SIEMENS

Configuration Manual

SIMATIC NET

Rugged Ethernet Switches

RUGGEDCOM ROS v4.3

For RS900W

Edition 06/2020

https://www.siemens.com

SIEMENS

SIMATIC NET

Rugged Ethernet Switches RUGGEDCOM ROS v4.3

Configuration Manual

For RS900W

06/2020

C79000-G8976-1280-08

Legal Information

Warning Notice System

This manual contains notices you have to observe in order to ensure your personal safety, as well as to prevent damage to property. The notices referring to your personal safety are highlighted in the manual by a safety alert symbol, notices referring only to property damage have no safety alert symbol. These notices shown below are graded according to the degree of danger.

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

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

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

⚠ NOTICE
indicates that property damage can result if proper precautions are not taken.

If more than one degree of danger is present, the warning notice representing the highest degree of danger will be used. A notice warning of injury to persons with a safety alert symbol may also include a warning relating to property damage.

Qualified Personnel

The product/system described in this documentation may be operated only by **personnel qualified** for the specific task in accordance with the relevant documentation, in particular its warning notices and safety instructions. Qualified personnel are those who, based on their training and experience, are capable of identifying risks and avoiding potential hazards when working with these products/systems.

Proper Use of Siemens Products

Note the following:

⚠ WARNING
Siemens products may only be used for the applications described in the catalog and in the relevant technical documentation. If products and components from other manufacturers are used, these must be recommended or approved by Siemens. Proper transport, storage, installation, assembly, commissioning, operation and maintenance are required to ensure that the products operate safely and without any problems. The permissible ambient conditions must be complied with. The information in the relevant documentation must be observed.

Trademarks

All names identified by ® are registered trademarks of Siemens AG. The remaining trademarks in this publication may be trademarks whose use by third parties for their own purposes could violate the rights of the owner.

Disclaimer of Liability

We have reviewed the contents of this publication to ensure consistency with the hardware and software described. Since variance cannot be precluded entirely, we cannot guarantee full consistency. However, the information in this publication is reviewed regularly and any necessary corrections are included in subsequent editions.

Siemens AG
Digital Industry
Process Automation
Postfach 48 48
90026 NÜRNBERG
GERMANY

© 06/2020 Subject to Change

Table of Contents

Preface

This guide describes v4.3 of ROS (Rugged Operating System) running on the RUGGEDCOM RS900W. 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.

> ⚠ **NOTICE**
>
> Some of the parameters and options described may not be available depending on variations in the device hardware. While every attempt is made to accurately describe the specific parameters and options available, this Guide should be used as a companion to the Help text included in the software.

CLI Command Syntax

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

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

Related Documents

Product Notes

Product notes specific to each release of RUGGEDCOM ROS are available on the Siemens' Industry Online Support portal [https://support.industry.siemens.com].

User/Reference Guides

Document Title	Link
RUGGEDCOM NMS v2.1 User Guide for Windows	https://support.industry.siemens.com/cs/ww/en/view/109737564
RUGGEDCOM NMS v2.1 User Guide for Linux	https://support.industry.siemens.com/cs/ww/en/view/109737563
RUGGEDCOM DIRECTOR v1.4 User Guide	https://support.industry.siemens.com/cs/ww/en/view/97691648
RUGGEDCOM EXPLORER v1.5 User Guide	https://support.industry.siemens.com/cs/ww/en/view/109480804
RUGGEDCOM PING v1.2 User Guide	https://support.industry.siemens.com/cs/ww/en/view/97674073

FAQs

Document Title	Link
How Do You Configure the SMP Function in a RUGGEDCOM Switch with RUGGEDCOM ROS?	https://support.industry.siemens.com/cs/ww/en/view/109474615
How to Secure RUGGEDCOM ROS Devices Before and After Field Deployment	https://support.industry.siemens.com/cs/ww/en/view/99858806
How to Implement Robust Ring Networks Using RSTP and eRSTP	https://support.industry.siemens.com/cs/ww/en/view/109738240
How to Implement Secure, Unattended Logging in ROS	https://support.industry.siemens.com/cs/ww/en/view/109756843

Installation Guides

Document Title	Link
RUGGEDCOM RS900W Installation Guide	https://support.industry.siemens.com/cs/ww/en/view/82237996

System Requirements

Each workstation used to connect to the RUGGEDCOM ROS interface must meet the following system requirements:

- Must have a working Ethernet interface compatible with at least one of the port types on the RUGGEDCOM device
- The ability to configure an IP address and netmask on the computer's Ethernet interface

Accessing Documentation

The latest user documentation for RUGGEDCOM ROS v4.3 is available online at https://support.industry.siemens.com . To request or inquire about a user document, contact Siemens Customer Support.

Training

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

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

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

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

Customer Support

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

Online

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

Telephone

Call a local hotline center to submit a Support Request (SR). To locate a local hotline center, visit https://w3.siemens.com/aspa_app/-?lang=en.

Mobile App

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

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

- Ask questions or share knowledge with fellow Siemens customers and the support community

1 Introduction

Welcome to the RUGGEDCOM ROS v4.3 Software Configuration Manual for the RUGGEDCOM RS900W devices. This Guide describes the wide array of carrier grade features made available by RUGGEDCOM ROS (Rugged Operating System).

This chapter provides a basic overview of the RUGGEDCOM ROS software.

1.1 Features and Benefits

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

- **Cyber Security Features**

  Cyber security is an urgent issue in many industries where advanced automation and communications networks play a crucial role in mission critical applications and where high reliability is of paramount importance. Key RUGGEDCOM ROS 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

- **Enhanced Rapid Spanning Tree Protocol (eRSTP)™**

  Siemens's eRSTP allows the creation of fault-tolerant ring and mesh Ethernet networks that incorporate redundant links that are *pruned* to prevent loops. eRSTP implements both STP and RSTP to promote interoperability with commercial switches, unlike other proprietary *ring* solutions. The fast root failover feature of eRSTP provides quick network convergence in case of an RSTP root bridge failure in a mesh topology.

- **Quality of Service (IEEE 802.1p)**

  Some networking applications such as real-time control or VoIP (Voice over IP) require predictable arrival times for Ethernet frames. Switches can introduce latency in times of heavy network traffic due to the internal queues that buffer frames and then transmit on a first come first serve basis. RUGGEDCOM ROS supports *Class of Service*, which allows time critical traffic to jump to the front of the queue, thus minimizing latency and reducing *jitter* to allow such demanding applications to operate correctly. RUGGEDCOM ROS allows priority classification by port, tags, MAC address, and IP Type of Service (ToS). A configurable *weighted fair queuing* algorithm controls how frames are emptied from the queues.

- **VLAN (IEEE 802.1Q)**

  Virtual Local Area Networks (VLAN) allow the segregation of a physical network into separate logical networks with independent broadcast domains. A measure of security is provided since hosts can only access other hosts on the same VLAN and traffic storms are isolated. RUGGEDCOM ROS supports 802.1Q tagged Ethernet frames and VLAN trunks. Port based classification allows legacy devices to be assigned to the correct VLAN. GVRP support is also provided to simplify the configuration of the switches on the VLAN.

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

  SNMP provides a standardized method, for network management stations, to interrogate devices from different vendors. SNMP versions supported by RUGGEDCOM ROS are v1, v2c and v3. SNMPv3 in particular provides security features (such as authentication, privacy, and access control) not present in earlier SNMP versions. RUGGEDCOM ROS also supports numerous standard MIBs (Management Information Base) allowing for easy integration with any Network Management System (NMS). A feature of SNMP 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.

- **NTP (Network Time Protocol)**

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

- **Port Rate Limiting**

  RUGGEDCOM ROS supports configurable rate limiting per port to limit unicast and multicast traffic. This can be essential to managing precious network bandwidth for service providers. It also provides edge security for Denial of Service (DoS) attacks.

- **Broadcast Storm Filtering**

  Broadcast storms wreak havoc on a network and can cause attached devices to malfunction. This could be disastrous on a network with mission critical equipment. RUGGEDCOM ROS limits this by filtering broadcast frames with a user-defined threshold.

- **Link Aggregation**

  Ethernet ports can be aggregated into a single logical link either statically or dynamically to increase bandwidth and balance the traffic load.

- **Port Mirroring**

  RUGGEDCOM ROS can be configured to duplicate all traffic on one port to a designated mirror port. When combined with a network analyzer, this can be a powerful troubleshooting tool.

- **Port Configuration and Status**

  RUGGEDCOM ROS allows individual ports to be *hard* configured for speed, duplex, auto-negotiation, flow control and more. This allows proper connection with devices that do not negotiate or have unusual settings. Detailed status of ports with alarm and SNMP trap on link problems aid greatly in system troubleshooting.

- **Port Statistics and RMON (Remote Monitoring)**

  RUGGEDCOM ROS 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.

- **Multicast Filtering**

  RUGGEDCOM ROS supports static multicast groups and the ability to join or leave multicast groups dynamically using IGMP (Internet Group Management Protocol) or GMRP (GARP Multicast Registration Protocol).

- **Event Logging and Alarms**

  RUGGEDCOM ROS records all significant events to a non-volatile system log allowing forensic troubleshooting. Events include link failure and recovery, unauthorized access, broadcast storm detection, and self-test diagnostics among others. Alarms provide a snapshot of recent events that have yet to be acknowledged by the network administrator. An external hardware relay is de-energized during the presence of critical alarms, allowing an external controller to react if desired.

- **HTML Web Browser User Interface**

  RUGGEDCOM ROS 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 facilitate setup and configuration. RUGGEDCOM ROS presents a common look and feel and standardized configuration process, allowing easy migration to other managed RUGGEDCOM products.

- **Brute Force Attack Prevention**

  Protection against Brute Force Attacks (BFAs) is standard in RUGGEDCOM ROS. If an external host fails to log in to the Terminal or Web interfaces after a fixed number of attempts, the service will be blocked for one hour.

1.2 Security Recommendations

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

Authentication

- Replace the default passwords for all user accounts and processes (where applicable) before the device is deployed.
- Use strong passwords with high randomization (i.e. entropy), without repetition of characters. Avoid weak passwords such as *password1*, *123456789*, *abcdefgh*, and any dictionary words or proper names in any combination. For more information about creating strong passwords, refer to the password requirements in "Configuring Passwords (Page 116)".
- Make sure passwords are protected and not shared with unauthorized personnel.
- Passwords should not be re-used across different user names and systems, or after they expire.
- If RADIUS authentication is done remotely, make sure all communications are within the security perimeter or on a secure channel.
- Generate and provision a custom SSL certificate and SSH host key pair before commissioning the device. For more information, refer to "Managing SSH/SSL Keys and Certificates (Page 135)".
- Use SSH public key authentication. For more information, refer to "Managing SSH/SSL Keys and Certificates (Page 135)".

Physical/Remote Access

- Do not connect the device to the Internet. Deploy the device only within a secure network perimeter.
- Restrict physical access to the device to only authorized personnel. A person with malicious intent could extract critical information, such as certificates, keys, etc. (user passwords are protected by hash codes), or reprogram the device.
- 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 the RUGGEDCOM ROS boot loader, which includes tools that may be used to gain complete access to the device.

- Only enable 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.
- Mirror ports allow bidirectional traffic (i.e. the device will not block incoming traffic to the mirror port or ports). For increased security, configure ingress filtering to control traffic flow when port mirroring is enabled. For more information about enabling port mirroring, refer to "Configuring Port Mirroring (Page 64)". For more information about enabling ingress filtering, refer to "Configuring VLANs Globally (Page 152)".
- 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 "Managing SNMP (Page 279)".
- Avoid using insecure services such as Telnet and TFTP, or disable them completely if possible. These services are available for historical reasons and are disabled by default.
- Disable RCDP if it is not intended for use.
- Limit the number of simultaneous Web Server, Telnet and SSH sessions allowed.
- Configure remote system logging to forward all logs to a central location. For more information, refer to "Managing Logs (Page 45)".
- Configuration files are provided in the CSV (comma separated values) 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.
- Management of the configuration file, certificates and keys is the responsibility of the device owner. Consider using RSA key sizes of at least 2048 bits in length and certificates signed with SHA256 for increased cryptographic strength. Before returning the device to Siemens for repair, make sure encryption is disabled (to create a cleartext version of the configuration file) and 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 and SSH are secure, others such as HTTP, Telnet, and RSH were not designed for this purpose. Appropriate safeguards against non-secure protocols should be taken to prevent unauthorized access to the device/network.
- Configure port security features on access ports to prevent an unauthorized third-party from physically connecting to the device. For more information, refer to "Managing Port Security (Page 126)".
- Be aware of insecure WLAN protocols, such as Open and WEP. Only use secure protocols when using WLAN, such as Wi-Fi Protected Access 2 (WPA2).

Hardware/Software

- Make sure the latest firmware version is installed, including all security-related patches. For the latest information on security patches for Siemens products, visit the Industrial Security website [https://www.siemens.com/global/en/home/company/topic-areas/future-of-manufacturing/industrial-security.html] or the ProductCERT Security Advisories website [http://www.siemens.com/innovation/en/technology-focus/siemens-cert/cert-security-advisories.htm]. Updates to Siemens Product Security Advisories can be obtained by subscribing to the RSS feed on the Siemens ProductCERT Security Advisories website, or by following @ProductCert on Twitter.
- Enable BPDU Guard on ports where RSTP BPDUs are not expected.
- Use the latest Web browser version compatible with RUGGEDCOM ROS to make sure the most secure Transport Layer Security (TLS) versions and ciphers available are employed.
- Modbus can be deactivated if not required by the user. If Modbus activation is required, then it is recommended to follow the security recommendations outlined in this User Guide and to configure the environment according to defense-in-depth best practices.
- 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.
- For optimal security, use SNMPv3 whenever possible. Use strong authentication keys and private keys without repetitive strings (e.g. *abc* or *abcabc*) with this feature. For more information about creating strong passwords, refer to the password requirements in "Configuring Passwords (Page 116)".
- Unless required for a particular network topology, the *IP Forward* setting should be set to `Disabled` to prevent the routing of packets.

Policy

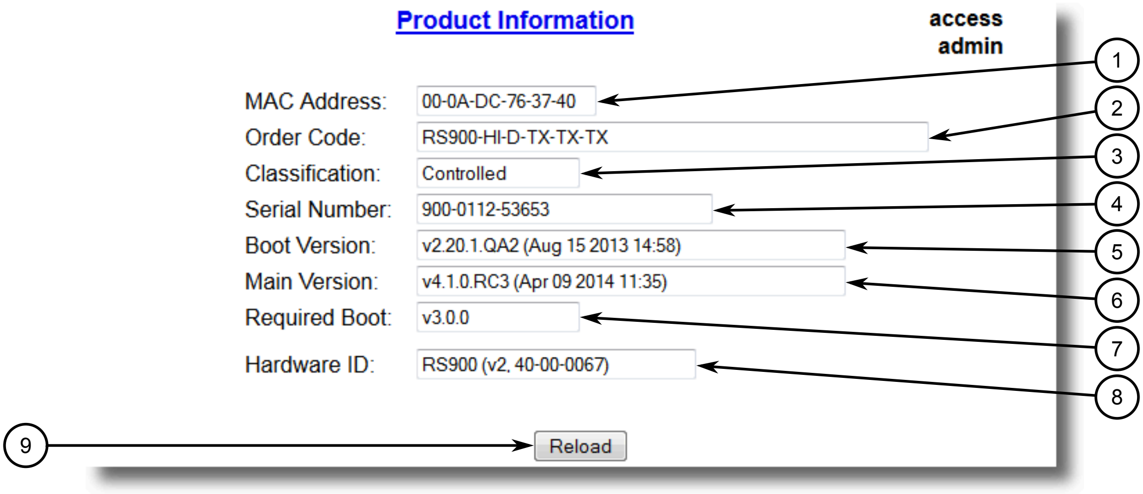
- Periodically audit the device to make sure it complies with these recommendations and/or any internal security policies.
- Review the user documentation for other Siemens products used in coordination with device for further security recommendations.

1.3 Controlled vs. Non-Controlled

RUGGEDCOM ROS devices are available as either Controlled (C) or Non-Controlled (NC).

- **Controlled** switches feature a variety of encryption capabilities.
- **Non-controlled** switches have limited encryption capabilities.

To determine if a device is classified as controlled or non-controlled, navigate to ***Diagnostics » View Product Information***. The `Classification` parameter on the **Product Information** form indicates if the device is controlled or non-controlled.



MAC Address:	00-0A-DC-76-37-40
Order Code:	RS900-HI-D-TX-TX-TX
Classification:	Controlled
Serial Number:	900-0112-53653
Boot Version:	v2.20.1.QA2 (Aug 15 2013 14:58)
Main Version:	v4.1.0.RC3 (Apr 09 2014 11:35)
Required Boot:	v3.0.0
Hardware ID:	RS900 (v2, 40-00-0067)

① MAC Address Box
② Order Code Box
③ Classification Box
④ Serial Number Box
⑤ Boot Version Box
⑥ Main Version Box
⑦ Required Boot Box
⑧ Hardware ID Box
⑨ Reload Button

Figure 1.1 Product Information Form (Example)

A non-controlled device can be converted to a controlled device by uploading the applicable controlled firmware version. For more information about uploading firmware to the device, refer to "Upgrading Firmware (Page 96)".

1.4 Supported Networking Standards

The following networking standards are supported by RUGGEDCOM ROS:

Standard	10 Mbps Ports	100 Mbps Ports	1000 Mbps Ports	Notes
IEEE 802.3x	•	•	•	Full Duplex Operation
IEEE 802.3z			•	1000Base-LX
IEEE 802.3ab			•	1000Base-Tx
IEEE 802.1D	•	•	•	MAC Bridges
IEEE 802.1Q	•	•	•	VLAN (Virtual LAN)
IEEE 802.1p	•	•	•	Priority Levels

1.5 Port Numbering Scheme

For quick identification, each port on a RUGGEDCOM RS900W device is assigned a number. All port numbers are silk-screened on the device.

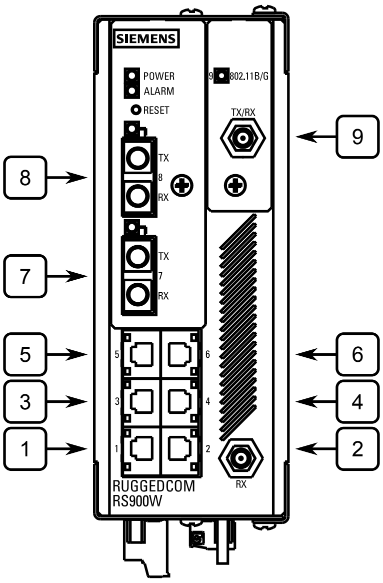


Figure 1.2 RUGGEDCOM RS900W Port Numbering (Typical)

Use these numbers to configure applicable features on select ports.

1.6 Available Services by Port

The following table lists the services available under RUGGEDCOM ROS. This table includes 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	Service Enabled/Disabled	Access Authorized	Note
Telnet	TCP/23	Disabled	Yes	Only available through management interfaces.
HTTP	TCP/80	Enabled, redirects to 443	—	Only redirects to 443 on Controlled versions
HTTPS	TCP/443	Enabled (configurable)	Yes	Only applicable to Controlled versions
RSH	TCP/514	Disabled (configurable)	Yes	Only available through management interfaces.
TFTP	UDP/69	Disabled (configurable)	No	Only available through management interfaces.
SFTP	TCP/22	Enabled	Yes	Only available through management interfaces.
SNMP	UDP/161	Disabled (configurable)	Yes	Only available through management interfaces.
SNTP	UDP/123	Enabled (configurable)	No	Only available through management interfaces.
SSH	TCP/22	Enabled	Yes	Only available through management interfaces.
ICMP	—	Enabled	No	
TACACS+	TCP/49 (configurable)	Disabled (configurable)	Yes	
RADIUS	UDP/1812 to send (configurable), opens random port to listen to	Disabled (configurable)	Yes	Only available through management interfaces.
Remote Syslog	UDP/514 (configurable)	Disabled (configurable)	No	Only available through management interfaces.
TCP Modbus (Server)	TCP/502	Disabled (configurable)	No	Only available through management interfaces.
TCP Modbus (Switch)	TCP/502	Disabled (configurable)	No	
DHCP, DHCP Agent	UDP/67, 68 sending msg if enabled - if received, always come to CPU, dropped if service not configured	Disabled (configurable)	No	
DHCP Server (WLAN)	UDP/67 for listening UDP/68 for responding	Enabled	No	
RCDP	—	Enabled (configurable)	Yes	

2 Using ROS

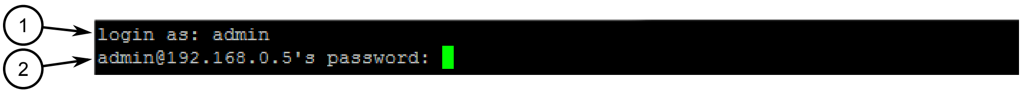
This chapter describes how to use RUGGEDCOM ROS.

2.1 Logging In

To log in to the device, do the following:

1. Connect to the device either directly or through a Web browser. For more information about how to connect to the device, refer to "Connecting to ROS (Page 33)".

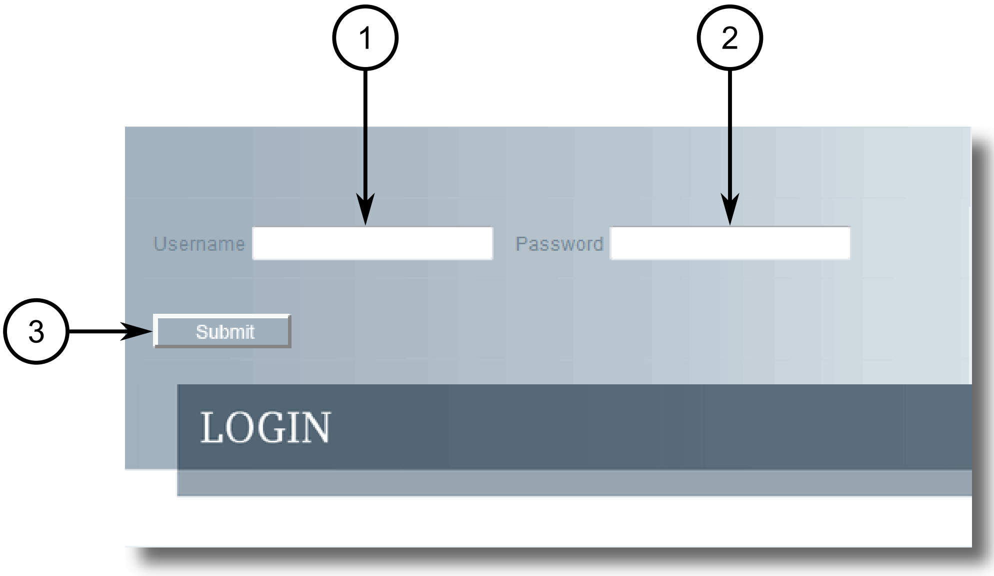
   Once the connection is established, the login form appears.



```
login as: admin
admin@192.168.0.5's password:
```

① User Name Box
② Password Box

Figure 2.1 SSH Login Screen (Console Interface)



① Username Box
② Password Box
③ Submit Button

Figure 2.2 Login Screen (Web Interface)

Note
The following default user names and passwords are set on the device for each user type:

Guest	Operator	Admin
User Name: guest	User Name: operator	User Name: admin

Password: guest	Password: operator	Password: admin

⚠ **CAUTION**

To prevent unauthorized access to the device, make sure to change the default guest, operator, and admin passwords before commissioning the device.

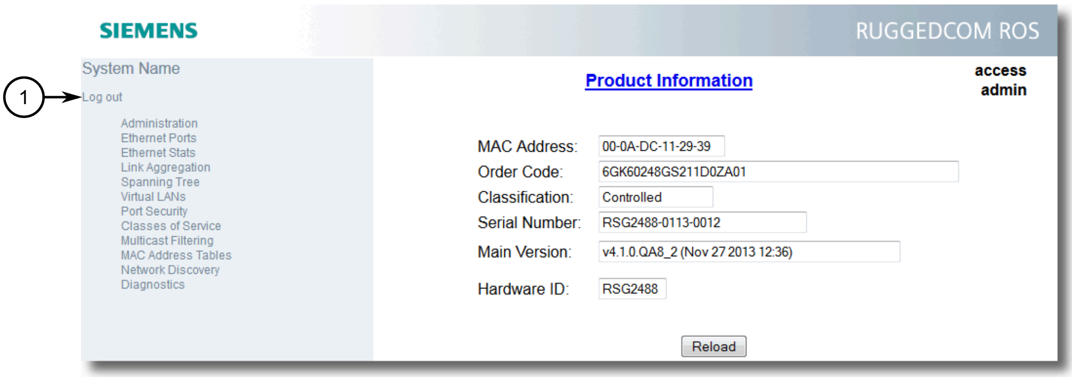
For more information about changing passwords, refer to "Configuring Passwords (Page 116)".

2. In the **User Name** field, type the user name for an account setup on the device.
3. In the **Password** field, type the password for the account.
4. Click **Enter** or click **Submit** (Web interface only).

2.2 Logging Out

To log out of the device, navigate to the main screen and do the following:

- To log out of the Console or secure shell interfaces, press **CTRL** + **X**.
- To log out of the Web interface, click **Logout**.



MAC Address: 00-0A-DC-11-29-39
Order Code: 6GK60248GS211D0ZA01
Classification: Controlled
Serial Number: RSG2488-0113-0012
Main Version: v4.1.0.QA8_2 (Nov 27 2013 12:36)
Hardware ID: RSG2488

① Logout

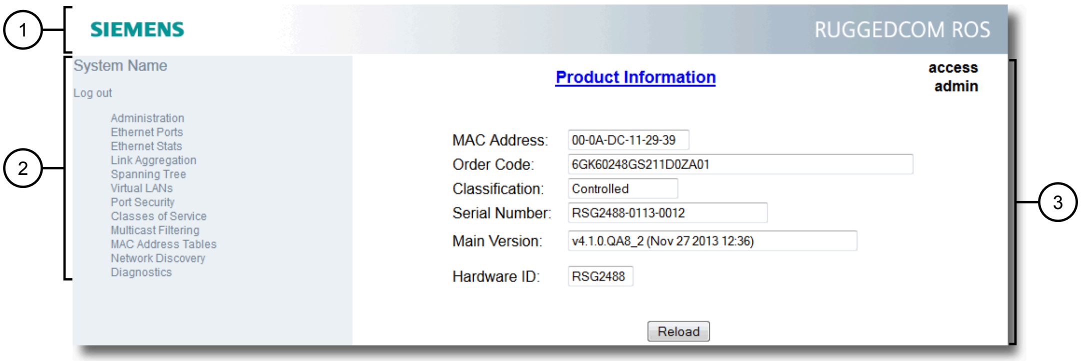
Figure 2.3 Web Interface (Example)

Note

If any pending configuration changes have not been committed, RUGGEDCOM ROS will request confirmation before discarding the changes and logging out of the device.

2.3 Using the Web Interface

The Web interface is a Web-based Graphical User Interface (GUI) for displaying important information and controls in a Web browser. The interface is divided into three frames: the banner, the menu and the main frame.



MAC Address: 00-0A-DC-11-29-39
Order Code: 6GK60248GS211D0ZA01
Classification: Controlled
Serial Number: RSG2488-0113-0012
Main Version: v4.1.0.QA8_2 (Nov 27 2013 12:36)
Hardware ID: RSG2488

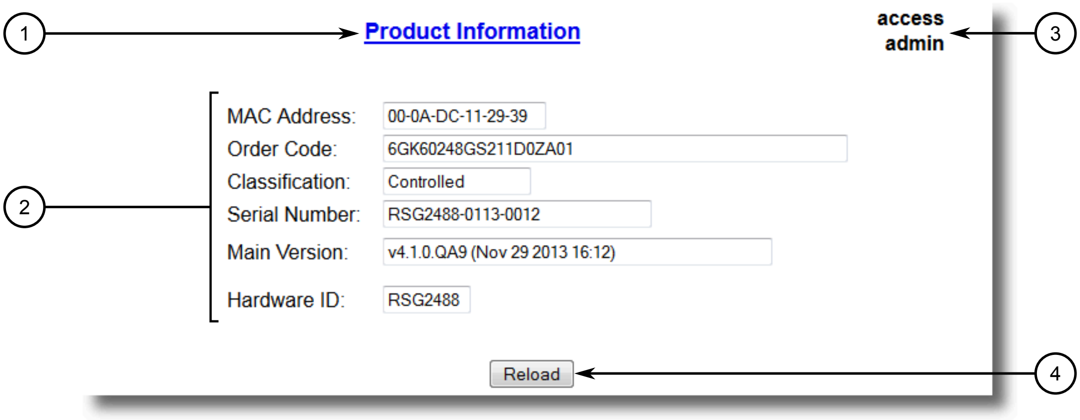
① Top Frame
② Side Frame
③ Main Frame

Figure 2.4 Web Interface Layout (Example)

Frame	Description
Top	The top frame displays the system name for the device.
Side	The side frame contains a logout option and a collapsible list of links that open various screens in the main frame. For information about logging out of RUGGEDCOM ROS, refer to "Logging Out (Page 13)".
Main	The main frame displays the parameters and/or data related to the selected feature.

Each screen consists of a title, the current user's access level, parameters and/or data (in form or table format), and controls (e.g. add, delete, refresh, etc.). The title provides access to context-specific Help for the screen that provides important information about the available parameters and/or data. Click on the link to open the Help information in a new window.

When an alarm is generated, an alarm notification replaces the current user's access level on each screen until the alarm is cleared. The notification indicates how many alarms are currently active. For more information about alarms, refer to "Managing Alarms (Page 102)".



MAC Address: 00-0A-DC-11-29-39
Order Code: 6GK60248GS211D0ZA01
Classification: Controlled
Serial Number: RSG2488-0113-0012
Main Version: v4.1.0.QA9 (Nov 29 2013 16:12)
Hardware ID: RSG2488

① Title
② Parameters and/or Data
③ Access Level or Alarm Notification
④ Controls

Figure 2.5 Elements of a Typical Screen (Example)

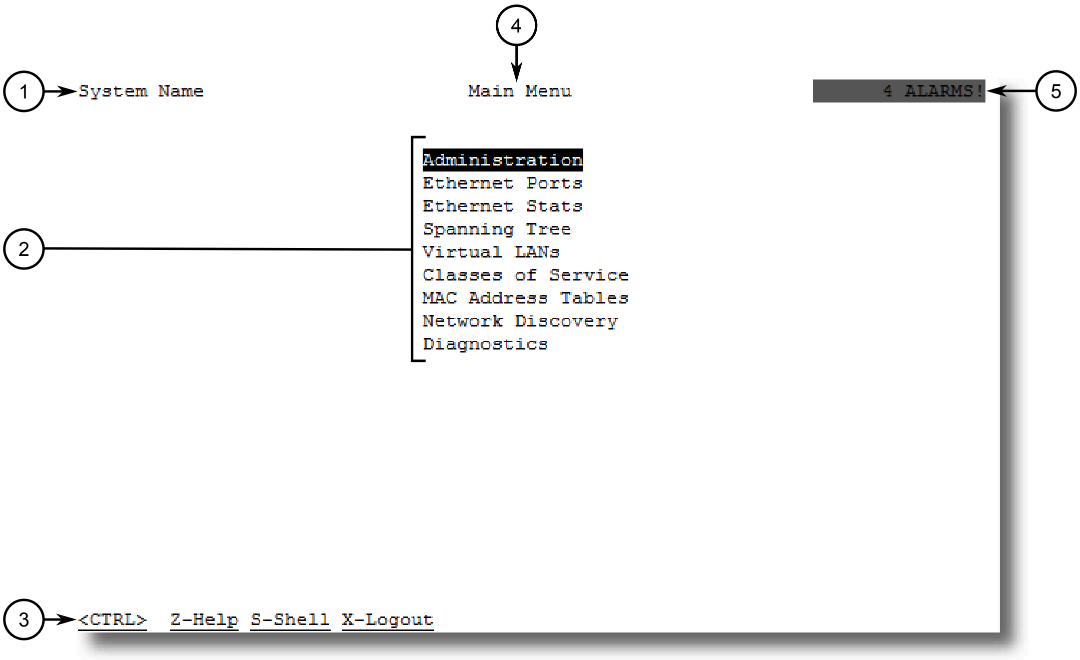
Note
If desired, the web interface can be disabled. For more information, refer to "Enabling/Disabling the Web Interface (Page 102)".

2.4 Using the Console Interface

The Console interface is a Graphical User Interface (GUI) organized as a series of menus. It is primarily accessible through a serial console connection, but can also be accessed through IP services, such as a Telnet, RSH (Remote Shell), SSH (Secure Shell) session, or SSH remote command execution.

Note
IP services can be restricted to control access to the device. For more information, refer to "Configuring IP Services (Page 81)".

Each screen consists of a system identifier, the name of the current menu, and a command bar. Alarms are also indicated on each screen in the upper right corner.



① System Identification
② Menus
③ Command Bar
④ Menu Name
⑤ Alarms Indicator

Figure 2.6 Console Interface (Example)

Note

The system identifier is user configurable. For more information about setting the system name, refer to "Configuring the System Information (Page 101)".

Navigating the Interface

Use the following controls to navigate between screens in the Console interface:

Enter	Select a menu item and press this **Enter** to enter the sub-menu or screen beneath.
Esc	Press **Esc** to return to the previous screen.

Configuring Parameters

Use the following controls to select and configure parameters in the Console interface:

Up/Down Arrow Keys	Use the up and down arrow keys to select parameters.
Enter	Select a parameter and press **Enter** to start editing a parameter. Press **Enter** again to commit the change.

Esc	When editing a parameter, press **Esc** to abort all changes.

Commands

The command bar lists the various commands that can be issued in the Console interface. Some commands are specific to select screens. The standard commands include the following:

Ctrl + A	Commits configuration changes made on the current screen. **Note** Before exiting a screen, RUGGEDCOM ROS will automatically prompt the user to save any changes that have not been committed.
Ctrl + I	Inserts a new record.
Ctrl + L	Deletes a record.
Ctrl + S	Opens the CLI interface.
Ctrl + X	Terminates the current session. This command is only available from the main menu.
Ctrl + Z	Displays important information about the current screen or selected parameter.

2.5 Using the Command Line Interface

The Command Line Interface (CLI) offers a series of powerful commands for updating RUGGEDCOM ROS, generating certificates/keys, tracing events, troubleshooting and much more. It is accessed via the Console interface by pressing **Ctrl-S**.

2.5.1 Available CLI Commands

The following commands are available at the command line:

Command	Description	Authorized Users
alarms all	Displays a list of available alarms. Optional and/or required parameters include: • all displays all available alarms	Guest, Operator, Admin
arp	Displays the IP to MAC address resolution table.	Admin
clearalarms	Clears all alarms.	Operator, Admin
cleareth stats [all | { *port* }]	Clears Ethernet statistics for one or more ports. Optional and/or required parameters include: • all clears statistics for all ports • { *port* }is a comma separated list of port numbers (e.g. 1,3-5,7)	Operator, Admin
clearlogs	Clears the system and crash logs.	Admin
clrcblstats [all | { *port* }]	Clears cable diagnostics statistics for one or more ports.	Admin

Command	Description	Authorized Users
	Optional and/or required parameters include: • `all` clears statistics for all ports • { *port* }is a comma separated list of port numbers (e.g. 1,3-5,7)	
clrstpstats	Clears all spanning tree statistics.	Operator, Admin
cls	Clears the screen.	Guest, Operator, Admin
dir	Prints the directory listing of the internal memory.	Guest, Operator, Admin
exit	Terminates the session.	Guest, Operator, Admin
factory	Enables factory mode, which includes several factory-level commands used for testing and troubleshooting. Only available to admin users. ⚠ **CAUTION** Misuse of the factory commands may corrupt the operational state of device and/or may permanently damage the ability to recover the device without manufacturer intervention.	Admin
flashfiles `{ info {` *filename* `} | defrag }`	A set of diagnostic commands to display information about the Flash filesystem and to defragment Flash memory. Optional and/or required parameters include: • `info {` *filename* `}` displays information about the specified file in the Flash file system • `defrag` defragments files in the Flash file system For more information about the **flashfiles** command, refer to "Managing the Flash File System (Page 30)".	Admin
flashleds `{` *timeout* `}`	Flashes the LED indicators on the device for a specified number of seconds. Optional and/or required parameters include: • { *timeout* }is the number of seconds to flash the LED indicators. To stop the LEDs from flashing, set the timeout period to 0 (zero).	Admin
fpgacmd	Provides access to the FPGA management tool for troubleshooting time synchronization.	Admin
help `{` *command* `}`	Displays a brief description of the specified command. If no command is specified, it displays a list of all available commands, including a description for each. Optional and/or required parameters include: • { *command* }is the command name.	Guest, Operator, Admin
ipconfig	Displays the current IP address, subnet mask and default gateway. This command provides the only way of determining these values when DHCP is used.	Guest, Operator, Admin
loaddflts	Loads the factory default configuration.	Admin
logout	Logs out of the shell.	Guest, Operator, Admin

Command	Description	Authorized Users
logs	Displays syslog entries in CLI shell.	Admin
passwd { *user_name* } { *new_password* }	Changes the selected user's password. Optional and/or required parameters include: • { *user_name* } is an existing user_name in RUGGEDCOM ROS. • { *new_password* } is the new password that will replace the existing password of the selected user. This command is unavailable in Telnet sessions.	Admin
ping { *address* } { { *count* } | { *timeout* } }	Sends an ICMP echo request to a remotely connected device. For each reply received, the round trip time is displayed. Use this command to verify connectivity to the next connected device. It is a useful tool for testing commissioned links. This command also includes the ability to send a specific number of pings with a specified time for which to wait for a response. Optional and/or required parameters include: • { *address* }is the target IP address. • { *count* }is the number of echo requests to send. The default is 4. • { *timeout* }is the time in milliseconds to wait for each reply. The range is 2 to 5000 seconds. The default is 300 milliseconds. **Note** The device to be pinged must support ICMP echo. Upon commencing the ping, an ARP request for the MAC address of the device is issued. If the device to be pinged is not on the same network as the device pinging the other device, the default gateway must be programmed.	Guest, Operator, Admin
purgemac	Purges the MAC Address table.	Operator, Admin
random	Display seeds or random numbers.	Admin
reset	Perform a hard reset of the switch.	Operator, Admin
resetport { all | { *ports* } }	Resets one or more Ethernet ports, which may be useful for forcing re-negotiation of speed and duplex, or in situations where the link partner has latched into an inappropriate state. Optional and/or required parameters include: • `all` resets all ports • { *ports* }is a comma separated list of port numbers (e.g. 1,3-5,7)	Operator, Admin
rmon	Displays the names of all RMON alarm eligible objects.	Guest, Operator, Admin
route	Displays the gateway configuration.	Guest, Operator, Admin
sfp { *port* } { base | alarms | diag | calibr | thr | all | no	Displays SFP (Small Form Factor Pluggable) device information and diagnostics. If optional or required parameters are not used, this command displays the base and extended information.	Admin

Command	Description	Authorized Users
`parameter specified }`	Optional and/or required parameters include: - { *port* }is the port number for which the data are required - `base` displays the base information - `alarms` displays alarms and warning flags - `diag` displays measured data - `calibr` displays calibration data for external calibration - `thr` displays thresholds data - `all` displays all diagnostic data	
sql `{ default | delete | help | info | insert | save | select | update }`	Provides an SQL-like interface for manipulating all system configuration and status parameters. All commands, clauses, table, and column names are case insensitive. Optional and/or required parameters include: - `default` sets all records in a table(s) to factory defaults - `delete` allows for records to be deleted from a table - `help` provides a brief description for any SQL command or clause - `info` displays a variety of information about the tables in the database - `insert` enables new records to be inserted into a table - `save` saves the database to non-volatile memory storage - `select` queries the database and displays selected records - `update` enable existing records in a table to be updated For more information about the **sql** command, refer to "Using SQL Commands (Page 26)".	Admin
sshkeygen `[ rsa | dsa ] [ 1024 | 2048 | 3072 ] {` *N* `}`	Generates new RSA or DSA keys in `ssh.keys`. Keys can be either 1024, 2048 or 3072 bits long.	Admin
sshpubkey	List, remove and update key entries in sshpub.keys file.	Admin
sslkeygen `{` *key type* `} {` *N* `}`	Generates a new SSL certificate in `ssl.crt`. Optional and/or required parameters include: - { *keytype* }is the type of key, either rsa or ecc - { *N* }is the number of bits in length. For RSA keys, the allowable sizes are 1024, 2048 or 3072. For ECC keys, the allowable sizes are 192, 224, 256, 384, or 521.	Admin
svcmod `-s {` *snmpaccess* `} { -i {` *GroupName* `} | -d {` *GroupName* `} }`	Modifies SNMP access groups.	Admin

Command	Description	Authorized Users
-sm { *SecurityModel* } -sl { *SecurityLevel* } -rv { *ReadViewName* } -wv { *WriteViewName* } -nv { *NotifyViewName* }	Optional and/or required parameters include: • -i { *GroupName* } creates a new access group with a specified group name or modifies parameters associated with a specified access group, if it already exists • -d { *GroupName* } deletes a specified access group • -sm { *SecurityModel* } specifies the security model to be used • -sl { *SecurityLevel* } specifies the SNMP security level to be granted to the specified access group. Allowable values are 'authPriv' (i.e. communication with authentication and privacy), 'authNoPriv' (i.e. communication with authentication and without privacy), or 'noAuthnoPriv' (i.e. communication with neither authentication nor privacy). • -rv { *ReadViewName* } identifies the MIB tree(s) to which this entry authorizes read access. Allowable values are 'noView', 'V1Mib', or 'allOfMib'. • -wv { *WriteViewName* } identifies the MIB tree(s) to which this entry authorizes write access. Allowable values are 'noView', 'V1Mib', or 'allOfMib'. • -nv { *NotifyViewName* } identifies the MIB tree(s) to which this entry authorizes access for notifications. Allowable values are 'noView', 'V1Mib', or 'allOfMib'.	
svcmod -s { *snmpgroup* } { -i { *UserName* } | -d { *UserName* } } -sm { *SecurityModel* } -g { *group* }	Modifies SNMP security-to-group maps. Optional and/or required parameters include: • -i { *UserName* } -sm { *SecurityModel* } creates a new user name and security profile as specified or modifies parameters associated with a specified user name and security profile, if they already exist • -d { *UserName* } -sm { *SecurityModel* } deletes a specified user name and security profile • -g { *group* } specifies the group to which the user name and secuirty profile belong	Admin
svcmod -s { *snmpuser* } { -i { *UserName* } | -d { *UserName* } } -c { *Community* } -ip { *IP* } -ap { *protocol* } -ak { *key* } -pp { *protocol* } -pk { *key* }	Modifies SNMP users. Optional and/or required parameters include: • -i { *UserName* } creates a new user name as specified or modifies parameters associated with a specified user name, if it already exists • -d { *UserName* } deletes a specified user name • -c { *Community* } specifies the SNMP community string (for SNMPv1 or SNMPv2c). • -ip { *IP* } configures a specified IP address to be used for SNMP authentication	Admin

Command	Description	Authorized Users
	- `-ap { protocol }` configures SNMP authetication via a specified authentication protocol. Allowable values are 'noAuth', 'HMACMD5', or 'HMACSHA'. - `-ak { key }` sets a secret key (of 0 or 6+ characters) to be used for SNMP authentication - `-pp { protocol }` configures data encryption via a specified privacy protocol. Allowable values are 'noPriv' or 'CBC-DES.' - `-ak { key }` sets a secret key (of 0 or 6+ characters) to be used for data encyrption	
svcmod `-s { radius } { -ip { 1 } | -ip { 2 } } -ip { IP } -ak { AuthKey } -pt { Port } -ux { UsernameExtension } -mr { MaxRetries } -to { timeout }`	Modifies RADIUS security server. Optional and/or required parameters include: - `-ip { 1 }` sets the specified server as the primary RADIUS server - `-ip { 2 }` sets the specified server as the backup RADIUS server - `-ip { 2 } -ip` deletes the primary RADIUS server - `-ip { 1 } -ip` deletes the backup RADIUS server - `-ip { IP }` specifies the IP address of the RADIUS server - `-ak { AuthKey }` specifies an authentication key to be shared with the RADIUS server - `-pt { Port }` specifies the port number of the IP port on the RADIUS server - `-ux { UsernameExtension }` defines an affix to be added when a user name is sent to the RADIUS server for authentication. Values may include predefined keywords (wrapped in % delimiters) or user-defined strings. Predefined keywords are '%Username%' (i.e. the name associated with the user profile), '%IPaddr%' (i.e. the management IP address of the Network Access Server), '%SysName%' (i.e. the system name given to the device), and '%SysLocation%' (i.e. the phyiscal location of the device). - `-mr { MaxRetries }` specifies the maximum number of times the authenticator will attempt to authenticate a user in the case of any failure. After the specified value is exceeded, authentication fails. - `-to { timeout }` specifies the number of milliseconds (ms) the authenticator will wait for a response from the RADUS server before reattempting authentication.	Admin
svcmod `-s { tacacsplus } { -ip { 1 } | -ip { 2 } } -ip { IP } -ak`	Modifies TACACS+ security server. Optional and/or required parameters include: - `-ip { 1 }` sets the specified server as the primary TACACS+ server	Admin

Command	Description	Authorized Users
`{ AuthKey } -pt { Port } -ux { UsernameExtension } -mr { MaxRetries } -to { timeout } -apl { AdminPrivilege } -opl { OperPrivilege } -gpl { GuestPrivilege }`	- `-ip { 2 }` sets the specified server as the backup TACACS+ server - `-ip { 2 } -ip` deletes the primary TACACS + server - `-ip { 1 } -ip` deletes the backup TACACS + server - `-ip { IP }` specifies the IP address of the TACACS+ server - `-ak { AuthKey }` specifies an authentication key to be shared with the TACACS+ server - `-pt { Port }` specifies the port number of the IP port on the TACACS+ server - `-ux { UsernameExtension }` defines an affix to be added when a user name is sent to the TACACS+ server for authentication. Values may include predefined keywords (wrapped in % delimiters) or user-defined strings. Predefined keywords are '%Username%' (i.e. the name associated with the user profile), '%IPaddr%' (i.e. the management IP address of the Network Access Server), '%SysName%' (i.e. the system name given to the device), and '%SysLocation%' (i.e. the phyiscal location of the device). - `-mr { MaxRetries }` specifies the maximum number of times the authenticator will attempt to authenticate a user in the case of any failure. After the specified value is exceeded, authentication fails. - `-to { timeout }` specifies the number of milliseconds (ms) the authenticator will wait for a response from the TACACS+ server before reattempting authentication. - `-apl { AdminPrivilege }` specifies the level to which administrator users are able to configure the TACACS+ server. Values must correspond with one or more option(s) defined numerically (between 0 and 15) in the TACACS+ configuration file. - `-opl { OperPrivilege }` specifies the level to which operator users are able to configure the TACACS+ server. Values must correspond with one or more option(s) defined numerically (between 0 and 15) in the TACACS+ configuration file. - `-gpl { GuestPrivilege }` specifies the level to which guest users are able to configure the TACACS+ server. Values must correspond with one or more option(s) defined numerically (between 0 and 15) in the TACACS+ configuration file.	
telnet `{ dest }`	Opens a telnet session. Press **Ctrl-C** to close the session.	Guest, Operator, Admin

Command	Description	Authorized Users
	Optional and/or required parameters include: • { *dest* }is the server's IP address	
tftp { *address* } [put | get] { *source* } { *target* }	Opens a TFTP session. Press **Ctrl-C** to close the session. Optional and/or required parameters include: • { *address* }is the IP address of the remote TFTP server • `put` indicates TFTP will be uploading the source file to replace the destination file • `get` indicates TFTP will be downloading the source file to replace the destination file • { *source* }is the name of the source file • { *target* }is the name of the file that will be replaced	Admin
trace	Starts event tracing. Run **trace ?** for more help.	Operator, Admin
type { *filename* }	Displays the contents of a text file. Optional and/or required parameters include: • { *filename* }is the name of the file to be read	Guest, Operator, Admin
usermod { -b | -r { *username* } | { *old_user_name* } { *new_user_name* } }	A set of commands to display, remove and change existing usernames. Optional and/or required parameters include: • `-b` browses through the existing user names in RUGGEDCOM ROS. • `-r {` *username* `}` removes a specified user name to disable the account • { *old_user_name* } and { *new_user_name* } define the user name to be changed This command is unavailable in Telnet sessions.	Admin
version	Prints the software version.	Guest, Operator, Admin
xmodem { send | receive } { *filename* }	Opens an XModem session. Optional and/or required parameters include: • `send` sends the file to the client. • `receive` receives the file from the client. • { *filename* }is the name of the file to be read.	Operator, Admin

2.5.2 Tracing Events

The CLI trace command provides a means to trace the operation of various protocols supported by the device. Trace provides detailed information, including STP packet decodes, IGMP activity and MAC address displays.

Note
Tracing has been designed to provide detailed information to expert users. Note that all tracing is disabled upon device startup.

To trace an event, do the following:

1. Log in to the device as an admin user and access the CLI shell. For more information about accessing the CLI shell, refer to "Using the Command Line Interface (Page 17)".
2. Determine the protocols and associated options available by typing:

   trace ?

   If an option such as `allon` or `alloff` is required, determine which options are available for the desired protocol by typing:

   trace { *protocol* } ?

   Note
   If required, expand the trace scope by stringing protocols and their associated options together using a vertical bar (|).

3. Select the type of trace to run by typing:

   trace { *protocol* } { *option* }

   Where:

   - { *protocol* } is the protocol to trace
   - { *option* } is the option to use during the trace

   Example:

   ```
   >trace transport allon
                         TRANSPORT: Logging is enabled
   ```

4. Start the trace by typing:

   trace

2.5.3 Executing Commands Remotely via RSH

The Remote Shell (RSH) facility can be used from a workstation to cause the product to act upon commands as if they were entered at the CLI prompt. The syntax of the RSH command is usually of the form:

rsh { *ipaddr* } -l { *auth_token* } { *command_string* }

Where:

- { *ipaddr* } is the address or resolved name of the device.
- { *auth_token* } is the user name (i.e. guest, operator or admin) and corresponding password separated by a comma. For example, *admin,secret*.
- { *command_string* } is the RUGGEDCOM ROS CLI command to execute.

Note

The access level (corresponding to the user name) selected must support the given command.

Note
Any output from the command will be returned to the workstation submitting the command. Commands that start interactive dialogs (such as **`trace`**) cannot be used.

2.5.4 Using SQL Commands

RUGGEDCOM ROS provides an *SQL-like* command facility that allows expert users to perform several operations not possible under the traditional Web or CLI interface. For instance:

- Restoring the contents of a specific table, but not the whole configuration, to their factory defaults.
- Search tables in the database for specific configurations.
- Make changes to tables predicated upon existing configurations.

When combined with RSH, SQL commands provide a means to query and configure large numbers of devices from a central location.

Note
For a list of parameters available under the **`sql`** command, refer to "Available CLI Commands (Page 17)".

Note
Read/write access to tables containing passwords or shared secrets is unavailable using SQL commands.

2.5.4.1 Finding the Correct Table

Many SQL commands operate upon specific tables in the database, and require the table name to be specified. Navigating the menu system in the console interface to the desired menu and pressing **Ctrl-Z** displays the name of the table. The menu name and the corresponding database table name will be cited.

Another way to find a table name is to type the following in the CLI:

```
sql info tables
```

This command also displays menu names and their corresponding database table names depending upon the features supported by the device. For example:

```
Table Description
-------------------------------------------------------------------------------
alarms Alarms
cpuDiags CPU Diagnostics
ethPortCfg Port Parameters
ethPortStats Ethernet Statistics
ethPortStatus Port Status
```

```
ipCfg IP Services
```

2.5.4.2 Retrieving Information

The following describes various methods for retrieving information about tables and parameters.

Retrieving Information from a Table

Use the following command to display a summary of the parameters within a table, as well as their values:

sql select from { *table* }

Where:

- { *table* } is the name of the table

Example:

```
>sql select from ipAddrtable

IP Address      Subnet          IfIndex    IfStats    IfTime     IfName
172.30.146.88   255.255.224.0   1001       17007888   2994       vlan1

1 records selected
```

Retrieving Information About a Parameter from a Table

Use the following command to retrieve information about a specific parameter from a table:

Note
The parameter name must be the same as it is displayed in the menu system, unless the name contains spaces (e.g. ip address). Spaces must be replaced with underscores (e.g. ip_address) or the parameter name must be wrapped in double quotes (e.g. "ip address").

sql select { *parameter* } from { *table* }

Where:

- { *parameter* } is the name of the parameter
- { *table* } is the name of the table

Example:

```
>sql select "ip address" from ipSwitchIfCfg

IP Address
192.168.0.1

1 records selected
```

Retrieving Information from a Table Using the Where Clause

Use the following command to display specific parameters from a table that have a specific value:

```
sql select from { table } where { parameter } = { value }
```

Where:

- { *table* } is the name of the table
- { *parameter* } is the name of the parameter
- { *value* } is the value of the parameter

Example:

```
>sql select from ethportcfg where media = 1000T

Port Name            ifName          Media       State    AutoN Speed Dupx  FlowCtrl
 LFI Alarm
   1  Port 1          1             1000T       Enabled  On    Auto  Auto  Off
 Off On
   2  Port 2          2             1000T       Enabled  On    Auto  Auto  Off
 Off On
   3  Port 3          3             1000T       Enabled  On    Auto  Auto  Off
 Off On
   4  Port 4          4             1000T       Enabled  On    Auto  Auto  Off
 Off On

4 records selected
```

Further refine the results by using `and` or `or` operators:

```
sql select from { table } where { parameter } = { value }
{ and | or } { parameter } = { value }
```

Where:

- { *table* } is the name of the table
- { *parameter* } is the name of the parameter
- { *value* } is the value of the parameter

Example:

```
>sql select from ethportcfg where media = 1000T and State = enabled

Port Name            ifName          Media       State    AutoN Speed Dupx  FlowCtrl
 LFI Alarm
   1  Port 1          1             1000T       Enabled  On    Auto  Auto  Off
 Off on
   2  Port 2          2             1000T       Enabled  On    Auto  Auto  Off
 Off On
   3  Port 3          3             1000T       Enabled  On    Auto  Auto  Off
 Off On
   4  Port 4          4             1000T       Enabled  On    Auto  Auto  Off
 Off On

4 records selected
```

2.5.4.3 Changing Values in a Table

Use the following command to change the value of parameters in a table:

sql update { *table* } set { *parameter* } = { *value* }

Where:

- { *table* } is the name of the table
- { *parameter* } is the name of the parameter
- { *value* } is the value of the parameter

Example:

```
>sql update iplcfg set IP_Address_Type = static
1 records updated
```

Conditions can also be included in the command to apply changes only to parameters that meet specific criteria. In the following example, flow control is enabled on ports that are operating in 100 Mbps full-duplex mode with flow control disabled:

```
>sql update ethportcfg set FlowCtrl = Off where ( Media = 100TX and FlowCtrl = On )
2 records updated
```

2.5.4.4 Resetting a Table

Use the following command to reset a table back to its factory defaults:

sql default into { *table* }

Where:

- { *table* } is the name of the table

2.5.4.5 Using RSH and SQL

The combination of remote shell scripting and SQL commands offers a means to interrogate and maintain a large number of devices. Consistency of configuration across sites may be verified by this method. The following presents a simple example where the devices to interrogate are drawn from the file `Devices`:

```
C:> type Devices
10.0.1.1
10.0.1.2

C:\> for /F %i in (devices) do rsh %i -l admin,admin sql select from ipAddrtable

C:\>rsh 10.0.1.1 -l admin,admin sql select from ipAddrtable

IP Address      Subnet          IfIndex    IfStats    IfTime     IfName
192.168.0.31    255.255.255.0   1001       274409096  2218       vlan1

1 records selected

C:\>rsh 10.0.1.2 -l admin,admin sql select from ipAddrtable
0 records selected
C:\
```

2.6 Selecting Ports in RUGGEDCOM ROS

Many features in ROS can be configured for one or more ports on the device. The following describes how to specify a single port, a range of ports, or all ports.

Select a single port by specifying the port number:

2

Select a range of ports using a dash (-) between the first port and the last port in the list:

1-4

Select multiple ports by defining a comma-separated list:

1,4,6,9

Use the *`All`* option to select all ports in the device, or, if available, use the *`None`* option to select none of the ports.

2.7 Managing the Flash File System

This section describes how to manage the file system.

2.7.1 Viewing a List of Flash Files

To view a list of files currently stored in Flash memory, do the following:

1. Log in to the device as an admin user and access the CLI shell. For more information about accessing the CLI shell, refer to "Using the Command Line Interface (Page 17)".
2. Type **`flashfiles`**. A list of files currently in Flash memory is displayed, along with their locations and the amount of memory they consume. For example:

```
>flashfiles
-----------------------------------------------------------------
Filename              Base    Size   Sectors      Used
-----------------------------------------------------------------
boot.bin          00000000 110000     0-16   1095790
main.bin          00110000 140000    17-36   1258403
syslog.txt        00260000 140000    38-57     19222
.
.
.
-----------------------------------------------------------------
```

2.7.2 Viewing Flash File Details

To view the details of a file currently stored in Flash memory, do the following:

1. Log in to the device as an admin user and access the CLI shell. For more information about accessing the CLI shell, refer to "Using the Command Line Interface (Page 17)".

2. Display information about a file by typing:

   flashfiles info { *filename* }

   Where:

   - { *filename* } is the name of the file stored in Flash memory

   Details, similar to the following, are displayed.

```
>flashfiles info main.bin

Flash file information for main.bin:
Header version   : 4
Platform         : ROS-CF52
File name        : main.bin
Firmware version : v4.3.0
Build date       : Sep 27 2014 15:50
File length      : 2624659
Board IDs        :  3d
Header CRC       : 73b4
Header CRC Calc  : 73b4
Body CRC         : b441
Body CRC Calc    : b441
```

2.7.3 Defragmenting the Flash File System

The flash memory is defragmented automatically whenever there is not enough memory available for a binary upgrade. However, fragmentation can occur whenever a new file is uploaded to the unit. Fragmentation causes sectors of available memory to become separated by ones allocated to files. In some cases, the total available memory might be sufficient for a binary upgrade, but that memory may not be available in one contiguous region.

To defragment the flash memory, do the following:

1. Log in to the device as an admin user and access the CLI shell. For more information about accessing the CLI shell, refer to "Using the Command Line Interface (Page 17)".
2. Defragment the flash memory by typing:

   flashfiles defrag

2.8 Accessing BIST Mode

BIST (Built-In-Self-Test) mode is used by service technicians to test and configure internal functions of the device. It should only be accessed for troubleshooting purposes.

⚠ **CAUTION**

Mechanical hazard – risk of damage to the device

Excessive use of BIST functions may cause increase wear on the device, which may void the warranty. Avoid using BIST functions unless instructed by a Siemens Customer Support representative.

To access BIST mode, do the following:

⚠ **NOTICE**

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

1. Disconnect the device from the network.
2. Connect to RUGGEDCOM ROS through the RS-232 console connection and a terminal application. For more information, refer to "Connecting Directly (Page 33)".
3. Reset the device. For more information, refer to "Resetting the Device (Page 98)".
4. During the boot up sequence, press **Ctrl-C** when prompted. The command prompt for BIST appears.

   ```
   >
   ```

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

3 Getting Started

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

⚠ **NOTICE**

Siemens recommends the following actions before commissioning the device:

- Replace the factory-provisioned, self-signed SSL certificate with one signed by a trusted Certificate Authority (CA)
- Configure the SSH client to use *diffie-hellman-group14-sha1* or better

3.1 Connecting to ROS

This section describes the various methods for connecting to the device.

3.1.1 Default IP Address

The default IP address for the device is 192.168.0.1/24.

3.1.2 Connecting Directly

RUGGEDCOM ROS can be accessed through a direct platform="RSG907R;RSG908C;RSG909R;RSG910C;RST2228">USB console connection for management and troubleshooting purposes. A console connection provides access to the console interface and CLI.

Using the Console Port

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

1. Connect a workstation (either a terminal or computer running terminal emulation software) to the console port on the device. For more information about the console port, refer to the *RS900W Installation Guide*.

   Note
   The baud rate for the device is printed on the chassis exterior near the console port.

2. Configure the workstation as follows:
   - Speed (baud): 57600
   - Data Bits: 8
   - Parity: None
   - Flow Control: Off
   - Terminal ID: VT100
   - Stop Bit: 1
3. Connect to the device. Once the connection is established, the login form appears. For more information about logging in to the device, refer to "Logging In (Page 12)".

3.1.3 Connecting Remotely

RUGGEDCOM ROS can be accessed securely and remotely either through a Web browser, terminal or workstation running terminal emulation software.

Using a Web Browser

Web browsers provide a secure connection to the Web interface for RUGGEDCOM ROS using the SSL (Secure Socket Layer) communication method. SSL encrypts traffic exchanged with its clients.

The RUGGEDCOM ROS Web server guarantees that all communications with the client are private. If a client requests access through an insecure HTTP port, the client is automatically rerouted to the secure port. Access to the Web server through SSL will only be granted to clients that provide a valid user name and password.

To establish a connection through a Web browser, do the following:

1. On the workstation being used to access the device, configure an Ethernet port to use an IP address falling within the subnet of the device. The default IP address is 192.168.0.1/24.

   For example, to configure the device to connect to one of the available Ethernet ports, assign an IP address to the Ethernet port on the workstation in the range of 192.168.0.3 to 192.168.0.254.
2. Open a Web browser. For a list of recommended Web browsers, refer to "System Requirements (Page xii)".

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

3. In the address bar, type the IP address for the port that is connected to the network. For example, to access the device using its factory default IP address, type `https://192.168.0.1` and press **Enter**. Once the connection is established, the login screen for the Web interface appears.

   For more information about logging in to the device, refer to "Logging In (Page 12)". For more information about the Web interface, refer to "Using the Web Interface (Page 14)".

Using a Terminal or Terminal Emulation Software

A terminal or computer running terminal emulation software provides access to the console interface for RUGGEDCOM ROS through a Telnet, RSH (Remote Shell) or SSH (Secure Shell) service.

Note
IP services can be restricted to control access to the device. For more information, refer to "Configuring IP Services (Page 81)".

To establish a connection through a terminal or terminal emulation software, do the following:

1. Select the service (i.e. Telnet, RSH or SSH).
2. Enter the IP address for the port that is connected to the network.
3. Connect to the device. Once the connection is established, the login form appears. For more information about logging in to the device, refer to "Logging In (Page 12)".

3.2 Configuring a Basic Network

To configure a basic network, do the following:

1. Connect a computer to one of the switch ports of the device and configure the computer to be on the same subnet as the port.
2. Configure the computer to use the address of VLAN1 as the default gateway.
3. Connect a second computer to a different switch port of the same device, and configure the computer to be on the same subnet as the port.
4. Configure the second computer to use the address of VLAN1 as the default gateway. The default IP address is 192.168.0.1.
5. Make sure both computers connected to the device can ping one another.

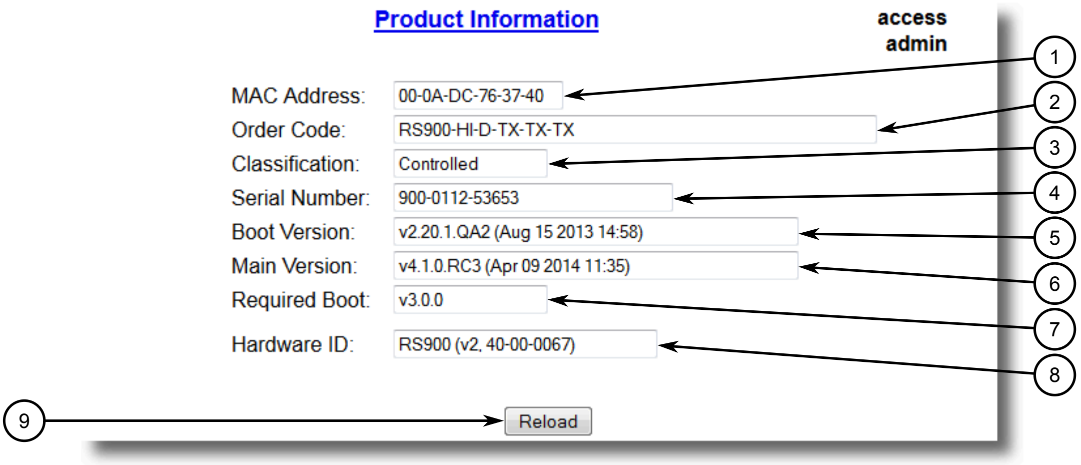
4 Device Management

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

4.1 Viewing Product Information

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

To view information about the device, navigate to ***Diagnostics » View Product Information***. The **Product Information** form appears.



Product Information

access
admin

MAC Address:	00-0A-DC-76-37-40
Order Code:	RS900-HI-D-TX-TX-TX
Classification:	Controlled
Serial Number:	900-0112-53653
Boot Version:	v2.20.1.QA2 (Aug 15 2013 14:58)
Main Version:	v4.1.0.RC3 (Apr 09 2014 11:35)
Required Boot:	v3.0.0
Hardware ID:	RS900 (v2, 40-00-0067)

① MAC Address Box
② Order Code Box
③ Classification Box
④ Serial Number Box
⑤ Boot Version Box
⑥ Main Version Box
⑦ Required Boot Box
⑧ Hardware ID Box
⑨ Descr Box
⑩ Reload Button

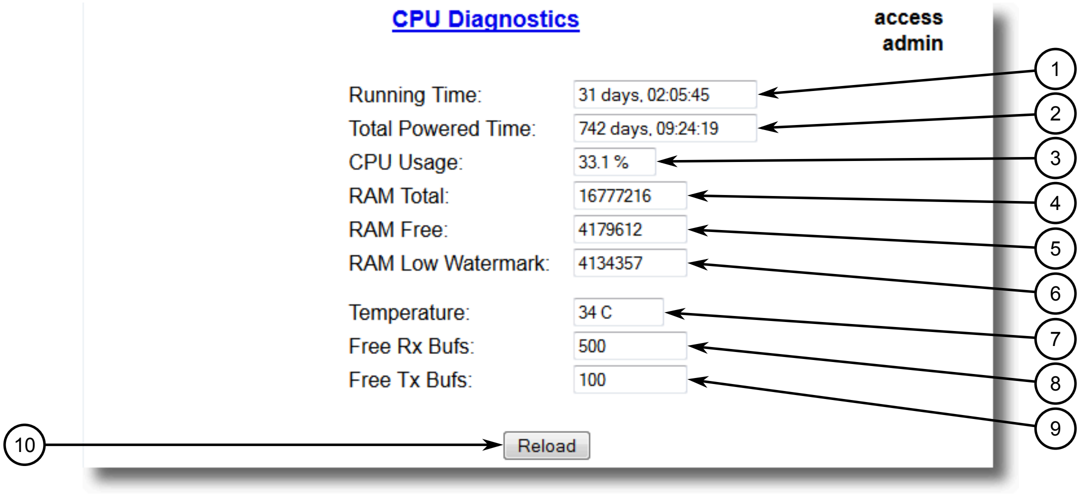
Figure 4.1 Product Information Form (Example)

This screen displays the following information:

Parameter	Description
`MAC Address`	**Synopsis:** ##-##-##-##-##-## where ## ranges 0 to FF Shows the unique MAC address of the device.
`Order Code`	**Synopsis:** A string 57 characters long Shows the order code of the device.
`Classification`	**Synopsis:** A string 15 characters long Provides system classification. The value `Controlled` indicates the main firmware is a Controlled release. The value `Non-Controlled` indicates the main firmware is a Non-Controlled release.
`Serial Number`	**Synopsis:** A string 31 characters long Shows the serial number of the device.
`Boot Version`	**Synopsis:** A string 47 characters long Shows the version and the build date of the boot loader software.
`Main Version`	**Synopsis:** A string 47 characters long Shows the version and build date of the main operating system software.
`Required Boot`	**Synopsis:** A string 15 characters long Shows the minimum boot software loader version required by running main.
`Hardware ID`	**Synopsis:** [RSMCPU (40-00-0008 Rev B1) | RSMCPU2 (40-00-0026 Rev A1) | RS400 (40-00-0010 Rev B2) | RMC30 | RS900 (40-00-0025 Rev B1) | RS900 (40-00-0032 Rev B1) | RS1600M | RS400 (40-00-0010 Rev C1) | RSG2100 | RS900G | RSG2200 | RS969 | RS900 (v2, 40-00-0066) | RS900 (v2, 40-00-0067) | RS416 (40-00-0078) | RMC30 (v2) | RS930 (40-00-0089) | RS969 (v2, 40-00-0090) | RS910 (40-00-0091-001 Rev A) | RS920L (40-00-0102-001 Rev A) | RS940G (40-00-0097-000 Rev A) | RSi80X series CPU board | RSG2300 | RS416v2 | ...] Shows the type, part number, and revision level of the hardware.

4.2 Viewing CPU Diagnostics

To view CPU diagnostic information useful for troubleshooting hardware and software performance, navigate to ***Diagnostics » View CPU Diagnostics***. The **CPU Diagnostics** form appears.



CPU Diagnostics

access
admin

Running Time: 31 days, 02:05:45

Total Powered Time: 742 days, 09:24:19

CPU Usage: 33.1 %

RAM Total: 16777216

RAM Free: 4179612

RAM Low Watermark: 4134357

Temperature: 34 C

Free Rx Bufs: 500

Free Tx Bufs: 100

① Running Time Box
② Total Powered Time Box
③ CPU Usage Box
④ RAM Total Box
⑤ RAM Free Box
⑥ RAM Low Watermark Box
⑦ Temperature Box
⑧ Free Rx Bufs Box
⑨ Free Tx Bufs Box
⑩ Reload Button

Figure 4.2 CPU Diagnostics Form

This screen displays the following information:

Parameter	Description
`Running Time`	**Synopsis:** DDDD days, HH:MM:SS The amount of time since the device was last powered on.
`Total Powered time`	**Synopsis:** DDDD days, HH:MM:SS The cumulative powered up time of the device.
`CPU Usage`	**Synopsis:** An integer between 0.0 and 100.0 The percentage of available CPU cycles used for device operation as measured over the last second.
`RAM Total`	**Synopsis:** An integer between 0 and 4294967295 The total size of RAM in the system.
`RAM Free`	**Synopsis:** An integer between 0 and 4294967295 The total size of RAM still available.
`RAM Low Watermark`	**Synopsis:** An integer between 0 and 4294967295 The size of RAM that have never been used during the system run-time.

Parameter	Description
`Temperature`	**Synopsis:** An integer between -32768 and 32767 The temperature on CPU board.
`Free Rx Bufs`	**Synopsis:** An integer between 0 and 4294967295 Free Rx Buffers.
`Free Tx Bufs`	**Synopsis:** An integer between 0 and 4294967295 Free Tx Buffers.

4.3 Restoring Factory Defaults

The device can be completely or partially restored to its original factory default settings. Excluding groups of parameters from the factory reset, such as those that affect basic connectivity and SNMP management, is useful when communication with the device is still required during the reset.

The following categories are not affected by a selective configuration reset:

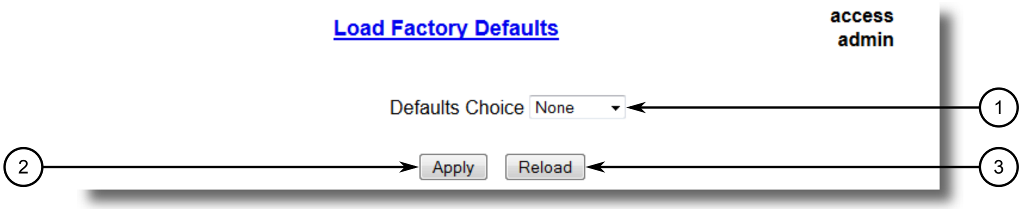
- IP Interfaces
- IP Gateways
- SNMP Users
- SNMP Security to Group Maps
- SNMP Access
- RUGGEDCOM Discovery Protocol™ (RCDP)

In addition, the following categories are not affected by a full or selective configuration reset:

- Time Zone
- DST Offset
- DST Rule

To restore factory defaults, do the following:

1. Navigate to ***Diagnostics » Load Factory Defaults***. The **Load Factory Defaults** form appears.



① Defaults Choice List
② Apply Button
③ Reload

Figure 4.3 Load Factory Defaults Form

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

Note
If the VLAN ID for the Management IP interface is not `1`, setting **Defaults Choice** to `Selected` will automatically set it to `1`.

Parameter	Description
`Defaults Choice`	**Synopsis:** [None | Selected | All] Setting some records like IP Interfaces management interface, default gateway, SNMP settings to default value would cause switch not to be accessible with management applications. This parameter allows user to choose to load defaults to Selected tables, which would preserve configuration for tables that are critical for switch management applications, or to force All tables to default settings.

3. Click **Apply**.

4.4 Uploading/Downloading Files

Files can be transferred between the device and a host computer using any of the following methods:

- Xmodem using the CLI shell over a Telnet or RS-232 console session
- TFTP client using the CLI shell in a console session and a remote TFTP server
- TFTP server from a remote TFTP client
- SFTP (secure FTP over SSH) from a remote SFTP client

⚠ **NOTICE**

Scripts can be used to automate the management of files on the device. However, depending on the size of the target file(s), a delay between any concurrent write and read commands may be required, as the file may not have been fully saved before the read command is issued. A general delay of five seconds is recommended, but testing is encouraged to optimize the delay for the target file(s) and operating environment.

Note

The contents of the internal file system are fixed. New files and directories cannot be created, and existing files cannot be deleted. Only the files that can be uploaded to the device can be overwritten.

Files that may need to be uploaded or downloaded include:

- `main.bin` – the main RUGGEDCOM ROS application firmware image
- `boot.bin` – the boot loader firmware image
- `fpga.xsvf` – the FPGA firmware binary image
- `config.csv` – the complete configuration database, in the form of a comma-delimited ASCII text file
- `factory.txt` – contains the MAC address, order code and serial number. Factory data must be signed.
- `banner.txt` – contains text that appears on the login screen
- `ssl.crt` – the SSL certificate. Contains both the SSL certificate and the corresponding RSA private key file.
- `ssh.keys` – the SSH keys for the device

4.4.1 Uploading/Downloading Files Using XMODEM

To updload or download a file using XMODEM, do the following:

Note

This method requires a host computer that has terminal emulation or Telnet software installed, and the ability to perform XMODEM transfers.

