit  120

!
```

If no filters have been configured, add filters as needed. For more information, refer to Section 5.19.6.3, “Adding an Autonomous System Path Filter”.

Section 5.19.6.2
Viewing a List of Autonomous System Path Entries

To view a list of entries for an autonomous system path filter, type:

```
show running-config routing bgp filter as-path name entry
```

Where:

- *name* is the name of the autonomous system path filter

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

```
ruggedcom# show running-config routing bgp filter as-path filter-allow-120 entry | tab
ACTION  MATCH
---------------
permit  120

 !
!
```

If no filters have been configured, add filters as needed. For more information, refer to Section 5.19.6.3, “Adding an Autonomous System Path Filter”.

Section 5.19.6.3
Adding an Autonomous System Path Filter

To add an autonomous system path filter for dynamic BGP routes, do the following:

1. Make sure the CLI is in Configuration mode.

2. Add the new filter by typing:

```
routing bgp filter as-path name
```

Where:

- *name* is the name of the autonomous system path filter

3. Add one or more entries. For more information, refer to Section 5.19.6.4, "Adding an Autonomous System Path Filter Entry".
4. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.19.6.4

Adding an Autonomous System Path Filter Entry

Create an entry for an autonomous system path filter to match a string or integer value in AS path and then perform an action. The match criteria is defined using regular expressions.

To add an entry for an autonomous system path filter, do the following:

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

```
routing bgp filter as-path name entry action match
```

Where:

- *name* is the name of the autonomous system path filter.
- *action* is the action.
- *match* is the regular expression to match with the autonomous system path. For more information about regular expressions, refer to Section 2.6.6, "Using Regular Expressions".

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

Section 5.19.6.5

Deleting an Autonomous System Path

To delete an autonomous system path filter for dynamic BGP routes, do the following:

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

```
no routing bgp filter as-path name
```

Where:

- *name* is the name of the autonomous system path filter

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

Section 5.19.6.6

Deleting an Autonomous System Path Filter Entry

To delete an entry for an autonomous system path filter, do the following:

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

```
no routing bgp filter as-path name entry action match
```

Where:

- *name* is the name of the autonomous system path filter.
- *action* is the action.
- *match* is the regular expression to match with the autonomous system path. For more information about regular expressions, refer to Section 2.6.6, “Using Regular Expressions”.

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

Section 5.19.7

Managing Neighbors

Neighbors are other routers with which to exchange routes. One or more neighbors must be specified in order for BGP to operate.

> **NOTE**
> *If neighbors are specified but no networks are specified, the router will receive BGP routing information from its neighbors but will not advertise any routes to them. For more information about networks, refer to Section 5.19.8, “Managing Networks”.*

The following sections describe how to configure and manage neighbors for dynamic BGP routes:

- Section 5.19.7.1, “Viewing a List of Neighbors”
- Section 5.19.7.2, “Adding a Neighbor”
- Section 5.19.7.3, “Deleting a Neighbor”

Section 5.19.7.1

Viewing a List of Neighbors

To view a list of neighbors configured for a BGP network, type:

```
show running-config routing bgp neighbor
```

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

```
ruggedcom# show running-config routing bgp neighbor
routing bgp
 neighbor 192.168.123.3
  remote-as 100
  no ebgp-multihop
  no maximum-prefix
  no next-hop-self
  no password
  no route-map in
  no route-map out
  no soft-reconfiguration
  no weight
 !
!
```

If no neighbors have been configured, add neighbors as needed. For more information, refer to Section 5.19.7.2, “Adding a Neighbor”.

Section 5.19.7.2
Adding a Neighbor

To add a neighbor for a BGP network, do the following:

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

   ```
   routing bgp neighbor address
   ```

   Where:

   - *address* is the IP address of the neighbor
3. Configure the route map settings by configuring the following parameter(s):

Parameter	Description
in { in }	Apply route map to incoming routes.
out { out }	Apply route map to outbound routes.

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

Parameter	Description
remote-as { remote-as }	A BGP neighbor.
ebgp-multihop { ebgp-multihop }	The maximum hop count. This allows EBGP neighbors not on directly connected networks.
maximum-prefix { maximum-prefix }	The maximum prefix number accepted from this peer.
next-hop-self	Disables the next hop calculation for this neighbor.
password { password }	Password.
update-source { update-source }	Source IP address of routing updates.
disable-connected-check	Disables connection verification when establishing an eBGP peering session with a single-hop peer that uses a loopback interface.
soft-reconfiguration	Per neighbor soft reconfiguration.
weight { weight }	The default weight for routes from this neighbor.

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

Section 5.19.7.3
Deleting a Neighbor

To delete a neighbor from a BGP network, do the following:

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

```
no routing bgp neighbor address
```

Where:

- *address* is the IP address of the neighbor

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

Section 5.19.8

Managing Networks

As opposed to neighbors, which are specific routers with which to exchange routes, networks are groups of routers that are either part of a specific subnet or connected to a specific network interface. They can be used at the same time as neighbors.

> **NOTE**
> *For point to point links, such as T1/E1 links, specify neighbors instead of a network. For more information, refer to Section 5.19.7.2, "Adding a Neighbor".*

> **NOTE**
> *Networks for the BGP protocol do not require a valid entry in the routing table. Since BGP is a broader gateway protocol, a more general network specification would typically be entered. For example, if a routed network inside the Autonomous System (AS) was comprised of many different Class C subnets (/24) of the 192.168.0.0/16 range, it is more efficient to advertise the one Class B network specification, 192.168.0.0/16, to its BGP neighbors.*

> **NOTE**
> *If neighbors are specified but no networks are specified, the router will receive routing information from its neighbors but will not advertise any routes to them. For more information about neighbors, refer to Section 5.19.7, "Managing Neighbors".*

The following sections describe how to configure and manage networks:

- Section 5.19.8.1, "Viewing a List of Networks"
- Section 5.19.8.2, "Adding a Network"
- Section 5.19.8.3, "Deleting a Network"
- Section 5.19.8.4, "Tracking Commands"

Section 5.19.8.1

Viewing a List of Networks

To view a list of networks configured for the BGP protocol, type:

```
show running-config routing bgp network
```

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

```
ruggedcom# show running-config routing bgp network
routing bgp
 network 192.168.12.0/24
 !
 network 192.168.123.0/24
```

```
  !
!
```

If no networks have been configured, add networks as needed. For more information, refer to Section 5.19.8.2, “Adding a Network”.

Section 5.19.8.2
Adding a Network

To add a network for the BGP protocol, do the following:

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

   ```
   routing bgp network address
   ```

   Where:

   - *address* is the IP subnet address and prefix for the network
3. If necessary, configure an event tracker to track network commands. For more information, refer to Section 5.19.8.4, “Tracking Commands”.
4. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.19.8.3
Deleting a Network

To delete a network configured for the BGP protocol, do the following:

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

   ```
   no routing bgp network address
   ```

   Where:

   - *address* is the IP subnet address and prefix for the network
3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.19.8.4
Tracking Commands

Network commands can be tracked using event trackers configured under ***global » tracking***. For more information about event trackers, refer to Section 3.16, “Managing Event Trackers”.

The network command is activated based on the event tracker's state. The `apply-when` parameter determines when the command is activated. For example, if the `apply-when` parameter is set to **down**, the network command becomes active (thereby advertising the network to a router's BGP peers) when the tracked target is unavailable.

To track a command for a BGP network, do the following:

1. Make sure the CLI is in Configuration mode.

2. Navigate to ***routing » bgp » network » {address} » track***, where *{address}* is the IP subnet address and prefix for the network.
3. Configure the following parameter(s) as required:

Parameter	Description
event { event }	Select an event.
apply-when { apply-when }	**Synopsis:** up, down **Default:** up Apply when the tracked event state goes UP or DOWN.

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

Section 5.19.9

Managing Aggregate Addresses

The following sections describe how to configure and manage aggregate addresses:

- Section 5.19.9.1, “Viewing a List of Aggregate Addresses”
- Section 5.19.9.2, “Adding an Aggregate Address”
- Section 5.19.9.3, “Deleting an Aggregate Address”

Section 5.19.9.1

Viewing a List of Aggregate Addresses

To view a list of aggregate addresses for dynamic BGP routes, type:

```
routing bgp aggregate-address
```

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

```
ruggedcom# show running-config routing bgp aggregate-address
routing bgp
 aggregate-address 11.11.0.0/16
  options summary-only
  !
 !
!
```

If no aggregate addresses have been configured, add addresses as needed. For more information, refer to Section 5.19.9.2, “Adding an Aggregate Address”.

Section 5.19.9.2

Adding an Aggregate Address

To add an aggregate address for dynamic BGP routes, do the following:

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

```
routing bgp aggregate-address address
```

Where:

- *address* is the subnet address and prefix for the aggregate address

3. If necessary, configure options for the address. For more information, refer to Section 5.19.10.2, “Adding an Aggregate Address Option”.
4. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.19.9.3
Deleting an Aggregate Address

To delete an aggregate address for dynamic BGP routes, do the following:

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

```
no routing bgp aggregate-address address
```

Where:

- *address* is the subnet address and prefix for the aggregate address

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

Section 5.19.10
Managing Aggregate Address Options

The following sections describe how to configure and manage options for aggregate addresses:

- Section 5.19.10.1, “Viewing a List of Aggregate Address Options”
- Section 5.19.10.2, “Adding an Aggregate Address Option”
- Section 5.19.10.3, “Deleting an Aggregate Address Option”

Section 5.19.10.1
Viewing a List of Aggregate Address Options

To view a list of options for an aggregate address, type:

```
routing bgp aggregate-address address options
```

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

```
ruggedcom# show running-config routing bgp aggregate-address 11.11.0.0/16 options
routing bgp
 aggregate-address 11.11.0.0/16
  options summary-only
  !
 !
!
```

If no options have been configured, add options as needed. For more information, refer to Section 5.19.10.2, “Adding an Aggregate Address Option”.

Section 5.19.10.2

Adding an Aggregate Address Option

To add an option for an aggregate address, do the following:

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

```
routing bgp aggregate-address address options [summary-only | as-set]
```

Where:

• *address* is the subnet address and prefix for the aggregate address

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

Section 5.19.10.3

Deleting an Aggregate Address Option

To delete an option for an aggregate address, do the following:

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

```
no routing bgp aggregate-address address options [summary-only | as-set]
```

Where:

• *address* is the subnet address and prefix for the aggregate address

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

Section 5.19.11

Managing Redistribution Metrics

Redistribution metrics redistribute routing information from other routing protocols, static routes or routes handled by the kernel. Routes for subnets that are directly connected to the router, but not part of the BGP network, can also be advertised.

The following sections describe how to configure and manage redistribution metrics for BGP:

• Section 5.19.11.1, “Viewing a List of Redistribution Metrics”
• Section 5.19.11.2, “Adding a Redistribution Metric”
• Section 5.19.11.3, “Deleting a Redistribution Metric”

Section 5.19.11.1

Viewing a List of Redistribution Metrics

To view a list of redistribution metrics for dynamic BGP routes, type:

```
routing bgp redistribute
```

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

```
ruggedcom# show running-config routing bgp redistribute
routing bgp
 redistribute rip
  no metric
 !
!
```

If no redistribution metrics have been configured, add metrics as needed. For more information, refer to Section 5.19.11.2, “Adding a Redistribution Metric”.

Section 5.19.11.2

Adding a Redistribution Metric

To add a redistribution metric for dynamic BGP routes, do the following:

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

   ```
   routing bgp redistribute [rip | ospf | connected | static | kernel]
   ```

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

Section 5.19.11.3

Deleting a Redistribution Metric

To delete a redistribution metric for dynamic BGP routes, do the following:

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

   ```
   no routing bgp redistribute [rip | ospf | connected | static | kernel]
   ```

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

Section 5.20

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 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 5.21, “Managing OSPF”.

RIP is a legacy routing protocol that has mostly been superseded by OSPF.

NOTE
In complex legacy networks, RIP, OSPF, BGP and IS-IS may all be active on the same router at the same time. Typically, however, only one dynamic routing protocol is employed at one time.

The following sections describe how to configure and manage RIP:

- Section 5.20.1, “Configuring RIP”
- Section 5.20.2, “Viewing the Status of Dynamic RIP Routes”
- Section 5.20.3, “Managing Prefix Lists and Entries”
- Section 5.20.4, “Managing Networks”
- Section 5.20.5, “Managing Network IP Address”
- Section 5.20.6, “Managing Network Interfaces”
- Section 5.20.7, “Managing Neighbors”
- Section 5.20.8, “Managing the Prefix List Distribution”
- Section 5.20.9, “Managing Key Chains and Keys”
- Section 5.20.10, “Managing Redistribution Metrics”
- Section 5.20.11, “Managing Routing Interfaces”

Section 5.20.1

Configuring RIP

To configure dynamic routing using the Routing Information Protocol (RIP) daemon, do the following:

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

Parameter	Description
enabled	Enables the RIP dynamic routing protocol.
default-information-originate	The route element makes a static route only inside RIP. This element should be used only by advanced users who are particularly knowledgeable about the RIP protocol. In most cases, we recommend creating a static route and redistributing it in RIP using the redistribute element with static type.
default-metric { default-metric }	**Default:** 1 Sets the default metric. With the exception of connected route types, the default metric is advertised when a metric has not been configured for a redistributed route. For connected route types, the default metric is 1 despite the value of this parameter.
distance-default { distance-default }	Sets the default RIP distance.
version { version }	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.
update { update }	**Default:** 30

Parameter	Description
	The routing table update timer (in seconds).
timeout { timeout }	**Default:** 180 The routing information timeout timer (in seconds).
garbage { garbage }	**Default:** 120 The garbage collection timer (in seconds).

3. Configure prefix lists. For more information, refer to Section 5.20.3.3, “Adding a Prefix List”.
4. Configure a network. For more information, refer to Section 5.20.4.1, “Configuring a Network”.
5. Configure the prefix list distribution. For more information, refer to Section 5.20.8.2, “Adding a Prefix List Distribution Path”.
6. Configure key chains. For more information, refer to Section 5.20.9.3, “Adding a Key Chain”.
7. Configure redistribution metrics. For more information, refer to Section 5.20.10.2, “Adding a Redistribution Metric”.
8. Configure interfaces. For more information, refer to Section 5.20.11.2, “Configuring a Routing Interface”.
9. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.20.2

Viewing the Status of Dynamic RIP Routes

To view the status of the dynamic RIP routes configured on the device, type:

```
show routing status rip route
```

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

```
ruggedcom# show routing status rip route | tab
NETWORK          TYPE       SUB TYPE   NEXT HOP     METRIC  FROM         TAG  TI
--------------------------------------------------------------------------------
192.168.0.0/24   connected  interface  0.0.0.0      1       self         0
192.168.5.0/24   rip        normal     192.168.0.3  2       192.168.0.3  0    02
192.168.6.0/24   rip        normal     192.168.0.3  2       192.168.0.3  0    02
192.168.50.0/24  connected  interface  0.0.0.0      1       self         0
192.168.60.0/24  connected  interface  0.0.0.0      1       self         0
```

This list provides the following information:

Parameter	Description
network	The network.
type	The route type.
sub-type	The route sub type.
next-hop	The next hop.
metric	The metric value.
from	Where this route comes from.
tag	Tag.

Parameter	Description
time	The route update time.

To view the status of the RIP interfaces configured on the device, type:

```
show routing status rip interface
```

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

```
ruggedcom# show routing status rip interface | tab
                                                    NEXT
NAME         NETWORK           TYPE       SUB TYPE  HOP      METRIC  FROM  TAG  TIME
--------------------------------------------------------------------------------------
switch.1112
             192.168.11.0/24   connected  interface  0.0.0.0  1       self  0
```

This list provides the following information:

Parameter	Description
network	The network.
type	The route type.
sub-type	The route sub type.
next-hop	Next hop.
metric	The metric value.
from	Where this route comes from.
tag	Tag.
time	The route update time.

If no dynamic RIP routes have been configured, configure RIP and add routes as needed. For more information about configuring RIP, refer to Section 5.20.1, “Configuring RIP”.

Section 5.20.3

Managing Prefix Lists and Entries

Neighbors can be associated with prefix lists, which allow the RIPs daemon to filter incoming or outgoing routes based on the *allow* and *deny* entries in the prefix list.

The following sections describe how to configure and manage prefix lists and entries for dynamic RIP routes:

- Section 5.20.3.1, “Viewing a List of Prefix Lists”
- Section 5.20.3.2, “Viewing a List of Prefix Entries”
- Section 5.20.3.3, “Adding a Prefix List”
- Section 5.20.3.4, “Adding a Prefix Entry”
- Section 5.20.3.5, “Deleting a Prefix List”
- Section 5.20.3.6, “Deleting a Prefix Entry”

Section 5.20.3.1
Viewing a List of Prefix Lists

To view a list of prefix lists for dynamic RIP routes, type:

```
show running-config routing rip filter prefix-list
```

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

```
ruggedcom# show running-config routing rip filter prefix-list | tab
NAME                  DESCRIPTION  SEQ  ACTION  SUBNET           LE  GE
-------------------------------------------------------------------------
list-permit-lan-22    -
                                   100  permit  192.168.33.0/24  -   -
list-withdraw-lan-11  -
                                   100  permit  192.168.33.0/24  -   -
                                   200  permit  192.168.33.0/24  32  -

!
```

If no prefix lists have been configured, add lists as needed. For more information, refer to Section 5.20.3.3, "Adding a Prefix List".

Section 5.20.3.2
Viewing a List of Prefix Entries

To view a list of entries for dynamic RIP prefix lists, type:

```
show running-config routing rip filter prefix-list name entry
```

Where:

- *name* is the name of the prefix list

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

```
ruggedcom# show running-config routing rip filter prefix-list test entry | tab
SEQ  ACTION  SUBNET           LE  GE
---------------------------------------------
5    permit  192.168.40.0/24  32  -
6    deny    192.168.5.21/32     -   -

 !
!
```

If no entries have been configured, add entries as needed. For more information, refer to Section 5.20.3.4, "Adding a Prefix Entry".

Section 5.20.3.3
Adding a Prefix List

To add a prefix list for dynamic RIP routes, do the following:

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

```
routing rip filter prefix-list name
```

Where:

- *name* is the name of the prefix list

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

Parameter	Description
description { description }	The description of the prefix list.

4. Add prefix entries as needed. For more information, refer to Section 5.20.3.4, “Adding a Prefix Entry”.
5. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.20.3.4
Adding a Prefix Entry

To add an entry for a dynamic RIP prefix list, do the following:

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

```
routing rip filter prefix-list name entry number
```

Where:

- *name* is the name of the prefix list
- *number* is the sequence number for the entry

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

Parameter	Description
action { action }	**Synopsis:** deny, permit **Default:** permit The action that will be performed.
subnet { subnet }	The IPv4 network address and prefix.
le { le }	The maximum prefix length to be matched.
ge { ge }	The minimum prefix length to be matched.

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

Section 5.20.3.5
Deleting a Prefix List

To delete a prefix list for dynamic RIP routes, do the following:

1. Make sure the CLI is in Configuration mode.

> **NOTE**
> *Deleting a prefix list removes all associate prefix entries as well.*

2. Delete the list by typing:

```
no routing rip filter prefix-list name
```

Where:

- *name* is the name of the prefix list

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

Section 5.20.3.6

Deleting a Prefix Entry

To delete an entry for a dynamic RIP prefix list, do the following:

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

```
no routing rip filter prefix-list name entry number
```

Where:

- *name* is the name of the prefix list
- *number* is the sequence number for the entry

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

Section 5.20.4

Managing Networks

As opposed to neighbors, which are specific routers with which to exchange routes, networks are groups of routers that are either part of a specific subnet or connected to a specific network interface. They can be used at the same time as neighbors.

> **NOTE**
> *For point to point links, such as T1/E1 links, specify neighbors instead of a network. For more information, refer to Section 5.20.7.2, "Adding a Neighbor".*

> **NOTE**
> *RIP v1 does not send subnet mask information in its updates. Any networks defined are restricted to the classic (i.e. Class A, B and C) networks.*

> **NOTE**
> *If neighbors are specified but no networks are specified, the router will receive routing information from its neighbors but will not advertise any routes to them. For more information about neighbors, refer to Section 5.20.7, "Managing Neighbors".*

The following sections describe how to configure and manage networks:

- Section 5.20.4.1, "Configuring a Network"
- Section 5.20.4.2, "Tracking Commands"

Section 5.20.4.1
Configuring a Network

To configure a network for the RIP protocol, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add one or more network IP addresses. For more information, refer to Section 5.20.5.2, “Adding a Network IP Address”.
3. Add one or more network interfaces. For more information, refer to Section 5.20.6.2, “Adding a Network Interface”.
4. Add one or more neighbors. For more information, refer to Section 5.20.7.2, “Adding a Neighbor”.

Section 5.20.4.2
Tracking Commands

Network commands can be tracked using event trackers configured under ***global » tracking***. For more information about event trackers, refer to Section 3.16, “Managing Event Trackers”.

A network command is activated based on the event tracker's state. The `apply-when` parameter determines when the command is activated. For example, if the `apply-when` parameter is set to **`down`**, the network command becomes active (thereby advertising the network to a router's RIP peers) when the tracked target is unavailable.

To track a command for a RIP network, do the following:

1. Make sure the CLI is in Configuration mode.
2. Navigate to ***routing » rip » distribute-prefix-list » {direction} {interface} » track***, where *{direction}* is the direction (incoming or outgoing) in which to filter routing updates and *{interface}* (optional) is the name of the interface.
3. Configure the following parameter(s) as required:

Parameter	Description
event { event }	Selects an event to track. The distribute-prefix-list is applied only when the tracked event is in the UP state.
apply-when { apply-when }	**Synopsis:** up, down **Default:** up Determines when to apply the distribute-prefix-list when the tracked event is in the UP or DOWN state.

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

Section 5.20.5
Managing Network IP Address

The following sections describe how to configure and manage network IP addresses for dynamic RIP routes:

- Section 5.20.5.1, “Viewing a List of Network IP Addresses”
- Section 5.20.5.2, “Adding a Network IP Address”
- Section 5.20.5.3, “Deleting a Network IP Address”

Section 5.20.5.1

Viewing a List of Network IP Addresses

To view a list of IP addresses configured for a RIP network, type:

```
show running-config routing rip network ip
```

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

```
ruggedcom# show running-config routing rip network ip
routing rip
 network ip 192.168.33.0/24
 !
!
```

If no IP addresses have been configured, add addresses as needed. For more information, refer to Section 5.20.5.2, “Adding a Network IP Address”.

Section 5.20.5.2

Adding a Network IP Address

To add an IP address for a RIP network, do the following:

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

   ```
   routing rip network ip address
   ```

   Where:

   - *address* is the IP subnet address and prefix for the network
3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.20.5.3

Deleting a Network IP Address

To delete an IP address from a RIP network, do the following:

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

   ```
   no routing rip network ip address
   ```

   Where:

   - *address* is the IP subnet address and prefix for the network
3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.20.6

Managing Network Interfaces

The following sections describe how to configure and manage interfaces for a RIP network:

- Section 5.20.6.1, "Viewing a List of Network Interfaces"
- Section 5.20.6.2, "Adding a Network Interface"
- Section 5.20.6.3, "Deleting a Network Interface"

Section 5.20.6.1
Viewing a List of Network Interfaces

To view a list of interfaces configured for a RIP network, type:

```
show running-config routing rip network interface
```

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

```
ruggedcom# show running-config routing rip network interface
routing rip
 network interface switch.4084
 !
!
```

If no interfaces have been configured, add neighbors as needed. For more information, refer to Section 5.20.7.2, "Adding a Neighbor".

Section 5.20.6.2
Adding a Network Interface

To add an interface for a RIP network, do the following:

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

   ```
   routing rip network interface name
   ```

   Where:

   - *name* is the name of the interface
3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.20.6.3
Deleting a Network Interface

To delete an interface from a RIP network, do the following:

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

   ```
   no routing rip network interface name
   ```

   Where:

   - *name* is the name of the interface
3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.20.7

Managing Neighbors

Neighbors are other routers with which to exchange routes.

The following sections describe how to configure and manage neighbor IP addresses for dynamic RIP routes:

- Section 5.20.7.1, “Viewing a List of Neighbors”
- Section 5.20.7.2, “Adding a Neighbor”
- Section 5.20.7.3, “Deleting a Neighbor”

Section 5.20.7.1

Viewing a List of Neighbors

To view a list of neighbors configured for a RIP network, type:

```
show running-config routing rip network neighbor
```

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

```
ruggedcom# show running-config routing rip network neighbor
routing rip
 network neighbor 192.168.33.2
 !
!
```

If no neighbors have been configured, add neighbors as needed. For more information, refer to Section 5.20.7.2, “Adding a Neighbor”.

Section 5.20.7.2

Adding a Neighbor

To add a neighbor for a RIP network, do the following:

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

   ```
   routing rip network neighbor address
   ```

   Where:

   - *address* is the IP address of the neighbor
3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.20.7.3

Deleting a Neighbor

To delete a neighbor from a RIP network, do the following:

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

```
no routing rip network neighbor address
```

Where:

- *address* is the IP address of the neighbor

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

Section 5.20.8

Managing the Prefix List Distribution

The following sections describe how to configure and manage the prefix list distribution:

- Section 5.20.8.1, “Viewing a List of Prefix List Distribution Paths”
- Section 5.20.8.2, “Adding a Prefix List Distribution Path”
- Section 5.20.8.3, “Deleting a Prefix List Distribution Path”

Section 5.20.8.1

Viewing a List of Prefix List Distribution Paths

To view a list of prefix list distribution paths for dynamic RIP routes, type:

```
show running-config routing rip distribute-prefix-list
```

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

```
ruggedcom# show running-config routing rip distribute-prefix-list
routing rip
 distribute-prefix-list out ""
  prefix-list list-permit-lan-22
 !
!
```

If no prefix list distribution paths have been configured, add distribution paths as needed. For more information, refer to Section 5.20.8.2, “Adding a Prefix List Distribution Path”.

Section 5.20.8.2

Adding a Prefix List Distribution Path

To add a prefix list distribution path for dynamic RIP routes, do the following:

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

```
routing rip distribute-prefix-list direction interface
```

Where:

- *direction* is the direction (incoming or outgoing) in which to filter routing updates.
- *interface* is the name of the interface. This parameter is optional.

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

Parameter	Description
prefix-list { prefix-list }	The name of the prefix list.

4. If necessary, configure an event tracker to track network commands. For more information, refer to Section 5.20.4.2, “Tracking Commands”.
5. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.20.8.3
Deleting a Prefix List Distribution Path

To delete a prefix list distribution path for dynamic RIP routes, do the following:

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

```
no routing rip distribute-prefix-list direction interface
```

   Where:

   - *direction* is the direction (incoming or outgoing) in which to filter routing updates.
   - *interface* is the name of the interface. This parameter is optional.
3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.20.9
Managing Key Chains and Keys

Key chains are collections of keys (or shared secrets), which are used to authenticate communications over a dynamic RIP network. Only routers with the same key are able to send and receive advertisements.

Multiple key chains can be configured for different groups of interfaces and the lifetime for each key within a chain can be separately configured.

The following sections describe how to configure and manage key chains and keys:

- Section 5.20.9.1, “Viewing a List of Key Chains”
- Section 5.20.9.2, “Viewing a List of Keys”
- Section 5.20.9.3, “Adding a Key Chain”
- Section 5.20.9.4, “Adding a Key”
- Section 5.20.9.5, “Deleting a Key Chain”
- Section 5.20.9.6, “Deleting a Key”

Section 5.20.9.1
Viewing a List of Key Chains

To view a list of key chains for dynamic RIP routes, type:

```
show running-config routing rip key-chain
```

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

```
ruggedcom# show running-config routing rip key-chain
routing rip
 key-chain key-1
  key 1
   key-string RUGGEDCOM
   accept-lifetime start 2013-01-01T01:01:01-00:00
   accept-lifetime expire 2022-01-01T01:01:01-00:00
   send-lifetime start 2013-01-01T01:01:01-00:00
   send-lifetime expire 2022-01-01T01:01:01-00:00
  !
 !
!
```

If no key chains have been configured, add key chains as needed. For more information, refer to Section 5.20.9.3, “Adding a Key Chain”.

Section 5.20.9.2
Viewing a List of Keys

To view a list of keys in a key chain, type:

```
show running-config routing rip rip key-chain name key
```

Where:

- *name* is the name of the key chain

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

```
ruggedcom# show running-config routing rip key-chain key
routing rip
 key-chain key-1
  key 1
   key-string RUGGEDCOM
   accept-lifetime start 2013-01-01T01:01:01-00:00
   accept-lifetime expire 2022-01-01T01:01:01-00:00
   send-lifetime start 2013-01-01T01:01:01-00:00
   send-lifetime expire 2022-01-01T01:01:01-00:00
  !
 !
!
```

If no keys have been configured, add keys as needed. For more information, refer to Section 5.20.9.4, “Adding a Key”.

Section 5.20.9.3
Adding a Key Chain

To add a key chain for dynamic RIP routes, do the following:

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

   ```
   routing rip key-chain name
   ```

   Where:

   - *name* is the name of the key chain

3. Configure one or more keys for the key chain. For more information, refer to Section 5.20.9.4, “Adding a Key”.
4. Configure a routing interface to use the key chain for authentication purposes. For more information, refer to Section 5.20.11.2, “Configuring a Routing Interface”
5. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.20.9.4
Adding a Key

Keys (or shared secrets) are used to authenticate communications over a RIP network. To maintain network stability, each key is assigned an accept and send lifetime.

The *accept* lifetime is the time period in which the key is accepted by the device.

The *send* lifetime is the time period in which they key can be sent to other devices.

This is referred to as hitless authentication key rollover, a method for seamlessly updating authentication keys without having to reset network sessions.

To add a key to a key chain, do the following:

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

```
routing rip key-chain name key id
```

Where:

- *name* is the name of the key chain
- *id* is the ID of the key

3. Configure the key name setting by configuring the following parameter(s):

Parameter	Description
key-string { key-string }	Sets the key string.

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

Parameter	Description
start { start }	**Synopsis:** The date-and-time type is a profile of the ISO 8601 standard for representation of dates and times using the Gregorian calendar. The profile is defined by the date-time production in Section 5.6 of RFC 3339. The date-and-time type is compatible with the dateTime XML schema type with the following notable exceptions: (a) The date-and-time type does not allow negative years. (b) The date-and-time time-offset -00:00 indicates an unknown time zone (see RFC 3339) while -00:00 and +00:00 and Z all represent the same time zone in dateTime. (c) The canonical format (see below) of data-and-time values differs from the canonical format used by the dateTime XML schema type, which requires all times to be in UTC using the time-offset 'Z'. This type is not equivalent to the DateAndTime textual convention of the SMIv2 since RFC 3339 uses a different separator between full-date and full-time and provides higher resolution of time-secfrac. The canonical format for date-and-time values with a known time zone uses a numeric time zone offset that is calculated using the device's configured known offset to UTC time. A change of the device's offset to UTC time will cause date-and-time values to change accordingly. Such changes might happen periodically in case a server follows automatically daylight saving time (DST) time zone offset changes. The canonical format for date-and-time values with an unknown time zone (usually referring to the notion of local time) uses the time-offset -00:00.

Parameter	Description
	The beginning time in which the key is considered valid. **Prerequisite:** The start time cannot be configured unless the expire time is configured.
expire { expire }	**Synopsis:** The date-and-time type is a profile of the ISO 8601 standard for representation of dates and times using the Gregorian calendar. The profile is defined by the date-time production in Section 5.6 of RFC 3339. The date-and-time type is compatible with the dateTime XML schema type with the following notable exceptions: (a) The date-and-time type does not allow negative years. (b) The date-and-time time-offset -00:00 indicates an unknown time zone (see RFC 3339) while -00:00 and +00:00 and Z all represent the same time zone in dateTime. (c) The canonical format (see below) of data-and-time values differs from the canonical format used by the dateTime XML schema type, which requires all times to be in UTC using the time-offset 'Z'. This type is not equivalent to the DateAndTime textual convention of the SMIv2 since RFC 3339 uses a different separator between full-date and full-time and provides higher resolution of time-secfrac. The canonical format for date-and-time values with a known time zone uses a numeric time zone offset that is calculated using the device's configured known offset to UTC time. A change of the device's offset to UTC time will cause date-and-time values to change accordingly. Such changes might happen periodically in case a server follows automatically daylight saving time (DST) time zone offset changes. The canonical format for date-and-time values with an unknown time zone (usually referring to the notion of local time) uses the time-offset -00:00., infinite Expire time. **Prerequisite:** The expire time cannot be configured unless the start time is configured.

5. Configure the send lifetime settings by configuring the following parameter(s):

Parameter	Description
start { start }	**Synopsis:** The date-and-time type is a profile of the ISO 8601 standard for representation of dates and times using the Gregorian calendar. The profile is defined by the date-time production in Section 5.6 of RFC 3339. The date-and-time type is compatible with the dateTime XML schema type with the following notable exceptions: (a) The date-and-time type does not allow negative years. (b) The date-and-time time-offset -00:00 indicates an unknown time zone (see RFC 3339) while -00:00 and +00:00 and Z all represent the same time zone in dateTime. (c) The canonical format (see below) of data-and-time values differs from the canonical format used by the dateTime XML schema type, which requires all times to be in UTC using the time-offset 'Z'. This type is not equivalent to the DateAndTime textual convention of the SMIv2 since RFC 3339 uses a different separator between full-date and full-time and provides higher resolution of time-secfrac. The canonical format for date-and-time values with a known time zone uses a numeric time zone offset that is calculated using the device's configured known offset to UTC time. A change of the device's offset to UTC time will cause date-and-time values to change accordingly. Such changes might happen periodically in case a server follows automatically daylight saving time (DST) time zone offset changes. The canonical format for date-and-time values with an unknown time zone (usually referring to the notion of local time) uses the time-offset -00:00. Sets the time period in which the key on the key chain is considered valid. **Prerequisite:** The start time cannot be configured unless the expire time is configured.
expire { expire }	**Synopsis:** The date-and-time type is a profile of the ISO 8601 standard for representation of dates and times using the Gregorian calendar. The profile is defined by the date-time production in Section 5.6 of RFC 3339. The date-and-time type is compatible with the dateTime XML schema type with the following notable exceptions: (a) The date-and-time type does not allow negative years. (b) The date-and-time time-offset -00:00 indicates an unknown time zone (see RFC 3339) while -00:00 and +00:00 and Z all represent the same time zone in dateTime. (c) The canonical format (see below) of data-and-time values differs from the canonical format used by the dateTime XML schema type, which requires all times to be in UTC using the time-offset 'Z'. This type is not equivalent to the DateAndTime textual convention of the SMIv2 since RFC 3339 uses a different separator between full-date and full-time and provides higher resolution of time-secfrac. The canonical format for date-and-time values with a known time zone uses a numeric time zone offset that is calculated using the device's

Parameter	Description
	configured known offset to UTC time. A change of the device's offset to UTC time will cause date-and-time values to change accordingly. Such changes might happen periodically in case a server follows automatically daylight saving time (DST) time zone offset changes. The canonical format for date-and-time values with an unknown time zone (usually referring to the notion of local time) uses the time-offset -00:00., infinite The time at which the key expires. **Prerequisite:** The expire time cannot be configured unless the start time is configured.

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

Section 5.20.9.5
Deleting a Key Chain

To delete a key chain for dynamic RIP routes, do the following:

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

```
no routing rip key-chain name
```

   Where:
   - *name* is the name of the key chain
3. Type **`commit`** and press **Enter** to save the changes, or type **`revert`** and press **Enter** to abort.

Section 5.20.9.6
Deleting a Key

To delete a key from a key chain, do the following:

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

```
no routing rip key-chain name key id
```

   Where:
   - *name* is the name of the key chain
   - *id* is the ID of the key
3. Type **`commit`** and press **Enter** to save the changes, or type **`revert`** and press **Enter** to abort.

Section 5.20.10
Managing Redistribution Metrics

Redistribution metrics redistribute routing information from other routing protocols, static routes or routes handled by the kernel. Routes for subnets that are directly connected to the router, but not part of the RIP networks, can also be advertised.

The following sections describe how to configure and manage redistribution metrics:

- Section 5.20.10.1, “Viewing a List of Redistribution Metrics”
- Section 5.20.10.2, “Adding a Redistribution Metric”
- Section 5.20.10.3, “Deleting a Redistribution Metric”

Section 5.20.10.1
Viewing a List of Redistribution Metrics

To view a list of redistribution metrics for dynamic RIP routes, type:

```
show running-config routing rip redistribute
```

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

```
ruggedcom# show running-config routing rip redistribute
routing rip
 redistribute bgp
  no metric
 !
!
```

If no redistribution metrics have been configured, add metrics as needed. For more information, refer to Section 5.20.10.2, “Adding a Redistribution Metric”.

Section 5.20.10.2
Adding a Redistribution Metric

To add a redistribution metric for dynamic RIP routes, do the following:

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

   ```
   routing rip redistribute [bgp | ospf | connected | static | kernel]
   ```

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

Section 5.20.10.3
Deleting a Redistribution Metric

To delete a redistribution metric for dynamic RIP routes, do the following:

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

   ```
   no routing rip redistribute [bgp | ospf | connected | static | kernel]
   ```

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

Section 5.20.11

Managing Routing Interfaces

The following sections describe how to configure and manage routing interfaces for dynamic RIP routes:

- Section 5.20.11.1, “Viewing a List of Routing Interfaces”
- Section 5.20.11.2, “Configuring a Routing Interface”

Section 5.20.11.1

Viewing a List of Routing Interfaces

To view a list of routing interfaces for a RIP network, type:

```
show running-config routing rip interface
```

A table or list similar to the following example appears:

```
ruggedcom# show running-config routing rip interface | tab
                   KEY                         RECEIVE  SEND     SPLIT
IFNAME       MODE  CHAIN  STRING  PASSIVE  VERSION  VERSION  HORIZON
----------------------------------------------------------------------
dummy0       -     -      -       -        -        -        yes
fe-cm-1      -     -      -       -        -        -        yes
switch.0001  -     -      -       -        -        -        yes
```

Section 5.20.11.2

Configuring a Routing Interface

To configure a routing interface for a RIP network, do the following:

> **NOTE**
> *OSPF regards router interfaces as either passive or active, sending OSPF messages on active interfaces and ignoring passive interfaces.*

1. Make sure the CLI is in Configuration mode.
2. Navigate to ***routing » rip » interface » {name}***, where *{name}* is the name of the interface.
3. Configure the authentication settings by typing the following commands:

Parameter	Description
mode { mode }	**Synopsis:** md5-rfc, md5-old-ripd, text, none The authentication mode.
key-chain { key-chain }	The authentication key chain.
string { string }	The authentication string.

4. Configure the interface settings by typing the following commands:

Parameter	Description
passive	The specified interface is set to passive mode. In passive mode, all received packets are processed normally and RIPd sends neither multicast nor unicast RIP packets except to RIP neighbors specified with a neighbor element.
receive-version { receive-version }	**Synopsis:** 1, 2, 1,2, 2,1 The version of RIP packets that will be accepted on this interface. By default, version 1 and version 2 packets will be accepted.
send-version { send-version }	**Synopsis:** 1, 2, 1,2, 2,1 The version of RIP to send packets with. By default, version 2 packets will be sent.
split-horizon { split-horizon }	**Synopsis:** yes, no, poisoned-reverse **Default:** yes A split horizon.

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

Section 5.21

Managing OSPF

The Open Path Shortest 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 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.*

The following sections describe how to configure and manage OSPF:

- Section 5.21.1, “OSPF Concepts”
- Section 5.21.2, “Configuring OSPF”
- Section 5.21.3, “Viewing the Status of Dynamic OSPF Routes”
- Section 5.21.4, “Managing Prefix Lists and Entries”

Section 5.21.1
OSPF Concepts

When an OSPF configured router starts operating, it issues a *hello* packet. Routers having the same OSPF Area, hello-interval and dead-interval timers will communicate with each other and are said to be neighbors.

After discovering its neighbors, a router will exchange Link State Advertisements in order to determine the network topology.

Every 30 minutes (by default), the entire topology of the network must be sent to all routers in an area.

If the link speeds are too low, the links are too busy or there are too many routes, some routes may fail to get re-announced and will be aged out.

Splitting the network into smaller areas to reduce the number of routes within an area or reducing the number of routes to be advertised may help to avoid this problem.

In shared access networks (i.e. routers connected by switches or hubs) a designated router and a backup designated are elected to receive route changes from subnets in the area. Once a designated router is picked, all routing state changes are sent to the designated router, which then sends the resulting changes to all the routers.

The election is decided based on the priority assigned to the interface of each router. The highest priority wins. If the priority is tied, the highest router-id wins.

Section 5.21.2
Configuring OSPF

To configure dynamic routing using the Open Shortest Path First (OSPF) daemon, do the following:

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

Parameter	Description
enabled	Enables the OSPF dynamic routing protocol.
abr-type { abr-type }	**Synopsis:** cisco, ibm, shortcut, standard **Default:** cisco The OSPF ABR type.
auto-cost-reference-bandwidth { auto-cost-reference-bandwidth }	**Default:** 100 Calculates the OSPF interface cost according to bandwidth [1-4294967 Mbps]
compatible-rfc1583	Enables the compatibility with the obsolete RFC1583 OSPF (the current is RFC2178)
default-information-originate	Advertises the default route.

Parameter	Description
default-metric { default-metric }	The default metric of redistribute routes.
distance { distance }	The administrative distance.
opaque-lsa	Enables the Opaque-LSA capability (rfc2370).
passive-default	**Default:** true Default passive value for new interface.
refresh-timer { refresh-timer }	**Default:** 10 The refresh timer.
router-id { router-id }	The Router ID for OSPF.
always	**Default:** false Always advertise default route even when there is no default route present in routing table.
metric { metric }	The metric value for default route.
metric-type { metric-type }	**Default:** 2 The mtric type for default route.
route-map { route-map }	The route map name.
external { external }	The administrative distance for external routes.
inter-area { inter-area }	The administrative distance for inter-area routes.
intra-area { intra-area }	The administrative distance for intra-area routes.

3. Configure prefix list filters. For more information, refer to Section 5.21.4.3, “Adding a Prefix List”.
4. Configure areas. For more information, refer to Section 5.21.5.2, “Adding an Area”.
5. Configure route map filters. For more information, refer to Section 5.21.6.3, “Adding a Route Map Filter”.
6. Configure redistribution metrics. For more information, refer to Section 5.21.8.2, “Adding a Redistribution Metric”.
7. Configure interfaces. For more information, refer to Section 5.21.9.2, “Configuring a Routing Interface”.
8. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.21.3
Viewing the Status of Dynamic OSPF Routes

To view the status of the dynamic OSPF routes configured on the device, type:

```
show routing status ospf route network
```

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

```
ruggedcom# show routing status ospf route network | tab
ID              DISCARD  INTER AREA  COST  AREA     HOW
---------------------------------------------------------------------------------
192.168.1.0/24  no       intra area  10    0.0.0.0
                                                    directly attached to fe-1-2
192.168.2.0/24  no       intra area  10    0.0.0.0
                                                    directly attached to fe-1-4
```

This list provides the following information:

Parameter	Description
id	Network Prefix.
discard	This entry is discarded entry.
inter-area	Is path type inter area.
cost	Cost.
area	Area.

To view the status of the dynamic OSPF neighbor configured on the device, type:

```
show routing status ospf neighbor
```

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

```
ruggedcom# show routing status ospf neighbor
                                                                               DEAD
ID            ADDRESS          INTERFACE                    PRIORITY  STATE        TIME
-----------------------------------------------------------------------------------------
21.21.21.21   192.168.212.21   switch.0212:192.168.212.22   1         Full/Backup  31.249s
```

This list provides the following information:

Parameter	Description
id	Neighbor ID.
address	Address.
interface	Interface.
priority	Priority.
state	State.
dead-time	Dead Time.

To view the status of the dynamic OSPF database configured on the device, type:

```
show routing status ospf database
```

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

```
ruggedcom# show routing status ospf database
 router
                                                     LINK
ID            AREA     ADV ROUTER   AGE   SEQNUM      COUNT
------------------------------------------------------------
21.21.21.21   0.0.0.0  21.21.21.21  1307  0x80000017  2
22.22.22.22   0.0.0.0  22.22.22.22  614   0x8000001c  1
22.22.22.22   0.0.0.1  22.22.22.22  1364  0x8000000e  1

 net
ID               AREA     ADV ROUTER   AGE  SEQNUM
-------------------------------------------------------
192.168.212.22  0.0.0.0  22.22.22.22  584  0x80000009

 summary
ID              AREA     ADV ROUTER   AGE   SEQNUM      ROUTE
-------------------------------------------------------------------------
192.168.22.0   0.0.0.0  22.22.22.22  1354  0x80000008  192.168.22.0/24
```

```
192.168.21.0   0.0.0.1  22.22.22.22  1434  0x80000009  192.168.21.0/24
192.168.212.0  0.0.0.1  22.22.22.22  44    0x80000008  192.168.212.0/24

 as-external
                                                METRIC
```

This list provides the following information:

About the router:

Parameter	Description
id	Link ID.
area	Area ID.
adv-router	Advertising Router.
age	Age.
seqnum	Sequence number.
link-count	Link count.

About the net:

Parameter	Description
id	Link ID.
area	Area ID.
adv-router	Advertising Router.
age	Age.
seqnum	Sequence number.

About the summary:

Parameter	Description
id	Link ID.
area	Area ID.
adv-router	Advertising Router.
age	Age.
seqnum	Sequence number.
route	Route.

If no dynamic OSPF routes have been configured, configure OSPF and add routes as needed. For more information about configuring OSPF, refer to Section 5.21.2, “Configuring OSPF”.

Section 5.21.4

Managing Prefix Lists and Entries

Neighbors can be associated with prefix lists, which allow the OSPF daemon to filter incoming or outgoing routes based on the *allow* and *deny* entries in the prefix list.

The following sections describe how to configure and manage prefix lists and entries for dynamic OSPF routes:

- Section 5.21.4.1, “Viewing a List of Prefix Lists”
- Section 5.21.4.2, “Viewing a List of Prefix Entries”
- Section 5.21.4.3, “Adding a Prefix List”
- Section 5.21.4.4, “Adding a Prefix Entry”
- Section 5.21.4.5, “Deleting a Prefix List”
- Section 5.21.4.6, “Deleting a Prefix Entry”

Section 5.21.4.1

Viewing a List of Prefix Lists

To view a list of prefix lists for dynamic OSPF routes, type:

```
routing ospf filter prefix-list
```

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

```
ruggedcom# show running-config routing ospf filter prefix-list | tab
NAME                  DESCOSPFTION  SEQ  ACTION  SUBNET           LE  GE
-------------------------------------------------------------------------
list-permit-lan-22    -
                                    100  permit  192.168.33.0/24  -   -
list-withdraw-lan-11  -
                                    100  permit  192.168.33.0/24  -   -
                                    200  permit  192.168.33.0/24  32  -

!
```

If no prefix lists have been configured, add lists as needed. For more information, refer to Section 5.21.4.3, “Adding a Prefix List”.

Section 5.21.4.2

Viewing a List of Prefix Entries

To view a list of entries for dynamic OSPF, OSPF, or OSPF prefix lists, type:

```
routing ospf filter prefix-list name entry
```

Where:

- *name* is the name of the prefix list

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

```
ruggedcom# show running-config routing ospf filter prefix-list test entry | tab
SEQ  ACTION  SUBNET           LE  GE
---------------------------------------------
5    permit  192.168.40.0/24  32  -
6    deny    192.168.5.21/32     -   -

 !
!
```

If no entries have been configured, add entries as needed. For more information, refer to Section 5.21.4.4, “Adding a Prefix Entry”.

Section 5.21.4.3
Adding a Prefix List

To add a prefix list for dynamic OSPF routes, do the following:

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

```
routing ospf filter prefix-list name
```

Where:

- *name* is the name of the prefix list

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

Parameter	Description
description { description }	The description of the prefix list.

4. Add prefix entries as needed. For more information, refer to Section 5.21.4.4, "Adding a Prefix Entry".
5. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.21.4.4
Adding a Prefix Entry

To add an entry for a dynamic OSPF prefix list, do the following:

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

```
routing ospf filter prefix-list name entry number
```

Where:

- *name* is the name of the prefix list
- *number* is the sequence number for the entry

3. Configure the following parameter(s) as required:

Parameter	Description
action { action }	**Synopsis:** deny, permit **Default:** permit Action.
subnet { subnet }	Network (xxx.xxx.xxx.xxx/xx).
le { le }	The maximum prefix length to match ipaddress within subnet.
ge { ge }	The minimum prefix length to match ipaddress within subnet.

4. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.21.4.5
Deleting a Prefix List

To delete a prefix list for dynamic OSPF routes, do the following:

1. Make sure the CLI is in Configuration mode.

   NOTE
   Deleting a prefix list removes all associate prefix entries as well.

2. Delete the list by typing:

   ```
   no routing ospf filter prefix-list name
   ```

   Where:

   - *name* is the name of the prefix list

3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.21.4.6
Deleting a Prefix Entry

To delete an entry for a dynamic OSPF prefix list, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the entry by typing:

   ```
   no routing ospf filter prefix-list name entry number
   ```

   Where:

   - *name* is the name of the prefix list
   - *number* is the sequence number for the entry

3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.21.5
Managing Areas

Network areas determine the regions within which routes are distributed to other routers. The subnets at a particular router can be added to its OSPF Area. The router will advertise these subnets to all routers in its area.

OSPF areas must be designed such that no single link failure will cause the network to be split into two disjointed networks.

A router can be part of multiple areas and function as a gateway between areas. When multiple areas are used on a network, area zero (0) is the backbone area. All areas must have a router connecting them to area zero (0).

The following sections describe how to configure and manage network areas for dynamic OSPF routes:

- Section 5.21.5.1, “Viewing a List of Areas”
- Section 5.21.5.2, “Adding an Area”
- Section 5.21.5.3, “Deleting an Area”

Section 5.21.5.1

Viewing a List of Areas

To view a list of areas configured for dynamic OSPF routes, type:

```
show running-config routing ospf area
```

If areas have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config routing ospf area | tab
AREA     NETWORK
--------------------------
0.0.0.0  192.168.12.0/24

!
```

If no areas have been configured, add areas as needed. For more information, refer to Section 5.21.5.2, “Adding an Area”.

Section 5.21.5.2

Adding an Area

To add an area for dynamic OSPF routes, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the area by typing:

```
routing ospf area id network/prefix
```

Where:

- *id* is the ID for the OSPF area. The ID must be in the format of *A.B.C.D*.
- *network/prefix* is the network and prefix for the OSPF area.