1. Establish a connection between the device and the host computer. For more information, refer to "Connecting to ROS (Page 33)".
2. Log in to the device as an admin user and access the CLI shell. For more information about accessing the CLI shell, refer to "Using the Command Line Interface (Page 17)".

3. At the CLI prompt, type:

   xmodem [send | receive] { *filename* }

   Where:

   - `send` sends the file to the host computer
   - `receive` pulls the file from the host computer
   - { *filename* } is the name of the file (i.e. main.bin)

   Note
   If available in the terminal emulation or Telnet software, select the *XModem 1K* protocol for transmission over the standard *XModem* option.

4. When the device responds with `Press Ctrl-X to cancel`, launch the XMODEM transfer from the host computer. The device will indicate when the transfer is complete.

   Note
   When SSH is used to establish a connection between the RS900W device and the host computer, XMODEM can take a long time to download an image.

   The following is an example from the CLI shell of a successful XMODEM file transfer:

```
>xmodem receive main.bin
Press Ctrl-X to cancel
Receiving data now ...C
Received 1428480 bytes. Closing file main.bin ...
main.bin transferred successfully
```

5. If the file has been uploaded, reset the device. For more information, refer to "Resetting the Device (Page 98)"

4.4.2 Uploading/Downloading Files Using a TFTP Client

To upload or download a file using a TFTP client, do the following:

⚠ **NOTICE**

TFTP does not define an authentication scheme. Any use of the TFTP client or server is considered highly insecure.

Note
This method requires a TFTP server that is accessible over the network.

1. Identify the IP address of the computer running the TFTP server.
2. Establish a connection between the device and the host computer. For more information, refer to "Connecting to ROS (Page 33)".

3. Log in to the device as an admin user and access the CLI shell. For more information about accessing the CLI shell, refer to "Using the Command Line Interface (Page 17)".
4. At the CLI prompt, type:

   ```
   tftp  { address }  [ get | put ]  { source-filename }
   { destination-filename }
   ```

   Where:

   - `get` copies files from the host computer to the device
   - `put` copies files from the device to the host computer
   - `{ address }` is the IP address of the computer running the TFTP server
   - `{ source-filename }` is the name of the file to be transferred
   - `{ destination-filename }` is the name of the file (on the device or the TFTP server) that will be replaced during the transfer

   The following is an example of a successful TFTP client file transfer:

   ```
   >tftp 10.0.0.1 get ROS-CF52_Main_v4.3.0.bin main.bin
   TFTP CMD: main.bin transfer ok. Please wait, closing file ...
   TFTP CMD: main.bin loading successful.
   ```
5. If the file has been uploaded, reset the device. For more information, refer to "Resetting the Device (Page 98)"

4.4.3 Uploading/Downloading Files Using a TFTP Server

To updload or download a file using a TFTP server, do the following:

⚠ NOTICE

TFTP does not define an authentication scheme. Any use of the TFTP client or server is considered highly insecure.

Note

This method requires a host computer that has TFTP server software installed.

⚠ NOTICE

Interaction with TFTP servers is strictly controlled within the device to prevent unauthorized access. Make sure the device is configured to accept the TFTP connection. For more information, refer to "Configuring IP Services (Page 81)".

1. Establish a connection between the device and the host computer. For more information, refer to "Connecting to ROS (Page 33)".

2. Initialize the TFTP server on the host computer and launch the TFTP transfer. The server will indicate when the transfer is complete.

   The following is an example of a successful TFTP server exchange:

   ```
   C:\>tftp -i 10.1.0.1 put C:\files\ROS-CF52_Main_v4.3.0.bin main.bin
   Transfer successful: 1428480 bytes in 4 seconds, 375617 bytes/s
   ```

3. If the file has been uploaded, reset the device. For more information, refer to "Resetting the Device (Page 98)"

4.4.4 Uploading/Downloading Files Using an SFTP Server

SFTP (Secure File Transfer Protocol) is a file transfer mechanism that uses SSH to encrypt every aspect of file transfer between a networked client and server.

Note
The device does not have an SFTP client and, therefore, can only receive SFTP files from an external source. SFTP requires authentication for the file transfer.

To updload or download a file using an SFTP server, do the following:

Note
This method requires a host computer that has SFTP client software installed.

1. Establish an SFTP connection between the device and the host computer.
2. Launch the SFTP transfer. The client will indicate when the transfer is complete.

   The following is an example of a successful SFTP server exchange:

   ```
   user@host$ sftp admin@ros_ip
   Connecting to ros_ip...
   admin@ros_ip's password:
   sftp> put ROS-CF52_Main_v4.3 .0.bin main.bin
   Uploading ROS-CF52_Main_v4.3 .0.bin to /main.bin
   ROS-CF52_Main_v4.3.0.bin 100% 2139KB 48.6KB/s 00:44sftp> put ROS-
   MPC83_Main_v4.3 .0.bin main.bin
   Uploading ROS-MPC83_Main_v4.3 .bin to /main.bin
   ROS-MPC83_Main_v4.3.0.bin 100% 2139KB 48.6KB/s 00:44
   sftp>
   ```

3. If the file has been uploaded, reset the device. For more information, refer to "Resetting the Device (Page 98)"

4.5 Managing Logs

The crash (`crashlog.txt`) and system (`syslog.txt`) log files contain historical information about events that have occurred during the operation of the device.

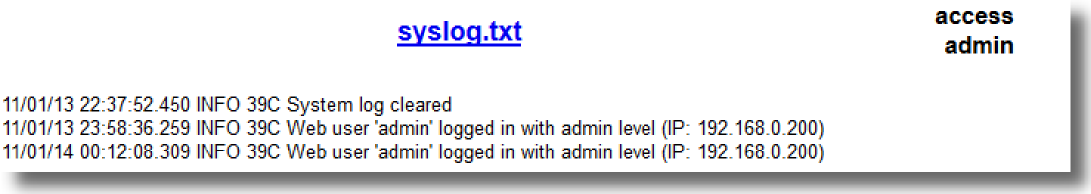
The crash log contains debugging information related to problems that might have resulted in unplanned restarts of the device or which may effect the operation of the device. A file size of 0 bytes indicates that no unexpected events have occurred.

The system log contains a record of significant events including startups, configuration changes, firmware upgrades and database re-initializations due to feature additions. The system log will accumulate information until it is full, holding approximately 2 MB of data.

4.5.1 Viewing Local and System Logs

The local crash and system logs can both be downloaded from the device and viewed in a text editor. For more information about downloading log files, refer to "Uploading/Downloading Files (Page 41)".

To view the system log through the Web interface, navigate to ***Diagnostics » View System Log***. The **syslog.txt** form appears.



```
11/01/13 22:37:52.450 INFO 39C System log cleared
11/01/13 23:58:36.259 INFO 39C Web user 'admin' logged in with admin level (IP: 192.168.0.200)
11/01/14 00:12:08.309 INFO 39C Web user 'admin' logged in with admin level (IP: 192.168.0.200)
```

Figure 4.4 syslog.txt Form

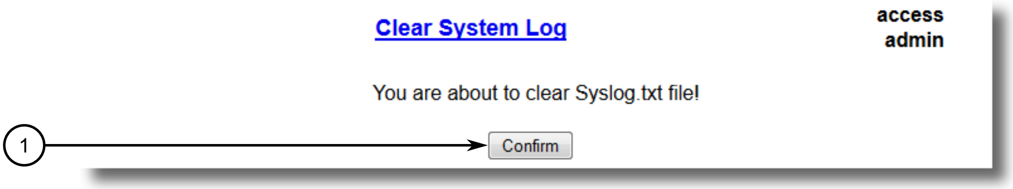
4.5.2 Clearing Local and System Logs

To clear both the local crash and system logs, log in to the CLI shell and type:

```
clearlogs
```

To clear only the local system log, log in to the Web interface and do the following:

1. Navigate to ***Diagnostics » Clear System Log***. The **Clear System Log** form appears.



You are about to clear Syslog.txt file!

① Confirm Button

Figure 4.5 Clear System Log Form

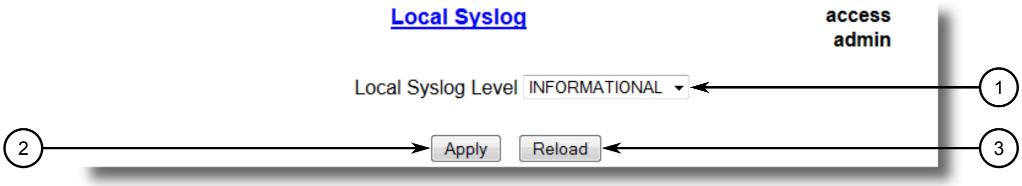
2. Click **Confirm**.

4.5.3 Configuring the Local System Log

To configure the severity level for the local system log, do the following:

Note
For maximum reliability, use remote logging. For more information, refer to "Managing Remote Logging (Page 47)".

1. Navigate to ***Administration » Configure Syslog » Configure Local Syslog***. The **Local Syslog** form appears.



① Local Syslog Level
② Apply Button
③ Reload Button

Figure 4.6 Local Syslog Form

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

Parameter	Description
`Local Syslog Level`	**Synopsis:** [EMERGENCY | ALERT | CRITICAL | ERROR | WARNING | NOTICE | INFORMATIONAL | DEBUGGING] **Default:** INFORMATIONAL The severity of the message that has been generated. Note that the severity level selected is considered the minimum severity level for the system. For example, if ERROR is selected, the system sends any syslog messages generated by Error, Critical, Alert and Emergency.

3. Click **Apply**.

4.5.4 Managing Remote Logging

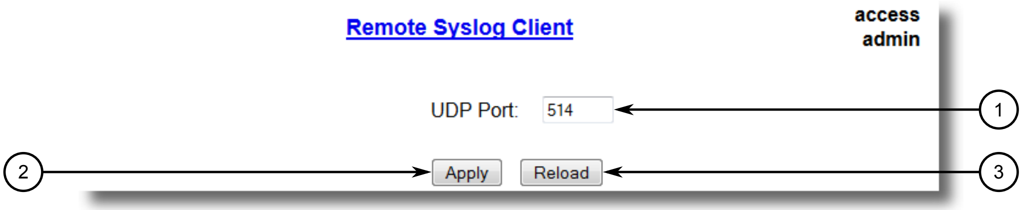
In addition to the local system log maintained on the device, a remote system log can be configured as well to collect important event messages. The syslog client resides on the device and supports up to 5 collectors (or syslog servers).

The remote syslog protocol, defined in RFC 3164, is a UDP/IP-based transport that enables the 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(s).

4.5.4.1 Configuring the Remote Syslog Client

To configure the remote syslog client, do the following:

1. Navigate to ***Administration » Configure Syslog » Configure Remote Syslog Client***. The **Remote Syslog Client** form appears.



① UDP Port
② Apply Button
③ Reload Button

Figure 4.7 Remote Syslog Client Form

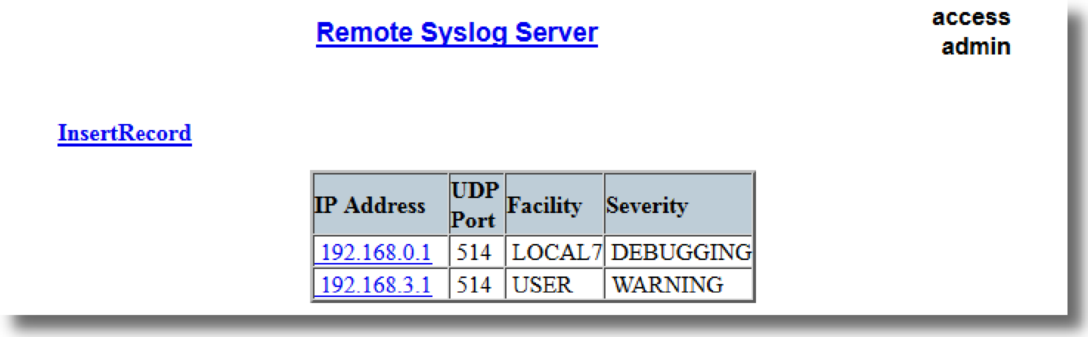
2. Configure the following parameter(s) as required:

Parameter	Description
`UDP Port`	**Synopsis:** An integer between 1025 and 65535 or [514] **Default:** 514 The local UDP port through which the client sends information to the server(s).

3. Click **Apply**.

4.5.4.2 Viewing a List of Remote Syslog Servers

To view a list of known remote syslog servers, navigate to ***Administration » Configure Syslog » Configure Remote Syslog Server***. The **Remote Syslog Server** table appears.



IP Address	UDP Port	Facility	Severity
192.168.0.1	514	LOCAL7	DEBUGGING
192.168.3.1	514	USER	WARNING

Figure 4.8 Remote Syslog Server Table

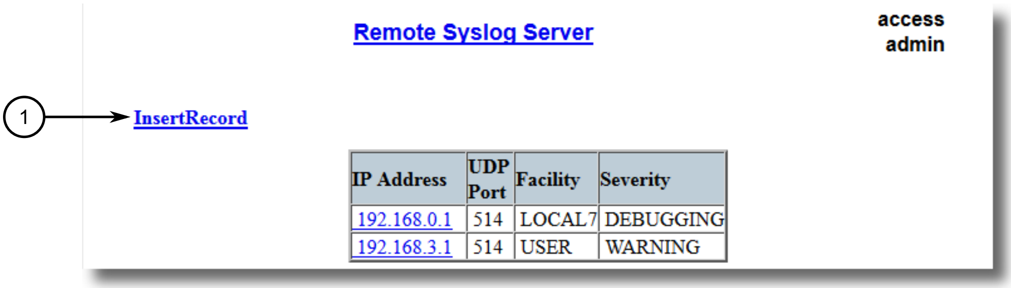
If remote syslog servers have not been configured, add the servers as needed. For more information, refer to "Adding a Remote Syslog Server (Page 49)".

4.5.4.3 Adding a Remote Syslog Server

RUGGEDCOM ROS supports up to 5 remote syslog servers (or collectors). Similar to the local system log, a remote system log server can be configured to log information at a specific severity level. Only messages of a severity level equal to or greater than the specified severity level are written to the log.

To add a remote syslog server to the list of known servers, do the following:

1. Navigate to ***Administration » Configure Syslog » Configure Remote Syslog Server***. The **Remote Syslog Server** table appears.

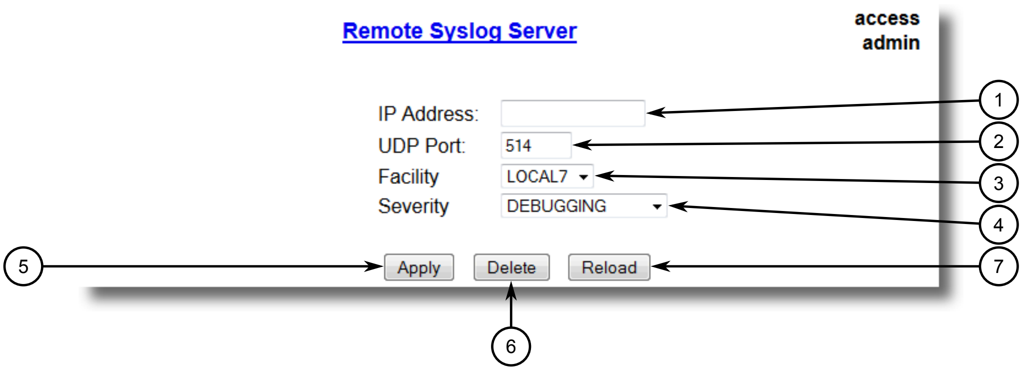


IP Address	UDP Port	Facility	Severity
192.168.0.1	514	LOCAL7	DEBUGGING
192.168.3.1	514	USER	WARNING

① InsertRecord

Figure 4.9 Remote Syslog Server Table

2. Click **InsertRecord**. The **Remote Syslog Server** form appears.


Remote Syslog Server

access
admin

IP Address:
UDP Port: 514
Facility LOCAL7
Severity DEBUGGING

① IP Address Box
② UDP Port Box
③ Facility Box
④ Severity Box
⑤ Apply Button
⑥ Delete Button
⑦ Reload Button

Figure 4.10 Remote Syslog Server Form

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

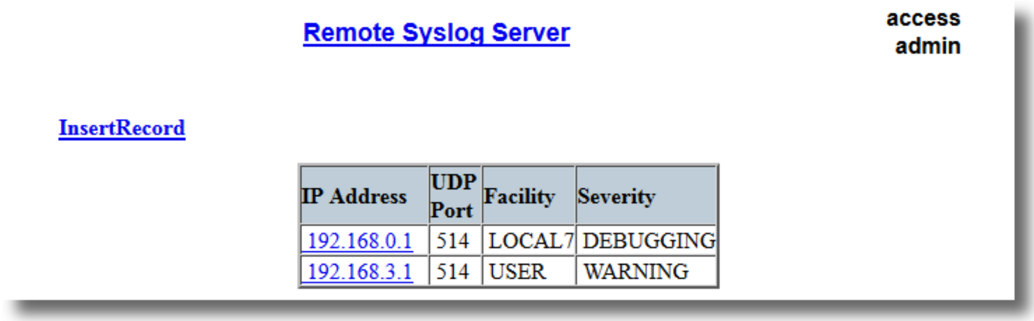
Parameter	Description
`IP Address`	**Synopsis:** ###.###.###.### where ### ranges from 0 to 255 Syslog server IP Address.
`UDP Port`	**Synopsis:** An integer between 1025 and 65535 or [514] **Default:** 514 The UDP port number on which the remote server listens.
`Facility`	**Synopsis:** [USER | LOCAL0 | LOCAL1 | LOCAL2 | LOCAL3 | LOCAL4 | LOCAL5 | LOCAL6 | LOCAL7] **Default:** LOCAL7 Syslog Facility is one information field associated with a syslog message. The syslog facility is the application or operating system component that generates a log message. ROS map all syslog logging information onto a single facility which is configurable by user to facilitate remote syslog server.
`Severity`	**Synopsis:** [EMERGENCY | ALERT | CRITICAL | ERROR | WARNING | NOTICE | INFORMATIONAL | DEBUGGING] **Default:** DEBUGGING The severity level is the severity of the message that has been generated. Please note that the severity level user select is accepted as the minimum severity level for the system. For example, if user selects the severity level as 'Error' then the system send any syslog message originated by Error, Critical, Alert and Emergency.

4. Click **Apply**.

4.5.4.4 Deleting a Remote Syslog Server

To delete a remote syslog server from the list of known servers, do the following:

1. Navigate to ***Administration » Configure Syslog » Configure Remote Syslog Server***. The **Remote Syslog Server** table appears.



Remote Syslog Server

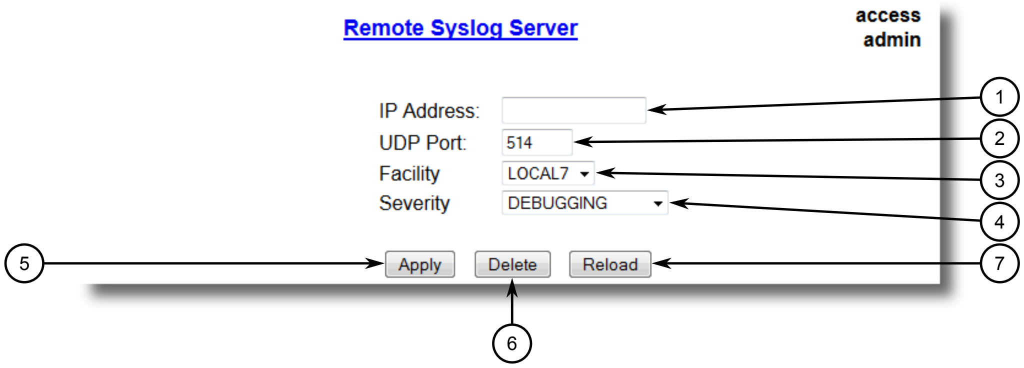
access
admin

InsertRecord

IP Address	UDP Port	Facility	Severity
192.168.0.1	514	LOCAL7	DEBUGGING
192.168.3.1	514	USER	WARNING

Figure 4.11 Remote Syslog Server Table

2. Select the server from the table. The **Remote Syslog Server** form appears.



Remote Syslog Server

access
admin

IP Address:	
UDP Port:	514
Facility	LOCAL7
Severity	DEBUGGING

① IP Address Box
② UDP Port Box
③ Facility Box
④ Severity Box
⑤ Apply Button
⑥ Delete Button
⑦ Reload Button

Figure 4.12 Remote Syslog Server Form

3. Click **Delete**.

4.6 Managing Ethernet Ports

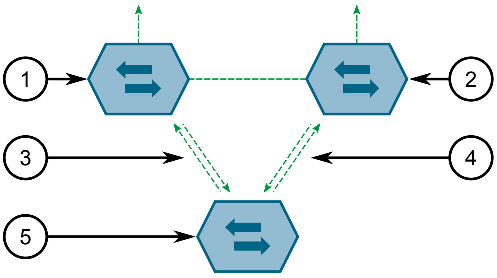
This section describes how to manage Ethernet ports.

Note
For information about configuring remote monitoring for Ethernet ports, refer to "Managing Remote Monitoring (Page 83)".

4.6.1 Controller Protection Through Link Fault Indication (LFI)

Modern industrial controllers often feature backup Ethernet ports used in the event of a link failure. When these interfaces are supported by media (such as fiber) that employ separate transmit and receive paths, the interface can be vulnerable to failures that occur in only one of the two paths.

Consider for instance two switches (A and B) connected to a controller. Switch A is connected to the main port on the controller, while Switch B is connected to the backup port, which is shut down by the controller while the link with Switch A is active. Switch B must forward frames to the controller through Switch A.



① Switch A
② Switch B
③ Main Transmit Path
④ Backup Transmit Path
⑤ Controller

Figure 4.13 Example

If the transmit path from the controller to Switch A fails, Switch A still generates a link signal to the controller through the receive path. The controller still detects the link with Switch A and does not failover to the backup port.

This situation illustrates the need for a notification method that tells a link partner when the link integrity signal has stopped. Such a method natively exists in some link media, but not all.

100Base-TX, 1000Base-T, 1000Base-X	Includes a built-in auto-negotiation feature (i.e. a special flag called Remote Fault Indication is set in the transmitted auto-negotiation signal).

100Base-FX Links	Includes a standard Far-End-Fault-Indication (FEFI) feature defined by the IEEE 802.3 standard for this link type. This feature includes: • **Transmitting FEFI** Transmits a modified link integrity signal in case a link failure is detected (i.e. no link signal is received from the link partner) • **Detecting FEFI** Indicates link loss in case an FEFI signal is received from the link partner
10Base-FL LInks	No standard support.

10Base-FL links do not have a native link partner notification mechanism and FEFI support in 100Base-FX links is optional according to the IEEE 802.3 standard, which means that some links partners may not support it.

Siemens offers an advanced Link-Fault-Indication (LFI) feature for the links that do not have a native link partner notification mechanism. With LFI enabled, the device bases the generation of a link integrity signal upon its reception of a link signal. In the example described previously, if switch A fails to receive a link signal from the controller, it will stop generating a link signal. The controller will detect the link failure and failover to the backkup port.

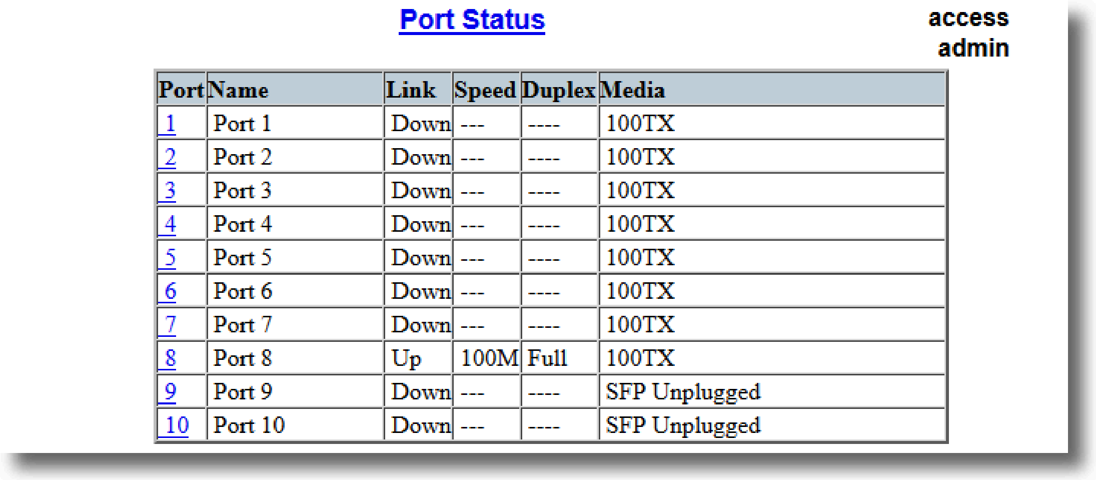
⚠ **NOTICE**

If both link partners have the LFI feature, it *must not* be enabled on both sides of the link. If it is enabled on both sides, the link will never be established, as each link partner will be waiting for the other to transmit a link signal.

The switch can also be configured to flush the MAC address table for the controller port. Frames destined for the controller will be flooded to Switch B where they will be forwarded to the controller (after the controller transmits its first frame).

4.6.2 Viewing the Status of Ethernet Ports

To view the current status of each Ethernet port, navigate to ***Ethernet Ports » View Port Status***. The **Port Status** table appears.



Port Status

access
admin

Port	Name	Link	Speed	Duplex	Media
1	Port 1	Down	---	----	100TX
2	Port 2	Down	---	----	100TX
3	Port 3	Down	---	----	100TX
4	Port 4	Down	---	----	100TX
5	Port 5	Down	---	----	100TX
6	Port 6	Down	---	----	100TX
7	Port 7	Down	---	----	100TX
8	Port 8	Up	100M	Full	100TX
9	Port 9	Down	---	----	SFP Unplugged
10	Port 10	Down	---	----	SFP Unplugged

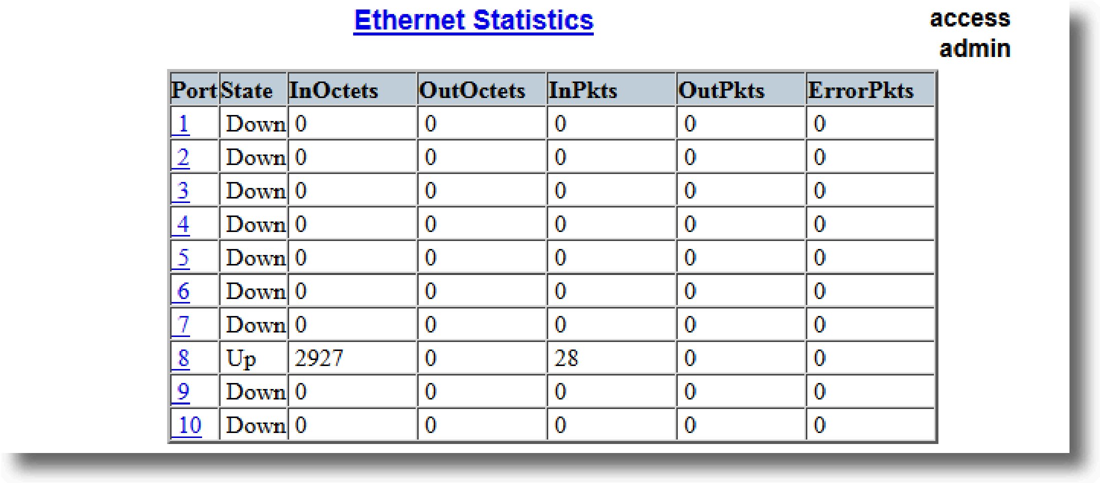
Figure 4.14 Port Status Table

This table displays the following information:

Parameter	Description
`Port`	**Synopsis:** 1 to maximum port number The port number as seen on the front plate silkscreen of the switch.
`Name`	**Synopsis:** A string 15 characters long A descriptive name that may be used to identify the device conected on that port.
`Link`	**Synopsis:** [---- | Down | Up] The port's link status.
`Speed`	**Synopsis:** [--- | 10M | 100M | 1G | 10G] The port's current speed.
`Duplex`	**Synopsis:** [---- | Half | Full] The port's current duplex status.

4.6.3 Viewing Statistics for All Ethernet Ports

To view statistics collected for all Ethernet ports, navigate to ***Ethernet Stats » View Ethernet Statistics***. The **Ethernet Statistics** table appears.



Ethernet Statistics

access
admin

Port	State	InOctets	OutOctets	InPkts	OutPkts	ErrorPkts
1	Down	0	0	0	0	0
2	Down	0	0	0	0	0
3	Down	0	0	0	0	0
4	Down	0	0	0	0	0
5	Down	0	0	0	0	0
6	Down	0	0	0	0	0
7	Down	0	0	0	0	0
8	Up	2927	0	28	0	0
9	Down	0	0	0	0	0
10	Down	0	0	0	0	0

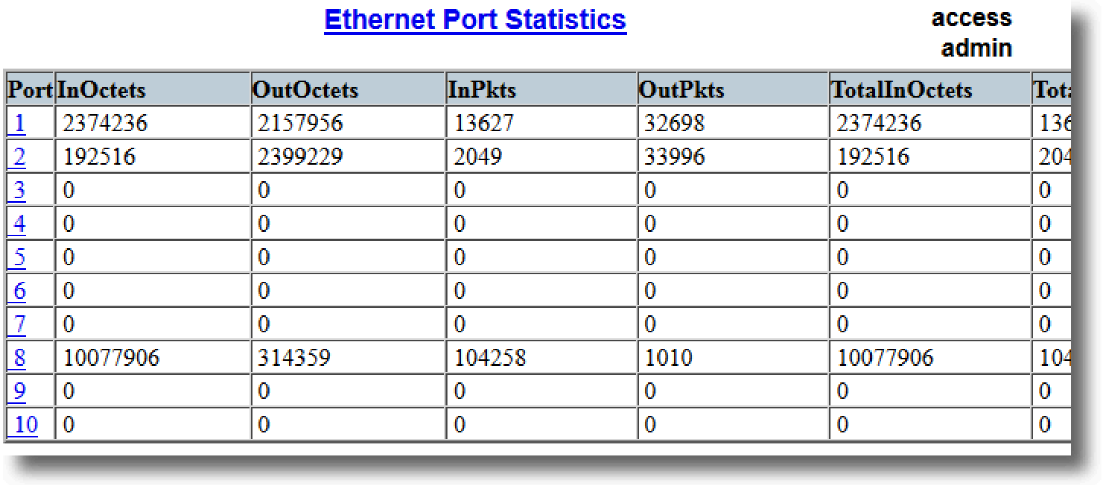
Figure 4.15 Ethernet Statistics Table

This table displays the following information:

Parameter	Description
`Port`	**Synopsis:** 1 to maximum port number The port number as seen on the front plate silkscreen of the switch.
`State`	**Synopsis:** [---- | Down | Up]
`InOctets`	**Synopsis:** An integer between 0 and 4294967295 The number of octets in received good packets (Unicast+Multicast+Broadcast) and dropped packets.
`OutOctets`	**Synopsis:** An integer between 0 and 4294967295 The number of octets in transmitted good packets.
`InPkts`	**Synopsis:** An integer between 0 and 4294967295 The number of received good packets (Unicast+Multicast+Broadcast) and dropped packets.
`OutPkts`	**Synopsis:** An integer between 0 and 4294967295 The number of transmitted good packets.
`ErrorPkts`	**Synopsis:** An integer between 0 and 4294967295 The number of any type of erroneous packet.

4.6.4 Viewing Statistics for Specific Ethernet Ports

To view statistics collected for specific Ethernet ports, navigate to ***Ethernet Stats » View Ethernet Port Statistics***. The **Ethernet Port Statistics** table appears.



Ethernet Port Statistics

access
admin

Port	InOctets	OutOctets	InPkts	OutPkts	TotalInOctets	Tot
1	2374236	2157956	13627	32698	2374236	136
2	192516	2399229	2049	33996	192516	204
3	0	0	0	0	0	0
4	0	0	0	0	0	0
5	0	0	0	0	0	0
6	0	0	0	0	0	0
7	0	0	0	0	0	0
8	10077906	314359	104258	1010	10077906	104
9	0	0	0	0	0	0
10	0	0	0	0	0	0

Figure 4.16 Ethernet Port Statistics Table

This table displays the following information:

Parameter	Description
`Port`	**Synopsis:** 1 to maximum port number The port number as seen on the front plate silkscreen of the switch.
`InOctets`	**Synopsis:** An integer between 0 and 18446744073709551615 The number of octets in received good packets (Unicast+Multicast+Broadcast) and dropped packets.
`OutOctets`	**Synopsis:** An integer between 0 and 18446744073709551615 The number of octets in transmitted good packets.
`InPkts`	**Synopsis:** An integer between 0 and 18446744073709551615 The number of received good packets (Unicast+Multicast+Broadcast) and dropped packets.
`OutPkts`	**Synopsis:** An integer between 0 and 18446744073709551615 The number of transmitted good packets.
`TotalInOctets`	**Synopsis:** An integer between 0 and 18446744073709551615 The total number of octets of all received packets. This includes data octets of rejected and local packets which are not forwarded to the switching core for transmission. It should reflect all the data octets received on the line.
`TotalInPkts`	**Synopsis:** An integer between 0 and 18446744073709551615 The number of received packets. This includes rejected, dropped local, and packets which are not forwarded to the switching core for transmission. It should reflect all packets received ont the line.
`InBroadcasts`	**Synopsis:** An integer between 0 and 18446744073709551615 The number of good Broadcast packets received.
`InMulticasts`	**Synopsis:** An integer between 0 and 18446744073709551615 The number of good Multicast packets received.

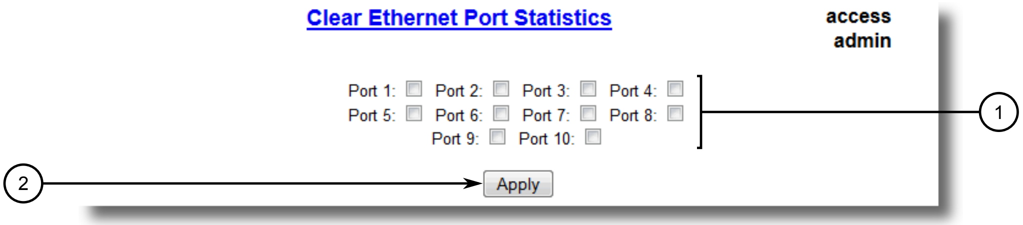
Parameter	Description
`CRCAlignErrors`	**Synopsis:** An integer between 0 and 4294967295 The number of packets received which meet all the following conditions: • Packet data length is between 64 and 1536 octets inclusive. • Packet has invalid CRC. • Collision Event has not been detected. • Late Collision Event has not been detected.
`OversizePkts`	**Synopsis:** An integer between 0 and 4294967295 The number of packets received with data length greater than 1536 octets and valid CRC.
`Fragments`	**Synopsis:** An integer between 0 and 4294967295 The number of packets received which meet all the following conditions: • Packet data length is less than 64 octets, or packet without SFD and is less than 64 octets in length. • Collision Event has not been detected. • Late Collision Event has not been detected. • Packet has invalid CRC.
`Jabbers`	**Synopsis:** An integer between 0 and 4294967295 The number of packets which meet all the following conditions: • Packet data length is greater that 1536 octets • Packet has invalid CRC
`Collisions`	**Synopsis:** An integer between 0 and 4294967295 The number of received packets for which Collision Event has been detected.
`LateCollisions`	**Synopsis:** An integer between 0 and 4294967295 The number of received packets for which Late Collision Event has been detected.
`Pkt64Octets`	**Synopsis:** An integer between 0 and 4294967295 The number of received and transmitted packets with 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.
`Pkt65to127Octets`	**Synopsis:** An integer between 0 and 4294967295 The number of received and transmitted packets with 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.
`Pkt128to255Octets`	**Synopsis:** An integer between 0 and 4294967295 The number of received and transmitted packets with 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.

Parameter	Description
`Pkt256to511Octets`	**Synopsis:** An integer between 0 and 4294967295 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.
`Pkt512to1023Octets`	**Synopsis:** An integer between 0 and 4294967295 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.
`Pkt1024to1536Octets`	**Synopsis:** An integer between 0 and 4294967295 The number of received and transmitted packets with 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.
`DropEvents`	**Synopsis:** An integer between 0 and 4294967295 The number of received packets that are droped due to lack of receive buffers.
`OutMulticasts`	**Synopsis:** An integer between 0 and 18446744073709551615 The number of transmitted Multicast packets. This does not include Broadcast packets.
`OutBroadcasts`	**Synopsis:** An integer between 0 and 18446744073709551615 The number of transmitted Broadcast packets.
`UndersizePkts`	**Synopsis:** An integer between 0 and 4294967295 The number of received packets which meet all the following conditions: • Packet data length is less than 64 octets. • Collision Event has not been detected. • Late Collision Event has not been detected. • Packet has valid CRC.

4.6.5 Clearing Statistics for Specific Ethernet Ports

To clear the statistics collected for one or more Ethernet ports, do the following:

1. Navigate to ***Ethernet Stats » Clear Ethernet Port Statistics***. The **Clear Ethernet Port Statistics** form appears.



Clear Ethernet Port Statistics

access
admin

Port 1: □ Port 2: □ Port 3: □ Port 4: □
Port 5: □ Port 6: □ Port 7: □ Port 8: □
Port 9: □ Port 10: □

① Port Check Boxes
② Confirm Button

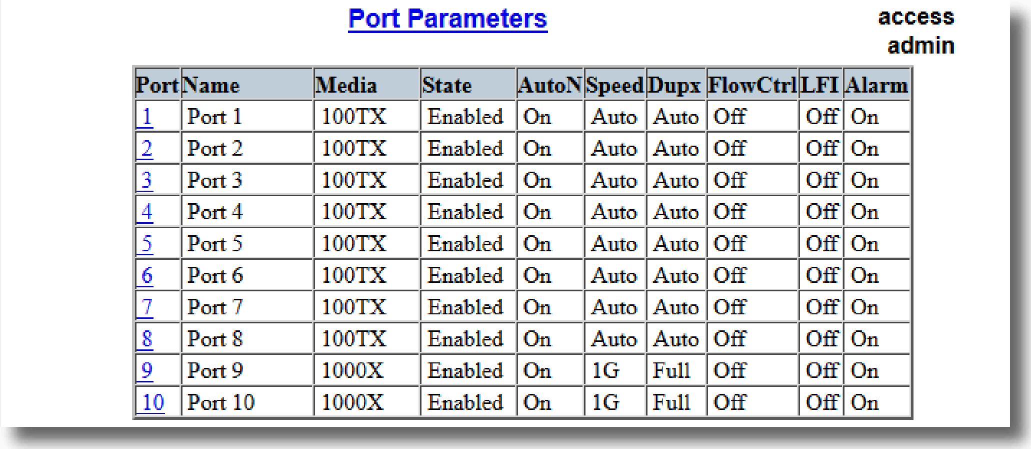
Figure 4.17 Clear Ethernet Port Statistics Form (Typical)

2. Select one or more Ethernet ports.
3. Click **Confirm**.

4.6.6 Configuring an Ethernet Port

To configure an Ethernet port, do the following:

1. Navigate to ***Ethernet Ports » Configure Port Parameters***. The **Port Parameters** table appears.



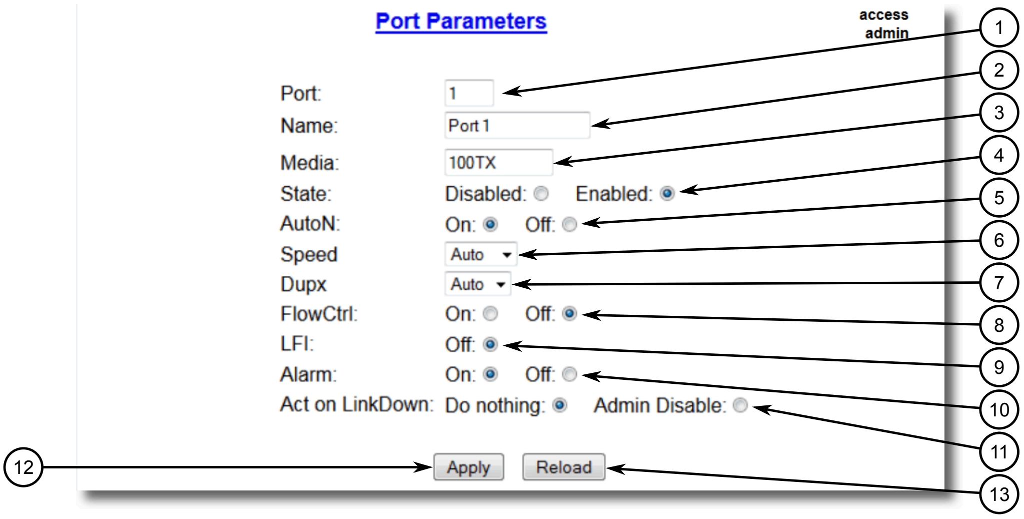
Port Parameters

access
admin

Port	Name	Media	State	AutoN	Speed	Dupx	FlowCtrl	LFI	Alarm
1	Port 1	100TX	Enabled	On	Auto	Auto	Off	Off	On
2	Port 2	100TX	Enabled	On	Auto	Auto	Off	Off	On
3	Port 3	100TX	Enabled	On	Auto	Auto	Off	Off	On
4	Port 4	100TX	Enabled	On	Auto	Auto	Off	Off	On
5	Port 5	100TX	Enabled	On	Auto	Auto	Off	Off	On
6	Port 6	100TX	Enabled	On	Auto	Auto	Off	Off	On
7	Port 7	100TX	Enabled	On	Auto	Auto	Off	Off	On
8	Port 8	100TX	Enabled	On	Auto	Auto	Off	Off	On
9	Port 9	1000X	Enabled	On	1G	Full	Off	Off	On
10	Port 10	1000X	Enabled	On	1G	Full	Off	Off	On

Figure 4.18 Port Parameters Table

2. Select an Ethernet port. The **Port Parameters** form appears.



Port Parameters

access
admin

Port:	1
Name:	Port 1
Media:	100TX
State:	Disabled: ○ Enabled: ●
AutoN:	On: ● Off: ○
Speed	Auto
Dupx	Auto
FlowCtrl:	On: ○ Off: ●
LFI:	Off: ●
Alarm:	On: ● Off: ○
Act on LinkDown:	Do nothing: ● Admin Disable: ○

①	Port Box
②	Name Box
③	Media Box
④	State Options
⑤	AutoN Options
⑥	Speed List
⑦	Dupx List
⑧	FlowCtrl Options
⑨	LFI Option
⑩	Alarm Options
⑪	Act on LinkDown Options
⑫	DownShift Options
⑬	Apply Button
⑭	Reload Button

Figure 4.19 Port Parameters Form

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

Parameter	Description
`Port`	**Synopsis:** 1 to maximum port number **Default:** 1 The port number as seen on the front plate silkscreen of the switch.
`Name`	**Synopsis:** A string 15 characters long **Default:** Port x A descriptive name that may be used to identify the device connected on that port.

Parameter	Description
Media	**Synopsis:** [100TX | 10FL | 100FX | 1000X | 1000T | 802.11g | EoVDSL | 100TX Only | 10FL/100SX | 10GX] **Default:** 100TX The type of the port media.
State	**Synopsis:** [Disabled | Enabled] **Default:** Enabled Disabling a port will prevent all frames from being sent and received on that port. Also, when disabled link integrity signal is not sent so that the link/activity LED will never be lit. You may want to disable a port for troubleshooting or to secure it from unauthorized connections. **Note** Disabling a port whose media type is set to 802.11g disables the corresponding wireless module.
AutoN	**Synopsis:** [Off | On] **Default:** On Enable or disable 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. 10Mbps and 100Mbps fiber optic media do not support auto-negotiation so these media must be explicitly configured to either half or full duplex. Full duplex operation requires that both ends are configured as such or else severe frame loss will occur during heavy network traffic.
Speed	**Synopsis:** [Auto | 10M | 100M | 1G] **Default:** Auto 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.
Dupx	**Synopsis:** [Auto | Half | Full] **Default:** Auto Duplex mode. 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.
Flow Control	**Synopsis:** [Off | On] **Default:** On Flow Control is useful for preventing frame loss during times of severe network traffic. Examples of this include multiple source ports sending to a single destination port or a higher speed port bursting to a lower speed port.

Parameter	Description
	When the port is half-duplex it is accomplished using 'backpressure' where the switch simulates collisions causing the sending device to retry transmissions according to the Ethernet backoff algorithm. When the port is full-duplex it is accomplished using PAUSE frames which causes the sending device to stop transmitting for a certain period of time.
`LFI`	**Synopsis:** [Off | On] **Default:** Off Enabling Link-Fault-Indication (LFI) inhibits transmitting link integrity signal when the receive link has failed. This allows the device at far end to detect link failure under all circumstances. **Note** This feature must not be enabled at both ends of a fiber link.
`Alarm`	**Synopsis:** [On | Off] **Default:** On Disabling link state alarms will prevent alarms and LinkUp and LinkDown SNMP traps from being sent for that port.
`Act on LinkDown`	**Synopsis:** [Do nothing | Admin Disable] **Default:** Do nothing The action to be taken upon a port LinkDown event. Options include: • Do nothing – No action is taken • Admin Disable – The port state is disabled

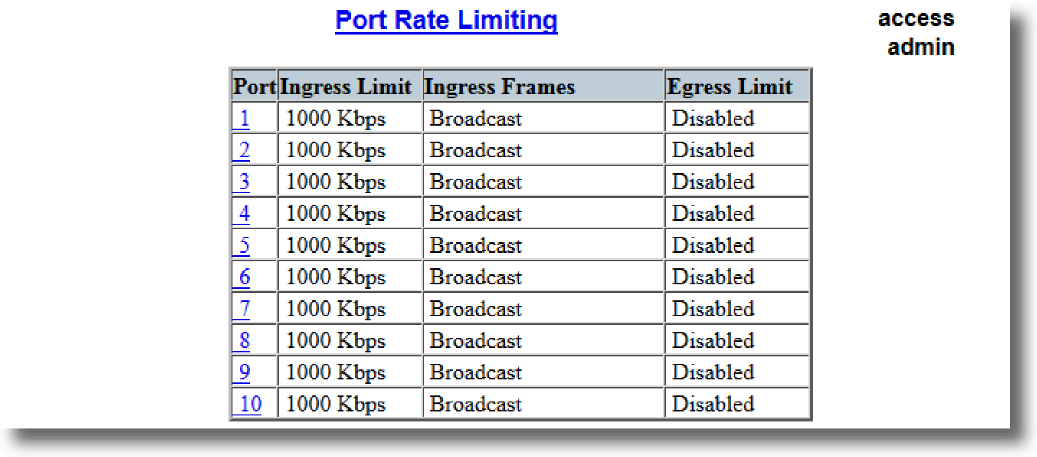
Note
If one end of the link is fixed to a specific speed and duplex type and the peer auto-negotiates, there is a strong possibility the link will either fail to raise, or raise with the wrong settings on the auto-negotiating side. The auto-negotiating peer will fall back to half-duplex operation, even when the fixed side is full duplex. Full-duplex operation requires that both ends are configured as such or else severe frame loss will occur during heavy network traffic. 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 excessive collisions. Ultimately, as traffic load approaches 100%, the link will become entirely unusable. These problems can be avoided by always configuring ports to the appropriate fixed values.

4. Click **Apply**.

4.6.7 Configuring Port Rate Limiting

To configure port rate limiting, do the following:

1. Navigate to ***Ethernet Ports » Configure Port Rate Limiting***. The **Port Rate Limiting** table appears.



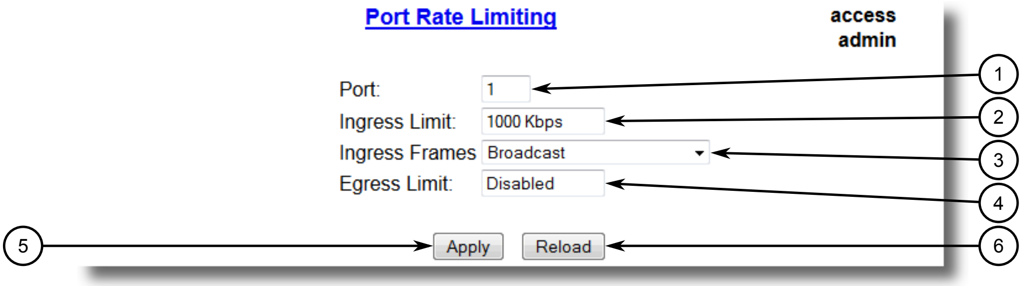
Port Rate Limiting

access
admin

Port	Ingress Limit	Ingress Frames	Egress Limit
1	1000 Kbps	Broadcast	Disabled
2	1000 Kbps	Broadcast	Disabled
3	1000 Kbps	Broadcast	Disabled
4	1000 Kbps	Broadcast	Disabled
5	1000 Kbps	Broadcast	Disabled
6	1000 Kbps	Broadcast	Disabled
7	1000 Kbps	Broadcast	Disabled
8	1000 Kbps	Broadcast	Disabled
9	1000 Kbps	Broadcast	Disabled
10	1000 Kbps	Broadcast	Disabled

Figure 4.20 Port Rate Limiting Table

2. Select an Ethernet port. The **Port Rate Limiting** form appears.



Port Rate Limiting

access
admin

Port:	1
Ingress Limit:	1000 Kbps
Ingress Frames	Broadcast
Egress Limit:	Disabled

①	Port Box
②	Ingress Limit Box
③	Ingress Frames List
④	Egress Limit Box
⑤	Apply Button
⑥	Reload Button

Figure 4.21 Port Rate Limiting Form

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

Parameter	Description
`Port`	**Synopsis:** 1 to maximum port number **Default:** 1 The port number as seen on the front plate silkscreen of the switch.

Parameter	Description
`Ingress Limit`	**Synopsis:** An integer between 62 and 256000 or [Disabled] **Default:** 1000 The rate after which received frames (of the type described by the ingress frames parameter) will be discarded by the switch.
`Ingress Frames`	**Synopsis:** [Broadcast | Bcast&Mcast | Bcast&Mcast&FloodUcast | Bcast&FloodUcast | FloodUcast | All] **Default:** Broadcast This parameter specifies the types of frames to be rate-limited on this port. It applies only to received frames: • Broadcast – Only broadcast frames • Bcast&Mcast – Broadcast and multicast frames • Bcast&FloodUcast – Broadcast and flooded unicast frames • Bcast&Mcast&FloodUcast – Broadcast, multicast and flooded unicast frames • FloodUcast – Only flooded unicast frames • All – All (multicast, broadcast and unicast) frames
`Egress Limit`	**Synopsis:** An integer between 62 and 256000 or [Disabled] **Default:** Disabled The maximum rate 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.

4. Click **Apply**.

4.6.8 Configuring Port Mirroring

Port mirroring is a troubleshooting tool that copies, or mirrors, all traffic received or transmitted on a designated port to a specified mirror port. If a protocol analyzer is attached to the target port, the traffic stream of valid frames on any source port is made available for analysis.

⚠ **NOTICE**

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.

⚠ **NOTICE**

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.

⚠ NOTICE

Before configuring port mirroring, note the following:

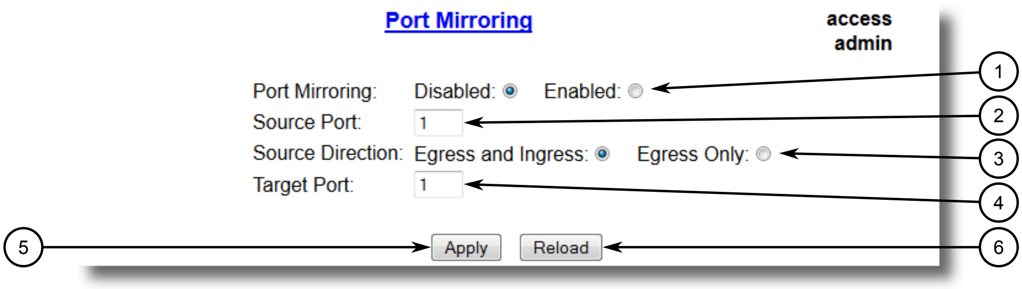
- Mirror ports allow bidirectional traffic, i.e. the device will not block incoming traffic to the mirror port(s). For increased security, configure ingress filtering to control traffic flow when port mirroring is enabled. For more information about enabling ingress filtering, refer to "Configuring VLANs Globally (Page 152)".
- Traffic will be mirrored onto the target port irrespective of its VLAN membership. It could be the same as or different from the source port's membership.
- Network management frames (such as RSTP, GVRP etc.) cannot be mirrored.
- Switch management frames generated by the switch (such as Telnet, HTTP, SNMP, etc.) cannot be mirrored.

Note

Invalid frames received on the source port will not be mirrored. These include CRC errors, oversize and undersize packets, fragments, jabbers, collisions, late collisions and dropped events.

To configure port mirroring, do the following:

1. Navigate to ***Ethernet Ports » Configure Port Mirroring***. The **Port Mirroring** form appears.



Port Mirroring

access
admin

Port Mirroring: Disabled: ● Enabled: ○

Source Port: 1

Source Direction: Egress and Ingress: ● Egress Only: ○

Target Port: 1

① Port Mirroring Options
② Source Port Box
③ Source Direction Options
④ Target Port Box
⑤ Apply Button
⑥ Reload Button

Figure 4.22 Port Mirroring Form

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

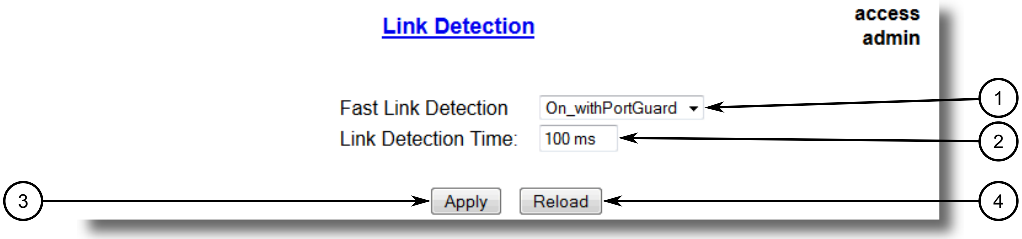
Parameter	Description
`Port Mirroring`	**Synopsis:** [Disabled | Enabled] **Default:** Disabled Enabling port mirroring causes all frames received and transmitted by the source port(s) to be transmitted out of the target port.
`Source Port`	**Synopsis:** Any combination of numbers valid for this parameter The port(s) being monitored.
`Source Direction`	**Synopsis:** [Egress and Ingress | Egress Only] **Default:** Egress and Ingress Specifies monitoring whether both egress and ingress traffics or only egress traffic of the source port.
`Target Port`	**Synopsis:** 1 to maximum port number **Default:** 1 The port where a monitoring device should be connected.

3. Click **Apply**.

4.6.9 Configuring Link Detection

To configure link detection, do the following:

1. Navigate to ***Ethernet Ports » Configure Link Detection***. The **Link Detection** form appears.



Fast Link Detection: On_withPortGuard
Link Detection Time: 100 ms

① Fast Link Detection Box
② Link Detection Time Box
③ Apply Button
④ Reload Button

Figure 4.23 Link Detection Form

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

Note
When Fast Link Detection is enabled, the system prevents link state change processing from consuming all available CPU resources. However, if Port Guard is

not used, it is possible for almost all available CPU time to be consumed by frequent link state changes, which could have a negative impact on overall system responsiveness.

Parameter	Description
`Fast Link Detection`	**Synopsis:** [Off | On | On_withPortGuard] **Default:** On_withPortGuard This parameter provides protection against faulty end devices generating an improper link integrity signal. When a faulty end device or a mis-matching fiber port is connected to the unit, a large number of continuous link state changes could be reported in a short period of time. These large number of bogus link state changes could render the system unresponsive as most, if not all, of the system resources are used to process the link state changes. This could in turn cause a serious network problem as the unit's RSTP process may not be able to run, thus allowing network loop to form. Three different settings are available for this parameter: • ON_withPortGuard – This is the recommended setting. With this setting, an extended period (~2 minutes) of excessive link state changes reported by a port will prompt Port Guard feature to disable FAST LINK DETECTION on that port and raise an alarm. By disabling FAST LINK DETECTION on the problematic port, excessive link state changes can no longer consume substantial amount of system resources. However if FAST LINK DETECTION is disabled, the port will need a longer time to detect a link failure. This may result in a longer network recovery time of up to 2s. Once Port Guard disables FAST LINK DETECTION of a particular port, user can re-enable FAST LINK DETECTION on the port by clearing the alarm. • ON – In certain special cases where a prolonged excessive link state changes constitute a legitimate link operation, using this setting can prevent Port Guard from disabling FAST LINK DETECTION on the port in question. If excessive link state changes persist for more than 2 minutes, an alarm will be generated to warn user about the observed bouncing link. If the excessive link state changes condition is resolved later on, the alarm will be cleared automatically. Since this option does not disable FAST LINK DETECTION, a persistent bouncing link could continue affect the system in terms of response time. This setting should be used with caution. • OFF – Turning this parameter OFF will disable FAST LINK DETECTION completely. The switch will need a longer time to detect a link failure. This will result in a longer network recovery time of up to 2s.
`Link Detection Time`	**Synopsis:** An integer between 100 and 1000 **Default:** 100 The time that the link has to continuously stay up before the "link up" decision is made by the device. (The device performs de-bouncing of Ethernet link detection to avoid multiple responses to an occasional link bouncing

Parameter	Description
	event, e.g. when a cable is shaking while being plugged-in or unplugged).

3. Click **Apply**.

4.6.10 Detecting Cable Faults

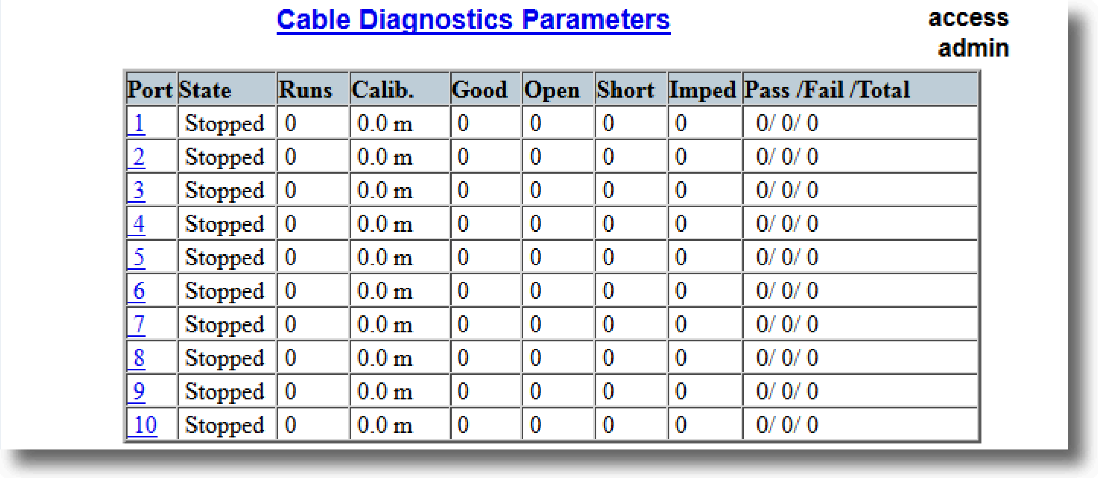
Connectivity issues can sometimes be attributed to faults in Ethernet cables. To help detect cable faults, short circuits, open cables or cables that are too long, RUGGEDCOM ROS includes a built-in cable diagnostics utility.

4.6.10.1 Viewing Cable Diagnostics Results

To view the results of previous diagnostic tests, navigate to ***Ethernet Ports » Configure/View Cable Diagnostics Parameters***. The **Cable Diagnostics Parameters** table appears.

Note

For information about how to start a diagnostic test, refer to "Performing Cable Diagnostics (Page 70)".



Port	State	Runs	Calib.	Good	Open	Short	Imped	Pass /Fail /Total
1	Stopped	0	0.0 m	0	0	0	0	0/ 0/ 0
2	Stopped	0	0.0 m	0	0	0	0	0/ 0/ 0
3	Stopped	0	0.0 m	0	0	0	0	0/ 0/ 0
4	Stopped	0	0.0 m	0	0	0	0	0/ 0/ 0
5	Stopped	0	0.0 m	0	0	0	0	0/ 0/ 0
6	Stopped	0	0.0 m	0	0	0	0	0/ 0/ 0
7	Stopped	0	0.0 m	0	0	0	0	0/ 0/ 0
8	Stopped	0	0.0 m	0	0	0	0	0/ 0/ 0
9	Stopped	0	0.0 m	0	0	0	0	0/ 0/ 0
10	Stopped	0	0.0 m	0	0	0	0	0/ 0/ 0

Figure 4.24 Cable Diagnostics Parameters Table

This table displays the following information:

Parameter	Description
`Port`	**Synopsis:** 1 to maximum port number The port number as seen on the front plate silkscreen of the switch.

Parameter	Description
`State`	**Synopsis:** [Stopped | Started] Control the start/stop of the cable diagnostics on the selected port. If a port does not support cable diagnostics, State will be reported as N/A.
`Runs`	**Synopsis:** An integer between 0 and 65535 The total number of times cable diagnostics to be performed on the selected port. If this number is set to 0, cable diagnostics will be performed forever on the selected port.
`Calib.`	**Synopsis:** An integer between -100.0 and 100.0 This calibration value can be used to adjust or calibrate the estimated distance to fault. User can take following steps to calibrate the cable diagnostics estimated distance to fault: • Pick a particular port which calibration is needed • Connect an Ethernet cable with a known length (e.g. 50m) to the port • DO NOT connect the other end of the cable to any link partner • Run cable diagnostics a few times on the port. OPEN fault should be detected • 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 • Enter the calibration value and run cable diagnostics a few more times • The distance to OPEN fault should now be at similar distance as the cable length • Distance to fault for the selected port is now calibrated
`Good`	**Synopsis:** An integer between 0 and 65535 The number of times GOOD TERMINATION (no fault) is detected on the cable pairs of the selected port.
`Open`	**Synopsis:** An integer between 0 and 65535 The number of times OPEN is detected on the cable pairs of the selected port.
`Short`	**Synopsis:** An integer between 0 and 65535 The number of times SHORT is detected on the cable pairs of the selected port.
`Imped`	**Synopsis:** An integer between 0 and 65535 The number of times IMPEDANCE MISMATCH is detected on the cable pairs of the selected port.
`Pass /Fail /Total`	**Synopsis:** A string 19 characters long This field summarizes the results of the cable diagnostics performed so far. • Pass – number of times cable diagnostics successfully completed on the selected port. • Fail – number of times cable diagnostics failed to complete on the selected port.

Parameter	Description
	• Total – total number of times cable diagnostics have been attempted on the selected port.

Note

For each successful diagnostic test, the values for **Good**, **Open**, **Short** or **Imped** will increment based on the number of cable pairs connected to the port. For a 100Base-T port, which has two cable pairs, the number will increase by two. For a 1000Base-T port, which has four cable pairs, the number will increase by four.

Note

When a cable fault is detected, an estimated distance-to-fault is calculated and recorded in the system log. The log lists the cable pair, the fault that was detected, and the distance-to-fault value. For more information about the system log, refer to "Viewing Local and System Logs (Page 46)".

4.6.10.2 Performing Cable Diagnostics

To perform a cable diagnostic test on one or more Ethernet ports, do the following:

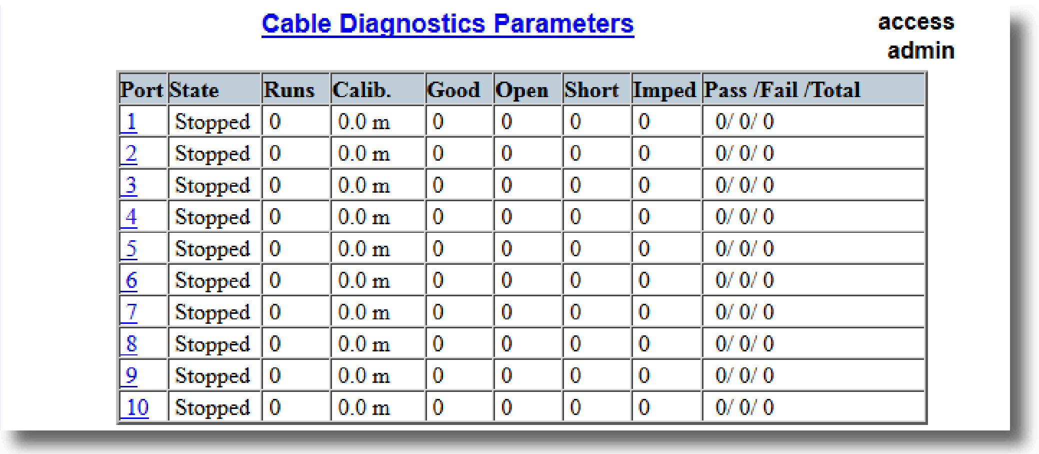
1. Connect a CAT-5 (or better quality) Ethernet cable to the selected Ethernet port.

   ⚠ **NOTICE**

   Both the selected Ethernet port and its partner port can be configured to run in *Enabled* mode with auto-negotiation, or in *Disabled* mode. Other modes are not recommended, as they may interfere with the cable diagnostics procedure.

2. Connect the other end of the cable to a similar network port. For example, connect a 100Base-T port to a 100Base-T port, or a 1000Base-T port to a 1000Base-T port.

3. In RUGGEDCOM ROS, navigate to ***Ethernet Ports » Configure/View Cable Diagnostics Parameters***. The **Cable Diagnostics Parameters** table appears.



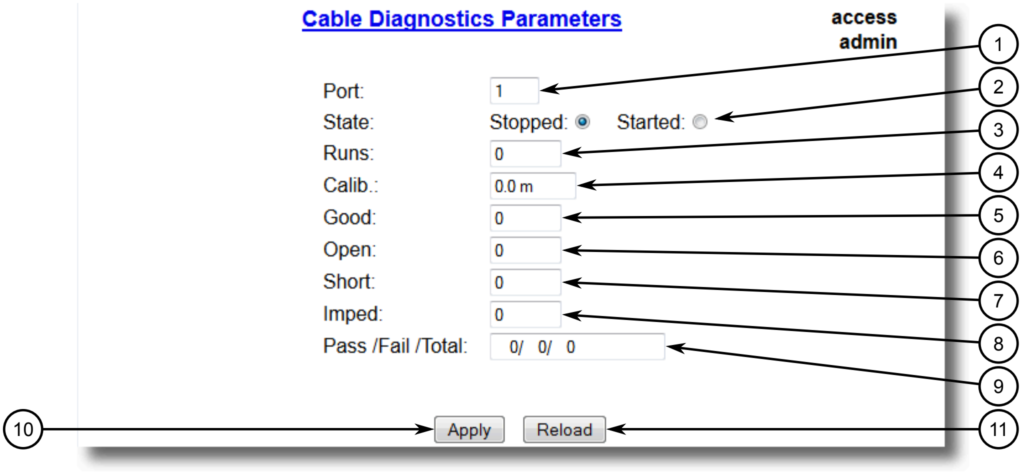
Cable Diagnostics Parameters

access
admin

Port	State	Runs	Calib.	Good	Open	Short	Imped	Pass /Fail /Total
1	Stopped	0	0.0 m	0	0	0	0	0/ 0/ 0
2	Stopped	0	0.0 m	0	0	0	0	0/ 0/ 0
3	Stopped	0	0.0 m	0	0	0	0	0/ 0/ 0
4	Stopped	0	0.0 m	0	0	0	0	0/ 0/ 0
5	Stopped	0	0.0 m	0	0	0	0	0/ 0/ 0
6	Stopped	0	0.0 m	0	0	0	0	0/ 0/ 0
7	Stopped	0	0.0 m	0	0	0	0	0/ 0/ 0
8	Stopped	0	0.0 m	0	0	0	0	0/ 0/ 0
9	Stopped	0	0.0 m	0	0	0	0	0/ 0/ 0
10	Stopped	0	0.0 m	0	0	0	0	0/ 0/ 0

Figure 4.25 Cable Diagnostics Parameters Table

4. Select an Ethernet port. The **Cable Diagnostics Parameters** form appears.



Cable Diagnostics Parameters

access
admin

Port:	1
State:	Stopped: ● Started: ○
Runs:	0
Calib.:	0.0 m
Good:	0
Open:	0
Short:	0
Imped:	0
Pass /Fail /Total:	0/ 0/ 0

① Port Box
② State Options
③ Runs Box
④ Calib. Box
⑤ Good Box
⑥ Open Box
⑦ Short Box
⑧ Imped Box
⑨ Pass/Fail/Total Box
⑩ Apply Button
⑪ Reload Button

Figure 4.26 Cable Diagnostics Parameters Form

5. Under **Runs**, enter the number of consecutive diagnostic tests to perform. A value of 0 indicates the test will run continuously until stopped by the user.
6. Under **Calib.**, enter the estimated Distance To Fault (DTF) value. For information about how to determine the DTF value, refer to "Determining the Estimated Distance To Fault (DTF) (Page 72)".
7. Select **Started**.

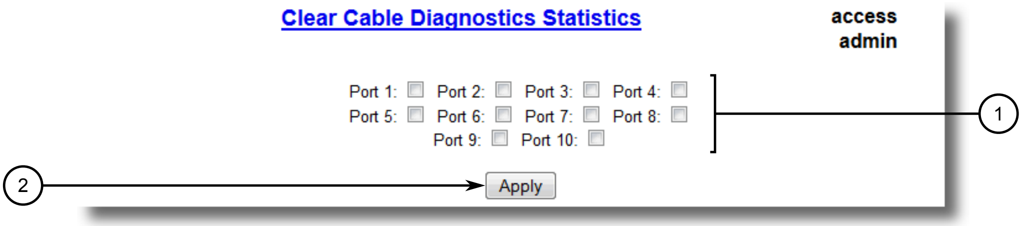
> ⚠ **NOTICE**
>
> A diagnostic test can be stopped by selecting **Stopped** and clicking **Apply**. However, if the test is stopped in the middle of a diagnostic run, the test will run to completion.

8. Click **Apply**. The state of the Ethernet port will automatically change to `Stopped` when the test is complete. For information about how to monitor the test and view the results, refer to "Viewing Cable Diagnostics Results (Page 68)".

4.6.10.3 Clearing Cable Diagnostics

To clear the cable diagnostic results, do the following:

1. Navigate to ***Ethernet Ports » Clear Cable Diagnostics Statistics***. The **Clear Cable Diagnostics Statistics** form appears.


Clear Cable Diagnostics Statistics
access
admin
Port 1: □ Port 2: □ Port 3: □ Port 4: □
Port 5: □ Port 6: □ Port 7: □ Port 8: □
Port 9: □ Port 10: □
Apply
1
2

① Port Check Boxes
② Apply Button

Figure 4.27 Clear Cable Diagnostics Statistics Form

2. Select one or more Ethernet ports.
3. Click **Apply**.

4.6.10.4 Determining the Estimated Distance To Fault (DTF)

To determine the estimate Distance To Fault (DTF), do the following:

1. Connect a CAT-5 (or better quality) Ethernet cable with a known length to the device. Do not connect the other end of the cable to another port.

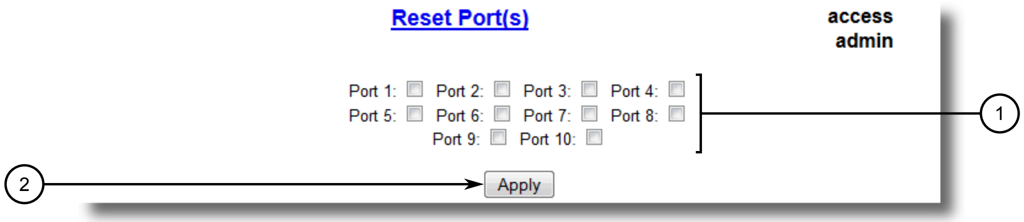
2. Configure the cable diagnostic utility to run a few times on the selected Ethernet port and start the test. For more information, refer to "Performing Cable Diagnostics (Page 70)". Open faults should be detected and recorded in the system log.
3. Review the errors recorded in the system log and determine the average distance of the open faults. For more information about the system log, refer to "Viewing Local and System Logs (Page 46)".
4. Subtract the average distance from the cable length to determine the calibration value.
5. Configure the cable diagnostic utility to run a few times with the new calibration value. The distance to the open fault should now be the same as the actual length of the cable. The Distance To Fault (DTF) is now calibrated for the selected Ethernet port.

4.6.11 Resetting Ethernet Ports

At times, it may be necessary to reset a specific Ethernet port, such as when the link partner has latched into an inappropriate state. This is also useful for forcing a re-negotiation of the speed and duplex modes.

To reset a specific Ethernet port(s), do the following:

1. Navigate to ***Ethernet Ports » Reset Port(s)***. The **Reset Port(s)** form appears.



Reset Port(s)

access
admin

Port 1: □ Port 2: □ Port 3: □ Port 4: □
Port 5: □ Port 6: □ Port 7: □ Port 8: □
Port 9: □ Port 10: □

① Ports
② Apply Button

Figure 4.28 Reset Port(s) Form

2. Select one or more Ethernet ports to reset.
3. Click **Apply**. The selected Ethernet ports are reset.

4.7 Managing IP Interfaces

RUGGEDCOM ROS allows one IP interface to be configured for each subnet (or VLAN), up to a maximum of 255 interfaces. One of the interfaces must also be configured to be a management interface for certain IP services, such as DHCP relay agent.