3. Configure the following parameter(s) as required:

Parameter	Description
shortcut { shortcut }	**Synopsis:** default, disable, enable **Default:** default Sets the area's shortcutting mode. Options include: • Default: If the Area Border Router (ABR) has an active backbone connection, the area is not used for shortcutting and a new bit (S-bit) is not set by the ABR in the router-LSA originated for the area. The opposite is true if the ABR does not have an active backbone connection. • Enable: If the ABR has an active backbone connection, it sets the new bit (S-bit) in the router-LSA originated for the area and uses it for shortcutting. Other ABRs in the area must also report the new bit. However, if the ABR does not have an active backbone connection, it uses the area unconditionally for shortcutting and sets the new bit in the router-LSA originated for the area. • Disable: The ABR does not use this area for shortcutting, or set the new bit (S-bit) in the router-LSA originated for it.

4. Type **`commit`** and press **Enter** to save the changes, or type **`revert`** and press **Enter** to abort.

Section 5.21.5.3
Deleting an Area

To delete an area for dynamic OSPF routes, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the area by typing:

```
no routing ospf area id network/prefix
```

   Where:

   - *id* is the ID for the OSPF area. The ID must be in the format of *A.B.C.D*.
   - *network/prefix* is the network and prefix for the OSPF area.

3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.21.6
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 ROX II, route maps are configured to filter routes based on their metric value, which defines the cost of the route. Once a match is found, the assigned action is taken.

Each route map requires a sequence number (e.g. 10, 20, 30, etc.), which allows for multiple route maps to be run in sequence until a match is found. It is recommended to create sequence numbers in intervals of 10, in case a new route map is required later between two existing route maps.

The following sections describe how to configure and manage route maps for OSPF:

- Section 5.21.6.1, “Viewing a List of Route Map Filters”
- Section 5.21.6.2, “Viewing a List of Route Map Filter Entries”
- Section 5.21.6.3, “Adding a Route Map Filter”
- Section 5.21.6.4, “Adding a Route Map Filter Entry”
- Section 5.21.6.5, “Deleting a Routing Map Filter”
- Section 5.21.6.6, “Deleting a Routing Map Filter Entry”
- Section 5.21.6.7, “Configuring Match Rules”

Section 5.21.6.1
Viewing a List of Route Map Filters

To view a list of route map filters for either dynamic OSPF routes, type:

```
show running-config routing [bgp | ospf] filter route-map
```

If filters have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config routing ospf filter route-map | tab
                        ON
                        MATCH   AS     PREFIX  PREFIX  PREFIX                              LOCAL
                  NEXT          ORIGINATOR
```

```
TAG  SEQ  ACTION  CALL  GOTO   PATH  LIST    LIST    LIST    METRIC  PEER  ORIGIN  AS  IP  PREFERENCE
 OPERATION  VALUE  HOP   ORIGIN  ID          WEIGHT
---------------------------------------------------------------------------------------------
map
     10   permit  -     -      -     -       -       -       -       -     -       -   -   -
 -          -      -     -       -            -

!
```

If no filters have been configured, add filters as needed. For more information, refer to Section 5.21.6.3, "Adding a Route Map Filter".

Section 5.21.6.2

Viewing a List of Route Map Filter Entries

To view a list of entries for a route map filter for either OSPF, type:

```
show running-config routing ospf filter route-map tag entry
```

Where:

- *tag* is the tag for the route map filter

If entries have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config routing ospf filter route-map map entry | tab
                   ON
                   MATCH  AS     PREFIX  PREFIX  PREFIX                              LOCAL
             NEXT          ORIGINATOR
SEQ  ACTION  CALL  GOTO   PATH  LIST    LIST    LIST    METRIC  PEER  ORIGIN  AS  IP  PREFERENCE
 OPERATION  VALUE  HOP   ORIGIN  ID          WEIGHT  AS
---------------------------------------------------------------------------------------------
10   permit  -     -      -     -       -       -       -       -     -       -   -   -           -
      -      -     -       -            -

 !
!
```

If no filters have been configured, add filters as needed. For more information, refer to Section 5.21.6.4, "Adding a Route Map Filter Entry".

Section 5.21.6.3

Adding a Route Map Filter

To add a route map filter for dynamic OSPF routes, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the new filter by typing:

   ```
   routing ospf filter route-map tag
   ```

   Where:

   - *tag* is the tag for the route map filter
3. Add one or more entries. For more information, refer to Section 5.21.6.4, "Adding a Route Map Filter Entry".
4. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.21.6.4
Adding a Route Map Filter Entry

To add an entry for an route map filter, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the new filter by typing:

```
routing ospf filter route-map tag entry number
```

Where:

- *tag* is the tag for the route map filter
- *number* is the sequence number for the entry

3. Configure the following parameter(s) as required:

Parameter	Description
{ seq }	The sequence number of the route-map entry.
action { action }	**Synopsis:** deny, permit **Default:** permit Action.
call { call }	Jump to another route-map after match+set.
on-match-goto { on-match-goto }	Go to this entry on match.
metric { metric }	Metric value.
metric-type { metric-type }	External route type.

4. Configure the match rules for the route map filter. For more information, refer to Section 5.21.6.7, “Configuring Match Rules”.
5. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.21.6.5
Deleting a Routing Map Filter

To delete a route map filter for dynamic OSPF routes, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the filter key by typing:

```
no routing ospf filter route-map tag
```

Where:

- *tag* is the tag for the route map filter

3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.21.6.6
Deleting a Routing Map Filter Entry

To delete an entry for a route map filter, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the filter key by typing:

```
no routing ospf filter route-map tag entry number
```

Where:

- *tag* is the tag for the route map filter
- *number* is the sequence number for the entry

3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.21.6.7

Configuring Match Rules

To configure match rules for a route map filter entry, do the following:

1. Make sure the CLI is in Configuration mode.
2. Navigate to ***routing*** » ***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.
3. Configure the following parameters as required:

Parameter	Description
prefix-list { prefix-list }	The prefix list name.
prefix-list { prefix-list }	The prefix list name.
ifname { ifname }	The interface name.

4. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.21.7

Managing Incoming Route Filters

Incoming route advertisements can be filtered by assigning one or route map filters. This can be useful for excluding specific OSPF routes from the routing table.

NOTE
For more information about route map filters, refer to Section 5.21.6, “Managing Route Maps”.

The following sections describe how to configure and manage incoming route filters:

- Section 5.21.7.1, “Viewing List of Incoming Route Filters”
- Section 5.21.7.2, “Adding an Incoming Route Filter”
- Section 5.21.7.3, “Deleting an Incoming Route Filter”

Section 5.21.7.1
Viewing List of Incoming Route Filters

To view a list of route filters configured for incoming advertised routes, type:

```
show running-config routing ospf incoming-route-filter
```

If route filters have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config routing ospf incoming-route-filter
routing ospf
 incoming-route-filter ospf_route_1
 !
!
```

If noroute filters have been configured, add filters as needed. For more information, refer to Section 5.21.7.2, “Adding an Incoming Route Filter”.

Section 5.21.7.2
Adding an Incoming Route Filter

To add a route filter for incoming advertised routes, do the following:

1. Make sure the CLI is in Configuration mode.
2. Make sure a route map has been configured. For more information, refer to Section 5.21.6, “Managing Route Maps”
3. Create the new incoming route filter by typing:

   ```
   routing ospf incoming-route-filter route-map
   ```

   Where:

   - *route-map* is the name of the route map.
4. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.21.7.3
Deleting an Incoming Route Filter

To delete a route filter configured for incoming advertised routes, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the address by typing:

   ```
   no routing ospf incoming-route-filter route-map
   ```

   Where:

   - *route-map* is the name of the route map.
3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.21.8

Managing Redistribution Metrics

Redistribution metrics redistribute routing information from other routing protocols, static routes or routes handled by the kernel. Routes for subnets that are directly connected to the router, but not part of the OSPF areas, can also be advertised.

The following sections describe how to configure and manage redistribution metrics:

- Section 5.21.8.1, “Viewing a List of Redistribution Metrics”
- Section 5.21.8.2, “Adding a Redistribution Metric”
- Section 5.21.8.3, “Deleting a Redistribution Metric”

Section 5.21.8.1

Viewing a List of Redistribution Metrics

To view a list of redistribution metrics for dynamic OSPF routes, type:

```
routing ospf redistribute
```

If metrics have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config routing ospf redistribute
routing ospf
 redistribute bgp
  no metric-type
  no metric
 !
!
```

If no redistribution metrics have been configured, add metrics as needed. For more information, refer to Section 5.21.8.2, “Adding a Redistribution Metric”.

Section 5.21.8.2

Adding a Redistribution Metric

To add a redistribution metric for dynamic OSPF routes, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the metric by typing:

```
routing ospf redistribute [bgp | rip | connected | static | kernel]
```

3. Configure the following parameter(s) as required:

Parameter	Description
metric-type { metric-type }	**Default:** 2 The OSPF exterior metric type for redistributed routes.
metric { metric }	The metric for redistributed routes.
route-map { route-map }	The route map name.

4. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.21.8.3
Deleting a Redistribution Metric

To delete a redistribution metric for dynamic OSPF routes, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the metric by typing:

```
no routing ospf redistribute [bgp | rip | connected | static | kernel]
```

3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.21.9
Managing Routing Interfaces

The following sections describe how to configure and manage routing interfaces for dynamic OSPF routes:

- Section 5.21.9.1, "Viewing a List of Routing Interfaces"
- Section 5.21.9.2, "Configuring a Routing Interface"

Section 5.21.9.1
Viewing a List of Routing Interfaces

To view a list of routing interfaces for an OSPF network, type:

```
show running-config routing OSPF interface
```

A table or list similar to the following example appears:

```
ruggedcom# show running-config routing ospf interface | tab
                                                   MINIMAL
                                         DEAD      HELLO       HELLO                           RETRANSMIT
 TRANSMIT  KEY
IFNAME       AUTHENTICATION  COST  INTERVAL  MULTIPLIER  INTERVAL  PRIORITY  PASSIVE  INTERVAL    DELAY
     ID   MD5
---------------------------------------------------------------------------------------------
dummy0       -               -     40        -           10        1         true     5           1
fe-cm-1      -               -     40        -           10        1         true     5           1
switch.0001  -               -     40        -           10        1         true     5           1
```

Section 5.21.9.2
Configuring a Routing Interface

To configure a routing interface for an OSPF network, do the following:

1. Make sure the CLI is in Configuration mode.
2. Navigate to ***routing » ospf » interface » {name}***, where *{name}* is the name of the interface.
3. Configure the dead interval settings by typing the following commands:

NOTE
For reliable operation, it is recommended that the `dead-interval` *value be at least four times the number of Hellos per second.*

NOTE
Lower values of `dead-interval` *and* `minimal-hello-multiplier` *will help speed up the change in network routes when the topology of the network changes. It will also increase the load on the router and the links, due to higher traffic caused by the increase in messages.*

Lower values will also put limits on the number of routes that can be distributed within an OSPF network area, as will running over slower links.

IMPORTANT!
The `dead-interval` *and number of Hellos per second must be identical on every router in an OSPF network area.*

Parameter	Description
dead-interval { dead-interval }	**Default:** 40 The time before considering a router dead (in seconds).
minimal-hello-multiplier { minimal-hello-multiplier }	The number of times a hello message can be sent within one second.

4. Configure the interface settings by typing the following commands:

NOTE
Link detection is enabled automatically for active network interfaces. It makes sure the appropriate routing daemon is notified when an interface goes down and stops advertising subnets associated with that interface. The routing daemon resumes advertising the subnet when the link is restored. This allows routing daemons to detect link failures more rapidly, as the router does not have to wait for the ***dead interval*** *to time out. Link detection also causes* ***redistributed*** *routes to start and stop being advertised based on the status of their interface links.*

NOTE
The link cost determines which route to use when multiple links can reach a given destination. By default, OSPF assigns the same cost to all links unless it is provided with extra information about the links. Each interface is assumed to be 10 Mbit, unless otherwise specified by the `auto-cost-bandwidth` *parameter set for the interface. For more information about the* `auto-cost-bandwidth`*, refer to* *Section 5.38.1, "Configuring Costing for Routable Interfaces".*

The default OSPF reference bandwidth for link cost calculations is 100 Mbit. The reference bandwidth divided by the link bandwidth gives the default cost for a link, which by default is 10. If a specific bandwidth is assigned to each link, the costs take this into account.

Link costs can be assigned manually under OSPF to each routable interface. This should be done when the speed of the link should not be used as the method for choosing the best link.

Parameter	Description
authentication { authentication }	**Synopsis:** message-digest, null The authentication type on this interface.

Parameter	Description
cost { cost }	The link cost. If not set, the cost is based on calculation of reference bandwidth divide by interface bandwidth.
hello-interval { hello-interval }	**Default:** 10 The time (in seconds) between sending hello packets.
priority { priority }	**Default:** 1 Priority of interface.
passive	**Default:** true Whether an interface is active or passive. Passive interfaces do not send LSAs to other routers and are not part of an OSPF area.
retransmit-interval { retransmit-interval }	**Default:** 5 Time (in seconds) between retransmitting lost link state advertisements.
transmit-delay { transmit-delay }	**Default:** 1 The link state transmit delay (in seconds).

5. Type **`commit`** and press **Enter** to save the changes, or type **`revert`** and press **Enter** to abort.

Section 5.21.10

Managing Message Digest Keys

Message digest keys use the MD5 algorithm to authenticate OSPF neighbors and prevent unauthorized routers from joining the OSPF network. By enabling authentication and configuring a shared key on all the routers, only routers which have the same authentication key will be able to send and receive advertisements within the OSPF network.

An ID for each key allows the router to use multiple passwords and prevent replay attacks where OSPF packets are captured, modified and transmitted to a router. To change passwords, simply create a new key and delete the old key.

IMPORTANT!
The router can only share routing information with neighbors that use the same authentication method and password.

NOTE
Authentication adds a small overhead due to the encryption of messages. It is not recommended for completely private networks with controlled access.

The following sections describe how to configure and manage message digest keys:

- Section 5.21.10.1, “Viewing a List of Message Digest Keys”
- Section 5.21.10.2, “Adding a Message Digest Key”
- Section 5.21.10.3, “Deleting a Message Digest Key”

Section 5.21.10.1

Viewing a List of Message Digest Keys

To view a list of message digest keys for an OSPF routing interface, type:

```
show running-config routing ospf interface name message-digest-key
```

Where:

- *name* is the name of the routing interface

If keys have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config routing ospf interface switch.0001 message-digest-key
routing ospf
 interface switch.0001
  message-digest-key 1
   md5 RUGGEDCOM
  !
 !
!
```

If no message digest keys have been configured, add keys as needed. For more information, refer to Section 5.21.10.2, “Adding a Message Digest Key”.

Section 5.21.10.2

Adding a Message Digest Key

To add a message digest key to an OSPF routing interface, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the key by typing:

   ```
   routing ospf interface name message-digest-key id
   ```

   Where:

   - *name* is the name of the routing interface
   - *id* is the ID for the message digest key
3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.21.10.3

Deleting a Message Digest Key

To delete a message digest key from an OSPF routing interface, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the key by typing:

   ```
   no routing ospf interface name message-digest-key id
   ```

   Where:

   - *name* is the name of the routing interface
   - *id* is the ID for the message digest key
3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.22

Managing Static Routing

Static routes can be manually added to the routing table when there are no notifications sent by other routers regarding network topology changes.

The following sections describe how to configure and manage static routes:

Section 5.22.1

Viewing a List of Static Routes

To view a list of routable Ethernet ports, type:

```
show running-config routing protocol
```

Where:

- *protocol* is either *IPv4* or *IPv6*

If routes have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config routing ipv4 | tab
                          HW
NETWORK         DISTANCE  ACCELERATE  GW            DISTANCE  INTERFACE    DISTANCE
-------------------------------------------------------------------------------------
0.0.0.0/0       -         -
                                      172.30.128.1  -
                                                              switch.0001  -
10.200.16.0/20  -         -
```

If no static routes have been configured, add routes as needed. For more information, refer to Section 5.22.2, “Adding an IPv4 Static Route” or Section 5.22.3, “Adding an IPv6 Static Route”.

Section 5.22.2

Adding an IPv4 Static Route

To add an IPv4 static route, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the IPv4 static route by typing:

```
routing ipv4 route subnet
```

Where:

- *subnet* is the subnet (network/prefix) of the static route

3. Configure the following parameter(s) as required:

Parameter	Description
hw-accelerate	If the static unicast route can be hardware accelerated, this option will be available. For a static unicast route to be accelerated, the ingress and egress interfaces must be switched.

4. If necessary, configure a black hole connection for the static route. For more information, refer to Section 5.22.5, “Configuring a Black Hole Connection for an IPv4 Static Route”.
5. If necessary, add gateways for the static route. For more information, refer to Section 5.22.6.3, “Adding a Gateway for an IPv4 Static Route”.
6. If necessary, add interfaces for the static route. For more information, refer to Section 5.22.7.3, “Adding an Interface for an IPv4 Static Route”.
7. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.22.3

Adding an IPv6 Static Route

To add an IPv6 static route, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the IPv6 static route by typing:

```
routing static ipv6 subnet
```

Where:

- *subnet* is the subnet (network/prefix) of the static route

3. If necessary, configure either a gateway or an interface for the static route. Only one can be configured per static route. For more informatoin, refer to Section 5.22.6.1, “Configuring Gateways for IPv6 Static Routes” or Section 5.22.7.1, “Configuring Interfaces for IPv6 Static Routes”.
4. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.22.4

Deleting a Static Route

To delete a static route, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the static route by typing:

```
no routing protocol route subnet
```

Where:

- *protocol* is either *IPv4* or *IPv6*
- *subnet* is the subnet (network/prefix) of the static route

3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.22.5

Configuring a Black Hole Connection for an IPv4 Static Route

To configure a black hole connection for an IPV4 static route, do the following:

1. Make sure the CLI is in Configuration mode.
2. Navigate to ***routing » ipv4 » {subnet} » blackhole***, where *subnet* is the subnet (network/prefix) of the static route.
3. Configure the following parameter(s) as required:

Parameter	Description
distance { distance }	**Default:** 1 The distance for this static route's blackhole. Default is 1.

4. Type **`commit`** and press **Enter** to save the changes, or type **`revert`** and press **Enter** to abort.

Section 5.22.6

Managing Gateways for Static Routes

The following sections describe how to configure and manage gateways for static routes:

- Section 5.22.6.1, "Configuring Gateways for IPv6 Static Routes"
- Section 5.22.6.2, "Viewing a List of Gateways for IPv4 Static Routes"
- Section 5.22.6.3, "Adding a Gateway for an IPv4 Static Route"
- Section 5.22.6.4, "Deleting a Gateway for an IPv4 Static Route"

Section 5.22.6.1

Configuring Gateways for IPv6 Static Routes

To configure a gateway address for an IPv6 static route, do the following:

1. Make sure the CLI is in Configuration mode.
2. Navigate to ***routing » ipv6 » route » {subnet} » via***, where *subnet* is the subnet (network/prefix) of the static route.
3. Configure the following parameter(s) as required:

Parameter	Description
gw { gw }	The gateway for the static route.
distance { distance }	The distance for the static route.

4. Type **`commit`** and press **Enter** to save the changes, or type **`revert`** and press **Enter** to abort.

Section 5.22.6.2

Viewing a List of Gateways for IPv4 Static Routes

To view a list of gateway addresses assigned to an IPv4 static route, type:

```
show running-config routing ipv4 route subnet via
```

Where:

- *subnet* is the subnet (network/prefix) of the static route

If gateway addresses have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config routing ipv4 route 0.0.0.0/0 via
routing ipv4 route 0.0.0.0/0
 via 172.30.128.1
  no distance
 !
!
```

If no gateway addresses have been configured, add addresses as needed. For more information, refer to Section 5.22.6.3, “Adding a Gateway for an IPv4 Static Route”.

Section 5.22.6.3

Adding a Gateway for an IPv4 Static Route

To add a gateway address for an IPv4 static route, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the gateway address by typing:

   ```
   routing ipv4 route subnet via gateway
   ```

   Where:

   - *subnet* is the subnet (network/prefix) of the static route
   - *gateway* is the gateway address for the static route
3. Configure the following parameter(s) as required:

Parameter	Description
distance { distance }	The distance for the static route.

4. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.22.6.4

Deleting a Gateway for an IPv4 Static Route

To delete a gateway for an IPv4 static route, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the gateway address by typing:

   ```
   no routing ipv4 route subnet via gateway
   ```

   Where:

- *subnet* is the subnet (network/prefix) of the static route
- *gateway* is the gateway address for the static route

3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.22.7
Managing Interfaces for Static Routes

The following sections describe how to configure and manage interfaces for static routes:

- Section 5.22.7.1, “Configuring Interfaces for IPv6 Static Routes”
- Section 5.22.7.2, “Viewing a List of Interfaces for IPv4 Static Routes”
- Section 5.22.7.3, “Adding an Interface for an IPv4 Static Route”
- Section 5.22.7.4, “Deleting an Interface for an IPv4 Static Route”

Section 5.22.7.1
Configuring Interfaces for IPv6 Static Routes

To configure an interface for an IPv6 static route, do the following:

1. Make sure the CLI is in Configuration mode.
2. Navigate to ***routing*** » ***ipv6*** » ***route*** » ***{subnet}*** » ***dev***, where *subnet* is the subnet (network/prefix) of the static route.
3. Configure the following parameter(s) as required:

Parameter	Description
interface { interface }	The interface for the static route.
distance { distance }	The distance for the static route.

4. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.22.7.2
Viewing a List of Interfaces for IPv4 Static Routes

To view a list of interfaces assigned to an IPv4 static route, type:

```
show running-config routing ipv4 route subnet dev
```

Where:

- *subnet* is the subnet (network/prefix) of the static route

If interfaces have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config routing ipv4 route 0.0.0.0/0 dev
routing ipv4 route 0.0.0.0/0
 dev switch.0001
  no distance
 !
```

```
!
```

If no interfaces have been configured, add interfaces as needed. For more information, refer to Section 5.22.7.3, “Adding an Interface for an IPv4 Static Route”.

Section 5.22.7.3

Adding an Interface for an IPv4 Static Route

To add an interface for an IPv4 static route, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the gateway address by typing:

   ```
   routing ipv4 route subnet dev interface
   ```

   Where:

   - *subnet* is the subnet (network/prefix) of the static route
   - *interface* is the name of the interface for the static route
3. Configure the following parameter(s) as required:

Parameter	Description
distance { distance }	The distance for the static route.

4. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.22.7.4

Deleting an Interface for an IPv4 Static Route

To delete an interface for an IPv4 static route, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the gateway address by typing:

   ```
   no routing ipv4 route subnet dev interface
   ```

   Where:

   - *subnet* is the subnet (network/prefix) of the static route
   - *interface* is the name of the interface for the static route
3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.23

Managing Static Multicast Routing

The following sections describe how to configure and manage static multicast routing:

- Section 5.23.1, “Enabling/Disabling Static Multicast Routing”
- Section 5.23.2, “Managing Static Multicast Groups”

- Section 5.23.3, “Managing Out-Interfaces”

Section 5.23.1
Enabling/Disabling Static Multicast Routing

To enable or disable static multicast routing, do the following:

1. Make sure the CLI is in Configuration mode.
2. Enable static multicast routing by typing:

```
routing multicast static enable
```

Configure the following parameter(s) as required:

Parameter	Description
enabled	Enables static multicast routing service **Prerequisite:** Dynamic and static multicast routing can not be enabled together.

3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.23.2
Managing Static Multicast Groups

The following sections describe how to configure and manage static multicast groups:

- Section 5.23.2.1, “Viewing a List of Static Multicast Groups”
- Section 5.23.2.2, “Adding a Static Multicast Group”
- Section 5.23.2.3, “Deleting a Static Multicast Group”

Section 5.23.2.1
Viewing a List of Static Multicast Groups

To view a list of static multicast groups, type:

```
show running-config routing multicast static
```

If static multicast groups have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config routing multicast static | tab
routing multicast static enabled
routing multicast static mcast-groups
                            MULTICAST     IN            HW
DESCRIPTION   SOURCE IP     IP            INTERFACE     ACCELERATE   IFNAME
------------------------------------------------------------------------------
test.001      169.150.24.12  238.1.12.12  switch.0001   -            fe-cm-1
```

If no static multicast groups have been configured, add groups as needed. For more information about adding static multicast groups, refer to Section 5.23.2.2, “Adding a Static Multicast Group”.

Section 5.23.2.2

Adding a Static Multicast Group

To add a static multicast group, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the multicast group by typing:

```
routing multicast static mcast-groups description
```

Where:

- *description* is the name of the multicast group. Up to 32 characters are allowed, excluding spaces.

3. Configure the following parameter(s) as required:

Parameter	Description
source-ip { source-ip }	The expected source IP address of the multicast packet, in the format xxx.xxx.xxx.xxx. This address is uniquely paired with the multicast address. You cannot use this IP address to create another multicast routing entry with a different Multicast-IP address.
multicast-ip { multicast-ip }	The multicast IP address to be forwarded, in the format xxx.xxx.xxx.xxx The address must be in the range of 224.0.0.0 to 239.255.255.255. This address is uniquely paired with the source IP address. You cannot use this IP address to create another multicast routing entry with a different Source-IP address.
in-interface { in-interface }	The interface upon which the multicast packet arrives.
hw-accelerate	If the multicast route can be hardware accelerated, the option will be available. For a multicast route to be accelerated, the ingress and egress interfaces must be switched.

4. Configure out-interfaces. Refer to Section 5.23.3.2, “Adding an Out-Interface”
5. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.23.2.3

Deleting a Static Multicast Group

To delete a static multicast group, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the multicast group by typing:

```
no routing multicast static mcast-groups description
```

Where:

- *description* is the name of the multicast group to be deleted

3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.23.3

Managing Out-Interfaces

The following sections describe how to configure and manage out-interfaces:

- Section 5.23.3.1, “Viewing a List of Out-Interfaces”

- Section 5.23.3.2, “Adding an Out-Interface”
- Section 5.23.3.3, “Deleting an Out-Interface”

Section 5.23.3.1
Viewing a List of Out-Interfaces

To view a list of out-interfaces, type:

```
show runing-config routing multicast static mcast-group out-interface
```

If out-interfaces have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config routing multicast static mcast-groups out-interface
routing multicast static mcast-groups test
 out-interface fe-cm-1
 !
!
```

If no out-interfaces have been configured, add groups as needed. For more information about adding out-interfaces, refer to Section 5.23.3.2, “Adding an Out-Interface”.

Section 5.23.3.2
Adding an Out-Interface

To add an out-interface, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the out-interface by typing:

   ```
   routing multicast static mcast-groups group out-interface ifname
   ```

   Where:

   - *group* is the name of the multicast group
   - *ifname* is a string of up to 15 characters used to name the out-interface
3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.23.3.3
Deleting an Out-Interface

To delete an out-interface, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the out-interface by typing:

   ```
   no routing multicast static mcast-groups group out-interface ifname
   ```

   Where:

   - *group* is the name of the group with the out-interface to be deleted
   - *ifname* is the name of the out-interface to be deleted
3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.24

Managing Dynamic Multicast Routing

The PIM-SM feature is used for Dynamic Multicast Routing. PIM-SM stands for Protocol Independent Multicast - Sparse Mode. It is a dynamic multicast routing protocol that can dynamically prune and maintain multicast routes. PIM relies on the router's unicast routing table for its capabilities and does not rely on any specific method for learning routes, therefore it is "Protocol Independent".

The following terms are used in PIM-SM:

- **Rendezvous Point**

  The rendezvous point (RP) is a destination in the network (one of the routers), where all multicast traffic is first registered. Whenever a PIM router receives a multicast stream, the source and the multicast address are registered with the rendezvous point.

- **Boot Strap Router**

  A PIM-SM boot strap router (BSR) is a router that announces the location of the rendezvous point to all other PIM routers on the network.

- **Designated Router**

  A designated router (DR) is a router directly attached to a multicast host or device. The router with the highest IP address usually becomes the designated router.

- **Shared Tree**

  The shared tree, also known as the RP-Tree, is a traffic distribution tree which begins from the rendezvous point. The rendezvous point will forward the particular multicast group traffic through this tree whenever there are subscribers for a given multicast flow. Note that the shared tree is on a per-group basis. This means that the shared tree for one group could be different than the shared tree for another on the same network depending on the distribution of the multicast traffic subscribers.

- **Shortest Path Tree**

  The shortest path tree (SPT) is a traffic distribution tree which begins at the source of the multicast traffic or rather the router nearest to the source. The shortest path tree is activated whenever there is a shorter path between the source and the receiver. The shortest path tree can only be triggered by the rendezvous point or the router connected directly to the subscriber.

- **Internet Group Management Protocol**

  Internet Group Management Protocol (IGMP) is the protocol used by hosts and routers to join and leave multicast groups. Routers will send IGMP queries at regular intervals querying whether there are any hosts interested in IP multicast traffic. Whenever an attached host is interested in receiving traffic for a certain group, it will send an IGMP report message expressing its interest. The router will then a) propagate this Join message to another router and b) send the relevant traffic to the segment to which the host is attached.

The following sections describe how to configure and manage PIM-SM:

- Section 5.24.1, “PIM-SM Concepts”
- Section 5.24.2, “Configuring PIM-SM”
- Section 5.24.3, “Viewing a List of PIM-SM Interfaces”
- Section 5.24.4, “Enabling/Disabling a PIM-SM Interface”
- Section 5.24.5, “Configuring a Static RP Address”
- Section 5.24.6, “Managing a Boot Strap Router”
- Section 5.24.7, “Viewing the Status of PIM-SM”

- Section 5.24.8, “Viewing the Status of Dynamic Multicast Routing”

Section 5.24.1
PIM-SM Concepts

When a PIM router receives a subscription from a host, e.g. Host A, for particular multicast traffic, the directly attached designated router (DR) sends a PIM join message for this multicast group towards the rendezvous point (RP). The message is sent hop-by-hop and thus any routers encountering the message would register the group and send the message onwards towards the RP. This would create the shared tree (RP-tree). The tree will not be complete, however, until any sources appear.

When a host or device sends multicast traffic destined to the multicast group subscribed by A, the directly attached designated router takes the traffic, encapsulates it with PIM Register headers and unicasts them to the RP. When the RP receives this traffic, it decapsulates the packets and sends the data towards the subscriber through the RP tree. The routers that receive these packets simply pass them on over the RP-Tree until it reaches the subscriber. Note that there may be other subscribers in the network and the path to those subscribers from the RP is also part of the RP Tree.

After the shared tree has been established, the traffic flows from the source to the RP to the receiver. There are two inefficiencies in this process. One, the traffic is encapsulated at the source and decapsulated at the RP, which may be a performance penalty for a high level of traffic. Two, the traffic may be taking a longer path than necessary to reach its receivers.

After the shared tree has been established, the RP may choose to to send a Join message to the source declaring that it only wants traffic for a group (e.g. group G) from the source (e.g. source S). The DR for the source then starts sending the traffic in multicast form (instead of unicast). Without encapsulation, there is little performance overhead other than what is normal for the traffic when routing in general. The RP will continue sending the traffic over the RP-tree after it receives it. This also means that the traffic may reach the RP-tree before it reaches the RP (in the case where the source branches off the RP-tree itself) which will also have the additional benefit of traffic flowing more efficiently towards receivers that are on the same side of the RP-tree as the source.

If the DR to the receiver decided that traffic coming from the RP-tree was using a suboptimal path than if it was received from the source itself, it would issue a source-specific Join message towards the source. This would then make all intermediate routers register the Join message and then traffic would start flowing along that tree. This is the shortest path tree (SP-tree). At this point, the receiver would receive the traffic from both the RP-tree and the SP-tree. After the flow starts from the SP-tree, the DR will drop the packets from the RP-tree and send a prune message for that traffic towards the RP. This will stop the traffic from arriving from the RP. This scenario will most likely only occur when the traffic has to take a detour when arriving from the RP. Otherwise the RP-tree itself is used.

Section 5.24.2
Configuring PIM-SM

PIM-SM can be used to establish and dynamically manage the Multicast Routing table.

To configure PIM-SM, do the following:

1. Make sure the CLI is in Configuration mode.
2. Navigate to ***routing*** » ***multicast*** » ***dynamic*** » ***pim-sm***.
3. Configure the following parameter(s) as required:

Parameter	Description
enabled	Enable PIM-SM service.
default-preference { default-preference }	**Default:** 1024 Default preference value. Preferences are used by assert elections to determine upstream routers.
default-metric { default-metric }	**Default:** 1024 Default metric value. Metric is the cost of sending data through interface.
broken-cisco-checksum	If your RP is a cisco and shows many PIM_REGISTER checksum errors from this router, setting this option will help.

4. Type **`commit`** and press **Enter** to save the changes, or type **`revert`** and press **Enter** to abort.

Section 5.24.3

Viewing a List of PIM-SM Interfaces

1. Make sure the CLI is in Configuration mode.
2. Navigate to ***routing » multicast » dynamic » pim-sm*** and press **Enter**.
3. At the command prompt, type **`show full-configuration`** and press **Enter**.The PIM-SM interfaces information appears:

```
ruggedcom(config-pim-sm)# show full-configuration | tab
routing multicast dynamic pim-sm
 enabled
 bsr-candidate local-address 1.1.1.1
 bsr-candidate priority 1
 rp-candidate local-address 1.1.1.1
 rp-candidate priority 1
 no broken-cisco-checksum
 interface
IFNAME       PASSIVE
----------------------
dummy0       false
fe-1-1       false
fe-1-16      false
fe-cm-1      true
ge-sm-1      false
switch.0001  true

 group-prefix
PREFIX
--------------
225.0.0.1/32
225.0.0.2/32

!
```

If no PIM-SM interfaces have been configured, enable interfaces as needed. For more information about enabling PIM-SM interfaces, refer to Section 5.24.4, “Enabling/Disabling a PIM-SM Interface”.

Section 5.24.4

Enabling/Disabling a PIM-SM Interface

To enable or disable a PIM-SM interface, do the following:

1. Make sure the CLI is in Configuration mode.
2. The interface is passive by default. Make it active for PIM-SM by typing:

```
no interface ifname passive
```

Where:

- *ifname* is the name of the interface
- *passive* determines whether the interface is passive (default) or active (no passive)

> **NOTE**
> *A maximum of 30 non-passive interfaces can be active for PIM-SM.*

3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.24.5

Configuring a Static RP Address

To configure a Static RP address, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the RP address by typing:

```
routing multicast dynamic pim-sm rp-candidate static-address group-address priority number
```

Where:

- *static-address* is the Static RP (Rendezvous Point) address.
- *group-address* is the multicast group the RP handles.
- *number* sets the priority for this CRP. Smaller value means higher priority.

3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.24.6

Managing a Boot Strap Router

The following sections describe how to configure and manage a Boot Strap Router:

- Section 5.24.6.1, “Configuring a BSR Candidate”
- Section 5.24.6.2, “Configuring a Group Prefix”
- Section 5.24.6.3, “Configuring an RP Candidate”

Section 5.24.6.1
Configuring a BSR Candidate

To configure a BSR candidate, do the following:

1. Make sure the CLI is in Configuration mode.
2. Navigate to ***routing*** » ***multicast*** » ***dynamic*** » ***pim-sm*** » ***bsr-candidate***
3. Configure the following parameters as required:

Parameter	Description
local-address { local-address }	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 { priority }	Bigger value means higher priority

4. Type **`commit`** and press **Enter** to save the changes, or type **`revert`** and press **Enter** to abort.

Section 5.24.6.2
Configuring a Group Prefix

To configure a group-prefix, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the group prefix by typing:

```
routing multicast dynamic pim-sm group-prefix prefix
```

Where:

- *prefix* is the multicast group prefix (for example, 225.1.2.0/24)

> **NOTE**
> *A maximum of 20 group prefixes can be defined for PIM-SM.*

3. Type **`commit`** and press **Enter** to save the changes, or type **`revert`** and press **Enter** to abort.

Section 5.24.6.3
Configuring an RP Candidate

To configure an RP candidate, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the RP candidate by typing:

```
routing multicast dynamic pim-sm RP-candidate local-address timer priority number
```

Where:

- *local-address* is the local address to be used in the Cand-RP messages. If not specified, the largest local IP address will be used (excluding passive interfaces).
- *timer* is the number of seconds to wait between advertising and Cand-RP message.
- *priority* sets the priority for this CRP. Smaller value means higher priority.

3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.24.7
Viewing the Status of PIM-SM

To view the status of PIM-SM, do the following:

1. Make sure the CLI is in Configuration mode.
2. At the command prompt, type **show routing status pim-sm** and press **Enter**. The PIM-SM routing status information appears:

```
ruggedcom# show routing status pim-sm
routing status pim-sm
bsr 1.1.1.1
vinterface
       LOCAL
INDEX  ADDRESS       SUBNET           FLAGS      ID
----------------------------------------------------------------
0      192.168.0.12  192.168.0.0/24   DISABLED
1      169.254.72.4  169.254.72.0/28  DISABLED
2      1.1.1.1       1.1.1.1/32       DR NO-NBR
3      169.254.0.1   169.254.0.0/24   DISABLED
4      192.168.11.1  192.168.11.0/24  DR NO-NBR
5      192.168.12.1  192.168.12.0/24  PIM
                                                 192.168.12.2
6      192.168.14.1  192.168.14.0/24  PIM
                                                 192.168.14.4

rp
ID       PREFIX         PRIORITY  HOLDTIME
--------------------------------------------
3.3.3.3
         225.0.0.1/32   1         105
         225.0.0.2/32   1         105
```

Parameter	Description
local-address	Local address.
subnet	Subnet.
flags	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.

Section 5.24.8
Viewing the Status of Dynamic Multicast Routing

To view the status of dynamic multicast routing, type:

```
show routing status multicast
```

If multicast routes have been configured, a table or list similar to the following example appears:

```
ruggedcom# show routing status multicast
                           IN           OUT
SOURCE          GROUP      INTERFACE    INTERFACE
------------------------------------------------------
192.168.11.101  225.0.0.1  switch.0011  switch.0012 switch.0014
```

Section 5.25

Managing Multicast Filtering

Multicast traffic can be filtered using either static multicast groups, IGMP (Internet Group Management Protocol) snooping, or GMRP (GARP Multicast Registration Protocol).

The following sections describe how to configure and manage multicast filtering:

- Section 5.25.1, “Multicast Filtering Concepts”
- Section 5.25.2, “Enabling and Configuring GMRP”
- Section 5.25.3, “Configuring IGMP Snooping”
- Section 5.25.4, “Managing Router Ports”
- Section 5.25.5, “Managing the Static Multicast Group Table”
- Section 5.25.6, “Managing Egress Ports for Multicast Groups”
- Section 5.25.7, “Viewing a Summary of Multicast Groups”
- Section 5.25.8, “Viewing a List of IP Multicast Groups”

Section 5.25.1

Multicast Filtering Concepts

The following sections describe some of the concepts important to the implementation of multicast filtering in ROX II:

- Section 5.25.1.1, “IGMP”
- Section 5.25.1.2, “GMRP (GARP Multicast Registration Protocol)”

Section 5.25.1.1

IGMP

IGMP is used by IP hosts to report their host group memberships with multicast routers. As hosts join and leave specific multicast groups, streams of traffic are directed to or withheld from that host.

The IGMP protocol operates between multicast routers and IP hosts. When an unmanaged switch is placed between multicast routers and their hosts, the multicast streams will be distributed to all ports.This may introduce significant traffic onto ports that do not require it and receive no benefit from it.

IGMP Snooping, when enabled, will act on IGMP messages sent from the router and the host, restricting traffic streams to the appropriate LAN segments.

Example: IGMP In Operation

The following network diagram provides a simple example of the use of IGMP.

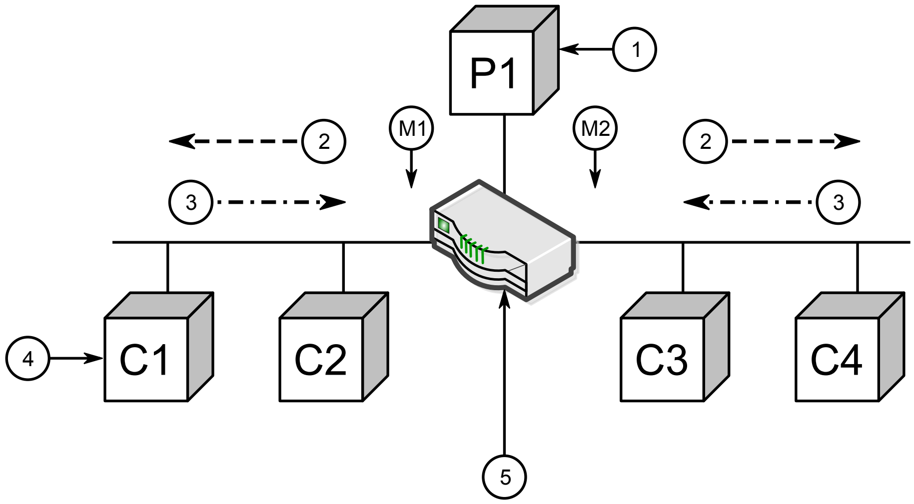

Figure 6: Example – IGMP In Operation

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 frames' 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.

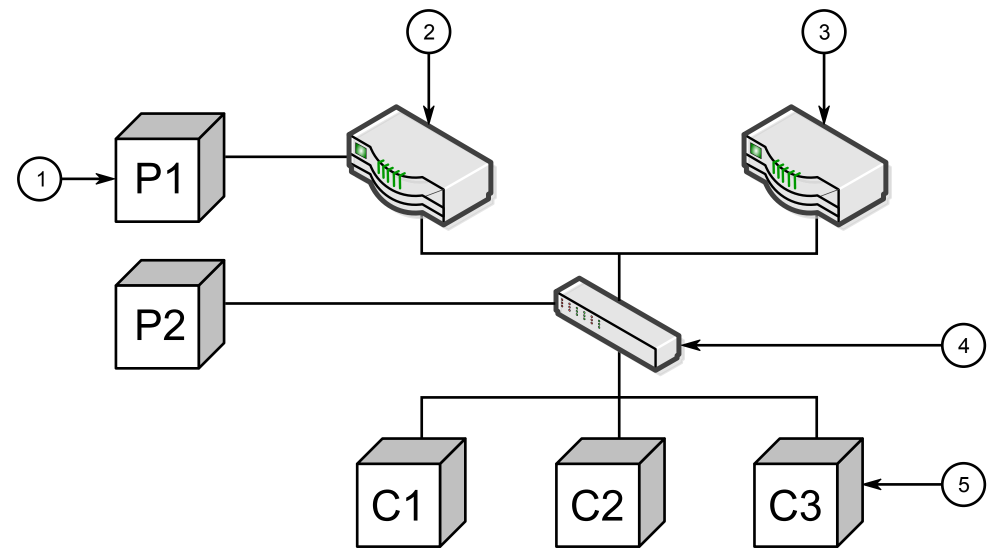

Figure 7: Example – Combined Router and Switch IGMP In Operation

1. Producer **2.** Multicast Router 1 **3.** Multicast Router 2 **4.** Switch **5.** Host

In this example:

- P1, Router 1, Router 2 and C3 are on VLAN 2
- P2 and C2 are on VLAN 3
- C1 is on both VLAN 2 and 3

Assuming that router 1 is the querier for VLAN 2 and router 2 is simply a non-querier, the switch will periodically receive queries from router 1 and maintain the information concerning which port links to the multicast router. However, the switch port that links to router 2 must be manually configured as a *router port*. Otherwise, the switch will send neither multicast streams nor joins/leaves to router 2.

Note that VLAN 3 does not have an external multicast router. The switch should be configured to operate in its *routerless* mode and issue general membership queries as if it is the router.

- **Processing Joins**

  If host C1 wants to subscribe to the multicast streams for both P1 and P2, it will generate two membership reports. The membership report from C1 on VLAN 2 will cause the switch to immediately initiate its own membership report to multicast router 1 (and to issue its own membership report as a response to queries).

The membership report from host C1 for VLAN 3 will cause the switch to immediately begin forwarding multicast traffic from producer P2 to host C2.

- **Processing Leaves**

  When host C1 decides to leave a multicast group, it will issue a leave request to the switch. The switch will poll the port to determine if host C1 is the last member of the group on that port. If host C1 is the last (or only) member, the group will immediately be pruned from the port.

  Should host C1 leave the multicast group without issuing a leave group message and then fail to respond to a general membership query, the switch will stop forwarding traffic after two queries.

  When the last port in a multicast group leaves the group (or is aged-out), the switch will issue an IGMP leave report to the router.

Section 5.25.1.2
GMRP (GARP Multicast Registration Protocol)

The GARP Multicast Registration Protocol (GMRP) is an application of the Generic Attribute Registration Protocol (GARP) that provides a Layer 2 mechanism for managing multicast group memberships in a bridged Layer 2 network. It allows Ethernet switches and end stations to register and unregister membership in multicast groups with other switches on a LAN, and for that information to be disseminated to all switches in the LAN that support Extended Filtering Services.

GMRP is an industry-standard protocol first defined in IEEE 802.1D-1998 and extended in IEEE 802.1Q-2005. GARP was defined in IEEE 802.1D-1998 and updated in 802.1D-2004.

NOTE
GMRP provides similar functionality at Layer 2 to what IGMP provides at Layer 3.

Joining a Multicast Group

In order to join a multicast group, an end station transmits a GMRP *join* message. The switch that receives the *join* message adds the port through which the message was received to the multicast group specified in the message. It then propagates the *join* message to all other hosts in the VLAN, one of which is expected to be the multicast source.

When a switch transmits GMRP updates (from GMRP-enabled ports), all of the multicast groups known to the switch, whether configured manually or learned dynamically through GMRP, are advertised to the rest of network.

As long as one host on the Layer 2 network has registered for a given multicast group, traffic from the corresponding multicast source will be carried on the network. Traffic multicast by the source is only forwarded by each switch in the network to those ports from which it has received join messages for the multicast group.

Leaving a Multicast Group

Periodically, the switch sends GMRP queries in the form of a *leave all* message. If a host (either a switch or an end station) wishes to remain in a multicast group, it reasserts its group membership by responding with an appropriate *join* request. Otherwise, it can either respond with a *leave* message or simply not respond at all. If the switch receives a *leave* message or receives no response from the host for a timeout period, the switch removes the host from the multicast group.

Notes About GMRP

Since GMRP is an application of GARP, transactions take place using the GARP protocol. GMRP defines the following two Attribute Types:

- The Group Attribute Type, used to identify the values of group MAC addresses
- The Service Requirement Attribute Type, used to identify service requirements for the group

Service Requirement Attributes are used to change the receiving port's multicast filtering behavior to one of the following:

- Forward All Multicast group traffic in the VLAN, or
- Forward All Unknown Traffic (Multicast Groups) for which there are no members registered in the device in a VLAN

If GMRP is disabled on the RX1500, GMRP packets received will be forwarded like any other traffic. Otherwise, GMRP packets will be processed by the 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.

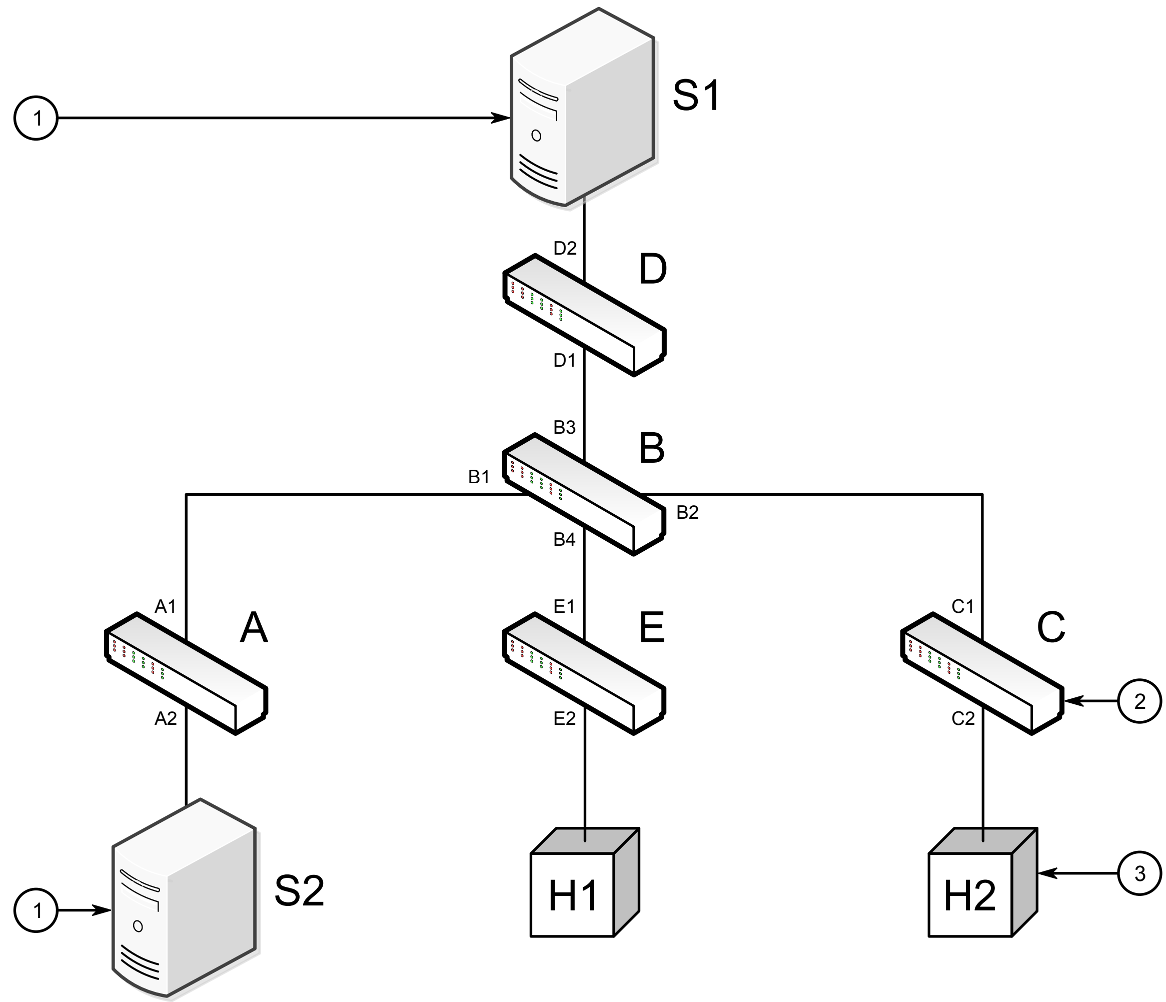

Figure 8: Example – Establishing Membership with GMRP

1. Multicast Source **2.** Switch **3.** Multicast Host

The hosts and switches establish membership with the Multicast Group 1 and 2 as follows:

- 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.
- 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.
- Switch B propagates the *join* message, causing Ports A1, C1 and D1 to become members of Multicast Group 1.
- 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.
- Switch C propagates the *join* message, causing Ports A1, B2, D1 and E1 to become members of Multicast Group 2.