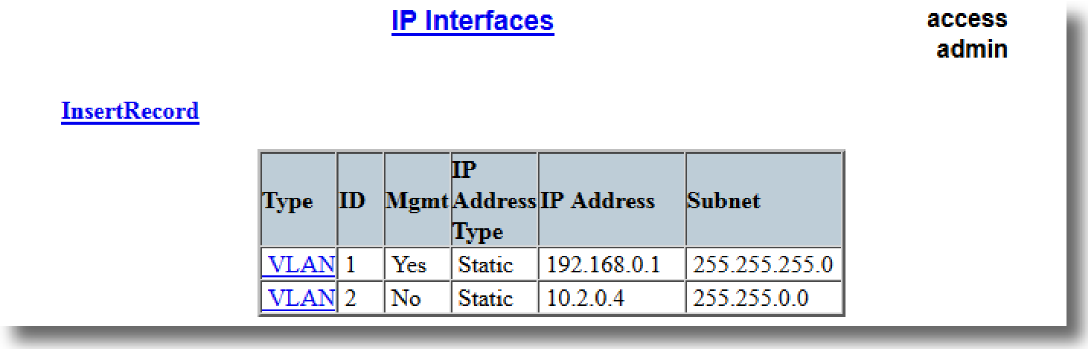
Each IP interface must be assigned an IP address. In the case of the management interface, the IP address type can be either static, DHCP, BOOTP or dynamic. For all other interfaces, the IP address must be static.

⚠ **CAUTION**

Configuration hazard – risk of communication disruption. Changing the ID for the management VLAN will break any active Raw Socket TCP connections. If this occurs, reset all serial ports.

4.7.1 Viewing a List of IP Interfaces

To view a list of IP interfaces configured on the device, navigate to ***Administration » Configure IP Interfaces » Configure IP Interfaces***. The **IP Interfaces** table appears.



Type	ID	Mgmt	IP Address Type	IP Address	Subnet
VLAN	1	Yes	Static	192.168.0.1	255.255.255.0
VLAN	2	No	Static	10.2.0.4	255.255.0.0

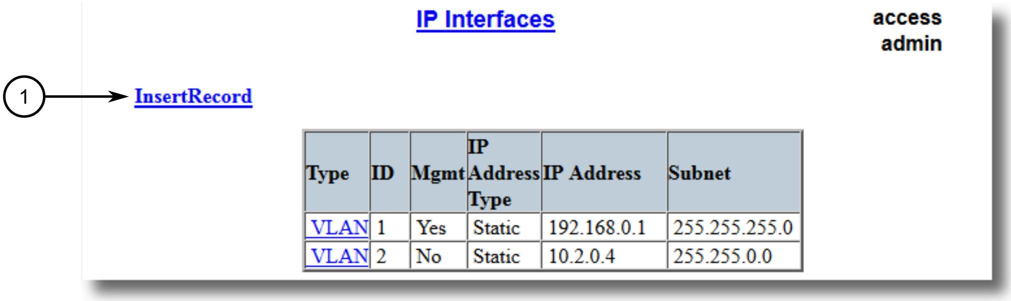
Figure 4.29 IP Interfaces Table

If IP interfaces have not been configured, add IP interfaces as needed. For more information, refer to "Adding an IP Interface (Page 75)".

4.7.2 Adding an IP Interface

To add an IP interface, do the following:

1. Navigate to ***Administration » Configure IP Interfaces***. The **IP Interfaces** table appears.

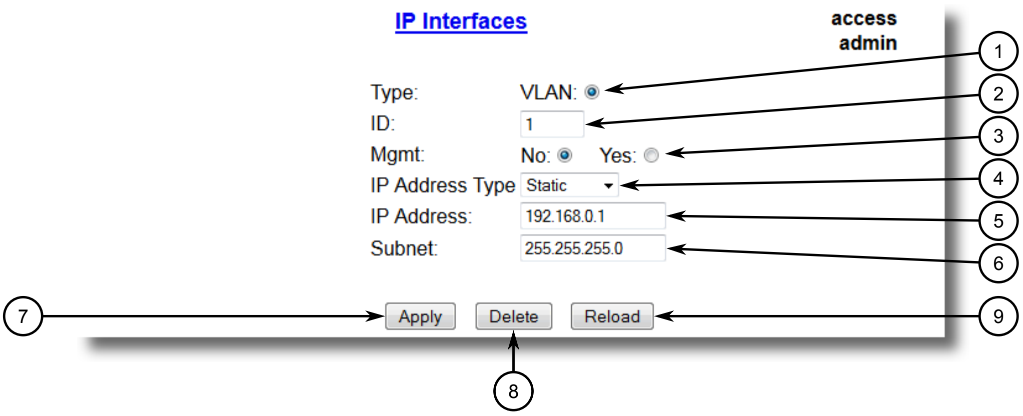


Type	ID	Mgmt	IP Address Type	IP Address	Subnet
VLAN	1	Yes	Static	192.168.0.1	255.255.255.0
VLAN	2	No	Static	10.2.0.4	255.255.0.0

① InsertRecord

Figure 4.30 IP Interfaces Table

2. Click **InsertRecord**. The **Switch IP Interfaces** form appears.



Type:	VLAN: ●
ID:	1
Mgmt:	No: ● Yes: ○
IP Address Type	Static
IP Address:	192.168.0.1
Subnet:	255.255.255.0

① Type Options
② ID Box
③ Mgmt Options
④ IP Address Type Box
⑤ IP Address Box
⑥ Subnet Box
⑦ Apply Button
⑧ Delete Button
⑨ Reload Button

Figure 4.31 IP Interfaces Form

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

Note
The IP address and mask configured for the management VLAN are not changed when resetting all configuration parameters to defaults and will be assigned a default VLAN ID of 1. Changes to the IP address take effect immediately. All IP connections in place at the time of an IP address change will be lost.

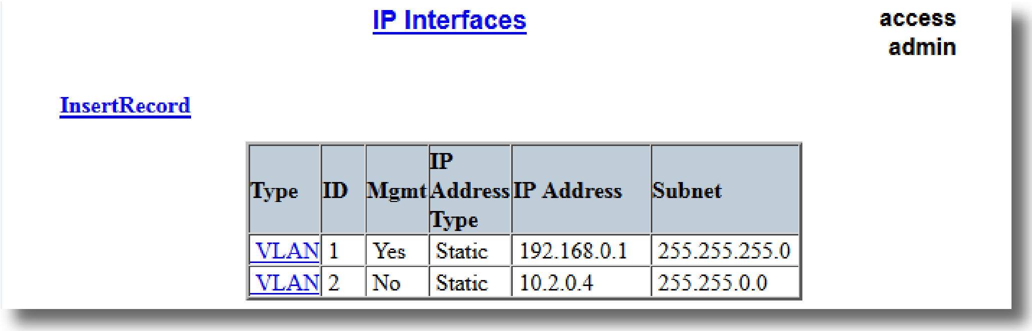
Parameter	Description
`Type`	**Synopsis:** [VLAN] **Default:** VLAN Specifies the type of the interface for which this IP interface is created.
`ID`	**Synopsis:** An integer between 1 and 4094 **Default:** 1 Specifies the ID of the interface for which this IP interface is created. If the interface type is VLAN, this represents the VLAN ID.
`Mgmt`	**Synopsis:** [No | Yes] **Default:** No Specifies whether the IP interface is the device management interface.
`IP Address Type`	**Synopsis:** [Static | Dynamic | DHCP | BOOTP] **Default:** Static Specifies whether the IP address is static or is dynamically assigned via DHCP or BOOTP>. The Dynamic option automatically switches between BOOTP and DHCP until it receives a response from the relevant server. The Static option must be used for non-management interfaces.
`IP Address`	**Synopsis:** ###.###.###.### where ### ranges from 0 to 255 **Default:** 192.168.0.1 Specifies the IP address of this device. An IP address is a 32-bit number that is notated by using four numbers from 0 through 255, separated by periods. Only a unicast IP address is allowed, which ranges from 1.0.0.0 to 233.255.255.255.
`Subnet`	**Synopsis:** ###.###.###.### where ### ranges from 0 to 255 **Default:** 255.255.255.0 Specifies the IP subnet mask of this device. An IP subnet mask is a 32-bit number that is notated by using four numbers from 0 through 255, separated by periods. Typically, subnet mask numbers use either 0 or 255 as values (e.g. 255.255.255.0) but other numbers can appear. ⚠ **NOTICE** Each IP interface must have a unique network address.

4. Click **Apply**.

4.7.3 Deleting an IP Interface

To delete an IP interface configured on the device, do the following:

1. Navigate to ***Administration » Configure IP Interfaces***. The **IP Interfaces** table appears.



IP Interfaces

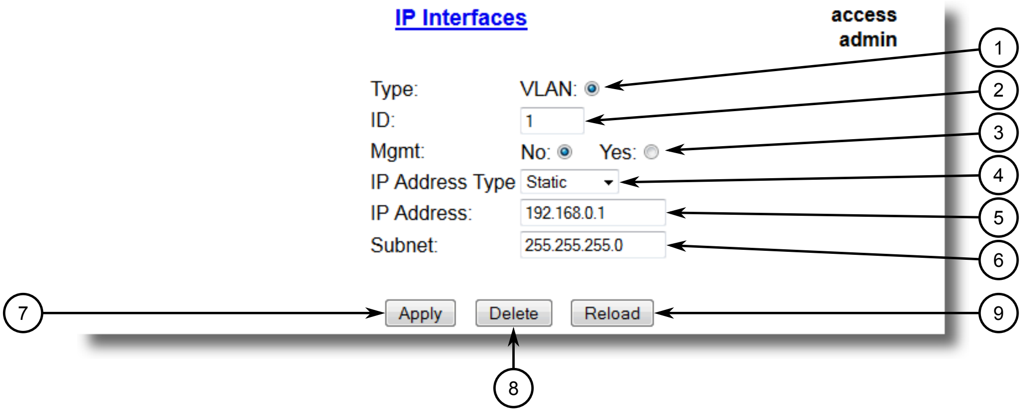
access
admin

InsertRecord

Type	ID	Mgmt	IP Address Type	IP Address	Subnet
VLAN	1	Yes	Static	192.168.0.1	255.255.255.0
VLAN	2	No	Static	10.2.0.4	255.255.0.0

Figure 4.32 IP Interfaces Table

2. Select the IP interface from the table. The **IP Interfaces** form appears.



IP Interfaces

access
admin

Type:	VLAN: ●
ID:	1
Mgmt:	No: ● Yes: ○
IP Address Type	Static
IP Address:	192.168.0.1
Subnet:	255.255.255.0

① Type Options
② ID Box
③ Mgmt Options
④ IP Address Type Box
⑤ IP Address Box
⑥ Subnet Box
⑦ Apply Button
⑧ Delete Button
⑨ Reload Button

Figure 4.33 IP Interfaces Form

3. Click **Delete**.

4.8 Managing IP Gateways

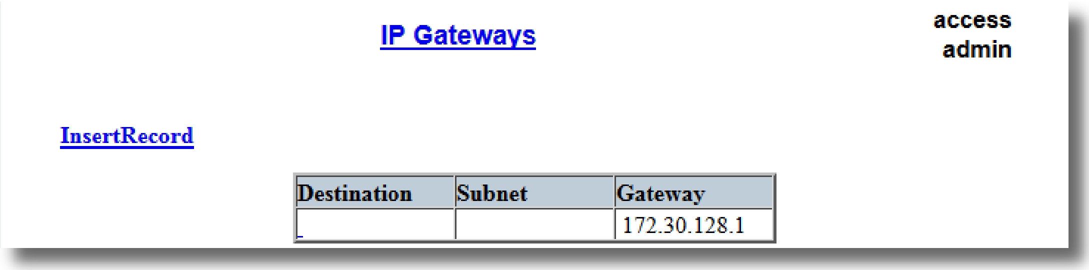
RUGGEDCOM ROS allows up to ten IP gateways to be configured. When both the **Destination** and **Subnet** parameters are blank, the gateway is considered to be a default gateway.

Note

The default gateway configuration will not be changed when resetting all configuration parameters to their factory defaults.

4.8.1 Viewing a List of IP Gateways

To view a list of IP gateways configured on the device, navigate to ***Administration » Configure IP Gateways***. The **IP Gateways** table appears.



IP Gateways

access
admin

InsertRecord

Destination	Subnet	Gateway
		172.30.128.1

Figure 4.34 IP Gateways Table

If IP gateways have not been configured, add IP gateways as needed. For more information, refer to "Adding an IP Gateway (Page 78)".

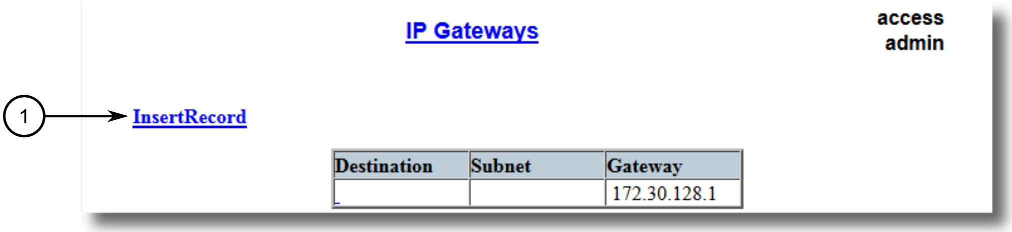
4.8.2 Adding an IP Gateway

⚠ **NOTICE**

DHCP-provided IP gateway addresses will override manually configured values.

To add an IP gateway, do the following:

1. Navigate to ***Administration » Configure IP Gateways***. The **IP Gateways** table appears.



IP Gateways

access
admin

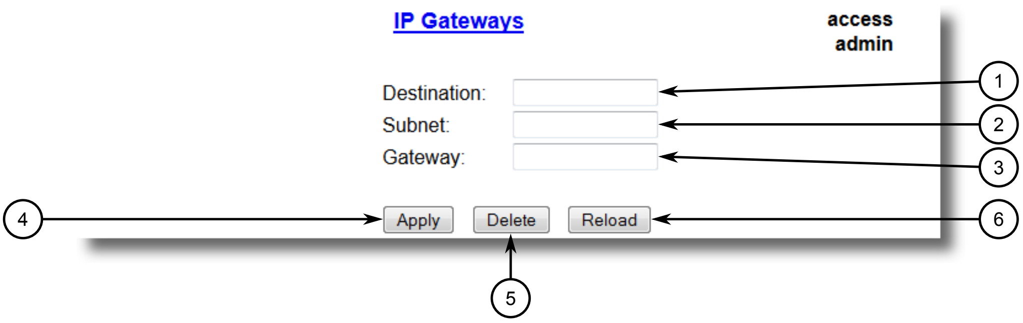
InsertRecord

Destination	Subnet	Gateway
		172.30.128.1

① InsertRecord

Figure 4.35 IP Gateways Table

2. Click **InsertRecord**. The **IP Gateways** form appears.



IP Gateways

access
admin

Destination:
Subnet:
Gateway:

① Destination Box
② Subnet Prefix Box
③ Gateway Box
④ Apply Button
⑤ Delete Button
⑥ Reload Button

Figure 4.36 IP Gateways

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

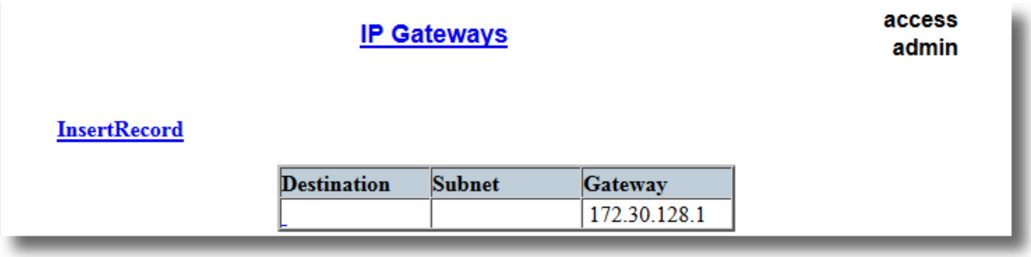
Parameter	Description
`Destination`	**Synopsis:** ###.###.###.### where ### ranges from 0 to 255 Specifies the IP address of destination network or host. For default gateway, both the destination and subnet are 0.
`Subnet`	**Synopsis:** ###.###.###.### where ### ranges from 0 to 255 Specifies the destination IP subnet mask. For default gateway, both the destination and subnet are 0.
`Gateway`	**Synopsis:** ###.###.###.### where ### ranges from 0 to 255 Specifies the gateway to be used to reach the destination.

4. Click **Apply**.

4.8.3 Deleting an IP Gateway

To delete an IP gateway configured on the device, do the following:

1. Navigate to ***Administration » Configure IP Gateways***. The **IP Gateways** table appears.



IP Gateways

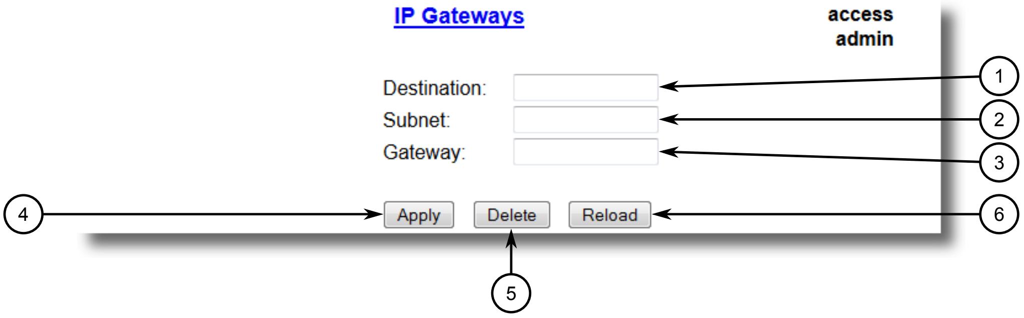
access
admin

InsertRecord

Destination	Subnet	Gateway
		172.30.128.1

Figure 4.37 IP Gateways Table

2. Select the IP gateway from the table. The **IP Gateways** form appears.



IP Gateways

access
admin

Destination:
Subnet:
Gateway:

① Destination Box
② Subnet Box
③ Gateway Box
④ Apply Button
⑤ Delete Button
⑥ Reload Button

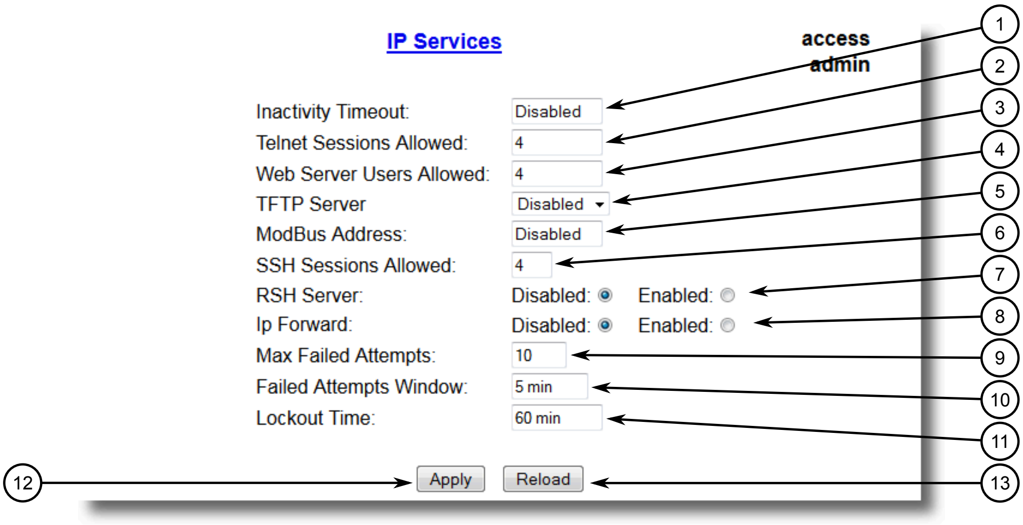
Figure 4.38 IP Gateways Form

3. Click **Delete**.

4.9 Configuring IP Services

To configure the IP services provided by the device, do the following:

1. Navigate to ***Administration » Configure IP Services***. The **IP Services** form appears.



IP Services

access
admin

Inactivity Timeout: Disabled

Telnet Sessions Allowed: 4

Web Server Users Allowed: 4

TFTP Server: Disabled

ModBus Address: Disabled

SSH Sessions Allowed: 4

RSH Server: Disabled: ● Enabled: ○

Ip Forward: Disabled: ● Enabled: ○

Max Failed Attempts: 10

Failed Attempts Window: 5 min

Lockout Time: 60 min

① Inactivity Timeout Box
② Telnet Sessions Allowed Box
③ Web Server Users Allowed Box
④ TFTP Server Box
⑤ Modbus Address Box
⑥ SSH Sessions Allowed Box
⑦ RSH Server Options
⑧ IP Forward Options
⑨ Max Failed Attempts Box
⑩ Failed Attempts Window Box
⑪ Lockout Time Box
⑫ Apply Button
⑬ Reload Button

Figure 4.39 IP Services Form

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

Parameter	Description
`Inactivity Timeout`	**Synopsis:** An integer between 1 and 60 or [Disabled] **Default:** 5 Specifies when the console will timeout and display the login screen if there is no user activity. A value of zero disables timeouts. For Web Server users maximum timeout value is limited to 30 minutes.

Parameter	Description
`Telnet Sessions Allowed`	**Synopsis:** An integer between 1 and 4 or [Disabled] **Default:** Disabled Limits the number of Telnet sessions. A value of zero prevents any Telnet access.
`Web Server Users Allowed`	**Synopsis:** An integer between 1 and 4 or [Disabled] **Default:** 4 Limits the number of simultaneous web server users.
`TFTP Server`	**Synopsis:** [Disabled | Get Only | Enabled] **Default:** Disabled As TFTP is a very insecure protocol, this parameter allows user to limit or disable TFTP Server access.. `Disabled` – disables read and write access to TFTP Server `Get Only` – only allows reading of files via TFTP Server `Enabled` – allows reading and writing of files via TFTP Server
`ModBus Address`	**Synopsis:** An integer between 1 and 255 or [Disabled] **Default:** Disabled Determines the Modbus address to be used for Management through Modbus.
`SSH Sessions Allowed (Controlled Version Only)`	**Synopsis:** An integer between 1 and 4 **Default:** 4 Limits the number of SSH sessions.
`RSH Server`	**Synopsis:** [Disabled | Enabled] **Default:** Disabled (controlled version) or Enabled (non-controlled version) Disables/enables Remote Shell access.
`IP Forward`	**Synopsis:** [Disabled | Enabled] Controls the ability of IP Forwarding between VLANs in Serial Server or IP segments. **Note** When upgrading to RUGGEDCOM ROS v4.3, the default will be set to { Enabled }.
`Max Failed Attempts`	**Synopsis:** An integer between 1 and 20 **Default:** 10 Maximum number of consecutive failed access attempts on service within Failed Attempts Window before blocking the service.
`Failed Attempts Window`	**Synopsis:** An integer between 1 and 30 **Default:** 5 The time in minutes (min) in which the maximum number of failed login attempts must be exceeded before a service is

Parameter	Description
	blocked. The counter of failed attempts resets to 0 when the timer expires.
`Lockout Time`	**Synopsis:** An integer between 1 and 120 **Default:** 60 The time in minutes (min) the service remains locked out after the maximum number of failed access attempts has been reached.

3. Click **Apply**.

4.10 Managing Remote Monitoring

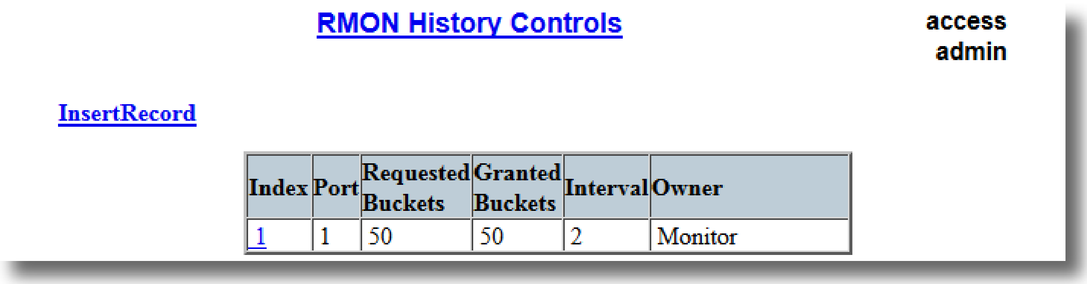
Remote Monitoring (RMON) is used to collect and view historical statistics related to the performance and operation of Ethernet ports. It can also record a log entry and/or generate an SNMP trap when the rate of occurrence of a specified event is exceeded.

4.10.1 Managing RMON History Controls

The history controls for Remote Monitoring take samples of the RMON-MIB history statistics of an Ethernet port at regular intervals.

4.10.1.1 Viewing a List of RMON History Controls

To view a list of RMON history controls, navigate to ***Ethernet Stats » Configure RMON History Controls***. The **RMON History Controls** table appears.



Index	Port	Requested Buckets	Granted Buckets	Interval	Owner
1	1	50	50	2	Monitor

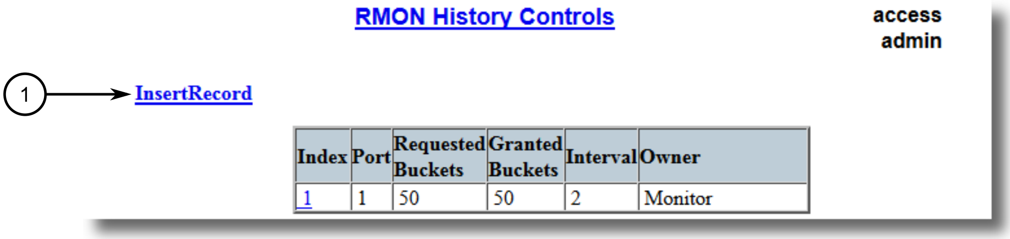
Figure 4.40 RMON History Controls Table

If history controls have not been configured, add controls as needed. For more information, refer to "Adding an RMON History Control (Page 84)".

4.10.1.2 Adding an RMON History Control

To add an RMON history control, do the following:

1. Navigate to ***Ethernet Stats » Configure RMON History Controls***. The **RMON History Controls** table appears.

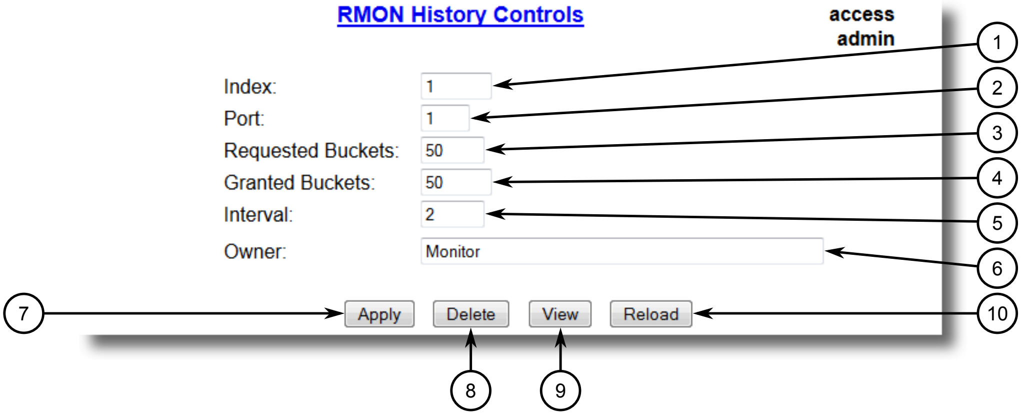


Index	Port	Requested Buckets	Granted Buckets	Interval	Owner
1	1	50	50	2	Monitor

① InsertRecord

Figure 4.41 RMON History Controls Table

2. Click **InsertRecord**. The **RMON History Controls** form appears.



Index:	1
Port:	1
Requested Buckets:	50
Granted Buckets:	50
Interval:	2
Owner:	Monitor

① Index Box
② Port Box
③ Requested Buckets Box
④ Granted Buckets Box
⑤ Interval Box
⑥ Owner Box
⑦ Apply Button
⑧ Delete Button
⑨ Reload Button

Figure 4.42 RMON History Controls Form

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

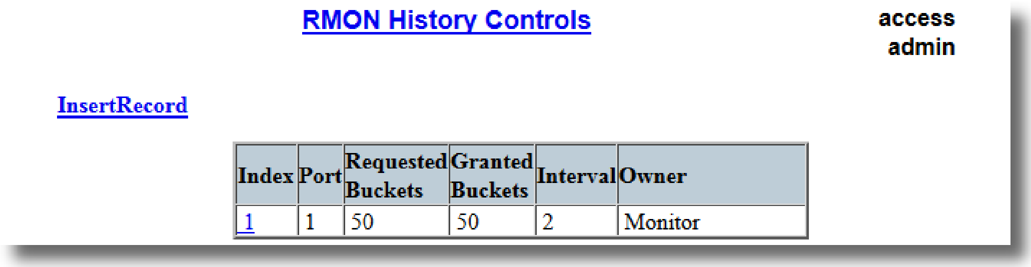
Parameter	Description
`Index`	**Synopsis:** An integer between 1 and 65535 **Default:** 1 The index of this RMON History Contol record.
`Port`	**Synopsis:** 1 to maximum port number **Default:** 1 The port number as seen on the front plate silkscreen of the switch.
`Requested Buckets`	**Synopsis:** An integer between 1 and 4000 **Default:** 50 The maximum number of buckets requested for this RMON collection history group of statistics. The range is 1 to 4000. The default is 50.
`Granted Buckets`	**Synopsis:** An integer between 0 and 65535 The number of buckets granted for this RMON collection history. This field is not editable.
`Interval`	**Synopsis:** An integer between 1 and 3600 **Default:** 1800 The number of seconds in over which the data is sampled for each bucket. The range is 1 to 3600. The default is 1800.
`Owner`	**Synopsis:** A string 127 characters long **Default:** Monitor The owner of this record. It is suggested to start this string withword 'monitor'.

4. Click **Apply**.

4.10.1.3 Deleting an RMON History Control

To delete an RMON history control, do the following:

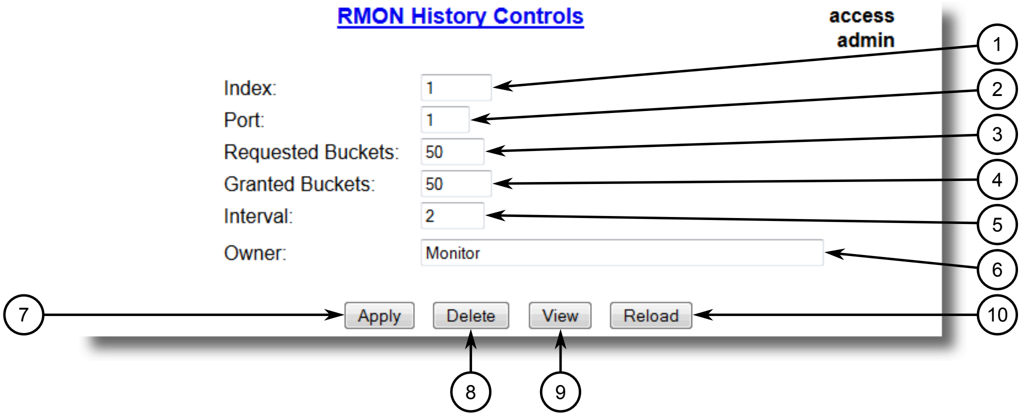
1. Navigate to ***Ethernet Stats » Configure RMON History Controls***. The **RMON History Controls** table appears.



Index	Port	Requested Buckets	Granted Buckets	Interval	Owner
1	1	50	50	2	Monitor

Figure 4.43 RMON History Controls Table

2. Select the history control from the table. The **RMON History Controls** form appears.



RMON History Controls

Index:	1
Port:	1
Requested Buckets:	50
Granted Buckets:	50
Interval:	2
Owner:	Monitor

① Index Box
② Port Box
③ Requested Buckets Box
④ Granted Buckets Box
⑤ Interval Box
⑥ Owner Box
⑦ Apply Button
⑧ Delete Button
⑨ Reload Button

Figure 4.44 RMON History Controls Form

3. Click **Delete**.

4.10.2 Managing RMON Alarms

When Remote Monitoring (RMON) alarms are configured, RUGGEDCOM ROS examines the state of a specific statistical variable.

Remote Monitoring (RMON) alarms define upper and lower thresholds for legal values of specific statistical variables in a given interval. This allows RUGGEDCOM ROS to detect events as they occur more quickly than a specified maximum rate or less quickly than a minimum rate.

When the rate of change for a statistics value exceeds its limits, an internal INFO alarm is always generated. For information about viewing alarms, refer to "Viewing and Clearing Latched Alarms (Page 104)".

Additionally, a statistic threshold crossing can result in further activity. An RMON alarm can be configured to point to a particular RMON event, which can generate an SNMP trap, an entry in the event log, or both. The RMON event can also direct alarms towards different users defined for SNMP.

The alarm can point to a different event for each of the thresholds. Therefore, combinations such as *trap on rising threshold* or *trap on rising threshold, log and trap on falling threshold* are possible.

Each RMON alarm may be configured such that its first instance occurs only for rising, falling, or all thresholds that exceed their limits.

The ability to configure upper and lower thresholds on the value of a measured statistic provides for the ability to add hysteresis to the alarm generation process.

If the value of the measured statistic over time is compared to a single threshold, alarms will be generated each time the statistic crosses the threshold. If the statistic's value fluctuates around the threshold, an alarm can be generated every measurement period. Programming different upper and lower thresholds eliminates spurious alarms. The statistic value must *travel* between the thresholds before alarms can be generated. The following illustrates the very different patterns of alarm generation resulting from a statistic sample and the same sample with hysteresis applied.

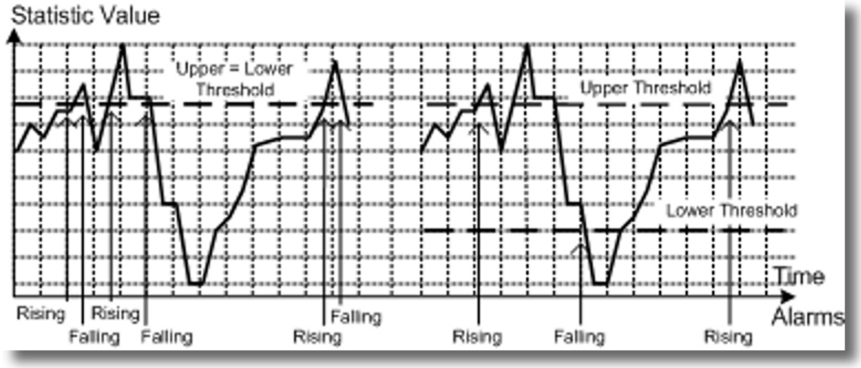


Figure 4.45 The Alarm Process

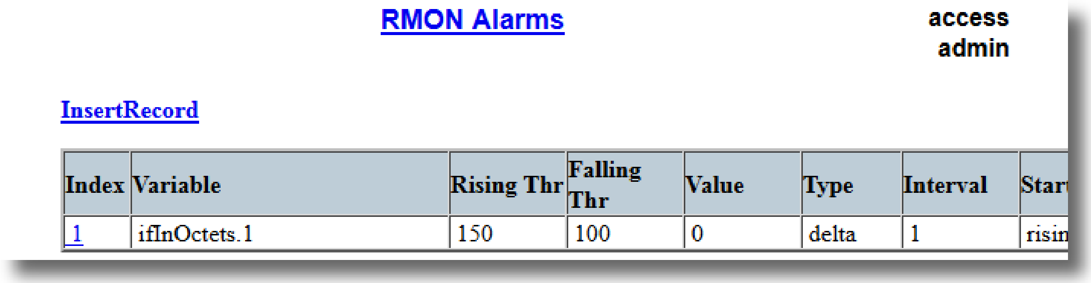
There are two methods to evaluate a statistic to determine when to generate an event: delta and absolute.

For most statistics, such as line errors, it is appropriate to generate an alarm when a rate is exceeded. The alarm defaults to the *delta* measurement method, which examines changes in a statistic at the end of each measurement period.

It may be desirable to alarm when the total, or absolute, number of events crosses a threshold. In this case, set the measurement period type to *absolute*.

4.10.2.1 Viewing a List of RMON Alarms

To view a list of RMON alarms, navigate to ***Ethernet Stats » Configure RMON Alarms***. The **RMON Alarms** table appears.



RMON Alarms

access
admin

InsertRecord

Index	Variable	Rising Thr	Falling Thr	Value	Type	Interval	Star
1	ifInOctets.1	150	100	0	delta	1	risin

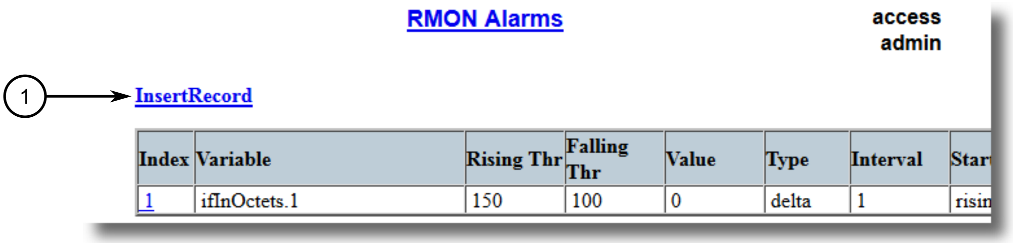
Figure 4.46 RMON Alarms Table

If alarms have not been configured, add alarms as needed. For more information, refer to "Adding an RMON Alarm (Page 88)".

4.10.2.2 Adding an RMON Alarm

To add an RMON alarm, do the following:

1. Navigate to ***Ethernet Stats » Configure RMON Alarms***. The **RMON Alarms** table appears.



RMON Alarms

access
admin

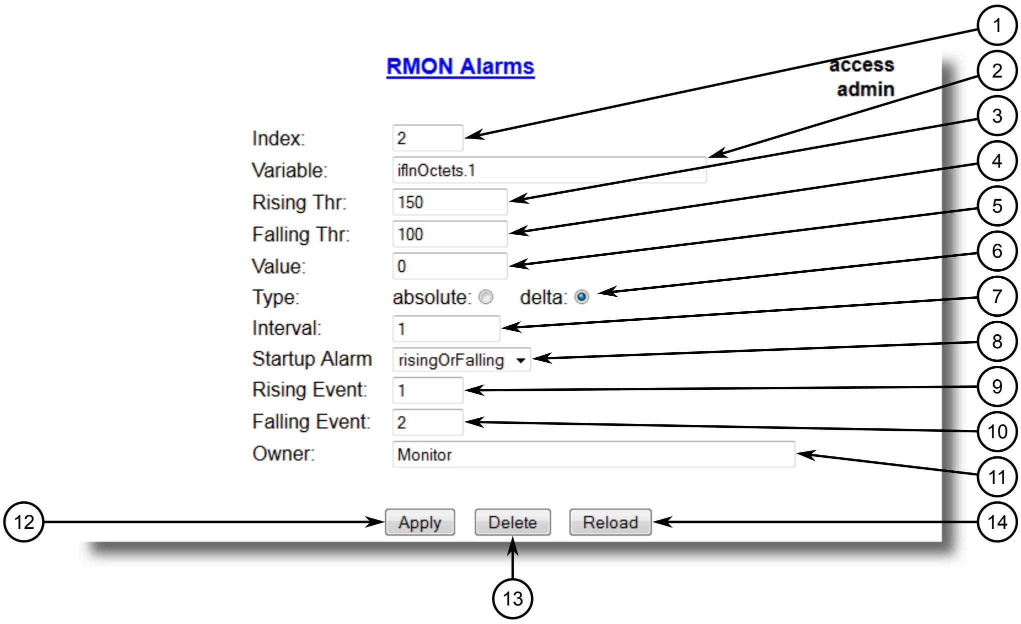
InsertRecord

Index	Variable	Rising Thr	Falling Thr	Value	Type	Interval	Star
1	ifInOctets.1	150	100	0	delta	1	risin

① InsertRecord

Figure 4.47 RMON Alarms Table

2. Click **InsertRecord**. The **RMON Alarms** form appears.



RMON Alarms

access
admin

Index:	2
Variable:	ifInOctets.1
Rising Thr:	150
Falling Thr:	100
Value:	0
Type:	absolute: ○ delta: ●
Interval:	1
Startup Alarm	risingOrFalling
Rising Event:	1
Falling Event:	2
Owner:	Monitor

① Index Box
② Variable Box
③ Rising Thr Box
④ Falling Thr Box
⑤ Value Box
⑥ Type Options
⑦ Interval Box
⑧ Startup Alarm List
⑨ Rising Event Box
⑩ Falling Event Box
⑪ Owner Box
⑫ Apply Button
⑬ Delete Button
⑭ Reload Button

Figure 4.48 RMON Alarms Form

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

Parameter	Description
`Index`	**Synopsis:** An integer between 1 and 65535 **Default:** 1 The index of this RMON Alarm record.
`Variable`	**Synopsis:** An integer The SNMP object identifier (OID) of the particular variable to be sampled. Only variables that resolve to an ASN.1 primitive type INTEGER (INTEGER, Integer32,Counter32, Counter64, Gauge, or TimeTicks) may be sampled. A list of objects can be printed using shell command 'rmon'. The OID format: objectName.in-

Parameter	Description
	dex1.index2... where index format depends on index object type.
`Rising Thr`	**Synopsis:** An integer between -2147483647 and 2147483647 **Default:** 0 A threshold for the sampled variable. When the current sampled variable value is greater than or equal to this threshold, and the value at the last sampling interval was less than this threshold, a single event will be generated. A single event will also be generated if the first sample after this record is created is greater than or equal to this threshold and the associated startup alarm ils equal to 'rising'.After rising alarm is generated, another such event will not be generated until the sampled value falls below this threshold and reaches the value of FallingThreshold.
`Falling Thr`	**Synopsis:** An integer between -2147483647 and 2147483647 **Default:** 0 A threshold for the sampled variable. When the current sampled variable value is less than or equal to this threshold, and the value at the last sampling interval was greater than this threshold, a single event will be generated. A single event will also be generated if the first sample after this record is created is less than or equal to this threshold and the associated startup alarm ils equal to 'falling'.After falling alarm is generated, another such event will not be generated until the sampled value rises above this threshold and reaches the value of RisingThreshold.
`Value`	**Synopsis:** An integer between -2147483647 and 2147483647 The value of monitoring object during the last sampling period. The presentation of value depends of sample type ('absolute' or 'delta').
`Type`	**Synopsis:** [absolute | delta] **Default:** delta The method of sampling the selected variable and calculating the value to be compared against the thresholds. The value of sample type can be 'absolute' or 'delta'.
`Interval`	**Synopsis:** An integer between 0 and 2147483647 **Default:** 60 The number of seconds in over which the data is sampled and compared with the rising and falling thresholds.
`Startup Alarm`	**Synopsis:** [rising | falling | risingOrFalling] **Default:** risingOrFalling The alarm that may be sent when this record is first created if condition for raising alarm is met. The value of startup alarm can be 'rising', 'falling' or 'risingOrFalling'.
`Rising Event`	**Synopsis:** An integer between 0 and 65535 **Default:** 0 The index of the event that is used when a falling threshold is crossed. If there is no corresponding entryl in the Event Table,

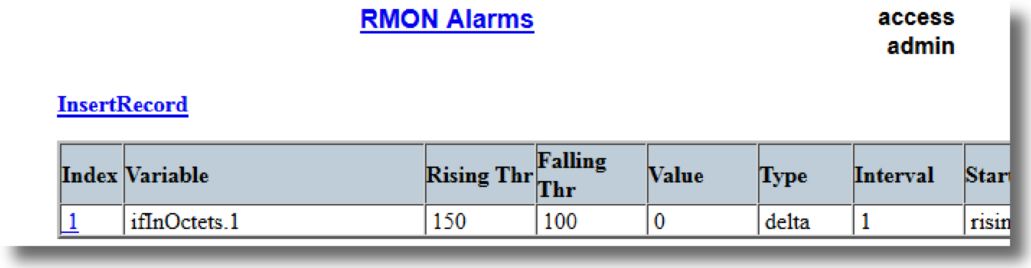
Parameter	Description
	then no association exists. In particular, if this value is zero, no associated event will be generated.
`Falling Event`	**Synopsis:** An integer between 0 and 65535 **Default:** 0 The index of the event that is used when a rising threshold is crossed. If there is no corresponding entryl in the Event Table, then no association exists. In particular, if this value is zero, no associated event will be generated.
`Owner`	**Synopsis:** A string 127 characters long **Default:** Monitor The owner of this record. It is suggested to start this string withword 'monitor'.

4. Click **Apply**.

4.10.2.3 Deleting an RMON Alarm

To delete an RMON alarm, do the following:

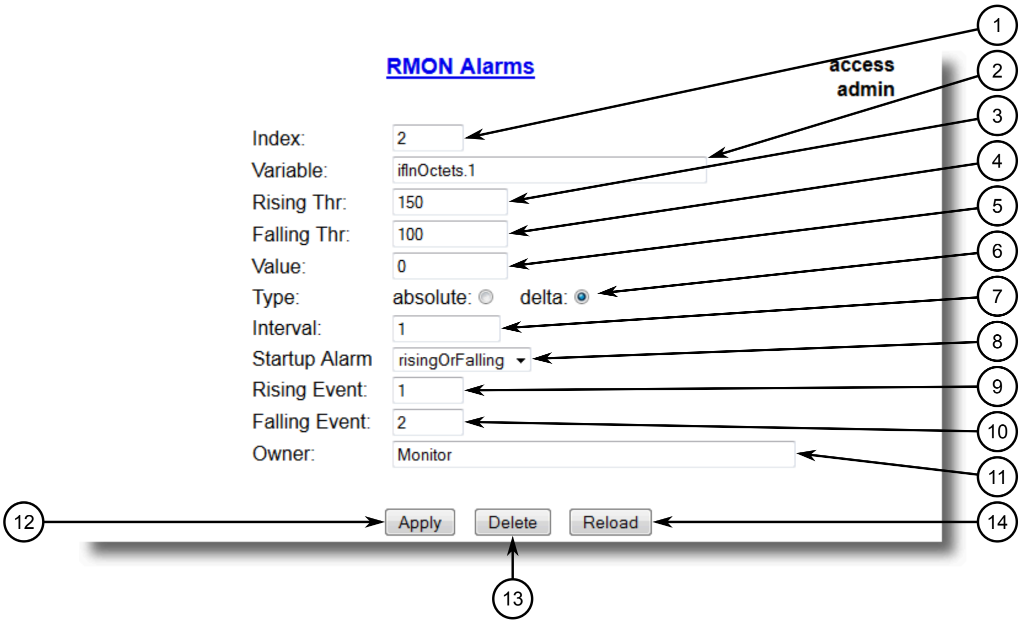
1. Navigate to ***Ethernet Stats » Configure RMON Alarms***. The **RMON Alarms** table appears.



Index	Variable	Rising Thr	Falling Thr	Value	Type	Interval	Star
1	ifInOctets.1	150	100	0	delta	1	risin

Figure 4.49 RMON Alarms Table

2. Select the alarm from the table. The **RMON Alarms** form appears.


RMON Alarms

access
admin

Index: 2
Variable: ifInOctets.1
Rising Thr: 150
Falling Thr: 100
Value: 0
Type: absolute: ○ delta: ●
Interval: 1
Startup Alarm risingOrFalling
Rising Event: 1
Falling Event: 2
Owner: Monitor

① Index Box
② Variable Box
③ Rising Thr Box
④ Falling Thr Box
⑤ Value Box
⑥ Type Options
⑦ Interval Box
⑧ Startup Alarm List
⑨ Rising Event Box
⑩ Falling Event Box
⑪ Owner Box
⑫ Apply Button
⑬ Delete Button
⑭ Reload Button

Figure 4.50 RMON Alarms Form

3. Click **Delete**.

4.10.3 Managing RMON Events

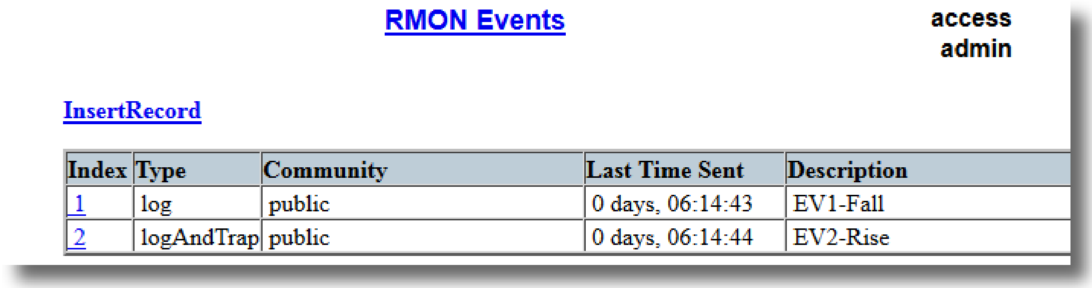
Remote Monitoring (RMON) events define behavior profiles used in event logging. These profiles are used by RMON alarms to send traps and log events.

Each alarm may specify that a log entry be created on its behalf whenever the event occurs. Each entry may also specify that a notification should occur by way of SNMP trap messages. In this case, the user for the trap message is specified as the *Community*.

Two traps are defined: risingAlarm and fallingAlarm.

4.10.3.1 Viewing a List of RMON Events

To view a list of RMON events, navigate to ***Ethernet Stats » Configure RMON Events***. The **RMON Events** table appears.



RMON Events

access
admin

InsertRecord

Index	Type	Community	Last Time Sent	Description
1	log	public	0 days, 06:14:43	EV1-Fall
2	logAndTrap	public	0 days, 06:14:44	EV2-Rise

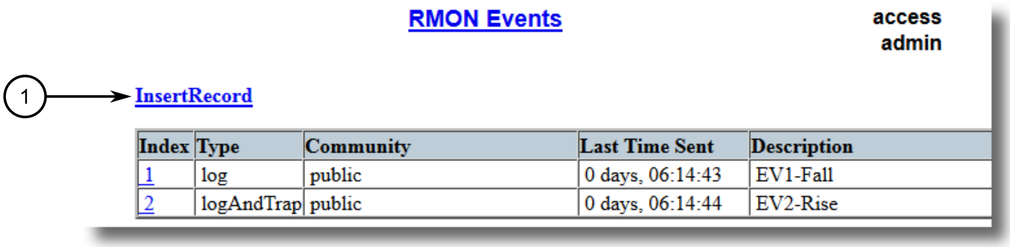
Figure 4.51 RMON Events Table

If events have not been configured, add events as needed. For more information, refer to "Adding an RMON Event (Page 93)".

4.10.3.2 Adding an RMON Event

To add an RMON alarm, do the following:

1. Navigate to ***Ethernet Stats » Configure RMON Events***. The **RMON Events** table appears.



RMON Events

access
admin

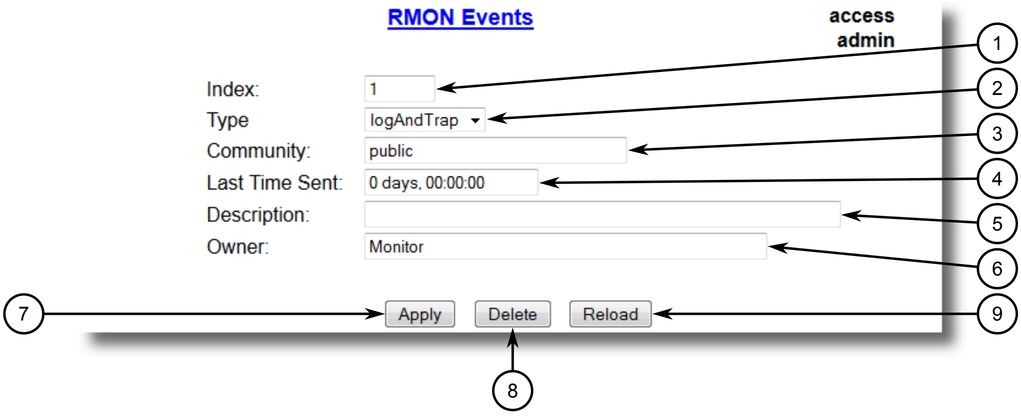
InsertRecord

Index	Type	Community	Last Time Sent	Description
1	log	public	0 days, 06:14:43	EV1-Fall
2	logAndTrap	public	0 days, 06:14:44	EV2-Rise

① InsertRecord

Figure 4.52 RMON Events Table

2. Click **InsertRecord**. The **RMON Events** form appears.



RMON Events

access admin

Index:	1
Type	logAndTrap
Community:	public
Last Time Sent:	0 days, 00:00:00
Description:	
Owner:	Monitor

① Index Box
② Type List
③ Community Box
④ Last Time Sent Box
⑤ Description Box
⑥ Owner Box
⑦ Apply Button
⑧ Delete Button
⑨ View Button
⑩ Reload Button

Figure 4.53 RMON Events Form

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

Parameter	Description
`Index`	**Synopsis:** An integer between 1 and 65535 **Default:** 3 The index of this RMON Event record.
`Type`	**Synopsis:** [none | log | snmpTrap | logAndTrap] **Default:** logAndTrap The type of notification that the probe will make about this event. In the case of 'log', an entry is made in the RMON Log table for each event. In the case of snmp_trap, an SNMP trap is sent to one or more management stations.
`Community`	**Synopsis:** A string 31 characters long **Default:** public If the SNMP trap is to be sent, it will be sent to the SNMP community specified by this string.
`Last Time Sent`	**Synopsis:** DDDD days, HH:MM:SS The time from last reboot at the time this event entry last generated an event. If this entry has not generated any events, this value will be 0.

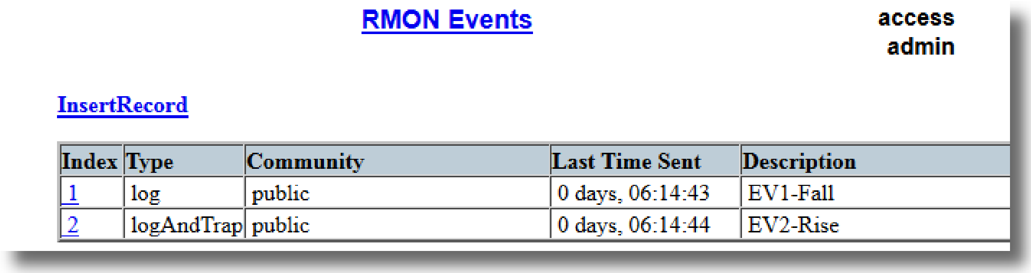
Parameter	Description
`Description`	**Synopsis:** A string 127 characters long **Default:** EV2-Rise A comment describing this event.
`Owner`	**Synopsis:** A string 127 characters long **Default:** Monitor The owner of this event record. It is suggested to start this string withword 'monitor'.

4. Click **Apply**.

4.10.3.3 Deleting an RMON Event

To delete an RMON event, do the following:

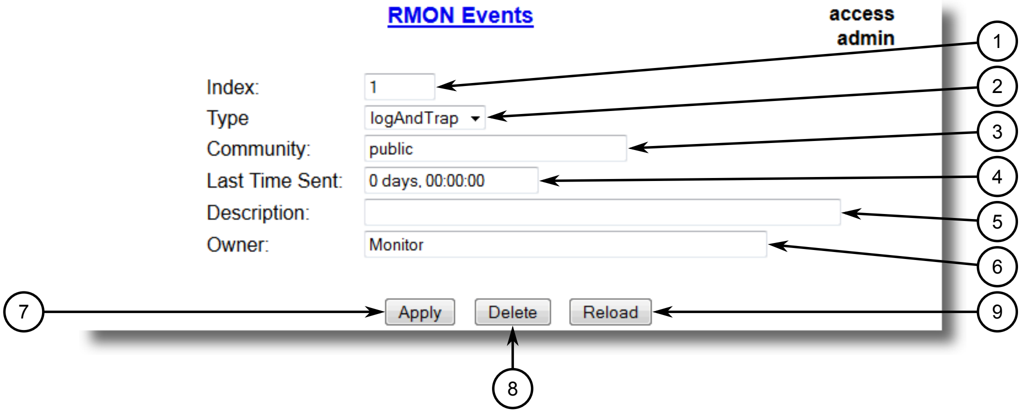
1. Navigate to ***Ethernet Stats » Configure RMON Events***. The **RMON Events** table appears.



Index	Type	Community	Last Time Sent	Description
1	log	public	0 days, 06:14:43	EV1-Fall
2	logAndTrap	public	0 days, 06:14:44	EV2-Rise

Figure 4.54 RMON Events Table

2. Select the event from the table. The **RMON Events** form appears.



RMON Events

access
admin

Index: 1
Type logAndTrap
Community: public
Last Time Sent: 0 days, 00:00:00
Description:
Owner: Monitor

① Index Box
② Type List
③ Community Box
④ Last Time Sent Box
⑤ Description Box
⑥ Owner Box
⑦ Apply Button
⑧ Delete Button
⑨ View Button
⑩ Reload Button

Figure 4.55 RMON Events Form

3. Click **Delete**.

4.11 Upgrading/Downgrading Firmware

This section describes how to upgrade and downgrade the firmware for RUGGEDCOM ROS.

4.11.1 Upgrading Firmware

Upgrading RUGGEDCOM ROS firmware, including the main, bootloader and FPGA firmware, may be necessary to take advantage of new features or bug fixes. Binary firmware releases, including updates, can be obtained by submitting a Support Request via the Siemens Industry Online Support [https://support.industry.siemens.com] website. For more information, refer to https://support.industry.siemens.com/My/ww/en/requests.

Binary firmware images transferred to the device are stored in non-volatile Flash memory and require a device reset to take effect.

Note

The IP address set for the device will not be changed following a firmware upgrade.

To upgrade the RUGGEDCOM ROS firmware, do the following:

1. Upload a different version of the binary firmware image to the device. For more information, refer to "Uploading/Downloading Files (Page 41)".
2. Reset the device to complete the installation. For more information, refer to "Resetting the Device (Page 98)".
3. Access the CLI shell and verify the new software version has been installed by typing **`version`**. The currently installed versions of the main and boot firmware are displayed.

```
>version
Current ROS-CF52 Boot Software v2.20.0 (Jan 01 4.3  00:01)
Current ROS-CF52 Main Software v4.3 .0 (Jan 01 4.3 00:01)
```

4.11.2 Downgrading Firmware

Downgrading the RUGGEDCOM ROS firmware is generally not recommended, as it may have unpredictable effects. However, if a downgrade is required, do the following:

⚠ NOTICE

Before downgrading the firmware, make sure the hardware and FPGA code types installed in the device are supported by the older firmware version. Refer to the Release Notes for the older firmware version to confirm.

⚠ CAUTION

Do not downgrade the RUGGEDCOM ROS boot version.

1. Disconnect the device from the network.
2. Log in to the device as an admin user. For more information, refer to "Logging In (Page 12)".
3. Make a local copy of the current configuration file. For more information, refer to "Uploading/Downloading Files (Page 41)".

   ⚠ NOTICE

   Never downgrade the firmware with encryption enabled to a version that does not support encryption.

4. Restore the device to its factory defaults. For more information, refer to "Restoring Factory Defaults (Page 40)".
5. Upload and apply the older firmware version and its associated FPGA files using the same methods used to install newer firmware versions. For more information , refer to "Upgrading Firmware (Page 96)".
6. Press **Ctrl-S** to access the CLI.

7. Clear all logs by typing:

   ```
   clearlogs
   ```

8. Clear all alarms by typing:

   ```
   clearalarms
   ```

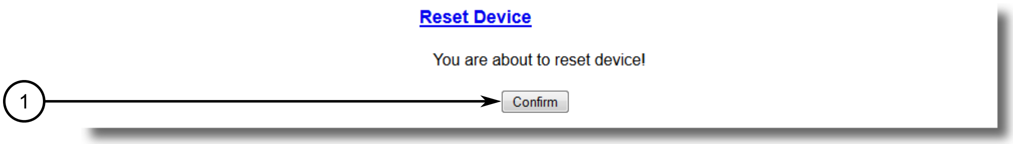
   > ⚠ **NOTICE**
   >
   > After downgrading the firmware and FPGA files, be aware that some settings from the previous configuration may be lost or reverted back to the factory defaults (including user passwords if downgrading from a security related version), as those particular tables or fields may not exist in the older firmware version. Because of this, the unit must be configured after the downgrade.

9. Configure the device as required.

4.12 Resetting the Device

To reset the device, do the following:

1. Navigate to ***Diagnostics » Reset Device***. The **Reset Device** form appears.



Reset Device

You are about to reset device!

① Confirm Button

Figure 4.56 Reset Device Form

2. Click **Confirm**.

4.13 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. Disconnect all network cables from the device.
2. Connect to the device via the RS-232 serial console port. For more information, refer to "Connecting Directly (Page 33)".
3. Restore all factory default settings for the device. For more information, refer to "Restoring Factory Defaults (Page 40)".

4. Access the CLI. For more information, refer to "Using the Command Line Interface (Page 17)".
5. Upload a blank version of the `banner.txt` file to the device to replace the existing file. For more information about uploading a file, refer to "Uploading/Downloading Files (Page 41)".
6. Confirm the upload was successful by typing:

   ```
   type banner.txt
   ```

7. Clear the system and crash logs by typing:

   ```
   clearlog
   ```

8. Generate a random SSL certificate by typing:

   ```
   sslkeygen
   ```

   This may take several minutes to complete. To verify the certificate has been generated, type:

   ```
   type syslog.txt
   ```

   When the phrase `Generated ssl.crt was saved` appears in the log, the SSL certificate has been generated.
9. Generate random SSH keys by typing:

   ```
   sshkeygen
   ```

   This may take several minutes to complete. To verify the keys have been generated, type:

   ```
   type syslog.txt
   ```

   When the phrase `Generated ssh.keys was saved` appears in the log, the SSH keys have been generated.
10. De-fragment and erase all free flash memory by typing:

    ```
    flashfile defrag
    ```

    This may take several minutes to complete.

System Administration

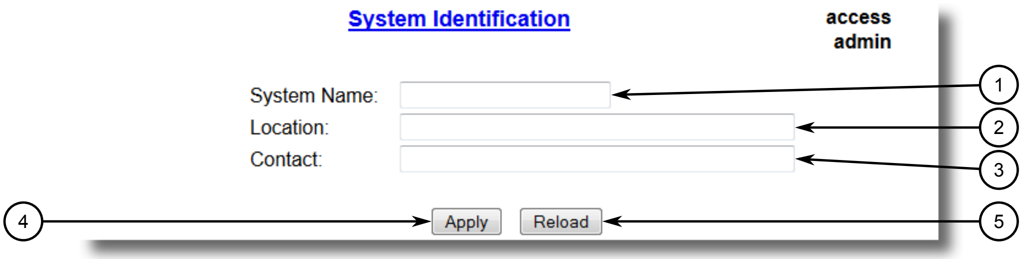
5

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

5.1 Configuring the System Information

To configure basic information that can be used to identify the device, its location, and/or its owner, do the following:

1. Navigate to ***Administration » Configure System Identification***. The **System Identification** form appears.



① System Name Box
② Location Box
③ Contact Box
④ Apply Button
⑤ Reload Button

Figure 5.1 System Identification Form

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

Parameter	Description
`System Name`	**Synopsis:** A string 24 characters long The system name is displayed in all RUGGEDCOM ROS menu screens. This can make it easier to identify the switches within your network provided that all switches are given a unique name.
`Location`	**Synopsis:** A string 49 characters long The location can be used to indicate the physical location of the switch. It is displayed in the login screen as another means to ensure you are dealing with the desired switch.

Parameter	Description
`Contact`	**Synopsis:** A string 49 characters long The contact can be used to help identify the person responsible for managing the switch. You can enter name, phone number, email, etc. It is displayed in the login screen so that this person may be contacted should help be required.

3. Click **Apply**.

5.2 Customizing the Login Screen

To display a custom welcome message, device information or any other information on the login screen for the Web and console interfaces, add text to the `banner.txt` file stored on the device.

If the `banner.txt` file is empty, only the **Username** and **Password** fields appear on the login screen.

To update the `banner.txt` file, download the file from the device, modify it and then load it back on to the device. For information about uploading and downloading files, refer to "Uploading/Downloading Files (Page 41)".

5.3 Enabling/Disabling the Web Interface

In some cases, users may want to disable the Web interface to increase cyber security.

To disable or enable the Web interface, do the following:

Note
The Web interface can be disabled via the Web UI by configuring the Web Server Users Allowed parameter in the **IP Services form**. For more information, refer to "Configuring IP Services (Page 81)".

1. Log in to the device as an admin user and access the CLI shell. For more information about accessing the CLI shell, refer to "Using the Command Line Interface (Page 17)".
2. Navigate to ***Administration » Configure IP Services » Web Server Users Allowed***.
3. Select **Disabled** to disable the Web interface, or select the desired number of Web server users allowed to enable the interface.

5.4 Managing Alarms

Alarms indicate the occurrence of events of either importance or interest that are logged by the device.

There are two types of alarms:

- **Active alarms** signify states of operation that are not in accordance with normal operation. Examples include links that should be up, but are not, or error rates that repeatedly exceed a certain threshold. These alarms are continuously active and are only cleared when the problem that triggered the alarms is resolved.
- **Passive alarms** are a record of abnormal conditions that occurred in the past and do not affect the current operation state of the device. Examples include authentication failures, Remote Network MONitoring (RMON) MIB generated alarms, or error states that temporarily exceeded a certain threshold . These alarms can be cleared from the list of alarms.

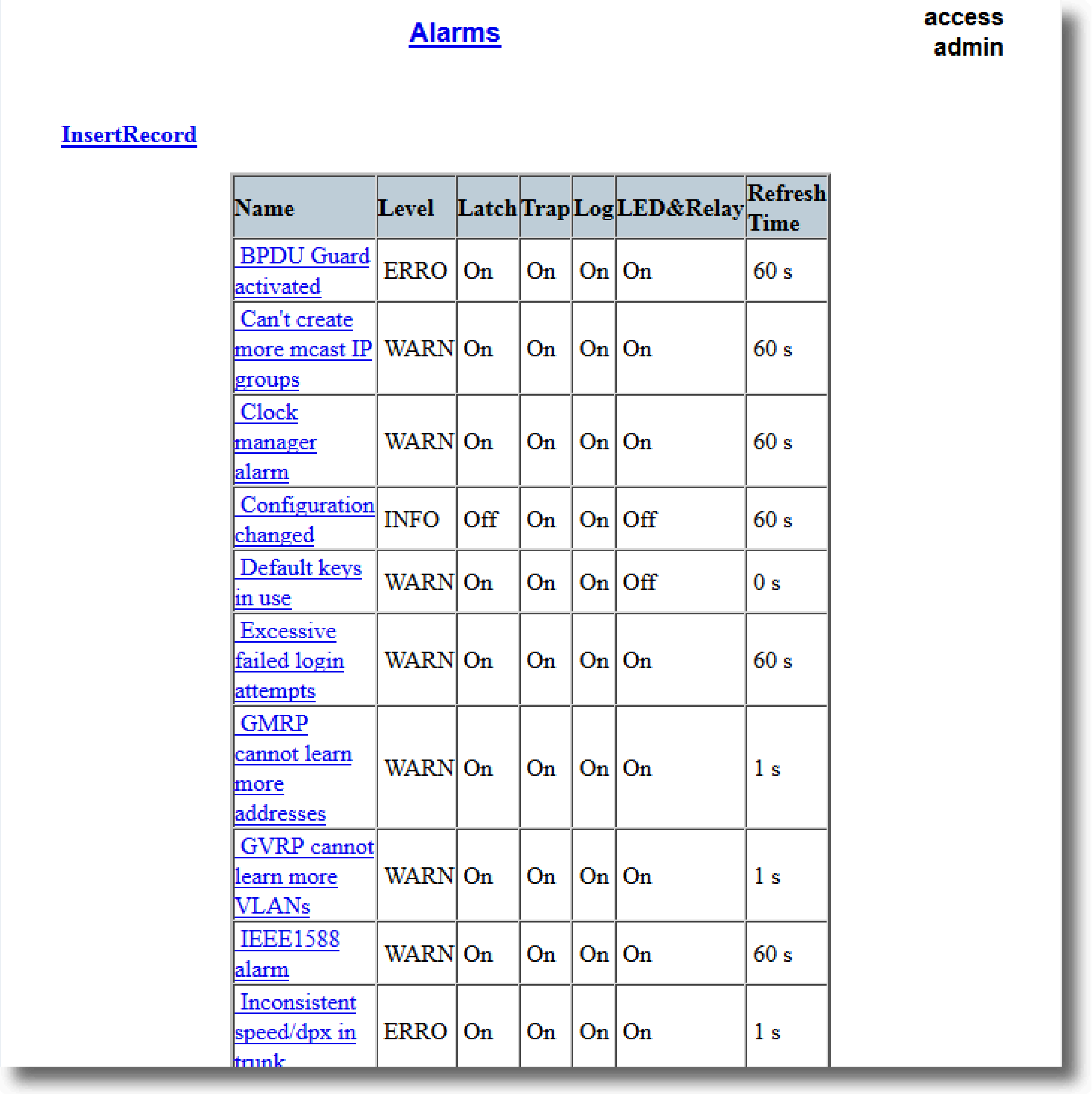
Note
For more information about RMON alarms, refer to "Managing RMON Alarms (Page 86)".

When either type of alarm occurs, a message appears in the top right corner of the user interface. If more than one alarm has occurred, the message will indicate the number of alarms. Active alarms also trip the Critical Failure Relay LED on the device. The message and the LED will remain active until the alarm is cleared.

Note
Alarms are volatile in nature. All alarms (active and passive) are cleared at startup.

5.4.1 Viewing a List of Pre-Configured Alarms

To view a list of alarms pre-configured for the device, navigate to ***Diagnostic » Configure Alarms***. The **Alarms** table appears.



Alarms

access
admin

InsertRecord

Name	Level	Latch	Trap	Log	LED&Relay	Refresh Time
BPDU Guard activated	ERRO	On	On	On	On	60 s
Can't create more mcast IP groups	WARN	On	On	On	On	60 s
Clock manager alarm	WARN	On	On	On	On	60 s
Configuration changed	INFO	Off	On	On	Off	60 s
Default keys in use	WARN	On	On	On	Off	0 s
Excessive failed login attempts	WARN	On	On	On	On	60 s
GMRP cannot learn more addresses	WARN	On	On	On	On	1 s
GVRP cannot learn more VLANs	WARN	On	On	On	On	1 s
IEEE1588 alarm	WARN	On	On	On	On	60 s
Inconsistent speed/dpx in trunk	ERRO	On	On	On	On	1 s

Figure 5.2 Alarms Table

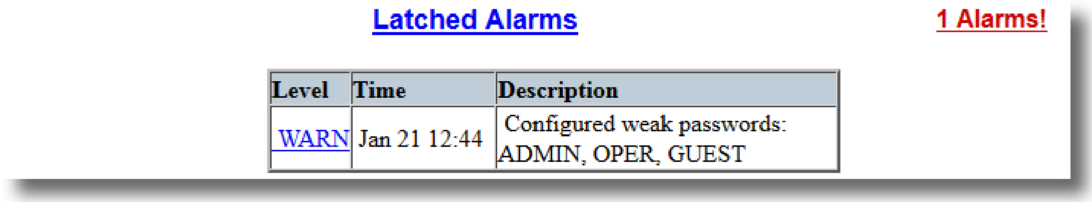
Note

This list of alarms (configurable and non-configurable) is accessible through the Command Line Interface (CLI) using the `alarms` command. For more information, refer to "Available CLI Commands (Page 17)".

For information about modifying a pre-configured alarm, refer to "Configuring an Alarm (Page 105)".

5.4.2 Viewing and Clearing Latched Alarms

To view a list of alarms that are configured to latch, navigate to ***Diagnostics » View Latched Alarms***. The **Latched Alarms** table appears.



Latched Alarms

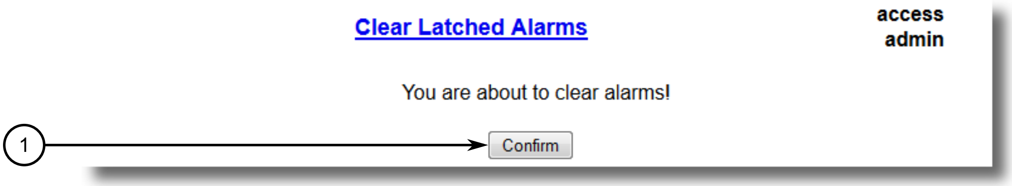
1 Alarms!

Level	Time	Description
WARN	Jan 21 12:44	Configured weak passwords: ADMIN, OPER, GUEST

Figure 5.3 Latched Alarms Table

To clear the passive alarms from the list, do the following:

1. Navigate to ***Diagnostics » Clear Latched Alarms***. The **Clear Latched Alarms** form appears.



Clear Latched Alarms

access
admin

You are about to clear alarms!

① Confirm Button

Figure 5.4 Clear Latched Alarms Form

2. Click **Confirm**.

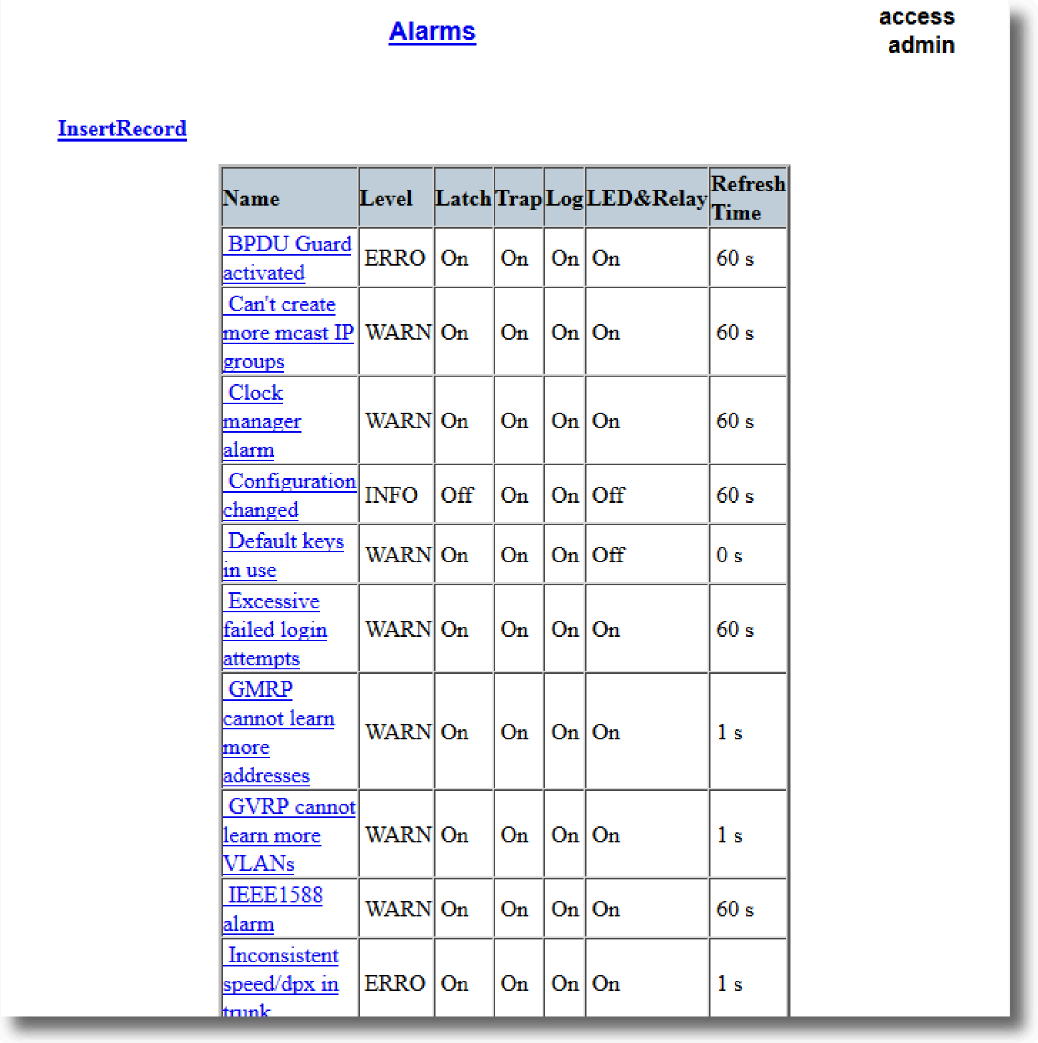
5.4.3 Configuring an Alarm

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

To configuring an alarm, do the following:

⚠ NOTICE
Critical and Alert level alarms are not configurable and cannot be disabled.

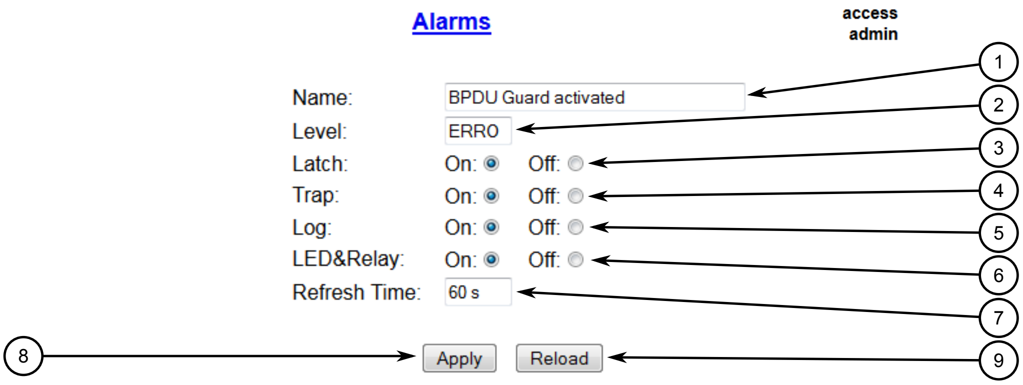
1. Navigate to ***Diagnostic » Configure Alarms***. The **Alarms** table appears.



Name	Level	Latch	Trap	Log	LED&Relay	Refresh Time
BPDU Guard activated	ERRO	On	On	On	On	60 s
Can't create more mcast IP groups	WARN	On	On	On	On	60 s
Clock manager alarm	WARN	On	On	On	On	60 s
Configuration changed	INFO	Off	On	On	Off	60 s
Default keys in use	WARN	On	On	On	Off	0 s
Excessive failed login attempts	WARN	On	On	On	On	60 s
GMRP cannot learn more addresses	WARN	On	On	On	On	1 s
GVRP cannot learn more VLANs	WARN	On	On	On	On	1 s
IEEE1588 alarm	WARN	On	On	On	On	60 s
Inconsistent speed/dpx in trunk	ERRO	On	On	On	On	1 s

Figure 5.5 Alarms Table

2. Select an alarm. The **Alarms** form appears.



Alarms

access
admin

Name:	BPDU Guard activated	
Level:	ERRO	
Latch:	On: ●	Off: ○
Trap:	On: ●	Off: ○
Log:	On: ●	Off: ○
LED&Relay:	On: ●	Off: ○
Refresh Time:	60 s	

① Name Box
② Level Box
③ Latch Box
④ Trap Box
⑤ Log Box
⑥ LED & Relay Box
⑦ Refresh Time Box
⑧ Apply Button
⑨ Reload Button

Figure 5.6 Alarms Form

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

Parameter	Description
`Name`	**Synopsis:** A string 34 characters long or [sys_alarm] **Default:** sys_alarm The alarm name, as obtained through the **`alarms`** CLI command.
`Level`	**Synopsis:** [EMRG | ALRT | CRIT | ERRO | WARN | NOTE | INFO | DEBG] Severity level of the alarm: • EMRG – The device has had a serious failure that caused a system reboot. • ALERT – The device has had a serious failure that did not cause a system reboot. • CRIT – The device has a serious unrecoverable problem. • ERRO – The device has a recoverable problem that does not seriously affect operation. • WARN – Possibly serious problem affecting overall system operation. • NOTE – Condition detected that is not expected or not allowed. • INFO – Event which is a part of normal operation, e.g. cold start, user login etc.

Parameter	Description
	• DEBG – Intended for factory troubleshooting only. This parameter is not configurable.
`Latch`	**Synopsis:** [On | Off] **Default:** Off Enables latching occurrence of this alarm in the Alarms Table.
`Trap`	**Synopsis:** [On | Off] **Default:** Off Enables sending an SNMP trap for this alarm.
`Log`	**Synopsis:** [On | Off] **Default:** Off Enables logging the occurrence of this alarm in syslog.txt.
`LED & Relay`	**Synopsis:** [On | Off] **Default:** Off Enables LED and fail-safe relay control for this alarm. If latching is not enabled, this field will remain disabled.
`Refresh Time`	**Synopsis:** An integer between 0 and 60 **Default:** 60 Refreshing time for this alarm.

4. Click **Apply**.

5.4.4 Authentication Related Security Alarms

This section describes the authentication-related security messages that can be generated by RUGGEDCOM ROS.

5.4.4.1 Security Alarms for Login Authentication

RUGGEDCOM ROS provides various logging options related to login authentication. A user can log into a RUGGEDCOM ROS device via four different methods: Web, console, SSH or Telnet. RUGGEDCOM ROS can log messages in the syslog, send a trap to notify an SNMP manager, and/or raise an alarm when a successful and unsuccessful login event occurs. In addition, when a weak password is configured on a unit or when the primary authentication server for TACACS+ or RADIUS is not reachable, RUGGEDCOM ROS will raise alarms, send SNMP traps and log messages in the syslog.

The following is a list of log and alarm messages related to user authentication:

- Weak Password Configured
- Login and Logout Information
- Excessive Failed Login Attempts

- RADIUS Server Unreachable
- TACACS Server Unreachable
- TACACS Response Invalid
- SNMP Authentication Failure

Note
All alarms and log messages related to login authentication are configurable. For more information about configuring alarms, refer to "Configuring an Alarm (Page 105)".

Weak Password Configured

RUGGEDCOM ROS generates this alarm and logs a message in the syslog when a weak password is configured in the **Passwords** table.

Message Name	Alarm	SNMP Trap	Syslog
Weak Password Configured	Yes	Yes	Yes

Default Keys In Use

RUGGEDCOM ROS generates this alarm and logs a message in the syslog when default keys are in use. For more information about default keys, refer to "Managing SSH/SSL Keys and Certificates (Page 135)".

Note
For Non-Controlled (NC) versions of RUGGEDCOM ROS, this alarm is only generated when default SSL keys are in use.

Message Name	Alarm	SNMP Trap	Syslog
Default Keys In Use	Yes	Yes	Yes

Login and Logout Information

RUGGEDCOM ROS generates this alarm and logs a message in the syslog when a successful and unsuccessful login attempt occurs. A message is also logged in the syslog when a user with a certain privilege level is logged out from the device.

Login attempts are logged regardless of how the user accesses the device (i.e. SSH, Web, Console, Telnet or RSH). However, when a user logs out, a message is only logged when the user is accessing the device through SSH, Telnet or Console.

Message Name	Alarm	SNMP Trap	Syslog
Successful Login	Yes	Yes	Yes
Failed Login	Yes	Yes	Yes
User Logout	No	No	Yes

Excessive Failed Login Attempts

RUGGEDCOM ROS generates this alarm and logs a message in the syslog after 10 failed login attempts by a user occur within a span of five minutes. Furthermore, the service the user attempted to access will be blocked for one hour to prevent further attempts.

Message Name	Alarm	SNMP Trap	Syslog
Excessive Failed Login Attempts	Yes	Yes	Yes

RADIUS Server Unreachable

RUGGEDCOM ROS generates this alarm and logs a message in the syslog when the primary RADIUS server is unreachable.

Message Name	Alarm	SNMP Trap	Syslog
Primary RADIUS Server Unreachable	Yes	Yes	Yes

TACACS+ Server Unreachable

RUGGEDCOM ROS generates this alarm and logs a message in the syslog when the primary TACACS+ server is unreachable.

Message Name	Alarm	SNMP Trap	Syslog
Primary TACACS Server Unreachable	Yes	Yes	Yes

TACACS+ Response Invalid

RUGGEDCOM ROS generate this alarm and logs a message in the syslog when the response from the TACACS+ server is received with an invalid CRC.

Message Name	Alarm	SNMP Trap	Syslog
TACACS Response Invalid	Yes	Yes	Yes

SNMP Authentication Failure

RUGGEDCOM ROS generates this alarm, sends an authentication failure trap, and logs a message in the syslog when an SNMP manager with incorrect credentials communicates with the SNMP agent in RUGGEDCOM ROS.

Message Name	Alarm	SNMP Trap	Syslog
SNMP Authentication Failure	Yes	Yes	Yes

5.4.4.2 Security Messages for Port Authentication

The following is the list of log and alarm messages related to port access control in RUGGEDCOM ROS:

- MAC Address Authorization Failure
- Secure Port X Learned MAC Addr on VLAN X
- Port Security Violated

MAC Address Authorization Failure

RUGGEDCOM ROS generates this alarm and logs a message in the syslog when a host connected to a secure port on the device is communicating using a source MAC address which has not been authorized by RUGGEDCOM ROS, or the dynamically learned MAC address has exceeded the total number of MAC addresses configured to be learned dynamically on the secured port. This message is only applicable when the port security mode is set to *Static MAC*.

Message Name	Alarm	SNMP Trap	Syslog
MAC Address Authorization Failure	Yes	Yes	Yes

RUGGEDCOM ROS logs a message in the syslog and sends a configuration change trap when a MAC address is learned on a secure port. Port X indicates the secured port number and VLAN number on that port. This message is not configurable in RUGGEDCOM ROS.

Message Name	SNMP Trap	Syslog
Secure Port X Learned MAC Addr on VLAN X	Yes	Yes

Port Security Violated

This message is only applicable when the security mode for a port is set to "802.1X or 802.1X/MAC-Auth"

RUGGEDCOM ROS this alarm and logs a message in the syslog when the host connected to a secure port tries to communicate using incorrect login credentials.

Message Name	Alarm	SNMP Trap	Syslog
802.1X Port X Authentication Failure	Yes	Yes	Yes
802.1X Port X Authorized Addr. XXX	No	No	Yes

5.5 Managing the Configuration File

The device configuration file for RUGGEDCOM ROS is a single CSV (Comma-Separate Value) formatted ASCII text file, named `config.csv`. It can be downloaded from the device to view, compare against other configuration files, or store for backup purposes. It can also be overwritten by a complete or partial configuration file uploaded to the device.

To prevent unauthorized access to the contents of the configuration file, the file can be encrypted and given a password/passphrase key.

5.5.1 Configuring Data Encryption

To encrypt the configuration file and protect it with a password/passphrase, do the following:

Note
Data encryption is not available in Non-Controlled (NC) versions of RUGGEDCOM ROS . When switching between Controlled and Non-Controlled (NC) versions of RUGGEDCOM ROS , make sure data encryption is disabled. Otherwise, the NC version of RUGGEDCOM ROS will ignore the encrypted configuration file and load the factory defaults.

Note
Only configuration data is encrypted. All comments and table names in the configuration file are saved as clear text.

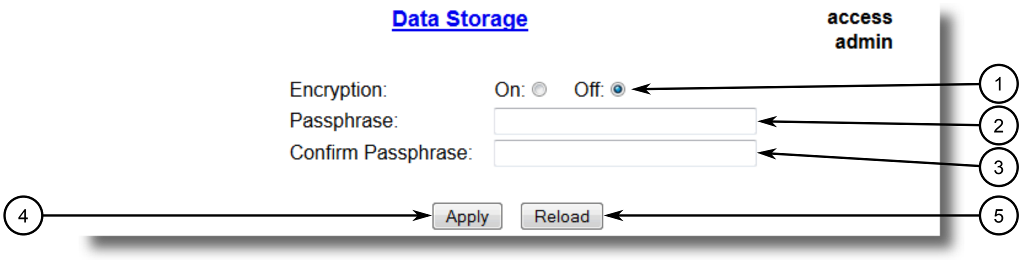
Note
When sharing a configuration file between devices, make sure both devices have the same passphrase configured. Otherwise, the configuration file will be rejected.

Note
Encryption must be disabled before the device is returned to Siemens or the configuration file is shared with Customer Support.

⚠ NOTICE

Never downgrade the RUGGEDCOM ROS software version beyond RUGGEDCOM ROS v4.3 when encryption is enabled. Make sure the device has been restored to factory defaults before downgrading.

1. Navigate to ***Administration » Configure Data Storage***. The **Data Storage** form appears.



Data Storage

Encryption: On: ○ Off: ●

Passphrase:

Confirm Passphrase:

① Encryption Options
② Passphrase Box
③ Confirm Passphrase Box
④ Apply Button
⑤ Reload Button

Figure 5.7 Data Storage Form

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

Parameter	Description
`Encryption`	**Synopsis:** [On | Off] Enable/disable encryption of data in configuration file.
`Passphrase`	**Synopsis:** A string 31 characters long This passphrase is used as a secret key to encrypt the configuration data. Encrypted data can be decrypted by any device configured with the same passphrase.
`Confirm Passphrase`	**Synopsis:** A string 31 characters long This passphrase is used as a secret key to encrypt the configuration data. Encrypted data can be decrypted by any device configured with the same passphrase.

3. Click **Apply**.

5.5.2 Updating the Configuration File

Once downloaded from the device, the configuration file can be updated using a variety of different tools:

Note
For information about uploading/downloading files, refer to "Uploading/Downloading Files (Page 41)".

- Any text editing program capable of reading and writing ASCII files

- Difference/patching tools (e.g. the UNIX *diff* and *patch* command line utilities)
- Source Code Control systems (e.g. CVS, SVN)

⚠ **CAUTION**

Configuration hazard – risk of data loss

Do not edit an encrypted configuration file. Any line that has been modified manually will be ignored.

RUGGEDCOM ROS also has the ability to accept partial configuration updates. For example, to update only the parameters for Ethernet port 1 and leave all other parameters unchanged, transfer a file containing only the following lines to the device:

```
# Port Parameters
ethPortCfg
Port,Name,Media,State,AutoN,Speed,Dupx,FlowCtrl,LFI,Alarm,
1,Port 1,100TX,Enabled,On,Auto,Auto,Off,Off,On,
```

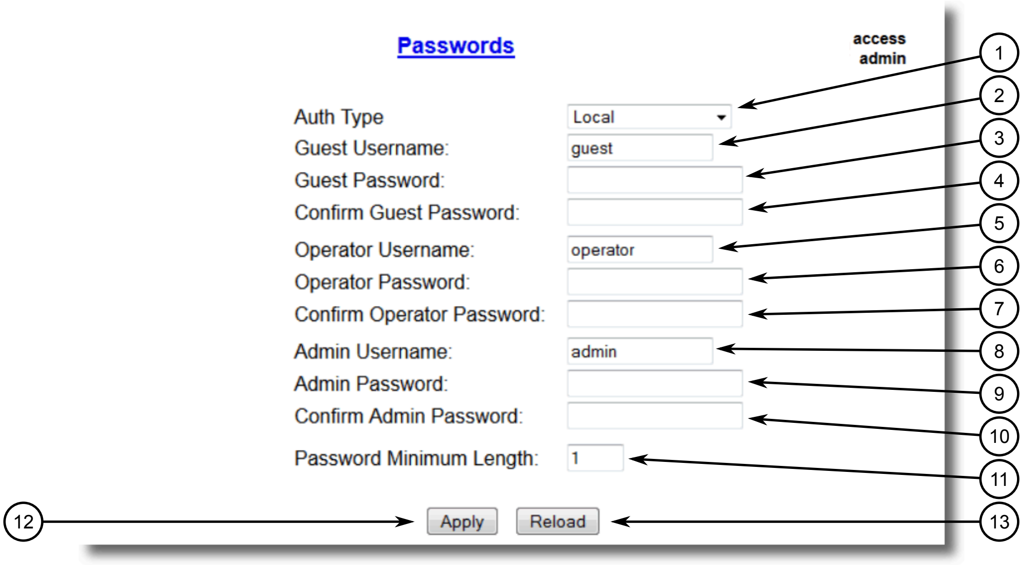
Security 6

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

6.1 Configuring Passwords

To configure passwords for one or more of the user profiles, do the following:

1. Navigate to ***Administration » Configure Passwords***. The **Configure Passwords** form appears.



Passwords

access
admin

Auth Type: Local
Guest Username: guest
Guest Password:
Confirm Guest Password:
Operator Username: operator
Operator Password:
Confirm Operator Password:
Admin Username: admin
Admin Password:
Confirm Admin Password:
Password Minimum Length: 1

① Auth Type Box
② Guest Username Box
③ Guest Password Box
④ Confirm Guest Password Box
⑤ Operator Username Box
⑥ Operator Password Box
⑦ Confirm Operator Password Box
⑧ Admin Username Box
⑨ Admin Password Box
⑩ Confirm Admin Password Box
⑪ Password Minimum Length Box
⑫ Apply Button
⑬ Reload Button

Figure 6.1 Configure Passwords Form

Note

RUGGEDCOM ROS requires that all user passwords meet strict guidelines to prevent the use of weak passwords. When creating a new password, make sure it adheres to the following rules:

- Must not be less than 8 characters in length.
- Must not include the username or any 4 continuous characters found in the username. For example, if the username is *Subnet25*, the password may not

be *subnet25admin*, *subnetadmin* or *net25admin*. However, *net-25admin* or *Sub25admin* is permitted.

- Must have at least one alphabetic character and one number. Special characters are permitted.
- Must not have more than 3 continuously incrementing or decrementing numbers. For example, *Sub123* and *Sub19826* are permitted, but *Sub12345* is not.

An alarm will generate if a weak password is configured. The weak password alarm can be disabled by the user. For more information about disabling alarms, refer to "Managing Alarms (Page 102)".

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

Parameter	Description
`Auth Type`	**Synopsis:** [Local | RADIUS | TACACS+ | RADIUSorLocal | TACACS +orLocal] **Default:** Local Password can be authenticated using localy configured values, or remote RADIUS or TACACS+ server. Setting value to any of combinations that involve RADIUS or TACACS+ require Security Server Table to be configured. Settings: • Local – Authentication from the local Password Table. • RADIUS – Authentication using a RADIUS server. • TACACS+ – Authentication using a TACACS+ server. • RADIUSOrLocal – Authentication using RADIUS. If the server cannot be reached, authenticate from the local Password Table. • TACACS+OrLocal – Authentication using TACACS+. If the server cannot be reached, authenticate from the local Password Table **Note** For console access, only local credentials are checked when Local, RADIUS, or TACACS+ authentication is selected. When RADIUSOrLocal or TACACS+OrLocal authentication is selected, RADIUS or TACACS+ credentials are checked first, respectively. If authentication fails , local credentials will then be checked.
`Guest Username`	**Synopsis:** A string 15 characters long **Default:** guest Related password is in field Guest Password; view only, cannot change settings or run any commands.
`Guest Password`	**Synopsis:** A string 19 characters long Related username is in field Guest Username; view only, cannot change settings or run any commands.

Parameter	Description
`Confirm Guest Password`	**Synopsis:** A string 19 characters long Related username is in field Guest Username; view only, cannot change settings or run any commands.
`Operator Username`	**Synopsis:** A string 15 characters long **Default:** operator Related password is in field Oper Password; cannot change settings; can reset alarms, statistics, logs, etc.
`Operator Password`	**Synopsis:** A string 19 characters long Related username is in field Oper Username; cannot change settings; can reset alarms, statistics, logs, etc
`Confirm Operator Password`	**Synopsis:** A string 19 characters long Related username is in field Oper Username; cannot change settings; can reset alarms, statistics, logs, etc.
`Admin Username`	**Synopsis:** A string 15 characters long **Default:** admin Related password is in field Admin Password; full read/write access to all settings and commands.
`Admin Password`	**Synopsis:** A string 19 characters long Related username is in field Admin Username; full read/write access to all settings and commands.
`Confirm Admin Password`	**Synopsis:** A string 19 characters long Related username is in field Admin Username; full read/write access to all settings and commands.
`Password Minimum Length`	**Synopsis:** An integer between 1 and 17 **Default:** 1 Configure the password string minimum length. The new password shorter than the minimum length will be rejected.

3. Click **Apply**.

6.2 Clearing Private Data

When enabled, during system boot up, a user with serial console access can clear all configuration data and keys stored on the device, and restore all user names and passwords to factory default settings.

To clear private data, do the following:

Note
The commands used in the following procedure are time-sensitive. If the specified time limits are exceeded before providing the appropriate response, the device will continue normal boot up.

1. Connect to the device via the RS-232 serial console port. For more information, refer to "Connecting Directly (Page 33)".
2. Cycle power to the device. As the device is booting up, the following prompt will appear:

   ```
   Press any key to start
   ```
3. Within four seconds, press **CTRL** + **r**. The access banner will appear, followed by the command prompt:

   ```
   >
   ```
4. Type the following command, then press **Enter** within 30 seconds:

   ```
   clear private data
   ```
5. When prompted "Do you want to clear private data (Yes/No)?", answer *yes* and press **Enter** within five seconds. All configuration and keys in flash will be zeroized. An entry in the event log will be created. Crashlog.txt files (if existing) and syslog.txt files will be preserved. The device will reboot automatically.

6.3 Managing User Authentication

This section describes the various methods for authenticating users.

6.3.1 Configuring User Name Extensions

When configured to authenticate users using RADIUS or TACACS+, RUGGEDCOM ROS can be configured to add information to each user name important to the authentication server. This can include the NAS IP address, system name, system location, or any other user-defined text.

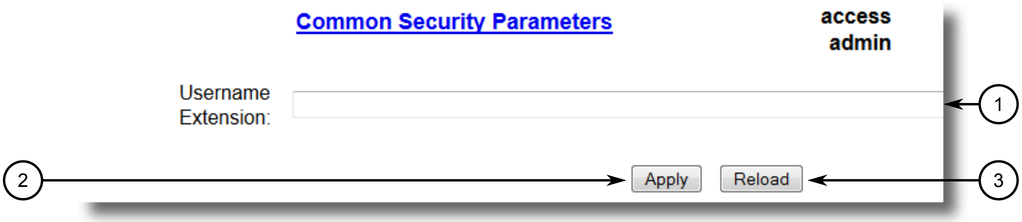
If the **Username Extension** parameter is left blank, only the user name will be sent to the authentication server.

Note

Extensions are ignored when IEEE 802.1x port-based authentication is enabled. RUGGEDCOM ROS will remain transparent and not make any changes to the username. For more information about IEEE 802.1x authentication, refer to "Port Security Concepts (Page 127)".

To configure a username extension, do the following:

1. Navigate to ***Administration » Configure Security Server » Configure Common Security Parameters***. The **Common Security Parameters** form appears.



① Username Extension Box
② Apply Button
③ Reload Button

Figure 6.2 Common Security Parameters Form

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

Parameter	Description
`Username Extension`	**Synopsis:** A string 127 characters long Defines the format of all user names sent to a RADIUS or TACACS+ server for authentication. A prefix or suffix can be added to the user name using predefined keywords (wrapped in % delimiters) or user-defined strings. Delimited values include: %Username%: The name associated with the user profile (e.g. admin, oper, etc.) %IPaddr%: The management IP address of the switch that acts as a Network Access Server (NAS). %SysName%: The system name given to the device. %SysLocation%: The system location given to the device. All pre-defined keywords are case-insensitive. Examples: %Username%@ABC.com %Username%_%SysLocation% If an extension is not defined, only the user name is sent to the authentication server.

3. Click **Apply**.

6.3.2 Managing RADIUS Authentication

RUGGEDCOM ROS can be configured to act as a RADIUS client and forward user credentials to a RADIUS (Remote Authentication Dial In User Service) server for remote authentication and authorization.

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).

⚠ **NOTICE**

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

⚠ **NOTICE**

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

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].

6.3.2.1 Configuring the RADIUS Server

Note

For information about configuring the RADIUS server, refer to the manufacturer's instructions of the server being configured.

The Vendor-Specific attribute (or VSA) sent to the RADIUS server as part of the RADIUS request is used to determine the access level from the RADIUS server. This attribute may be configured within the RADIUS server with the following information:

Attribute	Value
Vendor-Specific	Vendor-ID: 15004 Format: String Number: 2 Attribute: { Guest, Operator, Admin }

Note

If no access level is received in the response packet from the RADIUS server, access is denied.

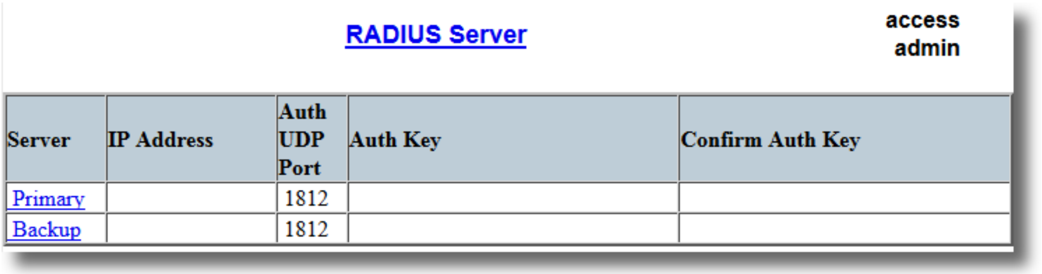
6.3.2.2 Configuring the RADIUS Client on the Device

The RADIUS client can be configured to use two RADIUS servers: a primary server and a backup server. If the primary server is unavailable, the device will automatically attempt to connect with the backup server.

Note
The RADIUS client uses the Password Authentication Protocol (PAP) to verify access.

To configure access to either the primary or backup RADIUS servers, do the following:

1. Navigate to ***Administration » Configure Security Server » Configure RADIUS Server***. The **RADIUS Server** table appears.



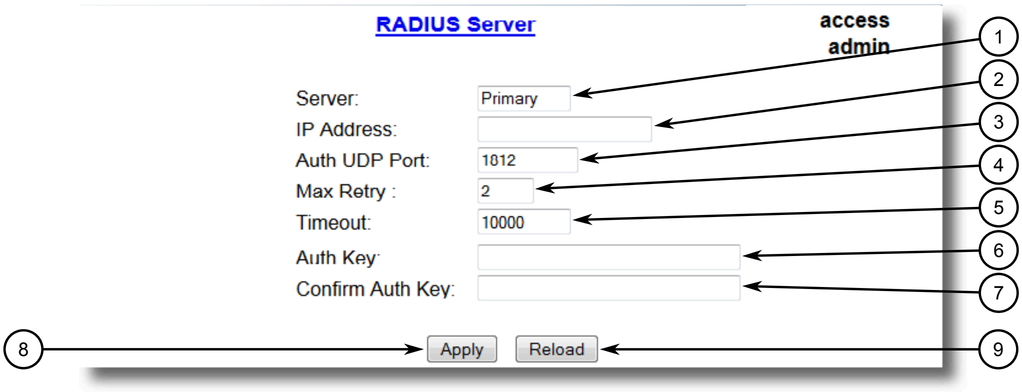
RADIUS Server

access
admin

Server	IP Address	Auth UDP Port	Auth Key	Confirm Auth Key
Primary		1812		
Backup		1812		

Figure 6.3 RADIUS Server Table

2. Select either **Primary** or **Backup** from the table. The **RADIUS Server** form appears.



RADIUS Server

access
admin

Server:	Primary
IP Address:	
Auth UDP Port:	1812
Max Retry :	2
Timeout:	10000
Auth Key:	
Confirm Auth Key:	

Apply Reload

① Server Box
② IP Address Box
③ Auth UDP Port Box
④ Max Retry Box
⑤ Timeout Box
⑥ Auth Key Box
⑦ Confirm Auth Key Box
⑧ Apply Button
⑨ Reload Button

Figure 6.4 RADIUS Server Form

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

Parameter	Description
`Server`	**Synopsis:** A string 8 characters long **Default:** Primary This field tells whether this configuration is for a Primary or a Backup Server.
`IP Address`	**Synopsis:** ###.###.###.### where ### ranges from 0 to 255 The Server IP Address.
`Auth UDP Port`	**Synopsis:** An integer between 1 and 65535 **Default:** 1812 The IP Port on server.
`Max Retry`	**Synopsis:** An integer between 1 and 10 **Default:** 2 The maximum number of times the Authenticator will attempt to contact the authentication server to authenticate the user in case of any failure.
`Timeout`	**Synopsis:** An integer between 1000 and 120000 **Default:** 10000 The amount of time in milliseconds the Authenticator will wait for a response from the authentication server.
`Auth Key`	**Synopsis:** A string 31 characters long The authentication key to be shared with server. Only available on Controlled versions.
`Confirm Auth Key`	**Synopsis:** A string 31 characters long The authentication key to be shared with server. Only available on Controlled versions.

4. Click **Apply**.

6.3.3 Managing TACACS+ Authentication

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

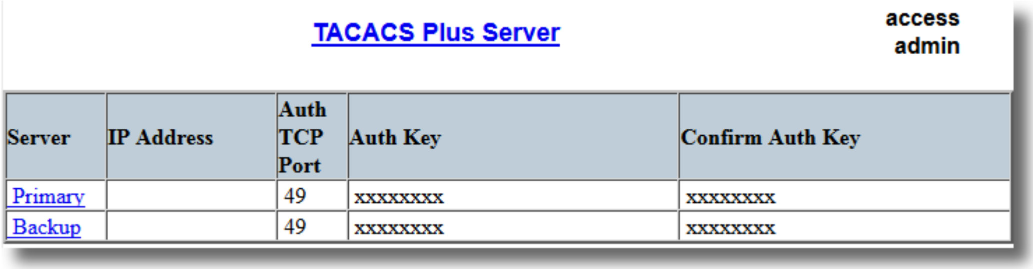
6.3.3.1 Configuring TACACS+

RUGGEDCOM ROS can be configured to use two TACACS+ servers: a primary server and a backup server. If the primary server is unavailable, the device will automatically attempt to connect with the backup server.

For CLI commands related to configuring TACACS+, refer to "Available CLI Commands (Page 17)".

To configure access to either the primary or backup TACACS+ servers, do the following:

1. Navigate to ***Administration » Configure Security Server » Configure TacPlus Server » Configure TACACS Plus Server***. The **TACACS Plus Server Table** appears.



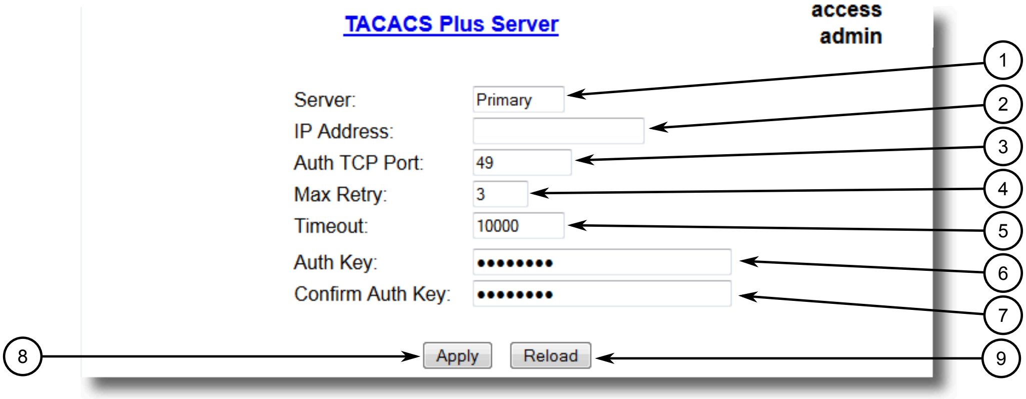
TACACS Plus Server

access
admin

Server	IP Address	Auth TCP Port	Auth Key	Confirm Auth Key
Primary		49	xxxxxxxx	xxxxxxxx
Backup		49	xxxxxxxx	xxxxxxxx

Figure 6.5 TACACS Plus Server Table

2. Select either **Primary** or **Backup** from the table. The **TACACS Plus Server** form appears.



TACACS Plus Server

access
admin

Server:	Primary
IP Address:	
Auth TCP Port:	49
Max Retry:	3
Timeout:	10000
Auth Key:	••••••••
Confirm Auth Key:	••••••••

① Server Box
② IP Address Box
③ Auth TCP Port Box
④ Max Retry Box
⑤ Timeout Port Box
⑥ Reachable Box
⑦ Auth Key Box
⑧ Confirm Key Box
⑨ Apply Button
⑩ Reload Button

Figure 6.6 TACACS Plus Server Form

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

Parameter	Description
`Server`	**Synopsis:** A string 8 characters long **Default:** Primary This field tells whether this configuration is for a Primary or a Backup Server.
`IP Address`	**Synopsis:** ###.###.###.### where ### ranges from 0 to 255 The Server IP Address.
`Auth TCP Port`	**Synopsis:** An integer between 1 and 65535 **Default:** 49 The IP Port on server.
`Max Retry`	**Synopsis:** An integer between 1 and 10 **Default:** 3 The maximum number of times the Authenticator will attempt to contact the authentication server to authenticate the user in case of any failure.
`Timeout`	**Synopsis:** An integer between 1000 and 120000 **Default:** 10000 The amount of time in milliseconds the Authenticator will wait for a response from the authentication server.
`Auth Key`	**Synopsis:** A string 31 characters long **Default:** mySecret The authentication key to be shared with server.
`Confirm Auth Key`	**Synopsis:** A string 31 characters long The authentication key to be shared with server.

4. Set the privilege levels for each user type (i.e. admin, operator and guest). For more information, refer to "Configuring User Privileges (Page 125)".

5. Click **Apply**.

6.3.3.2 Configuring User Privileges

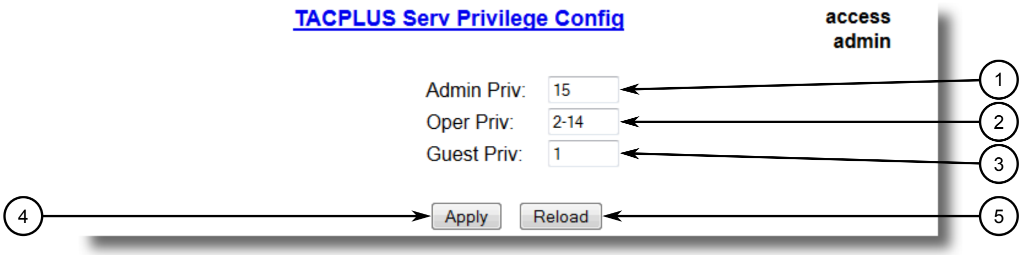
Each TACACS+ authentication request includes a *priv_lvl* attribute that is used to grant access to the device. By default, the attribute uses the following ranges:

- `15` represents the *admin* access level
- `2-14` represents the *operator* access level
- `1` represents the *guest* access level

For CLI commands related to configuring user privileges, refer to "Available CLI Commands (Page 17)".

To configure the privilege levels for each user type, do the following:

1. Navigate to ***Administration » Configure Security Server » Configure TacPlus Server » Configure TACPLUS Serv Privilege Config***. The **TACPLUS Serv Privilege Config** form appears.



Admin Priv: 15
Oper Priv: 2-14
Guest Priv: 1

① Admin Priv Box
② Oper Priv Box
③ Guest Priv Box
④ Apply Button
⑤ Reload Button

Figure 6.7 TACPLUS Serv Privilege Config Form

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

Parameter	Description
`Admin Priv`	**Synopsis:** (0 to 15)-(0 to 15) **Default:** 15 Privilege level to be assigned to the user.
`Oper Priv`	**Synopsis:** (0 to 15)-(0 to 15) **Default:** 2-14 Privilege level to be assigned to the user.
`Guest Priv`	**Synopsis:** (0 to 15)-(0 to 15) **Default:** 1 Privilege level to be assigned to the user.

3. Click **Apply**.

6.4 Managing Port Security

Port security, or port access control, provides the ability to filter or accept traffic from specific MAC addresses.

Port security works by inspecting the source MAC addresses of received frames and validating them against the list of MAC addresses authorized by the port. Unauthorized frames are filtered and, optionally, the part that received the frame can be shut down permanently or for a specified period of time. An alarm will be raised indicating the detected unauthorized MAC address.

Frames to unknown destination addresses are flooded through secure ports.

6.4.1 Port Security Concepts

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

6.4.1.1 Static MAC Address-Based Authentication

With this method, the switch validates the source MAC addresses of received frames against the contents in the Static MAC Address Table.

RUGGEDCOM ROS also supports a highly flexible Port Security configuration which provides a convenient means for network administrators to use the feature in various network scenarios.

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

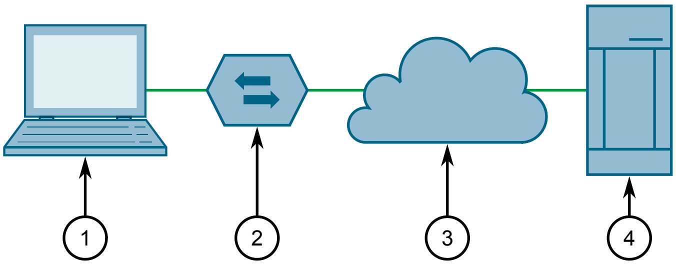
The switch can also be programmed to learn (and, thus, authorize) a pre-configured number of the first source MAC addresses encountered on a secure port. This enables the capture of the appropriate secure addresses when first configuring MAC address-based authorization on a port. Those MAC addresses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

6.4.1.2 IEEE 802.1x Authentication

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

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

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



① Supplicant
② Authenticator Switch
③ LAN
④ Authentication Server

Figure 6.8 IEEE 802.1x General Topology

⚠ NOTICE

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

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

RUGGEDCOM ROS communicates with the Authentication Server using EAP over RADIUS.

Note
The switch supports authentication of one host per port.

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

6.4.1.3 IEEE 802.1X Authentication with MAC Address-Based Authentication

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

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

1. The device connects to a switch port.
2. The switch learns the device MAC address upon receiving the first frame from the device (the device usually sends out a DHCP request message when first connected).

3. The switch sends an EAP Request message to the device, attempting to start 802.1X authentication.
4. The switch times out while waiting for the EAP reply, because the device does not support 802.1x.
5. The switch sends an authentication message to the authentication server, using the device MAC address as the username and password.
6. The switch authenticates or rejects the device according to the reply from the authentication server.

6.4.1.4 Assigning VLANS with Tunnel Attributes

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

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

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

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

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

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

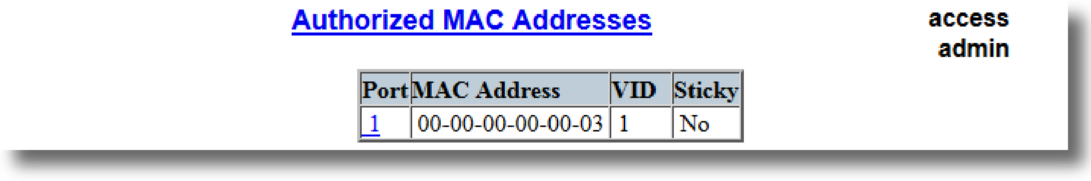
If the tunnel attributes are not returned by the authentication server, the VLAN assigned to the switch port remains unchanged.

6.4.2 Viewing a List of Authorized MAC Addresses

To view a list of static MAC addresses learned from secure ports, navigate to ***Network Access Control » Port Security » View Authorized MAC Addresses***. The **Authorized MAC Addresses** table appears.

Note

Only MAC addresses authorized on a static MAC port(s) are shown. MAC addresses authorized with IEEE 802.1X are not shown.



Authorized MAC Addresses

access admin

Port	MAC Address	VID	Sticky
1	00-00-00-00-00-03	1	No

Figure 6.9 Authorized MAC Addresses Table

This table displays the following information:

Parameter	Description
`Port`	**Synopsis:** 1 to maximum port number Port on which MAC address has been learned.
`MAC Address`	**Synopsis:** ##-##-##-##-##-## where ## ranges 0 to FF Authorized MAC address learned by the switch.
`VID`	**Synopsis:** An integer between 0 and 65535 VLAN Identifier of the VLAN upon which the MAC address operates.
`Sticky`	**Synopsis:** [No | Yes] This describes whether the authorized MAC address/Device can move to another port or not: • Yes – authorized MAC address/Device cannot move to a different switch port • No – authorized MAC address/Device may move to another switch port

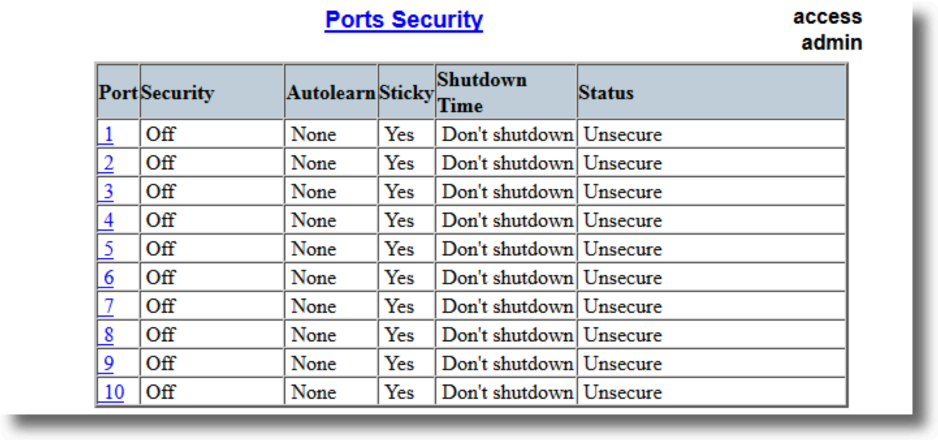
If a MAC address is not listed, do the following:

- Configure port security. For more information, refer to "Configuring Port Security (Page 131)".
- Configure IEEE 802.1X. For more information, refer to "Configuring IEEE 802.1X (Page 133)".

6.4.3 Configuring Port Security

To configure port security, do the following:

1. Navigate to ***Network Access Control » Port Security » Configure Ports Security***. The **Ports Security** table appears.



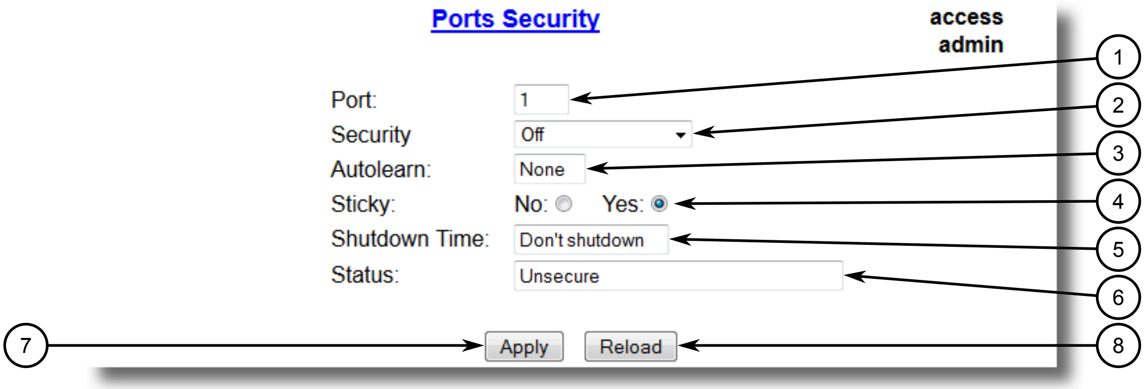
Ports Security

access
admin

Port	Security	Autolearn	Sticky	Shutdown Time	Status
1	Off	None	Yes	Don't shutdown	Unsecure
2	Off	None	Yes	Don't shutdown	Unsecure
3	Off	None	Yes	Don't shutdown	Unsecure
4	Off	None	Yes	Don't shutdown	Unsecure
5	Off	None	Yes	Don't shutdown	Unsecure
6	Off	None	Yes	Don't shutdown	Unsecure
7	Off	None	Yes	Don't shutdown	Unsecure
8	Off	None	Yes	Don't shutdown	Unsecure
9	Off	None	Yes	Don't shutdown	Unsecure
10	Off	None	Yes	Don't shutdown	Unsecure

Figure 6.10 Ports Security Table

2. Select an Ethernet port. The **Ports Security** form appears.



Ports Security

access
admin

Port:	1
Security	Off
Autolearn:	None
Sticky:	No: ○ Yes: ●
Shutdown Time:	Don't shutdown
Status:	Unsecure

① Port Box
② Security List
③ Autolearn Box
④ Sticky Options
⑤ Shutdown Time Box
⑥ Status Box
⑦ Apply Button
⑧ Reload Button

Figure 6.11 Ports Security Form

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

Parameter	Description
`Port`	**Synopsis:** 1 to maximum port number **Default:** 1 The port number as seen on the front plate silkscreen of the switch.
`Security`	**Synopsis:** [Off | Static MAC | 802.1X | 802.1x/MAC-Auth] **Default:** Off Enables or disables the port's security feature. Two types of port access control 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 it is not known to which port they will be connected), there is still an option to configure the switch to auto-learn certain number of MAC addresses. Once learned, they do not age out until the unit is reset or the link goes down. • IEEE 802.1X standard authentication. • IEEE 802.1X with MAC-Authentication, also known as MAC-Authentication Bypass. With this option, the device can authenticate clients based on the client’s MAC address if IEEE 802.1X authentication times out.
`Autolearn`	**Synopsis:** An integer between 1 and 16 or [None] **Default:** None Only applicable when the 'Security' field has been set to 'Static MAC'. It specifies 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.
`Sticky`	**Synopsis:** [No | Yes] **Default:** Yes Only applicable when the 'Security' field has been set to 'Static MAC'. Change the behaviour of the port to either sticky or non-sticky. If Sticky is 'Yes', MACs/Devices authorized on the port 'stick' to the port and the switch will not allow them to move to a different port. If Sticky is 'No', MACs/Devices authorized on the port may move to another port.
`Shutdown Time`	**Synopsis:** An integer between 1 and 86400 or [Until reset | Don't shutdown] **Default:** Don't shutdown Specifies for how long to shut down the port, if a security violation occurs.

Parameter	Description
`Status`	**Synopsis:** A string 31 characters long Describes the security status of the port.

Note

There are a few scenarios in which static MAC addresses can move:

- When the link is up/down on a *non-sticky* secured port
- When traffic switches from or to a *non-sticky* secured port

Note

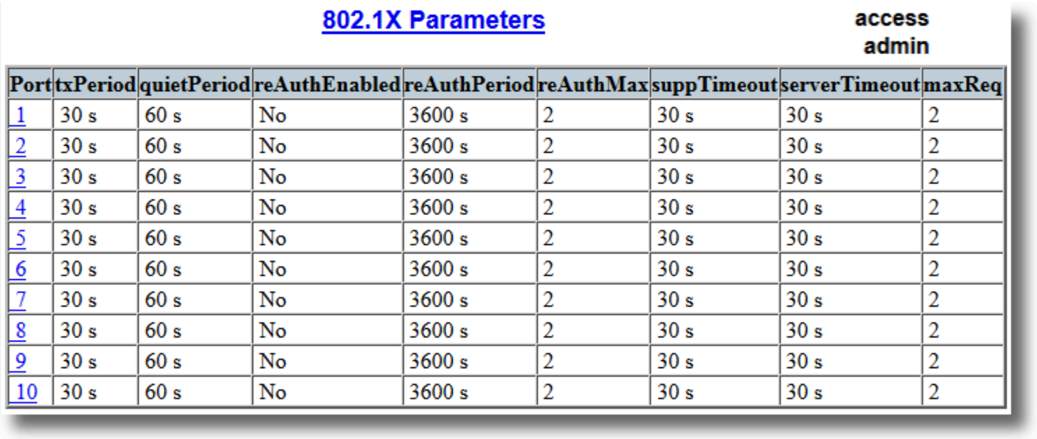
Traffic is lost until the source MAC Address of the incoming traffic is authorized against the static MAC address table.

4. Click **Apply**.

6.4.4 Configuring IEEE 802.1X

To configure IEEE 802.1X port-based authentication, do the following:

1. Navigate to ***Network Access Control » Port Security » Configure 802.1X***. The **802.1X Parameters** table appears.



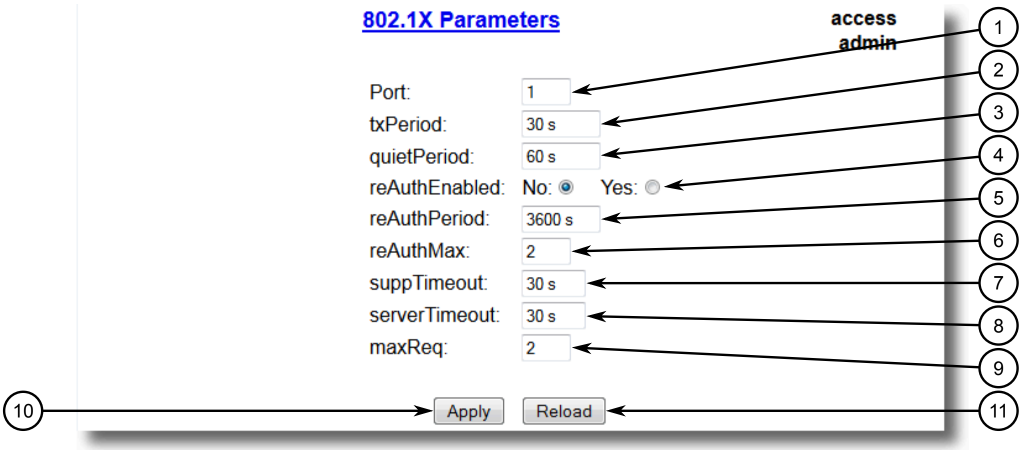
802.1X Parameters

access
admin

Port	txPeriod	quietPeriod	reAuthEnabled	reAuthPeriod	reAuthMax	suppTimeout	serverTimeout	maxReq
1	30 s	60 s	No	3600 s	2	30 s	30 s	2
2	30 s	60 s	No	3600 s	2	30 s	30 s	2
3	30 s	60 s	No	3600 s	2	30 s	30 s	2
4	30 s	60 s	No	3600 s	2	30 s	30 s	2
5	30 s	60 s	No	3600 s	2	30 s	30 s	2
6	30 s	60 s	No	3600 s	2	30 s	30 s	2
7	30 s	60 s	No	3600 s	2	30 s	30 s	2
8	30 s	60 s	No	3600 s	2	30 s	30 s	2
9	30 s	60 s	No	3600 s	2	30 s	30 s	2
10	30 s	60 s	No	3600 s	2	30 s	30 s	2

Figure 6.12 802.1X Parameters Table

2. Select an Ethernet port. The **802.1X Parameters** form appears.



802.1X Parameters

access
admin

Port:	1
txPeriod:	30 s
quietPeriod:	60 s
reAuthEnabled:	No: ● Yes: ○
reAuthPeriod:	3600 s
reAuthMax:	2
suppTimeout:	30 s
serverTimeout:	30 s
maxReq:	2

①	Port Box
②	tX Period Box
③	quietPeriod Box
④	reAuthEnabled Options
⑤	reAuthPeriod Box
⑥	reAuthMax Box
⑦	suppTimeout Box
⑧	serverTimeout Box
⑨	maxReq Box
⑩	Apply Button
⑪	Reload Button

Figure 6.13 802.1X Parameters Form

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

Parameter	Description
`Port`	**Synopsis:** 1 to maximum port number **Default:** 1 The port number as seen on the front plate silkscreen of the switch.
`txPeriod`	**Synopsis:** An integer between 1 and 65535 **Default:** 30 The time to wait for the Supplicant's EAP Response/Identity packet before retransmitting an EAP Request/Identity packet.
`quietPeriod`	**Synopsis:** An integer between 0 and 65535 **Default:** 60 The period of time not to attempt to acquire a Supplicant after the authorization session failed.
`reAuthEnabled`	**Synopsis:** [No | Yes] **Default:** No Enables or disables periodic re-authentication.

Parameter	Description
`reAuthPeriod`	**Synopsis:** An integer between 60 and 86400 **Default:** 3600 The time between periodic re-authentication of the Supplicant.
`reAuthMax`	**Synopsis:** An integer between 1 and 10 **Default:** 2 The number of re-authentication attempts that are permitted before the port becomes unauthorized.
`suppTimeout`	**Synopsis:** An integer between 1 and 300 **Default:** 30 The time to wait for the Supplicant's response to the authentication server's EAP packet.
`serverTimeout`	**Synopsis:** An integer between 1 and 300 **Default:** 30 The time to wait for the authentication server's response to the Supplicant's EAP packet.
`maxReq`	**Synopsis:** An integer between 1 and 10 **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.

4. Click **Apply**.

6.5 Managing SSH/SSL Keys and Certificates

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

⚠ NOTICE

Siemens recommends the following actions before commissioning the device:

- Replace the factory-provisioned, self-signed SSL certificate with one signed by a trusted Certificate Authority (CA)
- Configure the SSH client to use *diffie-hellman-group14-sha1* or better

Note

Only admin users can write certificates and keys to the device.

Each RUGGEDCOM ROS device is shipped with a unique RSA 1024 self-signed SSL certificate and a DSA 1024 SSH host key pair that are generated at and provisioned by the factory. The administrator may upload a new certificate and keys to the system at any time, which will overwrite the existing ones. In addition, CLI commands are available to regenerate SSL certificate and key pair as well as the SSH host key pair.

There are three types of certificates and keys used in RUGGEDCOM ROS:

Note
Network exposure to a ROS unit operating with the default keys, although always only temporary by design, should be avoided. The best way to reduce or eliminate this exposure is to provision user-created certificate and keys as quickly as possible, and preferably before the unit is placed in network service.

Note
The default certificate and keys are common to all RUGGEDCOM ROS versions without a certificate or key files. That is why it is important to either allow the key auto-generation to complete or to provision custom keys. In this way, one has at least unique, and at best, traceable and verifiable keys installed when establishing secure communication with the unit.

- **Default**

  A default certificate and SSL/SSH keys are built in to RUGGEDCOM ROS and are common across all RUGGEDCOM ROS units sharing the same firmware image. In the event that valid SSL certificate or SSL/SSH key files are not available on the device (as is usually only the case when upgrading from an old ROS version that does not support user-configurable keys and therefore does was not shipped with unique, factory-generated keys), the default certificate and keys are put into service *temporarily* so that SSH and SSL (HTTPS) sessions can be served until generated or provisioned keys are available.

- **Auto-Generated**

  If a default SSL certificate and SSL/SSH keys are in use, RUGGEDCOM ROS immediately begins to generate a unique certificate and SSL/SSH keys for the device in the background. This process may take several minutes to complete depending on the requested key length and how busy the device is at the time. If a custom certificate and keys are loaded while auto-generated certificates and keys are being generated, the generator will abort and the custom certificate and keys and will be used.

- **Custom (Recommended)**

  Custom certificates and keys are the most secure option. They give the user complete control over certificate and key management, allow for the provision of certificates signed by a public or local certificate authority, enable strictly controlled access to private keys, and allow authoritative distribution of SSL certificates, any CA certificates, and public SSH keys.

Note
The RSA or EC private key corresponding to the SSL certificate must be appended to the certificate in the `ssl.crt` file.

6.5.1 SSL Certificates

RUGGEDCOM ROS supports SSL certificates that conform to the following specifications:

- X.509 v3 digital certificate format
- PEM format
- For RUGGEDCOM ROS Controlled verions: RSA key pair, 1024, 2048 or 3072 bits; or NIST P-192, P-224, P-256, P-384 or P-521
- For RUGGEDCOM ROS Non-Controlled (NC) verions: RSA key pair, 512 to 2048 bits

Note
RSA keys smaller than 2048 bits in length are not recommended. Support is only included here for compatibility with legacy equipment.

Two standard PEM files are required: the SSL certificate and the corresponding RSA private key file. These are concatenated into the resulting `ssl.crt` file, which may then be uploaded to RUGGEDCOM ROS. For more information about transferring files between the device and a host computer, refer to "Uploading/Downloading Files (Page 41)".

While RUGGEDCOM ROS is capable of using self-signed certificates created using the **`sslkeygen`** command, Siemens recommends using an X.509 certificate issued by an organization's own Certificate Authority (CA).

6.5.2 SSH Host Key

Note
SSH is not supported in Non-Controlled (NC) versions of RUGGEDCOM ROS.

Controlled versions of RUGGEDCOM ROS support SSH public/private key pairs that conform to the following specifications:

- PEM format
- DSA key pair, 1024, 2048 or 3072 bits in length
- RSA key pair, 1024, 2048 or 3072 bits in length

Note
DSA or RSA key generation times increase depending on the key length. 1024 bit RSA keys take less than 5 minutes to generate on a lightly loaded unit, whereas 2048 bit keys may take significantly longer. A typical modern PC system, however, can generate these keys in seconds.

The following (bash) shell script fragment uses the `ssh-keygen` command line utility to generate a 2048 bit RSA key suitable for use in RUGGEDCOM ROS . The resulting `ssh.keys` file may then be uploaded to RUGGEDCOM ROS:

```
# RSA key size:
```

```
BITS=2048

# Make an SSH key pair:
ssh-keygen -t RSA -b $BITS -N '' -f ssh.keys
```

For an example of an SSH key generated by RUGGEDCOM ROS, refer to "Certificate and Key Examples (Page 141)".

6.5.3 Managing SSH Public Keys

RUGGEDCOM ROS allows admin users to list, add and delete SSH public keys. Public keys are added as non-volatile storage (i.e. flash) files on RUGGEDCOM ROS devices, and are retrieved at the time of SSH client authentication.

6.5.3.1 Public Key Requirements

Public keys are stored in a flash file, called *sshpub.keys*. The *sshpub.keys* file consists of ssh user public key entries. Similar to the config.csv file, each entry must be separated by an empty line. An entry has two components. They are, in sequence:

- Header
- Key

The header contains the parameters of the entry, separated by comma. The parameters are, in sequence:

- ID: A number between 0 and 9999
- Entry type: UserKey
- Access Level: (Admin, Operator or Guest)
- Revocation Status: active/inactive (always active for keys)
- User Name: This is the client's user name (not the RUGGEDCOM ROS user name). This will be used by clients to later SSH into the RUGGEDCOM ROS device.

The key must be in RFC4716 format, or in PEM format with any of the following header and footer lines:

```
-----BEGIN PUBLIC KEY-----
-----END PUBLIC KEY-----

-----BEGIN SSH2 PUBLIC KEY-----
-----END SSH2 PUBLIC KEY-----

-----BEGIN RSA PUBLIC KEY-----
-----END RSA PUBLIC KEY-----
```

The following is an example of a valid entry in the *sshpub.keys* file in PEM format:

```
1,userkey,admin,active,alice
---- BEGIN SSH2 PUBLIC KEY ----
AAAAB3NzaC1yc2EAAAABIwAAAQEA4mRrqfk+RKXnmGRvzMyWVDsbq5VwpGGrlLQYCrjVEa
NdbXsphqYKop8V5VUeXFRAUFzOy82yk8TF/5JxGPWq6wRNjhnYR7IY2AiMBq0+K8XeURl/
z5K2XNRjnqTZSFwkhaUVJeduvjGgOlNN4yvgUwF3n0idU9k3E1q/na+LmYIeGhOwzCqoAc
ipHAdR4fhD5u0jbmvjv+gDikTSZIbj9eFJfP09ekImMLHwbBry0SSBpqAKbwVdWEXIKQ47
zz7ao2/rs3rSV16IXSq3Qe8VZh2irah0Md6JFMOX2qm9fo1I62q1DDgheCOsOiGPf4xerH
```

```
rI2cs6FT31rAdx2JOjvw==
---- END SSH2 PUBLIC KEY ----
```

The following is an example of a valid entry in the *sshpub.keys* file in in RFC4716 format:

```
2,userkey,admin,active,bob
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDH0NivR8zzbTxlecvFPzR/GR24N
rRJa0Lc7scNsWRgi0XulHuGrRLRB5RoQ39+spdig88Y8CqhRI49XJx7uL
Je0Su3RvyNYz1jkdSwHq2hSZCpukJxJ6CK95Po/sVa5Gq2gMaHowiYDSkcx+AJywzK/eM6i/jc125l
RxFPdfkj74u+ob3PCvmIWz5z3WAJBrQU1IDPHDets511WMu8O9/mAPZRwjqrWhRsqmcXZuv5oo54wIop
CAZSo20SPzM2VmXFuUsEwDkvYMXLJK1koJPbDjH7yFFC7mwK2eMU/oMFFn934cbO5N6etsJSvplYQ4pM
Cw6Ok8Q/bB5cPSOa/rAt bob@work
```

RUGGEDCOM ROS allows only 16 user key entries to be stored. Each key entry must meet the following limits:

- Key type must be either RSA 2048 bits or RSA 3072 bits
- Key size must not exceed 4000 base64 encoded characters
- Entry Type in the header must not exceed 8 ASCII characters
- Access Level in the header must not exceed 8 ASCII characters (*operator* is maximum)
- Revocation status in the header must not exceed 8 ASCII characters (*inactive* is maximum)
- User Name must not exceed 12 ASCII characters

6.5.3.2 Adding a Public Key

Administrators can add one or more public keys to RUGGEDCOM ROS.

There are two ways to update *sshpub.keys*:

- Upload a locally-created file directly to the *sshpub.keys* file. The content of the file replace the content currently stored in flash memory.
- Upload a locally-created file to the *sshaddpub.keys* file. The content of the file is appended to the existing entries in the *sshpub.keys* file.

> ⚠ **NOTICE**
>
> The content of the *sshaddpub.keys* file must follow the same syntax as the *sshpub.keys* file.

To add keys, do the following:

1. Create a public key file via a host computer.
2. Transfer the public key file to the device using SFTP or Xmodem. For more information about transferring files, refer to "Uploading/Downloading Files (Page 41)".
3. Log in to the device as an admin user and access the CLI shell. For more information about accessing the CLI shell, refer to "Using the Command Line Interface (Page 17)".

4. Check the system log to make sure the files were properly transferred. For more information about viewing the system log, refer to "Viewing Local and System Logs (Page 46)".

6.5.3.3 Viewing a List of Public Keys

Admin users can view a list of existing public keys on the device.

To view public keys, do the following:

1. Log in to the device as an admin user and access the CLI shell. For more information about accessing the CLI shell, refer to "Using the Command Line Interface (Page 17)".
2. At the CLI prompt, type:

   ```
   sshpubkey list
   ```

   A list of public keys will appear, including their key ID, access level, revocation status, user name and key fingerprint.

6.5.3.4 Updating a Public Key

Admin users can update public keys.

To update public keys, do the following:

1. Log in to the device as an admin user and access the CLI shell. For more information about accessing the CLI shell, refer to "Using the Command Line Interface (Page 17)".
2. At the CLI prompt, type:

   ```
   sshpubkey list
   ```

   A list of public keys will appear, including their key ID, access level, revocation status, user name and key fingerprint.
3. Type the following commands to update the public keys:

Command	Description
sshpubkey update_id { *current_ID* } { *new_ID* }	Updates the ID of user public key. **Note** The user public key ID must be a number between 0 and 9999. • { *current_ID* } is the ID currently assigned to the public key • { *new_ID* } is the ID that will be used to identify the public key going forward
sshpubkey update_al { *AL* }	Updates the access level of a user public key. • { *AL* } is the access level (admin, operator or guest) of the public key to be updated

Command	Description
sshpubkey update_rs { *RS* }	Updates the revocation status (active, inactive) of a user public key. • { *RS* } is the revocation status of the public key to be updated
sshpubkey update_un { *UN* }	Updates the user name of a user public key. • { *UN* } is the user name of the public key to be updated

6.5.3.5 Deleting a Public Key

Admin users can delete one or more public keys.

To delete a public key, do the following:

1. Log in to the device as an admin user and access the CLI shell. For more information about accessing the CLI shell, refer to "Using the Command Line Interface (Page 17)".
2. At the CLI prompt, type:

   ```
   sshpubkey list
   ```

   A list of public keys will appear, including access level, revocation status, user name and key fingerprint.
3. Type the following commands to delete the public key(s):

Command	Description
sshpubkey remove { *ID* }	Removes a key from the non-volatile storage. • { *ID* } is the ID of the public key to be removed

6.5.4 Certificate and Key Examples

For SSL, certificates must meet the requirements outlined in "SSL Certificates (Page 137)".

The certificate and keys must be combined in a single `ssl.crt` file and uploaded to the device.

The following is an example of a combined SSL certificate and key:

```
-----BEGIN CERTIFICATE-----
MIIC9jCCAl+gAwIBAgIJAJh6rrehMt3iMA0GCSqGSIb3DQEBBQUAMIGuMQswCQYD
VQQGEwJDQTEQMA4GA1UECBMHT250YXJpbzEQMA4GA1UEBxMHQ29uY29yZDESMBAG
A1UEChMJUnVnZ2VkY29tMRkwFwYDVQQLExBDdXN0b21lciBTdXBwb3J0MSYwJAYD
VQQDEx1XUy1NSUxBTkdPVkFOLlJVR0dFRENPTS5MT0NBTDEkMCIGCSqGSIb3DQEJ
ARYVc3VwcG9ydEBydWdnZWRjb20uY29tMB4XDTEyMTAyMzIxMTA1M1oXDTE3MTAy
MjIxMTA1M1owgZwxCzAJBgNVBAYTAlVTMRAwDgYDVQQIEwdPbnRhcmlvMRAwDgYD
VQQHEwdDb25jb3JkMRIwEAYDVQQKEwlSdWdnZWRDb20xGTAXBgNVBAsTEEN1c3Rv
bWVyIFN1cHBvcnQxFDASBgNVBAMTCzE5Mi4xNjguMS4yMSQwIgYJKoZIhvcNAQkB
FhVTdXBwb3J0QHJ1Z2dlZGNvbS5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJ
AoGBALfE4eh2aY+CE3W5a4Wz1Z1RGRP02COHt153wFFrU8/fFQXNhKlQirlAHbNT
RSwcTR8ZFapivwYDivn0ogOGFXknYP90gv2oIaSVY08FqZkJW77g3kzkv/8Zrw3m
W/cBsZJ8SyKLIDfy401HkHpDOle5NsQFSrziGUPjAOIvvx4rAgMBAAGjLDAqMAkG
A1UdEwQCMAAwHQYDVR0OBBYEFER0utgQOifnrflnDtsqNcnvRB0XMA0GCSqGSIb3
```

```
DQEBBQUAA4GBAHtBsNZuh8tB3kdqR7Pn+XidCsD70YnI7w0tiy9yiRRhARmVXH8h
5Q1rOeHceri3JFFIOxIxQt4KgCUYJLu+c9Esk/nXQQar3zR7IQCt0qOABPkviiY8
c3ibVbhJjLpR2vNW4xRAJ+HkNNtBOg1xUlp4vOmJ2syYZR+7XAy/OP/S
-----END CERTIFICATE-----
-----BEGIN RSA PRIVATE KEY-----
MIIEpQIBAAKCAQEAn3UT94ZjlmBjygLXaA21ULum7EDmgsvFvg2tKYyaMj1en5UW
x172GvlDLUm5EwGmcG9u6DyuO3wOyv/taD1OUFkZA1W7cPu9NjeTtZjIQCx33xSU
1d6INMi2oOzwJmWzqwqIkIgy0uMdw78be4n7359U0UOOEtCStOmUfdw34jv6c38J
8sb+lC/FktX8Eilka4mDr07tf/ivC2kdwpPlGZIKt/xjcwjOsNHIBSfqbEbg5mO3
9OAPqsPRWKhBQZ6rM8aqEQjGPlrSTTNHrxO/CYVxAh0gtz+6qUytL3zi7Z9P7EzD
H8V8qNdXRNN0w5hsh2A5ZJj6+cbQJm0JHQeOowIDAQABAoIBAH2zXqUfBLyTibbC
3KoDPG7DLwhI9S4gkuaKg3ogg6GdLU2hys4p9to2qxU1a7cm8tzpi0V6KGNuHX87
lxw4T9cZFZXCbLvZR0RJNaDPKvUj2O87m0SpYzgxDX74qSuruqHX8OX26BHExj78
FR8jHDIhuUwp9AKy9yO0isFY65jkLov6tdRpNy5A+QrGyRVBilCIT6YFYKSzEEI8
6+29FkLtX+ERjqxJs+aGHyEPDWE4Zy7dBsuTk1Fwz8F6/rOz4PS2pNQXc2sWmomn
muQXv0hwKY5gMcovCkC3y/op3kNuc/3qeBHjeCBYEMLR0o25hZHGrKOrQahFsy+R
V48sgIECgYEA0H66Ijfcc7NpgKOQwyvCt9/uhRZ3RkeABoSBLb/wYfQjw4pMadqr
RMMzVPzOLC459Giv4m8GeikNPl53rYdTCRmd/t1nZClU/UQKhgj+RRt4xY2cJNsg
j2CTZDr5SJO8H957K1IbvN5mxdsWZuDc5dtf0wBMIaCJoXR/iDMcf2MCgYEAw8oK
Dkpz9PdhGkbTE0ARLeUv7okelBkfDIGgucXBFHUElHAGe+XLF5dMppmzRDHXi2NG
gSNPJsDOlgSyLJjKX7HapYeAJWm91w5kJEX+oERr1EnEPWPvOHI+OW5DjM6eR1s9
xRJ87e3ymgLIF7G5rmf0p3OlnVvCaQvIVYTB98ECgYEAl+sPI2nCp0eeY05LZ/rV
6fcwLCdfh4UHwzf/jF9j/2vON2fpH+RmkTcOiymd7NFOB0nUhtBRTufkr4JT/8wv
89yHpDKdaH05YUWXyWx6Ic7PpFr34F8OjYpYO1tBUuHa3PnWk41Dis4e4qIt446L
Rq0fWHbKAmKghlWFq69aX3MCgYEArKU2JM/mXHbfe0pEyk7OV0gn8hGbk0Brrp2H
2wjUb3OYbEQ0k4BYjB7wimAyQcoppVIPU8SNAUE3afYOH2FD4wp0IU7Q4yzRKBga
mhnWpABxjSrXDsNWqNGkqQPgMQPpcka0u1jILQ6LxN77Dlm7wF0O0bIash292t92
8mI0oIECgYEAql8/uRHGtwSk64rXWXI+uq+x4ewwZkVc+mMmJ0yCMuQsOzbQTxhx
v9GEi3xsFbNazGCx4b56+/6Bi6gf7aH+NeK2+7C4ddlpHGEawoEcW1CW8hRQ2brp
vWgC+m5nmQ2SaYGzlilzZVK3JE6qOZ/AG8k+ZEG9tsvakMliG1SoJXk=
-----END RSA PRIVATE KEY-----
```

For SSH, DSA or RSA host key pairs must meet the requirements outlined in "SSH Host Key (Page 137)".

The following is an example of a PEM formatted SSH key:

```
-----BEGIN DSA PRIVATE KEY-----
MIIBuwIBAAKBgQD0gcGbXx/rrEMu2913UW4cYo1OlcbnuUz7OZyd2mBLDx/GYbD8
X5TnRcMraJ0RuuGK+chqQJW5k3zQmZa/BS6q9U7wYwIAx8JSxxpwfPfl/t09VwKG
rtSJIMpLRoDq3qEwEVyR4kDUo4LFQDsljtiyhcz1n6kd6gqsd5Xu1vdh4wIVANXb
SBi97GmZ6/9f4UCvIIBtXLEjAoGAAfmhkcCCEnRJitUTiCE+MurxdFUr3mFs/d31
4cUDaLStQEhYYmx5dbFdQuapl4Y32B7lZQkohi5q1T1iUAa40/nUnJx1hFvblkYT
8DLwxcuDAaiu0VqsaPtJ+baL2dYNp96tFisj/475PEEWBGbP6GSe5kKa1Zdgwuie
9LyPb+ACgYBv856v5tb9UVG5+tX5Crfv/Nd8FFlSSFKmVWW3yzguhHajg2LQg8UU
sm1/zPSwYQ0SbQ9aOAJnpLc2HUkK0lji/0oKVI7y9MMc4B+bGu4W4OnryP7oFpnp
YYHt5PJY+zvLw/Wa+u3NOVFHkF1tGyfVBMXeV36nowPo+wrVMolAEgIVALLTnfpW
maV6uh6RxeE1d4XoxSg2
-----END DSA PRIVATE KEY-----
```

Layer 2

7

This chapter describes the Layer 2, or Data Link Layer (DLL), features of RUGGEDCOM ROS.

7.1 Managing Virtual LANs

A Virtual Local Area Network (VLAN) is a group of devices on one or more LAN segments that communicate as if they were attached to the same physical LAN segment. VLANs are extremely flexible because they are based on logical connections, rather than physical connections.

When VLANs are introduced, all traffic in the network must belong to one VLAN or another. Traffic on one VLAN cannot pass to another, except through an inter-network router or Layer 3 switch.

VLANs are created in three ways:

- **Explicitly**

  Static VLANs can be created in the switch. For more information about static VLANs, refer to "Managing Static VLANs (Page 156)".

- **Implicitly**

  When a VLAN ID (VID) is set for a port-based VLAN, static MAC address or IP interface, an appropriate VLAN is automatically created if it does not yet exist.