Once GMRP-based registration has propagated through the network, multicast traffic from S1 and S2 can reach its destination as follows:

- Source S1 transmits multicast traffic to Port D2 which is forwarded via Port D1, which has previously become a member of Multicast Group 1.
- Switch B forwards the Group 1 multicast via Port B4 towards Switch E.
- Switch E forwards the Group 1 multicast via Port E2, which has been statically configured for membership in Multicast Group 1.
- Host H1, connected to Port E2, thus receives the Group 1 multicast.
- Source S2 transmits multicast traffic to Port A2, which is then forwarded via port A1, which has previously become a member of Multicast Group 2.
- Switch B forwards the Group 2 multicast via Port B2 towards Switch C.
- Switch C forwards the Group 2 multicast via Port C2, which has previously become a member of Group 2.
- Ultimately, Host H2, connected to Port C2, receives the Group 2 multicast.

Section 5.25.2

Enabling and Configuring GMRP

To enable and configure GMRP (GARP Multicast Registration Protocol), do the following:

1. Make sure the CLI is in Configuration mode.
2. Navigate to ***switch » mcast-filtering*** and configure the following parameter(s) as required:

Parameter	Description
enabled	**Default:** false GMRP Enable
rstp-flooding	Determines whether or not multicast streams will be flooded out of all Rapid Spanning Tree Protocol (RSTP) non-edge ports upon detection of a topology change. Such flooding is desirable, if multicast stream delivery must be guaranteed without interruption.
leave-timer { leave-timer }	**Default:** 4000 The time in milliseconds to wait after issuing Leave or LeaveAll before removing registered multicast groups. If Join messages for specific addresses are received before this timer expires, the addresses will be kept registered.

3. Enable GMRP on one or more switched Ethernet ports. For more information, refer to Section 3.17.2, “Configuring a Switched Ethernet Port”.
4. Type `commit` and press **Enter** to save the changes, or type `revert` and press **Enter** to abort.

Section 5.25.3

Configuring IGMP Snooping

To configure IGMP snooping, do the following:

1. Make sure the CLI is in Configuration mode.
2. Navigate to ***switch » mcast-filtering » igmp-snooping*** and configure the following parameter(s) as required:

Parameter	Description
igmp-mode { igmp-mode }	**Synopsis:** active, passive **Default:** passive Specifies the IGMP mode: • PASSIVE : The switch passively snoops IGMP traffic and never sends IGMP queries. • ACTIVE : The switch generates IGMP queries, if no queries from a better candidate for the querier are detected for a while.
igmp-query-interval { igmp-query-interval }	**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	**Default:** true Whether or not multicast streams will always be forwarded to multicast routers.
rstp-flooding	Whether or not multicast streams will be flooded out of all Rapid Spanning Tree Protocol (RSTP) non-edge ports upon detection of a topology change. Such flooding is desirable, if multicast stream delivery must be guaranteed without interruption.

3. Assign one or more ports for IGMP to use when sending Membership Reports. For more information, refer to Section 5.25.4.2, “Adding a Router Port”.
4. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.25.4
Managing Router Ports

The following sections describe how to configure and manage router ports used for IGMP snooping:

- Section 5.25.4.1, “Viewing a List of Router Ports”
- Section 5.25.4.2, “Adding a Router Port”
- Section 5.25.4.3, “Deleting a Router Port”

Section 5.25.4.1
Viewing a List of Router Ports

To view a list of router ports used for IGMP snooping, type:

```
show running-config switch mcast-filtering igmp-snooping router-ports
```

If router ports have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config switch mcast-filtering igmp-snooping router-ports | tab
SLOT  PORT
------------
lm1   1

 !
!
```

If no router ports have been configured, add ports as needed. For more information, refer to Section 5.25.4.2, “Adding a Router Port”.

Section 5.25.4.2
Adding a Router Port

To add a router port for IGMP snooping, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the router port by typing:

```
switch mcast-filtering igmp-snooping router-ports slot port
```

Where:

- *slot* is the name of the module location
- *port* is the port number (or a list of ports, if aggregated in a port trunk) for the module

3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.25.4.3
Deleting a Router Port

To delete a router port for IGMP snooping, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the router port by typing:

```
no switch mcast-filtering igmp-snooping router-ports slot port
```

Where:

- *slot* is the name of the module location
- *port* is the port number (or a list of ports, if aggregated in a port trunk) for the module

3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.25.5
Managing the Static Multicast Group Table

The following sections describe how to configure and manage a list of known static multicast groups on other devices:

- Section 5.25.5.1, “Viewing a List of Static Multicast Group Entries”
- Section 5.25.5.2, “Adding a Static Multicast Group Entry”
- Section 5.25.5.3, “Deleting a Static Multicast Group Entry”

Section 5.25.5.1
Viewing a List of Static Multicast Group Entries

To view a list of entries for known static multicast groups on other devices, type:

```
show running-config switch mcast-filtering static-mcast-table
```

If entries have been established, a table or list similar to the following example appears:

```
ruggedcom# show running-config switch mcast-filtering static-mcast-table
switch mcast-filtering
 static-mcast-table 10 01:00:00:01:01:01
 !
!
```

If no entries have been configured, add entries as needed. For more information, refer to Section 5.25.5.2, "Adding a Static Multicast Group Entry".

Section 5.25.5.2

Adding a Static Multicast Group Entry

To list a static multicast group from another device in the Static Multicast Summary table, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the table entry by typing:

   > **NOTE**
   > *Letters in MAC addresses must be lowercase.*

   ```
   switch mcast-filtering static-mcast-table id address
   ```

   Where:

   - *id* is the ID for the VLAN upon which the static multicast group operates
   - *address* is the MAC address for the device in the form of 01:xx:xx:xx:xx:xx
3. Add one or more egress ports. For more information, refer to Section 5.25.6.2, "Adding an Egress Port".
4. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.25.5.3

Deleting a Static Multicast Group Entry

To delete a static multicast group from the Static Multicast Summary table, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the table entry by typing:

   ```
   no switch mcast-filtering static-mcast-table id address
   ```

   Where:

   - *id* is the ID for the VLAN upon which the static multicast group operates
   - *address* is the MAC address for the device in the form of 01:xx:xx:xx:xx:xx
3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.25.6

Managing Egress Ports for Multicast Groups

The following sections describe how to configure and manage egress ports for multicast groups:

- Section 5.25.6.1, “Viewing a List of Egress Ports”
- Section 5.25.6.2, “Adding an Egress Port”
- Section 5.25.6.3, “Deleting an Egress Port”

Section 5.25.6.1
Viewing a List of Egress Ports

To view a list of egress ports for a static multicast group defined in the Static Multicast Group Summary table, type:

```
show switch mcast-filtering static-mcast-table id address egress-ports
```

Where:

- *id* is the ID for the VLAN upon which the static multicast group operates
- *address* is the MAC address for the device in the form of 01:xx:xx:xx:xx:xx

If egress ports have been established, a table or list similar to the following example appears:

```
ruggedcom# show running-config switch mcast-filtering static-mcast-table 10 01:00:00:01:01:01 egress-
ports
switch mcast-filtering
 static-mcast-table 10 01:00:00:01:01:01
  egress-ports lm2 1
  !
 !
!
```

If no egress ports have been configured, add egress ports as needed. For more information, refer to Section 5.25.6.2, “Adding an Egress Port”.

Section 5.25.6.2
Adding an Egress Port

To add an egress port to a static multicast group defined in the Static Multicast Group Summary table, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the egress port by typing:

   ```
   switch mcast-filtering static-mcast-table id address egress-ports slot port
   ```

   Where:

   - *id* is the ID for the VLAN upon which the static multicast group operates
   - *address* is the MAC address for the device in the form of 01:xx:xx:xx:xx:xx
   - *slot* is the name of the module location
   - *port* is the port number (or a list of ports, if aggregated in a port trunk) for the module
3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.25.6.3

Deleting an Egress Port

To delete an egress port for a static multicast group defined in the Static Multicast Group Summary table, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the table entry by typing:

```
no switch mcast-filtering static-mcast-table id address egress-ports slot port
```

   Where:

   - *id* is the ID for the VLAN upon which the static multicast group operates
   - *address* is the MAC address for the device in the form of 01:xx:xx:xx:xx:xx
   - *slot* is the name of the module location
   - *port* is the port number (or a list of ports, if aggregated in a port trunk) for the module

3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.25.7

Viewing a Summary of Multicast Groups

To view a summary of all multicast groups, type:

```
show switch mcast-filtering mcast-group-summary
```

If multicast groups have been configured, a table or list similar to the following example appears:

```
ruggedcom# show switch mcast-filtering mcast-group-summary
                        STATIC  STATIC  GMRP  GMRP
VID  MAC                SLOT    PORTS   SLOT  PORTS
-----------------------------------------------------
10   01:00:00:01:01:01
                        lm1     4
```

This table or list provides the following information:

Parameter	Description
vid	The VLAN Identifier of the VLAN upon which the multicast group operates.
mac	The multicast group MAC address.

Section 5.25.8

Viewing a List of IP Multicast Groups

To view a list of all multicast groups, type:

```
show switch mcast-filtering ip-mcast-groups
```

If IP multicast groups have been configured, a table or list similar to the following example appears:

```
RX5000-88G-20# show switch mcast-filtering ip-mcast-groups
     IP                              JOINED  JOINED  ROUTER  ROUTER
```

```
VID  ADDRESS    MAC                SLOT    PORTS   SLOT    PORTS
-------------------------------------------------------------------
100  225.0.1.1  01:00:5e:00:01:01
                                   lm1     3
                                                   lm1     1
200  225.0.1.2  01:00:5e:00:01:02
                                   lm1     4
                                                   lm1     2
```

This table or list provides the following information:

Parameter	Description
vid	The VLAN Identifier of the VLAN upon which the multicast group operates.
ip-address	**Synopsis:** The ipv4-address type represents an IPv4 address in dotted-quad notation. The IPv4 address may include a zone index, separated by a % sign. The zone index is used to disambiguate identical address values. For link-local addresses, the zone index will typically be the interface index number or the name of an interface. If the zone index is not present, the default zone of the device will be used. The canonical format for the zone index is the numerical format The multicast group IP address.

Section 5.26
Managing VRRP

The Virtual Router Redundancy Protocol is a gateway redundancy protocol. VRRP provides a gateway failover mechanism that is invisible to the hosts and other devices that send traffic through that gateway. The Virtual Router Redundancy Protocol (VRRP) eliminates a single point of failure associated with statically routed networks by providing automatic failover using alternate routers. The 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 ROX II.*

The following sections describe how to configure VRRP:

- Section 5.26.1, “VRRP Concepts”
- Section 5.26.2, “Viewing the Status of VRRP”
- Section 5.26.3, “Enabling/Disabling VRRP”
- Section 5.26.4, “Managing VRRP Trackers”
- Section 5.26.5, “Managing VRRP Groups”
- Section 5.26.6, “Managing VRRP Instances”
- Section 5.26.7, “Managing VRRP Monitors”
- Section 5.26.8, “Managing Track Scripts”
- Section 5.26.9, “Managing Virtual IP Addresses”

Section 5.26.1

VRRP Concepts

The following sections describe some of the concepts important to the implementation of VRRP in ROX II:

- Section 5.26.1.1, “Static Routing vs. VRRP”
- Section 5.26.1.2, “VRRP Terminology”

Section 5.26.1.1

Static Routing vs. VRRP

Many network designs employ a statically configured default gateway in the network hosts. A static default gateway is simple to configure, requires little if any overhead to run, and is supported by virtually every IP implementation. When the Dynamic Host Configuration Protocol (DHCP) is employed, hosts may accept a configuration for only a single default gateway.

Unfortunately, this approach creates a single point of failure. Loss of the router supplying the default gateway, or the router’s WAN connection, results in isolating the hosts that rely upon the default gateway.

There are a number of ways to provide redundant connections for the hosts. Some hosts can configure alternate gateways while others are intelligent enough to participate in dynamic routing protocols such as the Routing Information Protocol (RIP) or Open Shortest Path First (OSPF) routing protocol. Even when available, these approaches are not always practical due to administrative and operation overhead.

VRRP solves the problem by allowing the establishment of a *virtual router group*, composed of a number of routers that provide one gateway IP. VRRP uses an election protocol to dynamically assign responsibility for the gateway to one of the routers in the group. This router is called the Master.

If the Master (or, optionally, a condition) fails, the alternate (or backup) routers in the group elect a new Master. The new master owns the virtual IP address and issues a gratuitous ARP to inform the network of where the gateway can be reached.

Since the host’s default route and MAC address does not change, packet loss at the hosts is limited to the amount of time required to elect a new router.

Section 5.26.1.2

VRRP Terminology

Each physical router running VRRP is known as a VRRP Router. Two or more VRRP Routers can be configured to form a *Virtual Router*. Each VRRP Router may participate in one or more Virtual Routers.

Each Virtual Router has a user-configured Virtual Router Identifier (VRID) and a Virtual IP address or set of IP addresses on the shared LAN. Hosts on the shared LAN are configured to use these addresses as the default gateway.

Each router in the Virtual Router Group has a specific priority, which is a number between 1 and 255. The router with the highest priority (or highest number) is elected the Master, while all other routers are considered Backups.

On RX1500 devices with 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.

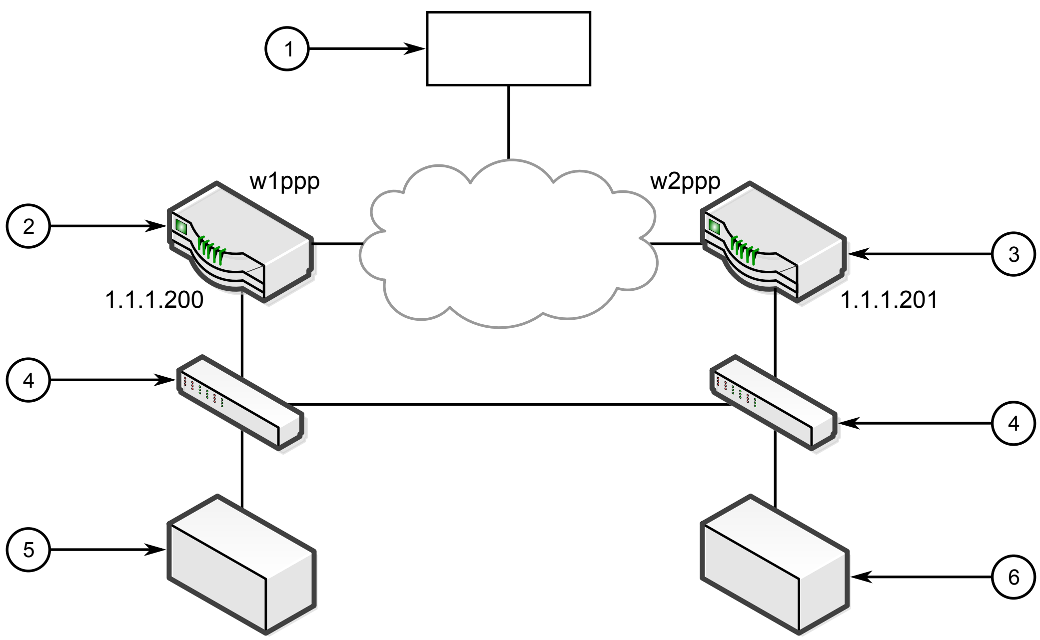

Figure 9: VRRP Example

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.

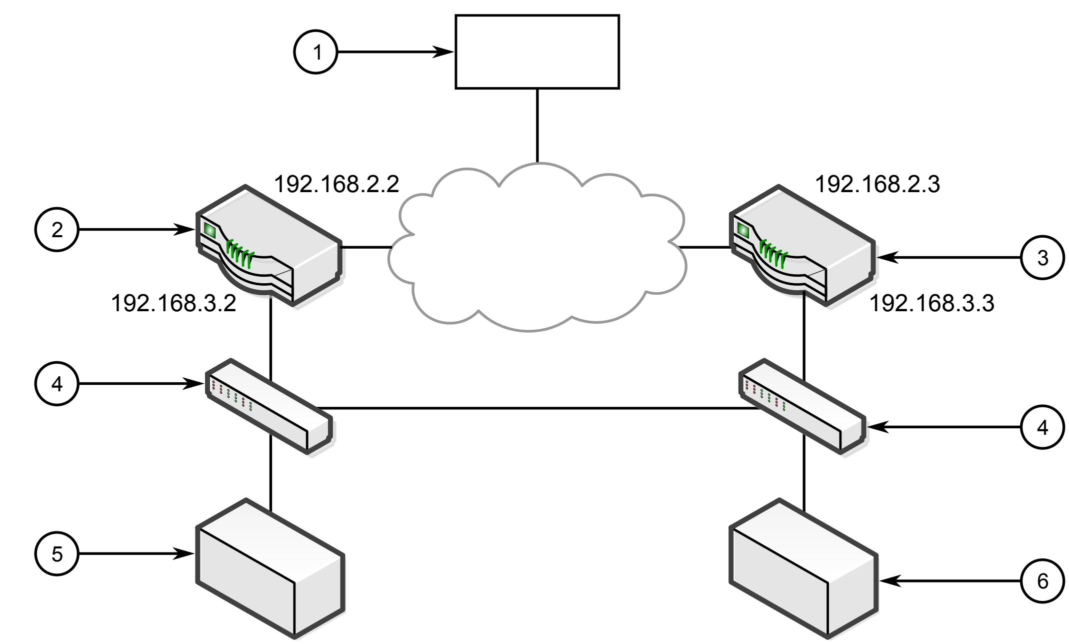

Figure 10: VRRP Group Example

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 5.26.2

Viewing the Status of VRRP

To view the status of VRRP, type:

```
show services vrrp status
```

A table or list similar to the following example appears:

```
ruggedcom# show services vrrp status
                                                                      MONITOR
                                                       INTERFACE      INTERFACE
NAME   STATE    PRIORITY  TIME CHANGE                  STATE          STATE
--------------------------------------------------------------------------------
v1     master   100       Sat Feb  2 06:30:41 EST 2013  fe-cm-1 is Up
```

This table or list provides the following information:

Parameter	Description
name	The VRRP instance name.
state	The VRRP instance state.
priority	The VRRP instance priority.
time-change	The time of change to the current state.
interface-state	The VRRP interface state.

Section 5.26.3

Enabling/Disabling VRRP

To enable or disable VRRP, do the following:

1. Make sure the CLI is in Configuration mode.
2. Enable or disable VRRP by typing:

   Enabling VRRP

   ```
   services vrrp enabled
   ```

   Disabling VRRP

   ```
   no services vrrp enabled
   ```

3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.26.4

Managing VRRP Trackers

VRRP trackers monitor the state/condition of a route. When the route is unavailable, VRRP will lower its priority or transition it to a fault state.

NOTE
The decision to increase or decrease the priority of a route must be done in coordination with any backup VRRP Routers since the priority decides whether a router becomes a Master or a Backup. For example, if Router X's priority is 150 and Router Y's priority is 145, Router X's priority must be lowered by 6 to make it a Backup router.

The following sections describe how to configure and manage VRRP trackers:

- Section 5.26.4.1, “Viewing a List of VRRP Trackers”
- Section 5.26.4.2, “Adding a VRRP Tracker”

- Section 5.26.4.3, “Deleting a VRRP Tracker”

Section 5.26.4.1
Viewing a List of VRRP Trackers

To view a list of VRRP trackers, type:

```
show running-config services vrrp trackers
```

If trackers have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config services vrrp trackers
services
 vrrp
  trackers tracker tracker1
   network   10.0.0.0/8
   interface dummy0
   interval  1
  !
 !
!
```

If no VRRP trackers have been configured, add trackers as needed. For more information, refer to Section 5.26.4.2, “Adding a VRRP Tracker”.

Section 5.26.4.2
Adding a VRRP Tracker

To add a VRRP tracker, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the tracker by typing:

   ```
   services vrrp trackers name
   ```

   Where:

   - *name* is the name of the VRRP tracker
3. Configure the following parameter(s) as required:

Parameter	Description
type { type }	**Synopsis:** route **Default:** route The type of condition for the tracker to check.
network { network }	The network to track. The tracker checks for a route to this network in the routing table.
interface { interface }	The interface to the tracked network. The tracker rises only when the route to the monitored network is through this interface.
interval { interval }	The number of seconds between tracker queries.
weight { weight }	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 { rise }	The number of successful tracker queries before changing the router priority.
fall { fall }	The number of unsuccessful tracker queries before changing the router priority.

4. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.26.4.3
Deleting a VRRP Tracker

To delete a VRRP tracker, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the tracker by typing:

```
no services vrrp trackers name
```

Where:

• *name* is the name of the VRRP tracker

3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.26.5
Managing VRRP Groups

Two or more VRRP instances can be assigned to be in the same VRRP Group, in which case, they can failover together.

The following sections describe how to configure and manage VRRP groups:

• Section 5.26.5.1, “Viewing a List of VRRP Groups”
• Section 5.26.5.2, “Adding a VRRP Group”
• Section 5.26.5.3, “Deleting a VRRP Group”

Section 5.26.5.1
Viewing a List of VRRP Groups

To view a list of VRRP groups, type:

```
show running-config services vrrp group
```

If groups have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config services vrrp group
services
 vrrp
  group group1
   !
  !
!
```

If no VRRP groups have been configured, add groups as needed. For more information, refer to Section 5.26.5.2, “Adding a VRRP Group”.

Section 5.26.5.2
Adding a VRRP Group

To add a VRRP group, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the group by typing:

```
services vrrp group name
```

   Where:

   - *name* is the name of the VRRP group
3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.26.5.3
Deleting a VRRP Group

To delete a VRRP group, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the group by typing:

```
no services vrrp group name
```

   Where:

   - *name* is the name of the VRRP group
3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.26.6
Managing VRRP Instances

The following sections describe how to configure and manage VRRP instances:

- Section 5.26.6.1, “Viewing a List of VRRP Instances”
- Section 5.26.6.2, “Adding a VRRP Instance”
- Section 5.26.6.3, “Deleting a VRRP Instance”

Section 5.26.6.1
Viewing a List of VRRP Instances

To view a list of VRRP instances, type:

```
show running-config services vrrp instance
```

If instances have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config services vrrp instance
services
 vrrp
  instance vid20
   interface switch.0001
   vrid      10
   priority  100
   group     group1
   monitor fe-cm-1
   !
   track-script tracker1
   !
   vrip 192.168.0.10/24
   !
  !
 !
!
```

If no VRRP instances have been configured, add instances as needed. For more information, refer to Section 5.26.6.2, "Adding a VRRP Instance".

Section 5.26.6.2
Adding a VRRP Instance

To add a VRRP instance, do the following:

1. Make sure the CLI is in Configuration mode.
2. Make sure a VRRP group has been configured. For more information, refer to Section 5.26.5.2, "Adding a VRRP Group".
3. Add the instance by typing:

```
services vrrp instance name
```

Where:

- *name* is the name of the VRRP instance. The name must not include spaces.

4. Configure the following parameter(s) as required:

> **NOTE**
> *A preemption occurs when either:*
> - *a backup VRRP router gains higher priority and transitions to the Master state*
> - *VRRP is initiated and this router has higher priority than that of any VRRP router on the network*

Parameter	Description
vrrp-version { vrrp-version }	**Default:** 2 Configure VRRP version for this instance.
interface { interface }	The interface that will host the VRIP when the router becomes the VRRP Master.
vrid { vrid }	The Virtual Router ID. All routers supplying the same VRIP should have the same VRID.
priority { priority }	The priority for the VRRP instance. When electing the master, the highest priority wins. The configurable range is 1 to 255. A value of zero (0) is invalid.
advert-interval { advert-interval }	**Default:** 1

Parameter	Description
	VRRP2 advertisement interval, in seconds.
advert-interval-millisecond { advert-interval-millisecond }	**Default:** 1000 **Prerequisite:** Value of advert-interval-millisecond must be multiple of 10. VRRP3 advertisement interval in millisecond, must be multiple of 10.
garp-delay { garp-delay }	**Default:** 5 Gratuitous ARP delay, in seconds. Sets the delay after the router changes state state before a second set of gratuitous ARPs are sent.
nopreempt	When enabled, a lower priority router maintains its role as master even if this router has a higher priority.
preempt-delay { preempt-delay }	**Default:** 0 The time, in seconds, after startup until preemption.
fault-to-master-delay { fault-to-master-delay }	**Default:** 0 The delay, in seconds, before a transition from the fault state to the master state occurs, thereby preempting the current master.
use-virtual-mac	When enabled, the router uses a virtual MAC address for the VRIP interface.
group { group }	Binds this VRRP instance to a VRRP group.

5. Add one or more VRRP monitors. For more information, refer to Section 5.26.7.2, “Adding a VRRP Monitor”.
6. Add one or more track scripts. For more information, refer to Section 5.26.8.2, “Adding a Track Script”.
7. Add one or more virtual IP addresses. For more information, refer to Section 5.26.9.2, “Adding a Virtual IP Address”.
8. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.26.6.3

Deleting a VRRP Instance

To delete a VRRP instance, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the instance by typing:

```
no services vrrp instance name
```

Where:

- *name* is the name of the VRRP instance

3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.26.7

Managing VRRP Monitors

A VRRP monitor selects an extra interface to monitor. If the interface becomes unavailable, the router will relinquish control of the gateway IP address to another VRRP Router.

The following sections describe how to configure and manage VRRP monitors:

- Section 5.26.7.1, “Viewing a List of VRRP Monitors”
- Section 5.26.7.2, “Adding a VRRP Monitor”
- Section 5.26.7.3, “Deleting a VRRP Monitor”

Section 5.26.7.1
Viewing a List of VRRP Monitors

To view a list of VRRP monitors, type:

```
show running-config services vrrp instance name monitor
```

Where:

- *name* is the name of the VRRP instance

If monitors have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config services vrrp instance monitor
services
 vrrp
  instance vid20
   monitor fe-cm-1
   !
  !
 !
!
```

If no VRRP monitors have been configured, add monitors as needed. For more information, refer to Section 5.26.7.2, “Adding a VRRP Monitor”.

Section 5.26.7.2
Adding a VRRP Monitor

To add a VRRP monitor, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the instance by typing:

   ```
   services vrrp instance name monitor interface
   ```

   Where:

   - *name* is the name of the VRRP instance
   - *interface* is the name of the extra interface to monitor
3. Configure the following parameter(s) as required:

Parameter	Description
weight { weight }	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.

4. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.26.7.3
Deleting a VRRP Monitor

To delete a VRRP monitor, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the monitor by typing:

```
no services vrrp instance name monitor interface
```

   Where:

   - *name* is the name of the VRRP instance
   - *interface* is the name of the extra interface to monitor
3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.26.8
Managing Track Scripts

Track scripts are used to associate VRRP trackers with VRRP instances.

The following sections describe how to configure and manage track scripts:

- Section 5.26.8.1, "Viewing a List of Track Scripts"
- Section 5.26.8.2, "Adding a Track Script"
- Section 5.26.8.3, "Deleting a Track Script"

Section 5.26.8.1
Viewing a List of Track Scripts

To view a list of track scripts, type:

```
show running-config services vrrp instance name monitor
```

Where:

- *name* is the name of the VRRP instance

If track scripts have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config services vrrp instance track-script
services
 vrrp
  instance vid20
   track-script tracker1
   !
  !
 !
!
```

If no VRRP monitors have been configured, add monitors as needed. For more information, refer to Section 5.26.7.2, "Adding a VRRP Monitor".

Section 5.26.8.2
Adding a Track Script

To add a track script, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the track script by typing:

```
services vrrp instance name track-script tracker
```

   Where:

   - *name* is the name of the VRRP instance
   - *tracker* is the name of the tracker to use to monitor the VRRP instance

3. Configure the following parameter(s) as required:

Parameter	Description
weight { weight }	This setting overwrites the weight setting in the tracker. If negative, the priority decreases by this amount when the tracker falls. If positive, the priority increases by this amount when the tracker rises. If not set, the weight value in the tracker will be used.

4. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.26.8.3
Deleting a Track Script

To delete a track script, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the track script by typing:

```
no services vrrp instance name track-script tracker
```

   Where:

   - *name* is the name of the VRRP instance
   - *tracker* is the name of the tracker to use to monitor the VRRP instance

3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.26.9
Managing Virtual IP Addresses

Virtual IP addresses represent the default gateways used by the hosts on the shared LAN.

The following sections describe how to configure and manage virtual IP addresses:

- Section 5.26.9.1, “Viewing a List of Virtual IP Addresses”
- Section 5.26.9.2, “Adding a Virtual IP Address”
- Section 5.26.9.3, “Deleting a Virtual IP Address”

Section 5.26.9.1

Viewing a List of Virtual IP Addresses

To view a list of virtual IP addresses, type:

```
show running-config services vrrp instance name vrip
```

Where:

- *name* is the name of the VRRP instance

If addresses have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config services vrrp instance vid20 vrip
services
 vrrp
  instance vid20
   vrip 192.168.0.10/24
   !
  !
 !
!
```

If no virtual IP addresses have been configured, add addresses as needed. For more information, refer to Section 5.26.9.2, “Adding a Virtual IP Address”.

Section 5.26.9.2

Adding a Virtual IP Address

To add a virtual IP address, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the instance by typing:

   ```
   services vrrp instance name vrip address
   ```

   Where:

   - *name* is the name of the VRRP instance
   - *address* is the address and subnet
3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.26.9.3

Deleting a Virtual IP Address

To delete a virtual IP address, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the virtual IP address by typing:

   ```
   no services vrrp instance name vrip address
   ```

   Where:

   - *name* is the name of the VRRP instance
   - *address* is the virtual IP address and netmask

3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.27

Managing Link Failover Protection

Link failover provides an easily configurable means of raising a backup link upon the failure of a designated main link. The main and backup links can 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.

The following sections describe how to configure link failover protection:

- Section 5.27.1, "Viewing the Link Failover Log"
- Section 5.27.2, "Viewing the Link Failover Status"
- Section 5.27.3, "Managing Link Failover Parameters"
- Section 5.27.4, "Managing Link Failover Backup Interfaces"
- Section 5.27.5, "Managing Link Failover Ping Targets"
- Section 5.27.6, "Testing Link Failover"
- Section 5.27.7, "Cancelling a Link Failover Test"

Section 5.27.1

Viewing the Link Failover Log

To view the link failover log, do the following:

1. Make sure the CLI is in Configuration mode.
2. Display the log by typing:

```
services link-failover log
```

A table or list similar to the following appears:

```
ruggedcom(config)# services link-failover switch.0001 log
link-backup-log /var/log/syslog:Jan 25 09:46:49 R1-RX1512 linkd[4183]: linkd initializing.
/var/log/syslog:Jan 25 09:46:49 R1-RX1512 linkd[4183]: linkd configured and started.
/var/log/syslog:Jan 25 09:46:49 R1-RX1512 linkd[4183]: linkd_interface_up: interface fe-cm-1 is up
/var/log/syslog:Jan 25 09:46:51 R1-RX1512 linkd[4183]: creating thread to monitor main=switch.0001
/var/log/syslog:Jan 25 09:46:51 R1-RX1512 linkd[4183]: setting new_backup_record
/var/log/syslog:Jan 25 09:46:51 R1-RX1512 linkd[4183]: setting new_backup_record done!
/var/log/syslog:Jan 25 09:46:51 R1-RX1512 linkd[4183]: dumping backup record:
/var/log/syslog:Jan 25 09:46:51 R1-RX1512 linkd[4183]:   main_interface = switch.0001
/var/log/syslog:Jan 25 09:46:51 R1-RX1512 linkd[4183]:     main_test_host = 10.10.10.10
/var/log/syslog:Jan 25 09:46:51 R1-RX1512 linkd[4183]:     start_delay = 180
/var/log/syslog:Jan 25 09:46:51 R1-RX1512 linkd[4183]:     main_path_down_timeout = 60
```

```
/var/log/syslog:Jan 25 09:46:51 R1-RX1512 linkd[4183]:     main_path_up_timeout = 60
/var/log/syslog:Jan 25 09:46:51 R1-RX1512 linkd[4183]:     backup_path_up_timeout = 60
/var/log/syslog:Jan 25 09:46:51 R1-RX1512 linkd[4183]:     ping_timeout = 2
/var/log/syslog:Jan 25 09:46:51 R1-RX1512 linkd[4183]:     ping_interval = 60
/var/log/syslog:Jan 25 09:46:51 R1-RX1512 linkd[4183]:     ping_retry_count = 3
/var/log/syslog:Jan 25 09:46:51 R1-RX1512 linkd[4183]:     backup_interface = fe-1-1
/var/log/syslog:Jan 25 09:46:51 R1-RX1512 linkd[4183]:       backup gateway = 192.168.1.2
/var/log/syslog:Jan 25 09:46:51 R1-RX1512 linkd[4183]:       ondemand = yes
/var/log/syslog:Jan 25 09:46:51 R1-RX1512 linkd[4183]:       distance = 1
/var/log/syslog:Jan 25 09:46:51 R1-RX1512 linkd[4183]:       transfer default route = yes
/var/log/syslog:Jan 25 09:46:51 R1-RX1512 linkd[4183]:     backup_interface = te1-2-1c01ppp
/var/log/syslog:Jan 25 09:46:51 R1-RX1512 linkd[4183]:       ondemand = yes
/var/log/syslog:Jan 25 09:46:51 R1-RX1512 linkd[4183]:       distance = 1
/var/log/syslog:Jan 25 09:46:51 R1-RX1512 linkd[4183]:       transfer default route = yes
/var/log/syslog:Jan 25 09:46:55 R1-RX1512 linkd[4183]: linkd_interface_up: interface fe-1-1 is up
/var/log/syslog:Jan 25 09:46:55 R1-RX1512 linkd[4183]: linkd_interface_down: interface fe-1-1 is
 down
/var/log/syslog:Jan 25 09:46:55 R1-RX1512 linkd[4183]: linkd_interface_up: interface fe-1-1 is up
/var/log/syslog:Jan 25 09:46:55 R1-RX1512 linkd[4183]: linkd_interface_down: interface fe-1-1 is
 down
/var/log/syslog:Jan 25 09:46:55 R1-RX1512 linkd[4183]: linkd_interface_up: interface fe-cm-1 is up
/var/log/syslog:Jan 25 09:46:55 R1-RX1512 linkd[4183]: linkd_interface_up: interface switch.0001 is
 up
/var/log/syslog:Jan 25 09:47:11 R1-RX1512 linkd[4183]: linkd_interface_down: interface switch.0001
 is down
/var/log/syslog:Jan 25 09:47:14 R1-RX1512 linkd[4183]: linkd_interface_up: interface switch.0001 is
 up
/var/log/syslog:Jan 25 09:49:52 R1-RX1512 linkd[4183]: Start monitoring link backup set:
 "switch.0001"
```

Section 5.27.2

Viewing the Link Failover Status

The Link Failover Status form displays the current link failover status. To view the link failover status, do the following:

```
show services link-failvover status
```

A table or list similar to the following appears:

```
ruggedcom# show services link-failover status
             MAIN    BACKUP  MAIN                                                   BACKUP
             LINK    LINK    PING  TIME OF LAST STATE                               INTERFACE
MAIN         STATUS  STATUS  TEST  CHANGE                      LINK BACKUP STATE     IN USE
---------------------------------------------------------------------------------------------
switch.0001  up      down    ok    Fri Jan 25 09:49:52 2013
  Main path is active
  fe-1-1
```

The table or list provides the following information:

Parameter	Description
main-link-status	The main link status.
backup-link-status	The backup link status.
main-ping-test	The results of pinging the target using the main interface.
time-of-last-state-change	The time of the last state change.
link-backup-state	The backup link state.

Parameter	Description
backup-interface-in-use	The name of the backup interface that is being used.

Section 5.27.3

Managing Link Failover Parameters

The following sections describe how to configure and manage parameters for link failover protection:

- Section 5.27.3.1, "Viewing a List of Link Failover Parameters"
- Section 5.27.3.2, "Adding a Link Failover Parameter"
- Section 5.27.3.3, "Deleting a Link Failover Parameter"

Section 5.27.3.1

Viewing a List of Link Failover Parameters

To view a list of link failover parameters, type:

```
show running-config services link-failvover
```

If parameters have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config services link-failover
services
 link-failover switch.0001
  enabled
  backup fe-1-1
   transfer-default-route
   backup-gateway         192.168.1.2
  !
  backup te1-2-1c01ppp
   priority               second
   transfer-default-route
  !
  target 10.10.10.10
  !
 !
!
```

If no parameters have been configured, add parameters as needed. For more information, refer to Section 5.27.3.2, "Adding a Link Failover Parameter".

Section 5.27.3.2

Adding a Link Failover Parameter

To add a link failover parameter, do the following:

> **NOTE**
> *The link failover feature can only be configured on a routable interface. For the link failover feature to be used on a switched port, another VLAN must be configured (for example, switch.0002) to logically differentiate the switched port from the default PVID VLAN 1 (switch.0001).*

1. Make sure the CLI is in Configuration mode.

2. Add the parameter by typing:

```
services link-failvover interface
```

Where:

- *interface* is the name of the interface

3. Configure the following parameter(s) as required:

Parameter	Description
enabled	Enables this link backup.
ping-timeout { ping-timeout }	**Default:** 2 The time interval, in seconds, before immediately retrying a ping.
ping-interval { ping-interval }	**Default:** 60 The time interval, in seconds, between ping tests.
ping-retry { ping-retry }	**Default:** 3 The number of ping retries before constructing a path failure.
start-delay { start-delay }	**Default:** 180 The delay time, in seconds, when first starting link failover.
main-down-timeout { main-down-timeout }	**Default:** 60 The delay time, in seconds, that the main trunk is down before starting the backup trunk.
main-up-timeout { main-up-timeout }	**Default:** 60 The delay time, in seconds, to confirm that the main trunk is up (returned to service) before stopping the backup trunk.

4. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.27.3.3

Deleting a Link Failover Parameter

To delete a link failover parameter, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the parameter by typing:

```
no services link-failvover interface
```

Where:

- *interface* is the name of the interface

3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.27.4

Managing Link Failover Backup Interfaces

A backup interface is the interface to which link failover switches when the main interface is determined to be down. You can add up to three backup interfaces to each link failover configuration.

The following sections describe how to configure and manage backup interfaces for link failover protection:

- Section 5.27.4.1, "Viewing a List of Link Failover Backup Interfaces"
- Section 5.27.4.2, "Adding a Link Failover Backup Interface"
- Section 5.27.4.3, "Deleting a Link Failover Backup Interface"

Section 5.27.4.1
Viewing a List of Link Failover Backup Interfaces

To view a list of link failover backup interfaces, type:

```
show running-config services link-failvover interface backup
```

Where:

- *interface* is the name of the interface

If backup interfaces have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config services link-failover switch.0001 backup
services
 link-failover switch.0001
  backup fe-1-1
   transfer-default-route
   backup-gateway         192.168.1.2
  !
  backup te1-2-1c01ppp
   priority               second
   transfer-default-route
  !
 !
!
```

If no backup interfaces have been configured, add backup interfaces as needed. For more information, refer to Section 5.27.4.2, "Adding a Link Failover Backup Interface".

Section 5.27.4.2
Adding a Link Failover Backup Interface

To set a link failover backup interface, do the following:

> **CAUTION!**
> *Configuration hazard – risk of connection loss. If a RUGGEDCOM APE module is installed, either avoid configuring switch.0001 as a link failover backup interface or configure a different VLAN for the APE module. By default, APE modules utilize VLAN 1 (switch.0001) and always keep the interface in the UP state. This would interfere with the link failover mechanism.*
>
> *To configure a different VLAN for the APE module, change the PVID for the associated switched Ethernet port. For information, refer to Section 3.17.2, "Configuring a Switched Ethernet Port".*

1. Make sure the CLI is in Configuration mode.
2. Add the backup interface by typing:

   ```
   services link-failvover interface backup backup-interface
   ```

   Where:

- *interface* is the name of the interface
- *backup-interface* is the name of the secondary, backup interface

3. Configure the following parameter(s) as required:

> **NOTE**
> *Do not configure the* `backup-gateway` *parameter for Point to Point (P2P) links.*

> **NOTE**
> *The* `on-demand` *parameter is set at the interface itself.*

Parameter	Description
priority { priority }	**Synopsis:** third, second, first **Default:** first The priority which is applied to the backup interface when switching.
transfer-default-route	The transfer default gateway on the switching main and backup interface. The default route on the device must have a *distance* greater than one.
backup-gateway { backup-gateway }	The IP address of the backup gateway.
on-demand	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.

Section 5.27.4.3
Deleting a Link Failover Backup Interface

To delete a link failover backup interface, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the backup interface by typing:

```
no services link-failvover interface backup backup-interface
```

Where:

- *interface* is the name of the interface
- *backup-interface* is the name of the secondary, backup interface

3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.27.5
Managing Link Failover Ping Targets

A link failover ping target is an IP address that link failover pings to determine if the main link is down. The address can be a dedicated host or a dummy address on a router. Up to three link failover ping targets can be added to each link failover configuration.

The following sections describe how to configure and manage ping targets for link failover protection:

- Section 5.27.5.1, “Viewing a List of Link Failover Ping Targets”
- Section 5.27.5.2, “Adding a Link Failover Ping Target”
- Section 5.27.5.3, “Deleting a Link Failover Ping target”

Section 5.27.5.1
Viewing a List of Link Failover Ping Targets

To view a list of link failover ping targets, type:

```
show running-config services link-failvover interface target
```

Where:

- *interface* is the name of the interface

If ping targets have been configured, a table or list similar to the following example appears:

```
R1-RX1512# show running-config services link-failover switch.0001 target
services
 link-failover switch.0001
  target 10.10.10.10
  !
 !
!
```

If no ping targets have been configured, add targets as needed. For more information, refer to Section 5.27.5.2, “Adding a Link Failover Ping Target”.

Section 5.27.5.2
Adding a Link Failover Ping Target

To add a link failover ping target, do the following:

> **NOTE**
> *Link failover pings each target separately. If all targets are down, the main link is considered to be down and it fails over to the backup interface. Backup links are used in the order of their Priority setting (first, second, and then third), always starting with the first priority interface. When a higher-priority interface becomes available again, the system reverts to the higher priority interface. For example, if the second priority interface is active, the system switches back to the first priority interface when the first priority interface becomes available again.*

1. Make sure the CLI is in Configuration mode.
2. Add the ping target by typing:

   ```
   services link-failvover interface target address
   ```

   Where:

   - *interface* is the name of the interface
   - *address* is the IP address of the target host to verify the main path
3. Configure the following parameter(s) as required:

Parameter	Description
{ host-ip }	The IP address of the target host to verify the main path.

Section 5.27.5.3

Deleting a Link Failover Ping target

To delete a link failover ping target, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the backup interface by typing:

```
no services link-failvover interface target address
```

   Where:

   - *interface* is the name of the interface
   - *address* is the IP address of the target host to verify the main path

3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.27.6

Testing Link Failover

The link failover settings can be tested to confirm that each link failover configuration works properly. To launch the test, specify for how long the system should operate on the backup interface, and for how long the system should delay before starting the test. Cancelling the test returns the interfaces to their pre-test condition.

While the test is running, monitor the status of the test to observe the main and backup link status, ping test results, state change, backup state, and backup interface information. As the test progresses, this information changes as link failover switches from the main interface to the backup interface. For more information on the **Link Fail Over Status** form, refer to Section 5.27.2, "Viewing the Link Failover Status".

To launch a link failover test, do the following:

> **NOTE**
> *The link failover test can be cancelled at any time. For more information about cancelling a link failover test, refer to Section 5.27.7, "Cancelling a Link Failover Test".*
>
> *Cancelling the test returns the interfaces to their pre-test condition.*

1. Make sure the CLI is in Configuration mode.
2. Start the test by typing:

```
services link-failover interface start-test start-test-delay delay test-duration duration
```

   Where:

   - *interface* is the name of the interface
   - *delay* is the time (in seconds) to wait before running the test
   - *duration* is the maximum time (in minutes) to run the test before restoring service to the main trunk

Section 5.27.7

Cancelling a Link Failover Test

To cancel a link failover test, type:

```
services link-failover interface cancel-test
```

Where:

- *interface* is the name of the interface

Section 5.28

Managing IPsec Tunnels

IPsec (Internet Protocol SECurity) uses strong cryptography to provide authentication and encryption services. Authentication ensures that packets are from the right sender and have not been altered in transit. Encryption prevents unauthorized reading of packet contents.

These services allow secure tunnels to be built through untrusted networks. Everything passing through the untrusted network is encrypted by the IPsec gateway and decrypted by the gateway at the other end. The result is a Virtual Private Network (VPN), a network which is effectively private even though it includes machines at several different sites connected by the insecure Internet.

For more information about IPsec tunnels, refer to Section 5.28.1, "IPsec Tunneling Concepts".

IMPORTANT!

IPsec is time-sensitive. To make sure proper re-keying between network peers, the time on both peers must be synchronized. It is strongly recommended that NTP (Network Time Protocol) be used on both IPsec peers to synchronize their clocks. For more information about configuring NTP, refer to Section 5.12.11, "Managing NTP Servers".

The following sections describe how to configure and manage an IPsec tunnel:

- Section 5.28.1, "IPsec Tunneling Concepts"
- Section 5.28.2, "Configuring IPsec Tunnels"
- Section 5.28.3, "Configuring Certificates and Keys"
- Section 5.28.4, "Viewing the IPsec Tunnel Status"
- Section 5.28.5, "Managing Pre-Shared Keys"
- Section 5.28.6, "Managing Connections"
- Section 5.28.7, "Managing the Internet Key Exchange (IKE) Protocol"
- Section 5.28.8, "Managing the Encapsulated Security Payload (ESP) Protocol"
- Section 5.28.9, "Configuring the Connection Ends"
- Section 5.28.10, "Managing Private Subnets"

Section 5.28.1

IPsec Tunneling Concepts

The IPsec suite of protocols were developed by the Internet Engineering Task Force (IETF) and are required as part of IP version 6. Openswan is the open source implementation of IPsec used by ROX II.

The protocols used by IPsec are the Encapsulating Security Payload (ESP) and Internet Key Exchange (IKE) protocols. ESP provides encryption and authentication (ensuring that a message originated from the expected sender and has not been altered on route). IKE negotiates connection parameters, including keys, for ESP. IKE is based on the Diffie-Hellman key exchange protocol, which allows two parties without any initial shared secret to create one in a manner immune to eavesdropping.

The following sections provide more information about IPsec and its implementation in ROX II:

- Section 5.28.1.1, “IPsec Modes”
- Section 5.28.1.2, “Supported Encryption Protocols”
- Section 5.28.1.3, “Public and Secret Key Cryptography”
- Section 5.28.1.4, “X509 Certificates”
- Section 5.28.1.5, “NAT Traversal”
- Section 5.28.1.6, “Remote IPsec Client Support”
- Section 5.28.1.7, “IPsec and Router Interfaces”

Section 5.28.1.1

IPsec Modes

IPsec has two basic modes of operation. In *transport* mode, IPsec headers are added as the original IP datagram is created. The resultant packet is composed of an IP header, IPsec headers and IP payload (including a transport header). Transport mode is most commonly used between IPsec end-stations, or between an end-station and a gateway.

In *tunnel* mode, the original IP datagram is created normally and then encapsulated into a new IP datagram. The resultant packet is composed of a new IP header, IPsec headers, old IP header and IP payload. Tunnel mode is most commonly used between gateways, the gateway acting as a proxy for the hosts behind it.

Section 5.28.1.2

Supported Encryption Protocols

Openswan supports the following standard encryption protocols:

- **3DES (Triple DES)**

  Uses three DES encryptions on a single data block, with at least two different keys, to get higher security than is available from a single DES pass. 3DES is the most CPU intensive cipher.

- **AES**

  The Advanced Encryption Standard protocol cipher uses a 128-bit block and 128, 192 or 256-bit keys. This is the most secure protocol in use today, and is much preferred to 3DES due to its efficiency.

Section 5.28.1.3

Public and Secret Key Cryptography

In *public key* cryptography, keys are created in matched pairs (called public and private keys). The public key is made public while the private key is kept secret. Messages can then be sent by anyone who knows the public key to the holder of the private key. Only the owner of the private key can decrypt the message.

When this form of encryption is used, each router configures its VPN connection to use the RSA algorithm and includes the public signature of its peer.

In *secret key* cryptography, a single key known to both parties is used for both encryption and decryption.

When this form of encryption is used, each router configures its VPN connection to use a secret pre-shared key. For information about how to configure pre-shared keys, refer to Section 5.28.5, “Managing Pre-Shared Keys”.

Section 5.28.1.4

X509 Certificates

In addition to pre-shared keys, IPsec also uses certificates to authenticate connections with hosts and routers. Certificates are digital signatures that are produced by a trusted source, namely a Certificate Authority (CA). For each host, the CA creates a certificate that contains CA and host information. The certificate is "signed” by creating a digest of all the fields in the certificate and then encrypting the hash value with its private key. The host’s certificate and the CA public key are installed on all gateways that the host connects to.

When the gateway receives a connection request, it uses the CA public key to decrypt the signature back into the digest. It then recomputes its own digest from the plain text in the certificate and compares the two. If both digests match, the integrity of the certificate is verified (it was not tampered with), and the public key in the certificate is assumed to be the valid public key of the connecting host.

Section 5.28.1.5

NAT Traversal

Historically, IPsec has presented problems when connections must traverse a firewall providing Network Address Translation (NAT). The Internet Key Exchange (IKE) used in IPsec is not NAT-translatable. When IPsec connections must traverse a firewall, IKE messages and IPsec-protected packets must be encapsulated as User Datagram Protocol (UDP) messages. The encapsulation allows the original untranslated packet to be examined by IPsec.

Encapsulation is enabled during the IPsec configuration process. For more information, refer to Section 5.28.2, “Configuring IPsec Tunnels”.

Section 5.28.1.6

Remote IPsec Client Support

If the router is to support a remote IPsec client and the client will be assigned an address in a subnet of a local interface, a proxy ARP must be activated for that interface. This will cause the router to respond to ARP requests on behalf of the client and direct traffic to it over its connection.

IPsec relies upon the following protocols and ports:

- protocol 51, IPSEC-AH Authentication Header (RFC2402)
- protocol 50, IPSEC-ESP Encapsulating Security Payload (RFC2046)

- UDP port 500

The firewall must be configured to accept connections on these ports and protocols. For more information, refer to Section 5.17.6, “Configuring the Firewall for a VPN”.

Section 5.28.1.7
IPsec and Router Interfaces

If IPsec works on an interface which could disappear, such as a PPP connection, or if the IP address could change, the **Monitor Interface** option must be set for the IPsec connection. When this option is set, IPsec will restart when the interface disappears and reappears, or the IP address is changed.

The **Monitor Interface** option is set on the **Connection** form available for each connection. For more information about connections, refer to Section 5.28.6, “Managing Connections”.

Section 5.28.2
Configuring IPsec Tunnels

To configure IPsec tunnels, do the following:

NOTE
ROX II supports the creation of policy-based VPNs, which can be characterized as follows:

- *No IPsec network interfaces have been created.*
- *The routing table is not involved in directing packets to IPsec.*
- *Only data traffic matching the tunnel's local and remote subnets is forwarded to the tunnel. Normal traffic is routed by one set of firewall rules and VPN traffic is routed based on separate rules.*
- *The firewall is configured with a VPN zone of type ipsec.*
- *As IPsec packets are received, they are decoded, flagged as IPsec-encoded, and presented as having arrived directly from the same network interface on which they were originally received.*
- *Firewall rules are written to allow traffic to and from VPN tunnels. These are based on the normal form of source/destination IP addresses, and IP protocol and port numbers. These rules, by virtue of the zones they match, use the policy flags inserted by the netkey to route matching data traffic to the proper interface.*

For more information about configuring a policy-based VPN, refer to Section 5.17, “Managing Firewalls”.

1. Make sure the CLI is in Configuration mode.
2. Navigate to ***tunnel » ipsec*** and configure the following parameter(s) as required:

Parameter	Description
enabled	Enables IPsec.
nat-traversal	Enables NAT Traversal.
keep-alive { keep-alive }	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.
status	The status of IPsec.

3. Configure one or more pre-shared keys. For more information, refer to Section 5.28.5.2, “Adding a Pre-Shared Key”.
4. Configure one or more encrypted connections. For more information, refer to Section 5.28.6.2, “Adding a Connection”.
5. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.28.3

Configuring Certificates and Keys

To configure certificates and keys for IPsec Tunnels, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add a CA certificate and Certificate Revocation List (CRL). For more information, refer to Section 4.7.1.3, “Adding a CA Certificate and CRL”
3. Add a private key. For more information, refer to Section 4.7.2.2, “Adding a Private Key”.
4. Add a certificate. For more information, refer to Section 4.7.4.3, “Adding a Certificate”.
5. Add a public key. For more information, refer to Section 4.7.3.2, “Adding a Public Key”.
6. Navigate to ***tunnel » ipsec » connection » {connection} » {end}***, where *{connection}* is the name of the connection and *{end}* is the either the left (local router) or right (remote router) connection end.
7. Configure the system public key by typing:

   ```
   tunnel ipsec connection connection [left | right] key type certificate
   ```

   Where:

   - *connection* is the name of the connection
8. Configure the system identifier by typing:

   ```
   tunnel ipsec connection connection [left | right] identifier type from-certificate
   ```

   Where:

   - *connection* is the name of the connection
9. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.28.4

Viewing the IPsec Tunnel Status

To view the status of the IPsec tunnel, type:

1. Make sure the CLI is in Configuration mode.
2. Display the status by typing:

   ```
   tunnel ipsec status
   ```

   A table or list similar to the following example appears:

   ```
   status
   =========================================================
   000 using kernel interface: netkey
   000 interface lo/lo ::1
   ```