- **Dynamically**

  VLANs can be learned through GVRP. For more information about GVRP, refer to "GARP VLAN Registration Protocol (GVRP) (Page 146)"

For more information about VLANs, refer to "VLAN Concepts (Page 143)".

7.1.1 VLAN Concepts

This section describes some of the concepts important to the implementation of VLANs in RUGGEDCOM ROS.

7.1.1.1 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.

7.1.1.2 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.

7.1.1.3 The Management VLAN

Management traffic, like all traffic on the network, must belong to a specific VLAN. The management VLAN is configurable and always defaults to VLAN 1. This VLAN is also the default native VLAN for all ports, thus allowing all ports the possibility of managing the product. Changing the management VLAN can be used to restrict management access to a specific set of users.

7.1.1.4 Edge and Trunk Port Types

Each port can be configured as an edge or trunk port.

An edge port attaches to a single end device, such as a PC or Intelligent Electronic Device (IED). An edge port carries traffic on the native VLAN.

Trunk ports are part of the network and carry traffic for all VLANs between switches. Trunk ports are automatically members of all VLANs configured in the switch.

The switch can 'pass through' traffic, forwarding frames received on one trunk port out of another trunk port. The trunk ports must be members of all VLANs that the 'pass through' traffic is part of, even if none of those VLANs are used on edge ports.

Frames transmitted out of the port on all VLANs other than the port's native VLAN are always sent tagged.

Note

It may be desirable to manually restrict the traffic on the trunk to a specific group of VLANs. For example, when the trunk connects to a device, such as a Layer 3 router, that supports a subset of the available LANs. To prevent the trunk port from being a member of the VLAN, include it in the VLAN's Forbidden Ports list.

For more information about the Forbidden Ports list, refer to "Forbidden Ports List (Page 145)".

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.

7.1.1.5 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:

- If an incoming frame is untagged or has a VID of 0 (priority tagged), the frame is associated with the ingress port's PVID
- If an incoming frame is tagged, the frame is allowed to pass, while keeping its VID
- Incoming frames are only dropped if ingress filtering is enabled and the frame is tagged with a VID that does not match any VLAN to which the ingress port is a member

Egress rules are applied as follows to all frames when they are transmitted by the switch.

- If PVID tagging is enabled, outgoing frames are tagged if they are associated with the egress port's native VLAN, regardless of the egress port's membership type (edge or trunk)
- Frames egressing on an edge interface are dropped if they are associated with a VLAN other than the egress port's native VLAN
- Frames egressing on a trunk interface are tagged if they are associated with a VLAN to which the egress port is a member

7.1.1.6 Forbidden Ports List

Each VLAN can be configured to exclude ports from membership in the VLAN using the forbidden ports list. For more information, refer to "Adding a Static VLAN (Page 156)".

7.1.1.7 VLAN-Aware and VLAN-Unaware Modes

The native operation mode for an IEEE 802.1Q compliant switch is VLAN-aware. Even if a specific network architecture does not use VLANs, RUGGEDCOM ROS'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.Q1 native mode of operation. For example, some applications explicitly require priority-tagged frames to be received by end devices.

To avoid conflicts and provide full compatibility with legacy (VLAN-unaware) devices, RUGGEDCOM ROS can be configured to work in VLAN-unaware mode.

In that mode:

- Frames ingressing a VLAN-unaware device are not associated with any VLAN
- Frames egressing a VLAN-unaware device are sent out unmodified (i.e. in the same untagged, 802.1Q-tagged or priority-tagged format as they were received)

7.1.1.8 GARP VLAN Registration Protocol (GVRP)

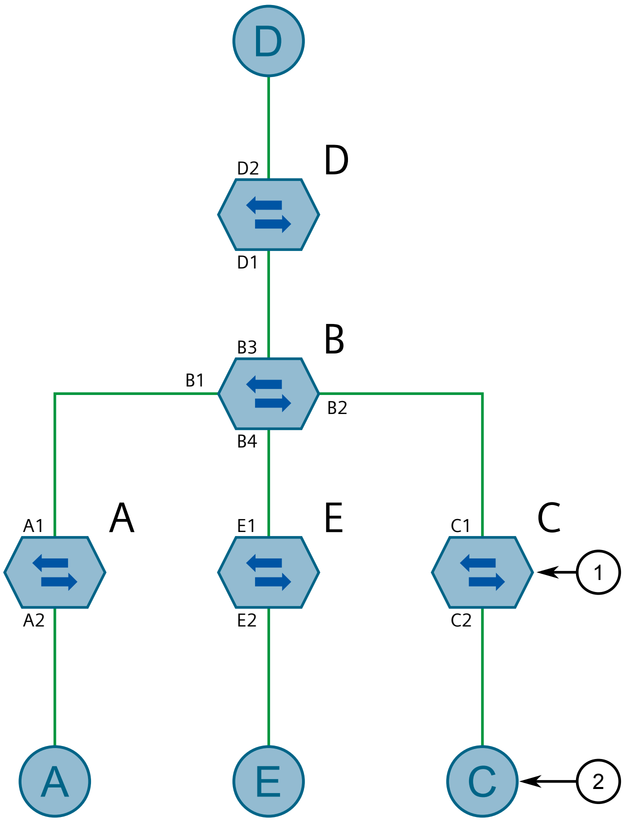
GARP VLAN Registration Protocol (GVRP) is a standard protocol built on GARP (Generic Attribute Registration Protocol) to automatically distribute VLAN configuration information in a network. Each switch in a network needs only to be configured with VLANs it requires locally. VLANs configured elsewhere in the network are learned through GVRP. A GVRP-aware end station (i.e. PC or Intelligent Electronic Device) configured for a particular VID can be connected to a trunk on a GVRP-aware switch and automatically become part of the desired VLAN.

When a switch sends GVRP bridge protocol data units (BPDUs) out of all GVRP-enabled ports, GVRP BPDUs advertise all the VLANs known to that switch (configured manually or learned dynamically through GVRP) to the rest of the network.

When a GVRP-enabled switch receives a GVRP BPDU advertising a set of VLANs, the receiving port becomes a member of those advertised VLANs and the switch begins advertising those VLANs through all the GVRP-enabled ports (other than the port on which the VLANs were learned).

To improve network security using VLANs, GVRP-enabled ports may be configured to prohibit the learning of any new dynamic VLANs but at the same time be allowed to advertise the VLANs configured on the switch.

The following is an example of how to use GVRP:



① Switch
② End Node

Figure 7.1 Using GVRP

- Switch B is the core switch, all others are edge switches
- Ports A1, B1 to B4, C1, D1, D2 and E1 are GVRP aware
- Ports B1 to B4, D1 and D2 are set to advertise and learn
- Ports A1, C1 and E1 are set to advertise only
- Ports A2, C2 and E2 are edge ports
- End node D is GVRP aware
- End nodes A, E and C are GVRP unaware
- Ports A2 and C2 are configured with PVID 7
- Port E2 is configured with PVID 20
- End node D is interested in VLAN 20, hence VLAN 20 is advertised by it towards switch D
- D2 becomes a member of VLAN 20
- Ports A1 and C1 advertise VID 7

- Ports B1 and B2 become members of VLAN 7
- Ports B1, B2 and D1 advertise VID 20
- Ports B3, B4 and D1 become members of VLAN 20

For more information about how to configure GVRP, refer to "Configuring VLANs for Specific Ethernet Ports (Page 153)".

7.1.1.9 PVLAN Edge

Private VLAN (PVLAN) Edge isolates multiple VLAN Edge ports from each other on a single device. When VLAN Edge ports are configured as *protected*, they 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.

For more information about how to configure a port as *protected*, refer to "Configuring VLANs for Specific Ethernet Ports (Page 153)".

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.

7.1.1.10 QinQ

QinQ, also referred to as Stacked VLANs, port bridging, double VLAN-tagging and Nested VLANs, is used to overlay a private Layer 2 network over a public Layer 2 network.

A large network service provider, for example, might have several clients whose networks each use multiple VLANs. It is likely the VLAN IDs used by these different client networks would conflict with one another, were they mixed together in the provider's network. Using double QinQ, each client network could be further tagged using a client-specific VID at the edges where the clients' networks are connected to the network service provider's infrastructure.

Any tagged frames ingressing an edge port of the service provider's switch are tagged with VIDs of the customer’s private network. When those frames egress the switch's QinQ-enabled port into the service provider network, the switch always adds an extra tag (called an *outer tag*) on top of the frame's original VLAN tag (called an *inner tag*). The outer tag VID is the PVID of the frame's ingress edge port. This means that traffic from an individual customer is tagged with their unique VID and is thus segregated from other customers' traffic. For untagged ingress frames, the switch will only add the outer VLAN tag.

Within the service provider network, switching is based on the VID in the outer tag.

The service provider strips the outer VID from the frame on egress, leaving the frame with its original VLAN ID tag. Those frames are then forwarded on the appropriate VLANs.

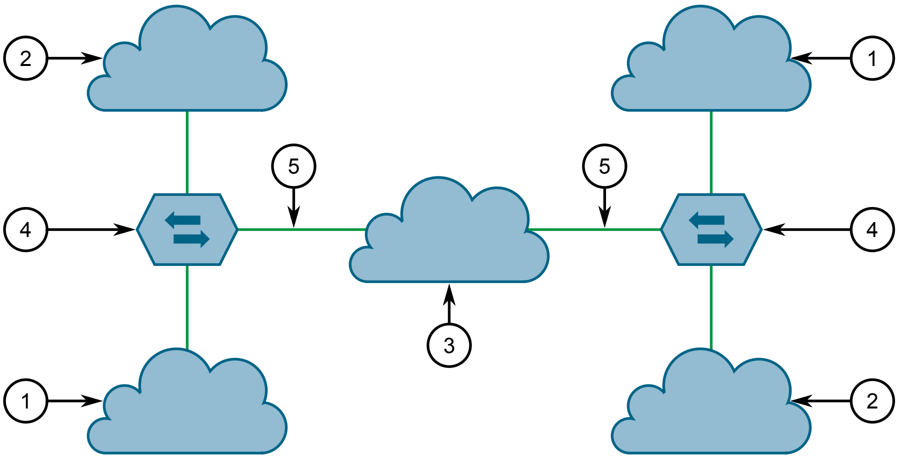
The following figure shows an example of traffic flow using QinQ.

For tagged frames:

- Frames received from customer 1 with VID 100 would carry an inner tag of 100 and an outer tag of VID X (i.e. VLAN 110) which is configured on the edge port connected to customer 1.
- Next, the frames from customer 1 are forwarded through the QinQ port carrying an inner and an outer tag.
- Finally, upon arrival of the frames in the peer switch, the outer VLAN tag is removed and the frames are forwarded with the inner VLAN tag towards customer 1.

For untagged frames:

- Frames received from customer 2 would carry an outer tag of VID Y(i.e VLAN 220) which is configured on the edge port connected to customer 2.
- Next, the frames from customer 2 are forwarded through the QinQ port carrying the outer tag.
- Finally, upon arrival of the frames in the peer switch, the outer VLAN tag is removed before the frames are forwarded to customer 2.



① Customer 1 (PVID is X)
② Customer 2 (PVID is Y)
③ Network Service Provider Infrastructure
④ Switch
⑤ QinQ

Figure 7.2 Using QinQ

Note

Depending on the hardware installed, some switch models allow only one switch port be configured to QinQ mode at a time.

Note
When QinQ is enabled, all non-QinQ ports will be untagged and cannot be changed, and all QinQ ports will be tagged, and cannot be changed.

7.1.1.11 VLAN Advantages

The following are a few of the advantages offered by VLANs.

Traffic Domain Isolation

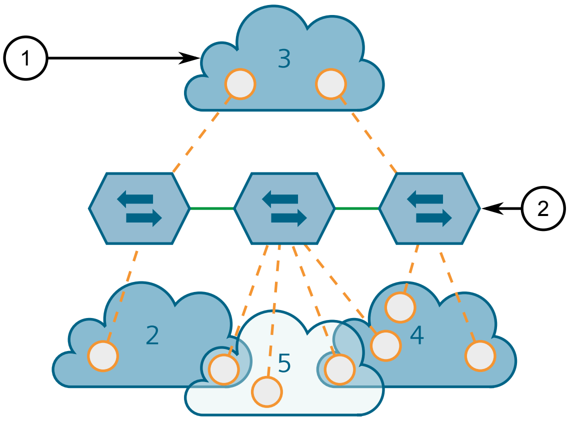
VLANs are most often used for their ability to restrict traffic flows between groups of devices.

Unnecessary broadcast traffic can be restricted to the VLAN that requires it. Broadcast storms in one VLAN need not affect users in other VLANs.

Hosts on one VLAN can be prevented from accidentally or deliberately assuming the IP address of a host on another VLAN.

The use of creative bridge filtering and multiple VLANs can carve seemingly unified IP subnets into multiple regions policed by different security/access policies.

Multi-VLAN hosts can assign different traffic types to different VLANs.



① VLAN
② Switch

Figure 7.3 Multiple Overlapping VLANs

Administrative Convenience

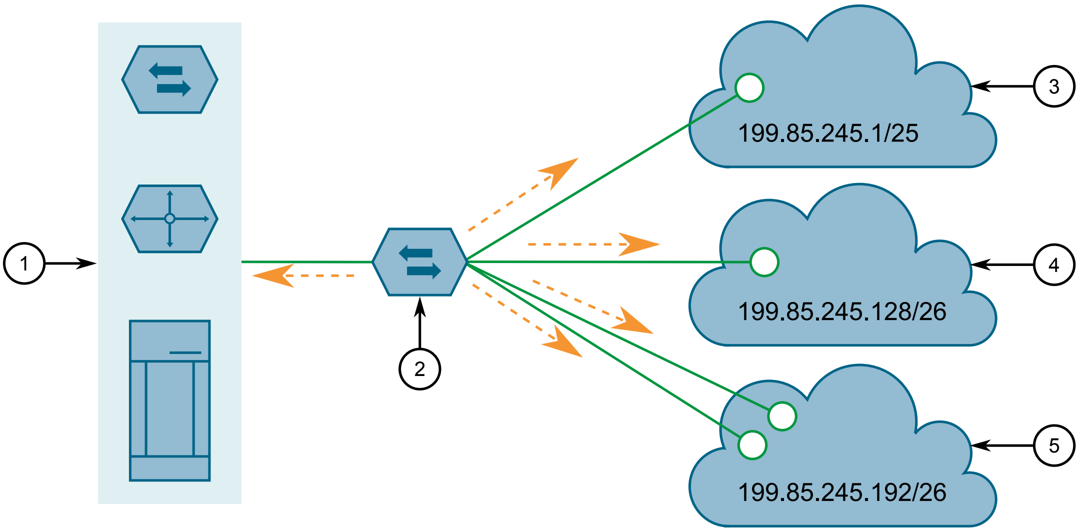
VLANs enable equipment moves to be handled by software reconfiguration instead of by physical cable management. When a host's physical location is changed, its connection point is often changed as well. With VLANs, the host's VLAN membership and priority are simply copied to the new port.

Reduced Hardware

Without VLANs, traffic domain isolation requires the use of separate bridges for separate networks. VLANs eliminate the need for separate bridges.

The number of network hosts may often be reduced. Often, a server is assigned to provide services for independent networks. These hosts may be replaced by a single, multi-horned host supporting each network on its own VLAN. This host can perform routing between VLANs.

Multi-VLAN hosts can assign different traffic types to different VLANs.

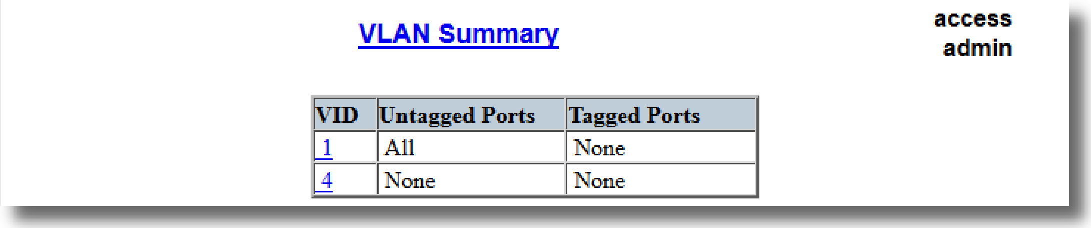


① Server, Router or Layer 3 Switch
② Switch
③ VLAN 2
④ VLAN 4
⑤ VLAN 4

Figure 7.4 Inter-VLAN Communications

7.1.2 Viewing a List of VLANs

To view a list of all VLANs, whether they were created statically, implicitly or dynamically, navigate to ***Virtual LANs » View VLAN Summary***. The **VLAN Summary** table appears.



VLAN Summary

access
admin

VID	Untagged Ports	Tagged Ports
1	All	None
4	None	None

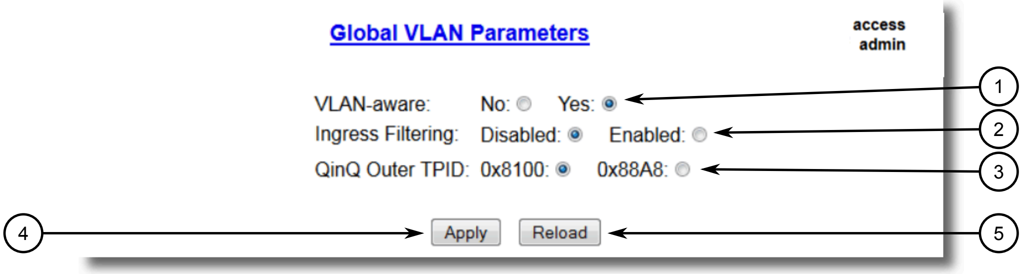
Figure 7.5 VLAN Summary Table

If a VLANs are not listed, add static VLANs as needed. For more information, refer to "Adding a Static VLAN (Page 156)".

7.1.3 Configuring VLANs Globally

To configure global settings for all VLANs, do the following:

1. Navigate to ***Virtual LANs » Configure Global VLAN Parameters***. The **Global VLAN Parameters** form appears.



Global VLAN Parameters

access
admin

VLAN-aware: No: ○ Yes: ●
Ingress Filtering: Disabled: ● Enabled: ○
QinQ Outer TPID: 0x8100: ● 0x88A8: ○

① VLAN-aware Options
② Ingress Filtering Options
③ QinQ Outer TPID options
④ Apply Button
⑤ Reload Button

Figure 7.6 Global VLAN Parameters Form

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

Parameter	Description
`VLAN-aware`	**Synopsis:** [No | Yes] **Default:** Yes Set either VLAN-aware or VLAN-unaware mode of operation.
`Ingress Filtering`	**Synopsis:** [Disabled | Enabled] **Default:** Disabled Enables or disables VLAN ingress filtering on all ports. When enabled, any tagged packet arriving at a port, which is not a member of a VLAN with which that packet is associated, is dropped. When disabled, packets are not dropped.

Parameter	Description
	Note Ingress filtering has no effect when ports are in either VLAN-unaware mode or Q-in-Q mode.
`QinQ Outer TPID`	**Synopsis:** [0x8100 | 0x88A8] **Default:** 0x8100 Selects an Ethertype to be used as the Tag Protocol Identifier (TPID) on VLAN QinQ ports when QinQ is enabled. Frames that ingress a VLAN QinQ port will be identified as outer VLAN tagged if the first Ethertype matches this value; an outer VLAN tag with the TPID field assigned to this value will be inserted to frames that egress a VLAN QinQ port. **Note** When QinQ is enabled, all non-QinQ ports will be untagged and cannot be changed, and all QinQ ports will be tagged, and cannot be changed.

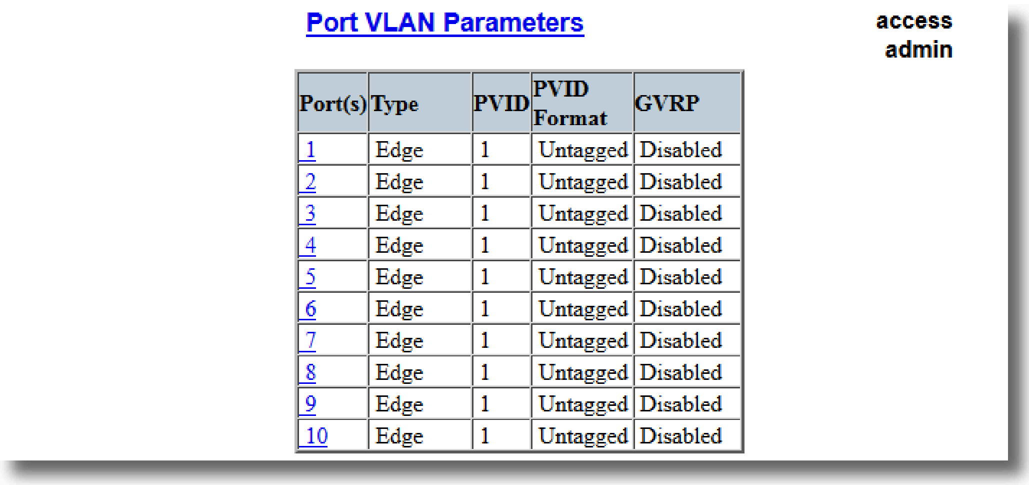
3. Click **Apply**.

7.1.4 Configuring VLANs for Specific Ethernet Ports

When a VLAN ID is assigned to an Ethernet port, the VLAN appears in the VLAN Summary table where it can be further configured.

To configure a VLAN for a specific Ethernet port, do the following:

1. Navigate to ***Virtual LANs » Configure Port VLAN Parameters***. The **Port VLAN Parameters** table appears.



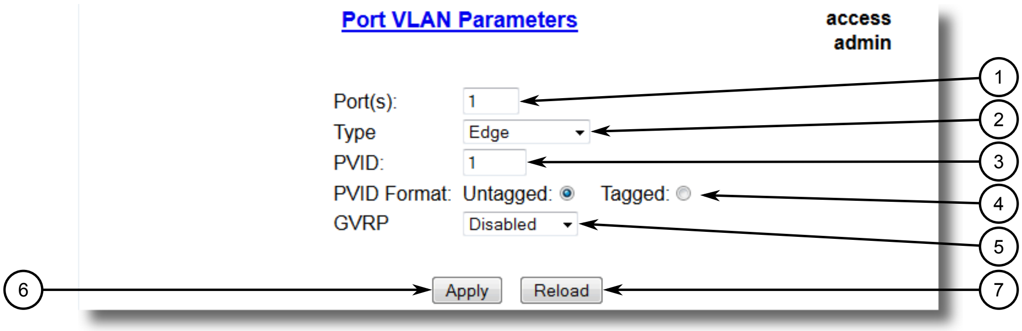
Port VLAN Parameters

access
admin

Port(s)	Type	PVID	PVID Format	GVRP
1	Edge	1	Untagged	Disabled
2	Edge	1	Untagged	Disabled
3	Edge	1	Untagged	Disabled
4	Edge	1	Untagged	Disabled
5	Edge	1	Untagged	Disabled
6	Edge	1	Untagged	Disabled
7	Edge	1	Untagged	Disabled
8	Edge	1	Untagged	Disabled
9	Edge	1	Untagged	Disabled
10	Edge	1	Untagged	Disabled

Figure 7.7 Port VLAN Parameters Table

2. Select a port. The **Port VLAN Parameters** form appears.



Port VLAN Parameters

access
admin

Port(s): 1
Type: Edge
PVID: 1
PVID Format: Untagged: ● Tagged: ○
GVRP: Disabled

① Port(s) Box
② Type List
③ PVID Box
④ PVID Format Options
⑤ GVRP List
⑥ Apply Button
⑦ Reload Button

Figure 7.8 Port VLAN Parameters Form

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

Parameter	Description
`Port(s)`	**Synopsis:** Any combination of numbers valid for this parameter The port number as seen on the front plate silkscreen of the switch (or a list of ports, if aggregated in a port trunk).
`Type`	**Synopsis:** [Edge | Trunk | PVLANEdge | QinQ] **Default:** Edge This parameter specifies how the port determines its membership in VLANs. There are few types of ports: • Edge – the port is only a member of one VLAN (its native VLAN specified by the PVID parameter). • 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. • PVLANEdge – the port is only a member of one VLAN (its native VLAN specified by the PVID parameter), and does not forward traffic to other PVLANedge ports within the same VLAN. • QinQ – the port is a trunk port using double-VLAN tagging, or nested VLANs. An extra VLAN tag is always added to all frames egressing this port. VID in the added extra tag is

Parameter	Description
	the PVID of the frame's ingress port. VLAN tag is always stripped from frames ingressing this port. **Note** Depending on the hardware installed, some switch models allow only one switch port be configured to QinQ mode at a time.
`PVID`	**Synopsis:** An integer between 1 and 4094 **Default:** 1 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. Modify this parameter with care! By default, the switch is programmed to use VLAN 1 for management and every port on the switch is programmed to use VLAN 1. If you modify a switch port to use a VLAN other than the management VLAN, devices on that port will not be able to manage the switch.
`PVID Format`	**Synopsis:** [Untagged | Tagged] **Default:** Untagged Specifies whether frames transmitted out of the port on its native VLAN (specified by the *`PVID`* parameter) will be tagged or untagged. **Note** When QinQ is enabled, all non-QinQ ports will be untagged and cannot be changed, and all QinQ ports will be tagged, and cannot be changed.
`GVRP`	**Synopsis:** [Adv&Learn | Adv Only | Disabled] **Default:** Disabled Configures 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 & LEARN – the port will declare all VLANs existing in the switch (configured or learned) and can dynamically learn VLANs. Only Trunk ports are GVRP-capable.

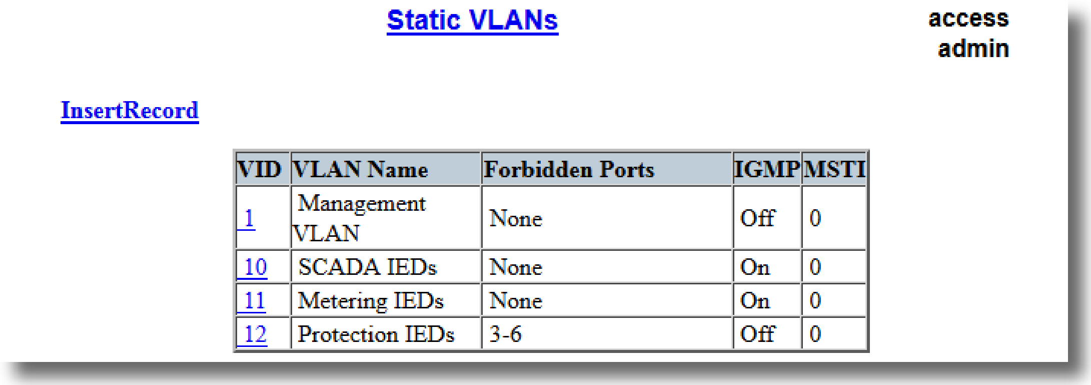
4. Click **Apply**.

7.1.5 Managing Static VLANs

This section describes how to configure and manage static VLANs.

7.1.5.1 Viewing a List of Static VLANs

To view a list of static VLANs, navigate to ***Virtual LANs » Configure Static VLANs***. The **Static VLANs** table appears.



Static VLANs

access
admin

InsertRecord

VID	VLAN Name	Forbidden Ports	IGMP	MSTI
1	Management VLAN	None	Off	0
10	SCADA IEDs	None	On	0
11	Metering IEDs	None	On	0
12	Protection IEDs	3-6	Off	0

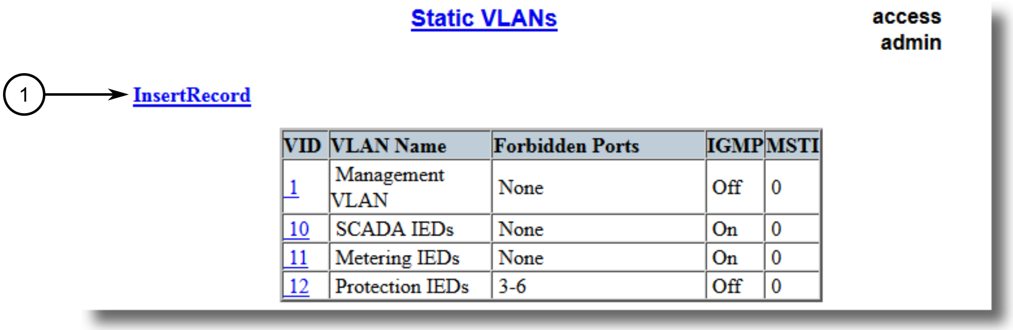
Figure 7.9 Static VLANs Table

If a static VLAN is not listed, add the VLAN. For more information, refer to "Adding a Static VLAN (Page 156)".

7.1.5.2 Adding a Static VLAN

To add a static VLAN, do the following:

1. Navigate to ***Virtual LANs » Configure Static VLANs***. The **Static VLANs** table appears.



Static VLANs

access
admin

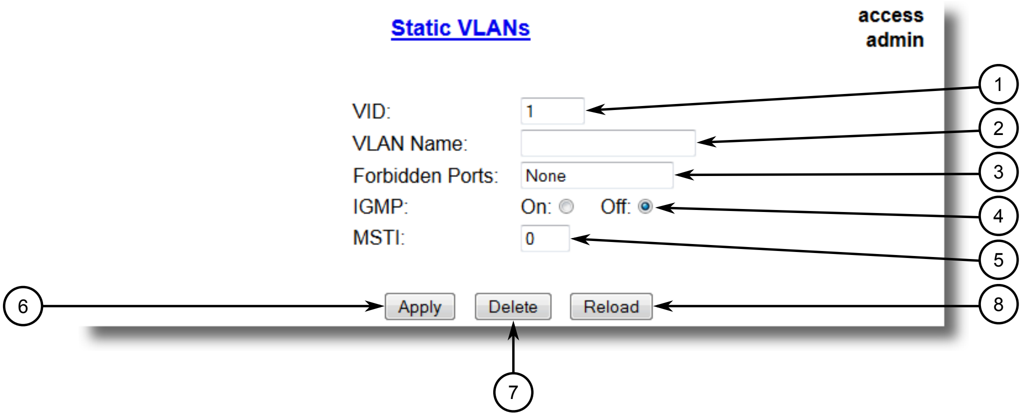
InsertRecord

VID	VLAN Name	Forbidden Ports	IGMP	MSTI
1	Management VLAN	None	Off	0
10	SCADA IEDs	None	On	0
11	Metering IEDs	None	On	0
12	Protection IEDs	3-6	Off	0

① InsertRecord

Figure 7.10 Static VLANs Table

2. Click **InsertRecord**. The **Static VLANs** form appears.



Static VLANs

VID: 1

VLAN Name:

Forbidden Ports: None

IGMP: On: ○ Off: ●

MSTI: 0

① VID Box
② VLAN Name Box
③ Forbidden Ports Box
④ IGMP Options
⑤ MSTI Box
⑥ Apply Button
⑦ Delete Button
⑧ Reload Button

Figure 7.11 Static VLANs Form

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

Note
If **IGMP Options** is not enabled for the VLAN, both IGMP messages and multicast streams will be forwarded directly to all members of the VLAN. If any one member of the VLAN joins a multicast group, then all members of the VLAN will receive the multicast traffic.

Parameter	Description
`VID`	**Synopsis:** An integer between 1 and 4094 **Default:** 1 The VLAN Identifier is used to identify the VLAN in tagged Ethernet frames according to IEEE 802.1Q.
`VLAN Name`	**Synopsis:** A string 19 characters long The VLAN name provides a description of the VLAN purpose (for example, Engineering VLAN).
`Forbidden Ports`	**Synopsis:** Any combination of numbers valid for this parameter These are ports that are not allowed to be members of the VLAN. Examples: • None – all ports of the switch are allowed to be members of the VLAN

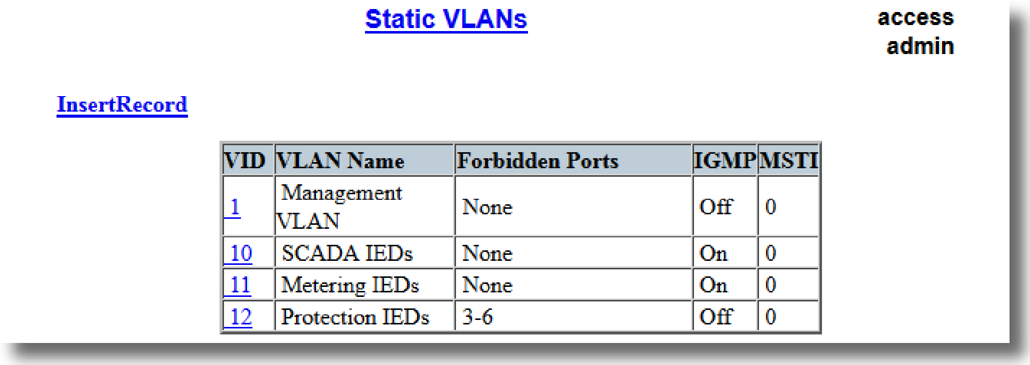
Parameter	Description
	• 2,4-6,8 – all ports except ports 2, 4, 6, 7 and 8 are allowed to be members of the VLAN
`IGMP`	**Synopsis:** [Off | On] **Default:** Off This parameter enables or disables IGMP Snooping on the VLAN.
`MSTI`	**Synopsis:** An integer between 0 and 16 **Default:** 0 This parameter is 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) to which the VLAN should be mapped.

4. Click **Apply**.

7.1.5.3 Deleting a Static VLAN

To delete a static VLAN, do the following:

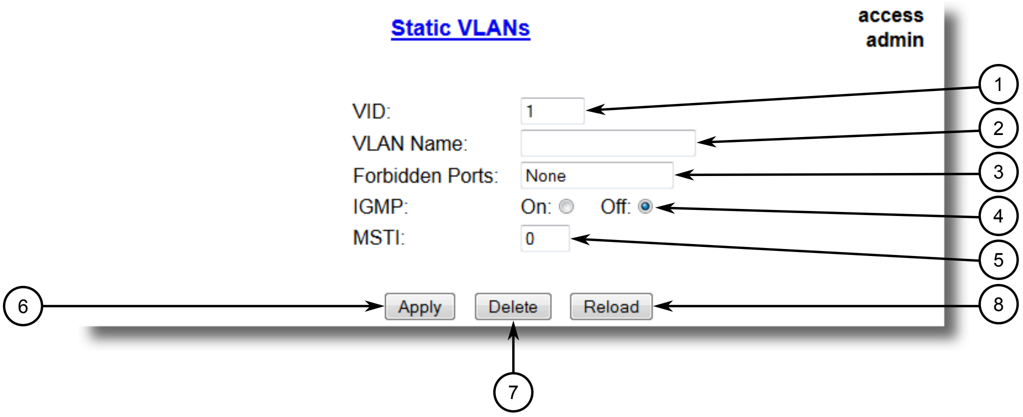
1. Navigate to ***Virtual LANs » Configure Static VLANs***. The **Static VLANs** table appears.



VID	VLAN Name	Forbidden Ports	IGMP	MSTI
1	Management VLAN	None	Off	0
10	SCADA IEDs	None	On	0
11	Metering IEDs	None	On	0
12	Protection IEDs	3-6	Off	0

Figure 7.12 Static VLANs Table

2. Select the static VLAN from the table. The **Static VLANs** form appears.



Static VLANs
access
admin

VID:	1
VLAN Name:	
Forbidden Ports:	None
IGMP:	On: ○ Off: ●
MSTI:	0

① VID Box
② VLAN Name Box
③ Forbidden Ports Box
④ IGMP Options
⑤ MSTI Box
⑥ Apply Button
⑦ Delete Button
⑧ Reload Button

Figure 7.13 Static VLANs Form

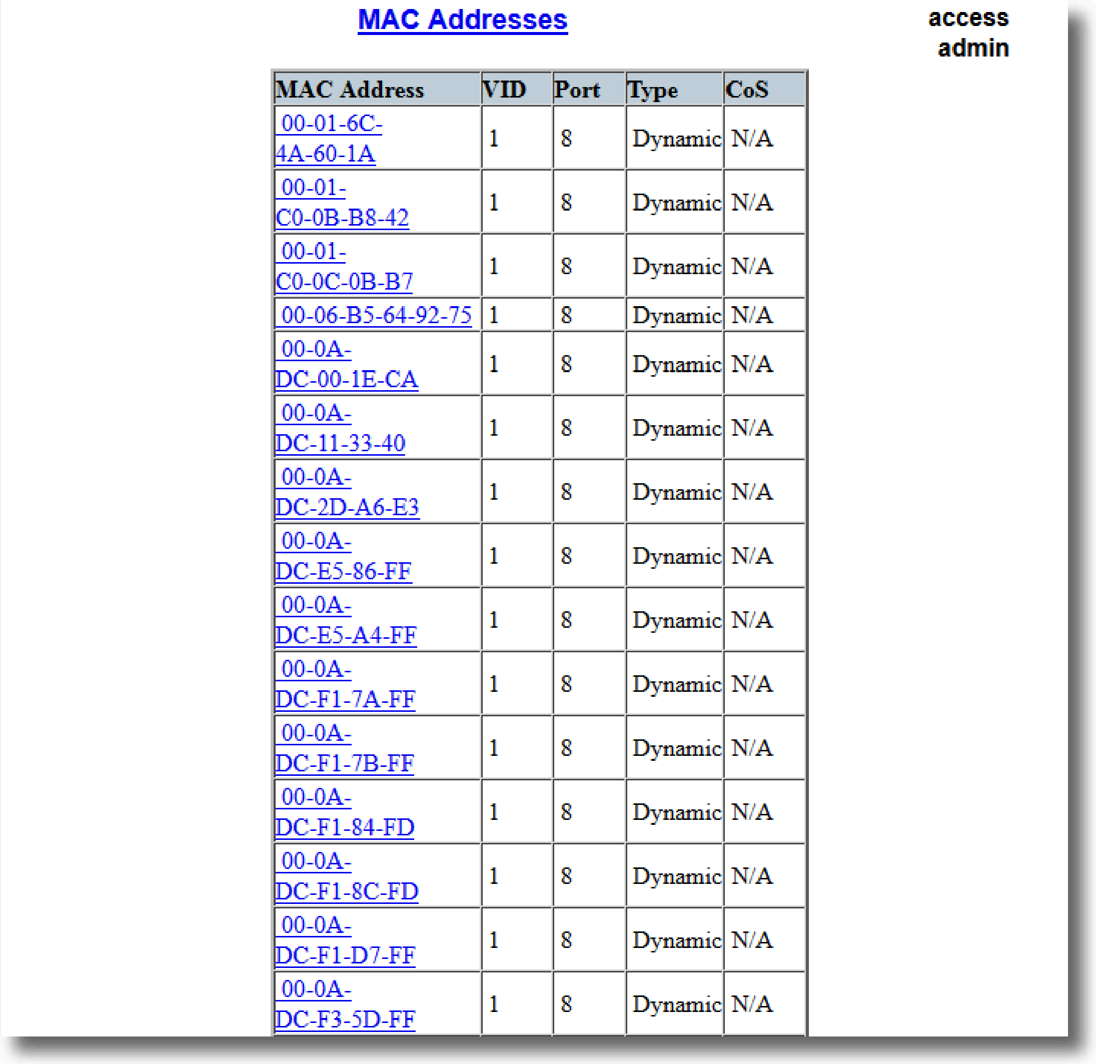
3. Click **Delete**.

7.2 Managing MAC Addresses

This section describes how to manage MAC addresses.

7.2.1 Viewing a List of MAC Addresses

To view a list of all static and dynamically learned MAC addresses, navigate to ***MAC Address Tables » View MAC Addresses***. The **MAC Addresses** table appears.



MAC Addresses

access
admin

MAC Address	VID	Port	Type	CoS
00-01-6C-4A-60-1A	1	8	Dynamic	N/A
00-01-C0-0B-B8-42	1	8	Dynamic	N/A
00-01-C0-0C-0B-B7	1	8	Dynamic	N/A
00-06-B5-64-92-75	1	8	Dynamic	N/A
00-0A-DC-00-1E-CA	1	8	Dynamic	N/A
00-0A-DC-11-33-40	1	8	Dynamic	N/A
00-0A-DC-2D-A6-E3	1	8	Dynamic	N/A
00-0A-DC-E5-86-FF	1	8	Dynamic	N/A
00-0A-DC-E5-A4-FF	1	8	Dynamic	N/A
00-0A-DC-F1-7A-FF	1	8	Dynamic	N/A
00-0A-DC-F1-7B-FF	1	8	Dynamic	N/A
00-0A-DC-F1-84-FD	1	8	Dynamic	N/A
00-0A-DC-F1-8C-FD	1	8	Dynamic	N/A
00-0A-DC-F1-D7-FF	1	8	Dynamic	N/A
00-0A-DC-F3-5D-FF	1	8	Dynamic	N/A

Figure 7.14 MAC Address Table

If a MAC address is not listed, do the following:

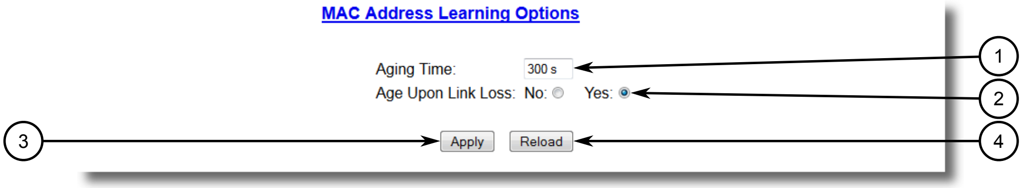
1. Configure the MAC address learning options to control the aging time of dynamically learned MAC addresses of other devices on the network. For more information, refer to "Configuring MAC Address Learning Options (Page 160)".
2. Configure the address on the device as a static MAC address. For more information, refer to "Adding a Static MAC Address (Page 164)".

7.2.2 Configuring MAC Address Learning Options

The MAC address learning options control how and when MAC addresses are removed automatically from the MAC address table. Individual addresses are removed when the aging timer is exceeded. Addresses can also be removed when a link failure or topology change occurs.

To configure the MAC address learning options, do the following:

1. Navigate to ***MAC Address Tables » Configure MAC Address Learning Options***. The **MAC Address Learning Options** form appears.



MAC Address Learning Options

Aging Time: 300 s

Age Upon Link Loss: No: ○ Yes: ●

① Aging Time Box
② Age Upon Link Loss Options
③ Apply Button
④ Reload Button

Figure 7.15 MAC Address Learning Options Form

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

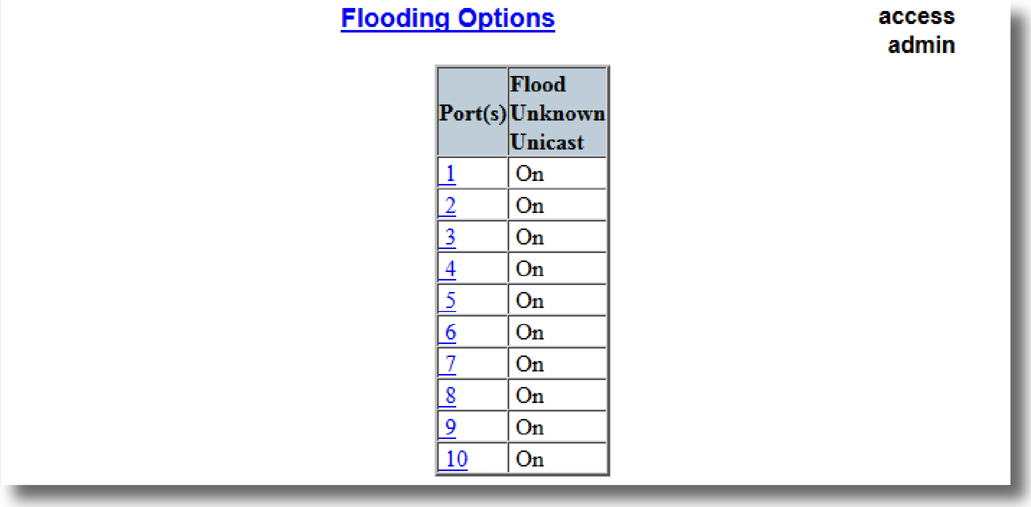
Parameter	Description
`Aging Time`	**Synopsis:** An integer between 15 and 800 **Default:** 300 This parameter configures the time that a learned MAC address is held before being aged out.
`Age Upon Link Loss`	**Synopsis:** [No | Yes] **Default:** Yes When set to Yes, all MAC addresses learned on a failed port will be aged-out immediately upon link failure detection. When link failure 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. Note that when a network redundancy protocol, e.g. RSTP/MSTP, is enabled on the switch, that redundancy protocol may, upon a link failure, flush MAC addresses learned on the failed port regardless of the setting of this parameter.

3. Click **Apply**.

7.2.3 Configuring MAC Address Flooding Options

To configure the MAC address flooding options, do the following:

1. Navigate to ***MAC Address Tables » Configure MAC Address Flooding Options***. The **Flooding Options** table appears.



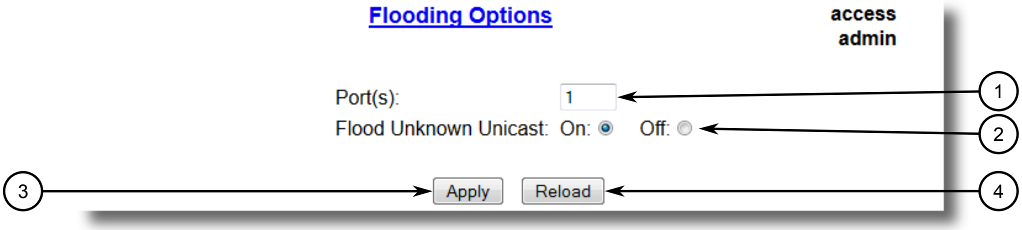
Flooding Options

access
admin

Port(s)	Flood Unknown Unicast
1	On
2	On
3	On
4	On
5	On
6	On
7	On
8	On
9	On
10	On

Figure 7.16 Flooding Options Table

2. Select a port. The **Flooding Options** form appears.



Flooding Options

access
admin

Port(s): 1

Flood Unknown Unicast: On: ● Off: ○

① Port(s) Box
② Flood Unknown Unicast Options
③ Apply Button
④ Reload Button

Figure 7.17 Flooding Options Form

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

Parameter	Description
Port(s)	**Synopsis:** Comma-separated list of ports The port number as seen on the front plate silkscreen of the switch (or a list of ports, if aggregated in a port trunk).

Parameter	Description
`Flood Unknown Unicast`	**Synopsis:** [On | Off] **Default:** On Normally, unicast traffic with an unknown destination address is flooded out of all ports. When a port is configured to turn off this kind of flooding, the unknown unicast traffic is not sent out from the selected port.

4. Click **Apply**.

7.2.4 Managing Static MAC Addresses

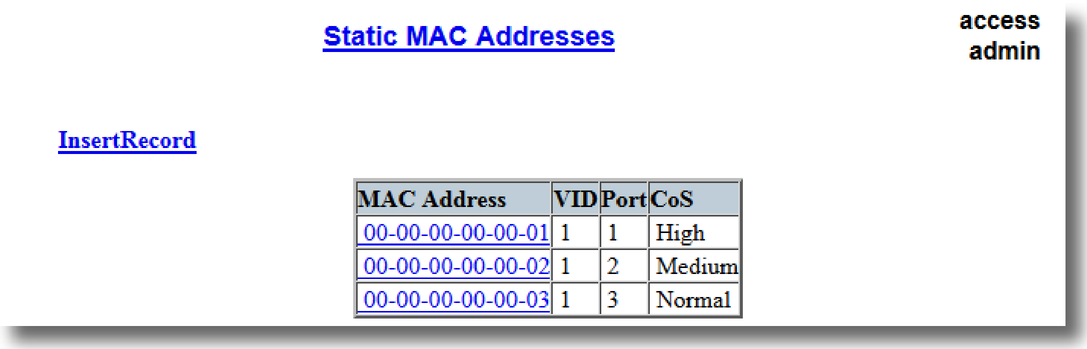
Static MAC addresses must be configured when the device is only able to receive frames, not transmit them. They may also need to be configured if port security (if supported) must be enforced.

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.

Note
A MAC address cannot be learned on a VLAN that has not been configured in the Static VLAN table. If a frame with an unknown VLAN tag arrives on a secured port, it is considered a security violation and RUGGEDCOM ROS will generate a port security alarm.

7.2.4.1 Viewing a List of Static MAC Addresses

To view a list of static MAC addresses configured on the device, navigate to ***MAC Address Tables » Configure Static MAC Addresses***. The **Static MAC Addresses** table appears.



MAC Address	VID	Port	CoS
00-00-00-00-00-01	1	1	High
00-00-00-00-00-02	1	2	Medium
00-00-00-00-00-03	1	3	Normal

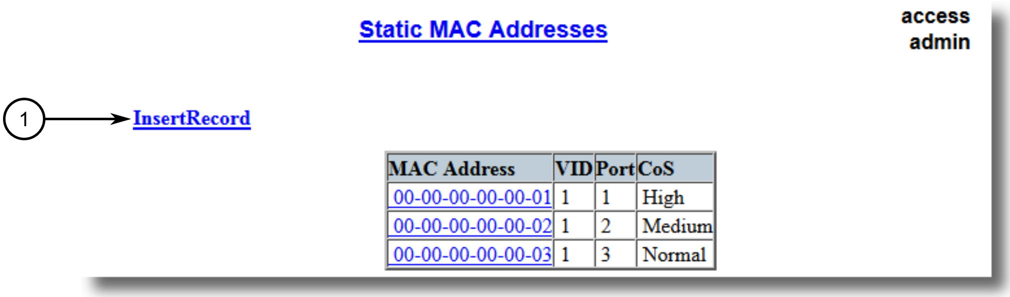
Figure 7.18 Static MAC Address Table

If static MAC addresses have not been configured, add addresses as needed. For more information, refer to "Adding a Static MAC Address (Page 164)".

7.2.4.2 Adding a Static MAC Address

To add a static MAC address to the Static MAC Address Table, do the following:

1. Navigate to ***MAC Address Tables » Configure Static MAC Addresses***. The **Static MAC Addresses** table appears.

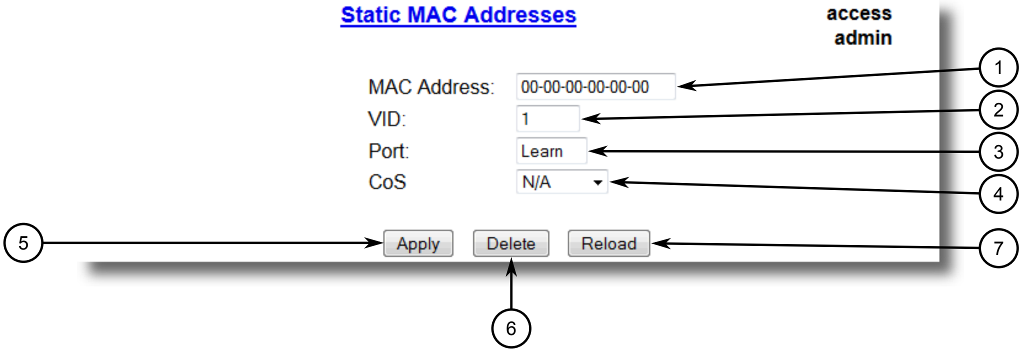


MAC Address	VID	Port	CoS
00-00-00-00-00-01	1	1	High
00-00-00-00-00-02	1	2	Medium
00-00-00-00-00-03	1	3	Normal

① InsertRecord

Figure 7.19 Static MAC Addresses Table

2. Click **InsertRecord**. The **Static MAC Addresses** form appears.



MAC Address:	00-00-00-00-00-00
VID:	1
Port:	Learn
CoS	N/A

① MAC Address Box
② VID Box
③ Port Box
④ CoS List
⑤ Apply Button
⑥ Delete Button
⑦ Reload Button

Figure 7.20 Static MAC Addresses Form

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

Parameter	Description
`MAC Address`	**Synopsis:** ##-##-##-##-##-## where ## ranges 0 to FF A MAC address learned by the switch. Maximum of 6 wildcard characters may be used to specify a range of MAC addresses allowed to be learned by the Port Se-

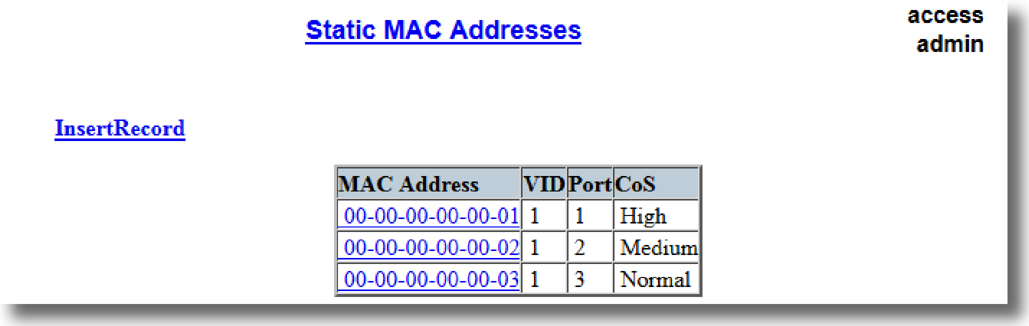
Parameter	Description
	curity module (when Port Security is set to 'Static MAC' mode). Wildcard must start from the right hand end and continuous. Examples: • 00-0A-DC-**-**-** means the entire MAC address space of RuggedCom. • 00-0A-DC-12-3*-** means the range 00-0A-DC-12-30-00 to 00-0A-DC-12-3F-FF.
`VID`	**Synopsis:** An integer between 1 and 4094 or [ANY] **Default:** 1 VLAN Identifier of the VLAN upon which the MAC address operates. Option ANY allows learning a MAC address through the Port Security module on any VLAN's that are configured on the switch.
`Port`	**Synopsis:** 1 to maximum port number or [Learn] **Default:** Learn Enter the port number upon which the device with this address is located. The security mode of the port being selected should not be '802.1X'. If the port should be auto-learned, set this parameter to 'Learn'. The option 'Learn' is applicable for Port Security in 'Static MAC' mode.
`CoS`	**Synopsis:** [N/A | Normal | Medium | High | Crit] **Default:** N/A Prioritizes traffic for the specified MAC address. To not prioritize traffic based on the address, select N/A.

4. Click **Apply**.

7.2.4.3 Deleting a Static MAC Address

To delete a static MAC address from the Static MAC Address Table, do the following:

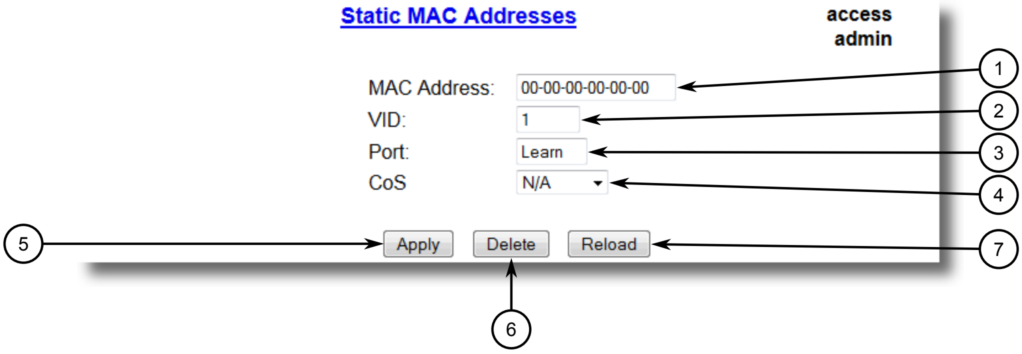
1. Navigate to ***MAC Address Tables » Configure Static MAC Addresses***. The **Static MAC Addresses** table appears.



MAC Address	VID	Port	CoS
00-00-00-00-00-01	1	1	High
00-00-00-00-00-02	1	2	Medium
00-00-00-00-00-03	1	3	Normal

Figure 7.21 Static MAC Addresses Table

2. Select the MAC address from the table. The **Static MAC Addresses** form appears.



MAC Address:	00-00-00-00-00-00
VID:	1
Port:	Learn
CoS	N/A

① MAC Address Box
② VID Box
③ Port Box
④ CoS List
⑤ Apply Button
⑥ Delete Button
⑦ Reload Button

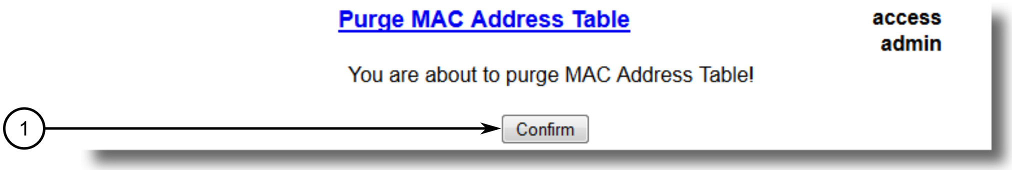
Figure 7.22 Static MAC Addresses Form

3. Click **Delete**.

7.2.5 Purging All Dynamic MAC Addresses

To purge the dynamic MAC address list of all entries, do the following:

1. Navigate to ***MAC Address Tables » Purge MAC Address Table***. The **Purge MAC Address Table** form appears.



Purge MAC Address Table

You are about to purge MAC Address Table!

① Confirm Button

Figure 7.23 Purge MAC Address Table Form

2. Click **Confirm**.

7.3 Managing Multicast Filtering

Multicast traffic can be filtered using IGMP (Internet Group Management Protocol) snooping or GMRP (GARP Multicast Registration Protocol).

7.3.1 Managing 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.

⚠ **NOTICE**

RUGGEDCOM ROS restricts IGMP hosts from subscribing to the following special multicast addresses:

- 224.0.0.0 to 224.0.0.255
- 224.0.1.129

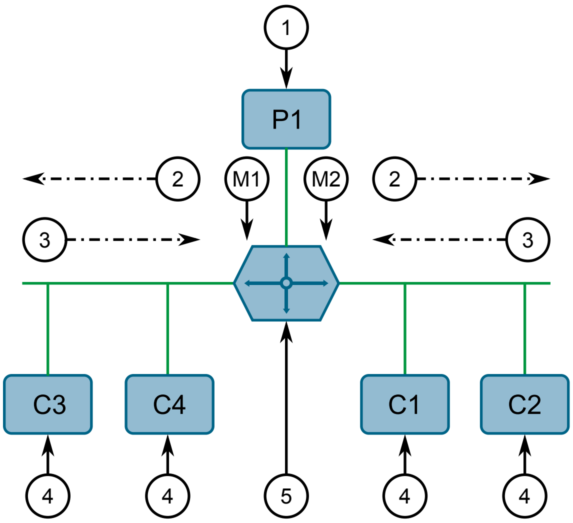
These addresses are reserved for routing protocols and IEEE 1588. If an IGMP membership report contains one of these addresses, the report is forwarded by the switch without learning about the host.

7.3.1.1 IGMP Concepts

The following describes some of the concepts important to the implementation of multicast filtering using IGMP:

IGMP In Operation

The following network diagram provides a simple example of the use of IGMP.



① Producer
② Membership Queries
③ Membership Reports
④ Consumer
⑤ Multicast Router

Figure 7.24 Example – IGMP In Operation

One *producer* IP host (P1) is generating two IP multicast streams, M1 and M2. There are four potential *consumers* of these streams, C1 through C4. The multicast router discovers which host wishes to subscribe to which stream by sending general membership queries to each segment.

In this example, the general membership query sent to the C1-C2 segment is answered by a membership report (or *join*) indicating the desire to subscribe to stream M2. The router will forward the M2 stream to the C1-C2 segment. In a similar fashion, the router discovers that it must forward stream M1 to segment C3-C4.

A *consumer* may join any number of multicast groups, issuing a membership report for each group. When a host issues a membership report, other hosts on the same network segment that also require membership to the same group suppress their own requests, since they would be redundant. In this way, the IGMP protocol guarantees the segment will issue only one membership report for each group.

The router periodically queries each of its segments in order to determine whether at least one consumer still subscribes to a given stream. If it receives no responses within a given time period (usually two query intervals), the router will prune the multicast stream from the given segment.

A more common method of pruning occurs when consumers wishing to unsubscribe issue an IGMP *leave group* message. The router will immediately issue a group-specific membership query to determine whether there are any remaining subscribers of that group on the segment. After the last consumer of a group has unsubscribed, the router will prune the multicast stream from the given segment.

Switch IGMP Operation

The IGMP Snooping feature provides a means for switches to snoop (i.e. watch) the operation of routers, respond with joins/leaves on the behalf of consumer ports, and prune multicast streams accordingly. There are two modes of IGMP the switch can be configured to assume: active and passive.

- **Active Mode**

  IGMP supports a *routerless* mode of operation.

  When such a switch is used without a multicast router, it is able to function as if it is a multicast router sending IGMP general queries.

- **Passive Mode**

  When such a switch is used in a network with a multicast router, it can be configured to run Passive IGMP. This mode prevents the switch from sending the queries that can confuse the router causing it to stop issuing IGMP queries.

Note
A switch running in passive mode requires the presence of a multicast router or it will be unable to forward multicast streams at all if no multicast routers are present.

Note
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 IGMPv2 *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.

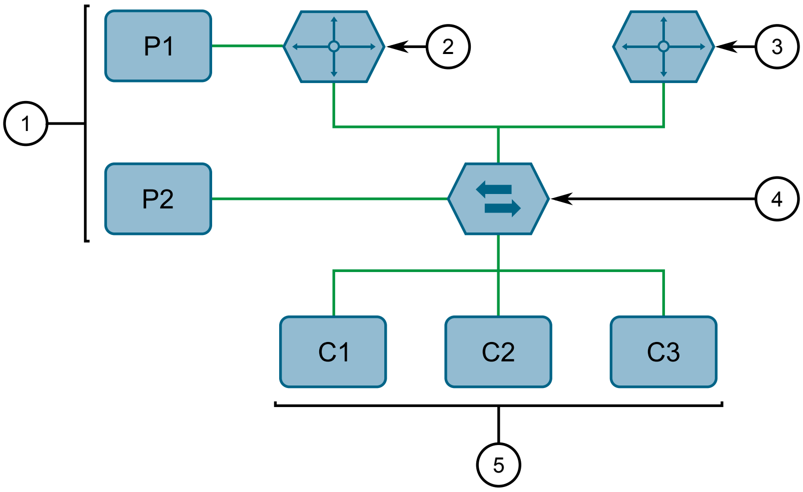
If RSTP detects a change in the network topology, IGMP will take some actions to avoid the loss of multicast connectivity and reduce network convergence time:

- 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 configured as RSTP Edge Ports.

Combined Router and Switch IGMP Operation

The following example illustrates the challenges faced with multiple routers, VLAN support and switching.

Producer P1 resides on VLAN 2 while P2 resides on VLAN 3. Consumer C1 resides on both VLANs whereas C2 and C3 reside on VLANs 3 and 2, respectively. Router 2 resides on VLAN 2, presumably to forward multicast traffic to a remote network or act as a source of multicast traffic itself.



① Producer
② Multicast Router 1
③ Multicast Router 2
④ Switch
⑤ Host

Figure 7.25 Example – Combined Router and Switch IGMP In Operation

In this example:

- P1, Router 1, Router 2 and C3 are on VLAN 2
- P2 and C2 are on VLAN 3
- C1 is on both VLAN 2 and 3

Assuming that router 1 is the querier for VLAN 2 and router 2 is simply a non-querier, the switch will periodically receive queries from router 1 and maintain the information concerning which port links to the multicast router. However, the switch port that links to router 2 must be manually configured as a *router port*. Otherwise, the switch will send neither multicast streams nor joins/leaves to router 2.

Note that VLAN 3 does not have an external multicast router. The switch should be configured to operate in its *routerless* mode and issue general membership queries as if it is the router.

- **Processing Joins**

  If host C1 wants to subscribe to the multicast streams for both P1 and P2, it will generate two membership reports. The membership report from C1 on VLAN 2 will cause the switch to immediately initiate its own membership report to multicast router 1 (and to issue its own membership report as a response to queries).

  The membership report from host C1 for VLAN 3 will cause the switch to immediately begin forwarding multicast traffic from producer P2 to host C2.

- **Processing Leaves**

  When host C1 decides to leave a multicast group, it will issue a leave request to the switch. The switch will poll the port to determine if host C1 is the last member of the group on that port. If host C1 is the last (or only) member, the group will immediately be pruned from the port.

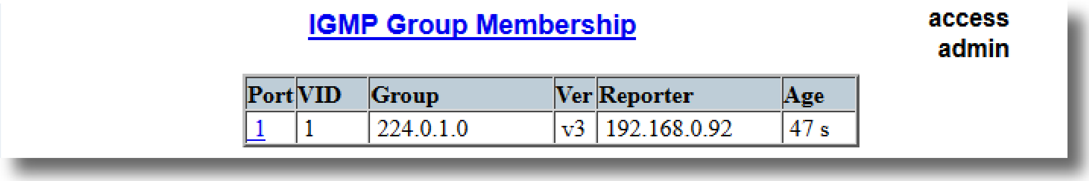
Should host C1 leave the multicast group without issuing a leave group message and then fail to respond to a general membership query, the switch will stop forwarding traffic after two queries.

When the last port in a multicast group leaves the group (or is aged-out), the switch will issue an IGMP leave report to the router.

7.3.1.2 Viewing a List of Multicast Group Memberships

Using IGMP snooping, RUGGEDCOM ROS records group membership information on a per-port basis based on membership reports it observes between the router and host.

To view a list of multicast group memberships, navigate to ***Multicast Filtering » View IGMP Group Membership***. The **IGMP Group Membership** table appears.



IGMP Group Membership

access
admin

Port	VID	Group	Ver	Reporter	Age
1	1	224.0.1.0	v3	192.168.0.92	47 s

Figure 7.26 IGMP Group Membership Table

This table provides the following information:

Parameter	Description
`Port`	**Synopsis:** 1 to maximum port number The port number as seen on the front plate silkscreen of the switch.
`VID`	**Synopsis:** An integer between 0 and 65535 VLAN Identifier of the VLAN upon which the multicast group operates.
`Group`	**Synopsis:** ###.###.###.### where ### ranges from 0 to 255 Multicast Group Address.
`Ver`	**Synopsis:** [v3 | v2 | v1] Specifies the IGMP version of the learnt multicast group.
`Reporter`	**Synopsis:** ###.###.###.### where ### ranges from 0 to 255 Specifies the source IP address that is reporting subscription to the multicast group.
`Age`	**Synopsis:** An integer between 0 and 7210 Specifies the current age of the IP multicast group learned on the port in seconds.

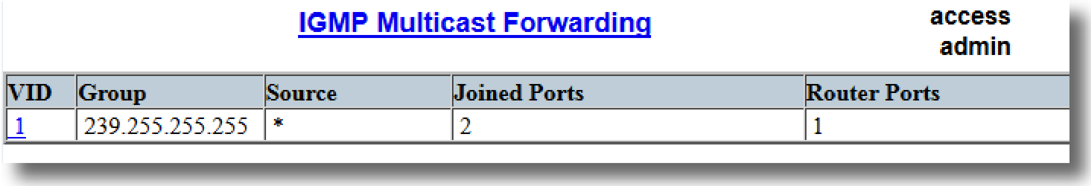
If the table is empty, do the following:

- Make sure traffic is being sent to the device.
- Make sure IGMP is properly configured on the device. For more information, refer to "Configuring IGMP (Page 174)".

7.3.1.3 Viewing Forwarding Information for Multicast Groups

Multicast forwarding information for every source, group and VLAN combination learned by RUGGEDCOM ROS is recorded in the IGMP Multicast Forwarding table.

To view the IGMP Multicast Forwarding table, navigate to ***Multicast Filtering » View IGMP Multicast Forwarding***. The **IGMP Multicast Forwarding** table appears.



IGMP Multicast Forwarding

access
admin

VID	Group	Source	Joined Ports	Router Ports
1	239.255.255.255	*	2	1

Figure 7.27 IGMP Multicast Forwarding Table

This table provides the following information:

Parameter	Description
VID	**Synopsis:** An integer between 0 and 65535 VLAN Identifier of the VLAN upon which the multicast group operates.
Group	**Synopsis:** ###.###.###.### where ### ranges from 0 to 255 Multicast Group Address.
Source	**Synopsis:** ###.###.###.### where ### ranges from 0 to 255 or [*] Source Address. * means all possible source addresses.
Joined Ports	**Synopsis:** Comma-separated list of ports All ports that currently receive multicast traffic for the specified multicast group.
Router Ports	**Synopsis:** Comma-separated list of ports All ports that have been manually configured or dynamically discovered (by observing router specific traffic) as ports that link to multicast routers.

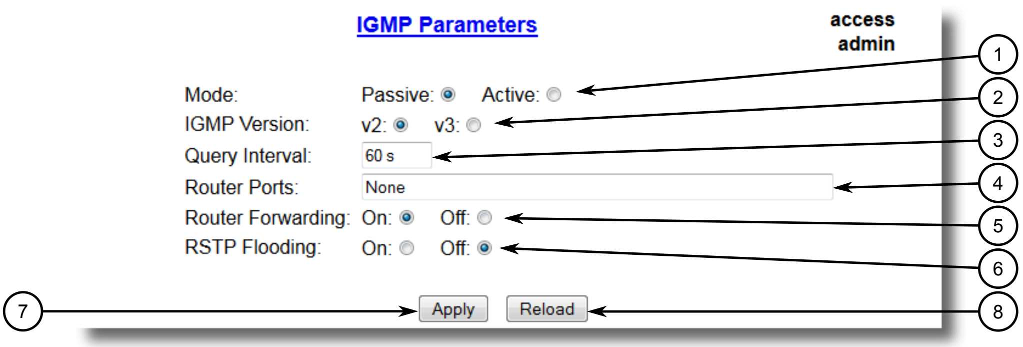
If the table is empty, do the following:

- Make sure traffic is being sent to the device.
- Make sure IGMP is properly configured on the device. For more information, refer to "Configuring IGMP (Page 174)".

7.3.1.4 Configuring IGMP

To configure the IGMP, do the following:

1. Make sure one or more static VLANs exist with IGMP enabled. For more information, refer to "Managing Static VLANs (Page 156)".
2. Navigate to ***Multicast Filtering » Configure IGMP Parameters***. The **IGMP Parameters** form appears.



IGMP Parameters

access
admin

Mode: Passive: ● Active: ○
IGMP Version: v2: ● v3: ○
Query Interval: 60 s
Router Ports: None
Router Forwarding: On: ● Off: ○
RSTP Flooding: On: ○ Off: ●

① Mode Options
② IGMP Version
③ Query Interval Box
④ Router Ports Box
⑤ Router Forwarding Options
⑥ RSTP Flooding Options
⑦ Apply Button
⑧ Reload Button

Figure 7.28 IGMP Parameters Form

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

Parameter	Description
`Mode`	**Synopsis:** [Passive | Active] **Default:** Passive Specifies the IGMP mode. Options include: • 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 being the querier are detected for a while.
`IGMP Version`	**Synopsis:** [v2 | v3] **Default:** v2 Specifies the configured IGMP version on the switch. Options include: • v2 – Sets the IGMP version to version 2. When selected for a snooping switch, all IGMP reports and queries greater than v2 are forwarded, but not added to the IGMP Multicast Forwarding table.

Parameter	Description
	• v3 – Sets the IGMP version to version 3. General queries are generated in IGMPv3 format, all versions of IGMP messages are processed by the switch, and traffic is pruned based on multicast group address only.
`Query Interval`	**Synopsis:** An integer between 10 and 3600 **Default:** 60 The time interval between IGMP queries generated by the switch. **Note** This parameter also affects the Group Membership Interval (i.e. the group subscriber aging time), therefore, it takes effect even in PASSIVE mode.
`Router Ports`	**Synopsis:** Comma-separated list of ports **Default:** None This parameter specifies ports that connect to multicast routers. If you do not configure known router ports, the switch may be able to detect them, however it is advisable to pre-configure them.
`Router Forwarding`	**Synopsis:** [Off | On] **Default:** On This parameter specifies whether multicast streams will be always forwarded to multicast routers.
`RSTP Flooding`	**Synopsis:** [Off | On] **Default:** Off This parameter specifies whether multicast streams will be flooded out of all RSTP non-edge ports upon topology change detection. Such flooding is desirable, if guaranteed multicast stream delivery after topology change is most important.

4. Click **Apply**.

7.3.2 Managing GMRP

The 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.

7.3.2.1 GMRP Concepts

The following describes some of the concepts important to the implementation of multicast filtering using GMRP:

Joining a Multicast Group

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:

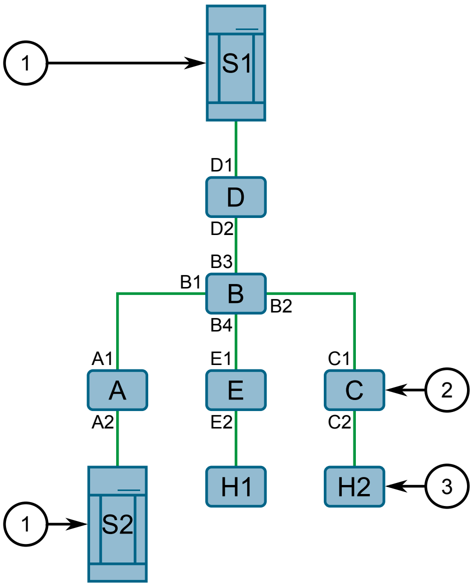
- Forward All Multicast group traffic in the VLAN, or
- Forward All Unknown Traffic (Multicast Groups) for which there are no members registered in the device in a VLAN

If GMRP is disabled, GMRP packets received will be forwarded like any other traffic. Otherwise, GMRP packets will be processed and not forwarded.

Establishing Membership with GMRP

The following example illustrates how a network of hosts and switches can dynamically join two multicast groups using GMRP.

In this scenario, there are two multicast sources, S1 and S2, multicasting to Multicast Groups 1 and 2, respectively. A network of five switches, including one core switch (B), connects the sources to two hosts, H1 and H2, which receive the multicast streams from S1 and S2, respectively.