```
000 interface lo/lo 127.0.0.1
000 interface vrf_gw0/vrf_gw0 169.254.0.1
000 interface switch.0001/switch.0001 192.168.0.2
000 interface switch.1000/switch.1000 172.30.151.38
000 %myid = (none)
000 debug none
000
000 virtual_private (%priv):
000 - allowed 0 subnets:
000 - disallowed 0 subnets:
000 WARNING: Either virtual_private= is not specified, or there is a syntax
000          error in that line. 'left/rightsubnet=vhost:%priv' will not work!
000 WARNING: Disallowed subnets in virtual_private= is empty. If you have
000          private address space in internal use, it should be excluded!
000
000 algorithm ESP encrypt: id=2, name=ESP_DES, ivlen=8, keysizemin=64, keysizemax=64
000 algorithm ESP encrypt: id=3, name=ESP_3DES, ivlen=8, keysizemin=192, keysizemax=192
000 algorithm ESP encrypt: id=11, name=ESP_NULL, ivlen=0, keysizemin=0, keysizemax=0
000 algorithm ESP encrypt: id=12, name=ESP_AES, ivlen=8, keysizemin=128, keysizemax=256
000 algorithm ESP encrypt: id=14, name=ESP_AES_CCM_A, ivlen=8, keysizemin=128, keysizemax=256
000 algorithm ESP encrypt: id=15, name=ESP_AES_CCM_B, ivlen=8, keysizemin=128, keysizemax=256
000 algorithm ESP encrypt: id=252, name=ESP_SERPENT, ivlen=8, keysizemin=128, keysizemax=256
000 algorithm ESP encrypt: id=253, name=ESP_TWOFISH, ivlen=8, keysizemin=128, keysizemax=256
000 algorithm ESP auth attr: id=1, name=AUTH_ALGORITHM_HMAC_MD5, keysizemin=128, keysizemax=128
000 algorithm ESP auth attr: id=2, name=AUTH_ALGORITHM_HMAC_SHA1, keysizemin=160, keysizemax=160
000 algorithm ESP auth attr: id=251, name=(null), keysizemin=0, keysizemax=0
000
000 algorithm IKE encrypt: id=0, name=(null), blocksize=16, keydeflen=131
000 algorithm IKE encrypt: id=3, name=OAKLEY_BLOWFISH_CBC, blocksize=8, keydeflen=128
000 algorithm IKE encrypt: id=65289, name=OAKLEY_TWOFISH_CBC_SSH, blocksize=16, keydeflen=128
000 algorithm IKE hash: id=1, name=OAKLEY_MD5, hashsize=16
000 algorithm IKE hash: id=2, name=OAKLEY_SHA1, hashsize=20
000 algorithm IKE hash: id=4, name=OAKLEY_SHA2_256, hashsize=32
000 algorithm IKE hash: id=6, name=OAKLEY_SHA2_512, hashsize=64
000 algorithm IKE dh group: id=2, name=OAKLEY_GROUP_MODP1024, bits=1024
000 algorithm IKE dh group: id=5, name=OAKLEY_GROUP_MODP1536, bits=1536
000 algorithm IKE dh group: id=18, name=OAKLEY_GROUP_MODP8192, bits=8192
000
000 stats db_ops: {curr_cnt, total_cnt, maxsz} :context={0,0,0} trans={0,0,0} attrs={0,0,0}
000
000 "ipsec-12": 192.168.22.0/24===192.168.12.2<192.168.12.2>[C=CA, ST=Ontario, O=RuggedCom,
 CN=router2, E=router2@example.com,+S=C]...192.168.12.1<192.168.12.1>[C=CA, ST=Ontari o,
 O=RuggedCom, CN=router1, E=router1@example.com,+S=C]===192.168.11.0/24; erouted; eroute owner: #2
000 "ipsec-12":     myip=unset; hisip=unset; myup=ipsec _updown --route yes; hisup=ipsec _updown --
route yes; mycert=router2;
000 "ipsec-12":   CAs: 'C=CA, ST=Ontario, O=RuggedCom, CN=CA, E=ca@example.com'...'%any'
000 "ipsec-12":   ike_life: 3600s; ipsec_life: 28800s; rekey_margin: 540s; rekey_fuzz: 100%;
 keyingtries: 0
000 "ipsec-12":   policy: RSASIG+ENCRYPT+TUNNEL+PFS+UP+IKEv2ALLOW+lKOD+rKOD; prio: 24,24;
 interface: switch.0012;
000 "ipsec-12":   newest ISAKMP SA: #4; newest IPsec SA: #2;
000 "ipsec-12":   IKE algorithm newest: AES_CBC_128-SHA1-MODP2048
000
000 #4: "ipsec-12":500 STATE_MAIN_I4 (ISAKMP SA established); EVENT_SA_REPLACE in 106s; newest
 ISAKMP; lastdpd=-1s(seq in:0 out:0); idle; import:admin initiate
000 #2: "ipsec-12":500 STATE_QUICK_I2 (sent QI2, IPsec SA established); EVENT_SA_REPLACE in 19349s;
 newest IPSEC; eroute owner; isakmp#1; idle; import:admin initiate
000 #2: "ipsec-12" esp.edfbc8f8@192.168.12.1 esp.53ffca14@192.168.12.2 tun.0@192.168.12.1
 tun.0@192.168.12.2 ref=0 refhim=4294901761
000
```

Section 5.28.5

Managing Pre-Shared Keys

Pre-shared keys are used in *secret key* cryptography. For more information about *secret key* cryptography and pre-shared keys, refer to Section 5.28.1.3, “Public and Secret Key Cryptography”.

The following sections describe how to configure and manage pre-shared keys for IPsec tunnels:

- Section 5.28.5.1, “Viewing a List of Pre-Shared Keys”
- Section 5.28.5.2, “Adding a Pre-Shared Key”
- Section 5.28.5.3, “Deleting a Pre-Shared Key”

Section 5.28.5.1

Viewing a List of Pre-Shared Keys

To view a list of pre-shared keys, type:

```
show running-config tunnel ipsec preshared-key
```

If pre-shared keys have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config tunnel ipsec preshared-key
tunnel
 ipsec
  preshared-key 192.168.12.1 192.168.12.2
   key $4$9YslfOBfkyYV8c1tqN4IDw==
  !
 !
!
```

If no pre-shared keys have been configured, add pre-shared keys as needed. For more information, refer to Section 5.28.5.2, “Adding a Pre-Shared Key”.

Section 5.28.5.2

Adding a Pre-Shared Key

To add a pre-shared key, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the pre-shared key by typing:

   ```
   tunnel ipsec preshared-key [remote-address | local-address] key key
   ```

   Where:

   - *remote-address* is the remote IP address
   - *local-address* is the local IP address
   - *key* is the is the content of the pre-shared key
3. Configure the following parameter(s) as required:

Parameter	Description
key { key }	**Synopsis:** The aes-cfb-128-encrypted-string works exactly like des3-cbc-encrypted-string but AES/128bits in CFB mode is used to encrypt the string. The prefix for encrypted values is '4'. The pre-shared key.

4. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.28.5.3
Deleting a Pre-Shared Key

To delete a pre-shared key, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the pre-shared key by typing:

```
no tunnel ipsec preshared-key [remote-address | local-address] key key
```

Where:

- *remote-address* is the remote IP address
- *local-address* is the local IP address
- *key* is the is the content of the pre-shared key

3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.28.6
Managing Connections

An IPsec connection is an encrypted connection between two devices who share the same pre-authorized authentication key.

The following sections describe how to configure and manage connections for an IPsec connection:

- Section 5.28.6.1, “Viewing a List of Connections”
- Section 5.28.6.2, “Adding a Connection”
- Section 5.28.6.3, “Configuring Dead Peer Detection”
- Section 5.28.6.4, “Deleting a Connection”

Section 5.28.6.1
Viewing a List of Connections

To view a list of connections configured for a VPN, type:

```
show tunnel ipsec connection
```

If connections have been configured, a table similar to the following example appears:

```
ruggedcom# show running-config tunnel ipsec connection
tunnel
```

```
 ipsec
  connection ipsec-12
   no l2tp
   ike algorithm 3des md5 modp8192
   !
   esp algorithm aes256 sha1
   !
   left
    public-ip type default-route
    subnet 192.168.11.0/24
    !
   !
   right
    public-ip type any
   !
  !
 !
!
```

If no connections have been configured, add connections as needed. For more information, refer to Section 5.28.6.2, “Adding a Connection”.

Section 5.28.6.2

Adding a Connection

To add a new connection for a VPN, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the connection by typing:

```
tunnel ipsec connection name
```

Where:

- `name` is the connection name. If the name is *default*, this makes it the default setting for all connections.

3. Configure the following parameter(s) as required:

Parameter	Description
startup { startup }	**Synopsis:** ignore, add, start, route, default **Default:** default The action to take when IPsec is initialized. The default value is 'ignore' unless overwritten by the default connection setting.
authenticate { authenticate }	**Synopsis:** default, rsasig, secret **Default:** default The authentication method. The default value is 'default' unless overwritten by the default connection setting.
connection-type { connection-type }	**Synopsis:** tunnel, transport, passthrough, default **Default:** default The connection type/mode. Options include: • tunnel: Encrypts traffic on host-to-host, host-to-subnet or subnet-to-subnet tunnels. This is the default type/mode unless overwritten by the default connection setting. • transport: Encrypts traffic on a host-to-host tunnel. • passthrough: Traffic is not encrypted.
address-family { address-family }	**Synopsis:** ipv4, ipv6 **Default:** ipv4

Parameter	Description
	The address-family to run for the connection. Accepted values include 'ipv4' (default) and 'ipv6'. All addresses used in the connection must have the same address family.
pfs { pfs }	**Synopsis:** default, yes, no **Default:** default Enables/disables Perfect Forwarding Secrecy (PFS). When enabled, IPsec negotiates new keys for each session. If an attacker compromises a key, only the session protected by the key is revealed. Not all clients support PFS. The default value is 'yes' unless overwritten by the default connection setting.
keylife { keylife }	**Synopsis:** default, **Default:** default The lifetime in seconds for the Security Association (SA) key. This determines how long a particular instance of a connection should last, from successful negotiation to expiry. Normally, the connection is renegotiated before it expires. The default value is 28800 unless overwritten by the default connection setting. Peers can specify different lifetime intervals. However, if peers do not agree, an excess of superseded connections will occur on the peer that believes the SA lifetime is longer.
ike-lifetime { ike-lifetime }	**Synopsis:** default, **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.
monitor-interface { monitor-interface }	The interface to monitor. If the selected interface goes down and then up, this connection will be restarted.

4. If required, enable and configure dead peer detection. For more information, refer to Section 5.28.6.3, “Configuring Dead Peer Detection”.
5. If required, configure the Internet Key Exchange (IKE) protocol by adding one or more algorithms. For more information, refer to Section 5.28.7.2, “Adding an IKE Algorithm”
6. If required, configure Encapsulated Security Payload (ESP) encryption for the connection. For more information, refer to Section 5.28.8, “Managing the Encapsulated Security Payload (ESP) Protocol”
7. If required, configure the left (local router) and right (remote router) ends of the connection. For more information, refer to Section 5.28.9, “Configuring the Connection Ends”
8. If required, configure L2TP tunnels. For more information, refer to Section 5.29.2, “Configuring L2TP Tunnels”.
9. If certificates and keys are required, make sure they are configured on the device. For more information, refer to Section 5.28.3, “Configuring Certificates and Keys”.
10. Type **`commit`** and press **Enter** to save the changes, or type **`revert`** and press **Enter** to abort.

Section 5.28.6.3
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 ROX II, DPD Requests are sent when there is no traffic detected by the peer. How long to wait before sending a DPD Request and how long to wait for a DPD Response is user configurable.

It is generally recommended that DPD be configured to clear connections with any dead peers.

To configure dead peer detection for an IPsec connection, do the following:

1. Make sure the CLI is in Configuration mode.
2. Enable dead peer detection by typing:

```
tunnel ipsec connection name dead-peer-detect enabled [true | false]
```

   Where:

   - *name* is the connection name.

3. Configure the following parameter(s) as required:

> **NOTE**
> *The timeout period must be two minutes longer than the interval period.*

Parameter	Description
interval { interval }	**Default:** 30 The interval (in seconds) between Dead Peer Detection keepalive messages sent for this connection when no traffic (idle) appears to be sent by a DPD enabled peer.
timeout { timeout }	**Default:** 120 The time in seconds to wait before a peer is declared dead. **Prerequisite:** The timeout period must be more than two times the interval.
action { action }	**Synopsis:** hold, clear, restart, restart-all-sa **Default:** restart The action to be taken when a DPD enabled peer is declared dead. Options include: • hold: The route will be put on hold status. • clear: The route and Security Association (SA) will both be cleared • restart: The SA will immediately be renegotiated • restart-all-sa: All SA's to the dead peer will be renegotiated

4. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.28.6.4
Deleting a Connection

To delete a connection for a VPN, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the connection by typing:

```
no tunnel ipsec connection name
```

   Where:

   - *name* is the name of the connection

3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.28.7

Managing the Internet Key Exchange (IKE) Protocol

The Internet Key Exchange (IKE) protocol negotiates connection parameters, including keys, for the Encapsulated Security Payload (ESP) protocol employed by IPsec. IKE is based on the Diffie-Hellman key exchange protocol, which allows two parties without any initially shared secret to create one in a manner immune to eavesdropping.

The following sections describe how to configure and manage the Internet Key Exchange (IKE) protocol:

- Section 5.28.7.1, "Viewing a List of IKE Algorithms"
- Section 5.28.7.2, "Adding an IKE Algorithm"
- Section 5.28.7.3, "Deleting an IKE Algorithm"

Section 5.28.7.1

Viewing a List of IKE Algorithms

To view a list of algorithms for the Internet Key Exchange (IKE) protocol, type:

```
show running-config tunnel ipsec connection connection ike algorithm
```

Where:

- *connection* is the name of the connection

If If algorithms have been configured, a table or list similar to the following example appears:

```
tunnel
 ipsec
  connection ipsec-12
   ike algorithm 3des md5 modp8192
   !
  !
 !
!
```

If no algorithms have been configured, add algorithms as needed. For more information, refer to Section 5.28.7.2, "Adding an IKE Algorithm".

Section 5.28.7.2

Adding an IKE Algorithm

To add a new algorithm for the Internet Key Exchange (IKE) protocol, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the algorithm by typing:

```
tunnel ipsec connection connection ike algorithm cipher cipher hash method modgroup modgroup
```

Where:

- *connection* is the name of the connection

- *cipher* is the cipher algorithm
- *method* is the hash method
- *modgroup* is the value of the modgroup

3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.28.7.3
Deleting an IKE Algorithm

To delete an algorithm for the Internet Key Exchange (IKE) protocol, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the algorithm by typing:

```
no tunnel ipsec connection connection ike algorithm cipher cipher hash method modgroup modgroup
```

Where:

- *connection* is the name of the connection
- *cipher* is the cipher algorithm
- *method* is the hash method
- *modgroup* is the value of the modgroup

3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.28.8
Managing the Encapsulated Security Payload (ESP) Protocol

The Encapsulated Security Payload (ESP) employed by IPsec provides encryption and authentication, making sure that messages originated from the expected sender have not been altered in transit.

The following sections describe how to configure and manage the ESP protocol:

- Section 5.28.8.1, “Configuring ESP Encryption”
- Section 5.28.8.2, “Viewing a List of ESP Algorithms”
- Section 5.28.8.3, “Adding ESP Algorithms”
- Section 5.28.8.4, “Deleting ESP Algorithms”

Section 5.28.8.1
Configuring ESP Encryption

To configure the encryption algorithm for the Encapsulate Security Payload (ESP), do the following:

1. Make sure the CLI is in Configuration mode.
2. Navigate to ***tunnel » ipsec » connection » {connection} » esp***, where *{connection}* is the name of the connection.
3. Configure the encryption algorithm by typing:

```
tunnel ipsec connection connection esp modgroup modgroup
```

Where:

- *connection* is the name of the connection
- *modgroup* is the value of the modgroup

4. If required, add additional cipher algorithms. For more information on how to add algorithms, refer to Section 5.28.8.3, "Adding ESP Algorithms"
5. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.28.8.2

Viewing a List of ESP Algorithms

To view a list of algorithms for the Encapsulate Security Payload (ESP) protocol, type:

```
show running-config tunnel ipsec connection connection esp algorithm
```

Where:

- *connection* is the name of the connection

If algorithms have been configured, a table or list similar to the following example appears:

```
tunnel
 ipsec
  connection ipsec-12
   esp algorithm aes256 sha1
   !
  !
 !
!
```

If no algorithms have been configured, add algorithms as needed. For more information, refer to Section 5.28.8.3, "Adding ESP Algorithms".

Section 5.28.8.3

Adding ESP Algorithms

To add a new algorithm for the Encapsulated Security Payload (ESP) protocol, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the algorithm by typing:

```
tunnel ipsec connection connection esp algorithm cipher cipher hash method
```

Where:

- *connection* is the name of the connection
- *cipher* is the cipher algorithm
- *method* is the hash method

3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.28.8.4
Deleting ESP Algorithms

To delete an algorithm for the Encapsulated Security Payload (ESP) protocol, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the algorithm by typing:

```
no tunnel ipsec connection connection esp algorithm cipher cipher hash method
```

   Where:
   - *connection* is the name of the connection
   - *cipher* is the cipher algorithm
   - *method* is the hash method
3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.28.9
Configuring the Connection Ends

Each IPsec tunnel has two ends: the local router and the remote router. These are otherwise referred to as the left and right connections, respectively. Both ends can have the same configuration or a unique configuration.

> **NOTE**
> *The configuration forms for the left and right connection ends are the same.*

To configure a connection end for an IPsec tunnel, do the following:

1. Make sure the CLI is in Configuration mode.
2. 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.
3. Configure the following parameter(s) as required:

Parameter	Description
nat-traversal-negotiation { nat-traversal-negotiation }	**Synopsis:** default, draft-ietf-ipsec-nat-t-ike-02, rfc-3947 **Default:** default The NAT traversal negotiation method. Some IPsec endpoints prefer RFC 3947 over draft-ietf-ipsec-nat-t-ike-02 when connecting with Openswan, as these implementations use different identifiers when NAT is involved. For example, when a Windows XP/2003 client connects, Openswan reports the main mode peer ID is ID_FQDN: '@example.com', but when a Vista, Windows 7 or other RFC 3947 compliant client connects, Openswan reports the main mode peer ID is ID_IPV4_ADDR: '192.168.1.1'. This will cause issues connecting to the IPsec server. In such cases, setting this option to draft-ietf-ipsec-nat-t-ike-02 will solve this problem. The default value is 'rfc-3947' unless overwritten by the default connection setting.
type { type }	**Synopsis:** none, default-route, any, address, hostname **Default:** none The public IP address type.
value { value }	The public hostname or IP address.
type { type }	**Synopsis:** default, none, from-certificate, address, hostname, der-asn1-dn, user-fqdn **Default:** default

Parameter	Description
	The system identifier type. The default value is 'left side public-ip' unless overwritten by the default connection setting.
value { value }	The hostname, IP address or the Distinguished Name in the certificate.
type { type }	**Synopsis:** none, rsasig, certificate-any, certificate **Default:** none Key type.
rsa-sig { rsa-sig }	The RSA signature key name.
rsa-sig-ipsec { rsa-sig-ipsec }	The RSA signature in IPsec format.
certificate { certificate }	The selected certificate.
type { type }	**Synopsis:** default, default-route, address **Default:** default The next hop type. The default value is 'right side public-ip' unless overwritten by the default connection setting.
value { value }	The IP address of the next hop that can be used to reach the destination network.

4. If required, configure a subnet for the connection end. For more information, refer to Section 5.28.10.1, “Configuring Private Subnets for Connection Ends”.
5. Type **`commit`** and press **Enter** to save the changes, or type **`revert`** and press **Enter** to abort.

Section 5.28.10

Managing Private Subnets

If the device is connected to an internal, private subnet, access to the subnet can be granted to the device at the other end of the IPsec tunnel. Only the IP address and mask of the private subnet is required.

The following sections describe how to configure and manage addresses for private subnets:

- Section 5.28.10.1, “Configuring Private Subnets for Connection Ends”
- Section 5.28.10.2, “Viewing a List of Addresses for Private Subnets”
- Section 5.28.10.3, “Adding an Address for a Private Subnet”
- Section 5.28.10.4, “Deleting an Address for a Private Subnet”

Section 5.28.10.1

Configuring Private Subnets for Connection Ends

To configure a private subnet for either the left (local router) or right (remote router) connection ends in a VPN, do the following:

1. Make sure the CLI is in Configuration mode.
2. Navigate to ***tunnel » ipsec » connection/{end} » subnet***, where *{end}* is the either the left (local router) or right (remote router) connection end.
3. Configure the following parameter(s) as required:

Parameter	Description
{ network }	The IP address/prefix.

4. Add one or more subnet addresses. For more information, refer to Section 5.28.10.3, “Adding an Address for a Private Subnet”.
5. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.28.10.2
Viewing a List of Addresses for Private Subnets

To view a list of addresses configured for private subnets, type:

```
show running-config tunnel ipsec connection connection {right | left} subnet
```

Where:

- *connection* is the name of the connection

If addresses have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config tunnel ipsec connection ipsec-12 left subnet
tunnel
 ipsec
  connection ipsec-12
   left
    subnet 192.168.11.0/24
    !
   !
  !
 !
!
```

If no addresses have been configured, add addresses as needed. For more information, refer to Section 5.28.10.3, “Adding an Address for a Private Subnet”.

Section 5.28.10.3
Adding an Address for a Private Subnet

To add a new address for a private subnet, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the address by typing:

```
tunnel ipsec connection connection {right | left} subnet address
```

   Where:

   - *address* is the address and prefix of the private subnet
3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.28.10.4

Deleting an Address for a Private Subnet

To delete an address for a private subnet, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the address by typing:

   ```
   no tunnel ipsec connection connection {right | left} subnet address
   ```

   Where:

   - *address* is the address and prefix of the private subnet
3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.29

Managing Layer 2 Tunnels

ROX II is capable of extending the range of services that communicate solely via Layer 2 protocols (i.e. at the level of Ethernet) by tunnelling them over routed IP networks. The Layer 2 Tunnel Daemon supports the IEC61850 GOOSE protocol as well as a generic mechanism for tunnelling by Ethernet type.

The following sections describe how to configure and manage Layer 2 tunnels:

Section 5.29.1

Viewing the Round Trip Time Statistics

The round trip time statistics reflect the measured round trip time to each remote daemon. The minimum, average, maximum and standard deviation of times is presented. Entries with a large difference between the `transmitted` and `received` parameters indicate potential problems.

To view the round trip time statistics, type:

> **NOTE**
> *Round trip time statistics are only available when remote daemon IP addresses are configured for generic tunnels. For more information about remote daemon IP addresses, refer to* *Section 5.29.8, “Managing Remote Daemon IP Addresses for Generic Tunnels”.*

```
show tunnel l2tunneld status round-trip-time
```

A table or list similar to the following example appears:

```
ruggedcom# show tunnel l2tunneld status round-trip-time
                                    MINIMUM   AVERAGE   MAXIMUM
REMOTE IP    TRANSMITTED  RECEIVED  RTT       RTT       RTT       DEVIATION
-----------------------------------------------------------------------------
192.168.5.1  45           42        0.277000  0.917000  3.735000  0.556000
```

This table or list provides the following information:

Parameter	Description
remote-ip	The IP address of remote daemon.

Section 5.29.2

Configuring L2TP Tunnels

The Layer Two Tunneling Protocol (L2TP) is used primarily to tunnel Point-to-Point Protocol (PPP) packets through an IP network, although it is also capable of tunneling other layer 2 protocols.

ROX II utilizes L2TPD in conjunction with Openswan and PPP to provide support for establishing a secure, private connection with the router using the Microsoft Windows VPN/L2TP client.

IMPORTANT!
L2TPD listens on UDP port 1701. If a firewall is enabled, it must be configured to only allow connections to L2TPD through IPsec . Direct connections to L2TPD must be prevented.

To configure L2TP tunnels, do the following:

1. Make sure the CLI is in Configuration mode.
2. Navigate to ***tunnel » l2tp*** and configure the following parameter(s) as required:

Parameter	Description
enabled	Enables L2TP.
local-ip { local-ip }	The local IP address. When set, all L2TP interfaces (l2tp-ppp-0, l2tp-ppp-1, etc.) will use the same IP address. To use different local IP addresses (chosen from an IP pool) for different L2TP interfaces, leave this parameter empty.
first-ip { first-ip }	The first address in the IP address pool. If local-ip is not set, both local and remote IP addresses will be taken from this pool.
max-connection { max-connection }	The maximum number of connections.
closing-wait-timeout { closing-wait-timeout }	**Default:** 60 The number of seconds to wait before the tunnel is cleaned up after the tunnel moves to closing-wait state.
primary { primary }	The primary DNS server.
secondary { secondary }	The secondary DNS server.
primary { primary }	The primary WINS server.
secondary { secondary }	The secondary WINS server.
auth-local	Authorizes locally instead of using radius server.

Parameter	Description
mtu { mtu }	**Default:** 1410 The Maximum Transmit Unit (MTU) or maximum packet size transmitted.
mru { mru }	**Default:** 1410 The Maximum Receive Unit (MRU) or maximum packet size passed when received.

3. Type **`commit`** and press **Enter** to save the changes, or type **`revert`** and press **Enter** to abort.

Section 5.29.3
Configuring L2TPv3 Tunnels

L2TPv3 improves the performance of bridging Ethernet frames over a WAN interface. Ethernet frames are bridged over an IP network at high data packet rates and low CPU consumption. IEC61850 GOOSE messages exchange and LAN extension are some applications of this feature.

ROX II supports Static L2TPv3 tunnel over UDP starting with version 2.5. Static tunnel is an unmanaged tunnel type. All tunnel information, such as tunnel id, session id, cookies etc., must be agreed in advance between two endpoints to establish a tunnel. There are no control messages exchanged with this type of tunnel.

To configure L2TPv3 tunnels, do the following:

1. Make sure the CLI is in Configuration mode.
2. Navigate to ***tunnel » l2tpv3 » static*** and configure the following parameter(s) as required:

Parameter	Description
enabled	Enables the static L2TPv3 service

3. Navigate to ***tunnel » l2tpv3 » static » tunnel*** and configure the following parameter(s) as required:

Parameter	Description
{ tunnel-name }	Tunnel name, contains any lower case letter or numerical digit. Prefix 'l2t-' will be added to tunnel name and session name to create l2tpv3 system interface name (ie. l2tp-1-1)
enabled	**Default:** true Enables/Disables the tunnel
tunnel-id { tunnel-id }	The local tunnel-id
remote-tunnel-id { remote-tunnel-id }	Tunnel-id of remote tunnel endpoint
local-ip { local-ip }	Ip address of local interface
local-port { local-port }	Local listening transport port for tunnel service
remote-ip { remote-ip }	Ip address of remote tunnel endpoint
remote-port { remote-port }	The listening transport port of remote device for tunnel service

4. Navigate to ***tunnel » l2tpv3 » static » tunnel » session*** and configure the following parameter(s) as required:

Parameter	Description
{ session-name }	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)
enabled	**Default:** true Enables/Disables the session
local-session-id { local-session-id }	The local session-id provides the necessary context for all further packet processing
remote-session-id { remote-session-id }	The remote session-id is used to identify the received data messages from remote session endpoint
mtu { mtu }	**Default:** 1488 MTU of network interface
size { size }	**Synopsis:** 4, 8 Cookie size in byte.
low-value { low-value }	Lower value of cookie. This value must match with low-value of other endpoint's remote cookie
high-value { high-value }	Higher value of cookie if the cookie size is 8. This value must match with high-value of other endpoint's remote cookie
size { size }	**Synopsis:** 4, 8 Cookie size in byte
low-value { low-value }	Lower value of cookie. This value must match with low-value of other endpoint's local cookie
high-value { high-value }	Higher value of cookie if its size is 8. This value must match with high-value of other endpoint's local cookie

5. Navigate to ***tunnel » l2tpv3 » static » tunnel » session » vlan*** and configure the following parameter(s) as required:

Parameter	Description
{ vid }	VLAN ID for this routable logical interface

For more information about VLANs, refer to Section 5.35, “Managing VLANs”.

6. Type **`commit`** and press **Enter** to save the changes, or type **`revert`** and press **Enter** to abort.

Section 5.29.4
Configuring the Layer 2 Tunnel Daemon

To configure the Layer 2 tunnel daemon, do the following:

> **IMPORTANT!**
> *Make sure there are no traffic loops possible between the substation LAN and other LANs that could forward GOOSE frames to the LAN. Do not employ a GOOSE gateway between substations that are already connected. The GOOSE daemon issues packets to the network with a built in Time-To-Live (TTL) count that is decremented with each transmission. This prevents an infinite loop of packets, but will not prevent excessive network utilization.*

1. Make sure the CLI is in Configuration mode.
2. Navigate to ***tunnel » l2tunneld*** and configure the following parameter(s) as required:

Parameter	Description
enabled	Enables the Layer 2 protocols server.
udp-port { udp-port }	**Default:** 1311 The UDP port to communicate with the other daemon.
beacon-interval { beacon-interval }	**Synopsis:** off **Default:** 60 The Round Trip Time (RTT) of the sent message

3. Add GOOSE or generic tunnels as required. For more information, refer to Section 5.29.5.3, “Adding a GOOSE Tunnel” or Section 5.29.7.3, “Adding a Generic Tunnel”.
4. Type **`commit`** and press **Enter** to save the changes, or type **`revert`** and press **Enter** to abort.

Section 5.29.5

Managing GOOSE Tunnels

The GOOSE tunnel feature provides the capability to bridge GOOSE frames over a Wide Area Network (WAN).

GOOSE tunnels provide the following features:

- GOOSE traffic is bridged over the WAN via UDP/IP.
- One GOOSE traffic source can be mapped to multiple remote router Ethernet interfaces in mesh fashion.
- To reduce bandwidth consumption, GOOSE daemons may be located at each of the *legs* and at the center of a star network. The centrally located daemon will accept GOOSE packets and re-distribute them.
- Statistics report availability of remote GOOSE daemons, packet counts and Round Trip Time (RTT) for each remote daemon.
- When the Virtual Router Redundancy Protocol (VRRP) is employed, GOOSE transport is improved by sending redundant GOOSE packets from each VRRP gateway.
- You can enable GOOSE forwarding by configuring a generic Layer 2 tunnel. When configured, the device listens for GOOSE packets on one VLAN and forwards them to another VLAN.

The GOOSE protocol is supported by the Layer 2 Tunnel Daemon. The daemon listens to configured Ethernet interfaces and to the network itself (i.e. for tunnel connections from other daemon instances) on a configurable UDP port.

The Media Access Control (MAC) destination address of frames received from Ethernet is inspected in order to determine which GOOSE group they are in. The frames are then encapsulated in network headers and forwarded (with MAC source and destination addresses intact) to the network as GOOSE packets.

IEC61850 recommends that the MAC destination address should be in the range 01:0c:cd:01:00:00 to 01:0c:cd:01:01:ff.

GOOSE packets received from the network are stripped of their network headers and forwarded to Ethernet ports configured for the same multicast address. The forwarded frames contain the MAC source address or the originating device, and not that of the transmitting interface. The VLAN used will be that programmed locally for the interface and may differ from the original VLAN. The frame will be transmitted with the highest 802.1p priority level (p4).

Packets received from the network will also be forwarded to any other remote daemons included in the group.

To enable forwarding for GOOSE packets, configure a generic Layer 2 tunnel to listen for GOOSE packets on one VLAN and forward them to a second VLAN. To configure the generic Layer 2 tunnel for this operation, set the following for the tunnel:

- Ethernet Interface: select the VLAN on which the GOOSE packets originate
- Ethernet Type: set as 0x88b8
- Remote Daemon: select the VLAN to which to forward the GOOSE packets

The following sections describe how to configure and manage GOOSE tunnels:

- Section 5.29.5.1, “Viewing the GOOSE Tunnel Statistics”
- Section 5.29.5.2, “Viewing a List of GOOSE Tunnels”
- Section 5.29.5.3, “Adding a GOOSE Tunnel”
- Section 5.29.5.4, “Deleting a GOOSE Tunnel”

Section 5.29.5.1
Viewing the GOOSE Tunnel Statistics

To view the GOOSE tunnel statistics, type:

```
show tunnel l2tunneld status goose
```

A table or list similar to the following example appears:

```
ruggedcom# show tunnel l2tunneld status goose
l2tunneld status goose test
 ifname    switch.0100
 mac       01:0c:cd:01:00:33
 rx frames 2
 tx frames 0
 rx chars  114
 tx chars  0
 errors    0
 connections
             RX       TX       RX      TX
REMOTE IP    PACKETS  PACKETS  BYTES   BYTES   ERRORS
-----------------------------------------------------
192.168.2.2  2        0        122     0       0
```

This table or list provides the following information:

Parameter	Description
tunnel-name	The GOOSE tunnel name.

Section 5.29.5.2
Viewing a List of GOOSE Tunnels

To view a list of GOOSE tunnels, type:

```
show running-config tunnel l2tunneld goose
```

If tunnels have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config tunnel l2tunneld goose tunnel | tab
                                      IP
```

```
NAME  INTERFACE    MULTICAST MAC      ADDRESS
-----------------------------------------------
1     switch.0001  01:0c:cd:01:01:01

!
```

If no GOOSE tunnels have been configured, add tunnels as needed. For more information, refer to Section 5.29.5.3, “Adding a GOOSE Tunnel”.

Section 5.29.5.3
Adding a GOOSE Tunnel

To configure a GOOSE tunnel, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the tunnel by typing:

```
tunnel l2tunneld goose tunnel name
```

Where:

- *name* is the name of the GOOSE tunnel

3. Configure the following parameter(s) as required:

Parameter	Description
interface { interface }	The interface to listen on for GOOSE frames.
multicast-mac { multicast-mac }	The multicast MAC address to listen for.

4. If necessary, configure one or more remote daemons for the tunnel. For more information, refer to Section 5.29.6.2, “Adding a Remote Daemon”.
5. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.29.5.4
Deleting a GOOSE Tunnel

To delete a GOOSE tunnel, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the GOOSE tunnel by typing:

```
no tunnel l2tunneld goose tunnel name
```

Where:

- *name* is the name of the GOOSE tunnel

3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.29.6

Managing Remote Daemons for GOOSE Tunnels

In place of a local Ethernet interface for the tunnel egress, IP addresses for a remote daemon can be specified. Several endpoints may be added with these fields using successive edits of the tunnel configuration.

The following sections describe how to configure and manage remote daemons for GOOSE tunnels:

- Section 5.29.6.1, “Viewing a List of Remote Daemons”
- Section 5.29.6.2, “Adding a Remote Daemon”
- Section 5.29.6.3, “Deleting a Remote Daemon”

Section 5.29.6.1

Viewing a List of Remote Daemons

To view a list of remote daemons configured for a GOOSE tunnel, type:

```
show running-config tunnel l2tunneld goose tunnel name remote-daemon
```

Where:

- *name* is the name of the GOOSE tunnel

If tunnels have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config tunnel l2tunneld goose tunnel 1 remote-daemon
tunnel
 l2tunneld goose tunnel 1
  remote-daemon 192.168.10.2
  !
 !
!
```

If no remote daemons have been configured, add daemons as needed. For more information, refer to Section 5.29.6.2, “Adding a Remote Daemon”.

Section 5.29.6.2

Adding a Remote Daemon

To configure a remote daemon for a GOOSE tunnel, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the remote daemon by typing:

   ```
   tunnel l2tunneld goose tunnel remote-daemon address
   ```

   Where:

   - *address* is the IP address of the remote daemon
3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.29.6.3

Deleting a Remote Daemon

To delete a remote daemon, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the remote daemon typing:

```
no tunnel l2tunneld goose tunnel name remote-daemon address
```

   Where:

   - *name* is the name of the GOOSE tunnel
   - *address* is the IP address of the remote daemon
3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.29.7

Managing Generic Tunnels

The Layer 2 Tunnel Daemon supports a generic mode of operation based on the Ethernet type of Layer 2 data traffic seen by the router. Multiple tunnels may be configured, each one with:

- an Ethernet type
- a tunnel ingress (Ethernet interface)
- a tunnel egress (either another locally connected Ethernet interface, or the remote IP address of another Layer 2 Tunnel daemon instance running on another Router)

The following sections describe how to configure and manage generic tunnels:

- Section 5.29.7.1, “Viewing the Generic Tunnel Statistics”
- Section 5.29.7.2, “Viewing a List of Generic Tunnels”
- Section 5.29.7.3, “Adding a Generic Tunnel”
- Section 5.29.7.4, “Deleting a Generic Tunnel”

Section 5.29.7.1

Viewing the Generic Tunnel Statistics

To view the generic tunnel statistics, type:

```
show tunnel l2tunneld status generic
```

A table or list similar to the following example appears:

```
ruggedcom# show tunnel l2tunneld status generic
TUNNEL                   RX      TX      RX     TX                               RX       TX       RX     TX
NAME     IFNAME          FRAMES  FRAMES  CHARS  CHARS  ERRORS  REMOTE IP    PACKETS  PACKETS  BYTES  BYTES
 ERRORS
---------------------------------------------------------------------------------------------
iso      switch.0002  5       6       300    360    0
                                                               192.168.5.1  11       0        704    0
 0
```

This table or list provides the following information:

Parameter	Description
tunnel-name	The generic tunnel name.

Section 5.29.7.2
Viewing a List of Generic Tunnels

To view a list of generic tunnels, type:

```
show running-config tunnel l2tunneld generic tunnel
```

If tunnels have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config tunnel l2tunneld generic tunnel | tab
                   REPLACE        EGRESS  IP
NAME  INGRESS IF   MAC      TYPE  IF      ADDRESS
---------------------------------------------------
1     switch.0001  -
                            iso

!
```

If no generic tunnels have been configured, add tunnels as needed. For more information, refer to Section 5.29.7.3, “Adding a Generic Tunnel”.

Section 5.29.7.3
Adding a Generic Tunnel

To configure a generic tunnel, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the tunnel by typing:

   ```
   tunnel l2tunneld generic tunnel name
   ```

   Where:

   - *name* is the name of the generic tunnel
3. Configure the following parameter(s) as required:

Parameter	Description
ingress-if { ingress-if }	The interface to listen on for Ethernet type frames.
replace-mac	Replaces the sender's MAC with the out-interface's MAC.

4. If necessary, configure one or more remote daemon IP addresses for the tunnel. For more information, refer to Section 5.29.8.2, “Adding an IP Address”.
5. If necessary, define one or more ethernet types to be forwarded. For more information, refer to Section 5.29.10.2, “Adding an Ethernet Type”.
6. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.29.7.4

Deleting a Generic Tunnel

To delete a generic tunnel, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the generic tunnel by typing:

   ```
   no tunnel l2tunneld generic tunnel name
   ```

   Where:

   - *name* is the name of the generic tunnel
3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.29.8

Managing Remote Daemon IP Addresses for Generic Tunnels

In place of a local Ethernet interface for the tunnel egress, IP addresses for a remote daemon can be specified. Several endpoints may be added with these fields using successive edits of the tunnel configuration.

> **NOTE**
> *When a remote daemon IP address is configured, the interface on the receiver side, where traffic leaves, should be configured on the ingress interface (instead of egress interface).*

The following sections describe how to configure and manage remote daemon IP addresses for generic tunnels:

- Section 5.29.8.1, “Viewing a List of IP Addresses”
- Section 5.29.8.2, “Adding an IP Address”
- Section 5.29.8.3, “Deleting an IP Address”

Section 5.29.8.1

Viewing a List of IP Addresses

To view a list of remote L2 protocol server IP addresses for a generic tunnel configuration, type:

```
show running-config tunnel l2tunneld generic tunnel remote-daemon
```

If tunnels have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config tunnel l2tunneld generic tunnel remote-daemon ip-address | tab
NAME  IP ADDRESS
--------------------
1
      172.112.10.1

!
```

If no generic tunnels have been configured, add tunnels as needed. For more information, refer to Section 5.29.7.3, “Adding a Generic Tunnel”.

Section 5.29.8.2
Adding an IP Address

To add the IP address of a remote L2 protocols server to a generic tunnel configuration, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the IP address by typing:

```
tunnel l2tunneld generic tunnel name remote-daemon ip-address address
```

   Where:

   - *name* is the name of the generic tunnel
   - *address* is the IP address of the remote L2 protocols server
3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.29.8.3
Deleting an IP Address

To delete the IP address of a remote L2 protocols server from a generic tunnel configuration, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the IP address by typing:

```
no tunnel l2tunneld generic tunnel name remote-daemon ip-address address
```

   Where:

   - *name* is the name of the generic tunnel
   - *address* is the IP address of the remote L2 protocols server
3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.29.9
Managing Remote Daemon Egress Interfaces for Generic Tunnels

The following sections describe how to configure and manage remote daemon egress interfaces for generic tunnels:

- Section 5.29.9.1, “Viewing a List of Egress Interfaces”
- Section 5.29.9.2, “Adding an Egress Interface”
- Section 5.29.9.3, “Deleting an Egress Interface”

Section 5.29.9.1
Viewing a List of Egress Interfaces

To view a list of egress interfaces configured for a generic tunnel, type:

```
show running-config tunnel l2tunneld generic tunnel remote-daemon egress-if
```

If egress interfaces have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config tunnel l2tunneld generic tunnel remote-daemon egress-if | tab
NAME  EGRESS IF
-------------------
1
      switch.0001

!
```

If no egress interfaces have been configured, add interfaces as needed. For more information, refer to Section 5.29.9.2, “Adding an Egress Interface”.

Section 5.29.9.2
Adding an Egress Interface

To add an egress interface for a generic tunnel, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the egress interface by typing:

   ```
   tunnel l2tunneld generic tunnel name remote-daemon egress-if interface
   ```

   Where:

   - *name* is the name of the generic tunnel
   - *interface* is the egress interface for Ethernet type frames
3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.29.9.3
Deleting an Egress Interface

To delete an egress interface for a generic tunnel, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the egress interface by typing:

   ```
   no tunnel l2tunneld generic tunnel name remote-daemon egress-if interface
   ```

   Where:

   - *name* is the name of the generic tunnel
   - *interface* is the egress interface for Ethernet type frames
3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.29.10
Managing Ethernet Types for Generic Tunnels

The following sections describe how to configure and manage Ethernet types for generic tunnels:

- Section 5.29.10.1, “Viewing a List of Ethernet Types”
- Section 5.29.10.2, “Adding an Ethernet Type”

- Section 5.29.10.3, “Deleting an Ethernet Type”

Section 5.29.10.1
Viewing a List of Ethernet Types

To view a list of Ethernet types configured for a generic tunnel, type:

```
show running-config tunnel l2tunneld generic tunnel ethernet-type
```

If Ethernet types have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config tunnel l2tunneld generic tunnel ethernet-type | tab
NAME  TYPE
------------
1
      iso

!
```

If no Ethernet types have been configured, add types as needed. For more information, refer to Section 5.29.10.2, “Adding an Ethernet Type”.

Section 5.29.10.2
Adding an Ethernet Type

To add an Ethernet type for a generic tunnel, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the Ethernet type by typing:

   ```
   tunnel l2tunneld generic tunnel name ethernet-type type
   ```

   Where:

   - *name* is the name of the generic tunnel
   - *type* is the Ethernet type to be forwarded (i.e. 0xFEFE)
3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.29.10.3
Deleting an Ethernet Type

To delete an Ethernet type for a generic tunnel, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the Ethernet type by typing:

   ```
   no tunnel l2tunneld generic tunnel name ethernet-type type
   ```

   Where:

   - *name* is the name of the generic tunnel
   - *type* is the Ethernet type (i.e. 0xFEFE)
3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.30

Managing Generic Routing Encapsulation Tunnels

ROX II can employ the Generic Routing Encapsulation (GRE) protocol to encapsulate multicast traffic and IPv6 packets together and transport them through an IPv4 network tunnel. As such, GRE tunnels can transport traffic through any number of intermediate networks.

The key parameters for GRE tunnels is the tunnel name, local router address, remote router address and remote subnet.

The following illustrates a typical GRE tunnel configuration:

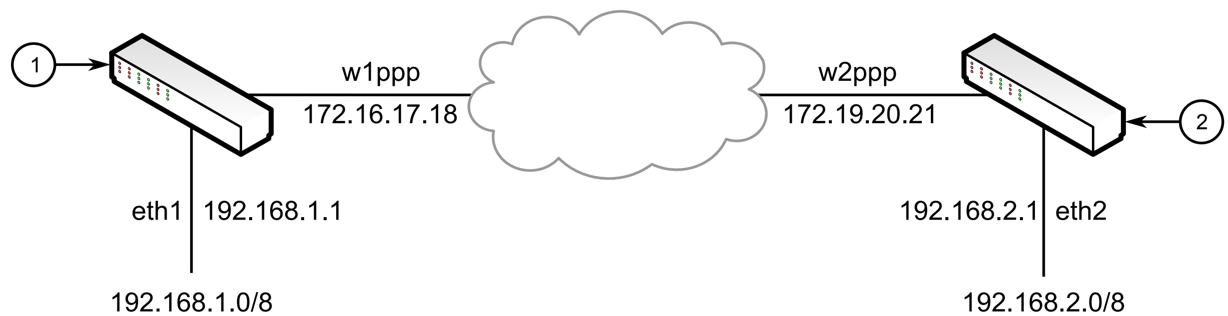

Figure 11: Example – GRE Tunnel Configuration

1. Router 1 **2.** Router 2

In this example, Router 1 establishes a GRE tunnel to Router 2 using a local router address of 172.16.17.18, a remote router address of 172.19.20.21, and a remote subnet of 192.168.2.0/24.

NOTE
When connecting a Cisco router (in place of Router 1 in the previous example), the local router address corresponds to the Cisco IOS source address and the remote router address corresponds to the destination address.

The cost of the GRE tunnel can also be set if another method of routing between Router 1 and Router 2 becomes available. The packets will automatically flow through the lowest cost route.

Packets can also be restricted by specifying a local egress device, such as w1pp in the case of Router 1 in the previous example.

The following sections describe how to configure and manage Generic Routing Encapsulation (GRE) tunnels:

- Section 5.30.1, “Viewing Statistics for GRE Tunnels”
- Section 5.30.2, “Viewing a List of GRE Tunnels”
- Section 5.30.3, “Adding a GRE Tunnel”
- Section 5.30.4, “Deleting a GRE Tunnel”

Section 5.30.1

Viewing Statistics for GRE Tunnels

To view the statistics collected for GRE tunnels, type:

```
show interfaces gre
```

A table or list similar to the following example appears:

```
ruggedcom# show interfaces gre
        TUNNEL  RX        RX       RX      TX        TX       TX
IFNAME  STATUS  PACKETS   ERRORS   DROPS   PACKETS   ERRORS   DROPS
----------------------------------------------------------------
g1      Active  52        0        0       855       51       0
g2      Active  0         0        0       0         791      0
```

This table or list provides the following information:

Parameter	Description
ifname	The GRE tunnel interface name.
tunnel-status	The status of the tunnel.
rx-packets	The number of packets received through the tunnel.
rx-errors	The error packets received through the tunnel.
rx-drops	The number of packets dropped by the tunnel.
tx-packets	The number of packets transmitted through the tunnel.
tx-errors	The number of error packets transmitted through the tunnel.
tx-drops	The number of packets dropped by the tunnel.

Section 5.30.2

Viewing a List of GRE Tunnels

To view a list of GRE tunnels, type:

```
show running-config tunnel gre
```

If GRE tunnels have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config tunnel gre | tab
IF
NAME  LOCAL IP      REMOTE IP     REMOTE NET      MTU   MULTICAST  COST
-------------------------------------------------------------------------
gre   172.16.17.18  172.19.20.21  192.168.2.0/24  1476  -          0
```

If no GRE tunnels have been configured, add tunnels as needed. For more information, refer to Section 5.30.3, “Adding a GRE Tunnel”.