① Multicast Source
② Switch
③ Multicast Host

Figure 7.29 Example – Establishing Membership with GMRP

The hosts and switches establish membership with the Multicast Group 1 and 2 as follows:

1. Host H1 is GMRP unaware, but needs to see traffic for Multicast Group 1. Therefore, Port E2 on Switch E is statically configured to forward traffic for Multicast Group 1.
2. Switch E advertises membership in Multicast Group 1 to the network through Port E1, making Port B4 on Switch B a member of Multicast Group 1.
3. Switch B propagates the *join* message, causing Ports A1, C1 and D1 to become members of Multicast Group 1.
4. Host H2 is GMRP-aware and sends a *join* request for Multicast Group 2 to Port C2, which thereby becomes a member of Multicast Group 2.

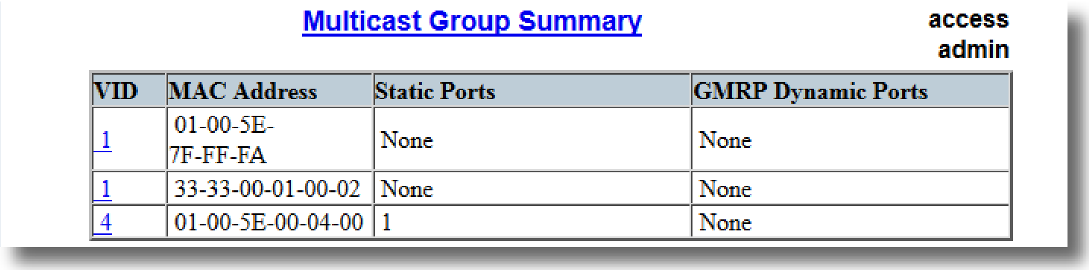
5. Switch C propagates the *join* message, causing Ports A1, B2, D1 and E1 to become members of Multicast Group 2.

Once GMRP-based registration has propagated through the network, multicast traffic from S1 and S2 can reach its destination as follows:

- Source S1 transmits multicast traffic to Port D2 which is forwarded via Port D1, which has previously become a member of Multicast Group 1.
- Switch B forwards the Group 1 multicast via Port B4 towards Switch E.
- Switch E forwards the Group 1 multicast via Port E2, which has been statically configured for membership in Multicast Group 1.
- Host H1, connected to Port E2, thus receives the Group 1 multicast.
- Source S2 transmits multicast traffic to Port A2, which is then forwarded via port A1, which has previously become a member of Multicast Group 2.
- Switch B forwards the Group 2 multicast via Port B2 towards Switch C.
- Switch C forwards the Group 2 multicast via Port C2, which has previously become a member of Group 2.
- Ultimately, Host H2, connected to Port C2, receives the Group 2 multicast.

7.3.2.2 Viewing a Summary of Multicast Groups

To view a summary of all multicast groups, navigate to ***Multicast Filtering » View Multicast Group Summary***. The **Multicast Group Summary** table appears.



Multicast Group Summary

access
admin

VID	MAC Address	Static Ports	GMRP Dynamic Ports
1	01-00-5E-7F-FF-FA	None	None
1	33-33-00-01-00-02	None	None
4	01-00-5E-00-04-00	1	None

Figure 7.30 Multicast Group Summary Table

This table provides the following information:

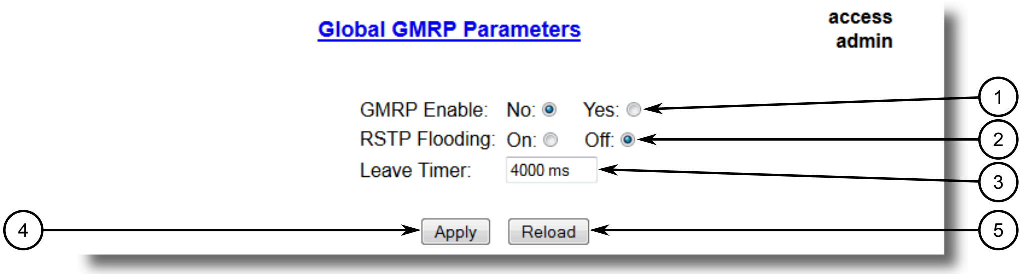
Parameter	Description
`VID`	**Synopsis:** An integer between 0 and 65535 VLAN Identifier of the VLAN upon which the multicast group operates.
`MAC Address`	**Synopsis:** ##-##-##-##-##-## where ## ranges 0 to FF Multicast group MAC address.

Parameter	Description
Static Ports	**Synopsis:** Any combination of numbers valid for this parameter Ports that joined this group statically through static configuration in Static MAC Table and to which the multicast group traffic is forwarded.
GMRP Dynamic Ports	**Synopsis:** Any combination of numbers valid for this parameter Ports that joined this group dynamically through GMRP Application and to which the multicast group traffic is forwarded.

7.3.2.3 Configuring GMRP Globally

To configure global settings for GMRP, do the following:

1. Navigate to ***Multicast Filtering » Configure Global GMRP Parameters***. The **Global GMRP Parameters** form appears.



GMRP Enable: No: ● Yes: ○
RSTP Flooding: On: ○ Off: ●
Leave Timer: 4000 ms

① GMRP Enable Options
② RSTP Flooding Options
③ Leave Timer Box
④ Apply Button
⑤ Reload Button

Figure 7.31 Global GMRP Parameters Form

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

Parameter	Description
GMRP Enable	**Synopsis:** [No | Yes] **Default:** No Globally enable or disable GMRP. When GMRP is globally disabled, GMRP configurations on individual ports are ignored. When GMRP is globally enabled, each port can be individually configured.
RSTP Flooding	**Synopsis:** [On | Off] **Default:** Off This parameter specifies whether multicast streams will be flooded out of all RSTP non-edge ports upon topology change

Parameter	Description
	detection. Such flooding is desirable, if guaranteed multicast stream delivery after topology change is most important.
`Leave Timer`	**Synopsis:** An integer between 600 and 300000 **Default:** 4000 Time (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.

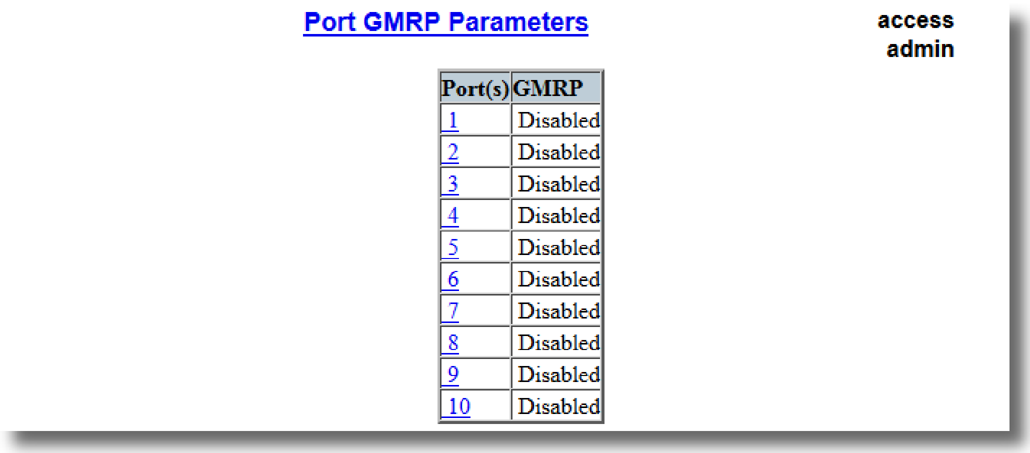
3. Click **Apply**.

7.3.2.4 Configuring GMRP for Specific Ethernet Ports

To configure GMRP for a specific Ethernet port, do the following:

1. Make sure the global settings for GMRP have been configured. For more information, refer to "Configuring GMRP Globally (Page 179)".

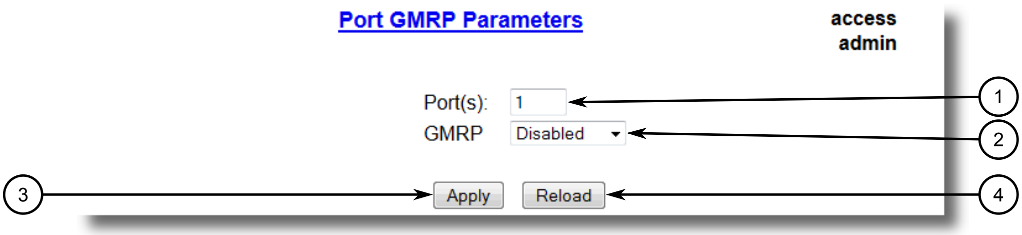
2. Navigate to ***Multicast Filtering » Configure Port GMRP Parameters***. The **Port GMRP Parameters** table appears.



Port(s)	GMRP
1	Disabled
2	Disabled
3	Disabled
4	Disabled
5	Disabled
6	Disabled
7	Disabled
8	Disabled
9	Disabled
10	Disabled

Figure 7.32 Port GMRP Parameters Table

3. Select an Ethernet port. The **Port GMRP Parameters** form appears.



Port GMRP Parameters

access
admin

Port(s): 1
GMRP Disabled

① Port(s) Box
② GMRP List
③ Apply Button
④ Reload Button

Figure 7.33 Port GMRP Parameters Form

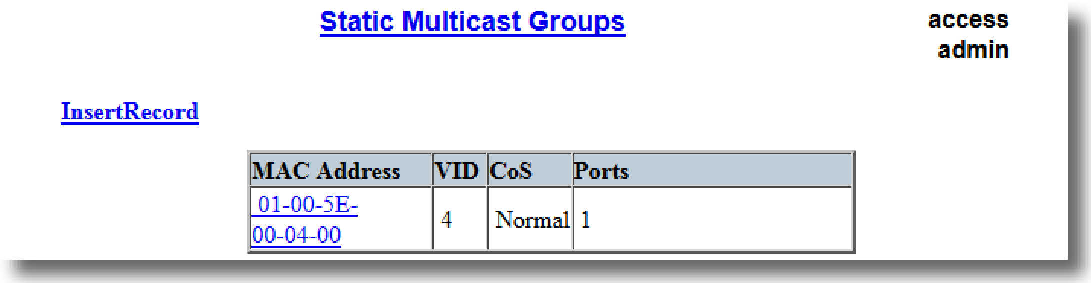
4. Configure the following parameter(s) as required:

Parameter	Description
`Port(s)`	**Synopsis:** Any combination of numbers valid for this parameter The port number as seen on the front plate silkscreen of the switch (or a list of ports, if aggregated in a port trunk).
`GMRP`	**Synopsis:** [Disabled | Adv Only | Adv&Learn] **Default:** Disabled Configures 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. • Adv Only – the port will declare all MCAST addresses existing in the switch (configured or learned) but will not learn any MCAST addresses. • Adv&Learn – the port will declare all MCAST Addresses existing in the switch (configured or learned) and can dynamically learn MCAST addresses.

5. Click **Apply**.

7.3.2.5 Viewing a List of Static Multicast Groups

To view a list of static multicast groups, navigate to ***Multicast Filtering » Configure Static Multicast Groups***. The **Static Multicast Groups** table appears.



MAC Address	VID	CoS	Ports
01-00-5E-00-04-00	4	Normal	1

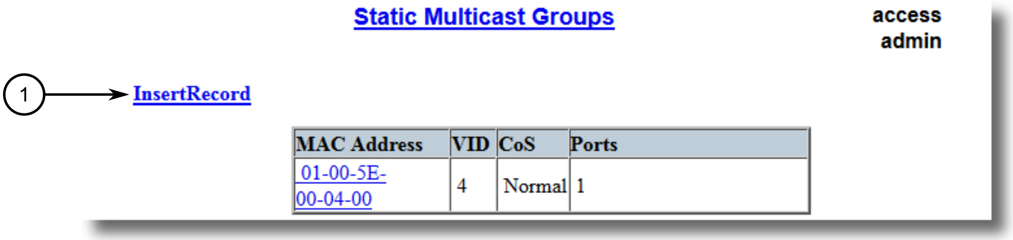
Figure 7.34 Static Multicast Groups Table

If a static multicast group is not listed, add the group. For more information, refer to "Adding a Static Multicast Group (Page 182)".

7.3.2.6 Adding a Static Multicast Group

To add a static multicast group from another device, do the following:

1. Navigate to ***Multicast Filtering » Configure Static Multicast Groups***. The **Static Multicast Groups** table appears.

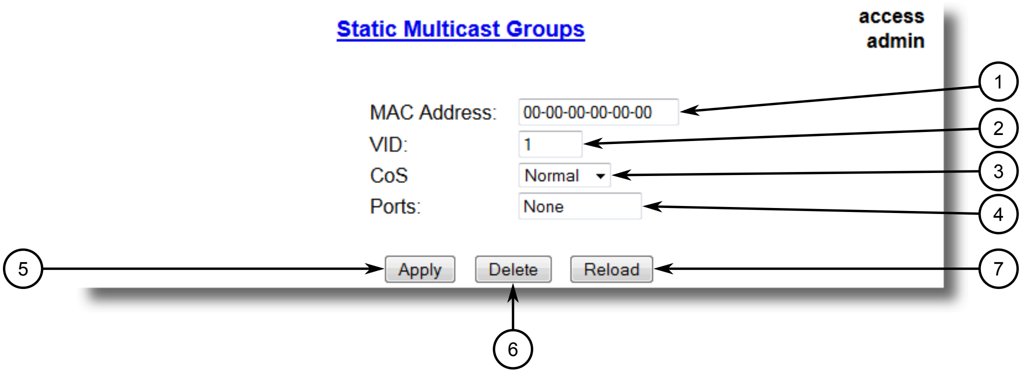


MAC Address	VID	CoS	Ports
01-00-5E-00-04-00	4	Normal	1

① InsertRecord

Figure 7.35 Static Multicast Groups Table

2. Click **InsertRecord**. The **Static Multicast Groups** form appears.



Static Multicast Groups

access
admin

MAC Address: 00-00-00-00-00-00

VID: 1

CoS: Normal

Ports: None

① MAC Address Box
② VID Box
③ CoS List
④ Ports Box
⑤ Apply Button
⑥ Delete Button
⑦ Reload Button

Figure 7.36 Static Multicast Groups Form

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

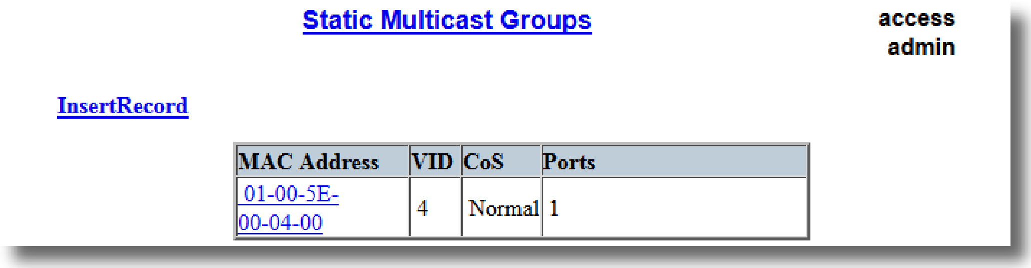
Parameter	Description
`MAC Address`	**Synopsis:** ##-##-##-##-##-## where ## ranges 0 to FF **Default:** 00-00-00-00-00-00 Multicast group MAC address.
`VID`	**Synopsis:** An integer between 1 and 4094 **Default:** 1 VLAN Identifier of the VLAN upon which the multicast group operates.
`CoS`	**Synopsis:** [N/A | Normal | Medium | High | Crit] **Default:** N/A Prioritizes traffic for the specified MAC address. To not prioritize traffic based on the address, select N/A.
`Ports`	**Synopsis:** Any combination of numbers valid for this parameter **Default:** None Ports to which the multicast group traffic is forwarded.

4. Click **Apply**.

7.3.2.7 Deleting a Static Multicast Group

To delete a static multicast group, do the following:

1. Navigate to ***Multicast Filtering » Configure Static Multicast Groups***. The **Static Multicast Groups** table appears.



Static Multicast Groups

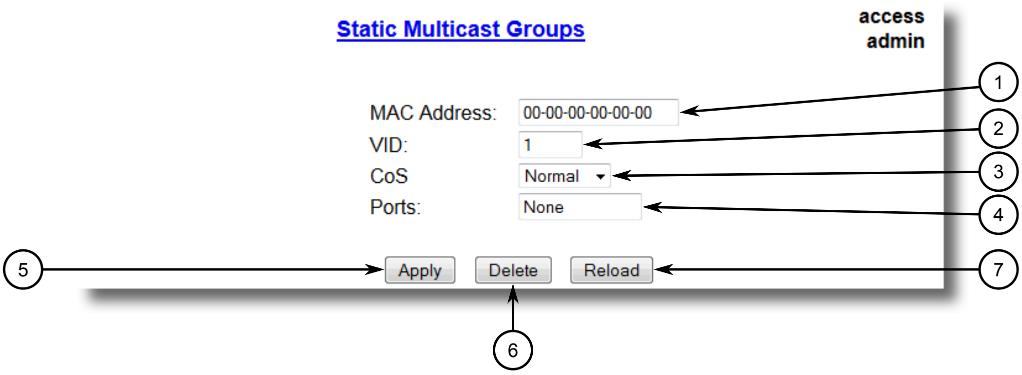
access
admin

InsertRecord

MAC Address	VID	CoS	Ports
01-00-5E-00-04-00	4	Normal	1

Figure 7.37 Static Multicast Groups Table

2. Select the group from the table. The **Static Multicast Groups** form appears.



Static Multicast Groups

access
admin

MAC Address:	00-00-00-00-00-00
VID:	1
CoS	Normal
Ports:	None

① MAC Address Box
② VID Box
③ Priority Box
④ Ports Box
⑤ Apply Button
⑥ Delete Button
⑦ Reload Button

Figure 7.38 Static Multicast Groups Form

3. Click **Delete**.

8 Redundancy

This chapter describes how to configure and manage the redundancy-related features of RUGGEDCOM ROS.

8.1 Managing Spanning Tree Protocol

This section describes how to manage the spanning tree protocol.

8.1.1 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.

A revised and highly optimized RSTP version was defined in the IEEE standard 802.1D-2004 edition. IEEE 802.1D-2004 RSTP reduces network recovery times to just milliseconds and optimizes RSTP operation for various scenarios.

RUGGEDCOM ROS supports IEEE 802.1D-2004 RSTP.

8.1.1.1 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 to determine its role in the network. When it is determined that the port will play an active part in the network, the state will change to learning.

The learning state is entered when the port is preparing to play an active part in the network. The port learns addresses in this state but does not participate in frame transfer. In a network of RSTP bridges, the time spent in this state is usually quite short. RSTP bridges operating in STP compatibility mode will spend six to 40 seconds in this state.

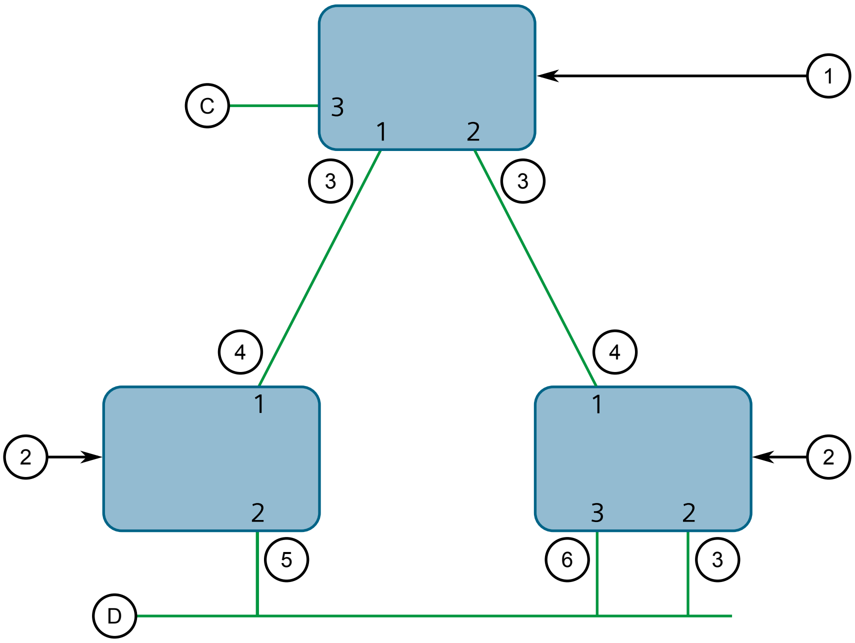
After *learning*, the bridge will place the port in the forwarding state. The port both learns addresses and participates in frame transfer while in this state.

> ⚠ **NOTICE**
>
> RUGGEDCOM ROS introduces two more states - Disabled and Link Down. Introduced purely for purposes of management, these states may be considered subclasses of the RSTP Discarding state. 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 others' messages and agree on which bridge is the Designated Bridge. The ports of other bridges on the segment must become either Root, Alternate or Backup ports.



- ① Root Bridge
- ② Designated Bridge
- ③ Designated Port
- ④ Root Port
- ⑤ Alternate Port
- ⑥ Backup Port

Figure 8.1 Bridge and Port Roles

A port is alternate when it receives a better message from another bridge on the LAN segment it is connected to. The message that an Alternate Port receives is better than the port itself would generate, but not good enough to convince it to become the Root Port. The port becomes the alternate to the current Root Port and will become the new Root Port should the current Root Port fail. The Alternate Port does not participate in the network.

A port is a Backup Port when it receives a better message from the LAN segment it is connected to, originating from another port on the same bridge. The port is a backup for another port on the bridge and will become active if that port fails. The Backup Port does not participate in the network.

8.1.1.2 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.

8.1.1.3 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.

8.1.1.4 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 IEEE 802.1D-1998 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 gigabits per second.

To remedy this problem in future applications, the IEEE 802.1w specification limits port costs to values of 1 to 20000000, and a link speed up to 10 Tb per second can be represented with a value of 2.

RUGGEDCOM bridges support interoperability with legacy STP bridges by selecting the style to use. In practice, it makes no difference which style is used as long as it is applied consistently across the network, or if costs are manually assigned.

8.1.1.5 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. To achieve extended ring sizes, Siemens 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.

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.

⚠ **NOTICE**

Raise the value of the maximum age parameter if implementing very large bridged networks or rings.

8.1.1.6 eRSTP

Siemens's enhanced Rapid Spanning Tree Protocol (eRSTP) improves the performance of RSTP in two ways:

- Improves the fault recovery time performance (< 5 ms per hop)
- Improves performance for large ring network topologies (up to 160 switches)

eRSTP is also compatible with standard RSTP for interoperability with commercial switches.

8.1.1.7 Fast Root Failover

Siemens’s *Fast Root Failover* feature is an enhancement to RSTP that may be enabled or disabled. Fast Root Failover improves upon RSTP’s handling of root bridge failures in mesh-connected networks.

⚠ **NOTICE**

In networks mixing RUGGEDCOM and non-RUGGEDCOM switches, or in those mixing Fast Root Failover algorithms, RSTP Fast Root Failover will not function properly and root bridge failure will result in an unpredictable failover time. To avoid potential issues, note the following:

- When using the Robust algorithm, all switches must be RUGGEDCOM switches
- When using the Relaxed algorithm, all switches must be RUGGEDCOM switches, with the exception of the root switch
- All RUGGEDCOM switches in the network must use the same Fast Root Failover algorithm

Two Fast Root Failover algorithms are available:

- **Robust** – Guarantees a deterministic root failover time, but requires support from all switches in the network, including the root switch
- **Relaxed** – Ensures a deterministic root failover time in most network configurations, but allows the use of a standard bridge in the root role

Note

The minimum interval for root failures is one second. Multiple, near simultaneous root failures (within less than one second of each other) are not supported by Fast Root Failover.

Fast Root Failover and RSTP Performance

- Running RSTP with Fast Root Failover disabled has no impact on RSTP performance in ring-connected networks.
- Fast Root Failover has no effect on RSTP performance in the case of failures that do not involve the root bridge or one of its links.
- The extra processing introduced by Fast Root Failover significantly decreases the worst-case failover time due to root bridge failure in mesh networks.

Recommendations On the Use of Fast Root Failover

- It is not recommended to enable Fast Root Failover in single ring network topologies.
- It is strongly recommended to always connect the root bridge to each of its neighbor bridges using more than one link when enabled in ring-connected networks.

8.1.2 RSTP Applications

This section describes various applications of RSTP.

8.1.2.1 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 8.2, “Example - Structured Wiring Configuration” would leave all the ports of bridges 555 through 888 connected to the network.

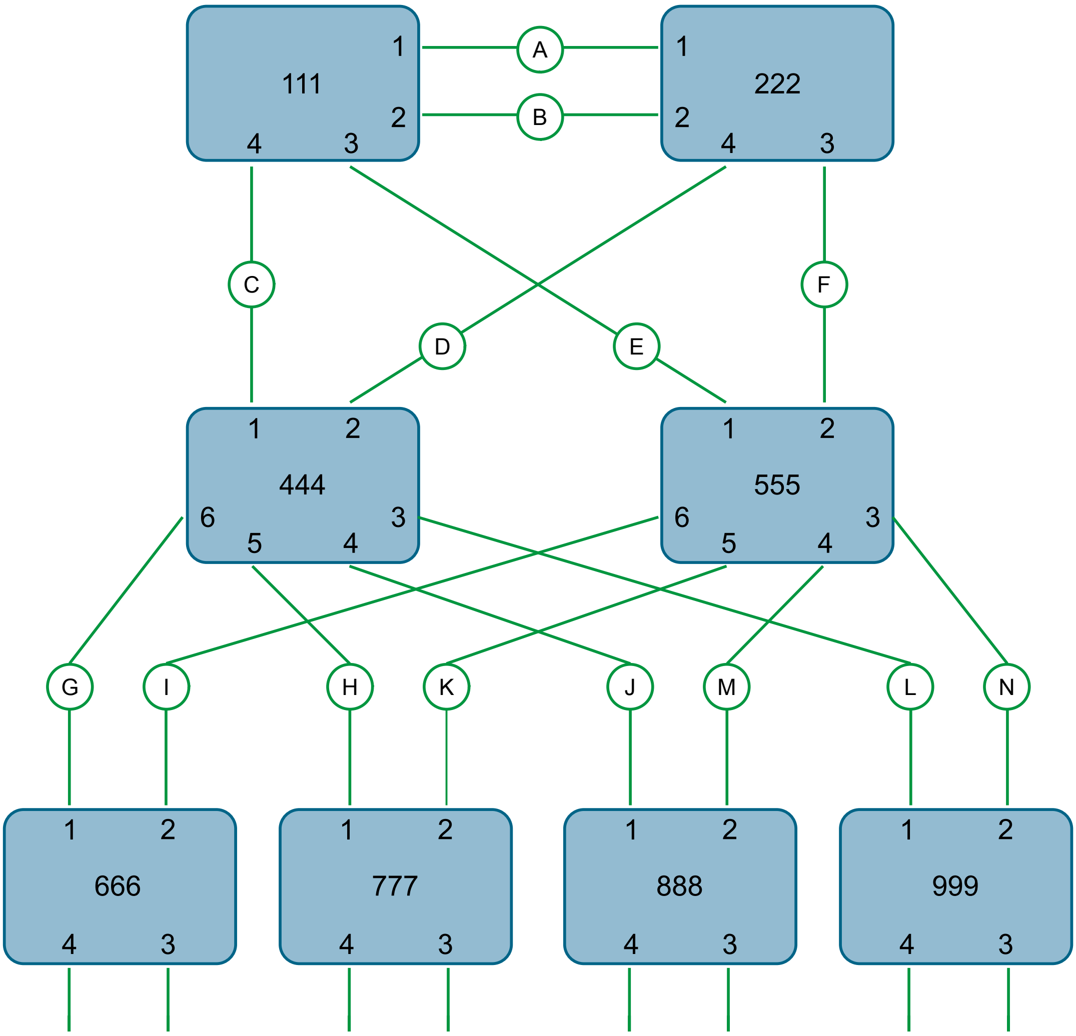


Figure 8.2 Example - Structured Wiring Configuration

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, Intelligent Electronic Devices (IEDs) and controllers may be set to edge ports 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 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.**

8.1.2.2 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 8.3, “Example - Ring Backbone Configuration”. 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.

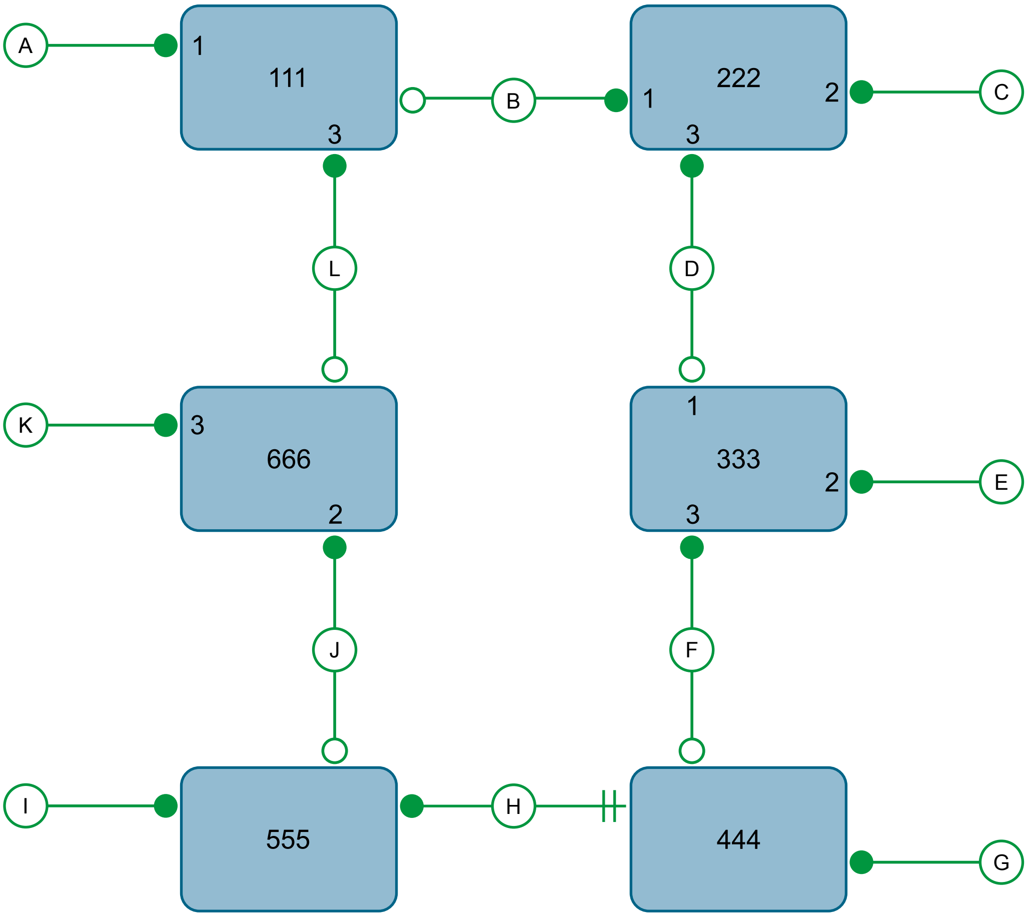


Figure 8.3 Example - Ring Backbone Configuration

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, Intelligent Electronic Devices (IEDs) and controllers may be set to edge ports 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.**

   The strategy that should be used is to assign each bridge's priority to correspond to its distance from the root bridge. If the root bridge is assigned the lowest priority of 0, the bridges on either side should use a priority of 4096 and the next bridges 8192 and so on. As there are 16 levels of bridge priority available, this method provides for up to 31 bridges in the ring.

6. **Decide upon a port cost calculation strategy.**

   It is recommended to use the auto-negotiated cost style, unless it is necessary for the network design to change the auto-negotiated cost style. Select whether the STP or RSTP cost style should be used. Make sure to configure the same cost style on all devices on the network.

7. **Disable RSTP Fast Root Failover option.**

   This is a proprietary feature of Siemens . In RUGGEDCOM ROS, 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.**

8.1.2.3 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.

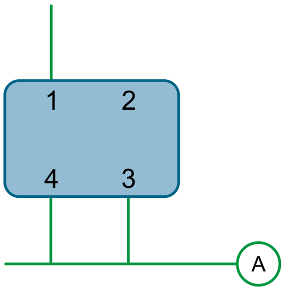


Figure 8.4 Example - Port Redundancy

8.1.3 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 another of several spanning trees by mapping one or more VLANs onto the network.

The sophistication and utility of the Multiple Spanning Tree 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, but at best, 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 that 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 that MSTP will likely be significantly slower than RSTP. Therefore, for mission critical applications, RSTP should be considered a better network redundancy solution than MSTP.

8.1.3.1 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; the internal detail of the MST region is 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 that 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 – see below). An MSTI is created by mapping a set of VLANs (in RUGGEDCOM ROS, via the VLAN configuration) to a given MSTI ID. The same mapping must be configured on all bridges that are intended to be part of the MSTI. Moreover, all VLAN to MSTI mappings must be identical for all bridges in an MST region.

RUGGEDCOM ROS supports 16 MSTIs in addition to the IST.

Each MSTI has a topology that is independent of every other. 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 (see below), which spans the entire bridged network, inside and outside of the MST region and all other RSTP and STP bridges, as well as any other MST regions.

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.

8.1.3.2 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

Role	Description
	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).

Role	Description
	- A CIST Designated Port, CIST Alternate/Backup Port, or Disabled. At the MSTP region boundary, the MSTI Port Role is the same as the CIST Port Role. A Boundary Port connected to an STP bridge will send only STP BPDUs. One connected to an RSTP bridge need not refrain from sending MSTP BPDUs. This is made possible by the fact that the MSTP carries the CIST Regional Root Identifier in the field that RSTP parses as the Designated Bridge Identifier.

8.1.3.3 Benefits of MSTP

Despite the fact that MSTP is configured by default to arrive automatically at a spanning tree solution for each configured MSTI, advantages may be gained from influencing the topology of MSTIs in an MST region. The fact that the Bridge Priority and each port cost are configurable per MST makes it possible to control the topology of each MSTI within a region.

Load Balancing

MSTP can be used to balance data traffic load among sets of VLANs, enabling more complete utilization of a multiply interconnected bridged network.

A bridged network controlled by a single spanning tree will block redundant links by design, to avoid harmful loops. Using MSTP, however, 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, using a single spanning tree, would have gone unused, 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 vs. 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.

8.1.3.4 Implementing MSTP on a Bridged Network

It is recommended the configuration of MSTP on a network proceed in the sequence outlined below.

Naturally, it is also recommended that network analysis and planning inform the steps of configuring the VLAN and MSTP parameters in particular.

Begin with a set of MSTP-capable Ethernet bridges and MSTP disabled. For each bridge in the 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. Configure and enable STP globally and/or for specific Ethernet ports. For more information, refer to "Configuring STP Globally (Page 201)" or "Configuring STP for Specific Ethernet Ports (Page 203)".

   Note
   Static VLANs must be used in an MSTP configuration. GVRP is not supported.

2. Add static VLANs and map them to MSTIs. For more information, refer to "Adding a Static VLAN (Page 156)".

   Note
   The Region Identifier and Revision Level must be the same for each bridge in the MST region.

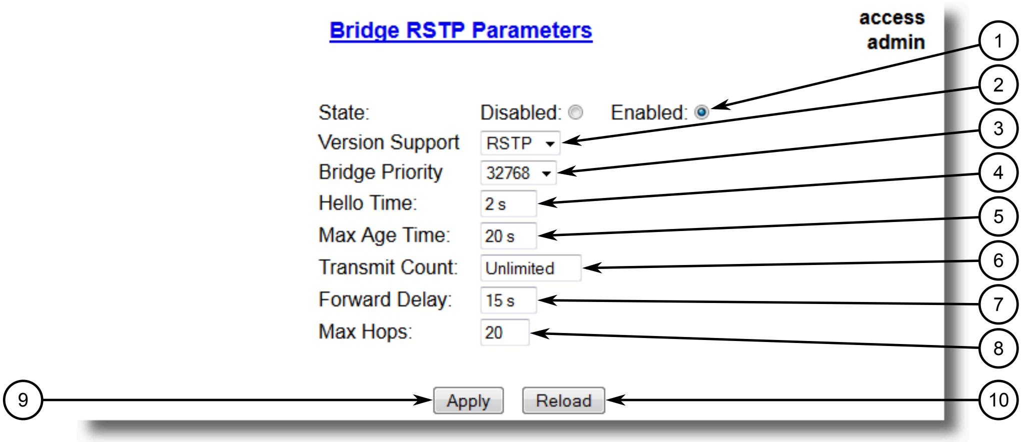
3. Configure the revision level for the MST Region Identifier. For more information, refer to "Configuring the MST Region Identifier (Page 216)".
4. Make sure the read-only digest for the MST Region Identifier is identical for each bridge in the MST region. If the digest is different, the set of mappings from VLANs to MSTIs differs.
5. Configure the Bridge Priority for the global MSTI. For more information, refer to "Configuring a Global MSTI (Page 218)".
6. Configure the Port Cost and Priority per Port for each MSTI. For more information, refer to "Configuring an MSTI for an Ethernet Port (Page 219)".

7. Set the STP Protocol Version to MSTP and enable STP. For more information, refer to "Configuring STP Globally (Page 201)"

8.1.4 Configuring STP Globally

To configure global settings for the Spanning Tree Protocol (STP), do the following:

1. Navigate to ***Spanning Tree » Configure Bridge RSTP Parameters***. The **Bridge RSTP Parameters** form appears.



Bridge RSTP Parameters

access
admin

State: Disabled: ○ Enabled: ●
Version Support: RSTP
Bridge Priority: 32768
Hello Time: 2 s
Max Age Time: 20 s
Transmit Count: Unlimited
Forward Delay: 15 s
Max Hops: 20

① State Options
② Version Support List
③ Bridge Priority List
④ Hello Time Box
⑤ Max Age Time Box
⑥ Transmit Count Box
⑦ Forward Delay Box
⑧ Max Hops Box
⑨ Apply Button
⑩ Reload Button

Figure 8.5 Bridge RSTP Parameters Form

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

Parameter	Description
`State`	**Synopsis:** [Disabled | Enabled] **Default:** Enabled Enable 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 Support`	**Synopsis:** [STP | RSTP | MSTP] **Default:** RSTP Selects the version of Spanning Tree Protocol to support, either only STP or Rapid STP or Multiple STP.

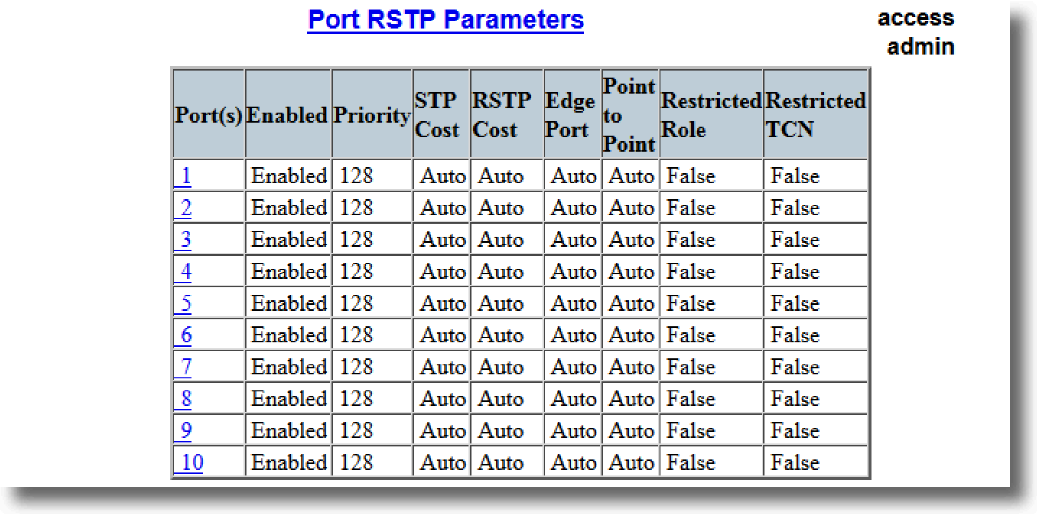
Parameter	Description
`Bridge Priority`	**Synopsis:** [0 | 4096 | 8192 | 12288 | 16384 | 20480 | 24576 | 28672 | 32768 | 36864 | 40960 | 45056 | 49152 | 53248 | 57344 | 61440] **Default:** 32768 Bridge Priority provides a way to control the topology of the STP connected network. The desired Root and Designated bridges can be configured for a particular topology. The bridge with the lowest priority will become root. In the event of a failure of the root bridge, the bridge with the next lowest priority will then become root. Designated bridges that (for redundancy purposes) service a common 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.
`Hello Time`	**Synopsis:** An integer between 1 and 10 **Default:** 2 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.
`Max Age Time`	**Synopsis:** An integer between 6 and 40 **Default:** 20 The time for which a configuration message remains valid after being issued by the root bridge. Configure this parameter with care when many tiers of bridges exist, or slow speed links (such as those used in WANs) are part of the network
`Transmit Count`	**Synopsis:** An integer between 3 and 100 or [Unlimited] **Default:** Unlimited Maximum number of BPDUs on each port that may be sent in one second. Larger values allow the network to recover from failed links/bridges more quickly.
`Forward Delay`	**Synopsis:** An integer between 4 and 30 **Default:** 15 The amount of time a bridge spends learning MAC addresses on a rising port before beginning to forward traffic. Lower values allow the port to reach the forwarding state more quickly, but at the expense of flooding unlearned addresses to all ports.
`Max Hops`	**Synopsis:** An integer between 6 and 40 **Default:** 20 Only applicable to MSTP. The maximum possible bridge diameter inside an MST region. MSTP BPDUs propagating inside an MST region specify a time-to-live that is decremented by every switch that propagates the BPDU. If the maximum number of hops inside the region exceeds the configured maximum, BPDUs may be discarded due to their time-to-live setting.

3. Click **Apply**.

8.1.5 Configuring STP for Specific Ethernet Ports

To configure the Spanning Tree Protocol (STP) for a specific Ethernet port, do the following:

1. Navigate to ***Spanning Tree » Configure Port RSTP Parameters***. The **Port RSTP Parameters** table appears.



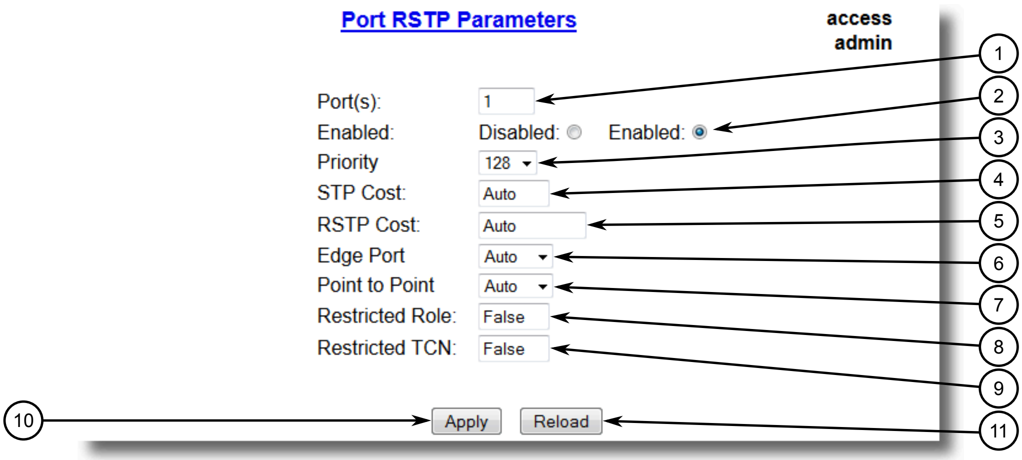
Port RSTP Parameters

access
admin

Port(s)	Enabled	Priority	STP Cost	RSTP Cost	Edge Port	Point to Point	Restricted Role	Restricted TCN
1	Enabled	128	Auto	Auto	Auto	Auto	False	False
2	Enabled	128	Auto	Auto	Auto	Auto	False	False
3	Enabled	128	Auto	Auto	Auto	Auto	False	False
4	Enabled	128	Auto	Auto	Auto	Auto	False	False
5	Enabled	128	Auto	Auto	Auto	Auto	False	False
6	Enabled	128	Auto	Auto	Auto	Auto	False	False
7	Enabled	128	Auto	Auto	Auto	Auto	False	False
8	Enabled	128	Auto	Auto	Auto	Auto	False	False
9	Enabled	128	Auto	Auto	Auto	Auto	False	False
10	Enabled	128	Auto	Auto	Auto	Auto	False	False

Figure 8.6 Port RSTP Parameters Table

2. Select an Ethernet port. The **Port RSTP Parameters** form appears.



Port RSTP Parameters

access admin

Port(s):	1
Enabled:	Disabled: ○ Enabled: ●
Priority	128
STP Cost:	Auto
RSTP Cost:	Auto
Edge Port	Auto
Point to Point	Auto
Restricted Role:	False
Restricted TCN:	False

① Port(s) Box
② Enabled Options
③ Priority List
④ STP Cost Box
⑤ RSTP Cost Box
⑥ Edge Port List
⑦ Point to Point List
⑧ Restricted Role Box
⑨ Restricted TCN Box
⑩ Apply Button
⑪ Reload Button

Figure 8.7 Port RSTP Parameters Form

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

Parameter	Description
`Port(s)`	**Synopsis:** Any combination of numbers valid for this parameter The port number as seen on the front plate silkscreen of the switch (or a list of ports, if aggregated in a port trunk).
`Enabled`	**Synopsis:** [Disabled | Enabled] **Default:** Enabled Enabling STP activates the STP or RSTP protocol for this port per the configuration in the STP Configuration menu. STP may be disabled for the port ONLY if the port does not attach to an STP enabled bridge in any way. Failure to meet this requirement WILL result in an undetectable traffic loop in the network. A better alternative to disabling the port is to leave STP enabled but to configure the port as an edge port. A good candidate for disabling STP would be a port that services only a single host computer.

Parameter	Description
`Priority`	**Synopsis:** [0 | 16 | 32 | 48 | 64 | 80 | 96 | 112 | 128 | 144 | 160 | 176 | 194 | 208 | 224 | 240] **Default:** 128 Selects the STP port priority. Ports of the same cost that attach to a common LAN will select the port to be used based upon the port priority.
`STP Cost`	**Synopsis:** An integer between 0 and 65535 or [Auto] **Default:** Auto Selects 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 (4 for 1Gbps, 19 for 100 Mbps links and 100 for 10 Mbps links). For MSTP, this parameter applies to both external and internal path cost.
`RSTP Cost`	**Synopsis:** An integer between 0 and 2147483647 or [Auto] **Default:** Auto Selects 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 cost.
`Edge Port`	**Synopsis:** [False | True | 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).
`Point to Point`	**Synopsis:** [False | True | Auto] **Default:** Auto RSTP uses a peer-to-peer protocol that provides 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.

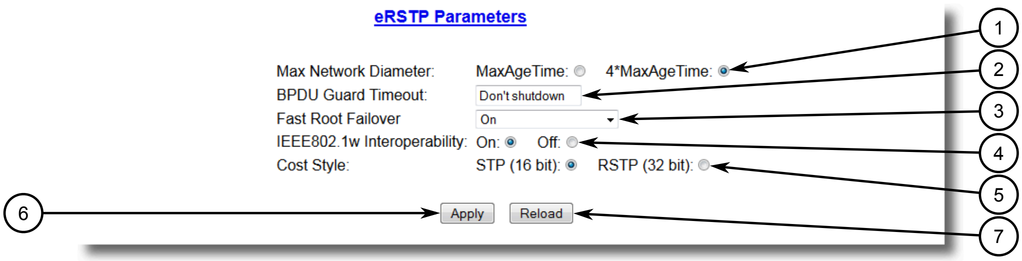
Parameter	Description
	Force the parameter false when the port operates the link in full-duplex mode, but is still not point-to-point (e.g. a full-duplex link to an unmanaged bridge that concentrates two other STP bridges).
`Restricted Role`	**Synopsis:** [True | False] **Default:** False A boolean value set by management. If TRUE, causes the Port not to be selected as the Root Port for the CIST or any MSTI, even if it has the best spanning tree priority vector. Such a Port will be selected as an Alternate Port after the Root Port has been selected. This parameter should be FALSE by default. If set, it can cause a lack of spanning tree connectivity. It is set by a network administrator to prevent bridges that are external to a core region of the network from influencing the spanning tree active topology. This may be necessary, for example, if those bridges are not under the full control of the administrator.
`Restricted TCN`	**Synopsis:** [True | False] **Default:** False A boolean value set by management. If TRUE, it causes the Port not to propagate received topology change notifications and topology changes to other Ports. 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. It is set by a network administrator to prevent bridges that are external to a core region of the network from causing address flushing in that region. This may be necessary, for example, if those bridges are not under the full control of the administrator or if the MAC_Operational status parameter for the attached LANs transitions frequently.

4. Click **Apply**.

8.1.6 Configuring eRSTP

To configure eRSTP, do the following:

1. Navigate to ***Spanning Tree » Configure eRSTP Parameters***. The **eRSTP Parameters** form appears.



eRSTP Parameters

Max Network Diameter: MaxAgeTime: ○ 4*MaxAgeTime: ●
BPDU Guard Timeout: Don't shutdown
Fast Root Failover: On
IEEE802.1w Interoperability: On: ● Off: ○
Cost Style: STP (16 bit): ● RSTP (32 bit): ○

① Max Network Diameter Options
② BPDU Guart Timeout Box
③ Fast Root Failover List
④ IEEE802.1w Interoperability Options
⑤ Cost Style Options
⑥ Apply Button
⑦ Reload Button

Figure 8.8 eRSTP Parameters Form

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

Parameter	Description
`Max Network Diameter`	**Synopsis:** [MaxAgeTime | 4*MaxAgeTime] **Default:** 4*MaxAgeTime The RSTP standard puts a limit on the maximum network size that can be controlled by the RSTP protocol. The network size is described by the term 'maximum network diameter', which is the number of switches that comprise the longest path that RSTP BPDUs have to traverse. The standard supported maximum network diameter is equal to the value of the 'MaxAgeTime' RSTP configuration parameter. eRSTP offers an enhancement to RSTP which allows it to cover networks larger than ones defined by the standard. This configuration parameter selects the maximum supported network size.
`BPDU Guard Timeout`	**Synopsis:** An integer between 1 and 86400 or [Until reset | Don't shutdown] **Default:** Don't shutdown The RSTP standard does not address network security. RSTP must process every received BPDU and take an appropriate action. This opens a way for an attacker to influence RSTP topology by injecting RSTP BPDUs into the network. BPDU Guard is a feature that protects the network from BPDUs received by a port where RSTP capable devices are not expected to be attached. If a BPDU is received by a port for which 'Edge'

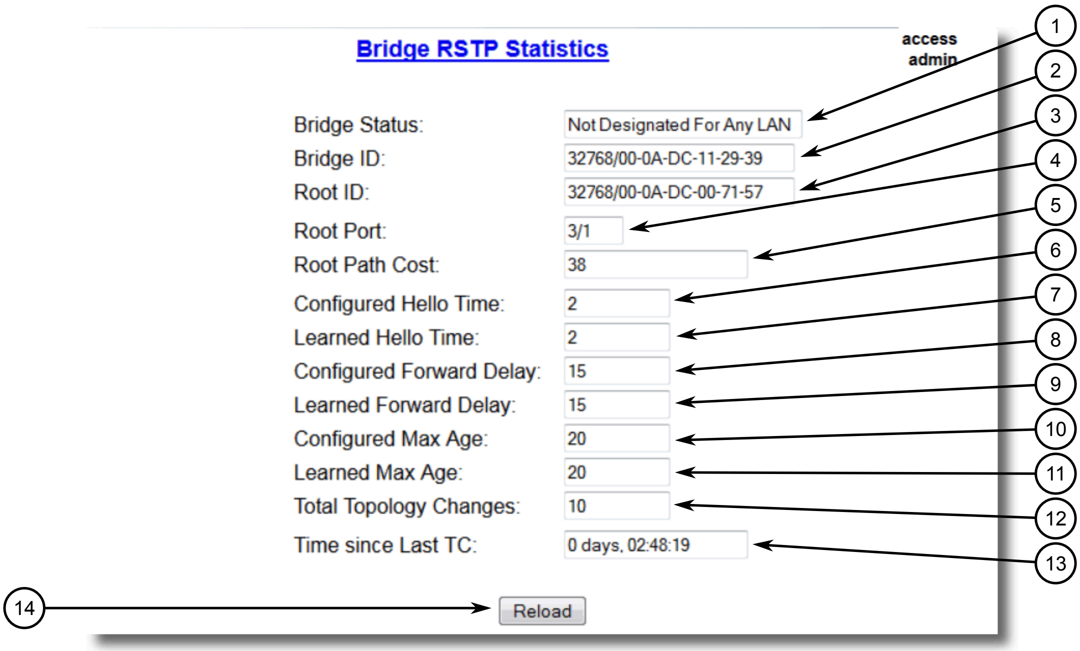
Parameter	Description
	parameter is set to 'TRUE' or RSTP is disabled, the port will be shutdown for the time period specified by this parameter. • Don't shutdown – BPDU Guard is disabled • Until reset – port will remain shutdown until the port reset command is issued by the user
`Fast Root Failover`	**Synopsis:** [On | On with standard root | Off] **Default:** On 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 hard to calculate and it 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. **Note** • 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 that the root might not suport 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. These are the supported configuration options: • Off – Fast Root Failover algorithm is disabled and hence a root switch failure may result in excessive connectivity recovery time. • On – Fast Root Failover is enabled and the most robust algorithm is used, which requires the appropriate support in the root switch. • On with standard root – Fast Root Failover is enabled but a "relaxed" algorithm is used, allowing the use of a standard switch in the root role.
`IEEE802.1w Interoperability`	**Synopsis:** [On | Off] **Default:** On The original RSTP protocol defined in the IEEE 802.1w standard has minor differences from more recent, enhanced, standard(s). Those differences cause interoperability issues which, although they do not completely break RSTP operation, can lead to a longer recovery time from failures in the network.

Parameter	Description
	eRSTP offers some enhancements to the protocol which make the switch fully interoperable with other vendors' switches, which may be running IEEE 802.2w RSTP. The enhancements do not affect interoperability with more recent RSTP editions. This configuration parameter enables the aforementioned interoperability mode.
`Cost Style`	**Synopsis:** [STP (16 bit) | RSTP (32 bit)] **Default:** STP (16 bit) The RSTP standard defines two styles of a path cost value. 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). However, switches from some vendors keep using the STP path cost style even in RSTP mode, which can cause confusion and interoperability problems. This configuration parameter selects the style of link costs to employ. 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 STP.

3. Click **Apply**.

8.1.7 Viewing Global Statistics for STP

To view global statistics for STP, navigate to ***Spanning Tree » View Bridge RSTP Statistics***. The **Bridge RSTP Statistics** form appears.



Bridge RSTP Statistics

Bridge Status:	Not Designated For Any LAN
Bridge ID:	32768/00-0A-DC-11-29-39
Root ID:	32768/00-0A-DC-00-71-57
Root Port:	3/1
Root Path Cost:	38
Configured Hello Time:	2
Learned Hello Time:	2
Configured Forward Delay:	15
Learned Forward Delay:	15
Configured Max Age:	20
Learned Max Age:	20
Total Topology Changes:	10
Time since Last TC:	0 days, 02:48:19

① Bridge Status Box
② Bridge ID Box
③ Root ID Box
④ Root Port Box
⑤ Root Path Cost Box
⑥ Configure Hello Time Box
⑦ Learned Hello Time Box
⑧ Configured Forward Delay Box
⑨ Learned Forward Delay Box
⑩ Configured Max Age Box
⑪ Learned Max Age Box
⑫ Total Topology Changes Box
⑬ Time Since Last TC Box
⑭ Reload Button

Figure 8.9 Bridge RSTP Statistics Form

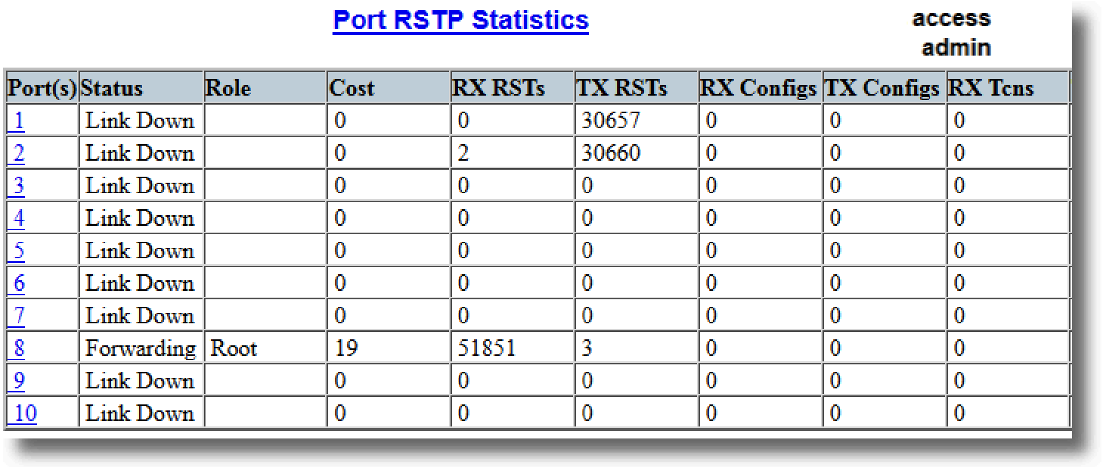
This table displays the following information:

Parameter	Description
`Bridge Status`	**Synopsis:** [Designated Bridge | Not Designated For Any LAN | Root Bridge] 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 designated for any of its ports.
`Bridge ID`	**Synopsis:** $$ / ##-##-##-##-##-## where $$ is 0 to 65535, ## is 0 to FF Bridge Identifier of this bridge.

Parameter	Description
Root ID	**Synopsis:** $$ / ##-##-##-##-##-## where $$ is 0 to 65535, ## is 0 to FF Bridge Identifier of the root bridge.
Root Port	**Synopsis:** 1 to maximum port number or [<empty string>] If the bridge is designated, this is the port that provides connectivity towards the root bridge of the network.
Root Path Cost	**Synopsis:** An integer between 0 and 4294967295 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 4, 100 Mbps ports will contribute 19 and 10 Mbps ports will contribute a cost of 100 to this figure. For the CIST instance of MSTP, this is an external root path cost, which is the cost of the path from the IST root (i.e. regional root) bridge to the CST root (i.e. network "global" root) bridge.
Configured Hello Time	**Synopsis:** An integer between 0 and 65535 The configured Hello time from the Bridge RSTP Parameters menu.
Learned Hello Time	**Synopsis:** An integer between 0 and 65535 The actual Hello time provided by the root bridge as learned in configuration messages. This time is used in designated bridges.
Configured Forward Delay	**Synopsis:** An integer between 0 and 65535 The configured Forward Delay time from the Bridge RSTP Parameters menu.
Learned Forward Delay	**Synopsis:** An integer between 0 and 65535 The actual Forward Delay time provided by the root bridge as learned in configuration messages. This time is used in designated bridges.
Configured Max Age	**Synopsis:** An integer between 0 and 65535 The configured Maximum Age time from the Bridge RSTP Parameters menu.
Learned Max Age	**Synopsis:** An integer between 0 and 65535 The actual Maximum Age time provided by the root bridge as learned in configuration messages. This time is used in designated bridges.
Total Topology Changes	**Synopsis:** An integer between 0 and 65535 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.
Time since Last TC	**Synopsis:** DDDD days, HH:MM:SS The time since the last time a topology change was detected by the bridge.

8.1.8 Viewing STP Statistics for Ethernet Ports

To view STP statistics for Ethernet ports, navigate to ***Spanning Tree » View Port RSTP Statistics***. The **Port RSTP Statistics** table appears.



Port RSTP Statistics

access
admin

Port(s)	Status	Role	Cost	RX RSTs	TX RSTs	RX Configs	TX Configs	RX Tcns
1	Link Down		0	0	30657	0	0	0
2	Link Down		0	2	30660	0	0	0
3	Link Down		0	0	0	0	0	0
4	Link Down		0	0	0	0	0	0
5	Link Down		0	0	0	0	0	0
6	Link Down		0	0	0	0	0	0
7	Link Down		0	0	0	0	0	0
8	Forwarding	Root	19	51851	3	0	0	0
9	Link Down		0	0	0	0	0	0
10	Link Down		0	0	0	0	0	0

Figure 8.10 Port RSTP Statistics Table

This table displays the following information:

Parameter	Description
`Port(s)`	**Synopsis:** Any combination of numbers valid for this parameter The port number as seen on the front plate silkscreen of the switch (or a list of ports, if aggregated in a port trunk).
`Status`	**Synopsis:** [Disabled | Listening | Learning | Forwarding | Blocking | Link Down | Discarding] Status of this port in Spanning Tree. This may be one of the following: • Disabled – 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.
`Role`	**Synopsis:** [Root | Designated | Alternate | Backup | Master] Role of this port in Spanning Tree. This may be one of the following: • Designated – The port is designated for (i.e. carries traffic towards the root for) the LAN it is connected to. • Root – The single port on the bridge, which provides connectivity towards the root bridge. • Backup – The port is attached to a LAN that is serviced by another port on the bridge. It is not used but is standing by. • Alternate – The port is attached to a bridge that provides connectivity to the root bridge. It is not used but is standing by.

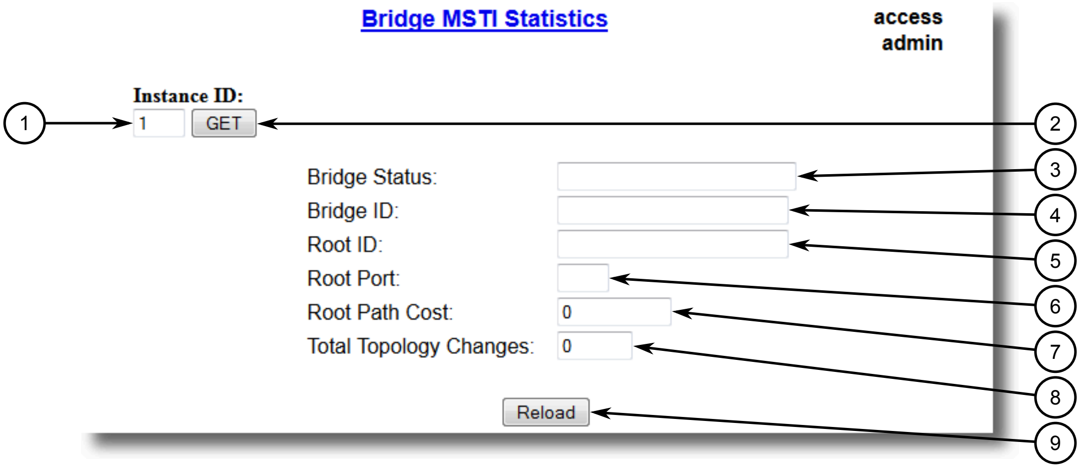
Parameter	Description
	- Master – Only exists in MSTP. The port is an MST region boundary port and the single port on the bridge, which provides connectivity for the Multiple Spanning Tree Instance towards the Common Spanning Tree root bridge (i.e. this port is the root port for the Common Spanning Tree Instance).
`Cost`	**Synopsis:** An integer between 0 and 4294967295 Cost offered by this port. If the Bridge RSTP Parameters Cost Style is set to STP, 1Gbps ports will contribute 4, 100 Mbps ports will contribute 19 and 10 Mbps ports contribute a cost of 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.
`RX RSTs`	**Synopsis:** An integer between 0 and 4294967295 The count of RSTP configuration messages received on this port.
`TX RSTs`	**Synopsis:** An integer between 0 and 4294967295 The count of RSTP configuration messages transmitted on this port.
`RX Configs`	**Synopsis:** An integer between 0 and 4294967295 The count of STP configuration messages received on this port.
`TX Configs`	**Synopsis:** An integer between 0 and 4294967295 The count of STP configuration messages transmitted on this port.
`RX Tcns`	**Synopsis:** An integer between 0 and 4294967295 The count of STP topology change notification messages received on this port. Excessively high or rapidly increasing counts signal network problems.
`TX Tcns`	**Synopsis:** An integer between 0 and 4294967295 The count of STP topology change notification messages transmitted on this port.
`Desig Bridge ID`	**Synopsis:** $$ / ##-##-##-##-##-## where $$ is 0 to 65535, ## is 0 to FF Provided on the root ports of designated bridges, the Bridge Identifier of the bridge this port is connected to.
`operEdge`	**Synopsis:** [True | False] The port is operating as an edge port or not.

8.1.9 Managing Multiple Spanning Tree Instances

This section describes how to configure and manage Multiple Spanning Tree Instances (MSTIs).

8.1.9.1 Viewing Statistics for Global MSTIs

To view statistics for global MSTIs, navigate to ***Spanning Tree » View Bridge MSTI Statistics***. The **Bridge MSTI Statistics** form appears.



Bridge MSTI Statistics

access
admin

Instance ID: 1

Bridge Status:
Bridge ID:
Root ID:
Root Port:
Root Path Cost: 0
Total Topology Changes: 0

① Instance Box
② Get Button
③ Bridge Status Box
④ Bridge ID Box
⑤ Root ID Box
⑥ Root Port Box
⑦ Root Path Cost Box
⑧ Total Topology Changes Box
⑨ Reload Button

Figure 8.11 Bridge MSTI Statistics Form

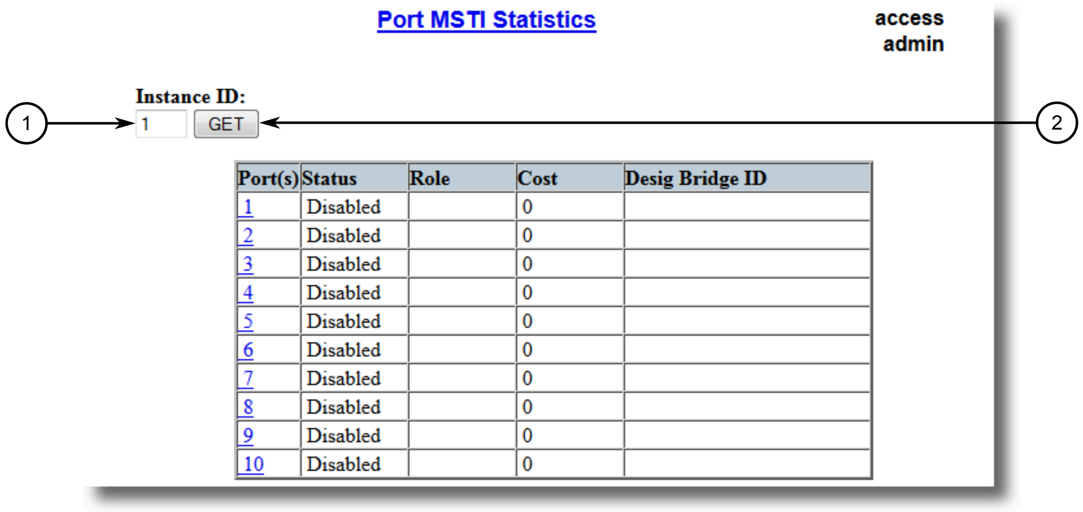
This table displays the following information:

Parameter	Description
`Bridge Status`	**Synopsis:** [Designated Bridge | Not Designated For Any LAN | Root Bridge] 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 designated for any of its ports.
`Bridge ID`	**Synopsis:** $$ / ##-##-##-##-##-## where $$ is 0 to 65535, ## is 0 to FF Bridge Identifier of this bridge.
`Root ID`	**Synopsis:** $$ / ##-##-##-##-##-## where $$ is 0 to 65535, ## is 0 to FF Bridge Identifier of the root bridge.
`Root Port`	**Synopsis:** 1 to maximum port number or [<empty string>] If the bridge is designated, this is the port that provides connectivity towards the root bridge of the network.

Parameter	Description
`Root Path Cost`	**Synopsis:** An integer between 0 and 4294967295 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 4, 100 Mbps ports will contribute 19 and 10 Mbps ports will contribute a cost of 100 to this figure. For the CIST instance of MSTP, this is an external root path cost, which is the cost of the path from the IST root (i.e. regional root) bridge to the CST root (i.e. network "global" root) bridge.
`Total Topology Changes`	**Synopsis:** An integer between 0 and 65535 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.

8.1.9.2 Viewing Statistics for Port MSTIs

To view statistics for port MSTIs, navigate to ***Spanning Tree » View Port MSTI Statistics***. The **Port MSTI Statistics** form appears.



Port(s)	Status	Role	Cost	Desig Bridge ID
1	Disabled		0	
2	Disabled		0	
3	Disabled		0	
4	Disabled		0	
5	Disabled		0	
6	Disabled		0	
7	Disabled		0	
8	Disabled		0	
9	Disabled		0	
10	Disabled		0	

① Instance ID Box
② Get Button

Figure 8.12 Port MSTI Statistics Form

This table displays the following information:

Parameter	Description
`Port(s)`	**Synopsis:** Any combination of numbers valid for this parameter The port number as seen on the front plate silkscreen of the switch (or a list of ports, if aggregated in a port trunk).

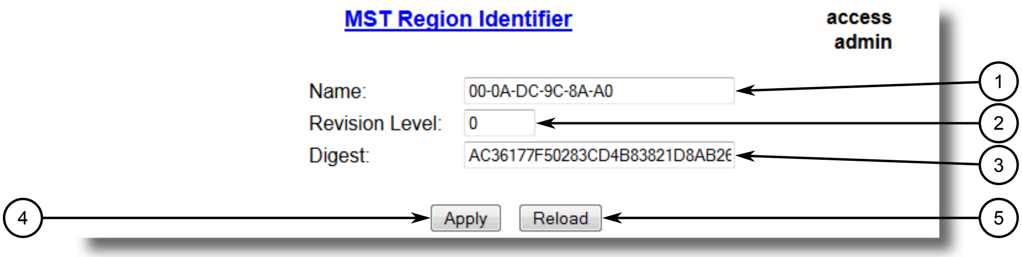
Parameter	Description
`Status`	**Synopsis:** [Disabled | Listening | Learning | Forwarding | Blocking | Link Down | Discarding] tatus of this port in Spanning Tree. This may be one of the following: • Disabled – STP is disabled on this port. • Link Down – STP is enabled on this port but the link is down. • 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.
`Role`	**Synopsis:** [Root | Designated | Alternate | Backup | Master] Role of this port in Spanning Tree. This may be one of the following: • Designated – The port is designated for (i.e. carries traffic towards the root for) the LAN it is connected to. • Root – The single port on the bridge, which provides connectivity towards the root bridge. • Backup – The port is attached to a LAN that is serviced by another port on the bridge. It is not used but is standing by. • Alternate – The port is attached to a bridge that provides connectivity to the root bridge. It is not used but is standing by. • Master – Only exists in MSTP. The port is an MST region boundary port and the single port on the bridge, which provides connectivity for the Multiple Spanning Tree Instance towards the Common Spanning Tree root bridge (i.e. this port is the root port for the Common Spanning Tree Instance).
`Cost`	**Synopsis:** An integer between 0 and 4294967295 Cost offered by this port. If the Bridge RSTP Parameters Cost Style is set to STP, 1Gbps ports will contribute 4, 100 Mbps ports will contribute 19 and 10 Mbps ports contribute a cost of 100. If the Cost Style is set to RSTP, 1Gbps will contribute 20,000, 100 Mbps ports will contribute a cost of 200,000 and 10 Mbps ports contribute a cost of 2,000,000. Note that even if the Cost style is set to RSTP, a port that migrates to STP will have its cost limited to a maximum of 65535.
`Desig Bridge ID`	**Synopsis:** $$ / ##-##-##-##-##-## where $$ is 0 to 65535, ## is 0 to FF Provided on the root ports of designated bridges, the Bridge Identifier of the bridge this port is connected to.

8.1.9.3 Configuring the MST Region Identifier

Configuring the region identifier and revision level puts the MSTP bridge in a defined group. Other bridges that have the same identifier and revision level are interconnected within this region. For more information, refer to "MSTP Regions and Interoperability (Page 196)".

To configure the Multiple Spanning Tree (MST) region identifier, do the following:

1. Navigate to ***Spanning Tree » Configure MST Region Identifier***. The **MST Region Identifier** form appears.



MST Region Identifier

access
admin

Name: 00-0A-DC-9C-8A-A0
Revision Level: 0
Digest: AC36177F50283CD4B83821D8AB26

① Name Box
② Revision Level Box
③ Digest Box
④ Apply Button
⑤ Reload Button

Figure 8.13 MST Region Identifier Form

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

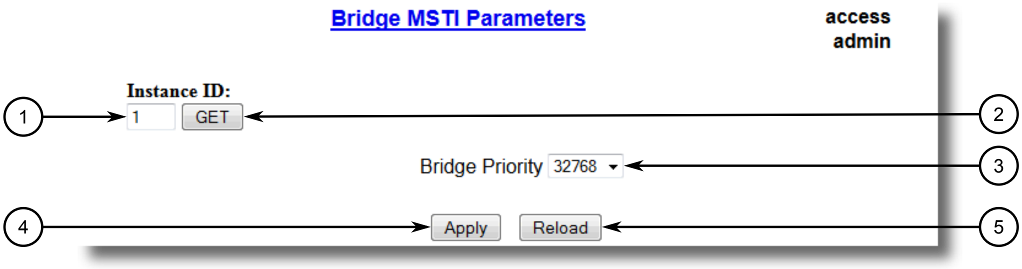
Parameter	Description
`Name`	**Synopsis:** A string 32 characters long **Default:** 00-0A-DC-92-00-00 The name of the MST region. All devices in the same MST region must have the same region name configured.
`Revision Level`	**Synopsis:** An integer between 0 and 65535 **Default:** 0 The revision level for 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 subregions under the same region name.
`Digest`	**Synopsis:** A string 32 characters long **Default:** 0 This is a read-only parameter and should be only used for network troubleshooting. In order to ensure consistent VLAN-to-instance mapping, it is necessary for the protocol to be able to exactly identify the boundaries of the MST regions. For that pupose, the characteristics of the region are included in BPDUs. There is no need to propagate the exact VLAN-to-instance mapping in the BPDUs because switches only need to know whether they are in the same region as a neighbor. Therefore, only this 16-octet digest created from the VLAN-to-instance mapping is sent in BPDUs.

3. Click **Apply**.

8.1.9.4 Configuring a Global MSTI

To configure a global Multiple Spanning Tree Instance (MSTI) for the Spanning Tree Protocol (STP), do the following:

1. Navigate to ***Spanning Tree » Configure Bridge MSTI Parameters***. The **Bridge MSTI Parameters** form appears.



① Instance ID Box
② Get Button
③ Bridge Priority List
④ Apply Button
⑤ Reload Button

Figure 8.14 Bridge MSTI Parameters Form

2. Under **Instance ID**, type an ID number for a Multiple Spanning Tree Instance (MSTI) and click **GET**. The settings for the MSTI are displayed. Any changes made to the configuration will be applied specifically to this instance ID.
3. Configure the following parameter(s) as required:

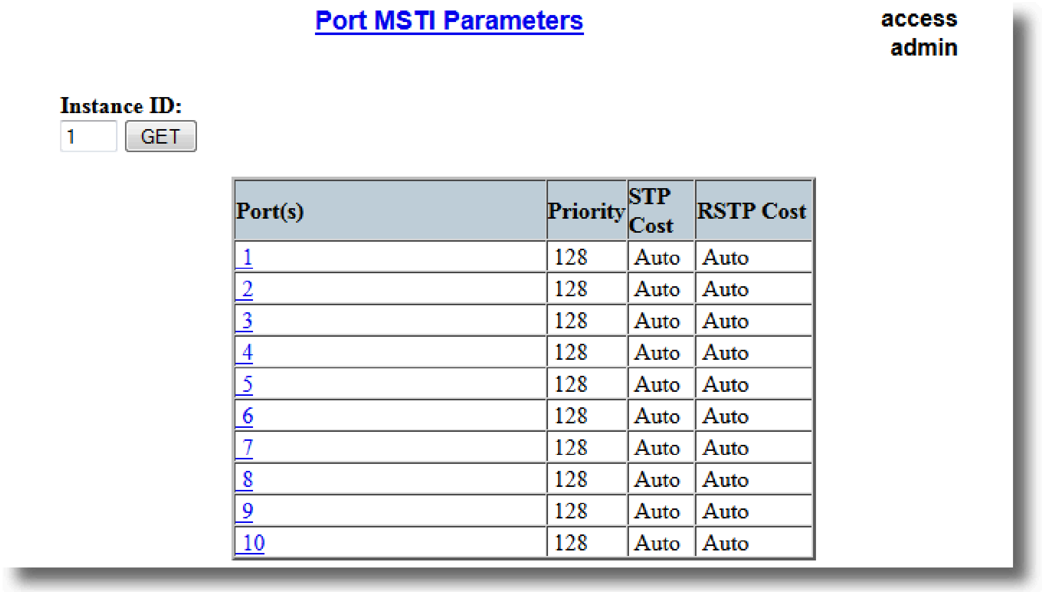
Parameter	Description
`Bridge Priority`	**Synopsis:** [0 | 4096 | 8192 | 12288 | 16384 | 20480 | 24576 | 28672 | 32768 | 36864 | 40960 | 45056 | 49152 | 53248 | 57344 | 61440] **Default:** 32768 Bridge Priority provides a way to control the topology of the STP connected network. The desired Root and Designated bridges can be configured for a particular topology. The bridge with the lowest priority will become root. In the event of a failure of the root bridge, the bridge with the next lowest priority will then become root. Designated bridges that (for redundancy purposes) service a common 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. Click **Apply**.

8.1.9.5 Configuring an MSTI for an Ethernet Port

To configure a Multiple Spanning Tree Instance (MSTI) for an Ethernet port, do the following

1. Navigate to ***Spanning Tree » Configure Port MSTI Parameters***. The **Port MSTI Parameters** table appears.



Port MSTI Parameters

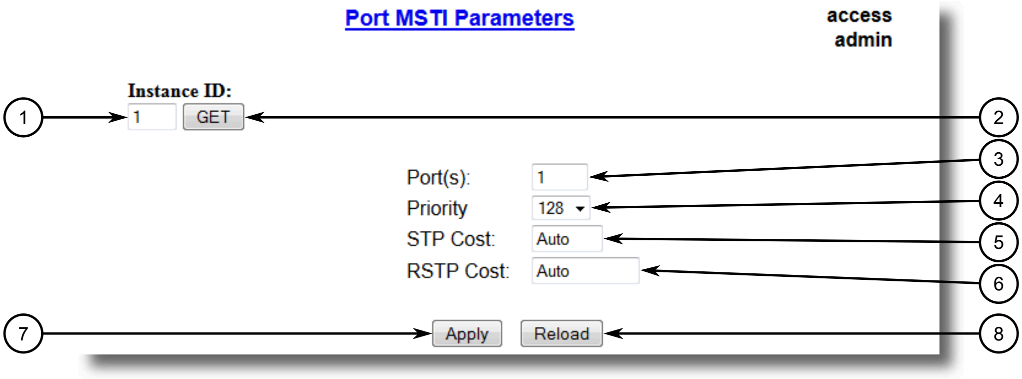
access
admin

Instance ID: 1

Port(s)	Priority	STP Cost	RSTP Cost
1	128	Auto	Auto
2	128	Auto	Auto
3	128	Auto	Auto
4	128	Auto	Auto
5	128	Auto	Auto
6	128	Auto	Auto
7	128	Auto	Auto
8	128	Auto	Auto
9	128	Auto	Auto
10	128	Auto	Auto

Figure 8.15 Port MSTI Parameters Table

2. Select an Ethernet port. The **Port MSTI Parameters** form appears.



Port MSTI Parameters

Instance ID: 1

Port(s): 1

Priority: 128

STP Cost: Auto

RSTP Cost: Auto

① Instance ID Box
② Get Button
③ Port(s) Box
④ Priority List
⑤ STP Cost Box
⑥ RSTP Cost Box
⑦ Apply Button
⑧ Reload Button

Figure 8.16 Port MSTI Parameters Form

3. Under **Instance ID**, type an ID number for a Multiple Spanning Tree Instance (MSTI) and click **GET**. The settings for the MSTI are displayed. Any changes made to the configuration will be applied specifically to this instance ID.
4. Configure the following parameter(s) as required:

Parameter	Description
`Port(s)`	**Synopsis:** Any combination of numbers valid for this parameter The port number as seen on the front plate silkscreen of the switch (or a list of ports, if aggregated in a port trunk).
`Priority`	**Synopsis:** [0 | 16 | 32 | 48 | 64 | 80 | 96 | 112 | 128 | 144 | 160 | 176 | 192 | 208 | 224 | 240] **Default:** 128 Selects the STP port priority. Ports of the same cost that attach to a common LAN will select the port to be used based upon the port priority.
`STP Cost`	**Synopsis:** An integer between 0 and 65535 or [Auto] **Default:** Auto Selects 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 (4 for 1Gbps, 19 for 100 Mbps links and 100 for 10 Mbps links).

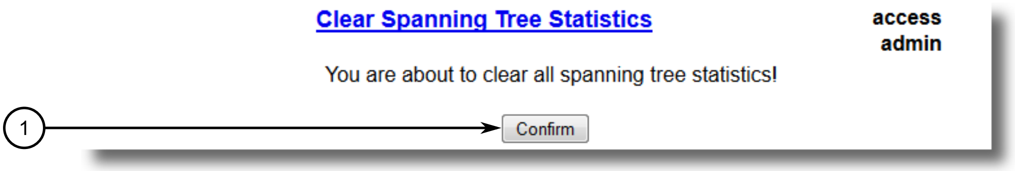
Parameter	Description
	For MSTP, this parameter applies to both external and internal path cost.
`RSTP Cost`	**Synopsis:** An integer between 0 and 2147483647 or [Auto] **Default:** Auto Selects the cost to use in cost calculations, when the Cost Style parameter is set to RSTP in the Bridge RSTP Parameters 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 cost.

5. Click **Apply**.

8.1.10 Clearing Spanning Tree Protocol Statistics

To clear all spanning tree protocol statistics, do the following:

1. Navigate to ***Spanning Tree » Clear Spanning Tree Statistics***. The **Clear Spanning Tree Statistics** form appears.



Clear Spanning Tree Statistics

access
admin

You are about to clear all spanning tree statistics!

① Confirm Button

Figure 8.17 Clear Spanning Tree Statistics Form

2. Click **Confirm**.

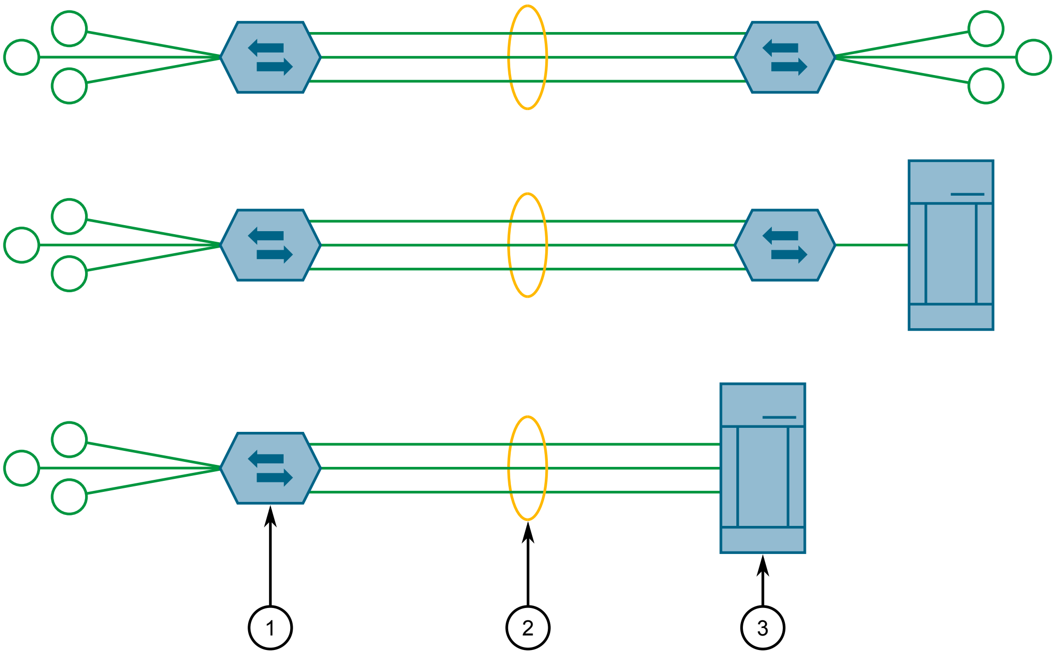
8.2 Managing Link Aggregation

Link aggregation, also referred to as port trunking or port bundling, provides the ability to aggregate or gather several Ethernet ports into one logical link (port trunk) with higher bandwidth. This allows for highly randomized load balancing between the aggregated links based on both the source and destination MAC addresses of the forwarded frames.

Link aggregation can be used for two purposes:

- To obtain increased, linearly incremental link bandwidth.

- To improve network reliability by creating link redundancy. If one of the aggregated links fails, the switch will balance the traffic between the remaining links.



① Switch
② Server

Figure 8.18 Examples of Link Aggregation

RUGGEDCOM ROS allows up to 15 port trunks to be configured on a single device, with each consisting of up to 8 ports.

Note
The maximum number of port trunks for each device depends on the number of ports available. At least two ports are required to configure a port trunk.

Note
The aggregated port with the lowest port number is called the Port Trunk Primary Port. Other ports in the trunk are called Secondary Ports.

8.2.1 Link Aggregation Concepts

This section describes some of the concepts important to the implementation of link aggregation in RUGGEDCOM ROS.

8.2.1.1 Rules and Limitations

The implementation of link aggregation must adhere to the following rules and limitations:

- Each port can belong to only one port trunk at a time.
- A port mirroring target port can not be a member of a port trunk. However, a port mirroring source port can be a member of a port trunk.
- If only one QinQ port is supported by the switch, the port working in QinQ mode cannot be a secondary member of a port trunk.
- DHCP Relay Agent Client port cannot be a member of a port trunk.
- Load balancing between the links of a bundle is randomized and may not be ideal. For instance, if three 100 Mbs links are aggregated, the resulting bandwidth of the port trunk may not be precisely 300 Mbs.
- A Static MAC Address should not be configured to reside on an aggregated port – it may cause some frames destined for that address to be dropped.
- A secure port cannot be a member of a port trunk.
- The IEEE 802.3ad Link Aggregation standard requires all physical links in the port trunk to run at the same speed and in full-duplex mode. If this requirement is violated, the performance of the port trunk will drop.

  The switch will raise an appropriate alarm, if such a speed/duplex mismatch is detected.
- STP dynamically calculates the path cost of the port trunk based on its aggregated bandwidth. However, if the aggregated ports are running at different speeds, the path cost may not be calculated correctly.
- Enabling STP is the best way for handling link redundancy in switch-to-switch connections composed of more than one physical link. If STP is enabled and increased bandwidth is not required, Link Aggregation should not be used because it may lead to a longer fail-over time.

8.2.1.2 Link Aggregation and Layer 2 Features

Layer 2 features (e.g. STP, VLAN, CoS, Multicast Filtering) treat a port trunk as a single link.

- If the Spanning Tree Protocol (STP) puts an aggregated port in blocking/forwarding, it does it for the whole port trunk.
- If one of the aggregated ports joins/leaves a multicast group (e.g. via IGMP or GMRP), all other ports in the trunk will join/leave too.
- Any port configuration parameter (e.g. VLAN, CoS) change will be automatically applied to all ports in the trunk.
- Configuration/status parameters of the secondary ports will not be shown and their port numbers will be simply listed next to the primary port number in the appropriate configuration/status UI sessions.

- When a secondary port is added to a port trunk, it inherits all the configuration settings of the primary port. When this secondary port is removed from the port trunk, the settings it had previous to the aggregation are restored.

8.2.1.3 Link Aggregation and Physical Layer Features

Physical layer features (e.g. physical link configuration, link status, rate limiting, Ethernet statistics) will still treat each aggregated port separately.

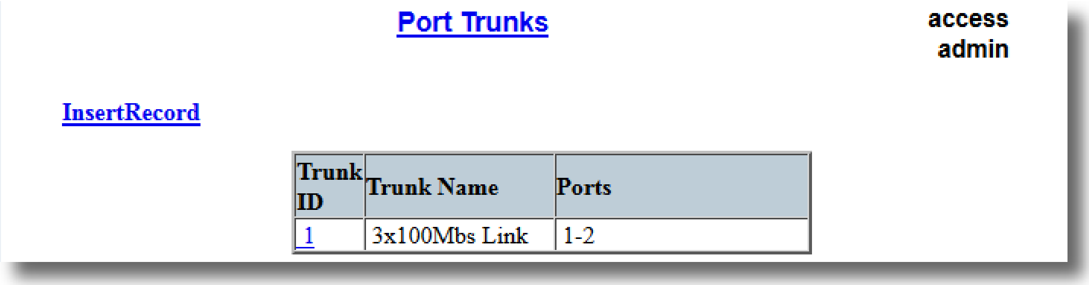
- Physical configuration/status parameters will NOT be automatically applied to other ports in the trunk and will be displayed for each port as usual.
- Make sure that only ports with the same speed and duplex settings are aggregated. If auto-negotiation is used, make sure it is resolved to the same speed for all ports in the port trunk.
- To get a value of an Ethernet statistics counter for the port trunk, add the values of the counters for all ports in the port trunk.

8.2.2 Managing Port Trunks

This section describes how to manage port trunks.

8.2.2.1 Viewing a List of Port Trunks

To view a list of port trunks configured on the device, navigate to ***Link Aggregation » Configure Port Trunks***. The **Port Trunks** table appears.



Trunk ID	Trunk Name	Ports
1	3x100Mbs Link	1-2

Figure 8.19 Port Trunks Table

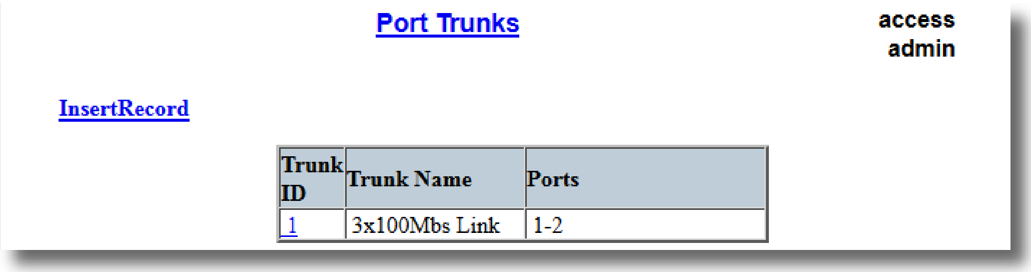
If port trunks have not been configured, add trunks as needed. For more information, refer to "Adding a Port Trunk (Page 225)".

8.2.2.2 Adding a Port Trunk

To add a port trunk, do the following:

> ⚠ **NOTICE**
>
> The port trunk must be properly configured on both sides of the aggregated link. In switch-to-switch connections, if the configuration of both sides does not match (i.e. some ports are mistakenly not included in the port trunk), it will result in a loop. Therefore, the following procedure is strongly recommended to configure a port trunk:
>
> 1. Disconnect or disable all the ports involved in the configuration, i.e. either being added to or removed from the port trunk.
> 2. Configure the port trunk on both switches.
> 3. Double-check the port trunk configuration on both switches.
> 4. Reconnect or re-enable the ports.
>
> If the port trunk is being configured while the ports are not disconnected or disabled, the port will be automatically disabled for a few seconds.

1. Navigate to ***Link Aggregation » Configure Port Trunks***. The **Port Trunks** table appears.



Port Trunks

access
admin

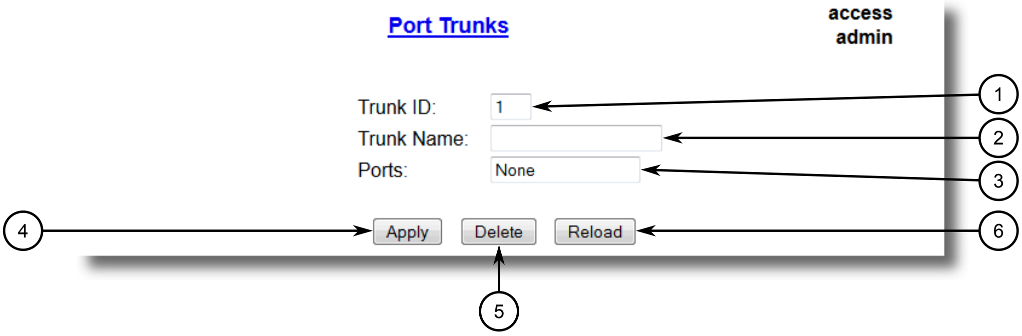
InsertRecord

Trunk ID	Trunk Name	Ports
1	3x100Mbs Link	1-2

① InsertRecord

Figure 8.20 Port Trunks Table

2. Click **InsertRecord**. The **Port Trunks** form appears.



① Trunk ID Box
② Trunk Name Box
③ Ports Box
④ Apply Button
⑤ Delete Button
⑥ Reload Button

Figure 8.21 Port Trunks

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

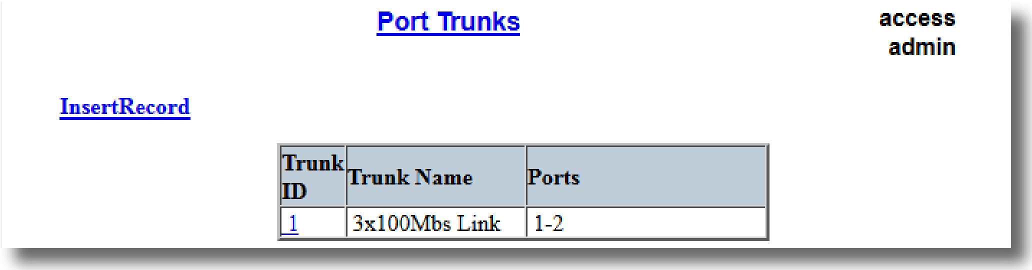
Parameter	Description
`Trunk ID`	**Synopsis:** An integer between 1 and 2 **Default:** 1 Trunk number. It doesn't affect port trunk operation in any way and is only used for identification.
`Trunk Name`	**Synopsis:** A string 19 characters long Provides a description of the aggregated link purpose.
`Ports`	**Synopsis:** Any combination of numbers valid for this parameter **Default:** None List of ports aggregated in the trunk.

4. Click **Apply**.

8.2.2.3 Deleting a Port Trunk

To delete a port trunk, do the following:

1. Navigate to ***Link Aggregation » Configure Port Trunks***. The **Port Trunks** table appears.



Port Trunks

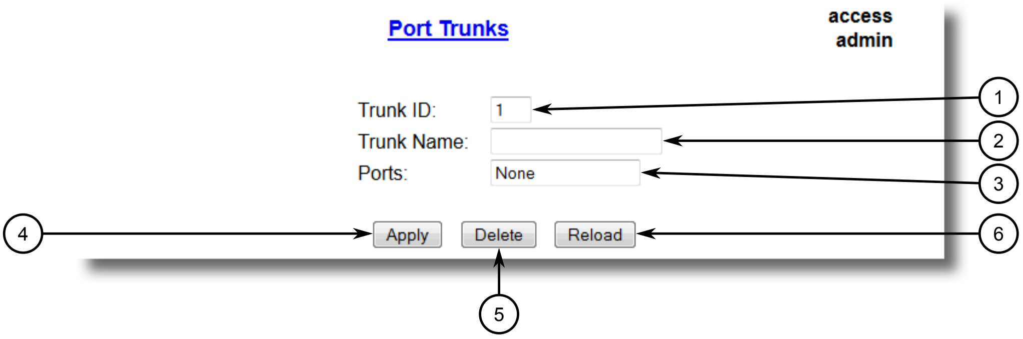
access
admin

InsertRecord

Trunk ID	Trunk Name	Ports
1	3x100Mbs Link	1-2

Figure 8.22 Port Trunks Table

2. Select the port trunk from the table. The **Port Trunks** form appears.



Port Trunks

access
admin

Trunk ID:	1
Trunk Name:	
Ports:	None

① Trunk ID Box
② Trunk Name Box
③ Ports Box
④ Apply Button
⑤ Delete Button
⑥ Reload Button

Figure 8.23 Port Trunks Form

3. Click **Delete**.

9 Wireless

This chapter describes how to configure and manage the various wireless interfaces and utilities available in RUGGEDCOM ROS.

Note

Some wireless features require the device to be equipped with a specific line module.

9.1 Managing Wireless LANs

This section describes how to manage wireless LANs.

⚠ **NOTICE**

Spanning Tree Protocols (e.g. STP, RSTP and MSTP) are designed for fixed, wired networks. These protocols are not well suited for wireless point-to-multipoint bridging. It is highly recommended to disable the Spanning Tree Protocol on the WLAN port, otherwise the WLAN interface might not perform as expected under certain conditions. For more information, refer to "Configuring STP for Specific Ethernet Ports (Page 203)".

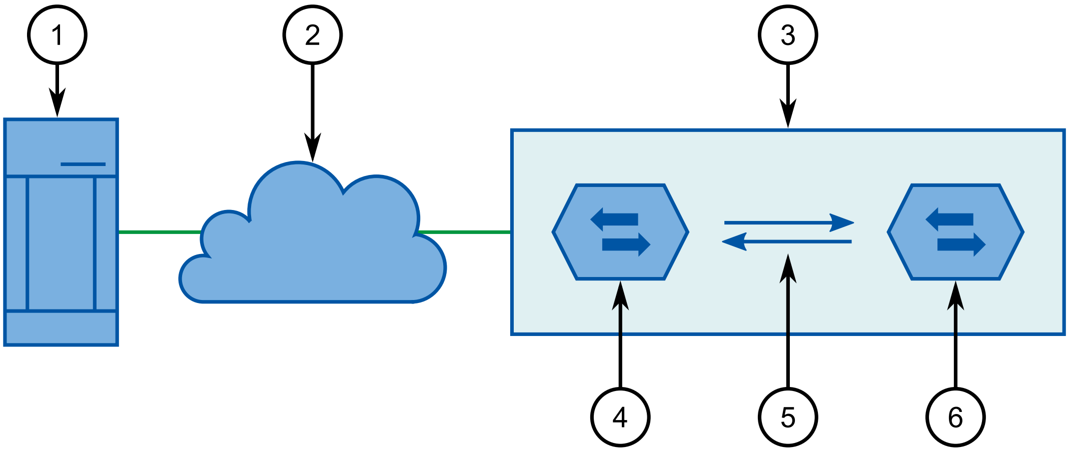
⚠ **NOTICE**

Make sure the wireless LAN is running before attempting to apply any changes. The configuration cannot be modified, for example, while the wireless LAN is initializing.

9.1.1 Wireless LAN Concepts

A typical IEEE 802.11 infrastructure network consists of four major physical components:

- Stations (STA)
- Access Point (AP)
- Wireless media
- Distribution System



① Authentication Server
② Distribution System
③ Infrastructure Basic Service Set (BSS)
④ Access Point (AP)
⑤ Wireless Media
⑥ Station (Client)

Figure 9.1 A Typical IEEE 802.11 Infrastructure Basic-Service-Set (Component)

The following are some key characteristics of all IEEE 802.11 infrastructure networks:

- Infrastructure BSS (Basic Service Set) represents the RF coverage area of AP.
- All communication inside the infrastructure BSS goes through the AP
- All Stations in a wireless network are identified by a unique 48-bit IEEE 802 MAC addresses.
- If a station (STA) wants to access the network resource, it must first associate with an Access Point. Association is the process by which a station joins an 802.11 network; it is logically equivalent to plugging in the network cable on an Ethernet switch.
- Standard 802.11 stations normally act as communications end points (i.e. with no bridging functionality, a single (wireless) STA supporting only a single network device).

Note
The AP device always supports a *bridged* (single) Layer 2 network across both domains (backhaul distribution system and the wireless IEEE 802.11 BSS).

9.1.1.1 Wireless Client/Bridge Operation

A WLAN in Client/Bridge operating mode is designed to operate along with a complimentary wireless Access Point (AP) device that supports the WDS extensions required by the Client/Bridge. As a standard approach to handling Layer 2 bridging over an IEE

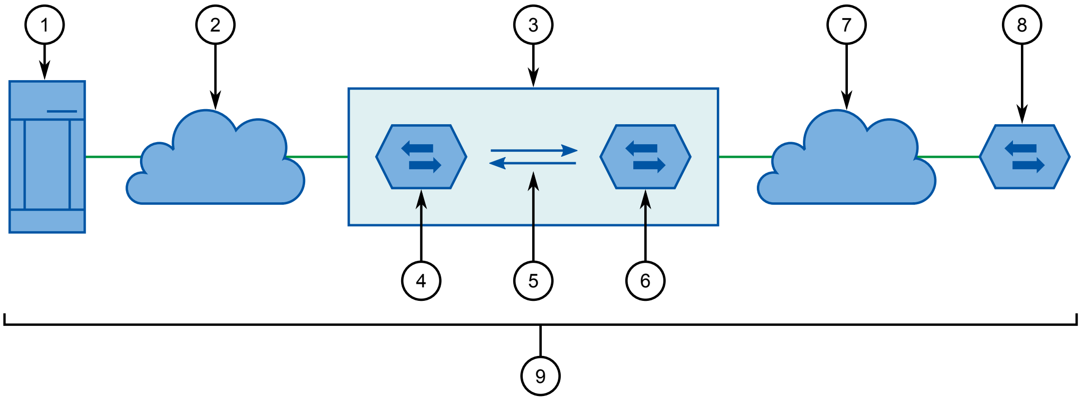
802.11 wireless network does not exist, there is no guarantee otherwise of interoperability between the Client/Bridge and a third party AP.

As an alternative to the wireless Client/Bridge operating mode, Siemens has introduced a wireless Client/IP Bridge mode. The Client/IP Bridge mode uses native IEEE 802.11 standards without any proprietary extensions, so that a RUGGEDCOM IEEE 802.11 client can inter-operate with any vendor's IEEE 802.11 compliant AP. This Client/IP Bridge mode utilizes *bi-directional layer 2 NAT* to allow traffic flow between the Client/IP Bridge Distribution System and the AP Distribution system. This enables wired devices located *behind* both the Station (STA) and the AP to exchange IP traffic.

The wireless Client/IP Bridge includes the following components:

- IEEE 802.11 infrastructure mode STA
- Bi-directional Layer 2 NAT

Note
A Client/IP Bridge only bridges IPv4 and ARP traffic.



① Authentication Server
② Distribution System
③ Infrastructure Basic Service Set (BSS)
④ Access Point (AP)
⑤ Wireless Media
⑥ Client/IPv4 Bridge
⑦ IPv4 Distribution System
⑧ IED
⑨ Layer 2 Bridged Network

Figure 9.2 Wireless Client/IP Bridge Infrastructure Basic-Service-Set Diagram

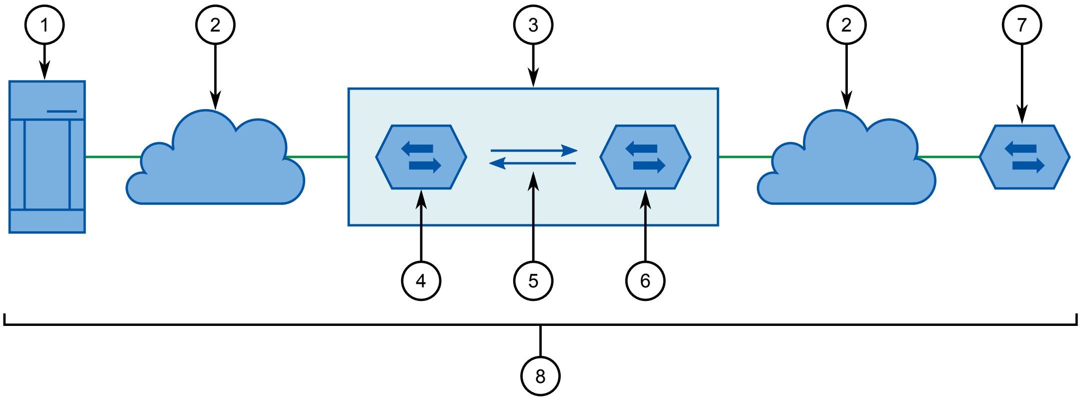
9.1.1.2 Wireless Extensions for Client/Bridge Operation

IEEE 802.11 defines a wireless station as a single endpoint in a wireless network. The interaction between a single associated station and an IEEE 802.11 Access Point (in infrastructure mode) does not support Layer 2 bridging of traffic for wired devices located *behind* a wireless station. In other words, the wireless network model expects that only the AP device will be connected to a *wired* LAN (i.e. fixed-end distribution service), while each station will represent an individual stand-alone remote client with a single network address. Examples of a typical IEEE 802.11 station device include PDAs, mobile gaming consoles, and laptop PCs.

The wireless network model extends the IEEE 802.11 infrastructure mode functionality to provide seamless wireless connectivity to multiple network devices connected to the *switched/wired* LAN side of a single wireless station device. In this way, full Layer 2 traffic bridging is achieved between the *switched/wired* LAN on the AP device and the*switched/wired* LAN on the Client/Bridge device, while communicating over a wireless medium.

The wireless Client/Bridge extensions include the integration of the following components:

- IEEE 802.11 infrastructure mode STA
- WDS (Wireless Distribution System)
- Ethernet bridging functionality (single/wireless STA bridging multiple wired devices)



① Authentication Server
② Distribution System
③ Infrastructure Basic Service Set (BSS)
④ RUGGEDCOM Access Point (AP)
⑤ Wireless Media
⑥ Client/Bridge
⑦ IED
⑧ Layer 2 Bridged Network

Figure 9.3 Wireless Client/Bridge Infrastructure Basic-Service-Set (Extensions)

Note

The Client/Bridge always supports a *bridged* (single) network across both domains (local devices connected to the switched ports and the IEEE 802.11 BSS).

9.1.1.3 Network Limitations

Network limitations exist for each available operational mode.

Operational Mode	Limitation
Access Point (AP)	When the RS900W is configured as an AP, there is a limit to the number of wireless client stations that can be associated at the same time. • No wireless (link) encryption: up to 63 wireless client stations • With WPA/WPA2 (using AES) enabled: up to 60 wireless client stations • With WPA/WPA2 (using TKIP) enabled: up to 30 wireless client stations **Note** In a wireless infrastructure network, all wireless clients will share the limited available wireless bandwidth, so that client link performance will decrease for all clients as additional clients become associated.
Client/Bridge	When the RS900W is configured as a Client/Bridge, there is a limit to the number of devices/addresses that can be connected to the wired switch ports, and bridged by the single wireless client. • Number of devices *bridged* by a single Client/Bridge unit: 31 devices (L2 addresses) **Note** The wireless Client/Bridge configuration is designed to operate with a wireless AP configuration. Siemens does not guarantee interoperability between the wireless Client/Bridge and other third party AP equipment.
Client/IP Bridge	When the RS900W is configured as a Client/IP Bridge, there is a limit to the number of device/addresses that can be connected to the wired switch ports, and bridged by the (single) wireless client. • Number of devices *bridged* by a single Client/IP Bridge unit: 31 devices (L2 addresses) **Note** The wireless Client/IP Bridge configuration is designed to bridge only IPv4 and ARP traffic.

The differences between Client/Bridge and Client/IP Bridge modes are as follows:

	Client/Bridge	Client/IP Bridge
Traffic Forwarding Supported	Any Ethernet-encapsulated protocol	Only IPv4 and ARP
Interoperability	Only Works with a wireless AP	Works with any AP

9.1.1.4 Frequently Asked Questions

The following are answers to commonly asked questions:

Radio Frequency (RF) Links

Q: What type of diversity is applied in the wireless models?

A: The type of diversity used is called *receiver diversity*, whereby a dual-antenna configuration will provide optimum performance in high multi-path environments such as warehouses, offices and other (typically) indoor installations. The receiver will have the benefit of being able to choose between two antennae, while the transmitter will utilize a single antenna.

Q: Can antenna 2 (RX) be disabled? Is a terminator required?

A: It is entirely optional to use the second antenna (RX). A terminator does not need to be installed on the connector if the second antenna is not used.

Q: How are received signals computed on the two RX antennae? Does it add both paths?

A: The wireless models use a simple heuristic in support of the receiver diversity. It will simply choose the stronger signal on the two antennas. It does *not* add both signal paths together. This type of summation cannot be done without a MIMO (Multiple-Input-Multiple-Output) configuration, which is not supported by RUGGEDCOM ROS.

Q: Will the performance be affected by using an external directional antenna 1 (TX/RX), and leaving the original antenna 2 (RX) in place?

A: Both antennae can be connected externally. The purpose behind the dual-antenna receiver-diversity feature is that, by using two antennae, the "capture surface" of the receive antenna is effectively increased. This does not increase the antenna gain, but it does allow for better reception in the presence of multi-path signals. In practice, multi-path signals are observed in indoor environments, where there tend to be more obstructions in the path of the radio line-of-sight. In outdoor scenarios, it is expected there are fewer obstructions and opportunities for reflections to generate multi-path signals.

Q: How does distance between the AP and station affect RF link quality?

A: Any wireless receiver can become saturated if the signal is too strong. This commonly occurs if the wireless station is located too close (1 to 2 meters) to the access point. Simply lowering the transmit (TX) power on the AP and Client/Bridge or alternatively, increasing the distance between the two units should resolve this problem.

Q: What is *RSSI*

A: RSSI stands for *Received Signal Strength Indication*. It is a measurement of the power present in the received radio signal, not of the signal quality.

In general, an RSSI value of *10 or less* represents a weak signal, although the hardware can often still decode low data-rate signals. An RSSI value of *approximately 20* is an acceptable signal level. An RSSI value of *40 or more* is a very strong signal and will easily support 54 MBit/s operation. The RSSI value will fluctuate with time due to interference, channel fading, etc.

Compatibility and Interoperability

Q: What is *WDS* and where is it used?

A: WDS stands for *Wireless Distribution System*. A WDS is an industry accepted extension for the IEEE 802.1 frame format. Fundamentally, it extends the IEEE 802.11 MAC frame format from a conventional three-address field format to a four-address field format. The ultimate use of the additional address field, however, remains unspecified within the WDS specification. As such, implementations relying on WDS are often vendor specific.

Wireless LAN relies on WDS features to implement the Client/Bridging operational mode. It is important to note the WDS features must be present in both the Access Point (AP) unit as well as the Client/Bridge device over the wireless network. Basically, for a wireless Client/Bridge device to operate correctly, it must be partnered with a wireless AP device.

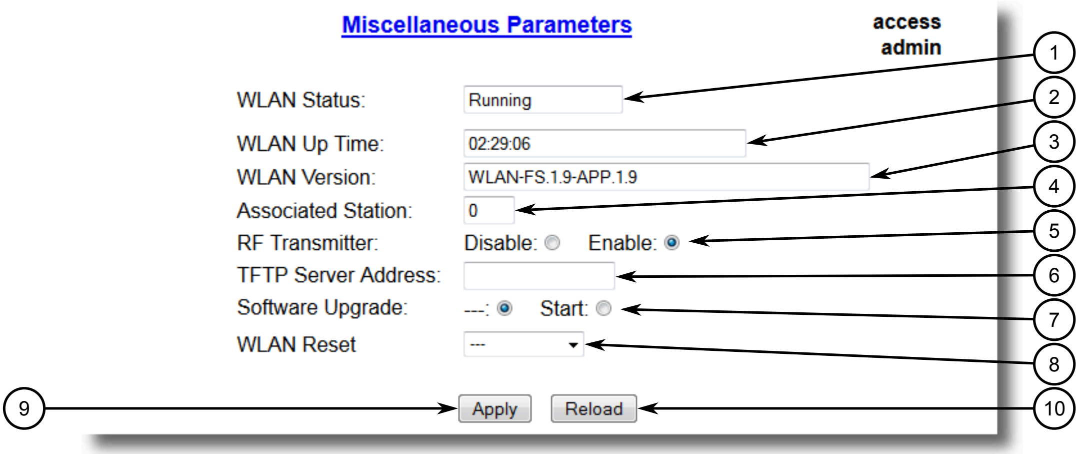
Q: What is the *Client/Bridge* mode of operation?

A: The wireless Client/Bridge operating mode allows for the construction of a single *bridged* wireless network consisting of one IP addressed subnet applied between the AP and every wirelessly associated Client/Bridge. The network extends to each individually connected end-point device that is attached to the Client/Bridge switched ports.

In summary, a common distribution system is maintained across the wireless medium, by a Layer 2 bridge between the Ethernet switched ports (i.e. backhaul LAN) of the AP and the Ethernet switched ports (i.e. device LAN) on the Client/Bridge. The wireless Client/Bridge operational mode will only be correctly supported by a wireless AP device.

9.1.2 Viewing the Status of the Wireless LAN

To view the status of the wireless LAN, navigate to ***WLAN Interface » Miscellaneous Parameters***. The **Miscellaneous Parameters** form appears.



Miscellaneous Parameters

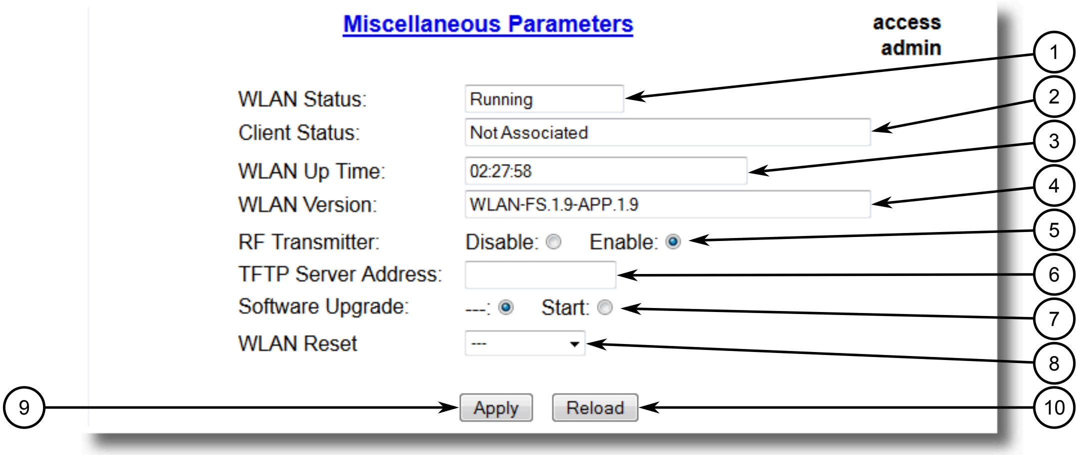
access
admin

WLAN Status: Running
WLAN Up Time: 02:29:06
WLAN Version: WLAN-FS.1.9-APP.1.9
Associated Station: 0
RF Transmitter: Disable: ○ Enable: ●
TFTP Server Address:
Software Upgrade: ---: ● Start: ○
WLAN Reset ---

① WLAN Status Box
② WLAN Up Time Box

③ WLAN Version Box
④ Associated Station Box
⑤ RF Transmitter Options
⑥ TFTP Server Address Box
⑦ Software Upgrade Options
⑧ WLAN Reset List
⑨ Apply Button
⑩ Reload Button

Figure 9.4 Miscellaneous Parameters Form (Access Point Mode)



Miscellaneous Parameters

access
admin

WLAN Status: Running
Client Status: Not Associated
WLAN Up Time: 02:27:58
WLAN Version: WLAN-FS.1.9-APP.1.9
RF Transmitter: Disable: ○ Enable: ●
TFTP Server Address:
Software Upgrade: ---: ● Start: ○
WLAN Reset ---

① WLAN Status Box
② Client Status Box
③ WLAN Up Time Box
④ WLAN Version Box
⑤ RF Transmitter Options
⑥ TFTP Server Address Box
⑦ Software Upgrade Options
⑧ WLAN Reset List
⑨ Apply Button
⑩ Reload Button

Figure 9.5 Miscellaneous Parameters Form (Client/Bridge or Client/IP Bridge)

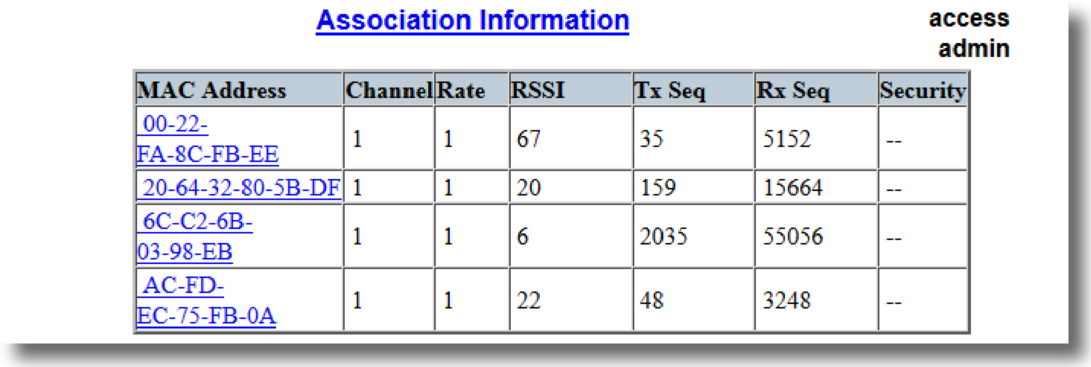
The following parameters detail the status of the wireless LAN:

Parameter	Description
`WLAN Status`	**Synopsis:** [--- | Booting | Running | Cmd Processing | Software Upgrade] This parameter reflects the current status of the wireless interface. This is a read only parameter.
`Client Status`	**Synopsis:** [Not Associated | Associated | Auth is in progress] Provides status information related to the client, for example, whether it is associated with an access point.

Parameter	Description
`WLAN Up Time`	**Synopsis:** A string 32 characters long Provides information about WLAN up time.
`WLAN Version`	**Synopsis:** A string 48 characters long Provides information about WLAN firmware version.

9.1.3 Viewing a List of Associations

To view a list of wireless links the device has with either associated/registered stations (if configured as an Access Point) or a single associated Access Point (if configured as a client), navgiate to ***WLAN Interface » Association Information***. The **Association Information** table appears.



Association Information

access
admin

MAC Address	Channel	Rate	RSSI	Tx Seq	Rx Seq	Security
00-22-FA-8C-FB-EE	1	1	67	35	5152	--
20-64-32-80-5B-DF	1	1	20	159	15664	--
6C-C2-6B-03-98-EB	1	1	6	2035	55056	--
AC-FD-EC-75-FB-0A	1	1	22	48	3248	--

Figure 9.6 Miscellaneous Parameters Table (Access Point Mode)

This table displays the following information:

Parameter	Description
`MAC Address`	**Synopsis:** ##-##-##-##-##-## where ## ranges 0 to FF Provides detailed information on (multiple) wireless links with associated (registered) station(s) – if the unit is configured as an AP. Otherwise this table will reflect the (single) link information to the associated AP – if the device is configure as a Client. Displayed information includes: MAC address – the address of associated (registered) station. Channel – Channel number in use. Rate – Current data rate. RSSI – Received Signal Strength Indication value, RSSI is a measurement of the power present in a received RF signal. Tx Seq – Transmitter sequence number. Rx Seq – Receiver sequence number. Security – Security setting.
`Channel`	**Synopsis:** An integer between 0 and 65535 Provides detailed information on (multiple) wireless links with associated (registered) station(s) – if the unit is configured as an AP.

Parameter	Description
	Otherwise this table will reflect the (single) link information to the associated AP – if the device is configure as a Client. Displayed information includes: MAC address – the address of associated (registered) station. Channel – Channel number in use. Rate – Current data rate. RSSI – Received Signal Strength Indication value, RSSI is a measurement of the power present in a received RF signal. Tx Seq – Transmitter sequence number. Rx Seq – Receiver sequence number. Security – Security setting.
`Rate`	**Synopsis:** An integer between 0 and 65535 Provides detailed information on (multiple) wireless links with associated (registered) station(s) – if the unit is configured as an AP. Otherwise this table will reflect the (single) link information to the associated AP – if the device is configure as a Client. Displayed information includes: MAC address – the address of associated (registered) station. Channel – Channel number in use. Rate – Current data rate. RSSI – Received Signal Strength Indication value, RSSI is a measurement of the power present in a received RF signal. Tx Seq – Transmitter sequence number. Rx Seq – Receiver sequence number. Security – Security setting.
`RSSI`	**Synopsis:** An integer between 0 and 4294967295 Provides detailed information on (multiple) wireless links with associated (registered) station(s) – if the unit is configured as an AP. Otherwise this table will reflect the (single) link information to the associated AP – if the device is configure as a Client. Displayed information includes: MAC address – the address of associated (registered) station. Channel – Channel number in use. Rate – Current data rate. RSSI – Received Signal Strength Indication value, RSSI is a measurement of the power present in a received RF signal. Tx Seq – Transmitter sequence number. Rx Seq – Receiver sequence number. Security – Security setting.
`Tx Seq`	**Synopsis:** An integer between 0 and 4294967295 Provides detailed information on (multiple) wireless links with associated (registered) station(s) – if the unit is configured as an AP. Otherwise this table will reflect the (single) link information to the associated AP – if the device is configure as a Client. Displayed information includes: MAC address – the address of associated (registered) station. Channel – Channel number in use. Rate – Current data rate.

Parameter	Description
	RSSI – Received Signal Strength Indication value, RSSI is a measurement of the power present in a received RF signal. Tx Seq – Transmitter sequence number. Rx Seq – Receiver sequence number. Security – Security setting.
`Rx Seq`	**Synopsis:** An integer between 0 and 4294967295 Provides detailed information on (multiple) wireless links with associated (registered) station(s) – if the unit is configured as an AP. Otherwise this table will reflect the (single) link information to the associated AP – if the device is configure as a Client. Displayed information includes: MAC address – the address of associated (registered) station. Channel – Channel number in use. Rate – Current data rate. RSSI – Received Signal Strength Indication value, RSSI is a measurement of the power present in a received RF signal. Tx Seq – Transmitter sequence number. Rx Seq – Receiver sequence number. Security – Security setting.
`Security`	**Synopsis:** A string 5 characters long Provides detailed information on (multiple) wireless links with associated (registered) station(s) – if the unit is configured as an AP. Otherwise this table will reflect the (single) link information to the associated AP – if the device is configure as a Client. Displayed information includes: MAC address – the address of associated (registered) station. Channel – Channel number in use. Rate – Current data rate. RSSI – Received Signal Strength Indication value, RSSI is a measurement of the power present in a received RF signal. Tx Seq – Transmitter sequence number. Rx Seq – Receiver sequence number. Security – Security setting.

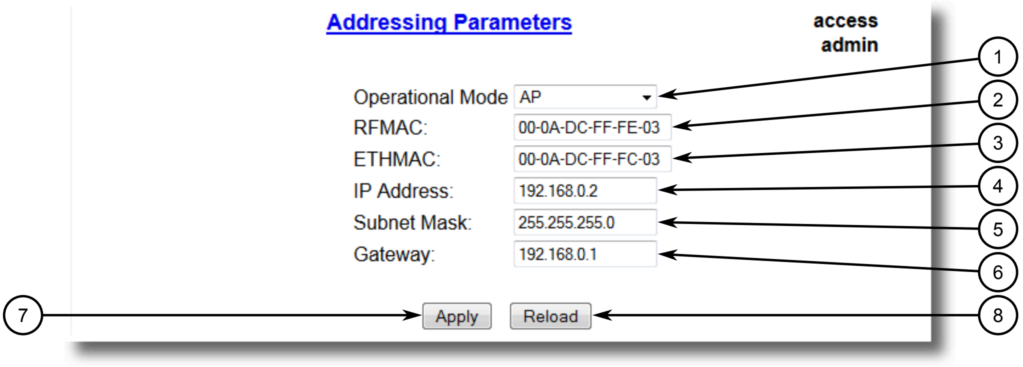
9.1.4 Configuring Addressing Settings

To configure addressing settings for the WLAN, do the following:

⚠ **NOTICE**

Typically, multiple parameters can be configured at once in RUGGEDCOM ROS. The `Operational Mode` parameter is an exception. Due to the underlying dependencies between this and other related parameters, the `Operational Mode` parameter must be configured first.

1. Navigate to ***WLAN Interface » Addressing Parameters***. The **Addressing Parameters** form appears.



Addressing Parameters

access admin

Operational Mode: AP

RFMAC: 00-0A-DC-FF-FE-03

ETHMAC: 00-0A-DC-FF-FC-03

IP Address: 192.168.0.2

Subnet Mask: 255.255.255.0

Gateway: 192.168.0.1

①	Operational Mode List
②	RFMAC Box
③	ETHMAC Box
④	IP Address Box
⑤	Subnet Mask Box
⑥	Gateway Box
⑦	Apply Button
⑧	Reload Button

Figure 9.7 Addressing Parameters Form

> ⚠ **NOTICE**
>
> Typically, multiple parameters can be configured at once in RUGGEDCOM ROS. The *`Operational Mode`* parameter is an exception. Due to the underlying dependencies between this and other related parameters, the *`Operational Mode`* parameter must be configured first.

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

Parameter	Description
`Operational Mode`	**Synopsis:** [AP | Client Bridge | Client IP Bridge] **Default:** AP Configure the wireless interface as an Access Point (AP), a Client/Bridge or Client/IP Bridge. Client/Bridge is basically the integration of an 802.11 station and Ethernet Bridge functionality. Client/IP Bridge is basically the integration of an 802.11 station and Ethernet/IP Bridge functionality. The Client/Bridge bridged all Ethernet traffic by incorporating RuggedCom specific extension. The Client/IP Bridge only bridged IP and ARP traffic without affecting the standard IEEE 802.11 station functionality. As a result Client/IP Bridge can works with any third parties AP.

Parameter	Description
RFMAC	**Synopsis:** ##-##-##-##-##-## where ## ranges 0 to FF **Default:** 00-0A-DC-00-00-00 A 48-bit 802.11 wireless address assigned to the wireless interface. This serves as the BSSID – Basic Service Set Identifier for the AP. This is a read only parameter.
ETHMAC	**Synopsis:** ##-##-##-##-##-## where ## ranges 0 to FF **Default:** 00-0A-DC-00-00-00 The 48-bit Ethernet address assigned to the wired interface. This is a read only parameter.
IP Address	**Synopsis:** ###.###.###.### where ### ranges from 0 to 255 **Default:** 192.168.0.2 The IP address assigned to the wireless interface.
Subnet Mask	**Synopsis:** ###.###.###.### where ### ranges from 0 to 255 **Default:** 255.255.255.0 The IP subnet mask assigned to the wireless interface.
Gateway	**Synopsis:** ###.###.###.### where ### ranges from 0 to 255 **Default:** 192.168.0.1 The IP address of the wireless interface default gateway. The gateway and IP address of the wireless interface must be on the same IP subnet.

3. Click **Apply**.
4. Reset/restart the WLAN. For more information, refer to "Resetting/Restarting the Wireless LAN (Page 256)".

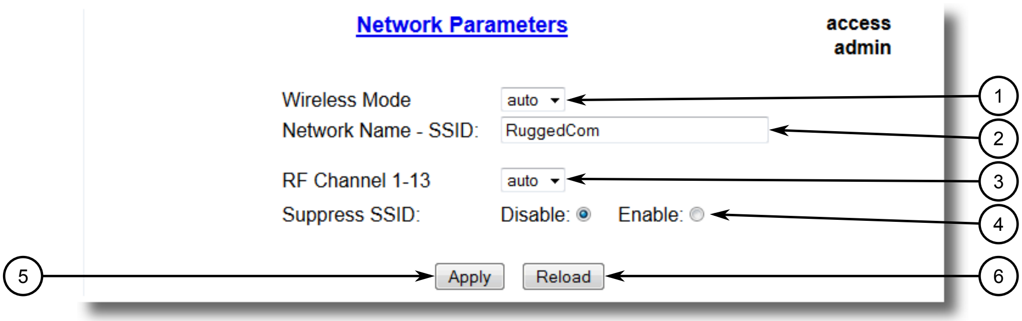
9.1.5 Configuring Network Settings

To configure network settings for the WLAN, do the following:

1. Navigate to ***WLAN Interface » Network Parameters***. The **Network Parameters** form appears.

Note

The parameters available are based on the operational mode of the WLAN. For information about configuring the operational mode, refer to "Configuring Addressing Settings (Page 239)".



Network Parameters

access
admin

Wireless Mode: auto

Network Name - SSID: RuggedCom

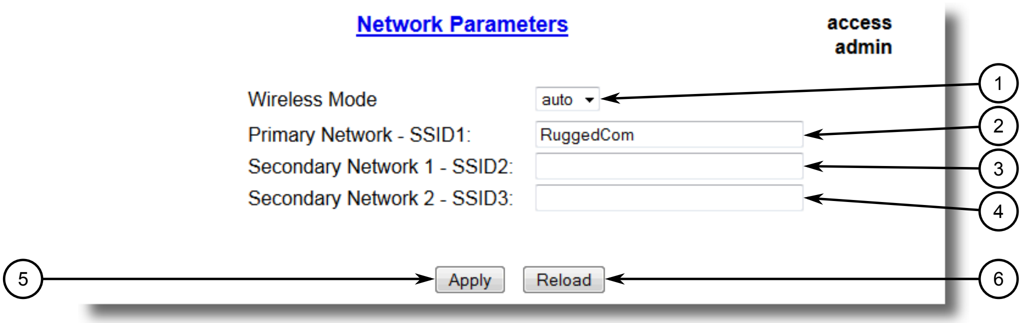
RF Channel 1-13: auto

Suppress SSID: Disable: ● Enable: ○

Apply Reload

① Wireless Mode List
② Network Name - SSID Box
③ RF Channel 1-13 Box
④ Suppress SSID Box
⑤ Apply Button
⑥ Reload Button

Figure 9.8 Networking Parameters Form (Access Point Mode)



Network Parameters

access
admin

Wireless Mode: auto

Primary Network - SSID1: RuggedCom

Secondary Network 1 - SSID2:

Secondary Network 2 - SSID3:

Apply Reload

① Wireless Mode List
② Primary Network - SSID1 Box
③ Secondary Network 1 - SSID2 Box
④ Secondary Network 2 - SSID3 Box
⑤ Apply Button
⑥ Reload Button

Figure 9.9 Networking Parameters Form (Client/Bridge or Client/IP Bridge Mode)

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

Parameter	Description
`Wireless Mode`	**Synopsis:** [auto | 11b | 11g] **Default:** auto This parameter allow user to select the wireless mode that is running on the wireless network. The choices are: [auto] allow Access Point to select the wireless mode. [11b] 802.11b mode only (up to 11 Mbps). [11g] 802.11g mode with 802.11b compatibility (up to 54 Mbps).
`Network Name - SSID`	**Synopsis:** A string 32 characters long **Default:** RuggedCom The SSID (Service Set IDentifier) is a unique name between 3 and 32 characters which is used to identify the wireless network.
`RF Channel 1-13`	**Synopsis:** [1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | auto] **Default:** auto Select appropriate channel from the channel list. All devices in the same BSSID must be communicating on the same channel in order to function correctly. [auto] option allows the device to scan and choose the best available channel, while channel number allows user to select specific channel. Users are responsible for ensuring that the channel configuration complies with the regulatory standards.
`Suppress SSID`	**Synopsis:** [Disable | Enable] **Default:** Disable This option will enable or disable the suppressing of the SSID information sent by the wireless Access Point.

3. Click **Apply**.

4. Reset/restart the WLAN. For more information, refer to "Resetting/Restarting the Wireless LAN (Page 256)".

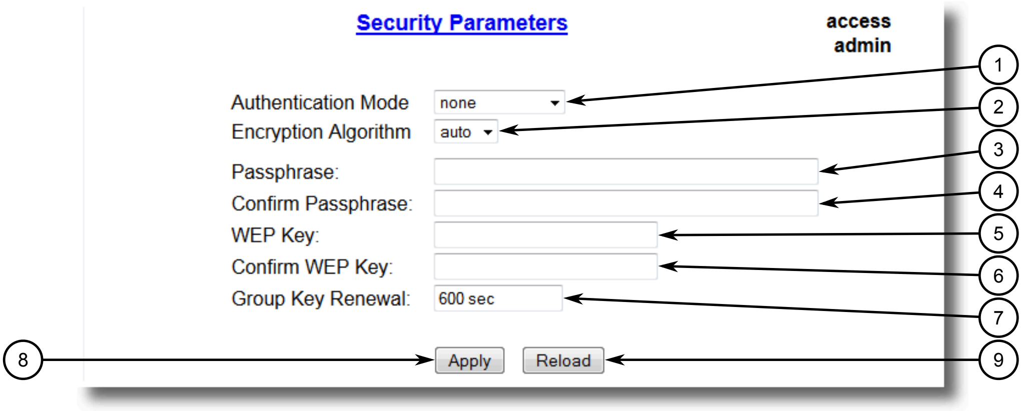
9.1.6 Configuring Security Settings

To configure security settings for the WLAN, do the following:

1. Navigate to ***WLAN Interface » Security Parameters***. The **Security Parameters** form appears.

Note

The parameters available are based on the operational mode of the WLAN. For information about configuring the operational mode, refer to "Configuring Addressing Settings (Page 239)".

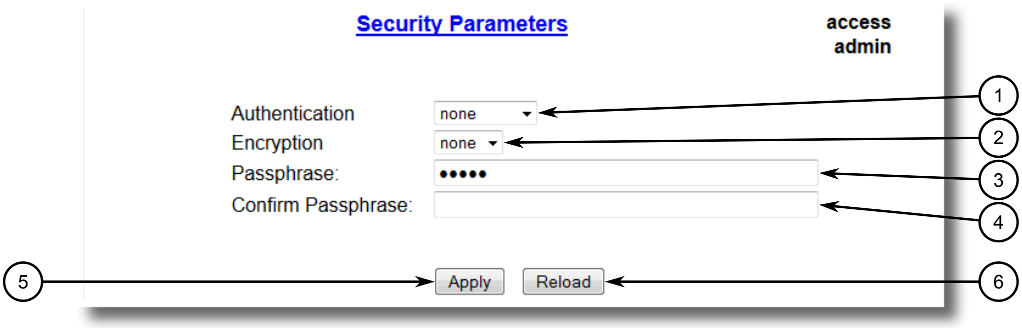

Security Parameters

access
admin

Authentication Mode: none
Encryption Algorithm: auto
Passphrase:
Confirm Passphrase:
WEP Key:
Confirm WEP Key:
Group Key Renewal: 600 sec

① Authentication Mode List
② Encryption Algorithm List
③ Passphrase Box
④ WEP Key Box
⑤ Group Key Removal Box
⑥ Apply Button
⑦ Reload Button

Figure 9.10 Security Parameters Form (Access Point Mode)


Security Parameters

access
admin

Authentication: none
Encryption: none
Passphrase: •••••
Confirm Passphrase:

① Authentication Mode List
② Encryption Algorithm List
③ Passphrase Box
④ Apply Button

⑤ Reload Button

Figure 9.11 Security Parameters Form (Client/Bridge or Client/IP Bridge Mode)

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

Parameter	Description
`Authentication Mode`	**Synopsis:** [none | wep | 802.1x | wpa | wpa-psk | wpa2 | wpa2-psk | wpa-auto | wpa-auto-psk] **Default:** none This parameter allow user to select the authentication mode. The choices are listed below: [none] No authentication. [wep] WEP as an authentication algorithm (Encryption algorithm must also be set to WEP). [802.1X] 802.1X based authentication with RADIUS client and server running on backend. [wpa] WPAv1 authentication type (Enterprise). [wpa-psk] WPAv1-PSK authentication type (Personal). [wpa2] WPAv2 authentication type (Enterprise). [wpa2-psk] WPAv2-PSK authentication type (Personal). [wpa-auto] WPAv1 or WPAv2 authentication type (Enterprise). [wpa-auto-psk] WPAv1 or WPAv2 authentication type (Personal).
`Encryption Algorithm`	**Synopsis:** [auto | wep | tkip | aes] **Default:** auto This parameter allow user to select the encryption algorithm which will be used, in conjunction with the authentication mode. Please note that only WPA2, WPA2-PSK and WPA-PSK authentication mode supports AES encryption.
`Passphrase`	**Synopsis:** A string 48 characters long The Passphrase is an ASCII string between 8 and 48 characters in length. Only applies when the authentication-mode is WPA/WPA2 Personal.
`Confirm Passphrase`	**Synopsis:** A string 48 characters long The Passphrase is an ASCII string between 8 and 48 characters in length. Only applies when the authentication-mode is WPA/WPA2 Personal.
`WEP Key`	**Synopsis:** A string 26 characters long This parameter allow user to configure WEP key of length 10 hex digits or 26 hex digits. Only applies when the authentication mode is WEP.
`Confirm WEP Key`	**Synopsis:** A string 26 characters long This parameter allow user to configure WEP key of length 10 hex digits or 26 hex digits. Only applies when the authentication mode is WEP.
`Group Key Renewal`	**Synopsis:** An integer between 1 and 2147483640 **Default:** 600 This parameter determines how often (in seconds) the group key should be changed. Only applies when the authentication mode is WAP/WPA2 (either Personal or Enterprise) modes.

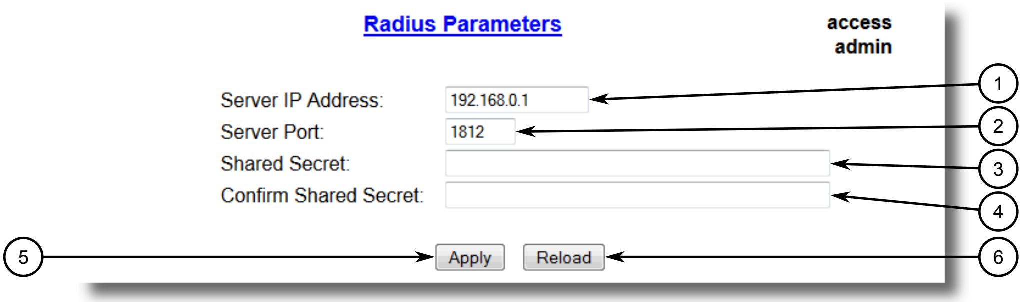
3. Click **Apply**.

4. Reset/restart the WLAN. For more information, refer to "Resetting/Restarting the Wireless LAN (Page 256)".

9.1.7 Configuring Authentication Settings

To configure RADIUS authentication for the WLAN, do the following:

1. Navigate to ***WLAN Interface » Radius Parameters***. The **Radius Parameters** form appears.



Radius Parameters

Server IP Address: 192.168.0.1
Server Port: 1812
Shared Secret:
Confirm Shared Secret:

① Server IP Address Box
② Server Port Box
③ Shared Secret Box
④ Apply Button
⑤ Reload Button

Figure 9.12 Radius Parameters Form

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

Parameter	Description
`Server IP Address`	**Synopsis:** ###.###.###.### where ### ranges from 0 to 255 **Default:** 192.168.0.1 IP address of RADIUS server.
`Server Port`	**Synopsis:** An integer between 1 and 65535 **Default:** 1812 Port number of RADIUS server.
`Shared Secret`	**Synopsis:** A string 48 characters long This is an ASCII string between 8 and 48 characters. This secret is shared between access point and radius server.
`Confirm Shared Secret`	**Synopsis:** A string 48 characters long This is an ASCII string between 8 and 48 characters. This secret is shared between access point and radius server.

3. Click **Apply**.

4. Reset/restart the WLAN. For more information, refer to "Resetting/Restarting the Wireless LAN (Page 256)".

9.1.8 Configuring DHCP Settings

The Dynamic Host Configuration Protocol (DHCP) service provides network configuration information to clients that request it. If a DHCP server is configured to serve a network segment, client network devices that are able to perform a DHCP request need not be configured by operator intervention. Instead, they will acquire an IP address and subnet mask at minimum, and optionally, a gateway and DNS server among other optional parameters, from the DHCP server. Lightweight DHCP server functionality is implement on WLAN.

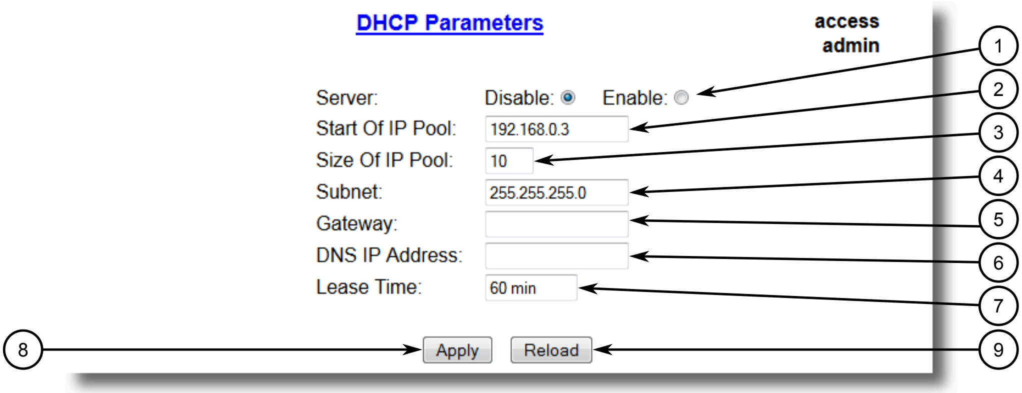
Note

When the wireless unit is configured for Access Point (AP) operational mode, DHCP responds to client requests from both the wired (backhaul) and wireless (IEEE 802.11 BSS) sides of the AP network.

An AP always supports a bridged (single) network across both domains (i.e. backhaul and IEEE 802.11 BSS).

To configure DHCP for the WLAN, do the following:

1. Navigate to ***WLAN Interface » DHCP Parameters***. The **DHCP Parameters** form appears.



DHCP Parameters

access
admin

Server: Disable: ● Enable: ○
Start Of IP Pool: 192.168.0.3
Size Of IP Pool: 10
Subnet: 255.255.255.0
Gateway:
DNS IP Address:
Lease Time: 60 min

① Server Options
② Start Of IP Pool Box
③ Size Of IP Pool Box
④ Subnet Box
⑤ Gateway Box
⑥ DNS IP Address Box
⑦ Lease Time Box
⑧ Apply Button
⑨ Reload Button

Figure 9.13 DHCP Parameters Form

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

Parameter	Description
`Server`	**Synopsis:** [Disable | Enable] **Default:** Disable This parameter allows the user to enable/disable the DHCP server functionality.
`Start Of IP Pool`	**Synopsis:** ###.###.###.### where ### ranges from 0 to 255 **Default:** 192.168.0.3 This parameter allow user to configure the beginning of IP address pool in the DHCP server configuration.
`Size Of IP Pool`	**Synopsis:** An integer between 1 and 64 **Default:** 10 This parameter allow user to configure the size of IP address pool in the DHCP server configuration.
`Subnet`	**Synopsis:** ###.###.###.### where ### ranges from 0 to 255 **Default:** 255.255.255.0 This parameter allow user to configure the IP subnet mask attribute in the DHCP server configuration.
`Gateway`	**Synopsis:** ###.###.###.### where ### ranges from 0 to 255 This parameter allow user to configure the default gateway attribute in the DHCP server configuration.
`DNS IP Address`	**Synopsis:** ###.###.###.### where ### ranges from 0 to 255 This parameter allow user to configure the IP address of DNS server attribute in the DHCP server configuration.
`Lease Time`	**Synopsis:** An integer between 1 and 3200 **Default:** 60 This parameter allow user to configure the lease time attribute in the DHCP server configuration.

3. Click **Apply**.
4. Reset/restart the WLAN. For more information, refer to "Resetting/Restarting the Wireless LAN (Page 256)".

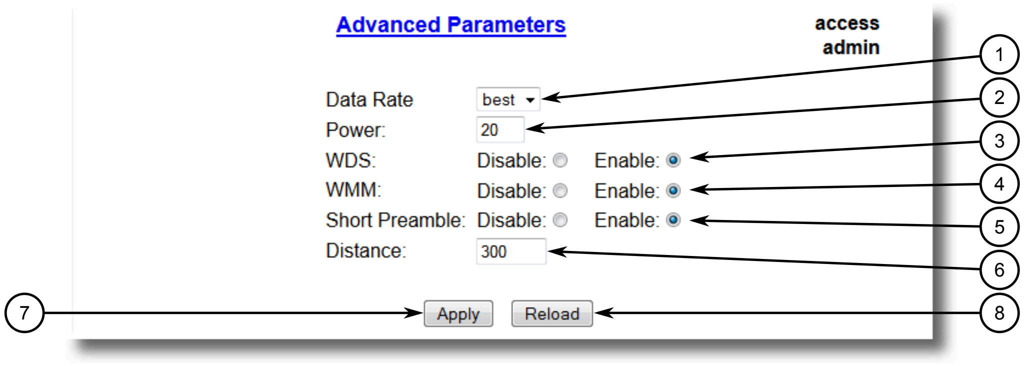
9.1.9 Configuring Advanced Settings

To configure advanced settings for the WLAN, do the following:

1. Navigate to ***WLAN Interface » Advanced Parameters***. The **Advanced Parameters** form appears.

Note

The parameters available are based on the operational mode of the WLAN. For information about configuring the operational mode, refer to "Configuring Addressing Settings (Page 239)".



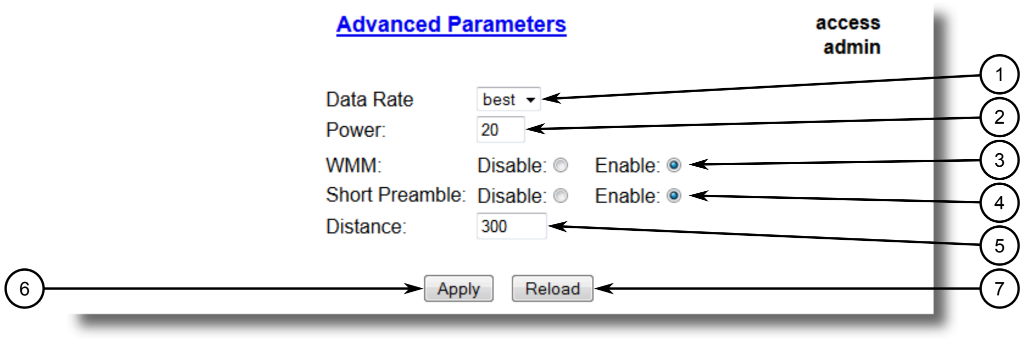
Advanced Parameters

access
admin

Data Rate: best
Power: 20
WDS: Disable: ○ Enable: ●
WMM: Disable: ○ Enable: ●
Short Preamble: Disable: ○ Enable: ●
Distance: 300

① Data Rate List
② Power Box
③ WDS Options
④ WMM Options
⑤ Short Preamble Options
⑥ Distance Box
⑦ Apply Button
⑧ Reload Button

Figure 9.14 Advanced Parameters Form (Access Point or Client Bridge Mode)



Advanced Parameters

access
admin

Data Rate: best
Power: 20
WMM: Disable: ○ Enable: ●
Short Preamble: Disable: ○ Enable: ●
Distance: 300

① Data Rate List
② Power Box
③ WMM Options
④ Short Preamble Options
⑤ Distance Box

⑥ Apply Button
⑦ Reload Button

Figure 9.15 Advanced Parameters Form (Client/IP Bridge Mode)

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

Parameter	Description
`Data Rate`	**Synopsis:** [best | 1 | 2 | 11 | 12 | 18 | 24 | 36 | 48 | 54] **Default:** best This parameter allows the user to control the data link rate of the wireless interface (in Mbps).
`Power`	**Synopsis:** An integer between 1 and 20 **Default:** 20 This parameter allows the user to control the (maximum) RF transmission power.
`WDS`	**Synopsis:** [Disable | Enable] **Default:** Enable This parameter allows the user to enable/disable the Wireless Distribution System (WDS) support. WDS is simply a mechanism for constructing 802.11 frames using the 4-address format. This parameter must be enabled on AP to support station(s) with Client/Bridge functionality.
`WMM`	**Synopsis:** [Disable | Enable] **Default:** Enable Enable QoS support for the wireless interface. In the presence of DS (DiffServ) field the mapping will be as follows: DSCP (DiffServ Code Point) 0x08 and 0x10 are mapped to 'Background'. DSCP 0x20 and 0x28 are mapped to 'Video'. DSCP 0x30 and 0x38 are mapped to 'Voice'. All other DSCP are mapped to 'Best Effort'.
`Short Preamble`	**Synopsis:** [Disable | Enable] **Default:** Enable Control the length of the preamble block in the frames during the wireless communication. This parameter must be disabled for 802.11b devices.
`Distance`	**Synopsis:** An integer between 300 and 15000 **Default:** 300 This parameter allow user to optimize the wireless communication parameters, especially for running wireless links over long distances. The configured distance (in meters) is measured between the AP and the farthest station.