Section 5.30.3

Adding a GRE Tunnel

To add a GRE tunnel, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the GRE tunnel by typing:

```
tunnel gre name
```

Where:

- *name* is the interface name of the GRE tunnel network. The interface name must start with a lowercase letter, but may contain any combination of lowercase letters, numbers and dashes up to a maximum of 10 characters. The prefix *gre-* will be added to this interface name.

3. Configure the following parameter(s) as required:

Parameter	Description
local-ip { local-ip }	The IP address of the local end of the tunnel.
remote-ip { remote-ip }	The IP address of the remote end of the tunnel.
remote-net { remote-net }	The target network of the remote end of the tunnel (xxx.xxx.xxx.xxx/xx).
mtu { mtu }	**Default:** 1476 The MTU of the GRE interface.
multicast	Enables multicast traffic on the tunnel interface.
cost { cost }	**Default:** 1 The routing cost associated with networking routing that directs traffic through the tunnel.

4. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.30.4

Deleting a GRE Tunnel

To delete a GRE tunnel, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the GRE tunnel by typing:

```
no tunnel gre name
```

Where:

- *name* is the name of the GRE tunnel

3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.31
Managing Layer 3 Switching

A switch is an inter-network device that makes frame forwarding decisions in hardware. A Layer 3 switch, sometimes called a multilayer switch, is one which makes hardware-based decisions for IP packets as well as Layer 2 frames. Traditionally, routers are used to make routing decisions using software. A Layer 3 switch will make the same decisions in hardware, which means that packet forwarding will be much faster than in a conventional router.

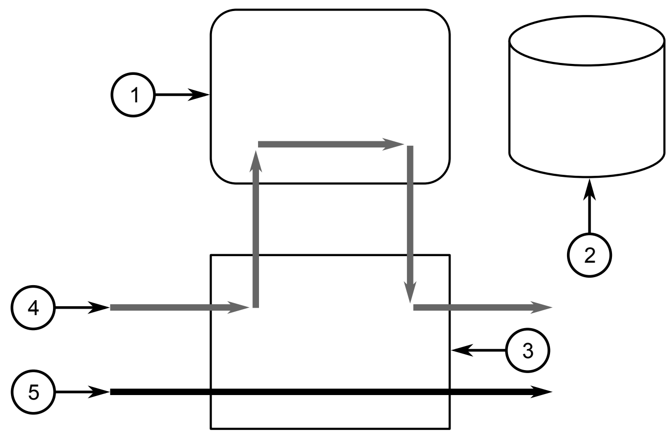

Figure 12: Conventional Layer 3 Router

1. Router **2.** Routing Table **3.** Switch **4.** Layer 3 Traffic **5.** Layer 2 Traffic

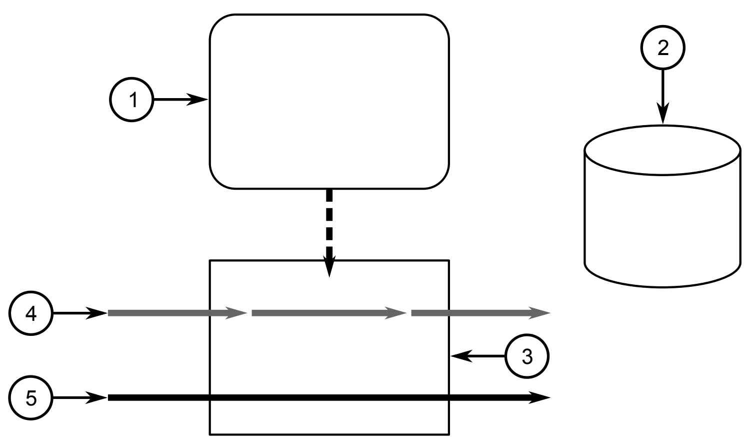

Figure 13: Layer 3 Switch

1. Router **2.** Forwarding Table **3.** Switch **4.** Layer 3 Traffic **5.** Layer 2 Traffic

The following sections describe how to configure and manage Layer 3 switching:

- Section 5.31.1, “Layer 3 Switching Concepts”
- Section 5.31.2, “Configuring Layer 3 Switching”
- Section 5.31.3, “Managing Static ARP Table Entries”

- Section 5.31.4, “Viewing a Static and Dynamic ARP Table Summary”
- Section 5.31.5, “Viewing Routing Rules”
- Section 5.31.6, “Flushing Dynamic Hardware Routing Rules”

Section 5.31.1

Layer 3 Switching Concepts

The following sections describe Layer 3 Switching concepts and rules:

- Section 5.31.1.1, “Layer 3 Switch Forwarding Table”
- Section 5.31.1.2, “Static Layer 3 Switching Rules”
- Section 5.31.1.3, “Dynamic Learning of Layer 3 Switching Rules”
- Section 5.31.1.4, “Layer 3 Switch ARP Table”
- Section 5.31.1.5, “Multicast Cross-VLAN Layer 2 Switching”
- Section 5.31.1.6, “Size of the Layer 3 Switch Forwarding Table”
- Section 5.31.1.7, “Interaction with the Firewall”

Section 5.31.1.1

Layer 3 Switch Forwarding Table

To route a packet with a specific destination IP address, a router needs the following information:

- **Egress interface (subnet):** this information is stored in the router's Routing Table.

> **NOTE**
> *In a Layer 2 switched network segment, a VLAN constitutes an IP subnet.*

- **Next-hop gateway Media Access Control (MAC) address:** this information is stored in the router's ARP Table.

> **NOTE**
> *If the next hop is the destination subnet itself, then the destination host MAC address is required.*

A Layer 3 Switch uses the routing information listed above and translates it into Layer 3 switching rules. These rules are known as the *Layer 3 Switch Forwarding Information Base (FIB)* or the *Layer 3 Switch Forwarding Table*. A Layer 3 switching rule is actually a set of parameters identifying a traffic flow to be switched and determining how to perform the switching.

Layer 3 switching Application-Specific Integrated Circuits (ASICs) store Layer 3 switching rules in a Ternary Content Addressable Memory (TCAM) table. Layer 3 switching rules can be statically configured or dynamically learned (also known as *auto-learned*).

Section 5.31.1.2

Static Layer 3 Switching Rules

When creating a static route through switch management, hardware acceleration can be explicitly configured. If hardware acceleration is selected, an appropriate Layer 3 switching rule is installed in the ASIC's TCAM and never ages out.

> **NOTE**
> *Only TCP and UDP traffic flows will be accelerated by the IP/Layer 3 switch fabric. Non-IP packet types, such as ICMP and IGMP, will not be accelerated.*

Section 5.31.1.3

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 5.31.1.4

Layer 3 Switch ARP Table

A router needs to know the destination host or next-hop gateway MAC address for it to forward a packet on the other subnet. Therefore, software maintains an Address Resolution Protocol (ARP) table that maps IP addresses to MAC addresses. The same information is also needed by the Layer 3 switching ASIC when it switches IP packets between subnets.

The destination or gateway MAC address is usually obtained through ARP. However, ARP entries can also be statically configured in the Layer 3 Switch so that they do not time out. When configuring a static ARP entry, if no value is entered for the MAC Address parameter, the address is automatically resolved through ARP and then saved statically. This is preserved across reboots of the device.

For a static Layer 3 switching rule, the destination MAC address for the rule is always resolved, and is also saved statically.

Section 5.31.1.5

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 egress VLAN in the multicast switching rule. For example, a multicast stream ingressing VLAN 1 and egressing VLAN 2 and VLAN 3 requires two TCAM table entries: one for VLAN 2 and one for VLAN 3.
- Supported bandwidth depends on the rule. Multicast traffic potentially has multiple egress VLANs, and the total utilized ASIC bandwidth is the ingress bandwidth multiplied by the number of ingress and egress VLANs. For example, a 256 Mbps multicast stream ingressing VLAN 1 and egressing VLANs 2 and 3 requires 768 Mbps (256 Mbps × 3) of ASIC bandwidth.
- If a multicast packet should be forwarded to multiple egress VLANs, it egresses those VLANs sequentially rather than concurrently. This means the packet will experience different latency for each egress VLAN.

Section 5.31.1.6

Size of the Layer 3 Switch Forwarding Table

The routing table in a software router is limited only by the amount of available memory; its size can be virtually unlimited. However, the size of the TCAM in Layer 3 switching ASICs is significantly limited and may not be sufficient to accommodate all Layer 3 switching rules. If the TCAM is full and a new static rule is created, the new rule replaces some dynamically learned rule. If all of the rules in the TCAM are static, then the new static rule is rejected.

Section 5.31.1.7

Interaction with the Firewall

If security is a concern and you use a firewall in a Layer 3 Switch, it is important to understand how the Layer 3 switch interacts with the firewall.

A software router always works in agreement with a firewall so that firewall rules are always applied. However, in a Layer 3 Switch, if a switching rule is set in the switching ASIC (for example, due to a statically configured route), the ASIC switches all the traffic matching the rule before the firewall inspects the traffic.

Layer 3 switch ASICs are somewhat limited in how switching rules can be defined. These limitations do not allow configuring arbitrary firewall rules directly in the Layer 3 switch hardware. For sophisticated firewall rules, the firewall has to be implemented in software and the Layer 3 Switch must not switch traffic that is subject to firewall processing.

Whenever a change is made to the firewall configuration, some of the dynamically learned Layer 3 switching rules might conflict with the new firewall configuration. To resolve potential conflicts, dynamically learned Layer 3 switching rules are flushed upon any changes to the firewall configuration. The dynamically learned Layer 3 switching rules then have to be re-learned while the new firewall rules are applied.

For statically configured Layer 3 switching rules, take care to avoid conflicts between Layer 3 switching and the firewall. It should be understood that static Layer 3 switching rules always take precedence. Therefore, you must thoroughly examine the switch configuration for potential conflicts with the firewall. For more information about firewalls, refer to Section 5.17, “Managing Firewalls”

Section 5.31.2

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. Make sure the CLI is in Configuration mode.
2. To configure Layer 3 Switching , type:

```
switch layer3-switching
```

Configure the following parameter(s) as required:

Parameter	Description
unicast-mode { unicast-mode }	**Synopsis:** disabled, auto, static **Default:** auto • Disabled: Layer 3 switching is disabled. The ability to disable routing hardware acceleration may be desired, for example, in a system with sophisticated firewall rules, which could not be supported by the Layer 3 switching ASIC and would require software processing. • Static: Only statically configured Layer 3 switching rules will be used. This mode may be useful, for example, in a system with complex configuration where static routes do not conflict with a firewall, while traffic flows following dynamic routes have to be subject to sophisticated firewall filtering. • Auto: Both statically configured and dynamically learned Layer 3 switching rules will be used. In this mode, maximum routing hardware acceleration is utilized.
multicast-mode { multicast-mode }	**Synopsis:** disabled, auto, static **Default:** auto • Disabled: Layer 3 switching is disabled. The ability to disable routing hardware acceleration may be desired, for example, in a system with sophisticated firewall rules, which could not be supported by the Layer 3 switching ASIC and would require software processing.

Parameter	Description
	• Static: Only statically configured Layer 3 switching rules will be used. This mode may be useful, for example, in a system with complex configuration where static routes do not conflict with a firewall, while traffic flows following dynamic routes have to be subject to sophisticated firewall filtering. • Auto: Both statically configured and dynamically learned Layer 3 switching rules will be used. In this mode, maximum routing hardware acceleration is utilized.

learn-mode { learn-mode }	**Synopsis:** flow-oriented, host-oriented
	Default: flow-oriented
	Defines how dynamically learned traffic flows are identified:
	• Flow-oriented: Traffic flows are identified by a 5-tuple signature:
	`Src IP address   +`
	`Dst IP address   +`
	`Protocol         +`
	`Src TCP/UDP port +`
	`Dst TCP/UDP port`
	This mode should be used, if fine-granularity firewall filtering is configured in the device (i.e. some flows between two hosts should be forwarded, while other flows between the same two hosts should be filtered). However, this mode utilizes more Layer 3 switching ASIC resources and is not recommended if fine-granularity firewall filtering is not required.
	• Host-oriented: Traffic flows are identified by a 2-tuple signature:
	`Src IP address   +`
	`Dst IP address`
	All traffic between two IP hosts is hardware-accelerated regardless of the protocol and TCP/UDP ports. This mode potentially controls multiple flows with a single rule and hence is more efficient in utilizing Layer3 switching ASIC resources.

aging-time { aging-time }	**Default:** 32 This parameter configures the time a dynamically learned rule for a traffic flow, which has become inactive, is held before being removed from the Layer 3 switch forwarding table.

3. Type **`commit`** and press **Enter** to save the changes, or type **`revert`** and press **Enter** to abort.

Section 5.31.3

Managing Static ARP Table Entries

The following sections describe how to manage static ARP table entries:

- Section 5.31.3.1, “Viewing a List of ARP Table Entries”
- Section 5.31.3.2, “Adding a Static ARP Table Entry”
- Section 5.31.3.3, “Deleting a Static ARP Table Entry”

Section 5.31.3.1

Viewing a List of ARP Table Entries

To view a list of static ARP table entries, type:

```
show switch layer3-switching arp-table
```

```
ruggedcom# show switch layer3-switching arp-table | tab
IP ADDRESS   MAC                VID
--------------------------------------------------------
192.11.0.2   00:11:94:11:00:01  4084
192.11.0.3   00:11:94:11:00:02  4084
192.11.0.4   00:11:94:11:00:03  4084
192.11.0.5   00:11:94:11:00:04  4084
192.11.0.6   00:11:94:11:00:05  4084
```

If no ARP table entries have been configured, add static ARP table entries as needed. For more information about adding static ARP table entries, refer to Section 5.31.3.2, “Adding a Static ARP Table Entry”.

Section 5.31.3.2
Adding a Static ARP Table Entry

To add a static ARP table entry, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the table entry by typing:

```
switch layer3-switching arp-table address
```

Where:

- *address* is the IP address for the network device the entry describes

3. Configure the following parameter(s) as required:

> **NOTE**
> *Letters in MAC addresses must be lowercase.*

Parameter	Description
mac { mac }	**Default:** 00:00:00:00:00:00 The MAC address of the network device specified by the IP address.
vid { vid }	The VLAN Identifier of the VLAN upon which the MAC address operates.
status	**Synopsis:** resolved, unresolved **Default:** unresolved Address Resolution Protocol (ARP) entry resolution status: • Resolved: The 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.

4. Type **`commit`** and press **Enter** to save the changes, or type **`revert`** and press **Enter** to abort.

Section 5.31.3.3
Deleting a Static ARP Table Entry

To delete a static ARP table entry, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the key by typing:

```
no switch layer3-switching arp-table address
```

Where:

- *address* is the IP address for the network device the entry describes

3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.31.4

Viewing a Static and Dynamic ARP Table Summary

To view a static and dynamic ARP table summary, type:

```
show switch layer3-switching arp-table-summary
```

If ARP table entries have been configured, a table or list similar to the following example appears:

```
ruggedcom# show switch layer3-switching arp-table-summary
IP ADDRESS   MAC                VID   STATIC  STATUS
---------------------------------------------------------
192.11.0.2   00:11:94:11:00:01  4084  false   resolved
192.11.0.3   00:11:94:11:00:02  4084  false   resolved
192.11.0.4   00:11:94:11:00:03  4084  false   resolved
192.11.0.5   00:11:94:11:00:04  4084  false   resolved
192.11.0.6   00:11:94:11:00:05  4084  false   resolved
```

This table or list provides the following information:

Parameter	Description
ip-address	**Synopsis:** The ipv4-address type represents an IPv4 address in dotted-quad notation. The IPv4 address may include a zone index, separated by a % sign. The zone index is used to disambiguate identical address values. For link-local addresses, the zone index will typically be the interface index number or the name of an interface. If the zone index is not present, the default zone of the device will be used. The canonical format for the zone index is the numerical format The IP address of the network device the entry describes.
mac	**Default:** 00:00:00:00:00:00 The MAC address of the network device specified by the IP address.
vid	The VLAN Identifier of the VLAN upon which the MAC address operates.
static	**Default:** true Whether the entry is static or dynamic. Static entries are configured as a result of management activity. Dynamic entries are automatically learned by the device and can be unlearned.
status	**Synopsis:** resolved, unresolved **Default:** unresolved The Address Resolution Protocol (ARP) entry resolution status: • Resolved: MAC-IP address pair is resolved and operational. • Unresolved: the device hasn't resolved the MAC-IP address pair and keeps sending ARP requests periodically.

Section 5.31.5
Viewing Routing Rules

To view a list of routing rules, type:

```
show switch layer3-switching routing-rules-summary
```

A table or list similar to the following example appears:

```
ruggedcom# show switch layer3-switching routing-rules-summary
  PACKETS
RULE  RULE     IN    OUT                        SRC                  DEST                 PER
  ROUTING
ID    TYPE     VLAN  VLAN  PROTO  SOURCE        PORT  DESTINATION    PORT  GATEWAY        SECOND   STATIC
  ACTION   STATUS
----------------------------------------------------------------------------------------------
0     unicast  -     -     17     192.12.1.120  1024  192.11.1.120   1024  192.11.1.120   11       false
  forward  active
1     unicast  -     -     17     192.12.1.69   1024  192.11.1.69    1024  192.11.1.69    11       false
  forward  active
2     unicast  -     -     17     192.11.0.160  1024  192.12.0.160   1024  192.12.0.160   11       false
  forward  active
3     unicast  -     -     17     192.11.0.92   1024  192.12.0.92    1024  192.12.0.92    11       false
  forward  active
4     unicast  -     -     17     192.12.0.92   1024  192.11.0.92    1024  192.11.0.92    11       false
  forward  active
5     unicast  -     -     17     192.12.0.254  1024  192.11.0.254   1024  192.11.0.254   11       false
  forward  active
6     unicast  -     -     17     192.12.0.223  1024  192.11.0.223   1024  192.11.0.223   11       false
  forward  active
7     unicast  -     -     17     192.11.0.85   1024  192.12.0.85    1024  192.12.0.85    11       false
  forward  active
8     unicast  -     -     17     192.12.0.95   1024  192.11.0.95    1024  192.11.0.95    11       false
  forward  active
9     unicast  -     -     17     192.12.0.180  1024  192.11.0.180   1024  192.11.0.180   12       false
  forward  active
10    unicast  -     -     17     192.12.0.67   1024  192.11.0.67    1024  192.11.0.67    11       false
  forward  active
11    unicast  -     -     17     192.12.0.161  1024  192.11.0.161   1024  192.11.0.161   11       false
  forward  active
12    unicast  -     -     17     192.11.2.190  1024  192.12.2.190   1024  192.12.2.190   11       false
  forward  active
```

This table or list provides the following information:

Parameter	Description
rule-id	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	Identifies the ingress VLAN. To match the rule, the packet's ingress VLAN must match the number.
out-vlans	**Synopsis:** "out-vlans" occurs in an array of at most 255 elements Identifies the egress VLAN. The matched multicast packet is sent to the identified VLAN.
proto	The IP Encapsulated Protocol number. Unless zero is specified, the incoming packet's IP protocol must match this number.
source	**Synopsis:** The ipv4-address type represents an IPv4 address in dotted-quad notation. The IPv4 address may include a zone index, separated by a % sign. The zone index is used to disambiguate identical address values. For link-local addresses, the zone index will typically

Parameter	Description
	be the interface index number or the name of an interface. If the zone index is not present, the default zone of the device will be used. The canonical format for the zone index is the numerical format, The ipv4-prefix type represents an IPv4 address prefix. The prefix length is given by the number following the slash character and must be less than or equal to 32. A prefix length value of n corresponds to an IP address mask that has n contiguous 1-bits from the most significant bit (MSB) and all other bits set to 0. The canonical format of an IPv4 prefix has all bits of the IPv4 address set to zero that are not part of the IPv4 prefix., any Identifies the source IP address or subnet. To match the rule, the incoming packet's source IP address must belong to the subnet.
src-port	The port associated with the source flow. A value of 0 means Not Applicable.
destination	**Synopsis:** The ipv4-address type represents an IPv4 address in dotted-quad notation. The IPv4 address may include a zone index, separated by a % sign. The zone index is used to disambiguate identical address values. For link-local addresses, the zone index will typically be the interface index number or the name of an interface. If the zone index is not present, the default zone of the device will be used. The canonical format for the zone index is the numerical format, The ipv4-prefix type represents an IPv4 address prefix. The prefix length is given by the number following the slash character and must be less than or equal to 32. A prefix length value of n corresponds to an IP address mask that has n contiguous 1-bits from the most significant bit (MSB) and all other bits set to 0. The canonical format of an IPv4 prefix has all bits of the IPv4 address set to zero that are not part of the IPv4 prefix., any Defines the destination IP address or subnet. To match the rule, the incoming packet's destination IP address must belong to the subnet.
dest-port	The port associated with the destination flow. A value of 0 means Not Applicable.
gateway	**Synopsis:** The ipv4-address type represents an IPv4 address in dotted-quad notation. The IPv4 address may include a zone index, separated by a % sign. The zone index is used to disambiguate identical address values. For link-local addresses, the zone index will typically be the interface index number or the name of an interface. If the zone index is not present, the default zone of the device will be used. The canonical format for the zone index is the numerical format Defines the nexthop IP address. The matched unicast packet is sent to the identified gateway.
packets-per-second	**Synopsis:** The gauge32 type represents a non-negative integer, which may increase or decrease, but shall never exceed a maximum value, nor fall below a minimum value. The maximum value cannot be greater than 2^32-1 (4294967295 decimal), and the minimum value cannot be smaller than 0. The value of a gauge32 has its maximum value whenever the information being modeled is greater than or equal to its maximum value, and has its minimum value whenever the information being modeled is smaller than or equal to its minimum value. If the information being modeled subsequently decreases below (increases above) the maximum (minimum) value, the gauge32 also decreases (increases). In the value set and its semantics, this type is equivalent to the Gauge32 type of the SMIv2. Displays the statistical throughput of all packets matching the rule, in packets per second.
static	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:

Parameter	Description
	• 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 5.31.6

Flushing Dynamic Hardware Routing Rules

Flushing dynamic hardware routing rules removed dynamic rules from the Routing Rules Summary table.

> **NOTE**
> *Only dynamic rules can be flushed. Static rules, enabled by activating hardware acceleration, never age out. For more information about enabling hardware acceleration, refer to Section 5.31.1, "Layer 3 Switching Concepts" .*

To flush dynamic hardware routing rules, type:

```
switch layer3-switching flush-dynamic-rules
```

Section 5.32

Managing Classes of Service

Classes of Service (CoS) provides the ability to expediate the transmission of certain frames and port traffic over others. The CoS of a frame can be set to Normal, Medium, High or Criticial. By default, ROX II enforces Normal CoS for all traffic.

> **IMPORTANT!**
> *Use the highest supported CoS with caution, as it is always used by the switch for handling network management traffic, such as RSTP BPDUs.*
>
> *If this CoS is used for regular network traffic, upon traffic bursts, it may result in the loss of some network management frames, which in turn may result in the loss of connectivity over the network.*

The process of controlling traffic based on CoS occurs over two phases:

. **Inspection Phase**

In the inspection phase, the CoS priority of a received frame is determined from:

- A specific CoS based upon the source and destination MAC address (as set in the Static MAC Address Table)
- The priority field in 802.1Q tags
- The Differentiated Services Code Point (DSCP) component of the Type Of Service (TOS) field, if the frame is IP
- The default CoS for the port

Each frame's CoS will be determined once the first examined parameter is found in the frame.

Received frames are first examined to determine if their destination or source MAC address is found in the Static MAC Address Table. If they are, the CoS configured for the static MAC address is used. If neither destination or source MAC address is in the Static MAC Address Table, the frame is then examined for 802.1Q tags and the priority field is mapped to a CoS. If a tag is not present, the frame is examined to determine if it is an IP frame. If the frame is IP and inspecting TOS is enabled, the CoS is determined from the DSCP field. If the frame is not IP or inspecting TOS is disabled, the default CoS for the port is used.

After inspection, the frame is forwarded to the egress port for transmission.

. **Forwarding Phase**

Once the CoS of the frame is determined, the frame is forwarded to the egress port, where it is collected into one of the priority queues according to the assigned CoS.

CoS weighting selects the degree of preferential treatment that is attached to different priority queues. The ratio of the number of higher CoS to lower CoS frames transmitted can be configured. If desired, the user can configure lower CoS frames to be transmitted only after all higher CoS frames have been serviced.

The following sections describe how to configure and manage classes of service:

- Section 5.32.1, “Configuring Classes of Service”
- Section 5.32.2, “Managing Priority to CoS Maps”
- Section 5.32.3, “Managing DSCP to CoS Maps”

Section 5.32.1

Configuring Classes of Service

To configure Classes of Service, do the following:

1. Make sure the CLI is in Configuration mode.
2. Configure the CoS weighting by typing:

```
switch classes-of-service cos-weighting weighting
```

   Where:

   - *weighting* is the weighting algorithm for transmitting different priority CoS frames. During traffic bursts, frames queued in the switch pending transmission on a port may have different CoS priorities.
3. If necessary, configure CoS mapping based on either the IEEE 802.1p priority or Differentiated Services (DS) field set in the IP header for each packet. For more information, refer to Section 5.32.2.2, “Adding a Priority” or Section 5.32.3.2, “Adding a DSCP”.
4. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.32.2

Managing Priority to CoS Maps

Assigning CoS to different IEEE 802.1p priority values in the frame is done by defining priority-to-CoS mapping table entries.

The following sections describe how to configure and manage priority-to-CoS mapping:

- Section 5.32.2.1, “Viewing a List of Priorities”
- Section 5.32.2.2, “Adding a Priority”

- Section 5.32.2.3, “Deleting a Priority”

Section 5.32.2.1
Viewing a List of Priorities

To view a list of priorites, type:

```
show running-config switch class-of-service priority-to-cos
```

If priorities have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config switch class-of-service priority-to-cos | tab
PRIORITY  COS
------------------
3         medium
4         medium
5         medium
6         high
7         high

!
```

If no priorities have been configured, add priorities as needed. For more information, refer to Section 5.32.2.2, “Adding a Priority”.

Section 5.32.2.2
Adding a Priority

To add a priority, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the priority by typing:

   ```
   switch class-of-service priority-to-cos priority
   ```

   Where:

   - *priority* is the value of the IEEE 802.1p priority
3. Configure the following parameter(s) as required:

Parameter	Description
cos { cos }	**Synopsis:** normal, medium, high, crit **Default:** normal The Class of Service (CoS) assigned to received tagged frames with the specified IEEE 802.1p priority value.

4. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.32.2.3
Deleting a Priority

To delete a priority, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the priority by typing:

   ```
   no switch class-of-service priority-to-cos priority
   ```

   Where:

   - *priority* is the value of the IEEE 802.1p priority
3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.32.3

Managing DSCP to CoS Maps

Assigning CoS to different values of the Differentiated Services Code Point (DSCP) field in the IP header of received packets is done by defining DSCP-to-CoS mapping table entries.

The following sections describe how to configure and manage DSCP-to-CoS mapping:

- Section 5.32.3.1, “Viewing a List of DSCPs”
- Section 5.32.3.2, “Adding a DSCP”
- Section 5.32.3.3, “Deleting a DSCP”

Section 5.32.3.1

Viewing a List of DSCPs

To view a list of priorites, type:

```
show running-config switch class-of-service dscp-to-cos
```

If DSCPs have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config switch class-of-service dscp-to-cos | tab
DSCP  COS
--------------
1     normal
3     high
4     medium
6     normal
7     normal

!
```

If no DSCPs have been configured, add DSCPs as needed. For more information, refer to Section 5.32.3.2, “Adding a DSCP”.

Section 5.32.3.2

Adding a DSCP

To add a DSCP, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the priority by typing:

```
switch class-of-service dscp-to-cos dscp
```

Where:

- *dscp* is the value of the 6 bit DiffServ field in the Type-Of-Service (TOS) field of the IP header

3. Configure the following parameter(s) as required:

Parameter	Description
cos { cos }	**Synopsis:** normal, medium, high, crit **Default:** normal The Class of Service (CoS) assigned to the received frames with the specified DSCP.

4. Configure the CoS parameters on select switched Ethernet ports and/or trunk interfaces as needed. For more information, refer to Section 3.17.2, "Configuring a Switched Ethernet Port" and/or Section 3.21.2, "Adding an Ethernet Trunk Interface".
5. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.32.3.3

Deleting a DSCP

To delete a DSCP, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the DSCP by typing:

```
no switch class-of-service dscp-to-cos dscp
```

Where:

- *dscp* is the value of the 6 bit DiffServ field in the Type-Of-Service (TOS) field of the IP header

3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.33

Managing MAC Addresses

The following sections describe how to configure and manage MAC addresses:

- Section 5.33.1, "Viewing a Dynamic List of MAC Addresses"
- Section 5.33.2, "Purging the Dynamic MAC Address List"
- Section 5.33.3, "Configuring MAC Address Learning Options"
- Section 5.33.4, "Managing Static MAC Addresses"

Section 5.33.1

Viewing a Dynamic List of MAC Addresses

To view a dynamic list of learned MAC addresses, type:

```
show switch mac-tables mac-table
```

A table or list similar to the following example appears:

```
ruggedcom# show switch mac-tables mac-table
MAC                VID   SLOT  PORT  TYPE     COS
------------------------------------------------------
00:0a:dc:78:f3:20  1     lm1   1     dynamic  normal
00:0a:dc:78:fc:45  1     lm1   1     dynamic  normal
00:0a:dc:f6:8b:ff  4085  lm1   2     static   normal
00:10:94:00:24:01  4084  lm1   1     static   normal
00:10:94:00:30:01  1     lm1   2     static   normal
00:10:94:00:40:01  4086  lm1   2     static   normal
00:13:3b:00:04:1a  1     lm1   1     dynamic  normal
00:13:3b:00:06:b5  1     lm1   1     dynamic  normal
```

This table or list provides the following information:

Parameter	Description
mac	The MAC address learned by the switch.
vid	The VLAN identifier of the VLAN upon which the MAC address operates.
slot	**Synopsis:** sm, lm1, lm2, lm3, lm4, lm5, lm6 The slot containing the module including the port.
port	The port on which the MAC address has been learned.
type	**Synopsis:** static, dynamic How the MAC address has been learned by the switch: • STATIC: The address has been learned as a result of static MAC address table configuration or some other management activity and cannot be automatically unlearned or relearned by the switch. • DYNAMIC: The address has been automatically learned by the switch and can be automatically unlearned.
cos	**Synopsis:** N/A, normal, medium, high, crit The Class Of Service (CoS) that is assigned to frames carrying this address as a source or destination address.

If a MAC address is not listed, do the following:

- Configure the MAC address learning options to dynamically detect the MAC addresses of other devices on the network. For more information, refer to Section 5.33.3, “Configuring MAC Address Learning Options”.
- Configure the address on the device as a static MAC address. For more information, refer to Section 5.33.4.2, “Adding a Static MAC Address”.

Section 5.33.2
Purging the Dynamic MAC Address List

To purge the dynamic MAC address list of all entries, type:

```
switch mac-tables purge-mac-table
```

Once the table is purged, the following message appears:

```
purge-mac-table-string Success
```

Section 5.33.3

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 adresses are removed when the aging timer is exceeded. Addresses can also be removed when a link failure or topology change occurs.

To configure the MAC address learning options, do the following:

1. Make sure the CLI is in Configuration mode.
2. Navigate to ***switch » mac-tables*** and configure the following parameter(s) as required:

Parameter	Description
mac-aging-time { mac-aging-time }	**Default:** 300 The time a learned MAC address is held before being aged out.
mac-age-on-loss	**Default:** true When link failure (and potentially a topology change) occurs, the switch may have some MAC addresses previously learned on the failed port. As long as those addresses are not aged-out, the switch will still be forwarding traffic to that port, thus preventing that traffic from reaching its destination via the new network topology. This parameter allows the aging-out of all MAC addresses learned on a failed port immediately upon link failure detection.

3. Type `commit` and press **Enter** to save the changes, or type `revert` and press **Enter** to abort.

Section 5.33.4

Managing Static MAC Addresses

Static MAC addresses must be configured when the device is only able to receive frames, not transmit them. They may also need to be configured if port security (if supported) must be enforced.

Prioritized MAC addresses are configured when traffic to or from a specific device on a LAN segment is to be assigned a higher CoS priority than other devices on that LAN segment.

The following sections describe how to configure and manage static MAC addresses:

- Section 5.33.4.1, “Viewing a List of Static MAC Addresses”
- Section 5.33.4.2, “Adding a Static MAC Address”
- Section 5.33.4.3, “Deleting a Static MAC Address”

Section 5.33.4.1

Viewing a List of Static MAC Addresses

To view a list of static MAC addresses configured on the device, type:

```
show running-config switch mac-tables static-mac-table
```

If static MAC addresses have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config switch mac-tables static-mac-table | tab
MAC                VID   LEARNED  SLOT  PORT  COS
-------------------------------------------------------
```

```
00:0a:dc:f6:8b:ff  4085  -        lm1   2     normal
00:10:94:00:24:01  4084  -        lm1   1     normal
00:10:94:00:30:01  1     -        lm1   2     normal
00:10:94:00:40:01  4086  -        lm1   2     normal

!
```

If no static MAC addresses have been configured, add addresses as needed. For more information, refer to Section 5.33.4.2, “Adding a Static MAC Address”.

Section 5.33.4.2
Adding a Static MAC Address

To add a static MAC address, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the static MAC address by typing:

> **NOTE**
> *Letters in MAC addresses must be lowercase.*

```
switch mac-tables static-mac-table static-mac address vlan
```

Where:

- *address* is the Unicast MAC address that is to be statically configured. It can have up to 6 '*' wildcard characters continuously applied from the right.
- *vlan* is the ID of the VLAN upon which the MAC address operates.

3. Configure the following parameter(s) as required:

Parameter	Description
learned	If set, the system will auto-learn the port upon which the device with this address is located.
slot { slot }	**Synopsis:** sm, lm1, lm2, lm3, lm4, lm5, lm6 The name of the module location provided on the silkscreen across the top of the device.
port { port }	The selected ports on the module installed in the indicated slot.
cos { cos }	**Synopsis:** N/A, normal, medium, high, crit **Default:** normal The priority of traffic for a specified address.

4. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.33.4.3
Deleting a Static MAC Address

To delete a static MAC address, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the static MAC address by the typing:

```
no switch mac-tables static-mac-table static-mac address vlan
```

Where:

- *address* is the Unicast MAC address that is to be statically configured. It can have up to 6 '*' wildcard characters continuously applied from the right.
- *vlan* is the ID of the VLAN upon which the MAC address operates.

3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.34

Managing Spanning Tree Protocol

The following sections describe how to configure and manage STP:

- Section 5.34.1, “RSTP Operation”
- Section 5.34.2, “RSTP Applications”
- Section 5.34.3, “MSTP Operation”
- Section 5.34.4, “Fast Root Failover Operation”
- Section 5.34.5, “Configuring STP Globally”
- Section 5.34.6, “Configuring STP for Switched Ethernet Ports”
- Section 5.34.7, “Configuring STP for Ethernet Trunk Interfaces”
- Section 5.34.8, “Managing Multiple Spanning Tree Instances”
- Section 5.34.9, “Managing Port Costs and Priorities”
- Section 5.34.10, “Viewing the Status of RSTP”
- Section 5.34.11, “Viewing RSTP Per-Port Statistics”
- Section 5.34.12, “Clearing Spanning Tree Protocol Statistics”

Section 5.34.1

RSTP Operation

The 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 802.1D, this period lasts 30 seconds.

The Rapid Spanning Tree Protocol (RSTP, IEEE 802.1w) was a further evolution of the 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. RSTP also offers a number of other significant innovations, including:

- Topology changes in RSTP can originate from and be acted upon by any designated bridges, leading to more rapid propagation of address information, unlike topology changes in STP, which must be passed to the root bridge before they can be propagated to the network.

- RSTP explicitly recognizes two blocking roles - Alternate and Backup Port - which are included in computations of when to learn and forward. STP, however, recognizes only one state - Blocking - for ports that should not forward.
- RSTP bridges generate their own configuration messages, even if they fail to receive any from the root bridge. This leads to quicker failure detection. STP, by contrast, must relay configuration messages received on the root port out its designated ports. If an STP bridge fails to receive a message from its neighbor, it cannot be sure where along the path to the root a failure occurred.
- RSTP offers edge port recognition, allowing ports at the edge of the network to forward frames immediately after activation, while at the same time protecting them against loops.

While providing much better performance than STP, IEEE 802.1w RSTP still required up to several seconds to restore network connectivity when a topology change occurred.

The following sections further describe the operation of RSTP:

- Section 5.34.1.1, “RSTP States and Roles”
- Section 5.34.1.2, “Edge Ports”
- Section 5.34.1.3, “Point-to-Point and Multipoint Links”
- Section 5.34.1.4, “Path and Port Costs”
- Section 5.34.1.5, “Bridge Diameter”

Section 5.34.1.1

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, 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.

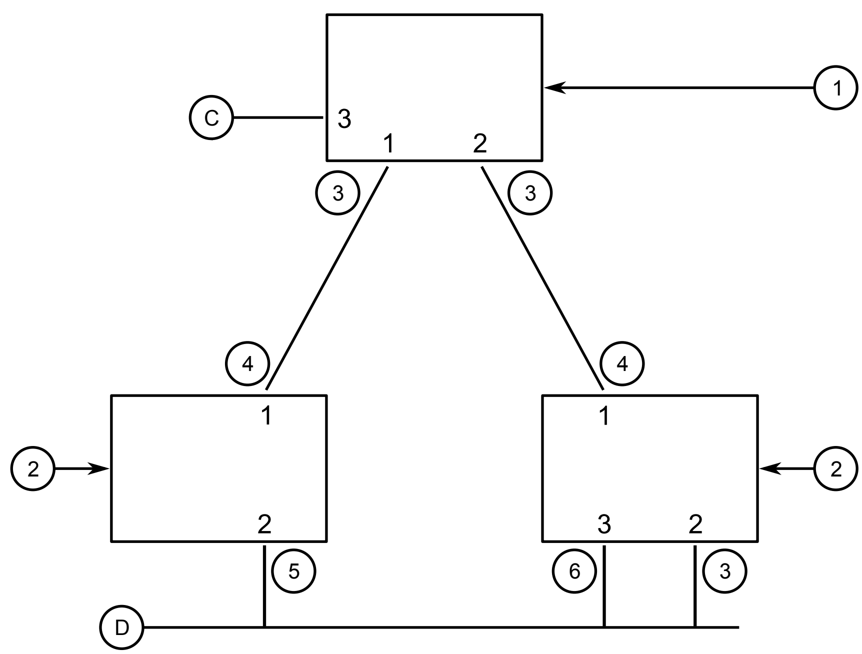

Figure 14: Bridge and Port Roles

1. Root Bridge **2.** Designated Bridge **3.** Designated Port **4.** Root Port **5.** Alternate Port **6.** Backup Port

A port is alternate when it receives a better message from another bridge on the LAN segment it is connected to. The message that an Alternate Port receives is better than the port itself would generate, but not good enough to convince it to become the Root Port. The port becomes the alternate to the current Root Port and will become the new Root Port should the current Root Port fail. The Alternate Port does not participate in the network.

A port is a Backup Port when it receives a better message from the LAN segment it is connected to, originating from another port on the same bridge. The port is a backup for another port on the bridge and will become active if that port fails. The Backup Port does not participate in the network.

Section 5.34.1.2

Edge Ports

A port may be designated as an Edge Port if it is directly connected to an end station. As such, it cannot create bridging loops in the network and can thus directly transition to forwarding, skipping the listening and learning stages.

Edge ports that receive configuration messages immediately lose their Edge Port status and become normal spanning tree ports. A loop created on an improperly connected edge port is thus quickly repaired.

Because an Edge Port services only end stations, topology change messages are not generated when its link toggles.

Section 5.34.1.3

Point-to-Point and Multipoint Links

RSTP uses a peer-peer protocol called Proposing-Agreeing to ensure transitioning in the event of a link failure. This protocol is point-to-point and breaks down in multipoint situations, i.e. when more than two bridges operate on a shared media link.

If RSTP detects this circumstance (based upon the port's half duplex state after link up) it will switch off Proposing-Agreeing. The port must transition through the learning and forwarding states, spending one forward delay in each state.

There are circumstances in which RSTP will make an incorrect decision about the point-to-point state of the link simply by examining the half-duplex status, namely:

- The port attaches only to a single partner, but through a half-duplex link.
- The port attaches to a shared media hub through a full-duplex link. The shared media link attaches to more than one RSTP enabled bridge.

In such cases, the user may configure the bridge to override the half-duplex determination mechanism and force the link to be treated in the proper fashion.

Section 5.34.1.4

Path and Port Costs

The STP path cost is the main metric by which root and designated ports are chosen. The path cost for a designated bridge is the sum of the individual port costs of the links between the root bridge and that designated bridge. The port with the lowest path cost is the best route to the root bridge and is chosen as the root port.

NOTE
In actuality the primary determinant for root port selection is the root bridge ID. Bridge ID is important mainly at network startup when the bridge with the lowest ID is elected as the root bridge. After startup (when all bridges agree on the root bridge's ID) the path cost is used to select root ports. If the path costs of candidates for the root port are the same, the ID of the peer bridge is used to select the port. Finally, if candidate root ports have the same path cost and peer bridge ID, the port ID of the peer bridge is used to select the root port. In all cases the lower ID, path cost or port ID is selected as the best.

How Port Costs Are Generated

Port costs can be generated either as a result of link auto-negotiation or manual configuration. When the link auto-negotiation method is used, the port cost is derived from the speed of the link. This method is useful when a well-connected network has been established. It can be used when the designer is not too concerned with the resultant topology as long as connectivity is assured.

Manual configuration is useful when the exact topology of the network must be predictable under all circumstances. The path cost can be used to establish the topology of the network exactly as the designer intends.

STP vs. RSTP Costs

The STP specification limits port costs to values of 1 to 65536. Designed at a time when 9600 bps links were state of the art, this method breaks down in modern use, as the method cannot represent a link speed higher than 10 Gbit/s.

To remedy this problem in future applications, the RSTP specification limits port costs to values of 1 to 20000000, and a link speed up to 10 Tbit/s can be represented with a value of 2.

Section 5.34.1.5

Bridge Diameter

The bridge diameter is the maximum number of bridges between any two possible points of attachment of end stations to the network.

The bridge diameter reflects the realization that topology information requires time to propagate hop by hop through a network. If configuration messages take too long to propagate end to end through the network, the result will be an unstable network.

There is a relationship between the bridge diameter and the maximum age parameter.

NOTE

The RSTP algorithm is as follows:

- *STP configuration messages contain age information.*
- *Messages transmitted by the root bridge have an age of 0. As each subsequent designated bridge transmits the configuration message it must increase the age by at least 1 second.*
- *When the age exceeds the value of the maximum age parameter the next bridge to receive the message immediately discards it.*

To achieve extended ring sizes, Siemens's eRSTP™ uses an age increment of ¼ of a second. The value of the maximum bridge diameter is thus four times the configured maximum age parameter.

IMPORTANT!

Raise the value of the maximum age parameter if implementing very large bridged networks or rings.

Section 5.34.2

RSTP Applications

The following sections describe various applications of RSTP:

- Section 5.34.2.1, “RSTP in Structured Wiring Configurations”
- Section 5.34.2.2, “RSTP in Ring Backbone Configurations”
- Section 5.34.2.3, “RSTP Port Redundancy”

Section 5.34.2.1

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 15 would leave all the ports of bridges 555 through 888 connected to the network.

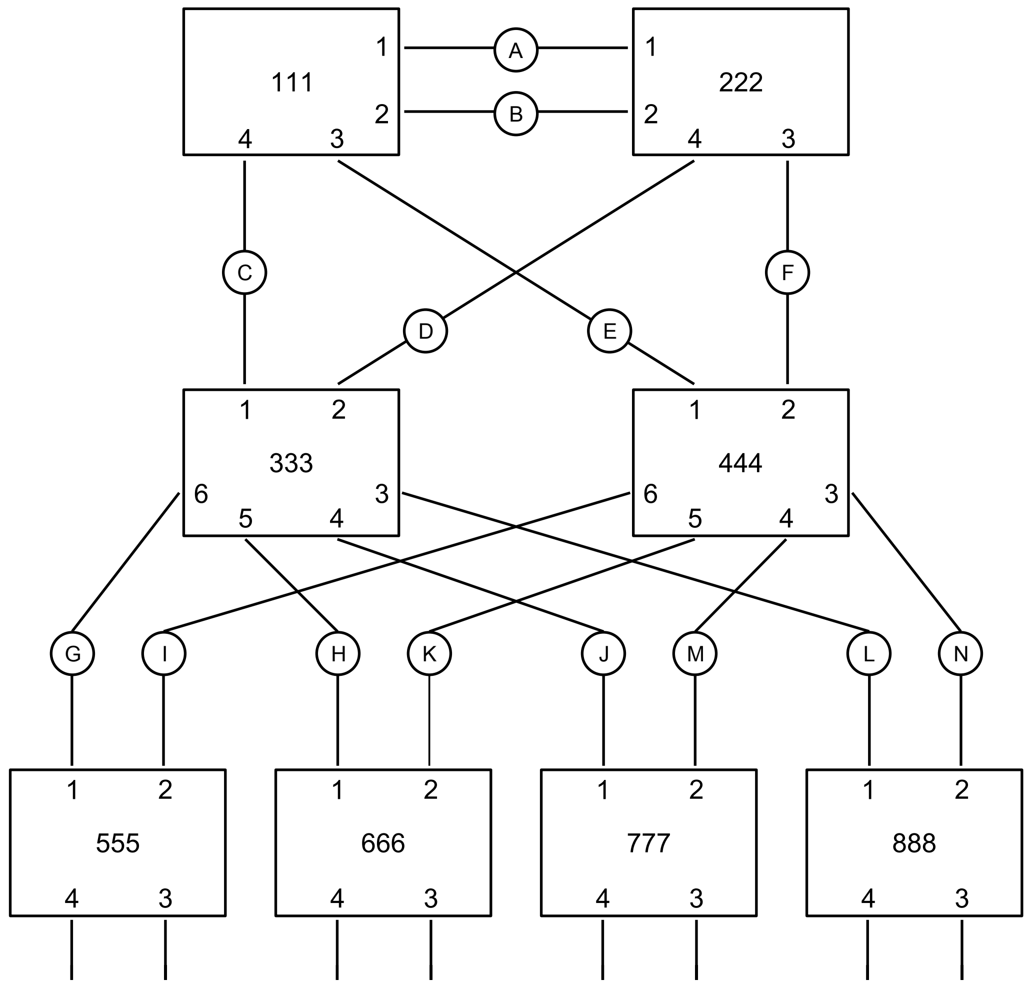

Figure 15: Example - Structured Wiring Configuration

To design a structured wiring configuration, do the following:

1. **Select the design parameters for the network.**

   What are the requirements for robustness and network failover/recovery times? Are there any special requirements for diverse routing to a central host computer? Are there any special port redundancy requirements?

2. **Identify required legacy support.**

   Are STP bridges used in the network? These bridges do not support rapid transitioning to forwarding. If these bridges are present, can they be re-deployed closer to the network edge?

3. **Identify edge ports and ports with half-duplex/shared media restrictions.**

Ports that connect to host computers, IEDs and controllers may be set to edge ports in order to guarantee rapid transitioning to forwarding as well as to reduce the number of topology change notifications in the network. Ports with half-duplex/shared media restrictions require special attention in order to guarantee that they do not cause extended fail-over/recovery times.

4. **Choose the root bridge and backup root bridge carefully.**

   The root bridge should be selected to be at the concentration point of network traffic. Locate the backup root bridge adjacent to the root bridge. One strategy that may be used is to tune the bridge priority to establish the root bridge and then tune each bridge's priority to correspond to its distance from the root bridge.

5. **Identify desired steady state topology.**

   Identify the desired steady state topology taking into account link speeds, offered traffic and QOS. Examine of the effects of breaking selected links, taking into account network loading and the quality of alternate links.

6. **Decide upon a port cost calculation strategy.**

   Select whether fixed or auto-negotiated costs should be used? It is recommended to use the auto-negotiated cost style, unless it is necessary for the network design to change the auto-negotiated cost style. Select whether the STP or RSTP cost style should be used. Make sure to configure the same cost style on all devices on the network.

7. **Enable RSTP Fast Root Failover option.**

   This is a proprietary feature of Siemens. In a mesh network with only RUGGEDCOM devices in the core of the network, it is recommended to enable the RSTP Fast Root Failover option to minimize the network downtime in the event of a Root bridge failure.

8. Calculate and configure priorities and costs.
9. Implement the network and test under load.

Section 5.34.2.2
RSTP in Ring Backbone Configurations

RSTP may be used in ring backbone configurations where rapid recovery from link failure is required. In normal operation, RSTP will block traffic on one of the links, for example, as indicated by the double bars through link H in Figure 16. In the event of a failure on link D, bridge 444 will unblock link H. Bridge 333 will communicate with the network through link F.

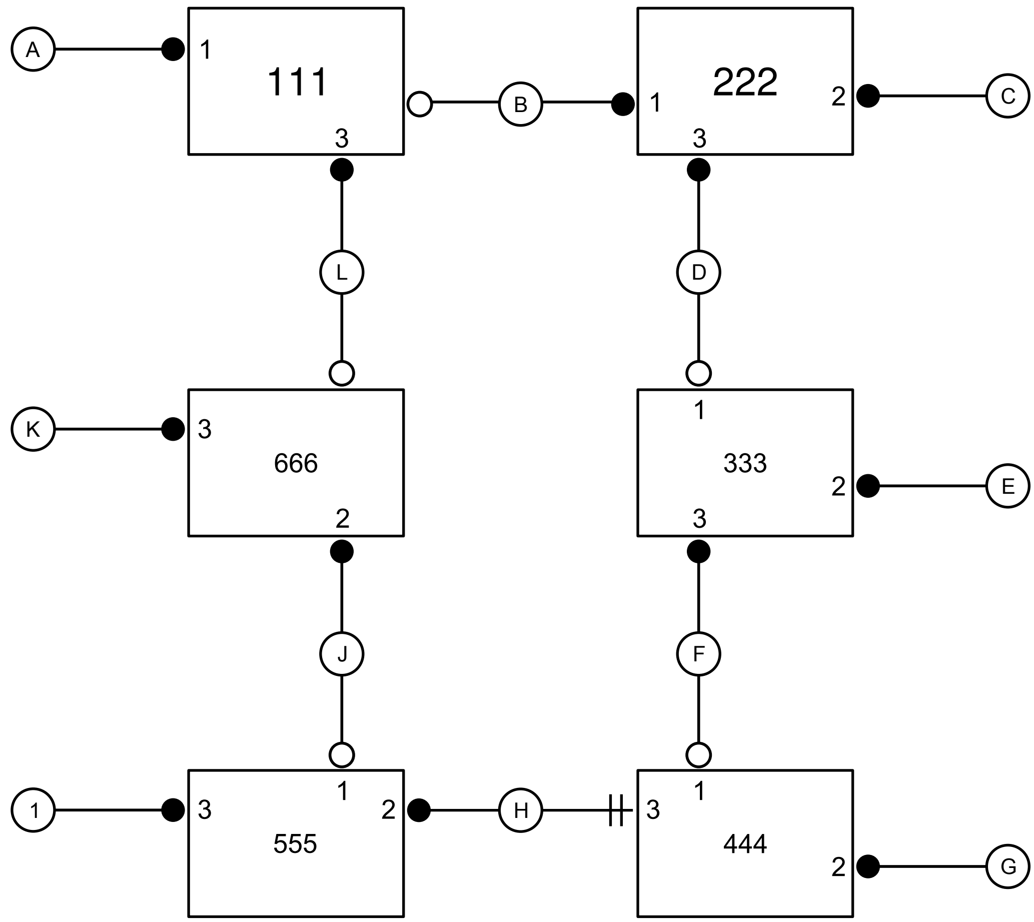

Figure 16: Example - Ring Backbone Configuration

To design a ring backbone configuration with RSTP, do the following:

1. **Select the design parameters for the network.**

   What are the requirements for robustness and network fail-over/recovery times? Typically, ring backbones are chosen to provide cost effective but robust network designs.

2. **Identify required legacy support and ports with half-duplex/shared media restrictions.**

   These bridges should not be used if network fail-over/recovery times are to be minimized.

3. **Identify edge ports.**

   Ports that connect to host computers, IEDs and controllers may be set to edge ports in order to guarantee rapid transitioning to forwarding as well as to reduce the number of topology change notifications in the network.

4. **Choose the root bridge.**

   The root bridge can be selected to equalize either the number of bridges, number of stations or amount of traffic on either of its legs. It is important to realize that the ring will always be broken in one spot and that traffic always flows through the root.

5. **Assign bridge priorities to the ring.**

For more information, refer to the RUGGEDCOM White Paper *Performance of the RSTP in Ring Network Topologies* available on www.siemens.com/ruggedcom.

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 ROX II, the RSTP Fast Root Failover option is enabled by default. It is recommended to disable this feature when operating in a Ring network.

8. Implement the network and test under load.

Section 5.34.2.3

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.

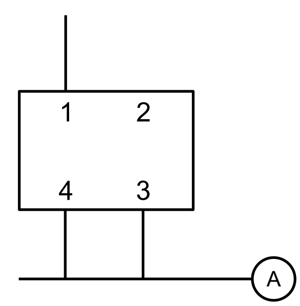

Figure 17: Example - Port Redundancy

Section 5.34.3

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 the network.

The sophistication and utility of the MSTP implementation on a given bridged network is proportional to the amount of planning and design invested in configuring MSTP.

If MSTP is activated on some or all of the bridges in a network with no additional configuration, the result will be a fully and simply connected network. At best though, the result will be the same as a network using only RSTP. Taking full advantage of the features offered by MSTP requires a potentially large number of configuration variables to be derived from an analysis of data traffic on the bridged network, and from requirements for load sharing, redundancy, and path optimization. Once these parameters have all been derived, it is also critical they are consistently applied and managed across all bridges in an MST region.

By design, MSTP processing time is proportional to the number of active STP instances. This means MSTP will likely be significantly slower than RSTP. Therefore, for mission critical applications, RSTP should be considered a better network redundancy solution than MSTP.

The following sections further describe the operation of MSTP:

- Section 5.34.3.1, “MSTP Regions and Interoperability”
- Section 5.34.3.2, “MSTP Bridge and Port Roles”
- Section 5.34.3.3, “Benefits of MSTP”
- Section 5.34.3.4, “Implementing MSTP on a Bridged Network”

Section 5.34.3.1

MSTP Regions and Interoperability

In addition to supporting multiple spanning trees in a network of MSTP-capable bridges, MSTP is capable of inter-operating with bridges that support only RSTP or legacy STP, without requiring any special configuration.

An MST region may be defined as the set of interconnected bridges whose MST Region Identification is identical. The interface between MSTP bridges and non-MSTP bridges, or between MSTP bridges with different MST Region Identification information, becomes part of an MST Region boundary.

Bridges outside an MST region will see the entire region as though it were a single (R)STP bridge, with the internal detail of the MST region being hidden from the rest of the bridged network. In support of this, MSTP maintains separate *hop counters* for spanning tree information exchanged at the MST region boundary versus information propagated inside the region. For information received at the MST region boundary, the (R)STP Message Age is incremented only once. Inside the region, a separate Remaining Hop Count is maintained, one for each spanning tree instance. The external Message Age parameter is referred to the (R)STP Maximum Age Time, whereas the internal Remaining Hop Counts are compared to an MST region-wide Maximum Hops parameter.

MSTI

An MSTI (Multiple Spanning Tree Instance) is one of sixteen independent spanning tree instances that may be defined in an MST region (not including the IST). An MSTI is created by mapping a set of VLANs to a given MSTI ID. The same mapping must be configured on all bridges that are intended to be part of the MSTI. Moreover, all VLAN-to-MSTI mappings must be identical for all bridges in an MST region.

ROX II supports 16 MSTIs in addition to the IST.

Each MSTI has a topology that is independent of others. Data traffic originating from the same source and bound to the same destination, but on different VLANs on different MSTIs, may therefore travel a different path across the network.

IST

An MST region always defines an IST (Internal Spanning Tree). The IST spans the entire MST region, and carries all data traffic that is not specifically allocated (by VLAN) to a specific MSTI. The IST is always computed and is defined to be MSTI zero.

The IST is also the extension inside the MST region of the CIST

CST

The CST (Common Spanning Tree) spans the entire bridged network, including MST regions and any connected STP or RSTP bridges. An MST region is seen by the CST as an individual bridge, with a single cost associated with its traversal.

CIST

The CIST (Common and Internal Spanning Tree) is the union of the CST and the ISTs in all MST regions. The CIST therefore spans the entire bridged network, reaching into each MST region via the latter's IST to reach every bridge on the network.

Section 5.34.3.2

MSTP Bridge and Port Roles

MSTP supports the following bridge and port roles:

Bridge Roles

Role	Description
CIST Root	The CIST Root is the elected root bridge of the CIST (Common and Internal Spanning Tree), which spans all connected STP and RSTP bridges and MSTP regions.
CIST Regional Root	The root bridge of the IST within an MSTP region. The CIST Regional Root is the bridge within an MSTP region with the lowest cost path to the CIST Root. Note that the CIST Regional Root will be at the boundary of an MSTP region. Note also that it is possible for the CIST Regional Root to be the CIST Root.
MSTI Regional Root	The root bridge for an MSTI within an MSTP region. A root bridge is independently elected for each MSTI in an MSTP region.

Port Roles

Each port on an MSTP bridge may have more than one CIST role depending on the number and topology of spanning tree instances defined on the port.

Role	Description
CIST Port Roles	• The Root Port provides the minimum cost path from the bridge to the CIST Root via the CIST Regional Root. If the bridge itself happens to be the CIST Regional Root, the Root Port is also the Master Port for all MSTIs, and provides the minimum cost path to a CIST Root located outside the region. • A Designated Port provides the minimum cost path from an attached LAN, via the bridge to the CIST Regional Root. • Alternate and Backup Ports function the same as they do in RSTP, but relative to the CIST Regional Root.
MSTI Port Roles	For each MSTI on a bridge: • The Root Port provides the minimum cost path from the bridge to the MSTI Regional Root, if the bridge itself is not the MSTI Regional Root. • A Designated Port provides the minimum cost path from an attached LAN, via the bridge to the MSTI Regional Root. • Alternate and Backup Ports function the same as they do in RSTP, but relative to the MSTI Regional Root. The Master Port, which is unique in an MSTP region, is the CIST Root Port of the CIST Regional Root, and provides the minimum cost path to the CIST Root for all MSTIs.
Boundary Ports	A Boundary Port is a port on a bridge in an MSTP region that connects to either: a bridge belonging to a different MSTP region, or a bridge supporting only RSTP or legacy STP. A Boundary Port blocks or forwards all VLANs from all MSTIs and the CIST alike. A Boundary Port may be: • The CIST Root Port of the CIST Regional Root (and therefore also the MSTI Master Port). • A CIST Designated Port, CIST Alternate/Backup Port, or Disabled. At the MSTP region boundary, the MSTI Port Role is the same as the CIST Port Role.

Role	Description
	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 5.34.3.3

Benefits of MSTP

MSTP is configured by default to arrive automatically at a spanning tree solution for each configured MSTI. However, advantages may be gained from influencing the topology of MSTIs in an MST region by way of the Bridge Priority and the cost of each port.

Load Balancing

MSTP can be used to balance the data traffic load among sets of VLANs, enabling more complete utilization of a bridged network that has multiple redundant interconnections between bridges.

A bridged network controlled by a single spanning tree will block redundant links by design to avoid harmful loops. However, when using MSTP, any given link may have a different blocking state for MSTI, as maintained by MSTP. Any given link, therefore, might be in blocking state for some VLANs, and in forwarding state for other VLANs, depending on the mapping of VLANs to MSTIs.

It is possible to control the spanning tree solution for each MSTI, especially the set of active links for each tree, by manipulating per MSTI the bridge priority and the port costs of links in the network. If traffic is allocated judiciously to multiple VLANs, redundant interconnections in a bridged network, which would have gone unused when using a single spanning tree, can now be made to carry traffic.

Isolation of Spanning Tree Reconfiguration.

A link failure in an MSTP region that does not affect the roles of Boundary ports will not cause the CST to be reconfigured, nor will the change affect other MSTP regions. This is due to the fact that MSTP information does not propagate past a region boundary.

MSTP versus PVST

An advantage of MSTP over the Cisco Systems Inc. proprietary Per-VLAN Spanning Tree (PVST) protocol is the ability to map multiple VLANs onto a single MSTI. Since each spanning tree requires processing and memory, the expense of keeping track of an increasing number of VLANs increases much more rapidly for PVST than for MSTP.

Compatibility with STP and RSTP

No special configuration is required for the bridges of an MST region to connect fully and simply to non-MST bridges on the same bridged network. Careful planning and configuration is, however, recommended to arrive at an optimal network design.

Section 5.34.3.4

Implementing MSTP on a Bridged Network

The following procedure is recommended for configuring MSTP on a network. Beginning with a set of MSTP-capable Ethernet bridges, do the following for each bridge on the network:

> **NOTE**
> *Careful network analysis and planning should inform each step of creating an MSTP network.*

> **NOTE**
> *MSTP does not need to be enabled to map a VLAN to an MSTI. However, the mapping must be identical for each bridge that belongs to the MSTP region.*

1. Disable STP. For more information, refer to Section 5.34.5, “Configuring STP Globally”.
2. Configure one or more Multiple Spanning Tree Instances (MSTI), each with a unique bridge priority. For more information, refer to Section 5.34.8.3, “Adding a Multiple Spanning Tree Instance”.
3. Create static VLANs and map them to the MSTIs. For more information, refer to Section 5.35.4.2, “Adding a Static VLAN”.
4. Configure the cost and priority for each switch or trunk port that will transmit/receive MST BPDU (Bridge Protocol Data Unit) traffic. For more information, refer to Section 5.34.9, “Managing Port Costs and Priorities”.
5. Set the STP protocol version to MSTP, configure the MST region identifier and revision level, and then enable STP. For more information, refer to Section 5.34.5, “Configuring STP Globally”

Section 5.34.4
Fast Root Failover Operation

In mesh network topologies, the standard RSTP algorithm does not guarantee deterministic network recovery time in the case of a root switch failure. Such a recovery time is difficult to calculate and can be different (and may be relatively long) for any given mesh topology. This configuration parameter enables Siemens's enhancement to RSTP, which detects a failure of the root switch and performs some extra RSTP processing steps, significantly reducing the network recovery time and making it deterministic.

This feature is only available in RSTP mode. In MSTP mode, the configuration parameter is ignored.

In a single ring topology, this feature is not needed and should be disabled to avoid longer network recovery times due to extra RSTP processing. The Fast Root Failover algorithm must be supported by all switches in the network, including the root, to guarantee optimal performance. However, it is not uncommon to assign the root role to a switch from a vendor different from the rest of the switches in the network. In other words, it is possible the root might not support the Fast Root Failover algorithm. In such a scenario, a relaxed algorithm should be used, which tolerates the lack of support in the root switch.

Section 5.34.5
Configuring STP Globally

To configure global settings for the Spanning Tree Protocol (STP), do the following:

1. Make sure the CLI is in Configuration mode.
2. Navigate to ***switch » spanning-tree***.
3. Configure the basic STP settings by configuring the following parameter(s):

Parameter	Description
enabled	**Default:** true

Parameter	Description
	Enables STP/RSTP/MSTP for the bridge globally. Note that STP/RSTP/MSTP is enabled on a port when it is enabled globally and along with enabling per port setting.
version { version }	**Synopsis:** stp, rstp, mstp **Default:** rstp The version (either only STP or Rapid STP or Multiple STP) of the Spanning Tree Protocol (STP) to support.
hello-time { hello-time }	**Default:** 2 The time between configuration messages issued by the root bridge. Shorter hello times result in faster detection of topology changes at the expense of moderate increases in STP traffic. (Relationship : maxAgeTime >= 2 * (helloTime + 1.0 seconds))
max-age { max-age }	**Default:** 20 The time for which a configuration message remains valid after being issued by the root bridge. Configure this parameter with care when many tiers of bridges exist, or slow speed links (such as those used in WANs) are part of the network. (Relationship : maxAgeTime >= 2 * (helloTime + 1.0 seconds))
tx-hold-count { tx-hold-count }	**Default:** 0 The maximum number of configuration messages on each port that may be sent in a special event, such as recovering from a failure or bringing up a new link. After the maximum number of messages is reached, Rapid Spanning Tree Protocol (RSTP) will be limited to one message per second. Larger values allow the network to recover from failed links more quickly. If RSTP is being used in a ring architecture, the transmit count should be larger than the number of switches in the ring. If a number is not defined, the value is considered unlimited.
forward-delay { forward-delay }	**Default:** 15 The amount of time a bridge spends learning MAC addresses on a rising port before beginning to forward traffic. Lower values allow the port to reach the forwarding state more quickly, but at the expense of flooding unlearned addresses to all ports.
max-hops { max-hops }	**Default:** 20 The maximum possible bridge diameter inside a Multiple Spanning Tree (MST) region. MST BPDUs propagating inside an MST region carry a time-to-live parameter decremented by every switch that propagates the BPDU. If the maximum number of hops inside the region exceeds the configured maximum, the BPDUs may be discarded due to their time-to-live information. This parameter is only applicable to Multiple Spanning Tree Protocol (MSTP) configurations.
mst-region-name { mst-region-name }	The name of the MST region. All devices in the same MST region must have the same region name configured
mst-revision-level { mst-revision-level }	**Default:** 0 The revision level for the MST configuration. Typically, all devices in the same MST region are configured with the same revision level. However, different revision levels can be used to create sub-regions under the same region name.

4. Configure the eRSTP settings by configuring the following parameter(s):

Parameter	Description
max-net-diameter-multiplier { max-net-diameter-multiplier }	**Synopsis:** 1, 4 **Default:** 4 The Max Network Diameter as a multiplier of the MaxAgeTime value.
bpdu-guard { bpdu-guard }	**Synopsis:** specify, noshutdown, untilreset **Default:** noshutdown The Rapid Spanning Tree Protocol (RSTP) standard does not address network security. RSTP must process every received Bridge Protocol Data Unit (BPDU) and take an

Parameter	Description
	appropriate action. This opens a way for an attacker to influence RSTP topology by injecting RSTP BPDUs into the network. BPDU Guard is a feature that protects the network from BPDUs received by a port where RSTP-capable devices are not expected to be attached. If a BPDU is received by a port for which the 'Edge' parameter is set to 'TRUE' or RSTP is disabled, the port will be shut down for the time period specified by this parameter. • NO SHUTDOWN: BPDU Guard is disabled. • UNTIL RESET: The port will remain shut down until the port reset command is issued by the user. • SPECIFY: A timeout period is specified for the port using the BPDU Timeout parameter.
bpdu-timeout { bpdu-timeout }	The time for which a port is shutdown. Only applicable when BPDU Guard Mode is set to *specify*.
fast-root-failover { fast-root-failover }	**Synopsis:** on, off, on-with-standard-root **Default:** on The Fast Root Failover algorithm. Options include: • Off: The Fast Root Failover algorithm is disabled. As such, a root switch failure may result in excessive connectivity recovery time in a mesh network. • On: Fast Root Failover is enabled and the most robust algorithm is used, which restores network connectivity quickly in case of root bridge failure in a mesh network. • On with standard root: Fast Root Failover is enabled but a relaxed algorithm is used, allowing the use of a standard switch in the root role.
dot1w-interop	**Default:** true Enables/disables IEEE 802.1w Interoperability
cost-style { cost-style }	**Synopsis:** stp, rstp **Default:** stp The style of link costs to employ. STP uses 16-bit path costs based upon 1x10E9/link speed (4 for 1Gbps, 19 for 100 Mbps and 100 for 10 Mbps) whereas RSTP uses 32-bit costs based upon 2x10E13/link speed (20,000 for 1Gbps, 200,000 for 100 Mbps and 2,000,000 for 10 Mbps). Note that RSTP link costs are used only when the bridge version support is set to allow RSTP and the port does not migrate to the Spanning Tree Protocol (STP).

5. Configure the RSTP instance settings by configuring the following parameter(s):

Parameter	Description
bridge-priority { bridge-priority }	**Synopsis:** 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 5.34.8.3, “Adding a Multiple Spanning Tree Instance”.
7. Type `commit` and press **Enter** to save the changes, or type `revert` and press **Enter** to abort.

Section 5.34.6
Configuring STP for Switched Ethernet Ports

To configure the Spanning Tree Protocol (STP) for a switched Ethernet port, do the following:

1. Make sure the CLI is in Configuration mode.

2. Navigate to ***interface » switch » {slot/port} » spanning-tree***, where *{slot/port}* is the slot name and port number of the switched Ethernet port.
3. Configure the following parameter(s):

Parameter	Description
enabled	**Default:** true Enables/disables STP/RSTP on the interface.
admin-edge { admin-edge }	**Synopsis:** forceTrue, forceFalse, auto **Default:** auto Edge ports are ports that do not participate in the spanning tree, but still send configuration messages. Edge ports transition directly to frame forwarding without any listening and learning delays. The MAC tables of edge ports do not need to be flushed when topology changes occur in the STP network. Unlike an STP-disabled port, accidentally connecting an edge port to another port in the spanning tree will result in a detectable loop. The *Edgeness* of the port will be switched off and the standard RSTP rules will apply (until the next link outage).
admin-point-to-point { admin-point-to-point }	**Synopsis:** forceTrue, forceFalse, auto **Default:** auto RSTP uses a peer-to-peer protocol that provides for rapid transitioning on point-to-point links. This protocol is automatically turned off in situations where multiple STP bridges communicate over a shared (non point-to-point) LAN. The bridge will automatically take point-to-point to be true when the link is found to be operating in full-duplex mode. The point-to-point parameter allows this behavior or overrides it, forcing point-to-point to be true or false. Force the parameter true when the port operates a point-to-point link but cannot run the link in full-duplex mode. Force the parameter false when the port operates the link in full-duplex mode, but is still not point-to-point (e.g. a full-duplex link to an unmanaged bridge that concentrates two other STP bridges).
restricted-role	If enabled, causes the port not to be selected as the root port for the CIST or any MSTI, even though it has the best spanning tree priority vector. This parameter should be FALSE by default.
restricted-tcn	If TRUE, causes the port not to propagate received topology change notifications and topology changes to other ports. This parameter should be FALSE by default. If set, it can cause a temporary loss of connectivity after changes in a spanning tree's active topology as a result of persistent, incorrectly learned station location information.
rstp-priority { rstp-priority }	**Synopsis:** 16, 32, 64, 96, 112, 128, 144, 160, 176, 192, 208, 224, 240 **Default:** 128 The STP port priority. Ports of the same cost that attach to a common LAN will select the port to be used based upon the port priority.
stp-cost { stp-cost }	**Synopsis:** auto-cost, **Default:** auto-cost The cost to use in cost calculations, when the cost style parameter is set to STP in the bridge RSTP parameters configuration. Setting the cost manually provides the ability to preferentially select specific ports to carry traffic over others. Leave this field set to 'auto' to use the standard STP port costs as negotiated (four for 1Gbps, 19 for 100 Mbps links and 100 for 10 Mbps links). For MSTP, this parameter applies to both external and internal path cost.
rstp-cost { rstp-cost }	**Synopsis:** auto-cost, **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 5.34.8.3, “Adding a Multiple Spanning Tree Instance”.
5. Type `commit` and press **Enter** to save the changes, or type `revert` and press **Enter** to abort.

Section 5.34.7
Configuring STP for Ethernet Trunk Interfaces

To configure the Spanning Tree Protocol (STP) for an Ethernet trunk interface, do the following:

1. Make sure the CLI is in Configuration mode.
2. Navigate to ***interface » trunks » {id} » spanning-tree***, where *{id}* is the ID given to the interface.
3. Configure the following parameter(s):

Parameter	Description
enabled	**Default:** true When the box is checked, the Spanning Tree Protocol is enabled on the interface. Enabling STP activates the STP or RSTP protocol for this interface per the configuration in the STP Configuration menu.
admin-edge { admin-edge }	**Synopsis:** forceTrue, forceFalse, auto **Default:** auto Edge ports are ports that do not participate in the Spanning Tree, but still send configuration messages. Edge ports transition directly to frame forwarding without any listening and learning delays. The MAC tables of Edge ports do not need to be flushed when topology changes occur in the STP network. Unlike an STP-disabled port, accidentally connecting an edge port to another port in the spanning tree will result in a detectable loop. The 'Edgeness' of the port will be switched off and the standard RSTP rules will apply (until the next link outage).
admin-point-to-point { admin-point-to-point }	**Synopsis:** forceTrue, forceFalse, auto **Default:** auto RSTP uses a peer to peer protocol that provides for rapid transitioning on point-to-point links. This protocol is automatically turned off in situations where multiple STP bridges communicate over a shared (non point-to-point) LAN. The bridge will automatically take point-to-point to be true when the link is found to be operating in full-duplex mode. The point-to-point parameter allows this behavior or overrides it, forcing point-to-point to be true or false. Force the parameter true when the port operates a point-to-point link but cannot run the link in full-duplex mode. Force the parameter false when the port operates the link full duplex, 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 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 temporary loss of connectivity after changes in a spanning tree's active topology as a result of persistent incorrectly learned station location information.
rstp-priority { rstp-priority }	**Synopsis:** 16, 32, 64, 96, 112, 128, 144, 160, 176, 192, 208, 224, 240 **Default:** 128 The STP port priority. Ports of the same cost that attach to a common LAN will select the port to be used based upon the port priority.
stp-cost { stp-cost }	**Synopsis:** auto-cost, **Default:** auto-cost

Parameter	Description
	The cost to use in cost calculations, when the cost style parameter is set to STP in the bridge RSTP parameter configuration. Setting the cost manually provides the ability to preferentially select specific ports to carrytraffic over others. Leave this field set to 'auto' to use the standard STP port costs as negotiated (four for 1Gbps, 19 for 100 Mbps links and 100 for 10 Mbps links). For MSTP, this parameter applies to both external and internal path costs.
rstp-cost { rstp-cost }	**Synopsis:** auto-cost, **Default:** auto-cost The cost to use in cost calculations, when the cost style parameter is set to RSTP in the bridge RSTP parameter configuration. Setting the cost manually provides the ability to preferentially select specific ports to carry traffic over others. Leave this field set to 'auto' to use the standard RSTP port costs as negotiated (20,000 for 1Gbps, 200,000 for 100 Mbps links and 2,000,000 for 10 Mbps links). For MSTP, this parameter applies to both external and internal path costs.

4. If necessary, add Multiple Spanning Tree Instances (MSTI). For more information, refer to Section 5.34.8.3, "Adding a Multiple Spanning Tree Instance".
5. Type **`commit`** and press **Enter** to save the changes, or type **`revert`** and press **Enter** to abort.

Section 5.34.8

Managing Multiple Spanning Tree Instances

MSTP (Multiple Spanning Tree Protocol), as defined by the IEEE 802.1 standard, is used to map multiple VLANs to a single Spanning Tree instance, otherwise referred to as a Multiple Spanning Tree Instance (MSTI).

Each MSTI is assigned an MST ID and a bridge priority:

- The MST ID is used to associate the MSTI with a VLAN.
- The bridge priority is used by all devices in the Spanning Tree topology to determine which device among them is elected the root device or backbone. An ideal root device is one that is central to the network and not connected to end devices.

For more information about MSTP, refer to Section 5.34.3, "MSTP Operation".

The following sections describe how to configure and manage Multiple Spanning Tree Instances:

- Section 5.34.8.1, "Viewing Statistics for MSTIs"
- Section 5.34.8.2, "Viewing a List of Multiple Spanning Tree Instances"
- Section 5.34.8.3, "Adding a Multiple Spanning Tree Instance"
- Section 5.34.8.4, "Deleting a Multiple Spanning Tree Instance"

Section 5.34.8.1

Viewing Statistics for MSTIs

To view statistics related to MSTIs, type:

```
show switch spanning-tree msti-status
```

A table or list similar to the following example appears:

```
ruggedcom# show switch spanning-tree msti-status | tab
                                                                           ROOT   ROOT   ROOT   TOTAL
```

```
INSTANCE           ROOT                           BRIDGE                         PORT   PORT   PATH   TOP
ID        STATUS   PRIORITY   ROOT MAC            PRIORITY   BRIDGE MAC          SLOT   PORT   COST   CHANGES
-----------------------------------------------------------------------------------------------
1         none     0          00:00:00:00:00:00   0          00:00:00:00:00:00   ---    -1     0      0
2         none     0          00:00:00:00:00:00   0          00:00:00:00:00:00   ---    -1     0      0
3         none     0          00:00:00:00:00:00   0          00:00:00:00:00:00   ---    -1     0      0
4         none     0          00:00:00:00:00:00   0          00:00:00:00:00:00   ---    -1     0      0
5         none     0          00:00:00:00:00:00   0          00:00:00:00:00:00   ---    -1     0      0
6         none     0          00:00:00:00:00:00   0          00:00:00:00:00:00   ---    -1     0      0
7         none     0          00:00:00:00:00:00   0          00:00:00:00:00:00   ---    -1     0      0
8         none     0          00:00:00:00:00:00   0          00:00:00:00:00:00   ---    -1     0      0
9         none     0          00:00:00:00:00:00   0          00:00:00:00:00:00   ---    -1     0      0
10        none     0          00:00:00:00:00:00   0          00:00:00:00:00:00   ---    -1     0      0
11        none     0          00:00:00:00:00:00   0          00:00:00:00:00:00   ---    -1     0      0
12        none     0          00:00:00:00:00:00   0          00:00:00:00:00:00   ---    -1     0      0
13        none     0          00:00:00:00:00:00   0          00:00:00:00:00:00   ---    -1     0      0
14        none     0          00:00:00:00:00:00   0          00:00:00:00:00:00   ---    -1     0      0
15        none     0          00:00:00:00:00:00   0          00:00:00:00:00:00   ---    -1     0      0
16        none     0          00:00:00:00:00:00   0          00:00:00:00:00:00   ---    -1     0      0
```

This table or list provides the following information:

Parameter	Description
instance-id	The bridge identifier of this bridge.
status	**Synopsis:** none, designatedBridge, notDesignatedForAnyLAN, rootBridge The spanning tree status of the bridge. The status may be root or designated. This field may show text saying 'not designated for any LAN' if the bridge is not the designated bridge for any of its ports.
root-priority	The bridge identifier of the root bridge.
root-mac	The bridge identifier of the root bridge.
bridge-priority	The bridge identifier of this bridge.
bridge-mac	The bridge identifier of this bridge.
root-port-slot	**Synopsis:** sm, lm1, lm2, lm3, lm4, lm5, lm6, trnk If the bridge is designated, this is the slot containing the port that provides connectivity towards the root bridge of the network.
root-port-port	If the bridge is designated, this is the port of the slot that provides connectivity towards the root bridge of the network.
root-path-cost	The total cost of the path to the root bridge composed of the sum of the costs of each link in the path. If custom costs have not been configured, 1Gbps ports will contribute a cost of four, 100 Mbps ports will contribute 19 and 10 Mbps ports will contribute 100. For the Common and Internal Spanning Tree (CIST) instance of the Multiple Spanning Tree Protocol (MSTP), this is an external root path cost, which is the cost of the path from the Internal Spanning Tree (IST) root (i.e. regional root) bridge to the Common Spanning Tree (CST) root (i.e. network "global" root) bridge.
total-top-changes	A count of topology changes in the network, as detected on this bridge through link failures or as signaled from other bridges. Excessively high or rapidly increasing counts signal network problems.

Section 5.34.8.2

Viewing a List of Multiple Spanning Tree Instances

To view a list of Multiple Spanning Tree Instances (MSTIs), type:

```
show running-config switch spanning-tree mstp-instance
```

If instances have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config switch spanning-tree mstp-instance | tab
INSTANCE  BRIDGE
ID        PRIORITY
--------------------
1         32768
2         57344

!
```

If no MSTIs have been configured, add instances as needed. For more information, refer to Section 5.34.8.3, “Adding a Multiple Spanning Tree Instance”.

Section 5.34.8.3
Adding a Multiple Spanning Tree Instance

To add a Multiple Spanning Tree Instance (MSTI), do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the Multiple Spanning Tree Instance by typing:

   ```
   switch spanning-tree mstp-instance id
   ```

   Where:

   - *id* is the ID for the Multiple Spanning Tree Instance
3. Configure the following parameter(s) as required:

Parameter	Description
{ instance-id }	The Multiple Spanning Tree Protocol (MSTP) instance ID.
bridge-priority { bridge-priority }	**Synopsis:** 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440 **Default:** 32768 Bridge priority provides a way to control the topology of the Spanning Tree Protocol (STP) connected network. The desired root and designated bridges can be configured for a particular topology. The bridge with the lowest priority will become the root. In the event of a failure of the root bridge, the bridge with the next lowest priority will then become the root. Designated bridges that (for redundancy purposes) service a common Local Area Network (LAN) also use priority to determine which bridge is active. In this way, careful selection of bridge priorities can establish the path of traffic flows in normal and abnormal conditions.

4. Create one or more static VLANs and map them to the MSTI. For more information, refer to Section 5.35.4.2, “Adding a Static VLAN”.
5. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.34.8.4
Deleting a Multiple Spanning Tree Instance

To delete a Multiple Spanning Tree Instance (MSTI), do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the multiple spanning tree instance by typing:

```
no switch spanning-tree mstp-instance ID
```

   Where:

   - *ID* is the ID of the multiple spanning tree instance
3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.34.9

Managing Port Costs and Priorities

The following sections describe how to configure and manage port costs and priorities for individual ports:

- Section 5.34.9.1, “Viewing a List of Port Costs and Priorities”
- Section 5.34.9.2, “Adding Port Costs and Priorities”
- Section 5.34.9.3, “Deleting Port Costs and Priorities”

Section 5.34.9.1

Viewing a List of Port Costs and Priorities

To view a list of the port costs and priorities configured for switched Ethernet ports or Ethernet trunk interfaces, type:

- **For switched Ethernet ports:**

```
show running-config interface switch slot port spanning-tree msti
```

  Where:

  - *slot* is the name of the module location
  - *port* is the port number (or a list of ports, if aggregated in a port trunk) for the module
- **For Ethernet trunk interfaces:**

```
show running-config interface trunk id spanning-tree msti
```

  Where:

  - *id* is the ID given to the interface

If instances have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config interface trunks 1 spanning-tree msti | tab
INSTANCE  MSTP
ID        PRIORITY  STP COST   RSTP COST
------------------------------------------
1         128       auto-cost  auto-cost
2         128       auto-cost  auto-cost

 !
!

show running-config interface trunk id spanning-tree msti
```

Where:

- *id* is the ID given to the interface

If instances have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config interface trunks 1 spanning-tree msti | tab
INSTANCE  MSTP
ID        PRIORITY  STP COST   RSTP COST
------------------------------------------
1         128       auto-cost  auto-cost
2         128       auto-cost  auto-cost

 !
!
```

If no port costs or priorities have been configured, add them as needed. For more information, refer to Section 5.34.9.2, “Adding Port Costs and Priorities”.

Section 5.34.9.2
Adding Port Costs and Priorities

To add port costs and priorities for a switched Ethernet port or an Ethernet trunk interface, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the Multiple Spanning Tree Instance by typing:
   - **For switched Ethernet ports:**

     ```
     interface switch slot port spanning-tree msti id
     ```

     Where:
     - *slot* is the name of the module location
     - *port* is the port number (or a list of ports, if aggregated in a port trunk) for the module
     - *id* is the ID for the Multiple Spanning Tree Instance
   - **For Ethernet trunk interfaces:**

     ```
     interface trunks id spanning-tree msti mstp-id
     ```

     Where:
     - *id* is the ID given to the interface
     - *mstp-id* is the ID for the Multiple Spanning Tree Instance
3. Configure the following parameter(s) as required:

Parameter	Description
mstp-priority { mstp-priority }	**Synopsis:** 16, 32, 64, 96, 112, 128, 144, 160, 176, 192, 208, 224, 240 **Default:** 128 The STP port priority. Ports of the same cost that attach to a common LAN will select the port to be used based upon the port priority.
stp-cost { stp-cost }	**Synopsis:** auto-cost, **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

Parameter	Description
	links and 100 for 10 Mbps links). For MSTP, this parameter applies to both external and internal path costs.
rstp-cost { rstp-cost }	**Synopsis:** auto-cost, **Default:** auto-cost The cost to use in cost calculations, when the cost style parameter is set to RSTP in the bridge RSTP parameter configuration. Setting the cost manually provides the ability to preferentially select specific ports to carry traffic over others. Leave this field set to 'auto' to use the standard RSTP port costs as negotiated (20,000 for 1Gbps, 200,000 for 100 Mbps links and 2,000,000 for 10 Mbps links). For MSTP, this parameter applies to both external and internal path costs.

4. Type **`commit`** and press **Enter** to save the changes, or type **`revert`** and press **Enter** to abort.

Section 5.34.9.3
Deleting Port Costs and Priorities

To delete port costs and priorities configured for a switched Ethernet port or an Ethernet trunk interface, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the multiple spanning tree instance by typing:
   - **For switched Ethernet ports:**

     ```
     no interface switch slot port spanning-tree msti id
     ```

     Where:
     - *slot* is the name of the module location
     - *port* is the port number (or a list of ports, if aggregated in a port trunk) for the module
     - *id* is the ID for the Multiple Spanning Tree Instance
   - **For Ethernet trunk interfaces:**

     ```
     no interface trunks id spanning-tree msti mstp-id
     ```

     Where:
     - *id* is the ID given to the interface
     - *mstp-id* is the ID for the Multiple Spanning Tree Instance
3. Type **`commit`** and press **Enter** to save the changes, or type **`revert`** and press **Enter** to abort.

Section 5.34.10
Viewing the Status of RSTP

To view the status of the RSTP network, type:

```
show switch spanning-tree rstp-status
```

A list similar to the following appears:

```
ruggedcom# show switch spanning-tree rstp-status
rstp-status
```

```
status                   notDesignatedForAnyLAN
bridge priority          32768
bridge mac               00:0a:dc:f6:c6:ff
root priority            32768
root mac                 00:0a:dc:00:71:57
regional root priority   32768
regional root mac        00:0a:dc:f6:c6:ff
root port slot           lm1
root port port           1
root path cost           38
regional root path cost  0
configured hello time    2
learned hello time       2
configured forward delay 15
learned forward delay    15
configured max age       20
learned max age          20
total top changes        5
```

This list provides the following information:

Parameter	Description
status	**Synopsis:** none, designatedBridge, notDesignatedForAnyLAN, rootBridge The spanning tree status of the bridge. The status may be root or designated. This field may show text saying 'not designated for any LAN' if the bridge is not the designated bridge for any of its ports.
bridge-priority	The bridge identifier of this bridge.
bridge-mac	The bridge identifier of this bridge.
root-priority	The ports to which the multicast group traffic is forwarded.
root-mac	The ports to which the multicast group traffic is forwarded.
regional-root-priority	The bridge identifier of the Internal Spanning Tree (IST) regional root bridge for the Multiple Spanning Tree (MST) region this device belongs to.
regional-root-mac	The bridge identifier of the Internal Spanning Tree (IST) regional root bridge for the Multiple Spanning Tree (MST) region this device belongs to.
root-port-slot	**Synopsis:** sm, lm1, lm2, lm3, lm4, lm5, lm6, trnk If the bridge is designated, this is the slot containing the port that provides connectivity towards the root bridge of the network.
root-port-port	If the bridge is designated, this is the port of the slot that provides connectivity towards the root bridge of the network.
root-path-cost	The total cost of the path to the root bridge, composed of the sum of the costs of each link in the path. If custom costs have not been configured. 1Gbps ports will contribute a cost of four, 100 Mbps ports will contribute 19 and 10 Mbps ports will contribute 100. For the Common and Internal Spanning Tree (CIST) instance of the Multiple Spanning Tree Protocol (MSTP), this is an external root path cost, which is the cost of the path from the Internal Spanning Tree (IST) root (i.e. regional root) bridge to the Common Spanning Tree (CST) root (i.e. network "global" root) bridge.
regional-root-path-cost	For the Common and Internal Spanning Tree (CIST) instance of the Multiple Spanning Tree Protocol (MSTP), this is the cost of the path to the Internal Spanning Tree (IST) root (i.e. regional root) bridge
configured-hello-time	The configured hello time from the Bridge RSTP Parameters menu.
learned-hello-time	The actual hello time provided by the root bridge as learned in configuration messages. This time is used in designated bridges.
configured-forward-delay	The configured forward delay time from the Bridge RSTP Parameters menu.

Parameter	Description
learned-forward-delay	The actual forward delay time provided by the root bridge as learned in configuration messages. This time is used in designated bridges.
configured-max-age	The configured maximum age time from the Bridge RSTP Parameters menu.
learned-max-age	The actual maximum age time provided by the root bridge as learned in configuration messages. This time is used in designated bridges.
total-top-changes	A count of topology changes in the network, as detected on this bridge through link failures or as signaled from other bridges. Excessively high or rapidly increasing counts signal network problems.

Section 5.34.11

Viewing RSTP Per-Port Statistics

To view Rapid Spanning Tree Protocol (RSTP) statistics for each port, type:

```
show switch spanning-tree port-rstp-stats
```

A table or list similar to the following example appears:

```
ruggedcom# show switch spanning-tree port-rstp-stats | tab
                                    DESG
                        STP         BRIDGE                       OPER   RX     TX     RX        TX
 RX     TX
SLOT   PORT  STP STATE   ROLE  COST  PRIORITY  DESG BRIDGE MAC    EDGE   RSTS   RSTS   CONFIGS   CONFIGS
 TCNS  TCNS
---------------------------------------------------------------------------------------------
lm1    1     forwarding  root  19    32768     00:0a:dc:78:fc:40  false  432    0      0         0        0
     0
lm1    2     linkDown    ----  0     0         00:00:00:00:00:00  false  0      0      0         0        0
     0
```

This table or list provides the following information:

Parameter	Description
slot	**Synopsis:** sm, lm1, lm2, lm3, lm4, lm5, lm6, trnk The slot of the module that contains this port.
port	The port number as seen on the front plate silkscreen of the module.
stp-state	**Synopsis:** disabled, blocking, listening, learning, forwarding, linkDown, discarding Describes the status of this interface in the spanning tree: • Disabled: Spanning Tree Protocol (STP) is disabled on this port. • Link Down: STP is enabled on this port but the link is down. • Discarding: The link is not used in the STP topology but is standing by. • Learning: The port is learning MAC addresses in order to prevent flooding when it begins forwarding traffic. • Forwarding : The port is forwarding traffic.
stp-role	**Synopsis:** ----, root, designated, alternate, backup, master The role of this port in the spanning tree: • Designated: The port is designated for (i.e. carries traffic towards the root for) the Local Area Network (LAN) it is connected to. • Root: The single port on the bridge, which provides connectivity towards the root bridge.

Parameter	Description
	• Backup: The port is attached to a LAN that is serviced by another port on the bridge. It is not used but is standing by. • Alternate: The port is attached to a bridge that provides connectivity to the root bridge. It is not used but is standing by. • Master: Only exists in Multiple Spanning Tree Protocol (MSTP). The port is a Multiple Spanning Tree (MST) region boundary port and the single port on the bridge, which provides connectivity for the Multiple Spanning Tree Instance (MSTI) towards the Common Spanning Tree (CST) root bridge (i.e. this port is the root port for the Common Spanning Tree Instance).
cost	The cost offered by this port. If the Bridge RSTP Parameters Cost Style is set to STP, 1Gbps ports will contribute a cost of four, 100 Mbps ports will contribute 19 and 10 Mbps ports contribute 100. If the Cost Style is set to RSTP, 1Gbps will contribute 20,000, 100 Mbps ports will contribute a cost of 200,000 and 10 Mbps ports contribute a cost of 2,000,000. Note that even if the Cost style is set to RSTP, a port that migrates to STP will have its cost limited to a maximum of 65535.
desg-bridge-priority	Provided on the root ports of the designated bridges, the bridge identifier of the bridge this port is connected to.
desg-bridge-mac	Provided on the root ports of the designated bridges, the bridge identifier of the bridge this port is connected to.
oper-edge	Whether or not the port is operating as an edge port.
rx-rsts	The number of Rapid Spanning Tree Protocol (RSTP) configuration messages received on this port.
tx-rsts	The number of Rapid Spanning Tree Protocol (RSTP) configuration messages transmitted on this port.
rx-configs	The number of Spanning Tree Protocol (STP) configuration messages received on this port.
tx-configs	The number of Spanning Tree Protocol (STP) configuration messages transmitted on this port.
rx-tcns	The number of configuration change notification messages received on this port. Excessively high or rapidly increasing counts signal network problems.
tx-tcns	The number of configuration messages transmitted from this port.

Section 5.34.12

Clearing Spanning Tree Protocol Statistics

To clear all Spanning Tree Protocol statistics, type:

```
switch spanning-tree clear-stp-stats
```

Section 5.35

Managing VLANs

A Virtual Local Area Network (VLAN) is a group of devices on one or more LAN segments that communicate as if they were attached to the same physical LAN segment. VLANs are extremely flexible because they are based on logical connections, rather than physical connections.

When VLANs are introduced, all traffic in the network must belong to one VLAN or another. Traffic on one VLAN cannot pass to another, except through an inter-network router or Layer 3 switch.

VLANs are created in three ways:

- **Explicitly**

  Static VLANs can be created in the switch. For more information about static VLANs, refer to Section 5.35.4, “Managing Static VLANs”.

- **Implicitly**

  When a VLAN ID (VID) is set for a Port VLAN (PVLAN), static MAC address or IP interface, an appropriate VLAN is automatically created if it does not yet exist.

- **Dynamically**

  VLANs can be learned through GVRP. For more information about GVRP, refer to Section 5.35.1.7, “GARP VLAN Registration Protocol (GVRP)”

For more information about VLANs, refer to Section 5.35.1, “VLAN Concepts”.

The following sections describe how to configure and manage VLANs:

- Section 5.35.2, “Configuring VLANs for Switch Ethernet Ports”
- Section 5.35.3, “Configuring the Internal VLAN Range”
- Section 5.35.4, “Managing Static VLANs”
- Section 5.35.5, “Managing Forbidden Ports”
- Section 5.35.6, “Managing VLANs for HDLC-ETH Connections”
- Section 5.35.7, “Managing VLANs for Virtual Switches”
- Section 5.35.8, “Managing VLAN IDs”

Section 5.35.1

VLAN Concepts

The following sections describe some of the concepts important to the implementation of VLANs in ROX II:

- Section 5.35.1.1, “Tagged vs. Untagged Frames”
- Section 5.35.1.2, “Native VLAN”
- Section 5.35.1.3, “Edge and Trunk Port Types”
- Section 5.35.1.4, “Ingress and Egress Rules”
- Section 5.35.1.5, “Forbidden Ports List”
- Section 5.35.1.6, “VLAN-Aware Mode of Operation”
- Section 5.35.1.7, “GARP VLAN Registration Protocol (GVRP)”
- Section 5.35.1.8, “PVLAN Edge”
- Section 5.35.1.9, “VLAN Advantages”

Section 5.35.1.1

Tagged vs. Untagged Frames

VLAN tags identify frames as part of a VLAN network. When a switch receives a frame with a VLAN (or 802.1Q) tag, the VLAN identifier (VID) is extracted and the frame is forwarded to other ports on the same VLAN.

When a frame does not contain a VLAN tag, or contains an 802.1p (prioritization) tag that only has prioritization information and a VID of 0, it is considered an untagged frame.

Section 5.35.1.2

Native VLAN

Each port is assigned a native VLAN number, the Port VLAN ID (PVID). When an untagged frame ingresses a port, it is associated with the port's native VLAN.

By default, when a switch transmits a frame on the native VLAN, it sends the frame untagged. The switch can be configured to transmit tagged frames on the native VLAN.

Section 5.35.1.3

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 5.35.1.5, "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 5.35.1.4

Ingress and Egress Rules

Ingress and egress rules determine how traffic is received and transmitted by the switch.

Ingress rules are applied as follows to all frame when they are received by the switch:

Frame Received[a]	Untagged	Priority Tagged (VID = 0)	Tagged (Valid VID)
VLAN ID associated with the frame	PVID	PVID	VID in the Tag
Frame dropped due to its tagged/untagged format	No	No	No
Frame dropped if the frame associated with the VLAN is not configured (or learned) in the switch			Yes
Frame dropped if the ingress port is not a member of the VLAN the frame is associated with			No

[a] *Does not depend on the ingress port's VLAN configuration parameters.*

Egress rules are applied as follows to all frames when they are transmitted by the switch.

Egress Port Type	On Egress Port's Native VLAN	On Other VLAN	
		Port Is a Member Of the VLAN	Port Is Not a Member Of the VLAN
Edge	According to the egress port's **PVID Format** parameter	Dropped	
Trunk		Tagged	Dropped

Section 5.35.1.5

Forbidden Ports List

Each VLAN can be configured to exclude ports from membership in the VLAN using the forbidden ports list. For more about configuring a list of forbidden ports, refer to Section 5.35.5, “Managing Forbidden Ports”.

Section 5.35.1.6

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, ROX II's default VLAN settings allow the switch to still operate in a VLAN-aware mode, while providing functionality required for almost any network application. However, the IEEE 802.1Q standard defines a set of rules that must be followed by all VLAN-aware switches:

- Valid VIDs are within the range of 1 to 4094. VIDs equal to 0 or 4095 are invalid.
- Each frame ingressing a VLAN-aware switch is associated with a valid VID.
- Each frame egressing a VLAN-aware switch is either untagged or tagged with a valid VID. Priority-tagged frames with an invalid VID will never sent out by a VLAN-aware switch.

> **NOTE**
> *Some applications have requirements conflicting with IEEE 802.Q native mode of operation. For example, some applications explicitly require priority-tagged frames to be received by end devices.*

Section 5.35.1.7
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:

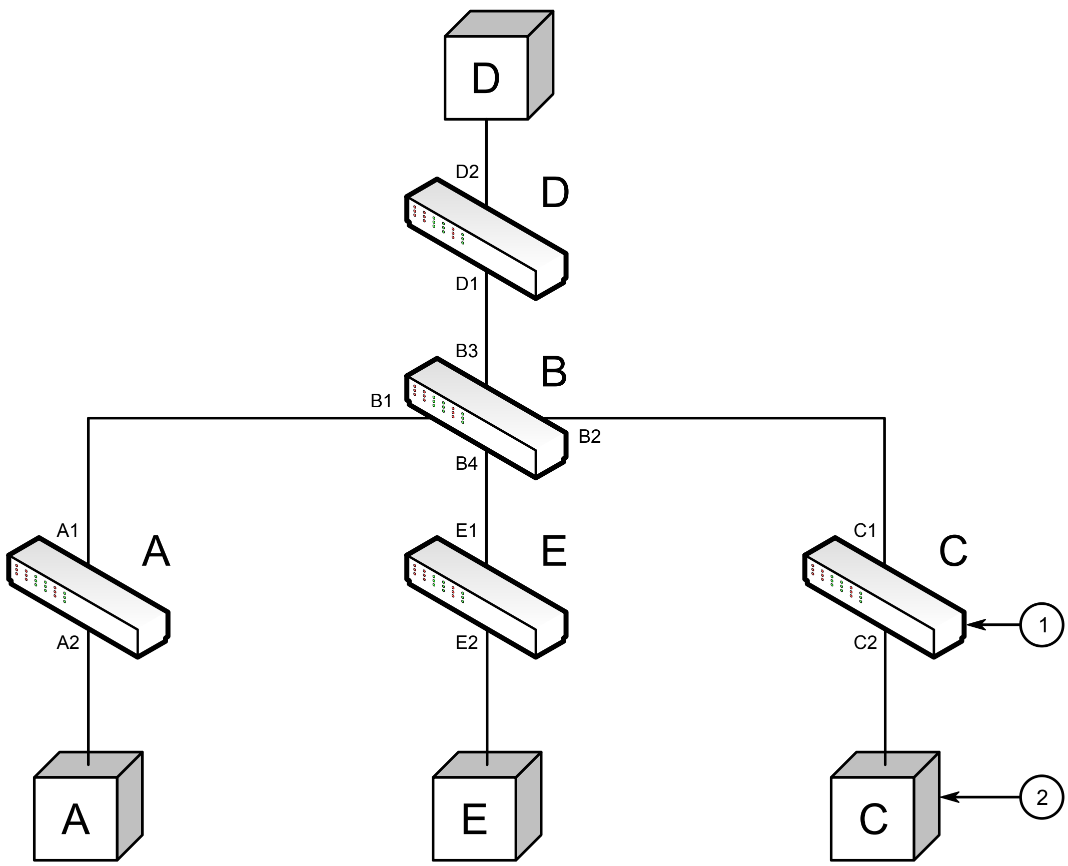

Figure 18: Using GVRP

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 5.35.1.8

PVLAN Edge

Protected VLAN (PVLAN) Edge refers to a feature of the switch that isolates multiple VLAN Edge ports from each other on a single device. All VLAN Edge ports in a switch that are configured as *protected* in this way are prohibited from sending frames to one another, but are still permitted to send frames to other, non-protected ports within the same VLAN. This protection extends to all traffic on the VLAN, including unicast, multicast and broadcast traffic.

> **NOTE**
> *This feature is strictly local to the switch. PVLAN Edge ports are not prevented from communicating with ports outside of the switch, whether protected (remotely) or not.*

Ports belonging to a specific PVID and a VLAN type of PVLAN Edge are part of one PVLAN Edge group. A PVLAN Edge group should include a minimum of two ports. There can be multiple PVLAN Edge groups on a switch.

It is not possible to combine a Gbit port with a 10/100 Mbit port as part of the same PVLAN Edge group.

Possible combinations of a PVLAN Edge group are listed below:

- A PVLAN Edge group with 10/100 Mbit ports from any line modules, with the exception of 2-port 100Base-FX line modules
- A PVLAN Edge group with Gbit ports from any line modules
- A PVLAN Edge group with 10/10 Mbit ports from 2-port 100Base-FX and Gbit ports from any line modules

Section 5.35.1.9

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.

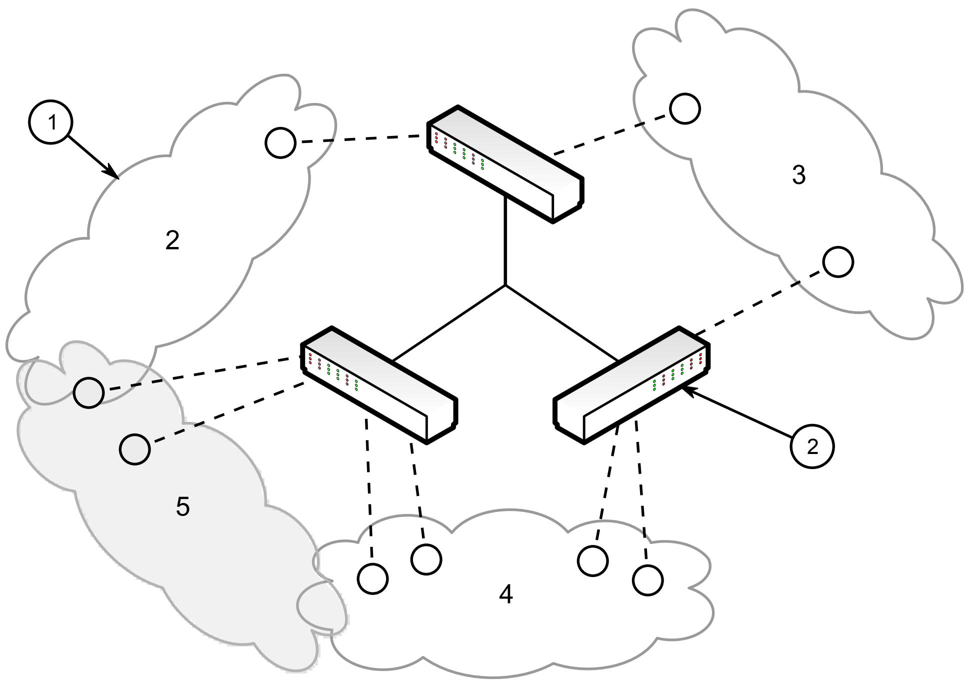

Figure 19: Multiple Overlapping VLANs

1. VLAN **2.** Switch

Administrative Convenience

VLANs enable equipement 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.

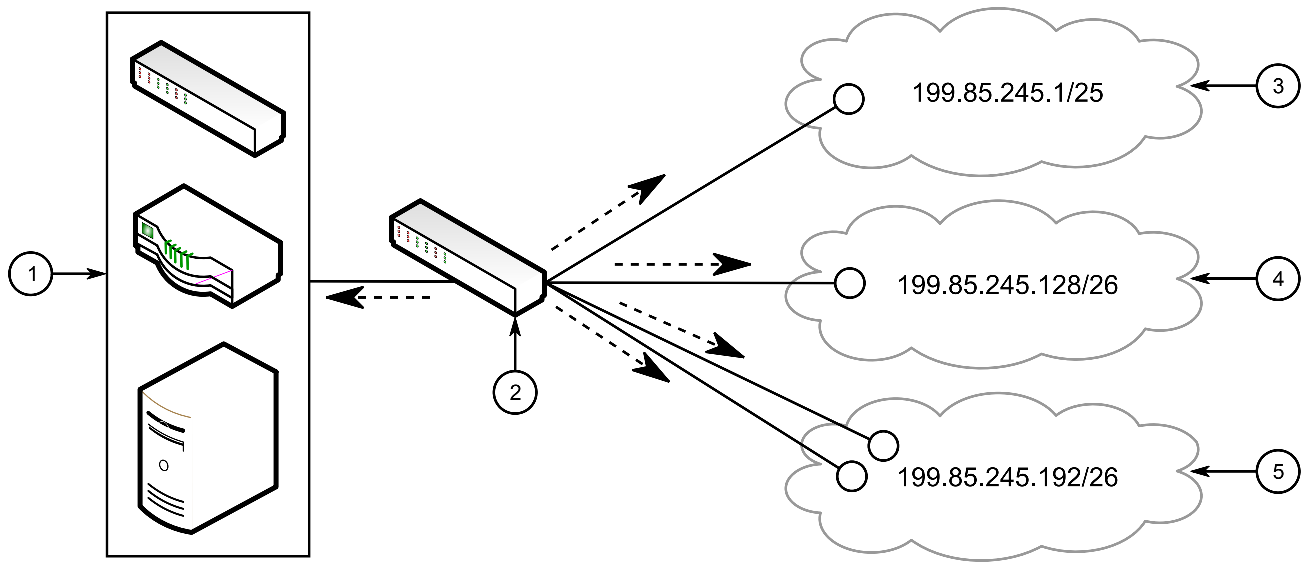

Figure 20: Inter-VLAN Communications

1. Server, Router or Layer 3 Switch **2.** Switch **3.** VLAN 2 **4.** VLAN 3 **5.** VLAN 4

Section 5.35.2

Configuring VLANs for Switch Ethernet Ports

When a VLAN ID is assigned to a switched Ethernet port, the VLAN appears in the All-VLANs Table where it can be further configured.

To configure a VLAN for a switched Ethernet port, do the following:

1. Make sure the CLI is in Configuration mode.
2. Navigate to ***switch » vlans » all-vlans » {id}***, where *{id}* is the ID of the VLAN and configure the following parameter(s) as needed:

Parameter	Description
ip-address-src { ip-address-src }	**Synopsis:** static, dynamic Whether the IP address is static or dynamically assigned via Dynamic Host Configuration Protocol (DHCP) or Bootstrap Protocol (BOOTP). The DYNAMIC option is a common case of a dynamically assigned IP address. It switches between BOOTP and DHCP until it gets the response from the relevant server. This must be static for non-management interfaces.
proxyarp	Enables/Disables whether the VLAN will respond to ARP requests for hosts other than itself.
on-demand	Brings up this interface on demand only.
mtu { mtu }	**Default:** 1500 The maximum transmission unit (the largest packet size allowed for this interface).

3. Add Quality of Service (QoS) maps to the VLAN. For more information, refer to Section 5.37.7.2, “Adding a QoS Map”.

4. Type **`commit`** and press **Enter** to save the changes, or type **`revert`** and press **Enter** to abort.

Section 5.35.3

Configuring the Internal VLAN Range

ROX II creates and utilizes internal VLANs for internal functions. To provide ROX II with a pool of VLAN IDs to pull from when creating internal VLANs, a range of VLAN IDs must be reserved.

> **CAUTION!**
> *Configuration hazard – risk of data loss. If the range-start or range-end values are changed in a way that invalidates any configured internal VLANs, the configurations defined for the affected VLANs will be lost upon repositioning.*

> **IMPORTANT!**
> *VLAN IDs reserved for internal VLANs should not be used by the network.*

> **NOTE**
> *Changing the `range-end` value repositions the matching serial VLAN. However, the matching serial VLAN is not affected when the `range-start` value is changed.*

> **NOTE**
> *If no internal VLANs are available when a switched Ethernet or trunk port is configured, the range is automatically extended so a unique value can be assigned.*

> **NOTE**
> *Routable Ethernet ports and trunks cannot be configured if internal VLANS are not enabled.*

To configure the internal VLAN range, do the following:

1. Make sure the CLI is in Configuration mode.
2. Navigate to ***admin » switch-config*** and configure the following parameter(s) as required:

Parameter	Description
enabled	**Default:** false Enables/disables the Internal VLAN Range settings.
range-start { range-start }	**Default:** 4094 **Prerequisite:** range-start must be less than or equal to range-end Defines the lower end of a range of VLANs used for the device only. VLAN ID 1 is not permitted.
range-end { range-end }	**Default:** 4094 **Prerequisite:** range-end must be greater than or equal to range-start Defines the higher end of a range of VLANs used for the device only.VLAN ID 1 is not permitted.

3. Type **`commit`** and press **Enter** to save the changes, or type **`revert`** and press **Enter** to abort.

Section 5.35.4

Managing Static VLANs

The following sections describe how to configure and manage static VLANs:

- Section 5.35.4.1, “Viewing a List of Static VLANs”
- Section 5.35.4.2, “Adding a Static VLAN”
- Section 5.35.4.3, “Deleting a Static VLAN”

Section 5.35.4.1

Viewing a List of Static VLANs

To view a list of static VLANs, type:

```
show running-config switch vlans static-vlan
```

If static VLANs have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config switch vlans static-vlan | tab
     IGMP
VID  SNOOPING  MSTI  SLOT  PORT
---------------------------------
1    -         cst

!
```

If no static VLANs have been configured, add static VLANs as needed. For more information, refer to Section 5.35.4.2, “Adding a Static VLAN”.

Section 5.35.4.2

Adding a Static VLAN

To add a static VLAN for either a routable Ethernet port or virtual switch, do the following:

1. Make sure the CLI is in Configuration mode.
2. Configure the following parameter(s) as required:

Parameter	Description
{ vid }	<int, 1 \.\. 15>;;The VLAN identifier is used to identify the VLAN in tagged Ethernet frames according to IEEE 802.1Q.
igmp-snooping	Enables or disables IGMP Snooping on the VLAN.
msti { msti }	**Synopsis:** cst, **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.

3. If needed, configure a forbidden ports list. For more information, refer to Section 5.35.5.2, “Adding a Forbidden Port”.
4. Configure the VLAN for the port. For more information, refer to Section 5.35.2, “Configuring VLANs for Switch Ethernet Ports”.

5. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.35.4.3
Deleting a Static VLAN

To delete a static VLAN for either a routable Ethernet port or virtual switch, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the static VLAN by typing:

   ```
   no switch vlans static-vlan id
   ```

   Where:

   - *id* is the ID of the VLAN
3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.35.5
Managing Forbidden Ports

Static VLANs can be configured to exclude ports from membership in the VLAN using the forbidden ports list.

The following sections describe how to configure and manage a list of forbidden ports:

- Section 5.35.5.1, “Viewing a List of Forbidden Ports”
- Section 5.35.5.2, “Adding a Forbidden Port”
- Section 5.35.5.3, “Deleting a Forbidden Port”

Section 5.35.5.1
Viewing a List of Forbidden Ports

To view a list of forbidden ports, type:

```
show running-config switch vlans static-vlan forbidden-ports
```

If ports have been forbidden, a table or list similar to the following example appears:

```
ruggedcom# show running-config switch vlans static-vlan forbidden-ports | tab
VID  SLOT  PORT
-----------------
50
     lm1   1
     lm1   2
60
     lm1   2
     lm1   3
     lm1   4
70
     lm1   5

!
```

If no ports have been forbidden, add forbidden ports as needed. For more information, refer to Section 5.35.5.2, “Adding a Forbidden Port”.

Section 5.35.5.2
Adding a Forbidden Port

To add a forbidden port, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the forbidden port by typing:

```
switch vlans static-vlan name forbidden-ports slot port
```

Where:

- *name* is the name of the static VLAN
- *slot* is the name of the module location
- *port* is the port number (or a list of ports, if aggregated in a port trunk) for the module

3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.35.5.3
Deleting a Forbidden Port

To delete a forbidden port, do the following:

1. Make sure the CLI is in Configuration mode.
2. Configure the following parameter(s) as required:

```
no switch vlans static-vlan name forbidden-ports slot port
```

Where:

- *name* is the name of the static VLAN
- *slot* is the name of the module location
- *port* is the port number (or a list of ports, if aggregated in a port trunk) for the module

3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.35.6
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.*

The following sections describe how to configure and manage VLANs for HDLC-ETH connections:

- Section 5.35.6.1, “Viewing a List of HDLC-ETH VLANs”
- Section 5.35.6.2, “Adding an HDLC-ETH VLAN”
- Section 5.35.6.3, “Deleting an HDLC-ETH VLAN”

Section 5.35.6.1

Viewing a List of HDLC-ETH VLANs

To view a list of VLANs configured for an HDLC-ETH connection, type:

```
show running-config interface wan interface protocol channel connection hdlc-eth vlan id
```

Where:

- *interface* is the WAN interface
- *protocol* is either T1 or E1
- *id* is the ID of the VLAN

If VLANs have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config interface wan lm4 1 t1 channel connection hdlc-eth vlan | tab
                                   IP
                    ON             ADDRESS
CHANNELNUMBER  VID  DEMAND  MTU    SRC      QOS  INGRESS  MARK
---------------------------------------------------------------
1
               100  -       1500   static
               200  -       1500   static

 !
!
```

If no VLANs have been configured, add VLANs as needed. For more information, refer to Section 5.35.6.2, “Adding an HDLC-ETH VLAN”.

Section 5.35.6.2

Adding an HDLC-ETH VLAN

To add a VLAN to an HDLC-ETH connection, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the VLAN by typing:

   ```
   interface wan interface protocol channel number connection hdlc-eth vlan id
   ```

   Where:

   - *interface* is the WAN interface
   - *protocol* is either T1 or E1
   - *number* is the channel number
   - *id* is the ID of the VLAN
3. Configure the following parameter(s) as required:

Parameter	Description
on-demand	This interface is up or down on demand of link fail over.
mtu { mtu }	**Default:** 1500 Maximum transmission unit (largest packet size allowed for this interface).
ip-address-src { ip-address-src }	**Synopsis:** static, dynamic **Default:** static

Parameter	Description
	Whether the IP address is static or dynamically assigned via DHCP or BOOTP. 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

4. Add Quality of Service (QoS) maps to the VLAN. For more information, refer to Section 5.37.7.2, “Adding a QoS Map”.
5. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.35.6.3
Deleting an HDLC-ETH VLAN

To delete a VLAN for an HDLC-ETH connection, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the VLAN by typing:

```
no interface wan interface protocol channel number connection hdlc-eth vlan id
```

   Where:

   - *interface* is the WAN interface
   - *protocol* is either T1 or E1
   - *number* is the channel number
   - *id* is the ID of the VLAN
3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.35.7
Managing VLANs for Virtual Switches

The following sections describe how to configure and manage VLANs for virtual switch interfaces:

- Section 5.35.7.1, “Viewing a List of Virtual Switch VLANs”
- Section 5.35.7.2, “Adding a Virtual Switch VLAN”
- Section 5.35.7.3, “Deleting a Virtual Switch VLAN”

Section 5.35.7.1
Viewing a List of Virtual Switch VLANs

To view a list of virtual switch VLANs, type:

```
show running-config interface virtualswitch id vlan
```

Where:

- *id* is the ID assigned to the virtual switch

If VLANs have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config interface virtualswitch 1 vlan | tab
     IP
     ADDRESS
VID  SRC       QOS  INGRESS  MARK
----------------------------------
100  static

 !
!
```

If no virtual switch VLANs have been configured, add VLANs as needed. For more information, refer to Section 5.35.7.2, “Adding a Virtual Switch VLAN”.

Section 5.35.7.2
Adding a Virtual Switch VLAN

To add virtual switch VLAN, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the virtual switch by typing:

```
interface virtualswitch id vlan vlan-id
```

Where:

- *id* is the ID assigned to the virtual switch
- *vlan-id* is the ID assigned to the VLAN

3. Configure the following parameter(s) as required:

Parameter	Description
ip-address-src { ip-address-src }	**Synopsis:** static, dynamic **Default:** static Whether the IP address is static or dynamically assigned via DHCP or BOOTP.

4. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.35.7.3
Deleting a Virtual Switch VLAN

To delete a virtual switch VLAN, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the chosen VLAN by typing:

```
no interface virtualswitch id vlan vlan-id
```

Where:

- *id* is the ID assigned to the virtual switch
- *vlan-id* is the ID assigned to the VLAN

3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.35.8

Managing VLAN IDs

The following sections describe how to configure and manage VLAN IDs for routable Ethernet ports and virtual switches:

- Section 5.35.8.1, “Viewing a List of VLAN IDs for Routable Ethernet Ports and Virtual Switches”
- Section 5.35.8.2, “Viewing a List of VLAN IDs for T1/E1 Lines”
- Section 5.35.8.3, “Adding a VLAN ID to a Routable Ethernet Port or Virtual Switch”
- Section 5.35.8.4, “Adding a VLAN ID to a T1/E1 Line”
- Section 5.35.8.5, “Deleting a VLAN ID for a Routable Ethernet Port or Virtual Switch”
- Section 5.35.8.6, “Deleting a VLAN ID for a T1/E1 Line”

Section 5.35.8.1

Viewing a List of VLAN IDs for Routable Ethernet Ports and Virtual Switches

To view a list of VLAN IDs (VIDs) configured for either a routable Ethernet port or virtual switch, type:

```
show running-config interface interface vlan
```

Where:

- *interface* is the type of interface (either *eth* or *virtualswitch*)

If VLAN IDs have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config interface eth vlan | tab
                 IP
                 ADDRESS  ON
SLOT  PORT  VID  SRC      DEMAND  QOS  INGRESS  MARK
------------------------------------------------------
cm    1
            999  static   -

!
```

If no VLAN IDs have been configured, add VLAN IDs as needed. For more information about configuring VLAN IDs for either a routable Ethernet port or virtual switch, refer to Section 5.35.8.3, “Adding a VLAN ID to a Routable Ethernet Port or Virtual Switch”.

Section 5.35.8.2

Viewing a List of VLAN IDs for T1/E1 Lines

To view a list of VLAN IDs (VIDs) configured for either a T1 or E1 line, type:

```
show running-config interface wan slot port protocol channel number connection hdlc-eth vlan
```

Where:

- *slot* is the name of the module location
- *port* is the port number (or a list of ports, if aggregated in a port trunk) for the module
- *protocol* is either T1 or E1
- *number* is the channel number

If VLAN IDs have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config interface wan lm4 1 t1 channel 1 connection hdlc-eth vlan
interface
 wan lm4 1
  t1 channel 1
   connection hdlc-eth vlan 4024
   !
  !
 !
!
```

If no VLAN IDs have been configured, add VLAN IDs as needed. For more information about configuring VLAN IDs for either a T1 or E1 line, refer to Section 5.35.8.4, “Adding a VLAN ID to a T1/E1 Line”.

Section 5.35.8.3
Adding a VLAN ID to a Routable Ethernet Port or Virtual Switch

To add a VLAN ID (VID) to either a routable Ethernet port or virtual switch, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the new VLAN ID by typing:

   ```
   interface interface interface-name vlan id
   ```

   Where:

   - *interface* is the type of interface (either *eth* or *virtualswitch*)
   - *interface-name* is the name of the interface
   - *id* is the ID of the VLAN
3. Configure the following parameter(s) as required:

Parameter	Description
ip-address-src { ip-address-src }	**Synopsis:** static, dynamic **Default:** static Whether the IP address is static or dynamically assigned via DHCP or BOOTP. The DYNAMIC option is a common case of a dynamically assigned IP address. It switches between BOOTP and DHCP until it gets the response from the relevant server. It must be static for non-management interfaces.
on-demand	This interface is up or down on the demand of the link failover.

4. Add a QoS map for the VLAN. For more information, refer to Section 5.37.7.2, “Adding a QoS Map”.
5. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.35.8.4
Adding a VLAN ID to a T1/E1 Line

To add a VLAN ID (VID) to a T1/E1 line, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the new VLAN ID by typing:

```
interface wan slot port protocol channel number connection hdlc-eth vlan id
```

Where:

- *slot* is the name of the module location
- *port* is the port number (or a list of ports, if aggregated in a port trunk) for the module
- *protocol* is either T1 or E1
- *number* is the channel number
- *id* is the ID of the VLAN

3. Configure the following parameter(s) as required:

Parameter	Description
on-demand	This interface is up or down on demand of link fail over.
mtu { mtu }	**Default:** 1500 Maximum transmission unit (largest packet size allowed for this interface).
ip-address-src { ip-address-src }	**Synopsis:** static, dynamic **Default:** static Whether the IP address is static or dynamically assigned via DHCP or BOOTP. The DYNAMIC option is a common case of a dynamically assigned IP address. It switches between BOOTP and DHCP until it gets the response from the relevant server. It must be static for non-management interfaces

4. Add a QoS map for the VLAN. For more information, refer to Section 5.37.7.2, “Adding a QoS Map”.
5. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.35.8.5

Deleting a VLAN ID for a Routable Ethernet Port or Virtual Switch

To delete a VLAN ID (VID) configured for either a routable Ethernet port or virtual switch, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the traffic control rule by typing:

```
no interface interface interface-name vlan id
```

Where:

- *interface* is the type of interface (either *eth* or *virtualswitch*)
- *interface-name* is the name of the interface
- *id* is the ID of the VLAN

3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.35.8.6

Deleting a VLAN ID for a T1/E1 Line

To delete a VLAN ID (VID) configured for either a T1 or E1 line, do the following:

1. Make sure the CLI is in Configuration mode.

2. Delete the traffic control rule by typing:

```
no interface wan slot port protocol channel number connection hdlc-eth vlan id
```

Where:

- *slot* is the name of the module location
- *port* is the port number (or a list of ports, if aggregated in a port trunk) for the module
- *protocol* is either T1 or E1
- *number* is the channel number
- *id* is the ID of the VLAN

3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.36

Managing Network Discovery and LLDP

ROX II supports the Link Layer Discovery Protocol (LLDP), a Layer 2 protocol for automated network discovery.

LLDP is an IEEE standard protocol, IEEE 802.11AB, which allows a networked device to advertise its own basic networking capabilities and configuration. It can simplify the troubleshooting of complex networks and can be used by Network Management Systems (NMS) to obtain and monitor detailed information about a network's topology. LLDP data are made available via SNMP (through support of LLDP-MIB).

LLDP allows a networked device to discover its neighbors across connected network links using a standard mechanism. Devices that support LLDP are able to advertise information about themselves, including their capabilities, configuration, interconnections, and identifying information.

LLDP agent operation is typically implemented as two modules: the LLDP transmit module and LLDP receive module. The LLDP transmit module, when enabled, sends the local device's information at regular intervals, in 802.1AB standard format. Whenever the transmit module is disabled, it transmits an LLDPDU (LLDP data unit) with a time-to-live (TTL) TLV containing *0* in the information field. This enables remote devices to remove the information associated with the local device in their databases. The LLDP receive module, when enabled, receives information about remote devices and updates its LLDP database of remote systems. When new or updated information is received, the receive module initiates a timer for the valid duration indicated by the TTL TLV in the received LLDPDU. A remote system's information is removed from the database when an LLDPDU is received from it with TTL TLV containing *0* in its information field.

CAUTION!
Security hazard – risk of unauthorized access and/or exploitation. LLDP is not secure by definition. Avoid enabling LLDP on devices connected to external networks. Siemens recommends using LLDP only in secure environments operating within a security perimeter.

NOTE
LLDP is implemented to keep a record of only one device per Ethernet port. Therefore, if there are multiple devices sending LLDP information to a switch port on which LLDP is enabled, information about the neighbor on that port will change constantly.

The following sections describe how to configure and manage LLDP:

- Section 5.36.1, "Configuring LLDP"
- Section 5.36.2, "Viewing Global Statistics and Advertised System Information"
- Section 5.36.3, "Viewing Statistics for LLDP Neighbors"

- Section 5.36.4, “Viewing Statistics for LLDP Ports”

Section 5.36.1
Configuring LLDP

To configure the Link Layer Discovery Protocol (LLDP), do the following:

1. Make sure the CLI is in Configuration mode.
2. Navigate to ***switch » net-discovery » lldp*** and configure the following parameter(s) as required:

Parameter	Description
enabled	**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.
tx-interval { tx-interval }	**Default:** 30 The interval at which Link Layer Discovery Protocol (LLDP) frames are transmitted on behalf of this LLDP agent.
tx-hold { tx-hold }	**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))
reinit-delay { reinit-delay }	**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.
tx-delay { tx-delay }	**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 { notification-interval }	**Default:** 5 Controls transmission of LLDP traps. The agent must not generate more than one trap in an indicated period.

3. Type **`commit`** and press **Enter** to save the changes, or type **`revert`** and press **Enter** to abort.

Section 5.36.2
Viewing Global Statistics and Advertised System Information

To view global statistics for LLDP, type:

```
show switch net-discovery lldp global-statistics
```

A table or list similar to the following appears:

```
ruggedcom# show switch net-discovery lldp global-statistics
global-statistics
 inserts          21
 deletes          20
 drops            0
 ageouts          8
```

```
 last change time 3D14m19s
```

This table or list displays the following information:

Parameter	Description
inserts	The number of times an entry was inserted into the LLDP Neighbor Information Table.
deletes	The number of times an entry was deleted from the LLDP Neighbor Information Table.
drops	The number of times an entry was deleted from the LLDP Neighbor Information Table because the information timeliness interval has expired.
ageouts	The number of all TLVs discarded.
last-change-time	The duration of time between power-on and when this information was received.

To view the system information that is advertised to neighbors, type:

```
show switch net-discovery lldp local-system
```

A table or list similar to the following appears:

```
ruggedcom#  show switch net-discovery lldp local-system
local-system
 local chassis subtype     macAddress
 local chassis id          00:0a:dc:ff:9a:00
 local system name         R12.localdomain
 local system desc         RX5000-R-MNT-HI-HI-SM61-CM01-L3SEC-16TX01-XX-XX-XX-4FG50-XX
 local system caps         bridge,router
 local system caps enabled bridge,router
```

This table or list displays the following information:

Parameter	Description
local-chassis-subtype	**Synopsis:** chassisComponent, interfaceAlias, portComponent, macAddress, networkAddress, interfaceName, local local-chassis-subtype
local-chassis-id	local-chassis-id
local-system-name	local-system-name
local-system-desc	local-system-desc
local-system-caps	local-system-caps
local-system-caps-enabled	local-system-caps-enabled

Section 5.36.3
Viewing Statistics for LLDP Neighbors

To view statistics for LLDP neighbors, type:

```
show switch net-discovery lldp port-lldp-neighbors
```

A table or list similar to the following appears:

```
ruggedcom# show switch net-discovery lldp port-lldp-neighbors
port-lldp-neighbors lm1 1
 chassis id             ""
```

```
port id                ""
system name            ""
system desc            ""
port desc              ""
man address            ""
man address if id      0
system caps            ""
system caps enabled    ""
chassis subtype        macAddress
port subtype           interfaceName
man address subtype    other
man address if subtype unknown
last update            0s
```

This table or list displays the following information:

Parameter	Description
slot	**Synopsis:** pm1, pm2, main, sm, lm1, lm2, lm3, lm4, lm5, lm6, cm, em, trnk The slot of the module that contains this port.
port	The port number as seen on the front plate silkscreen of the module.
chassis-id	The Chassis ID information received from a remote Link Layer Discovery Protocol (LLDP) agent.
port-id	The port ID (MAC) information received from a remote Link Layer Discovery Protocol (LLDP) agent.
system-name	The system name information received from a remote Link Layer Discovery Protocol (LLDP) agent
system-desc	The system descriptor information received from a remote Link Layer Discovery Protocol (LLDP) agent.
port-desc	The port description information received from a remote Link Layer Discovery Protocol (LLDP) agent.
man-address	The management address received from a remote Link Layer Discovery Protocol (LLDP) agent.
man-address-if-id	The Management Address Interface ID received from a remote Link Layer Discovery Protocol (LLDP) agent.
system-caps	The system capabilities that are advertised for the remote device.
system-caps-enabled	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.
man-address-subtype	**Synopsis:** other, ipV4, ipV6, nsap, hdlc, bbn1822, all802, e163, e164, f69, x121, ipx, appleTalk, decnetIV, banyanVines, e164withNsap, dns, distinguishedName, asNumber, xtpOverIpv4, xtpOverIpv6, xtpNativeModeXTP, fibreChannelWWPN, fibreChannelWWNN, gwid, afi, reserved The management address subtype received from a remote Link Layer Discovery Protocol (LLDP) agent.
man-address-if-subtype	**Synopsis:** unknown, ifIndex, systemPortNumber

Parameter	Description
	The management address interface subtype received from a remote Link Layer Discovery Protocol (LLDP) agent.
last-update	The duration of time between power-on and when this information was received.

Section 5.36.4

Viewing Statistics for LLDP Ports

To view statistics for LLDP ports, type:

```
show switch net-discovery lldp port-lldp-stats
```

A table or list similar to the following appears:

```
ruggedcom# show switch net-discovery lldp port-lldp-stats
             FRM  ERR  FRM   FRM            TLVS  TLVS
SLOT  PORT   DRP  FRM  IN    OUT   AGEOUTS  DROP  UNKNOWN
-----------------------------------------------------------
lm1   1      0    0    0     0     0        0     0
lm1   2      0    0    8583  8577  8        0     0
lm1   3      0    0    0     0     0        0     0
lm1   4      0    0    0     0     0        0     0
lm1   5      0    0    0     0     0        0     0
lm1   6      0    0    0     0     0        0     0
lm1   7      0    0    0     0     0        0     0
lm1   8      0    0    8934  8934  0        0     0
lm1   9      0    0    0     0     0        0     0
lm1   10     0    0    0     0     0        0     0
lm1   11     0    0    0     0     0        0     0
lm1   12     0    0    0     0     0        0     0
lm1   13     0    0    0     0     0        0     0
lm1   14     0    0    0     0     0        0     0
lm1   15     0    0    0     0     0        0     0
lm1   16     0    0    0     0     0        0     0
lm5   1      0    0    0     0     0        0     0
lm5   2      0    0    0     0     0        0     0
lm5   3      0    0    0     0     0        0     0
lm5   4      0    0    0     0     0        0     0
cm    1      0    0    8915  8900  0        0     0
```

This table or list displays the following information:

Parameter	Description
slot	**Synopsis:** pm1, pm2, main, sm, lm1, lm2, lm3, lm4, lm5, lm6, cm, em, trnk The slot of the module that contains this port.
port	The port number as seen on the front plate silkscreen of the module.
frm-drp	A counter of all Link Layer Discovery Protocol (LLDP) frames discarded.
err-frm	A counter of all Link Layer Discovery Protocol Units (LLDPUs) received with detectable errors.
frm-in	A counter of all Link Layer Discovery Protocol Units (LLDPUs) received.
frm-out	A counter of all Link Layer Discovery Protocol Units (LLDPUs) transmitted.
ageouts	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

Parameter	Description
tlvs-drop	A counter of all TLVs discarded
tlvs-unknown	A counter of all TLVs received on the port that are not recognized by the Link Layer Discovery Protocol (LLDP) local agent

Section 5.37

Managing Traffic Control

Traffic control is a firewall subsystem that manages the amount of bandwidth for each network interface that different types of traffic are permitted to use. For a traffic control configuration to work, a firewall must be configured.

NOTE
For more information about firewalls, refer to Section 5.17, “Managing Firewalls”.

ROX II allows up to 4 different firewall configurations, enabling users to quickly change between configurations. Users can quickly assess different configurations without needing to save and reload any part of the configuration. In contrast, there is only one traffic control configuration. When enabled, a traffic control configuration is used with the current firewall configuration. A current firewall configuration is defined as one that is specified in either work-config and/or active-config. It does not have to be enabled to be validated.

NOTE
Traffic control is not available for Ethernet traffic on any line module when Layer 3 hardware acceleration is enabled. It is intended to be used only on WAN interfaces.

The following sections describe how to configure and manage traffic control settings:

- Section 5.37.1, “Enabling and Configuring Traffic Control”
- Section 5.37.2, “Managing Traffic Control Interfaces”
- Section 5.37.3, “Managing Traffic Control Priorities”
- Section 5.37.4, “Managing Traffic Control Classes”
- Section 5.37.5, “Managing Traffic Control Devices”
- Section 5.37.6, “Managing Traffic Control Rules”
- Section 5.37.7, “Managing QoS Mapping for VLANs”
- Section 5.37.8, “Managing Egress Markers for QoS Maps”
- Section 5.37.9, “Viewing QoS Statistics”

Section 5.37.1

Enabling and Configuring Traffic Control

Traffic control functions are divided into two modes:

- **Basic Mode**

  Basic mode offers a limited set of options and parameters. Use this mode to set the outgoing bandwidth for an interface, the interface priority (high, medium or low), and some simple traffic control characteristics. Basic traffic shaping affects traffic identified by protocol, port number, address and interface. Note that some of these options are mutually exclusive. Refer to the information given for each option.

In basic mode, a packet is categorized based on the contents of its Type of Service (ToS) field if it does not match any of the defined classes.

- **Advanced Mode**

  In advanced mode, each interface to be managed is assigned a total bandwidth for incoming and outgoing traffic. Classes are then defined for each interface, each with its own minimum assured bandwidth and a maximum permitted bandwidth. The combined minimum of the classes on an interface must be no more than the total outbound bandwidth specified for the interface. Each class is also assigned a priority, and any bandwidth left over after each class has received its minimum allocation (if needed) will be allocated to the lowest priority class up until it reaches its maximum bandwidth, after which the next priority is allocated more bandwidth. When the specified total bandwidth for the interface is reached, no further packets are sent, and any further packets may be dropped if the interface queues are full.

  Packets are assigned to classes on the outbound interface based on either a mark assigned to the packet, or the Type of Service (ToS) field in the IP header. If the ToS field matches a defined class, the packet is allocated to that class. Otherwise, it is allocated to any class that matches the mark assigned to the packet. If no class matches the mark, the packet is assigned to the default class.

  Marks are assigned to packets by traffic control rules that are based on a number of parameters, such as IP address, port number, protocol, packet length, and more.

The two modes cannot be accessed simultaneously. Only the mode that is currently configured can be accessed.

To enable and configure traffic control, do the following:

1. Make sure the CLI is in Configuration mode.
2. Configure the following parameter(s) as required:

Parameter	Description
enabled	Enables/disables traffic control (TC) for the current firewall configuration. The current firewall configuration is the one that is committed. When an active configuration is committed to the system, then an **enabled** TC configuration will be included. When a work configuration is committed, the **enabled** TC configuration will be included in the work configuration. **A TC configuration needs a firewall configuration to operate**.
mode-choice { mode-choice }	**Synopsis:** basic, advanced **Default:** basic Choose to use either 'simple' or 'advanced' configuration modes. Click again on traffic-control after making a choice.

3. If basic mode is enabled, do the following:
   - Add traffic control interfaces. For more information, refer to Section 5.37.2.2, “Adding a Traffic Control Interface”.
   - Add traffic control priorities. For more information, refer to Section 5.37.3.2, “Adding a Traffic Control Priority”.
4. If advanced mode is enabled, do the following:
   - Add traffic control classes. For more information, refer to Section 5.37.4.2, “Adding a Traffic Control Class”.
   - Add traffic control devices. For more information, refer to Section 5.37.5.2, “Adding a Traffic Control Device”.
   - Add traffic control rules. For more information, refer to Section 5.37.6.2, “Adding a Traffic Control Rule”.
5. Type `commit` and press **Enter** to save the changes, or type `revert` and press **Enter** to abort.

Section 5.37.2

Managing Traffic Control Interfaces

Traffic control interfaces define interfaces used for traffic shaping, mainly for outbound bandwith and the outgoing device.

> **NOTE**
> *Traffic control interfaces can only be configured in basic mode. For more information about setting the traffic control mode, refer to Section 5.37.1, "Enabling and Configuring Traffic Control".*

The following sections describe how to configure and manage traffic control interfaces:

- Section 5.37.2.1, "Viewing a List of Traffic Control Interfaces"
- Section 5.37.2.2, "Adding a Traffic Control Interface"
- Section 5.37.2.3, "Deleting a Traffic Control Interface"

Section 5.37.2.1

Viewing a List of Traffic Control Interfaces

To view a list of traffic control interfaces, type:

```
show running-config qos traffic-control basic-configuration tcinterfaces
```

If interfaces have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config qos traffic-control basic-configuration tcinterfaces
qos
 traffic-control
  basic-configuration
   tcinterfaces te1-2-1c01ppp
    type          external
    inbandwidth   1500
    in-unit       kilobits
    outbandwidth  1500
    out-unit      kilobits
    description   "TC on T1 Link"
   !
  !
 !
!
```

If no interfaces have been configured, add interfaces as needed. For more information, refer to Section 5.37.2.2, "Adding a Traffic Control Interface".

Section 5.37.2.2

Adding a Traffic Control Interface

To add a new traffic control interface, do the following:

1. Make sure the CLI is in Configuration mode.
2. Configure the following parameter(s) as required:

Parameter	Description
{ interface }	An interface to which traffic shaping will apply. Lowercase alphanumerical as well as '.' and '-' characters are allowed.
type { type }	**Synopsis:** internal, external, none **Default:** none (optional) 'external' (facing toward the Internet) or 'internal' (facing toward a local network). 'external' causes the traffic generated by each unique source IP address to be treated as a single flow. 'internal' causes the traffic generated by each unique destination IP address to be treated as a single flow. Internal interfaces seldom benefit from simple traffic shaping.
inbandwidth { inbandwidth }	(optional) The incoming bandwidth of this interface. If incoming traffic exceeds the given rate, received packets are dropped randomly. When unspecified, maximum speed is assumed. Specify only the number here. The unit (kilobits, megabits) is specified in the in-unit.
in-unit { in-unit }	**Synopsis:** none, kilobits, megabits **Default:** none The unit for inbandwidth, per second.
outbandwidth { outbandwidth }	The outgoing bandwidth for this interface. Specify only the number here. The unit (kilobits, megabits) is specified in the out-unit.
out-unit { out-unit }	**Synopsis:** kilobits, megabits **Default:** megabits The unit for outgoing bandwidth, per second.
description { description }	A description for this configuration item.

3. Type **`commit`** and press **Enter** to save the changes, or type **`revert`** and press **Enter** to abort.

Section 5.37.2.3
Deleting a Traffic Control Interface

To delete a traffic control interface, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the traffic control interface by typing:

```
no qos traffic-control basic-configuration tcinterfaces interface
```

Where:

- *`interface`* is the name of the traffic control interface

3. Type **`commit`** and press **Enter** to save the changes, or type **`revert`** and press **Enter** to abort.

Section 5.37.3

Managing Traffic Control Priorities

Traffic control priorities define priorities used for traffic shaping.

> **NOTE**
> *Traffic control priorities can only be configured in basic mode. For more information about setting the traffic control mode, refer to Section 5.37.1, “Enabling and Configuring Traffic Control”.*

The following sections describe how to configure and manage traffic control priorities:

- Section 5.37.3.1, “Viewing a List of Traffic Control Priorities”
- Section 5.37.3.2, “Adding a Traffic Control Priority”
- Section 5.37.3.3, “Deleting a Traffic Control Priority”

Section 5.37.3.1

Viewing a List of Traffic Control Priorities

To view a list of traffic control priorities, type:

```
show running-config qos traffic-control basic-configuration tcpriorities
```

If priorities have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config qos traffic-control basic-configuration tcpriorities
qos
 traffic-control
  basic-configuration
   tcpriorities high
    band        high
    protocol    tcp
    port        80
    description "High priority traffic"
   !
   tcpriorities medium
    protocol    udp
    port        1500
    description "Medium priority traffic"
   !
   tcpriorities low
    band        low
    protocol    icmp
    description "Low priority traffic"
   !
  !
 !
!
```

If no priorities have been configured, add priorities as needed. For more information, refer to Section 5.37.3.2, “Adding a Traffic Control Priority”.

Section 5.37.3.2

Adding a Traffic Control Priority

To add a new traffic control priority, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the static MAC address by typing:

```
qos traffic-control basic-configuration tcpriority name
```

Where:

- *name* is the name of the traffic control priority entry

3. Configure the following parameter(s) as required:

Parameter	Description
band { band }	**Synopsis:** high, medium, low **Default:** medium Priority (band) : high, medium, low... **High band includes:** Minimize Delay (md) (0x10), md + Minimize Monetary Cost (mmc) (0x12), md + Maximize Reliability (mr) (0x14), mmc+md+mr (0x16). **Medium band includes:** Normal Service (0x0), mr (0x04), mmc +mr (0x06), md + Maximize Throughput (mt) (0x18), mmc+mt+md (0x1a), mr+mt+md (0x1c), mmc+mr+mt+md (0x1e). **Low band includes:** mmc (0x02), mt (0x08), mmc+mt (0x0a), mr+mt (0x0c), mmc+mr+mt (0x0e).
protocol { protocol }	**Synopsis:** tcp, udp, icmp, all (choice) A targeted protocol.
port { port }	(choice) Source port - can be specified **only if** protocol is TCP, UDP, DCCP, SCTP or UDPlite **Prerequisite:** A port number can be specified only when the protocol is either TCP, UDP, DCCP, SCTP or UDPlite
address { address }	(choice) The source address. This can be specified **only if** the protocol, port and interface are not defined. **Prerequisite:** An address can be specified only if neither a protocol or port nor an interface are specified.
interface { interface }	(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. **Prerequisite:** An interface can be specified only if neither a protocol, port nor an address are specified.
description { description }	(optional) A description for this configuration.

4. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.37.3.3

Deleting a Traffic Control Priority

To delete a traffic control priority, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the traffic control priority by typing:

```
no qos traffic-control basic-configuration tcpriority name
```

Where:

- *name* is the name of the traffic control priority entry

3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.37.4
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].*

The following sections describe how to configure and manage traffic control classes:

- Section 5.37.4.1, “Viewing a List of Traffic Control Classes”
- Section 5.37.4.2, “Adding a Traffic Control Class”
- Section 5.37.4.3, “Deleting a Traffic Control Class”

Section 5.37.4.1
Viewing a List of Traffic Control Classes

To view a list of traffic control classes, type:

```
show running-config qos traffic-control advanced-configuration tcclasses
```

If classes have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config qos traffic-control advanced-configuration tcclasses
qos
 traffic-control
  advanced-configuration
   tcclasses TCP
    interface     te1-2-1c01ppp
    mark          1
    min-bandwidth full/2
    max-bandwidth full
    priority      1
   !
  !
 !
!
```

If no classes have been configured, add classes as needed. For more information, refer to Section 5.37.4.2, “Adding a Traffic Control Class”.

Section 5.37.4.2
Adding a Traffic Control Class

To add a new traffic control class, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the static MAC address by typing:

```
qos traffic-control advanced-configuration tcclasses name
```

Where:

- *name* is the name of the traffic control class entry

3. Configure the following parameter(s) as required:

Parameter	Description
{ name }	The name for this TC class entry.
interface { interface }	The interface to which this class applies. Each interface must be listed only once. Lowercase alphanumerical as well as '.' and '-' characters are allowed.
mark { mark }	A mark that identifies traffic belonging to this class. This is a unique integer between 1-255. Each class must have its own unique mark.
min-bandwidth { min-bandwidth }	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.
minbw-unit { minbw-unit }	**Synopsis:** none, kilobits, megabits **Default:** none (per second) Only if the minimum bandwidth is a **single numerical value**
max-bandwidth { max-bandwidth }	The maximum bandwidth this class is allowed to use when the link is idle. This can be either a numeric value or a calculated expression based on the bandwidth of the interface. A fixed numerical value must only be a number - its unit is specified in Maxbw-unit. A calculated expression is based on a fraction of the 'full' bandwidth, such as: . 'full/3' for a third of the bandwidth and . 'full*9/10' for nine tenths of the bandwidth. In such a case, do not specify any maxbw-unit.
maxbw-unit { maxbw-unit }	**Synopsis:** none, kilobits, megabits **Default:** none (per second) only if max-bandwidth is a **single numerical value**
priority { priority }	**Default:** 0 The priority in which classes will be serviced. Higher priority classes will experience less delay since they are serviced first. Priority values are serviced in ascending order (e.g. 0 is higher priority than 1. Minimum: 7).
description { description }	A description for this configuration item.
tos-minimize-delay	**Default:** false Value/mask encoding: 0x10/0x10
tos-maximize-throughput	**Default:** false Value/mask encoding: 0x08/0x08

Parameter	Description
tos-maximize-reliability	**Default:** false Value/mask encoding: 0x04/0x04
tos-minimize-cost	**Default:** false Value/mask encoding: 0x02/0x02
tos-normal-service	**Default:** false Value/mask encoding: 0x00/0x1e
default	**Default:** false **One default class** per interface **must** be defined.
tcp-ack	**Default:** false All TCP ACK packets into this class. This option should be specified only once per interface.
tos-value { tos-value }	A custom classifier for the given value/mask. The values are hexadecimal, prefixed by '0x'. Ex.: 0x56[/0x0F]

4. Type **`commit`** and press **Enter** to save the changes, or type **`revert`** and press **Enter** to abort.

Section 5.37.4.3
Deleting a Traffic Control Class

To delete a traffic control class, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the traffic control class by typing:

```
no qos traffic-control advanced-configuration tcclasses name
```

   Where:

   - *name* is the name of the traffic control class entry
3. Type **`commit`** and press **Enter** to save the changes, or type **`revert`** and press **Enter** to abort.

Section 5.37.5
Managing Traffic Control Devices

Traffic control devices define devices used for traffic shaping.

> **NOTE**
> *Traffic control devices can only be configured in advanced mode. For more information about setting the traffic control mode, refer to Section 5.37.1, "Enabling and Configuring Traffic Control".*

The following sections describe how to configure and manage traffic control devices:

- Section 5.37.5.1, "Viewing a List of Traffic Control Devices"
- Section 5.37.5.2, "Adding a Traffic Control Device"

- Section 5.37.5.3, “Deleting a Traffic Control Device”

Section 5.37.5.1
Viewing a List of Traffic Control Devices

To view a list of traffic control devices, type:

```
show running-config qos traffic-control advanced-configuration tcdevices
```

If devices have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config qos traffic-control advanced-configuration tcdevices
qos
 traffic-control
  advanced-configuration
   tcdevices te1-2-1c01ppp
    inbandwidth  1500
    in-unit      kilobits
    outbandwidth 1500
    out-unit     kilobits
   !
  !
 !
!
```

If no devices have been configured, add devices as needed. For more information, refer to Section 5.37.5.2, “Adding a Traffic Control Device”.

Section 5.37.5.2
Adding a Traffic Control Device

To add a new traffic control device, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the traffic control device by typing:

   ```
   qos traffic-control advanced-configuration tcdevices name
   ```

   Where:

   - *name* is the name of the interface to which traffic shaping will apply. Lowercase alphanumerical as well as '.' and '-' characters are allowed.
3. Configure the following parameter(s) as required:

Parameter	Description
{ interface }	An interface to which traffic shaping will apply. Lowercase alphanumerical as well as '.' and '-' characters are allowed.
inbandwidth { inbandwidth }	**Default:** 0 Incoming bandwidth. Default: 0 = ignore ingress. Defines the maximum traffic allowed for this interface in total. If the rate is exceeded, the packets are dropped.
in-unit { in-unit }	**Synopsis:** none, kilobits, megabits **Default:** none

Parameter	Description
	Unit for inbandwidth, per second.
outbandwidth { outbandwidth }	Maximum outgoing bandwidth... This is the maximum speed that can be handled. Additional packets will be dropped. This is the bandwidth that can be refrred-to as 'full' when defining classes.
out-unit { out-unit }	**Synopsis:** kilobits, megabits **Default:** megabits Unit for outgoing bandwidth, per second.
description { description }	A description for this configuration item.

4. Type **`commit`** and press **Enter** to save the changes, or type **`revert`** and press **Enter** to abort.

Section 5.37.5.3
Deleting a Traffic Control Device

To delete a traffic control device, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the traffic control device by typing:

```
no qos traffic-control advanced-configuration tcdevices name
```

Where:

- *`name`* is the name of the interface to which traffic shaping will apply.

3. Type **`commit`** and press **Enter** to save the changes, or type **`revert`** and press **Enter** to abort.

Section 5.37.6
Managing Traffic Control Rules

Traffic control rules define rules packet marking.

> **NOTE**
> *Traffic control rules can only be configured in advanced mode. For more information about setting the traffic control mode, refer to Section 5.37.1, “Enabling and Configuring Traffic Control”.*

The following sections describe how to configure and manage traffic control rules:

- Section 5.37.6.1, “Viewing a List of Traffic Control Rules”
- Section 5.37.6.2, “Adding a Traffic Control Rule”
- Section 5.37.6.3, “Configuring QoS Marking”
- Section 5.37.6.4, “Deleting aTraffic Control Rule”

Section 5.37.6.1
Viewing a List of Traffic Control Rules

To view a list of traffic control rules, type:

```
show running-config qos traffic-control advanced-configuration tcrules
```

If rules have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config qos traffic-control advanced-configuration tcrules
qos
 traffic-control
  advanced-configuration
   tcrules rule1
    mark-choice set
     mark 1
    !
    source       all
    destination  all
    protocol     tcp
    source-ports 80
   !
  !
 !
!
```

If no rules have been configured, add rules as needed. For more information, refer to Section 5.37.6.2, "Adding a Traffic Control Rule".

Section 5.37.6.2
Adding a Traffic Control Rule

To add a new traffic control rule, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the traffic control rule by typing:

```
qos traffic-control advanced-configuration tcrule name
```

Where:

- *name* is the name of the traffic control rule entry.

3. Configure the following parameter(s) as required:

Parameter	Description
{ name }	A distinct name for this rule.
source { source }	IF name, comma-separated list of hosts or IPs, MAC addresses, or 'all'. When using MAC addresses, use '~' as prefix and '-' as separator. Ex.: ~00-1a-6b-4a-72-34,~00-1a-6b-4a-71-42
destination { destination }	IF name, comma-separated list of hosts or IPs, or 'all'.
protocol { protocol }	**Synopsis:** tcp, udp, icmp, all **Default:** all The protocol to match.
destination-ports { destination-ports }	(Optional) A comma-separated list of port names, port numbers or port ranges.

Parameter	Description
source-ports { source-ports }	(Optional) A comma- separated list of port names, port numbers or port ranges.
test { test }	(Optional) Defines a test on the existing packet or connection mark. The default is a packet mark. For testing a connection mark, add ':C' at the end of the test value. Ex.: Test if the packet mark is not zero: **!0** Test if the connection mark is not zero: **!0:C**
length { length }	(Optional) Matches the length of a packet against a specific value or range of values... Greater than and lesser than, as well as ranges are supported in the form of min:max. Ex.: Equal to 64 **64** Greater or equal to 65 **65:** Lesser or equal to 65 **:65** In-between 64 and 768 **64:768**
tos { tos }	**Synopsis:** minimize-delay, maximize-throughput, maximize-reliability, minimize-cost, normal-service (Optional) Type of Service . A pre-defined ToS value or a numerical value. The numerical value is hexadecimal. Ex.: 0x38
description { description }	A description for this configuration item.

4. Type **`commit`** and press **Enter** to save the changes, or type **`revert`** and press **Enter** to abort.

Section 5.37.6.3

Configuring QoS Marking

Quality of Service (QoS) marking applies a mark to important data packets that should receive preferential treatment as they travel through the network. Only one QoS mark is allowed for each traffic control rule. Options include:

- **Set:** Determines whether the packet or the connection is assigned the QoS mark.
- **Modify:** Changes the QoS mark value using an AND or OR argument.
- **Save/Restore:** Replaces the connection's QoS mark value with an assigned value.
- **Continue:** If the packet matches, no more traffic control rules are checked and the packet is automatically forwarded to the specified chain.
- **DSCP Marking:** Determines whether the packet is assign the DSCP mark.

To configure the QoS mark for a traffic control rule, do the following:

Configuring a Set Mark

1. Make sure the CLI is in Configuration mode.
2. Select the Set option by typing:

```
qos traffic-control advanced-configuration tcrules name mark-choice set
```

   Where:

   - *name* is the name of the traffic control rule
3. Configure the following parameter(s):

NOTE

The `chain-options` parameter specifies the chain in which the rule will be processed.

- ***Pre-Routing - Mark the connection in the PREROUTING chain.***

  This can be used with DNAT, SNAT and Masquerading rules in the firewall. An example of such a rule is Source.IP:192.168.2.101, Chain-option: preroute or default, but the actual Source.NAT address is 2.2.2.2.

- ***Post-Routing - Mark the connection in the POSTROUTING chain.***

  This can be used with DNAT, SNAT and Masquerading rules in the firewall. An example of such rule is Destination.IP:192.168.3.101, Chain-option:preroute or default. In this case, the actual destination address is 192.168.3.101, but it will be translated to 192.168.3.33 by DNAT. Another example of a traffic control rule is Destination.IP:192.168.3.33, Chain-option:postrouting.

- ***Forward - Mark the connection in the FORWARD chain.***

  This is the default chain option and it can be used for normal IP traffic without any address or port translation.

Parameter	Description
object { object }	**Synopsis:** packet, connection **Default:** packet Sets the mark on either a packet or a connection.
mark { mark }	A mark that corresponds to a class mark (decimal value).
mask { mask }	(optional) A mask to determine which mark bits will be set.
chain-options { chain-options }	**Synopsis:** forward, postrouting, prerouting **Default:** forward A chain where the set operation will take place.

4. Type **`commit`** and press **Enter** to save the changes, or type **`revert`** and press **Enter** to abort.

Configuring a Modify Mark

1. Make sure the CLI is in Configuration mode.
2. Select the Modify option by typing:

```
qos traffic-control advanced-configuration tcrules name mark-choice modify
```

   Where:

   - *`name`* is the name of the traffic control rule

3. Configure the following parameter(s):

Parameter	Description
logic-op { logic-op }	**Synopsis:** and, or A logical operation to perform on the current mark: AND/OR.
mark-value { mark-value }	A mark to perform the operation with (decimal value).
modify-chain { modify-chain }	**Synopsis:** forward, postrouting, prerouting **Default:** forward A chain in which the operation will take place.

4. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Configuring a Save Mark

1. Make sure the CLI is in Configuration mode.
2. Configure the Save option by typing:

```
qos traffic-control advanced-configuration tcrules name mark-choice save
```

Where:

- *name* is the name of the traffic control rule

3. Configure the following parameter(s):

Parameter	Description
value-mask { value-mask }	Mask to process the mark with
op-chain { op-chain }	**Synopsis:** forward, prerouting **Default:** forward A chain in which the operation will take place.

4. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Configuring a Restore Mark

1. Make sure the CLI is in Configuration mode.
2. Select the Restore option by typing:

```
qos traffic-control advanced-configuration tcrules name mark-choice restore
```

Where:

- *name* is the name of the traffic control rule

3. Configure the following parameter(s):

Parameter	Description
value-mask { value-mask }	A mask to process the mark with.
op-chain { op-chain }	**Synopsis:** forward, prerouting **Default:** forward A chain in which the operation will take place.

4. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Configuring a Continue Mark

1. Make sure the CLI is in Configuration mode.
2. Select the Continue option by typing:

```
qos traffic-control advanced-configuration tcrules name mark-choice continue
```

Where:

- *name* is the name of the traffic control rule

3. Configure the following parameter(s):

Parameter	Description
continue-chain { continue-chain }	**Synopsis:** forward, prerouting **Default:** forward A chain in which the operation will take place.

4. Type **`commit`** and press **Enter** to save the changes, or type **`revert`** and press **Enter** to abort.

Configuring a DSCP Mark

1. Make sure the CLI is in Configuration mode.
2. Select the DSCP Marking option by typing:

```
qos traffic-control advanced-configuration tcrules name mark-choice dscpmarking
```

Where:

- *name* is the name of the traffic control rule

3. Configure the following parameter(s):

Parameter	Description
dscp-mark { dscp-mark }	**Synopsis:** BE, AF11, AF12, AF13, AF21, AF22, AF23, AF31, AF32, AF33, AF41, AF42, AF43, CS1, CS2, CS3, CS4, CS5, CS6, CS7, EF A DSCP class value chosen amongst the given list.
dscpchain { dscpchain }	**Synopsis:** forward, postrouting, prerouting **Default:** forward A chain where the DSCP marking will take place.

4. Type **`commit`** and press **Enter** to save the changes, or type **`revert`** and press **Enter** to abort.

Section 5.37.6.4

Deleting aTraffic Control Rule

To delete a traffic control rule, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the traffic control rule by typing:

```
no qos traffic-control advanced-configuration tcrule name
```

Where:

- *name* is the name of the traffic control rule entry

3. Type **`commit`** and press **Enter** to save the changes, or type **`revert`** and press **Enter** to abort.

Section 5.37.7

Managing QoS Mapping for VLANs

Quality of Service (QoS) mapping is used to map QoS traffic. It assigns a traffic control mark to incoming IP traffic based on the priority value of a tagged frame. The incoming traffic is then classified and placed in the priority queues according to the traffic control rules specified for the marked rule. In addition, traffic control can assign the same priority or a different priority value when a frame needs to be egressed with a VLAN tag through a traffic control interface.

QoS maps can be configured for VLAN connections on routable Ethernet ports and virtual switches.

The following sections describe how to configure and manage QoS maps for VLAN connections:

- Section 5.37.7.1, “Viewing a List of QoS Maps”
- Section 5.37.7.2, “Adding a QoS Map”
- Section 5.37.7.3, “Deleting a QoS Map”

Section 5.37.7.1

Viewing a List of QoS Maps

To view a list of QoS maps for a VLAN connection, type:

```
show running-config interface [eth | virtualswtich] slot port vlan id qosmap
```

Where:

- *slot* is the name of the module location
- *port* is the port number (or a list of ports, if aggregated in a port trunk) for the module
- *id* is the ID given to the VLAN

If QoS maps have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config interface virtualswitch vlan 100 qosmap
interface
 virtualswitch 1
  vlan 100
   qosmap 2
    ingress 10
   !
  !
 !
!
```

If no QoS maps have been configured, add maps as needed. For more information, refer to Section 5.37.7.2, “Adding a QoS Map”.

Section 5.37.7.2

Adding a QoS Map

To add a QoS map for a VLAN connection, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the QoS map by typing:

   Ethernet and Virtual Switch Interfaces

   ```
   interface [eth | virtualswtich] slot port vlan id qosmap priority
   ```

   Where:

   - *slot* is the name of the module location
   - *port* is the port number (or a list of ports, if aggregated in a port trunk) for the module

- *id* is the ID given to the VLAN
- *priority* is the priority assigned to the QoS map

WAN Interfaces

```
wan interface protocol channel number connection hdlc-eth vlan id qosmap priority
```

Where:

- *interface* is the WAN interface
- *protocol* is either T1 or E1
- *number* is the channel number
- *id* is the ID of the VLAN
- *priority* is the priority assigned to the QoS map

3. Configure the following parameter(s) as required:

Parameter	Description
ingress { ingress }	Map the ingress to a mark.

4. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.37.7.3

Deleting a QoS Map

To delete a QoS map for a VLAN connection, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the QoS map for the VLAN connection by typing:

```
no interface [eth | virtualswtich] vlan slot port qosmap priority
```

Where:

- *slot* is the name of the module location
- *port* is the port number (or a list of ports, if aggregated in a port trunk) for the module
- *priority* is the priority assigned to the QoS map

3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.37.8

Managing Egress Markers for QoS Maps

Egress markers for QoS maps are used to assign priority to traffic that shares the same mark as one of the egress marks configured for the device.

The following sections describe how to configure and manage egress markers for QoS maps:

- Section 5.37.8.1, “Viewing a List of Egress Marks”
- Section 5.37.8.2, “Adding an Egress Mark”
- Section 5.37.8.3, “Deleting an Egress Mark”

Section 5.37.8.1
Viewing a List of Egress Marks

To view a list of egress marks for a QoS map, type:

```
show running-config interface [eth | virtualswtich] slot port vlan id qosmap priority egress
```

Where:

- *slot* is the name of the module location
- *port* is the port number (or a list of ports, if aggregated in a port trunk) for the module
- *id* is the ID given to the VLAN
- *priority* is the priority assigned to the QoS map

If egress marks have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config interface eth cm 1 vlan 2 qosmap 1 egress
interface
 eth cm 1
  vlan 2
   qosmap 1
    egress 10
    !
    egress 11
    !
   !
  !
 !
!
```

If no egress marks have been configured, add egress marks as needed. For more information, refer to Section 5.37.8.2, “Adding an Egress Mark”.

Section 5.37.8.2
Adding an Egress Mark

To add an egress mark for a QoS Map, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the QoS map by typing:

   ```
   interface [eth | virtualswtich] slot port vlan id qosmap priority egress mark
   ```

   Where:

   - *slot* is the name of the module location
   - *port* is the port number (or a list of ports, if aggregated in a port trunk) for the module
   - *id* is the ID given to the VLAN
   - *priority* is the priority assigned to the QoS map
   - *mark* is the value of the egress mark
3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.37.8.3

Deleting an Egress Mark

To delete an egress mark for a QoS map, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the QoS map for the VLAN connection by typing:

```
no interface [eth | virtualswtich] slot port vlan id qosmap priority egress mark
```

   Where:

   - *slot* is the name of the module location
   - *port* is the port number (or a list of ports, if aggregated in a port trunk) for the module
   - *id* is the ID given to the VLAN
   - *priority* is the priority assigned to the QoS map
   - *mark* is the value of the egress mark

3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.37.9

Viewing QoS Statistics

ROX II provides statistics for traffic going through each class that has been configured. Packets are assigned to classes on the outbound interface based on rules. If a packet matches the specified criteria, it is considered to be a member of the class and is forwarded to that class. If the packet does not match any rule, it is forwarded to the default class.

For more information about traffic control classes, refer to Section 5.37.4, “Managing Traffic Control Classes”.

NOTE
Statistics are only available when traffic control is enabled in advanced mode. For more information about enabling traffic control, refer to Section 5.37.1, “Enabling and Configuring Traffic Control”.

To view the QoS statistics, type:

```
show qos statistics
```

A table or list similar to the following example appears:

```
ruggedcom# show qos statistics | tab
           MIN        MAX
CLASSNAME  BANDWIDTH  BANDWIDTH  SENTBYTES  SENTPACKETS  DROPPEDPACKETS  RATE       AVERAGE
--------------------------------------------------------------------------------------------
High       1200Kbit   1500Kbit   4956594    9953         0               446104bit  112pps
Default    300000bit  1500Kbit   3029832    6084         3869            270088bit  68pps
```

This table provides the following information:

Parameter	Description
classname	
min-bandwidth	The minimum guaranteed bandwidth. This is based on the device's defined characteristics.
max-bandwidth	The maximum guaranteed bandwidth in absence of any higher prioritized traffic. This is based on the device's defined characteristics.

Parameter	Description
sentbytes	The number of bytes that were sent through this class.
sentpackets	The number of packets that were sent through this class.
droppedpackets	The number of packets that were dropped in this class.
rate	Based on a 10-second average.
average	Based on a 10-second average.

Section 5.38

Managing IP Addresses for Routable Interfaces

The following sections describe how to configure and manage IP addresses for routable interfaces:

- Section 5.38.1, “Configuring Costing for Routable Interfaces”
- Section 5.38.2, “Viewing Statistics for Routable Interfaces”
- Section 5.38.3, “Managing IPv4 Addresses”
- Section 5.38.4, “Configuring IPv6 Neighbor Discovery”
- Section 5.38.5, “Managing IPv6 Network Prefixes”
- Section 5.38.6, “Managing IPv6 Addresses”

Section 5.38.1

Configuring Costing for Routable Interfaces

To configure the costing for a routable interface, do the following:

1. Make sure the CLI is in Configuration mode.
2. Set the costing by typing:

   ```
   ip interface bandwidth cost
   ```

   Where:

   - *interface* is the name of the routable interface
   - *cost* is the value used in auto-cost calculations for the routable logical interface in kbps
3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.38.2

Viewing Statistics for Routable Interfaces

To view statistics for all routable interfaces, type:

```
show interfaces ip
```

A table or list similar to the following appears:

```
ruggedcom# show interfaces ip
interfaces ip dummy0
 admin state down
 state       down
 pointopoint false
 receive
  bytes   0
  packets 0
  errors  0
  dropped 0
 transmit
  bytes      0
  packets    0
  errors     0
  dropped    0
  collisions 0
interfaces ip fe-cm-1
.
.
.
```

This table or list displays the following information:

Parameter	Description
admin-state	**Synopsis:** up, down, testing, unknown, dormant, notPresent, lowerLayerDown The port's administrative status.
state	**Synopsis:** up, down, testing, unknown, dormant, notPresent, lowerLayerDown Shows whether the link is up or down.
pointopoint	The point-to-point link.
bytes	The number of bytes received.
packets	The number of packets received.
errors	The number of error packets received.
dropped	The number of packets dropped by the receiving device.
bytes	The number of bytes transmitted.
packets	The number of packets transmitted.
errors	The number of error packets transmitted.
dropped	The number of packets dropped by the transmitting device.
collisions	The number of collisions detected on the port.

Section 5.38.3
Managing IPv4 Addresses

The following sections describe how to configure and manage IPv4 addresses:

- Section 5.38.3.1, “Viewing a List of IPv4 Addresses”
- Section 5.38.3.2, “Adding an IPv4 Address”
- Section 5.38.3.3, “Deleting an IPv4 Address”

Section 5.38.3.1
Viewing a List of IPv4 Addresses

To view a list of IPv4 address for a routable interface, type:

```
show running-config ip interface ipv4
```

Where:

- *interface* is the name of the interface

If addresses have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config ip ipv4 | tab
IFNAME        IPADDRESS         PEER
-------------------------------------
dummy0
              1.1.1.1/32        -
fe-cm-1
              192.168.0.12/24   -
              172.30.150.12/19  -
switch.0001
switch.0011
              192.168.11.1/24   -
switch.0012
              192.168.12.1/24   -
switch.0014
              192.168.14.1/24   -
```

If no addresses have been configured, add addresses as needed. For more information, refer to Section 5.38.3.2, "Adding an IPv4 Address".

Section 5.38.3.2
Adding an IPv4 Address

To add an IPv4 address to a routable interface, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the address by typing:

   ```
   ip interface ipv4 address address
   ```

   Where:

   - *interface* is the name of the interface
   - *address* is the IPv4 address
3. Configure the following parameter(s) as required:

Parameter	Description
peer { peer }	The peer IPv4 Address (xxx.xxx.xxx.xxx, PPP, MLPPP, FrameRelay link only).

4. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.38.3.3

Deleting an IPv4 Address

To delete an IPv4 address for a routable interface, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the address by typing:

   ```
   no ip interface ipv4 address address
   ```

   Where:

   - *address* is the IPv4 address
3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.38.4

Configuring IPv6 Neighbor Discovery

The Neighbor Discovery (ND) protocol in IPv6 is a replacement for IPv4 ARP messages. The protocol uses ICMPv6 messages with for various purposes including:

- Find a link-layer address of a neighbor
- Discover neighbor routers
- Determine any change in the link-layer address
- Determine when a neighbor is down
- Send network information from routers to hosts, which includes hop limit, MTU size, determining the network prefix used on a link, address auto configuration, and the default route information

The Neighbor Discovery protocol uses five types of ICMPv6 messages:

- **Router Solicitation (ICMPv6 type 133)**

  This message is sent by hosts to routers as a request to router advertisement message. It uses a destination multicast address (i.e. FF02::2).
- **Router Advertisement Messages (ICMPv6 type 134)**

  This message is used by routers to announce its presence in a network. The message includes network information related to IPv6 prefixes, default route, MTU size, hop limit and auto configuration flag. It uses a destination multicast address (i.e. FF02::1).
- **Neighbor Solicitation Messages (ICMPv6 type 135)**

  This message is sent by hosts to determine the existence of another host on the same. The goal is to find the link-layer of neighbor nodes on the same link.
- **Neighbor Advertisement Messages (ICMPv6 type 136)**

  This message is sent by hosts to indicate the existence of the host and it provides information about its own link-layer address.
- **Redirect Messages (ICMPv6 type 137)**

  This message is sent by a router to inform a host about a better router to reach a particular destination address.

Neighbor Discovery should be configured on all Ethernet interfaces enabled for IPv6.

To enable and configure settings for IPv6 Neighbor Discovery, do the following:

1. Make sure the CLI is in Configuration mode.
2. Type the following command:

```
ip interface ipv6 nd
```

Where:

- *interface* is the name of the interface

3. Configure the following parameter(s) as required:

Parameter	Description
enable-ra	Enable to send router advertisement messages.
adv-interval-option	Includes an Advertisement Interval option which indicates to hosts the maximum time in milliseconds, between successive unsolicited router advertisements.
home-agent-config-flag	Sets/unsets the flag in IPv6 router advertisements which indicates to hosts that the router acts as a home agent and includes a home agent option.
home-agent-lifetime { home-agent-lifetime }	**Default:** 1800 The value to be placed in the home agent option, when the home agent configuration flag is set, which indicates the home agent lifetime to hosts. A value of 0 means to place a router lifetime value.
home-agent-preference { home-agent-preference }	**Default:** 0 The value to be placed in the home agent option, when the home agent configuration flag is set, which indicates the home agent preference to hosts.
managed-config-flag	The flag in IPv6 router advertisements, which indicates to hosts that they should use the managed (stateful) protocol for addresses autoconfiguraiton in addition to any addresses autoconfigured using stateless address autoconfiguration.
other-config-flag	The flag in IPv6 router advertisements, which indicates to hosts that they should use the administered (stateful) protocol to obtain autoconfiguration information other than addresses.
ra-lifetime { ra-lifetime }	**Default:** 1800 The value (in seconds) to be placed in the Router Lifetime field of router advertisements sent from the interface. Indicates the usefulness of the router as a default router on this interface. Setting the value to zero indicates that the router should not be considered a default router on this interface. It must be either zero or between the value specified with the IPv6 nd ra-interval (or default) and 9000 seconds.
reachable-time-msec { reachable-time-msec }	**Default:** 0 The value (in milliseconds) to be placed in the Reachable Time field in the router advertisement messages sent by the router. The configured time enables the router to detect unavailable neightbors. The value zero means unspecified (by this router).

4. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.38.5

Managing IPv6 Network Prefixes

An IPv6-capable interface can use Neighbor Discovery to advertise IPv6 network prefixes to its neighbor on the same link.

The following sections describe how to configure and manage IPv6 network prefixes:

- Section 5.38.5.1, “Adding an IPv6 Network Prefix”

• Section 5.38.5.2, “Deleting an IPv6 Network Prefix”

Section 5.38.5.1
Adding an IPv6 Network Prefix

To add a network prefix to the neightbor discovery configuration for an IPv6 address, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the network prefix by typing:

```
ip interface ipv6 nd prefix prefix
```

Where:

- *interface* is the name of the interface
- *prefix* is the IPv6 address and prefix

3. Configure the lifetime settings by configuring the following parameter(s):

Parameter	Description
valid { valid }	**Synopsis:** infinite The length of time in seconds during which time the prefix is valid for the purpose of on-link determination. **Prerequisite:** The valid lifetime cannot be configured unless the preferred lifetime is configured.
preferred { preferred }	**Synopsis:** infinite The length of time in seconds during which addresses generated from the prefix remain preferred. **Prerequisite:** The preferred lifetime cannot be configured unless the valid lifetime is configured.

4. Configure the prefix settings by configuring the following parameter(s):

Parameter	Description
off-link	Indicates that advertisement makes no statement about on-link or off-link properties of the prefix.
no-autoconfig	Indicates to hosts on the local link that the specified prefix cannot be used for IPv6 autoconfiguration.
router-address	Indicates to hosts on the local link that the specified prefix contains a complete IP address by setting the R flag. **Prerequisite:** The router address can not be set unless off-link or no-autoconfig are set.

5. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.38.5.2
Deleting an IPv6 Network Prefix

To delete a network prefix to the neighbor discovery configuration for an IPv6 address, do the following:

1. Make sure the CLI is in Configuration mode.

2. Delete the address by typing:

```
no ip interface ipv6 address address
```

Where:

- *interface* is the name of the interface
- *address* is the IPv6 address

3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.38.6

Managing IPv6 Addresses

The following sections describe how to configure and manage IPv6 addresses:

- Section 5.38.6.1, “Viewing a List of IPv6 Addresses”
- Section 5.38.6.2, “Adding an IPv6 Address”
- Section 5.38.6.3, “Deleting an IPv6 Address”

Section 5.38.6.1

Viewing a List of IPv6 Addresses

To view a list of IPv6 address for a routable interface, type:

```
show running-config ip interface ipv6 address
```

Where:

- *interface* is the name of the interface

If addresses have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config ip dummy0 ipv6 address
ip dummy0
 ipv6
  address FDD1:9AEF:3DE4::2/24
  !
  address FDD2:8AEF:4DE4::2/24
  !
 !
!
```

If no addresses have been configured, add addresses as needed. For more information, refer to Section 5.38.6.2, “Adding an IPv6 Address”.

Section 5.38.6.2

Adding an IPv6 Address

To add an IPv6 address to a routable interface, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add the address by typing:

```
ip interface ipv6 address address
```

Where:

- *interface* is the name of the interface
- *address* is the IPv6 address

3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.38.6.3
Deleting an IPv6 Address

To delete an IPv6 address for a routable interface, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete the address by typing:

```
no ip interface ipv6 address address
```

Where:

- *interface* is the name of the interface
- *address* is the IPv6 address

3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.39
Managing MPLS

MPLS stands for Multi-Protocol Label Switching. MPLS operates between layer 2 and layer 3 of the OSI (Open Systems Interconnection) model and it provides a mechanism to carry traffic for any network layer protocols. MPLS makes forwarding decision based on labels where the labels are mapped to destination IP networks. MPLS traffic flows are connection-oriented, as it operates on a pre-configured LSPs (Label Switch Paths) that is built based on the dynamic Label Distribution Protocol (LDP) or through static label bindings.

The following sections describe how to configure and manage MPLS:

- Section 5.39.1, “Viewing the Status of IP Binding”
- Section 5.39.2, “Viewing the Status of the Forwarding Table”
- Section 5.39.3, “Enabling/Disabling MPLS Routing”
- Section 5.39.4, “Managing the MPLS Interfaces”
- Section 5.39.5, “Managing Static Label Binding”
- Section 5.39.6, “Managing Static Cross-Connects”
- Section 5.39.7, “Managing LDP”

Section 5.39.1

Viewing the Status of IP Binding

To view the status of the IP binding on the device, type:

```
show mpls status ip-binding
```

If IP binding has been configured, a table similar to the following example appears:

```
ruggedcom# show mpls status ip-binding
                  LOCAL                  REMOTE
PREFIX            LABEL     NEXT HOP      LABEL
----------------------------------------------------
1.1.1.1/32        17        192.168.10.1  imp-null
2.2.2.2/32        18        192.168.10.1  imp-null
3.3.3.3/32        imp-null
4.4.4.4/32        imp-null
5.5.5.5/32        19        192.168.20.2  imp-null
6.6.6.6/32        20        192.168.20.2  imp-null
10.200.16.0/20    16
172.30.128.0/19   imp-null
192.168.10.0/24   imp-null
192.168.20.0/24   imp-null
192.168.100.0/24  21        192.168.10.1  imp-null
192.168.200.0/24  22        192.168.20.2  imp-null
```

This table provides the following information:

Parameter	Description
prefix	The destination address prefix.
local-label	The incoming (local) label.
next-hop	The destination next hop router.
remote-label	The remote label

Section 5.39.2

Viewing the Status of the Forwarding Table

To view the status of the forwarding table on the device, type:

```
show mpls status forwarding-table
```

A table or list similar to the following example appears:

```
ruggedcom# show mpls status forwarding-table
LOCAL  OUTGOING                    OUTGOING
LABEL  LABEL     PREFIX            INTERFACE    NEXT HOP      UPTIME
-------------------------------------------------------------------------
17     Pop       1.1.1.1/32        switch.0010  192.168.10.1  01:04:31
18     Pop       2.2.2.2/32        switch.0010  192.168.10.1  01:04:31
19     Pop       5.5.5.5/32        switch.0020  192.168.20.2  01:04:33
20     Pop       6.6.6.6/32        switch.0020  192.168.20.2  01:04:33
21     Pop       192.168.100.0/24  switch.0010  192.168.10.1  01:04:31
22     Pop       192.168.200.0/24  switch.0020  192.168.20.2  01:04:33
```

This table or list provides the following information:

Parameter	Description
local-label	The incoming (local) label
outgoing-label	The outgoing (remote) label.
prefix	The destination address prefix.
outgoing-interface	The outgoing interface.
next-hop	The destination next hop router.
uptime	The time this entry has been up.

Section 5.39.3
Enabling/Disabling MPLS Routing

To enable MPLS routing, do the following:

1. Make sure the CLI is in Configuration mode.
2. Enable or disable MPLS by typing the following commands:

   Enable

   ```
   mpls enable
   ```

   Disable

   ```
   no mpls enable
   ```

3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.39.4
Managing the MPLS Interfaces

The following sections describe how to manage the MPLS interfaces:

- Section 5.39.4.1, “Viewing the Status of MPLS Interfaces”
- Section 5.39.4.2, “Viewing a List of MPLS Interfaces”
- Section 5.39.4.3, “Enabling/Disabling an MPLS Interface”

Section 5.39.4.1
Viewing the Status of MPLS Interfaces

To view the status of the MPLS interfaces on the device, type:

```
show mpls status interfaces
```

If MPLS interfaces have been enabled on the device, a table similar to the following example appears:

```
show mpls status interfaces
MPLS
INTERFACES   STATUS
---------------------
```

```
switch.0010  yes
switch.0020  yes
```

This table provides the following information:

Parameter	Description
mpls-interfaces	The interface that has been enabled for MPLS.
status	The operational status.

If no MPLS interface has been enabled, enable interfaces as needed. For more information about enabling MPLS interfaces, refer to Section 5.39.4.3, “Enabling/Disabling an MPLS Interface”.

Section 5.39.4.2
Viewing a List of MPLS Interfaces

To view a list of MPLS interfaces, type:

```
show running-config mpls interface-mpls
```

If interfaces have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config mpls interface-mpls | tab
IFNAME     ENABLED
----------------------
fe-cm-1     false
switch.0001  false
switch.0010  true
switch.0020  false

!
```

Where:

- *IFNAME* is the name of the interface
- *ENABLED* refers to the status of the MPLS operation on the interface

If no MPLS interfaces have been configured, enable interfaces as needed. For more information about enabling MPLS interfaces, refer to Section 5.39.4.3, “Enabling/Disabling an MPLS Interface”.

Section 5.39.4.3
Enabling/Disabling an MPLS Interface

To enable or disable an MPLS interface, do the following:

1. Make sure the CLI is in Configuration mode.
2. Enable or disable MPLS interfaces by typing the following commands:

   Enable

   ```
   mpls interface-mpls interface enable
   ```

   Disable

   ```
   no mpls interface-mpls interface enable
   ```

   Where:

- *interface* is the name of the interface

3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.39.5

Managing Static Label Binding

The following sections describe how to configure and manage static label binding for MPLS:

- Section 5.39.5.1, "Viewing the Status of Static Label Binding"
- Section 5.39.5.2, "Viewing a List of Static Labels"
- Section 5.39.5.3, "Adding a Static Label"
- Section 5.39.5.4, "Deleting a Static Label"

Section 5.39.5.1

Viewing the Status of Static Label Binding

To view the status of all configured static label binding, type:

```
show mpls status static-binding
```

If static label binding has been configured, a table similar to the following example appears:

```
ruggedcom# show mpls status static-binding
                    IN      OUT
IP ADDRESS          LABEL   LABEL   NEXTHOP
----------------------------------------------
192.168.20.0/24     90      101     192.168.10.2
192.168.200.0/24    95      100     192.168.10.2
```

This table provides the following information:

Parameter	Description
ip-address	The destination address prefix.
in-label	The incoming (local) label.
out-label	The outgoing (remote) label.
nexthop	The destination next hop router.

If no static label binding has been configured, configure binding as needed. For more information about configuring static-binding, refer to Section 5.39.5.3, "Adding a Static Label".

Section 5.39.5.2

Viewing a List of Static Labels

To view a list of static labels, type:

```
show running-config mpls static-mpls binding [ipv4 | ipv6]
```

If static labels have been configured, a list similar to the following example appears:

```
ruggedcom# show running-config mpls static-mpls binding ipv4
mpls
 static-mpls
  binding
   ipv4
    dest-address 192.168.52.52/32
     next-hop  192.168.10.2
     out-label 16
    !
   !
  !
 !
!
```

If no static labels have been configured, add labels as needed. For more information about adding static labels, refer to Section 5.39.5.3, “Adding a Static Label”.

Section 5.39.5.3
Adding a Static Label

To add a static label, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add a static label by typing:

```
mpls static-mpls binding [ipv4 | ipv6] dest-address address
```

   Where:

   - *address* is the destination address and prefix.
3. Configure the following parameter(s) as required:

Parameter	Description
in-label { in-label }	The incoming label: integer 16 -> 1048575.
next-hop { next-hop }	The IP address for the destination next-hop router. **Prerequisite:** The destination out-label must also be defined.
out-label { out-label }	**Synopsis:** explicit-null, implicit-null, The outgoing label: 'explicit-null', 'implicit-null' or integer 16 -> 1048575. **Prerequisite:** The destination next-hop must also be defined.

4. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.39.5.4
Deleting a Static Label

To delete a static label, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete a static label by typing:

```
no mpls static-mpls binding [ipv4 | ipv6] dest-address address
```

Where:

- *address* is the destination address and prefix.

3. Configure the following parameter(s) as required:

Parameter	Description
in-label { in-label }	The incoming label: integer 16 -> 1048575.
next-hop { next-hop }	The IP address for the destination next-hop router. **Prerequisite:** The destination out-label must also be defined.
out-label { out-label }	**Synopsis:** explicit-null, implicit-null, The outgoing label: 'explicit-null', 'implicit-null' or integer 16 -> 1048575. **Prerequisite:** The destination next-hop must also be defined.

4. Type **`commit`** and press **Enter** to save the changes, or type **`revert`** and press **Enter** to abort.

Section 5.39.6

Managing Static Cross-Connects

The following sections describe how to configure and manage static cross-connects for MPLS:

- Section 5.39.6.1, "Viewing the Status of Static Cross-Connects"
- Section 5.39.6.2, "Viewing a List of Static Cross-Connects"
- Section 5.39.6.3, "Adding a Static Cross-Connect"
- Section 5.39.6.4, "Deleting a Static Cross-Connect"

Section 5.39.6.1

Viewing the Status of Static Cross-Connects

To view the status of all configured static cross-connects, type:

```
show mpls status static-crossconnect
```

If static cross-connects have been configured, a table similar to the following example appears:

```
ruggedcom# show mpls status static-crossconnect
LOCAL  OUTGOING  OUTGOING
LABEL  LABEL     INTERFACE    NEXT HOP
--------------------------------------------
200    205       switch.0010  192.168.10.2
215    250       switch.0010  192.168.10.2
```

This table provides the following information:

Parameter	Description
local-label	The incoming (local) label.
outgoing-label	The outgoing (remote) label.
outgoing-interface	The outgoing interface.

Parameter	Description
next-hop	The destination next hop router.

If no static cross-connects have been configured, add cross-connects as needed. For more information about adding static cross-connects, refer to Section 5.39.6.3, “Adding a Static Cross-Connect”.

Section 5.39.6.2
Viewing a List of Static Cross-Connects

To view a list of configured static cross-connects, type:

```
show running-config mpls static-mpls crossconnects
```

If static cross-connects have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config mpls static-mpls crossconnect | tab
       OUT                        OUT
LABEL  INTERFACE     NEXT HOP      LABEL
-----------------------------------------
20     switch.0001  192.168.10.2  32

 !
!
```

If no static cross-connects have been configured, add cross-connects as needed. For more information about adding static cross-connects, refer to Section 5.39.6.3, “Adding a Static Cross-Connect”.

Section 5.39.6.3
Adding a Static Cross-Connect

To add a static cross-connect, do the following:

1. Make sure the CLI is in Configuration mode.
2. Add a static cross-connect by typing:

```
mpls static-mpls crossconnect in-label in-label
```

   Where:

   - *in-label* is the incoming label
3. Configure the following parameter(s) as required:

Parameter	Description
out-interface { out-interface }	The outgoing interface.
next-hop { next-hop }	**Synopsis:** The ip-address type represents an IP address and is IP version neutral. The format of the textual representations implies the IP version. The destination next-hop router (IPv4 or IPv6 format).
out-label { out-label }	**Synopsis:** explicit-null, implicit-null, The outgoing label: 'explicit-null', 'implicit-null' or integer 16 -> 1048575.

4. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.39.6.4

Deleting a Static Cross-Connect

To delete a static cross-connect, do the following:

1. Make sure the CLI is in Configuration mode.
2. Delete a static cross-connect by typing:

```
no mpls static-mpls crossconnect in-label in-label
```

   Where:

   - *in-label* is the incoming label

3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

Section 5.39.7

Managing LDP

LDP (Label Distribution Protocol), defined by RFC 5036 [http://tools.ietf.org/html/rfc5036], is a method of hop-by-hop forwarding to determine the destination of packets without sending them up to the network layer (layer 3). When a router receives a packet, it looks up the incoming label in its forwarding table and then forwards the packet to the next hop destination. This is opposed to looking up the IP header information in a packet, as in IP forwarding.

LDP works by enabling Label Switch Routers (LSRs) to discover and bind labels to their neighbors within the MPLS network. The LSRs then identify their peers and exchange their label information with one another. Label information is stored in Label Information Base (LIB) and Label Forwarding Information Base (LFIB) tables.

The following sections describe how to configure and manage LDP:

- Section 5.39.7.1, “Viewing the Status of LDP Binding”
- Section 5.39.7.2, “Viewing the Status of the LDP Discovery Interfaces”
- Section 5.39.7.3, “Viewing the Status of the LDP Neighbor Local Node Information”
- Section 5.39.7.4, “Viewing the Status of the LDP Neighbor Connection Information”
- Section 5.39.7.5, “Viewing the Status of the LDP Neighbor Discovery Information”
- Section 5.39.7.6, “Configuring LDP”
- Section 5.39.7.7, “Configuring Neighbor Discovery”
- Section 5.39.7.8, “Viewing a List of LDP Interfaces”
- Section 5.39.7.9, “Enabling/Disabling an LDP Interface”

Section 5.39.7.1

Viewing the Status of LDP Binding

To view the status of the LDP binding on the device, type:

```
show mpls ldp status binding
```

A table or list similar to the following example appears:

```
ruggedcom# show mpls ldp status binding
               LOCAL     NEXT     REMOTE
```

```
PREFIX          LABEL      HOP       LABEL      IN USE
----------------------------------------------------
1.1.1.1         17         2.2.2.2   imp-null   in-use
1.1.1.1         17         6.6.6.6   17
2.2.2.2         18         2.2.2.2   imp-null   in-use
2.2.2.2         18         6.6.6.6   18
3.3.3.3         imp-null
4.4.4.4         imp-null
5.5.5.5         19         2.2.2.2   19
5.5.5.5         19         6.6.6.6   imp-null   in-use
```

This table or list provides the following information:

Parameter	Description
prefix	The LDP transport prefix.
local-label	The incoming (local) label.
next-hop	The destination next hop router.
remote-label	The LDP remote label.
in-use	The LDP in-use flag.

Section 5.39.7.2

Viewing the Status of the LDP Discovery Interfaces

To view the status of the LDP discovery interfaces on the device, type:

```
show mpls ldp status discovery
```

If LDP discovery interfaces have been configured, a table similar to the following example appears:

```
ruggedcom# show mpls ldp status discovery
status discovery
 local id 4.4.4.4
 interfaces
INTERFACE     SRC IP ADDR    PEER ID   PEER IP       STATE
-------------------------------------------------------
switch.0010   192.168.10.2   2.2.2.2   192.168.10.1  OPER
switch.0020   192.168.20.1   6.6.6.6   192.168.20.2  OPER
```

This table provides the following information:

Parameter	Description
interface	The LDP discovery interface.
src-ip-addr	The LDP discovery source IP address.
peer-id	The LDP discovery peer ID.
peer-ip	LDP discovery peer IP address
state	The LDP discovery interface state.

For more information about configuring LDP discovery interfaces, refer to Section 5.39.7.9, “Enabling/Disabling an LDP Interface”.

Section 5.39.7.3

Viewing the Status of the LDP Neighbor Local Node Information

To view the status of the local node(s) for the LDP neighbor on the device, type:

```
show mpls ldp status neighbor local-node-information
```

A table or list similar to the following example appears:

```
ruggedcom# show mpls ldp status neighbor local-node-information
                   KEEPALIVE
LDP ID   HOLDTIME  INTERVAL
------------------------------
4.4.4.4   15s       180s
```

This table or list provides the following information:

Parameter	Description
ldp-id	The LDP ID of the LDP neighbor local node.
holdtime	LDP holdtime of the neighbor local node.
keepalive-interval	The keepalive interval of the LDP neighbor local node.

Section 5.39.7.4

Viewing the Status of the LDP Neighbor Connection Information

To view the status of the LDP neighbor connection on the device, type:

```
show mpls ldp status neighbor connection-information
```

A table similar to the following example appears:

```
ruggedcom# show mpls ldp status neighbor connection-information
         TCP
PEER ID  CONNECTION    STATE  UPTIME
----------------------------------------
2.2.2.2  192.168.10.1  OPER   00:51:51
-        192.168.10.2
6.6.6.6  192.168.20.2  OPER   00:51:53
-        192.168.20.1
```

Parameter	Description
peer-id	The peer ID of the LDP neighbor connection.
tcp-connection	The TCP connection of the LDP neighbor connection.
state	The state of the LDP neighbor connection.
uptime	The up time of the LDP neighbor connection.

This table provides the following information:

Parameter	Description
peer-id	The peer ID of the LDP neighbor connection.
tcp-connection	The TCP connection of the LDP neighbor connection.

Parameter	Description
state	The state of the LDP neighbor connection.
uptime	The up time of the LDP neighbor connection.

Section 5.39.7.5

Viewing the Status of the LDP Neighbor Discovery Information

To view the status of the LDP neighbor discovery information on the device, type:

```
show mpls ldp status neighbor discovery-information
```

A table or list similar to the following example appears:

```
ruggedcom# show mpls ldp status neighbor discovery-information
                                                          P
                                                P         KEEPALIVE
PEER ID  PEER IP       INTERFACE    LOCAL IP      HOLDTIME  INTERVAL
---------------------------------------------------------------------------
2.2.2.2  192.168.10.1  switch.0010  192.168.10.2  15s       180s
6.6.6.6  192.168.20.2  switch.0020  192.168.20.1  15s       180s
```

This table or list provides the following information:

Parameter	Description
peer-id	The peer ID of the LDP neighbor discovery.
peer-ip	The peer ID of the LDP neighbor discovery.
interface	The local IP address of the LDP neighbor discovery.
local-ip	LDP neighbor discovery state.
p-holdtime	The peer holdtime of the LDP neighbor discovery.
p-keepalive-interval	The peer keepalive interval of the LDP neighbor discovery.

Section 5.39.7.6

Configuring LDP

To configure the LDP, do the following:

1. Make sure the CLI is in Configuration mode.
2. Enable or disable the LDP by typing the following commands:

   Enable

   ```
   mpls ldp enable
   ```

   Disable

   ```
   no mpls ldp enable
   ```

3. Configure the following parameter(s) as required:

Parameter	Description
enabled	**Default:** false A boolean flag to indicate that Label Distribution Protocol (LDP) is enabled. **Prerequisite:** MPLS must be enabled before enabling LDP. **Prerequisite:** MPLS static bindings must be removed before enabling LDP.
holdtime { holdtime }	**Default:** 180 The time (in seconds) for which a Label Distribution Protocol (LDP) session is maintained in the absence of LDP messages from the session peer.

Section 5.39.7.7
Configuring Neighbor Discovery

To configure the LDP neighbor discovery, do the following:

1. Make sure the CLI is in Configuration mode.
2. To configure the LDP Neighbor Discovery, type the following command:

```
mpls ldp discovery
```

3. Configure the following parameter(s) as required:

Parameter	Description
interval { interval }	**Default:** 5 The time (in seconds) between the sending of consecutive Hello messages.
holdtime { holdtime }	**Default:** 15 The time (in seconds) that a discovered LDP neighbor is remembered without receipt of an LDP Hello message from the neighbor.

Section 5.39.7.8
Viewing a List of LDP Interfaces

To view a list of LDP interfaces, type:

```
show running-config mpls ldp interface-ldp
```

If interfaces have been configured, a table or list similar to the following example appears:

```
ruggedcom# show running-config mpls ldp interface-ldp | tab
TRANSPORT             TRANSPORT IP
IFNAME       ENABLED  ADDRESS
------------------------------------
fe-cm-1      false    -
switch.0001  false    -
switch.0010  true     192.168.10.1
switch.0020  false    -

 !
!
```

For more information about enabling LDP interfaces, refer to Section 5.39.7.9, “Enabling/Disabling an LDP Interface”.

Section 5.39.7.9
Enabling/Disabling an LDP Interface

To enable or disable an LDP interface, do the following:

1. Make sure the CLI is in Configuration mode.
2. Enable/disable the LDP interface by typing the following commands:

   Enable

   ```
   mpls ldp interface-ldp name
   ```

   Disable

   ```
   no mpls ldp interface-ldp name
   ```

   Where:

   - *name* is the name of the transport interface to be enabled or disabled.
3. Type **commit** and press **Enter** to save the changes, or type **revert** and press **Enter** to abort.

6 Troubleshooting

This chapter describes troubleshooting steps for common issues that may be encountered when using ROX II or designing a network. It describes the following tasks:

> **IMPORTANT!**
> *For further assistance, contact a Customer Service representative.*

Section 6.1

Feature Keys

The following describes common problems related to feature keys.

Problem	Solution
A file-based feature key does not match the hardware	Each file-based feature key is licensed to a particular device. When transfering 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 6.2

Ethernet Ports

The following describes common problems related to Ethernet ports.

Problem	Solution
A link seems fine when traffic levels are low, but fails as traffic rates increase OR a link can be pinged but has problems with FTP/SQL/HTTP/etc.	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

Problem	Solution
	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 Logical File Inclusion (LFI) protection feature.	Make sure LFI is not enabled on the peer as well. If both sides of the link have LFI enabled, then both sides will withhold link signal generation from each other.

Section 6.3
Multicast Filtering

The following describes common problems related to multicast filtering.

Problem	Solution
When started, a multicast traffic feed is always distributed to all members of the VLAN.	Is IGMP enabled for the VLAN? Multicasts will be distributed to all members of the VLAN unless IGMP is enabled.
Computers connected to the switch receive multicast traffic, but not when they are connected to a router.	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 3.17.4, “Viewing Switched Ethernet Port Statistics”. Verify the traffic count transmitted to the router is the same as the traffic count received from the multicasting source.
The video stream at an end station is of poor quality.	Video serving is a resource-intensive application. Because it uses isochronous workload, data must be fed at a prescribed rate or end users will see glitches in the video. Networks that carry data from the server to the client must be engineered to handle this heavy, isochronous workload. Video streams can consume large amounts of bandwidth. Features and capacity of both server and network (including routers, bridges, switches and interfaces) impact the streams. Do not exceed 60% of the maximum interface bandwidth. For example, if using a 10 Mbps Ethernet, run a single multicasting source at no more than 6 Mbps, or two sources at 3 Mbps. It is important to consider these ports in the network design, as router ports will carry the traffic of all multicast groups. **IMPORTANT!** *Multicasting will introduce latency in all traffic on the network. Plan the network carefully in order to account for capacity and latency concerns.*
Multicast streams of some groups are not forwarded properly. Some segments without subscribers receive the traffic, while some segments with subscribers do not.	Make sure different multicast groups do not have multicast IP addresses that map to the same multicast MAC address. The switch forwarding operation is MAC address-based and will not work properly for several groups mapping to the same MAC address.
Computers on the switch issue join requests, but do not receive multicast streams from a router.	Is the multicast route running IGMP version 2? It must run IGMP version 2 in order for IGMP Snooping to operate properly.
Unable to connect or disconnect some switch ports, and multicast goes everywhere. Is IGMP broken?	IGMP is not broken. This may in fact be proper switch behavior. When the switch detects a change in the network topology through RSTP, it acts to avoid loss of multicast traffic. If configured to do so, it starts forwarding all multicast traffic to all ports that are not RSTP Edge ports (because they may potentially link to routers). This may result in some undesired flooding of multicast traffic, which will stop after a few minutes. However, it guarantees that all devices interested in the traffic will keep receiving it without interruption. The same behavior will be observed when the switch resets or when IGMP Snooping is being disabled for the VLAN.

Section 6.4
Spanning Tree

The following describes common problems related to the Spanning Tree Protocol (STP).

Problem	Solution
The network locks up when a new port is connected and the port status LEDs are flashing rapidly.	Is it possible that one of the switches in the network or one of the ports on a switch in the network has STP disabled and accidentally connects to another switch? If this has occurred, then a traffic loop has been formed.
Occasionally, the ports seem to experience significant flooding for a brief period of time.	If the problem appears to be transient in nature, it is possible that ports that are part of the spanning tree have been configured as edge ports. After the link layers have come up on edge ports, STP will directly transition them (perhaps improperly) to the forwarding state. If an RSTP configuration message is then received, the port will be returned to blocking. A traffic loop may be formed for the length of time the port was in forwarding.
A switch displays a strange behavior where the root port hops back and forth between two switch ports and never settles down.	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 multipoint ports converge slowly after failures occur. Is it possible that the port has migrated to STP? If the port is connected to the LAN segment by shared media and STP bridges are connected to that media, then convergence after link failure will be slow. Delays on the order of tens or hundreds of milliseconds can result in circumstances where the link broken is the sole link to the root bridge and the secondary root bridge is poorly chosen. The worst of all possible designs occurs when the secondary root bridge is located at the farthest edge of the network from the root. In this case, a configuration message will have to propagate out to the edge and then back in order to reestablish the topology.
The network is composed of a ring of bridges, of which two (connected to each other) are managed and the rest are unmanaged. Why does the RSTP protocol work quickly when a link is broken between the managed bridges, but not in the unmanaged bridge part of the ring?	A properly operating unmanaged bridge is transparent to STP configuration messages. The managed bridges will exchange configuration messages through the unmanaged bridge part of the ring as if it is non-existent. When a link in the unmanaged part of the ring fails however, the managed bridges will only be able to detect the failure through timing out of hello messages. Full connectivity will require three hello times plus two forwarding times to be restored.

Problem	Solution
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 occassionally lost.	Review the network statistics to determine whether the root bridge is receiving TCNs around the time of observed frame loss. It may be possible there are problems with intermittent links in the network.
The root is receiving a number of TCNs. Where are they coming from?	Examine the RSTP port statistics to determine the port from which the TCNs are arriving. Sign-on to the switch at the other end of the link attached to that port. Repeat this step until the switch generating the TCNs is found (i.e. the switch that is itself not receiving a large number of TCNs). Determine the problem at that switch.

Section 6.5

VLANs

The following describes common problems related to the VLANs.

Problem	Solution
VLANs are not needed on the network. Can they be turned off?	Yes. Simply leave all ports set to type *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.