3. Click **Apply**.

4. Reset/restart the WLAN. For more information, refer to "Resetting/Restarting the Wireless LAN (Page 256)".

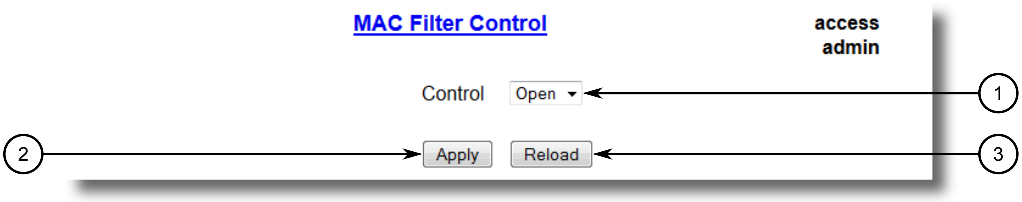
9.1.10 Managing MAC Filtering

This section describes how to configure MAC filtering for the wireless LAN.

9.1.10.1 Configuring MAC Filtering

To configure MAC filtering, do the following:

1. Navigate to ***WLAN Interface » MAC Filtering » MAC Filter Control***. The **MAC Filter Control** form appears.



① Control Box
② Apply Button
③ Reload Button

Figure 9.16 MAC Filter Control Form

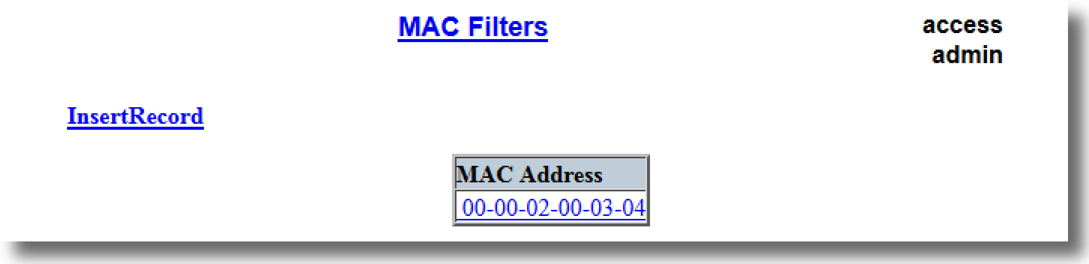
2. Configure the following parameter(s) as required:

Parameter	Description
`Control`	**Synopsis:** [Open | Allow | Deny] **Default:** Open This parameter allow user to control MAC filter policy. The choices are listed below: [Open] No MAC filtering is performed. [Allow] Only allow specified MACs in the list. [Deny] Only deny specified MACs in the list.

3. Click **Apply**.

9.1.10.2 Viewing a List of Filtered MAC Addresses

To view a list of filtered MAC addresses, navigate to ***WLAN Interface » MAC Filtering » MAC Filters***. The **MAC Filters** form appears.



MAC Filters

access
admin

InsertRecord

MAC Address
00-00-02-00-03-04

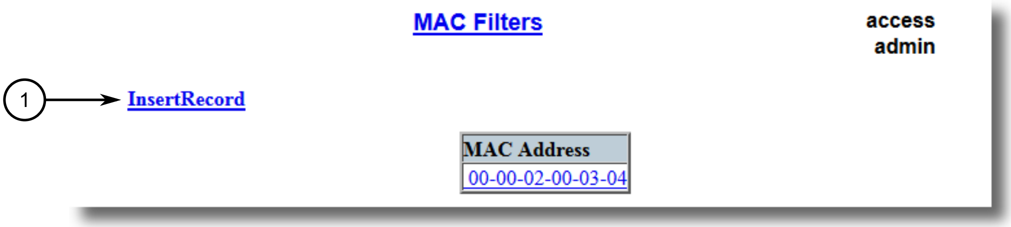
Figure 9.17 MAC Filters Table

If MAC addresses have not been configured, add addresses as needed. For more information, refer to "Adding a MAC Address (Page 252)".

9.1.10.3 Adding a MAC Address

To add a MAC address for filtering, do the following:

1. Navigate to ***WLAN Interface » MAC Filtering » MAC Filters***. The **MAC Filters** table appears.



MAC Filters

access
admin

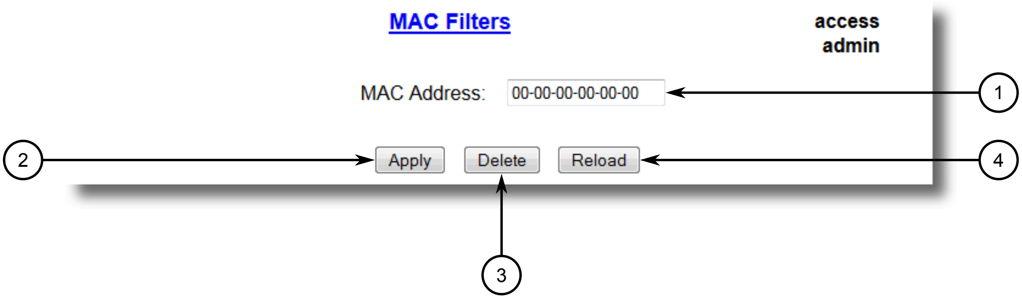
InsertRecord

MAC Address
00-00-02-00-03-04

① InsertRecord

Figure 9.18 MAC Filters Table

2. Click **InsertRecord**. The **MAC Filters** form appears.



① MAC Address Box
② Apply Button
③ Delete Button
④ Reload Button

Figure 9.19 MAC Filters Form

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

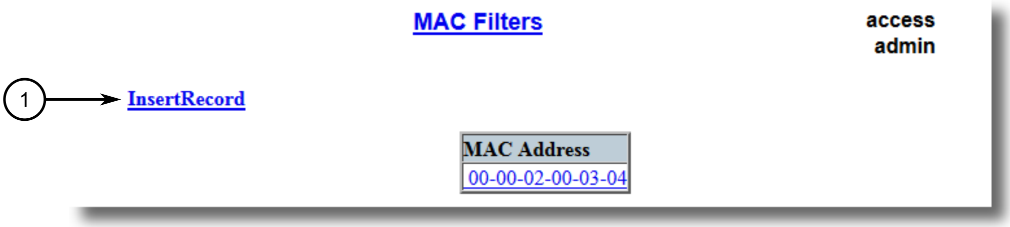
Parameter	Description
`MAC Address`	**Synopsis:** ##-##-##-##-##-## where ## ranges 0 to FF **Default:** 00-00-00-00-00-00 List of MAC address of wireless units which are part of MAC filter.

4. Click **Apply**.

9.1.10.4 Deleting a MAC Address

To delete a MAC address, do the following:

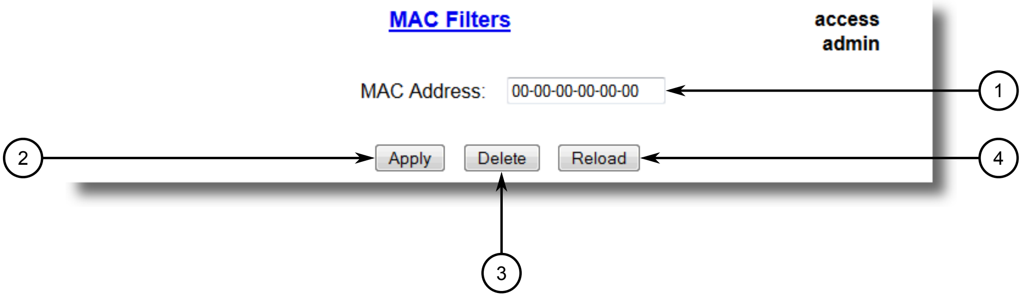
1. Navigate to ***WLAN Interface » MAC Filtering » MAC Filters***. The **MAC Filters** table appears.



① InsertRecord

Figure 9.20 MAC Filters Table

2. Select the MAC address from the table. The **MAC Filters** form appears.



① MAC Address Box
② Apply Button
③ Delete Button
④ Reload Button

Figure 9.21 MAC Filters Form

3. Click **Delete**.

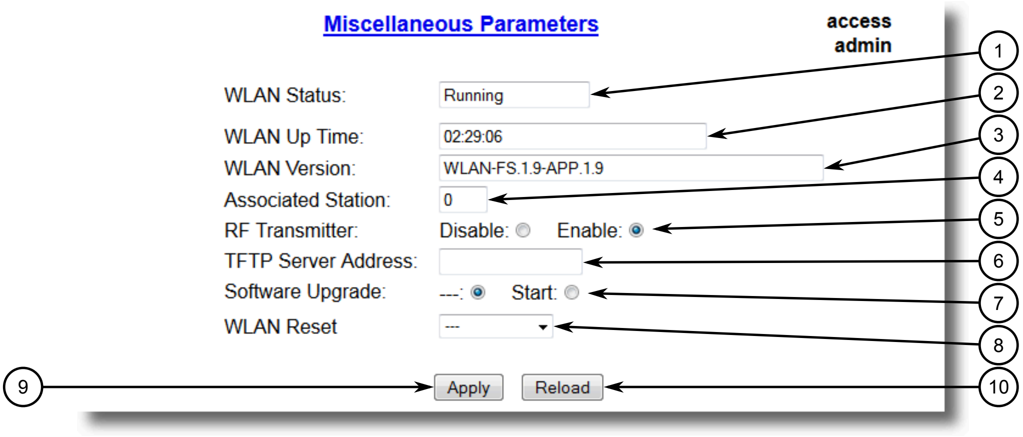
9.1.11 Upgrading Wireless LAN Software

To upgrade the firmware for the wireless LAN, do the following:

Note
The duration of the software upgrade process is approximately 15 minutes.

1. Make sure the new firmware is available on a TFTP server accessible by the device.

2. Navigate to ***WLAN Interface » Miscellaneous Parameters***. The **Miscellaneous Parameters** form appears.



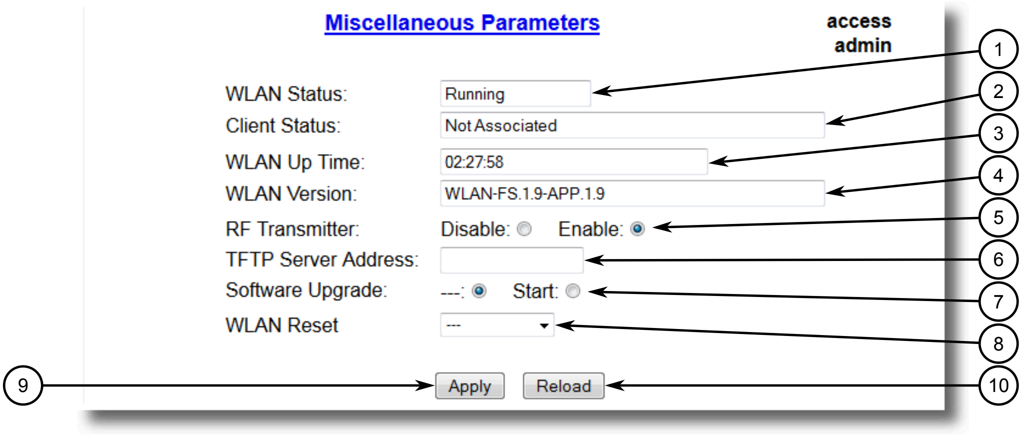
Miscellaneous Parameters

access
admin

WLAN Status: Running
WLAN Up Time: 02:29:06
WLAN Version: WLAN-FS.1.9-APP.1.9
Associated Station: 0
RF Transmitter: Disable: ○ Enable: ●
TFTP Server Address:
Software Upgrade: ---: ● Start: ○
WLAN Reset ---

① WLAN Status Box
② WLAN Up Time Box
③ WLAN Version Box
④ Associated Station Box
⑤ RF Transmitter Options
⑥ TFTP Server Address Box
⑦ Software Upgrade Options
⑧ WLAN Reset List
⑨ Apply Button
⑩ Reload Button

Figure 9.22 Miscellaneous Parameters Form (Access Point Mode)



Miscellaneous Parameters

access
admin

WLAN Status: Running
Client Status: Not Associated
WLAN Up Time: 02:27:58
WLAN Version: WLAN-FS.1.9-APP.1.9
RF Transmitter: Disable: ○ Enable: ●
TFTP Server Address:
Software Upgrade: ---: ● Start: ○
WLAN Reset ---

① WLAN Status Box
② Client Status Box
③ WLAN Up Time Box
④ WLAN Version Box
⑤ RF Transmitter Options
⑥ TFTP Server Address Box
⑦ Software Upgrade Options

⑧ WLAN Reset List
⑨ Apply Button
⑩ Reload Button

Figure 9.23 Miscellaneous Parameters Form (Client/Bridge or Client/IP Bridge)

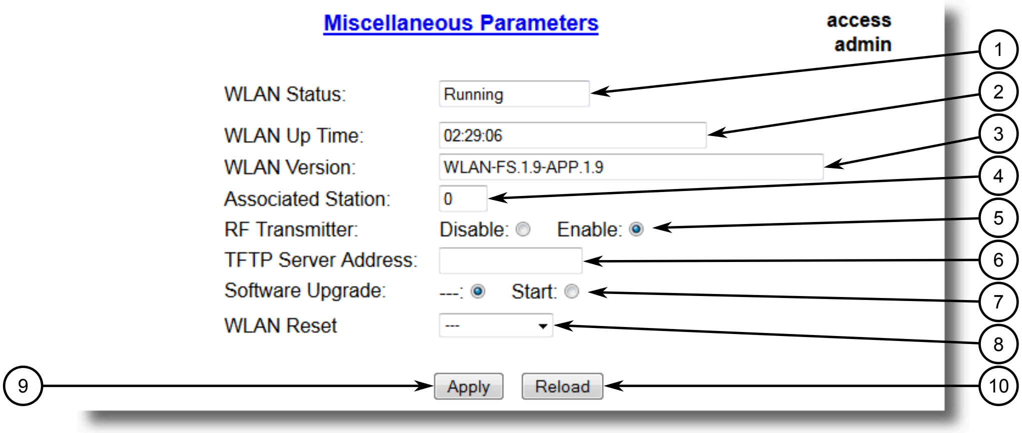
3. Under **TFTP Server Address**, specify the IP address for the TFTP server where the new firmware version is located.
4. Under **Software Upgrade**, select **Start**.
5. Click **Apply**. The software upgrade process begins.

9.1.12 Resetting/Restarting the Wireless LAN

The wireless LAN must be reset/restarted to apply configuration changes. This can be done after one or several parameters are modified.

To reset/restart the wireless LAN, do the following:

1. Navigate to ***WLAN Interface » Miscellaneous Parameters***. The **Miscellaneous Parameters** form appears.



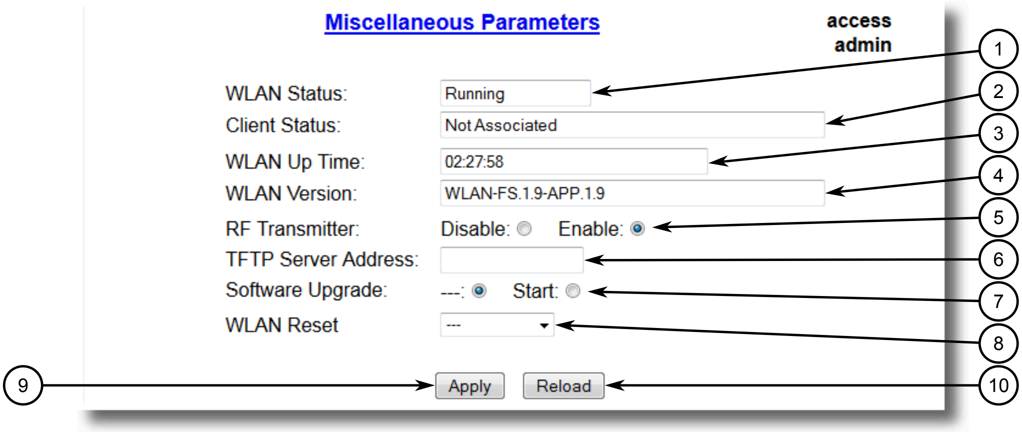
Miscellaneous Parameters

access
admin

WLAN Status: Running
WLAN Up Time: 02:29:06
WLAN Version: WLAN-FS.1.9-APP.1.9
Associated Station: 0
RF Transmitter: Disable: ○ Enable: ●
TFTP Server Address:
Software Upgrade: ---: ● Start: ○
WLAN Reset: ---

① WLAN Status Box
② WLAN Up Time Box
③ WLAN Version Box
④ Associated Station Box
⑤ RF Transmitter Options
⑥ TFTP Server Address Box
⑦ Software Upgrade Options
⑧ WLAN Reset List
⑨ Apply Button
⑩ Reload Button

Figure 9.24 Miscellaneous Parameters Form (Access Point Mode)



Miscellaneous Parameters

access
admin

WLAN Status: Running
Client Status: Not Associated
WLAN Up Time: 02:27:58
WLAN Version: WLAN-FS.1.9-APP.1.9
RF Transmitter: Disable: ○ Enable: ●
TFTP Server Address:
Software Upgrade: ---: ● Start: ○
WLAN Reset: ---

① WLAN Status Box
② Client Status Box
③ WLAN Up Time Box
④ WLAN Version Box
⑤ RF Transmitter Options

⑥ TFTP Server Address Box
⑦ Software Upgrade Options
⑧ WLAN Reset List
⑨ Apply Button
⑩ Reload Button

Figure 9.25 Miscellaneous Parameters Form (Client/Bridge or Client/IP Bridge)

2. Under the **WLAN Reset** list, select either `Full reset` or `Quick reset`.

   Note
   A quick reset is often sufficient for applying configuration changes.

   - *`Full reset`* resets both the Radio Frequency (RF) and Ethernet interfaces of the wireless LAN. The duration of a full reset is approximately 70 seconds.
   - *`Quick reset`* resets only the Radio Frequency (RF) interface of the wireless LAN. The duration of a quick reset is approximately 10 seconds.

3. Click **Apply**. The wireless LAN begins to reset/restart. When the wireless LAN is running again, the **WLAN Status** box will indicate *`Running`*.

10 Traffic Control and Classification

Use the traffic control and classification subsystems to control the flow of data packets to connected network interfaces.

10.1 Managing Classes of Service

Classes of Service (CoS) provides the ability to expedite the transmission of certain frames and port traffic over others. The CoS of a frame can be set to Normal, Medium, High, or Critical. By default, other than the control frames, RUGGEDCOM ROS enforces Normal CoS for all incoming traffic received without a priority tag.

> ⚠ **NOTICE**
>
> Use the highest supported CoS with caution, as it is always used by the switch for handling network management traffic, such as RSTP BPDUs.
>
> If this CoS is used for regular network traffic, upon traffic bursts, it may result in the loss of some network management frames, which in turn may result in the loss of connectivity over the network.

The process of controlling traffic based on CoS occurs over two phases:

1. **Inspection Phase**

   In the inspection phase, the CoS priority of a received frame is determined from either:

   - A specific CoS based upon the source and destination MAC address (as set in the Static MAC Address Table)
   - The priority field in the IEEE 802.1Q tags
   - The Differentiated Services Code Point (DSCP) component of the Type Of Service (TOS) field in the IP header, 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.

   Note
   For information on how to configure the **Inspect TOS** parameter, refer to "Configuring Classes of Service for Specific Ethernet Ports (Page 261)".

   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 IEEE 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 an IP frame and **Inspect TOS** is enabled in RUGGEDCOM ROS, the CoS is determined from the DSCP field. If the frame is not an IP frame or **Inspect TOS** is disabled, the default CoS for the port is used.

After inspection, the frame is forwarded to the egress port for transmission.

2. **Forwarding Phase**

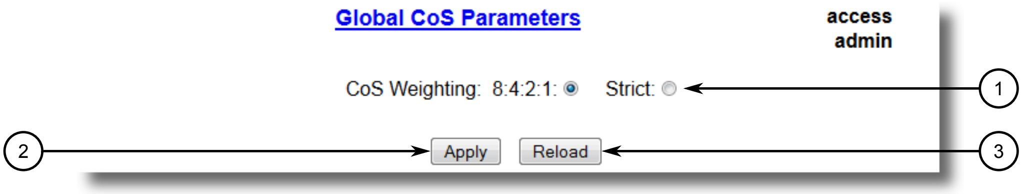
   Once the CoS of the frame is determined, the frame is forwarded to the egress port, where it is collected into one of the priority queues according to the assigned CoS.

   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, lower CoS frames can be transmitted only after all higher CoS frames have been serviced.

10.1.1 Configuring Classes of Service Globally

To configure global settings for Classes of Service (CoS), do the following:

1. Navigate to ***Classes of Service » Configure Global CoS Parameters***. The **Global CoS Parameters** form appears.



Global CoS Parameters

access
admin

CoS Weighting: 8:4:2:1: ● Strict: ○

① CoS Weighting Options
② Apply Button
③ Reload Button

Figure 10.1 Global CoS Parameters Form

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

Parameter	Description
`CoS Weighting`	**Synopsis:** [8:4:2:1 | Strict] **Default:** 8:4:2:1 During traffic bursts, frames queued in the switch pending transmission on a port may have different CoS priorities. This parameter specifies weighting algorithm for transmitting different priority CoS frames. Examples: • 8 –

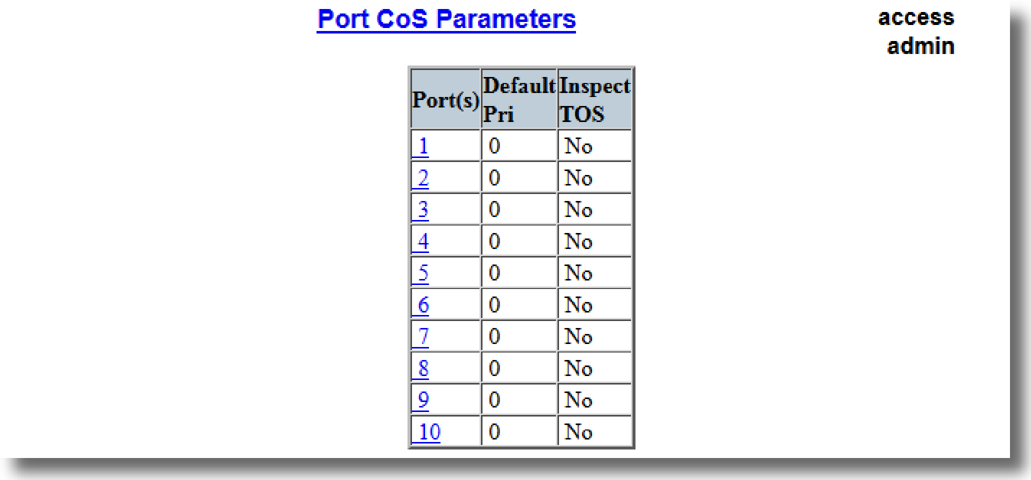
Parameter	Description
	- Strict – lower priority CoS frames will be only transmitted after all higher priority CoS frames have been transmitted

3. Click **Apply**.
4. If necessary, configure CoS mapping based on either the IEEE 802.1p priority or Differentiated Services (DS) field set in the IP header for each packet. For more information, refer to "Configuring Priority to CoS Mapping (Page 262)" or "Configuring DSCP to CoS Mapping (Page 264)".

10.1.2 Configuring Classes of Service for Specific Ethernet Ports

To configure Classes of Service (CoS) for one or more Ethernet ports, do the following:

1. Navigate to ***Classes of Service » Configure Port CoS Parameters***. The **Port CoS Parameters** table appears.



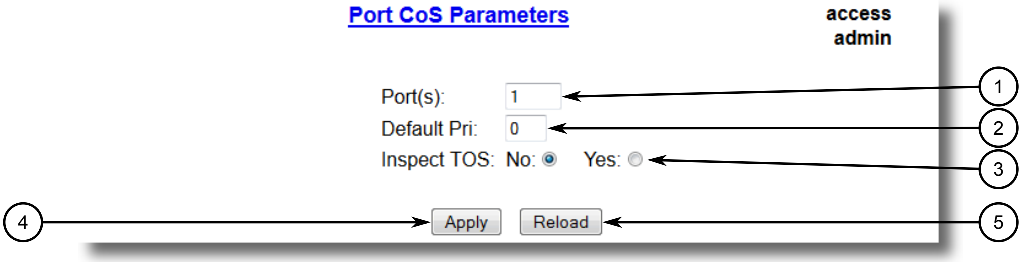
Port CoS Parameters

access
admin

Port(s)	Default Pri	Inspect TOS
1	0	No
2	0	No
3	0	No
4	0	No
5	0	No
6	0	No
7	0	No
8	0	No
9	0	No
10	0	No

Figure 10.2 Port CoS Parameters Table

2. Select an Ethernet port. The **Port CoS Parameters** form appears.


Port CoS Parameters

Port(s): 1
Default Pri: 0
Inspect TOS: No: ● Yes: ○

① Port(s) Box
② Default Pri Box
③ Inspect TOS Options
④ Apply Button
⑤ Reload Button

Figure 10.3 Port CoS Parameters Form

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

Parameter	Description
`Port(s)`	**Synopsis:** Any combination of numbers valid for this parameter The port number as seen on the front plate silkscreen of the switch (or a list of ports, if aggregated in a port trunk).
`Default Pri`	**Synopsis:** An integer between 0 and 7 **Default:** 0 This parameter allows to prioritize frames received on this port that are not prioritized based on the frames contents (e.g. priority field in the VLAN tag, DiffServ field in the IP header, prioritized MAC address).
`Inspect TOS`	**Synopsis:** [No | Yes] **Default:** No This parameters 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.

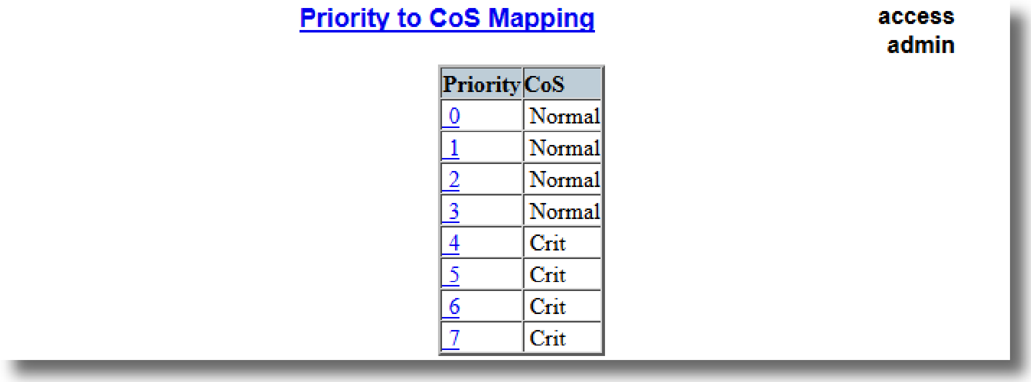
4. Click **Apply**.

10.1.3 Configuring Priority to CoS Mapping

Frames received untagged can be automatically assigned a CoS based on their priority level.

To map a priority level to a CoS, do the following:

1. Navigate to ***Classes of Service » Configure Priority to CoS Mapping***. The **Priority to CoS Mapping** table appears.



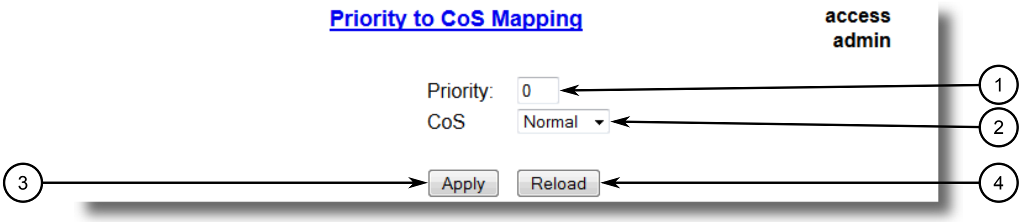
Priority to CoS Mapping

access
admin

Priority	CoS
0	Normal
1	Normal
2	Normal
3	Normal
4	Crit
5	Crit
6	Crit
7	Crit

Figure 10.4 Priority to CoS Mapping Table

2. Select a priority level. The **Priority to CoS Mapping** form appears.



Priority to CoS Mapping

access
admin

Priority: 0
CoS: Normal

① Priority Box
② CoS List
③ Apply Button
④ Reload Button

Figure 10.5 Priority to CoS Mapping Form

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

Parameter	Description
`Priority`	**Synopsis:** An integer between 0 and 7 **Default:** 0 Value of the IEEE 802.1p priority.
`CoS`	**Synopsis:** [Normal | Medium | High | Crit] **Default:** Normal CoS assigned to received tagged frames with the specified IEEE 802.1p priority value.

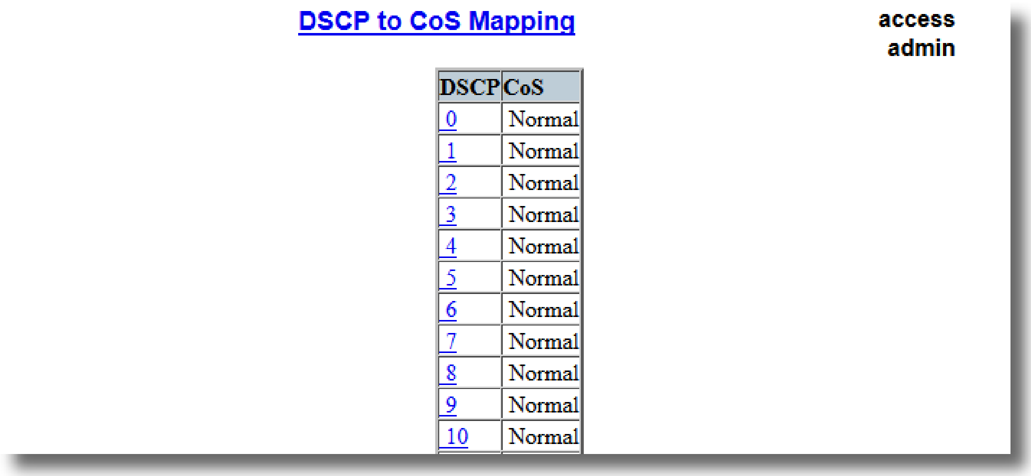
4. Click **Apply**.

10.1.4 Configuring DSCP to CoS Mapping

Mapping CoS to the Differentiated Services (DS) field set in the IP header for each packet is done by defining Differentiated Services Code Points (DSCPs) in the CoS configuration.

To map a DSCP to a Class of Service, do the following:

1. Navigate to ***Classes of Service » Configure DSCP to CoS Mapping***. The **DSCP to CoS Mapping** table appears.



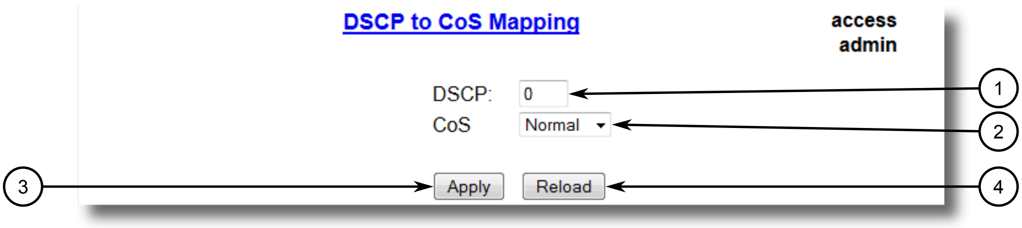
DSCP to CoS Mapping

access
admin

DSCP	CoS
0	Normal
1	Normal
2	Normal
3	Normal
4	Normal
5	Normal
6	Normal
7	Normal
8	Normal
9	Normal
10	Normal

Figure 10.6 DSCP to CoS Mapping Table

2. Select a DSCP level. The **DSCP to CoS Mapping** form appears.



DSCP to CoS Mapping

access
admin

DSCP: 0
CoS: Normal

① DSCP Box
② CoS List
③ Apply Button
④ Reload Button

Figure 10.7 DSCP to CoS Mapping Form

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

Parameter	Description
`DSCP`	**Synopsis:** An integer between 0 and 63 **Default:** 0 Differentiated Services Code Point (DSCP) – a value of the 6 bit DiffServ field in the Type-Of-Service (TOS) field of the IP header.

Parameter	Description
`CoS`	**Synopsis:** [Normal | Medium | High | Crit] **Default:** Normal Class of Service assigned to received frames with the specified DSCP.

4. Click **Apply**.
5. Configure the CoS parameters on select switched Ethernet ports as needed. For more information, refer to "Configuring Classes of Service for Specific Ethernet Ports (Page 261)".

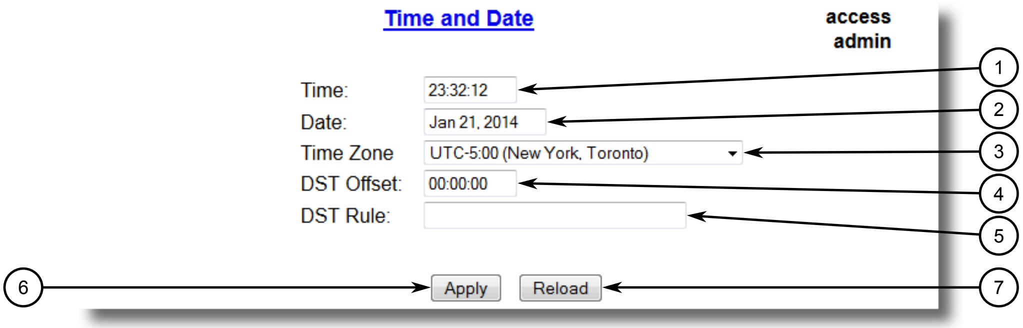
11 Time Services

This chapter describes the time-keeping and time synchronization features in RUGGEDCOM ROS.

11.1 Configuring the Time and Date

To set the time, date and other time-keeping related parameters, do the following:

1. Navigate to ***Administration » System Time Manager » Configure Time and Date***. The **Time and Date** form appears.



Time and Date

access
admin

Time: 23:32:12
Date: Jan 21, 2014
Time Zone: UTC-5:00 (New York, Toronto)
DST Offset: 00:00:00
DST Rule:

① Time
② Date
③ Time Zone
④ DST Offset
⑤ DST Rule
⑥ Apply Button
⑦ Reload Button

Figure 11.1 Time and Date Form

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

Parameter	Description
`Time`	**Synopsis:** HH:MM:SS This parameter allows for both the viewing and setting of the local time.
`Date`	**Synopsis:** MMM DD, YYYY This parameter allows for both the viewing and setting of the local date.

Parameter	Description
`Time Zone`	**Synopsis:** [UTC-12:00 (Eniwetok, Kwajalein) | UTC-11:00 (Midway Island, Samoa) | UTC-10:00 (Hawaii) | UTC-9:00 (Alaska) | UTC-8:00 (Los Angeles, Vancouver) | UTC-7:00 (Calgary, Denver) | UTC-6:00 (Chicago, Mexico City) | UTC-5:00 (New York, Toronto) | UTC-4:30 (Caracas) | UTC-4:00 (Santiago) | UTC-3:30 (Newfoundland) | UTC-3:00 (Brasilia, Buenos Aires) | UTC-2:00 (Mid Atlantic) | UTC-1:00 (Azores) | UTC-0:00 (Lisbon, London) | UTC+1:00 (Berlin, Paris, Rome) | ...] **Default:** UTC-5:00 (New York, Toronto) This setting allows for the conversion of UTC (Universal Coordinated Time) to local time.
`DST Offset`	**Synopsis:** HH:MM:SS **Default:** 00:00:00 This parameter specifies the amount of time to be shifted forward/backward when DST begins and ends. For example for most part of USA and Canada, DST time shift is 1 hour (01:00:00) forward when DST begins and 1 hour backward when DST ends.
`DST Rule`	**Synopsis:** mm.n.d/HH:MM:SS mm.n.d/HH:MM:SS This parameter specifies a rule for time and date when the transition between Standard and Daylight Saving Time occurs. • mm – Month of the year (01 – January, 12 – December) • n – nth d-day in the month (1 – 1st d-day, 5 – 5th/last d-day) • d – day of the week (0 – Sunday, 6 – Saturday) • HH – hour of the day (0 – 24) • MM – minute of the hour (0 – 59) • SS – second of the minute (0 – 59) Example: The following rule applies in most part of USA and Canada: `03.2.0/02:00:00 11.1.0/02:00:00` DST begins on March's 2nd Sunday at 2:00am. DST ends on November's 1st Sunday at 2:00am.

11.2 Managing NTP

RUGGEDCOM ROS may be configured to refer periodically to a specified NTP server to correct any accumulated drift in the on-board clock. RUGGEDCOM ROS will also serve time via the Simple Network Time Protocol (SNTP) to hosts that request it.

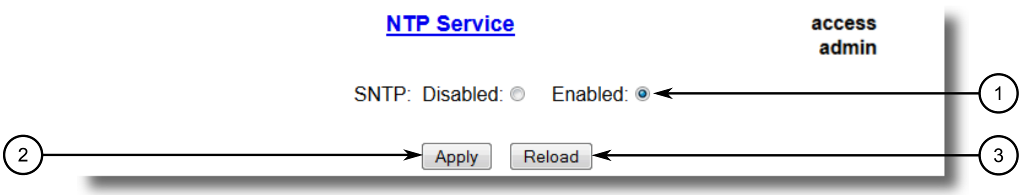
Two NTP servers (primary and backup) may be configured for the device. The primary server is contacted first for each attempt to update the system time. If the primary server fails to respond, the backup server is contacted. If either the primary or backup server fails to respond, an alarm is raised.

11.2.1 Enabling/Disabling NTP Service

To enable or disable NTP Service, do the following:

Note
If the device is running as an NTP server, NTP service must be enabled.

1. Navigate to ***Administration » System Time Manager » Configure NTP » Configure NTP Service***. The **SNTP Parameters** form appears.



SNTP: Disabled: ○ Enabled: ●

① SNTP Options
② Apply Button
③ Reload Button

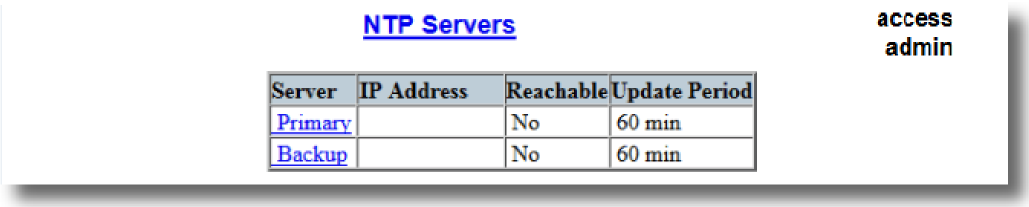
Figure 11.2 SNTP Parameters Form

2. Select **Enabled** to enable SNTP, or select **Disabled** to disable SNTP.
3. Click **Apply**.

11.2.2 Configuring NTP Servers

To configure either the primary or backup NTP server, do the following:

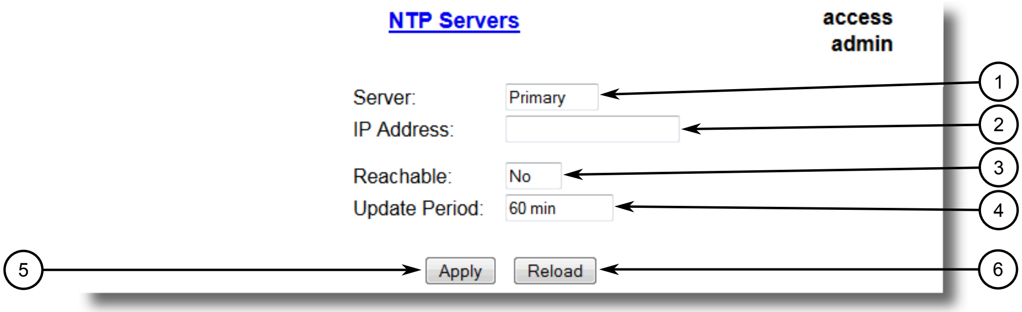
1. Navigate to ***Administration » System Time Manager » Configure NTP » Configure NTP Servers***. The **NTP Servers** table appears.



Server	IP Address	Reachable	Update Period
Primary		No	60 min
Backup		No	60 min

Figure 11.3 NTP Servers Table

2. Select either **Primary** or **Backup**. The **NTP Servers** form appears.



NTP Servers

access
admin

Server: Primary

IP Address:

Reachable: No

Update Period: 60 min

① Server Box
② IP Address Box
③ Reachable Box
④ Update Period Box
⑤ Apply Button
⑥ Reload Button

Figure 11.4 NTP Servers Form

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

Parameter	Description
`Server`	**Synopsis:** A string 8 characters long **Default:** Primary This field tells whether this configuration is for a Primary or a Backup Server.
`IP Address`	**Synopsis:** ###.###.###.### where ### ranges from 0 to 255 The Server IP Address.
`Reachable`	**Synopsis:** [No | Yes] Shows the status of the server.
`Update Period`	**Synopsis:** An integer between 1 and 1440 **Default:** 60 Determines how frequently the (S)NTP server is polled for a time update.If the server cannot be reached in three attempts that are made at one minute intervals an alarm is generated.

4. Click **Apply**.

12 Network Discovery and Management

RUGGEDCOM ROS supports the following protocols for automatic network discovery, monitoring and device management:

- **RUGGEDCOM Discovery Protocol (RCDP)**

  Use RCDP to discover RUGGEDCOM ROS-based devices over a Layer 2 network.

- **Link Layer Device Protocol (LLDP)**

  Use LLDP to broadcast the device's network capabilities and configuration to other devices on the network, as well as receive broadcasts from other devices.

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

  Use SNMP to notify select users or groups of certain events that happen during the operation of the device, such as changes to network topology, link state, spanning tree root, etc.

12.1 Enabling/Disabling RCDP

RUGGEDCOM ROS supports the RUGGEDCOM Discovery Protocol (RCDP). RCDP supports the deployment of RUGGEDCOM ROS -based devices that have not been configured since leaving the factory. RUGGEDCOM ROS devices that have not been configured all have the default IP (Layer 3) address. Connecting more than one of them on a Layer 2 network means that one cannot use standard IP-based configuration tools to configure them. The behavior of IP-based mechanisms such as the web interface, SSH, telnet, or SNMP will all be undefined.

Since RCDP operates at Layer 2, it can be used to reliably and unambiguously address multiple devices even though they may share the same IP configuration.

Siemens 's RUGGEDCOM EXPLORER is a lightweight, standalone Windows application that supports RCDP. It is capable of discovering, identifying and performing basic configuration of RUGGEDCOM ROS-based devices via RCDP. The features supported by RCDP include:

- Discovery of RUGGEDCOM ROS-based devices over a Layer 2 network.
- Retrieval of basic network configuration, RUGGEDCOM ROS version, order code, and serial number.
- Control of device LEDs for easy physical identification.
- Configuration of basic identification, networking, and authentication parameters.

For security reasons, RUGGEDCOM EXPLORER will attempt to disable RCDP or set all devices to *Get Only* mode when EXPLORER is shut down.

Additionally, RUGGEDCOM EXPLORER will set all devices to *Get Only* mode in the following conditions:

- 60 minutes after the last RCDP frame has been received.
- The IP address, subnet, gateway or any passwords are changed for the device via SSH, RSH, Telnet, serial console or SNMP.

⚠ **NOTICE**

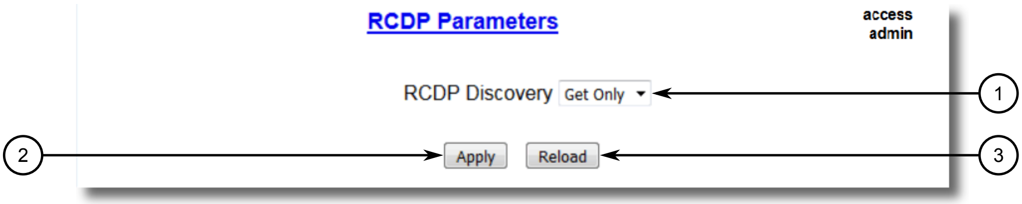
For increased security, Siemens recommends disabling RCDP if it is not intended for use.

Note
RCDP is not compatible with VLAN-based network configurations. For correct operation of RUGGEDCOM EXPLORER, no VLANs (tagged or untagged) must be configured. All VLAN configuration items must be at their default settings.

Note
RUGGEDCOM ROS responds to RCDP requests only. It does not under any circumstances initiate any RCDP-based communication.

To enable or disable RCDP, do the following:

1. Navigate to ***Network Discovery » RuggedCom Discovery Protocol » Configure RCDP Parameters***. The **RCDP Parameters** form appears.



① RCDP Discovery List
② Apply Button
③ Reload Button

Figure 12.1 RCDP Parameters Form

2. Under **RCDP Discovery**, select one of the following options:

   ⚠ **NOTICE**

   The `Enabled` option is only available for devices loaded with factory default settings. This option will not be selectable once a device has been configured.

   - `Disabled` – Disables read and write access
   - `Get Only` – Enables only read access
   - `Enabled` – Enables read and write access

3. Click **Apply**.

12.2 Managing LLDP

The Link Layer Discovery Protocol (LLDP) defined by IEEE 802.11AB allows a networked device to advertise its own basic networking capabilities and configuration.

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.

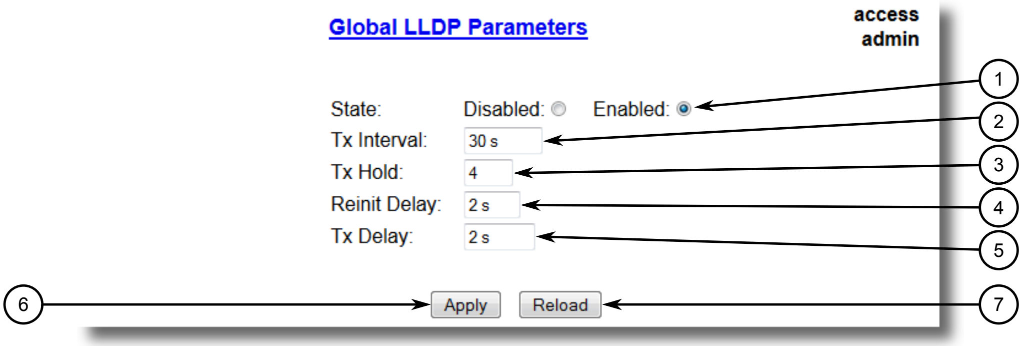
LLDP agent operation is typically implemented as two modules: the LLDP transmit module and LLDP receive module. The LLDP transmit module, when enabled, sends the local device's information at regular intervals, in IEEE 802.1AB standard format. Whenever the transmit module is disabled, it transmits an LLDPDU (LLDP data unit) with a time-to-live (TTL) type-length-value (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 remote devices' information 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.

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.

12.2.1 Configuring LLDP Globally

To configure the global settings for LLDP, do the following:

1. Navigate to ***Network Discovery » Link Layer Discovery Protocol » Configure Global LLDP Parameters***. The **Global LLDP Parameters** form appears.



Global LLDP Parameters

access
admin

State: Disabled: ○ Enabled: ●

Tx Interval: 30 s

Tx Hold: 4

Reinit Delay: 2 s

Tx Delay: 2 s

① State Options
② Tx Interval Box
③ Tx Hold Box
④ Reinit Delay Box
⑤ Tx Delay Box
⑥ Apply Button
⑦ Reload Button

Figure 12.2 Global LLDP Parameters Form

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

Parameter	Description
`State`	**Synopsis:** [Disabled | Enabled] **Default:** Enabled Enables LLDP protocol. Note that LLDP is enabled on a port when LLDP is enabled globally and along with enabling per port setting in Port LLDP Parameters menu.
`Tx Interval`	**Synopsis:** An integer between 5 and 32768 **Default:** 30 The interval at which LLDP frames are transmitted on behalf of this LLDP agent.
`Tx Hold`	**Synopsis:** An integer between 2 and 10 **Default:** 4 The multiplier of the Tx Interval parameter that determines the actual time-to-live (TTL) value used in a LLDPDU. The actual TTL value can be expressed by the following formula: `TTL = MIN(65535, (Tx Interval * Tx Hold)`

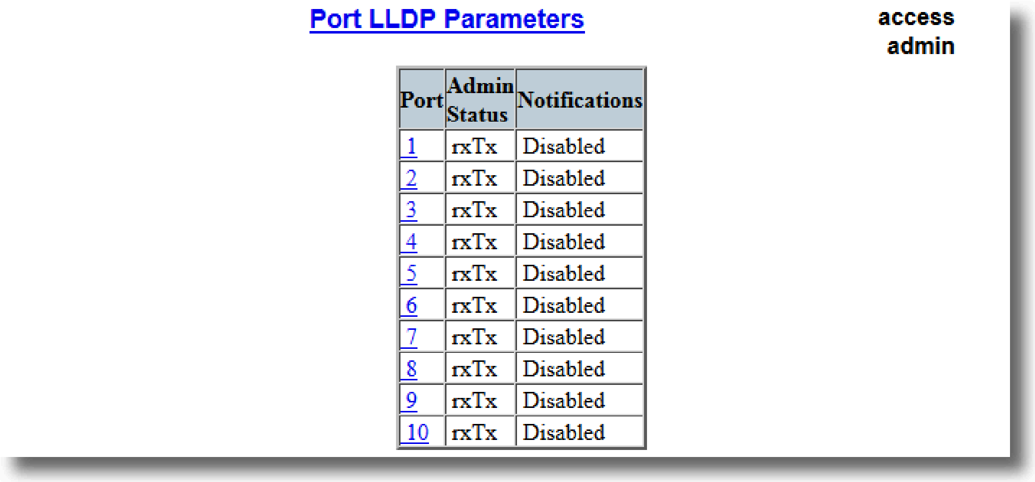
Parameter	Description
`Reinit Delay`	**Synopsis:** An integer between 1 and 10 **Default:** 2 The delay in seconds from when the value of Admin Status parameter of a particular port becomes 'Disbled' until re-initialization will be lattempted.
`Tx Delay`	**Synopsis:** An integer between 1 and 8192 **Default:** 2 The delay in seconds between successive LLDP frame transmissions initiated by value or status changed. The recommended value is set by the following formula: `1 <= txDelay <= (0.25 * Tx Interval)`

3. Click **Apply**.

12.2.2 Configuring LLDP for an Ethernet Port

To configure LLDP for a specific Ethernet Port, do the following:

1. Navigate to ***Network Discovery » Link Layer Discovery Protocol » Configure Port LLDP Parameters***. The **Port LLDP Parameters** table appears.



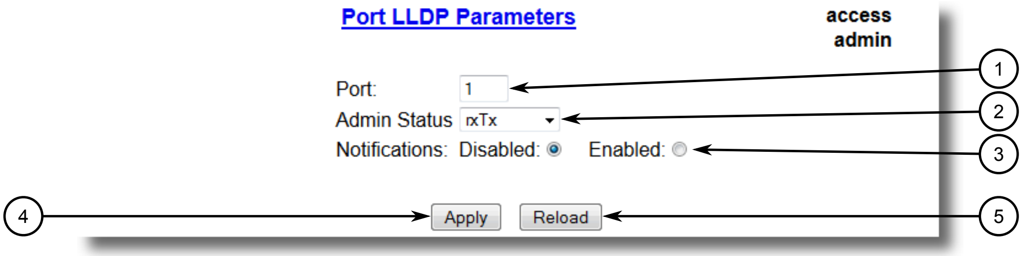
Port LLDP Parameters

access
admin

Port	Admin Status	Notifications
1	rxTx	Disabled
2	rxTx	Disabled
3	rxTx	Disabled
4	rxTx	Disabled
5	rxTx	Disabled
6	rxTx	Disabled
7	rxTx	Disabled
8	rxTx	Disabled
9	rxTx	Disabled
10	rxTx	Disabled

Figure 12.3 Port LLDP Parameters Table

2. Select a port. The **Port LLDP Parameters** form appears.



① Port Box
② Admin Status List
③ Notifications Options
④ Apply Button
⑤ Reload Button

Figure 12.4 Port LLDP Parameters Form

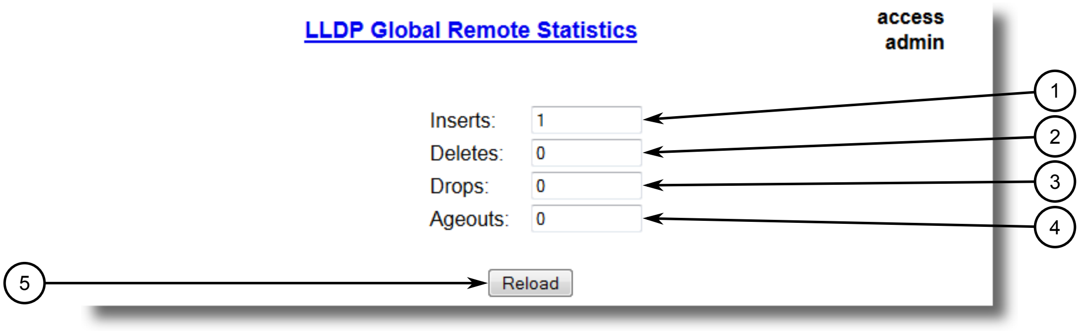
3. Configure the following parameter(s) as required:

Parameter	Description
`Port`	**Synopsis:** 1 to maximum port number **Default:** 1 The port number as seen on the front plate silkscreen of the switch.
`Admin Status`	**Synopsis:** [rxTx | txOnly | rxOnly | Disabled] **Default:** rxTx 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. disabled: the local LLDP agent can neither transmit or receive LLDP frames.
`Notifications`	**Synopsis:** [Disabled | Enabled] **Default:** Disabled Disabling notifications will prevent sending notifications and generating alarms for particular port from the LLDP agent.

4. Click **Apply**.

12.2.3 Viewing Global Statistics and Advertised System Information

To view global statistics for LLDP and the system information that is advertised to neighbors, navigate to ***Network Discovery » Link Layer Discovery Protocol » View LLDP Global Remote Statistics***. The **LLDP Global Remote Statistics** form appears.



LLDP Global Remote Statistics

Inserts: 1
Deletes: 0
Drops: 0
Ageouts: 0

① Inserts Box
② Deletes Box
③ Drops Box
④ Ageouts Box
⑤ Reload Button

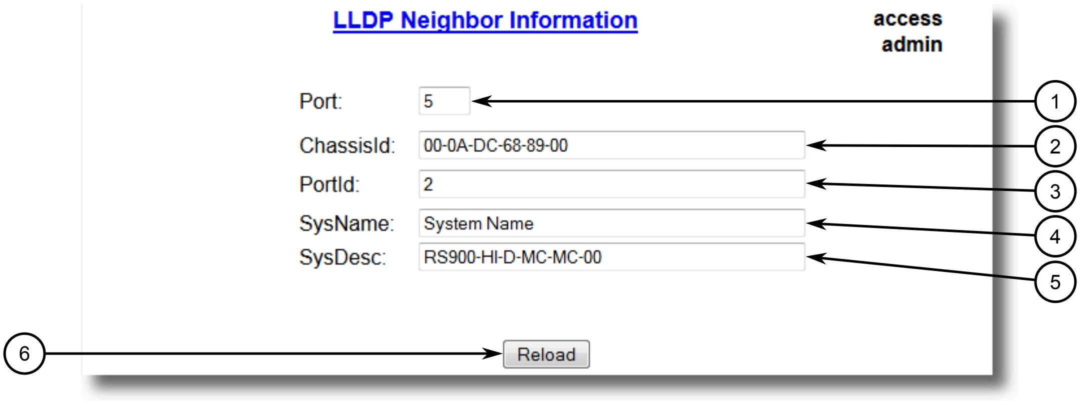
Figure 12.5 LLDP Global Remote Statistics Form

This form displays the following information:

Parameter	Description
`Inserts`	**Synopsis:** An integer between 0 and 4294967295 A number of times the entry in LLDP Neighbor Information Table was inserted.
`Deletes`	**Synopsis:** An integer between 0 and 4294967295 A number of times the entry in LLDP Neighbor Information Table was deleted.
`Drops`	**Synopsis:** An integer between 0 and 4294967295 A number of times an entry was deleted from LLDP Neighbor Information Table because the information timeliness interval has expired.
`Ageouts`	**Synopsis:** An integer between 0 and 4294967295 A counter of all TLVs discarded.

12.2.4 Viewing Statistics for LLDP Neighbors

To view statistics for LLDP neighbors, navigate to ***Network Discovery » Link Layer Discovery Protocol » View LLDP Neighbor Information***. The **LLDP Neighbor Information** table appears.



Port: 5

ChassisId: 00-0A-DC-68-89-00

PortId: 2

SysName: System Name

SysDesc: RS900-HI-D-MC-MC-00

① Port Box
② ChassisId Box
③ PortId Box
④ SysName Box
⑤ SysDesc Box
⑥ Reload Button

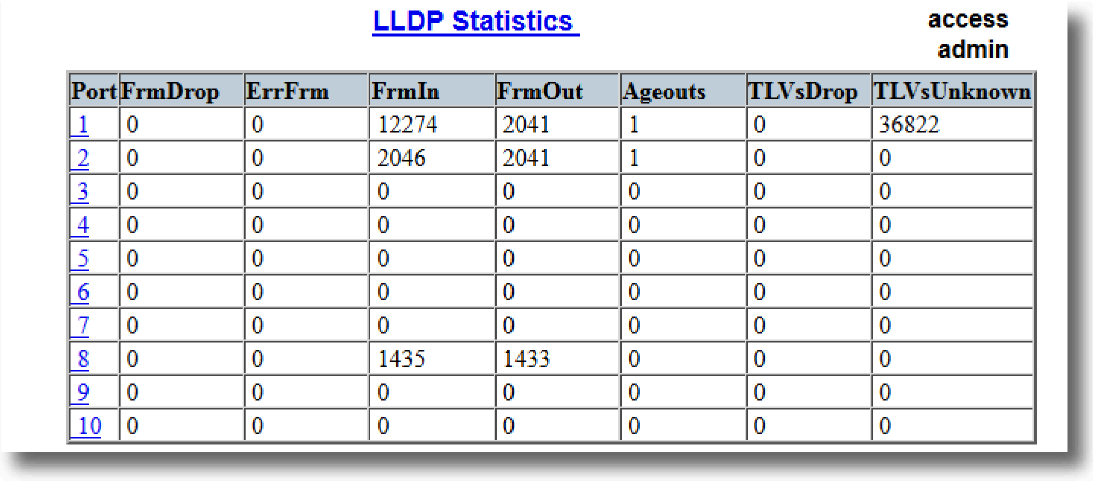
Figure 12.6 LLDP Neighbor Information Table

This form displays the following information:

Parameter	Description
`Port`	**Synopsis:** 1 to maximum port number The local port associated with this entry.
`ChassisId`	**Synopsis:** A string 45 characters long Chassis Id information received from remote LLDP agent.
`PortId`	**Synopsis:** A string 45 characters long Port Id information received from remote LLDP agent.
`SysName`	**Synopsis:** A string 45 characters long System Name information received from remote LLDP agent.
`SysDesc`	**Synopsis:** A string 45 characters long System Descriptor information received from remote LLDP agent.

12.2.5 Viewing Statistics for LLDP Ports

To view statistics for LLDP ports, navigate to ***Network Discovery » Link Layer Discovery Protocol » View LLDP Statistics***. The **LLDP Statistics** table appears.



LLDP Statistics

access
admin

Port	FrmDrop	ErrFrm	FrmIn	FrmOut	Ageouts	TLVsDrop	TLVsUnknown
1	0	0	12274	2041	1	0	36822
2	0	0	2046	2041	1	0	0
3	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0
8	0	0	1435	1433	0	0	0
9	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0

Figure 12.7 LLDP Statistics Table

This table displays the following information:

Parameter	Description
Port	**Synopsis:** 1 to maximum port number The port number as seen on the front plate silkscreen of the switch.
FrmDrop	**Synopsis:** An integer between 0 and 4294967295 A counter of all LLDP frames discarded.
ErrFrm	**Synopsis:** An integer between 0 and 4294967295 A counter of all LLDPDUs received with detectable errors.
FrmIn	**Synopsis:** An integer between 0 and 4294967295 A counter of all LLDPDUs received.
FrmOut	**Synopsis:** An integer between 0 and 4294967295 A counter of all LLDPDUs transmitted.
Ageouts	**Synopsis:** An integer between 0 and 4294967295 A counter of the times that a neighbor's information has been deleted from the LLDP remote system MIB because the txinfoTTL timer has expired.
TLVsDrop	**Synopsis:** An integer between 0 and 4294967295 A counter of all TLVs discarded.
TLVsUnknown	**Synopsis:** An integer between 0 and 4294967295 A counter of all TLVs received on the port that are not recognized by the LLDP local agent.

12.3 Managing SNMP

RUGGEDCOM ROS supports versions 1, 2 and 3 of the Simple Network Management Protocol (SNMP), otherwise referred to as SNMPv1, SNMPv2c and SNMPv3 respectively. SNMPv3 provides secure access to the devices through a combination of authentication and packet encryption over the network. Security features for this protocol include:

Feature	Description
Message Integrity	Makes sure that a packet has not been tampered with in-transit.
Authentication	Determines if the message is from a valid source.
Encryption	Encrypts the contents of a packet to prevent it from being seen by an unauthorized source.

SNMPv3 provides security models and security levels. A security model is an authentication strategy setup 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 level will determine which security mechanism is employed when handling an SNMP packet.

Before configuring SNMPv3, 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 (i.e. reading, writing and creating notifications)
- A group determines the list of notifications its users can receive
- A group also defines the security model and security level for its users

For SNMPv1 and SNMPv2c, a community string can be configured. The string is mapped to the group and access level with a security name, which is configured as **User Name**.

12.3.1 SNMP Management Interface Base (MIB) Support

RUGGEDCOM ROS supports a variety of standard MIBs, proprietary RUGGEDCOM MIBs and Agent Capabilities MIBs, all for SNMP (Simple Network Management Protocol).

12.3.1.1 Supported Standard MIBs

RUGGEDCOM ROS supports the following standard MIBs:

Standard	MIB Name	Title
RFC 2578	SNMPv2-SMI	Structure of Management Information Version 2
RFC 2579	SNMPv2-TC	Textual conventions for SMIv2
RFC 2580	SNMPv2-CONF	Conformance statements for SMIv2
	IANAifType	Enumerated values of the ifType Object Defined ifTable defined in IF-MIB
RFC 1907	SNMPv2-MIB	Management Information Base for SNMPv2
RFC 2011	IP-MIB	SNMPv2 Management Information Base for Internet Protocol using SMIv2

Standard	MIB Name	Title
RFC 2012	TCP-MIB	SNMPv2 Management Information Base for the Transmission Control Protocol using SMIv2
RFC 2013	UDP-MIB	Management Information Base for the UDP using SMIv2
RFC 1659	RS-232-MIB	Definitions of managed objects for RS-232-like hardware devices
RFC 2863	IF-MIB	The Interface Group MIB
RFC 2819	RMON-MIB	Remote Network Monitoring (RMON) management Information base
RFC 4188	BRIDGE-MIB	Definitions of managed objects for bridges
RFC 4318	RSTP-MIB	Definitions of managed objects for bridges with Rapid Spanning Tree Protocol (RSTP)
RFC 3411	SNMP-FRAMEWORK-MIB	An architecture for describing Simple Network Management Protocol (SNMP) Management Framework
RFC 3414	SNMP-USER-BASED-SM-MIB	User-based Security Model (USM) for Version 3 of the Simple Network Management Protocol (SNMPv3)
RFC 3415	SNMP-VIEW-BASED-ACM-MIB	View-based Access Control Model (VACM) for the Simple Management Protocol (SNMP)
IEEE 802.3ad	IEEE8023-LAG-MIB	Management Information Base Module for link aggregation
IEEE 802.1AB-2005	LLDP-MIB	Management Information Base Module for LLDP configuration, statistics, local system data and remote systems data components
RFC 4363	Q-BRIDGE-MIB	Definitions of Managed Objects for Bridges with traffic classes, multicast filtering, and virtual LAN extensions
IEC-62439-2	IEC-62439-2-MIB	MRP node configuration MIB

12.3.1.2 Supported Proprietary RUGGEDCOM MIBs

RUGGEDCOM ROS supports the following proprietary RUGGEDCOM MIBs:

File Name	MIB Name	Description
RUGGEDCOM-MIB.mib	RUGGEDCOM-MIB	RUGGEDCOM enterprise SMI
RUGGEDCOM-TRAPS-MIB.mib	RUGGEDCOM-TRAPS-MIB	RUGGEDCOM traps definition
RUGGEDCOM-SYS-INFO-MIB.mib	RUGGEDCOM-SYS-INFO-MIB	General system information about RUGGEDCOM device
RUGGEDCOM-DOT11-MIB.mib	RUGGEDCOM-DOT11-MIB	Managemet for wireless interface on RUGGEDCOM device
RUGGEDCOM-POE-MIB.mib	RUGGEDCOM-POE-MIB	Management for PoE ports on RUGGEDCOM device
RUGGEDCOM-SERIAL-MIB.mib	RUGGEDCOM-SERIAL-MIB	Managemet for seral ports on RUGGEDCOM device
RUGGEDCOM-STP-MIB.mib	RUGGEDCOM-STP-MIB	Management for RSTP protocol

File Name	MIB Name	Description
RUGGEDCOM-NTP-MIB.mib	RUGGEDCOM-NTP-MIB	RUGGEDCOM proprietary MIB to control and monitor NTP module

12.3.1.3 Supported Agent Capabilities

RUGGEDCOM ROS supports the following agent capabilities for the SNMP agent:

Note
For information about agent capabilities for SNMPv2, refer to RFC 2580 [http://tools.ietf.org/html/rfc2580].

File Name	MIB Name	Supported MIB
RC-SNMPv2-MIB-AC.mib	RC-SNMPv2-MIB-AC	SNMPv2-MIB
RC-UDP-MIB-AC.mib	RC-UDP-MIB-AC	UDP-MIB
RC-TCP-MIB-AC.mib	RC-TCP-MIB-AC	TCP-MIB
RC-SNMP-USER-BASED-SM-MIB-AC.mib	RC-SNMP-USER-BASED-SM-MIB-AC	SNMP-USER-BASED-SM-MIB-AC
RC-SNMP-VIEW-BASED-ACM-MIB-AC.mib	RC-SNMP-VIEW-BASED-ACM-MIB-AC	SNMP-VIEW-BASED-ACM-MIB-AC
RC-IF-MIB-AC.mib	RC-IF-MIB-AC	IF-MIB
RC-BRIDGE-MIB-AC.mib	RC-BRIDGE-MIB-AC	BRIDGE-MIB
RC-RMON-MIB-AC.mib	RC-RMON-MIB-AC	RMON-MIB
RC-Q-BRIDGE-MIB-AC.mib	RC-Q-BRIDGE-MIB-AC	Q-BRIDGE-MIB
RC-IP-MIB-AC.mib	RC-IP-MIB-AC	IP-MIB
RC-LLDP-MIB-AC.mib	RC-LLDP-MIB-AC	LLDP-MIB
RC-LAG-MIB-AC.mib	RC-LAG-MIB-AC	IEEE8023-LAG-MIB
RC_RSTP-MIB-AC.mib	RC_RSTP-MIB-AC	RSTP-MIB
RC-RUGGEDCOM-DOT11-MIB-AC.mib	RC-RUGGEDCOM-DOT11-MIB-AC	RUGGEDCOM-DOT11- MIB
RC-RUGGEDCOM-POE-MIB-AC.mib	RC-RUGGEDCOM-POE-MIB-AC	RUGGEDCOM-POE-MIB
RC-RUGGEDCOM-STP-AC-MIB.mib	RC-RUGGEDCOM-STP-AC-MIB	RUGGEDCOM-STP-MIB
RC-RUGGEDCOM-SYS-INFO-MIB-AC.mib	RC-RUGGEDCOM-SYS-INFO-MIB-AC	RUGGEDCOM-SYS-INFO-MIB
RC-RUGGEDCOM-TRAPS-MIB-AC.mib	RC-RUGGEDCOM-TRAPS-MIB-AC	RUGGEDCOM-TRAPS-MIB
RUGGEDCOM_RS-232-MIB-AC.mib	RUGGEDCOM_RS-232-MIB-AC	RS-232-MIB
RC-RUGGEDCOM-SERIAL-MIB-AC.mib	RC-RUGGEDCOM-SERIAL-MIB-AC	RUGGEDCOM-SERIAL-MIB
RC-NTP-MIB-AC.mib	RC-NTP-MIB-AC	NTP-MIB

12.3.2 SNMP Traps

The device generates the following traps.

Standard Traps

Trap	MIB
linkDown	IF-MIB

Trap	MIB
linkUp	
authenticationFailure	SNMPv2-MIB
coldStart	
newRoot	BRIDGE-MIB
topologyChage	
risingAlarm	RMON-MIB
fallingAlarm	
lldpRemoteTablesChange	LLDP-MIB

Specific Proprietary Traps

Trap	MIB
genericTrap	RUGGEDCOM-TRAPS-MIB
powerSupplyTrap	
swUpgradeTrap	
cfgChangeTrap	
weakPasswordTrap	
defaultKeysTrap	
privKeySnmpV3UserUnknwnTrap	
serialCommBlockedTrap	
unknownRouteSerialProto	
incopatibleFpgaTrap	
clockMngrTrap	
ieee1588Trap	
rcLoopedBpduRcvd	
rcBpduGuardActivated	
rcGMRPCannotLearMoreAddresses	
rcGVRPCannotLearMoreAddresses	
rcMcastCpuFiltTblFull	
rcIgmpGroupMembershipTblFull	
rcIgmpMcastForwardTblFull	
rcMacAddressNotLearned	
excessLoginFailureTrap	
loginInfoTrap	
loginFailureTrap	
radiusServiceAvailableChange	
tacacsServiceAvailableChange	
rcDeviceError	
rcPortSecurityViolatedTrap	
rcMacAddrAuthFailedTrap	
rcRstpNewTopology	

Generic Proprietary Traps

Generic traps carry information about events in their severity and description objects. They are sent at the same time an alarm is generated for the device. The following are examples of RUGGEDCOM generic traps:

Note
Information about generic traps can be retrieved using the CLI command **`alarms`**. For more information about the **`alarms`** command, refer to "Available CLI Commands (Page 17)".

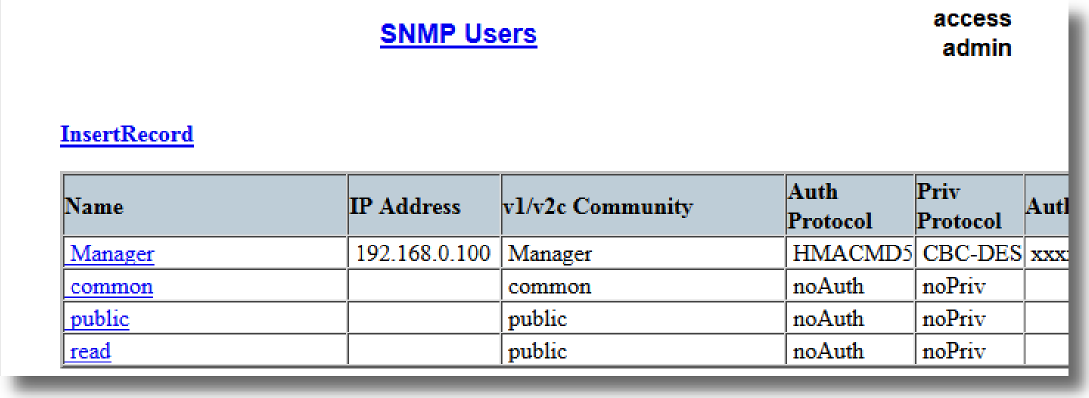
Trap	Severity
TACACS+ response invalid	Warning
Unable to obtain IP address	Critical
SPP is rejected on Port 1	Error
BootP client: TFTP transfer failure	Error
received two consecutive confusing BPDUs on port, forcing down	Error

12.3.3 Managing SNMP Users

This section describes how to manage SNMP users.

12.3.3.1 Viewing a List of SNMP Users

To view a list of SNMP users configured on the device, navigate to ***Administration » Configure SNMP » Configure SNMP Users***. The **SNMP Users** table appears.



SNMP Users

access
admin

InsertRecord

Name	IP Address	v1/v2c Community	Auth Protocol	Priv Protocol	Autl
Manager	192.168.0.100	Manager	HMACMD5	CBC-DES	xxx
common		common	noAuth	noPriv	
public		public	noAuth	noPriv	
read		public	noAuth	noPriv	

Figure 12.8 SNMP Users Table

If users have not been configured, add users as needed. For more information, refer to "Adding an SNMP User (Page 285)".

12.3.3.2 Adding an SNMP User

Multiple users (up to a maximum of 32) can be configured for the local SNMPv3 engine, as well as SNMPv1 and SNMPv2c communities.

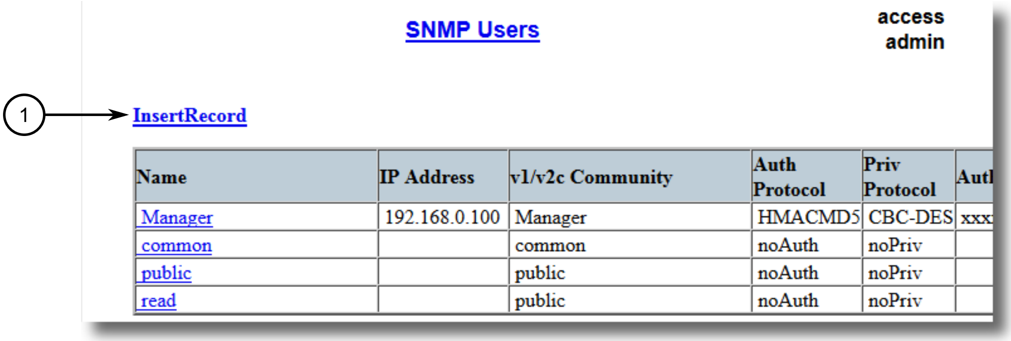
Note

When employing the SNMPv1 or SNMPv2c security level, the **User Name** parameter maps the community name with the security group and access level.

For CLI commands related to adding an SNMP user, refer to "Available CLI Commands (Page 17)".

To add a new SNMP user, do the following:

1. Navigate to ***Administration » Configure SNMP » Configure SNMP Users***. The **SNMP Users Table** appears.

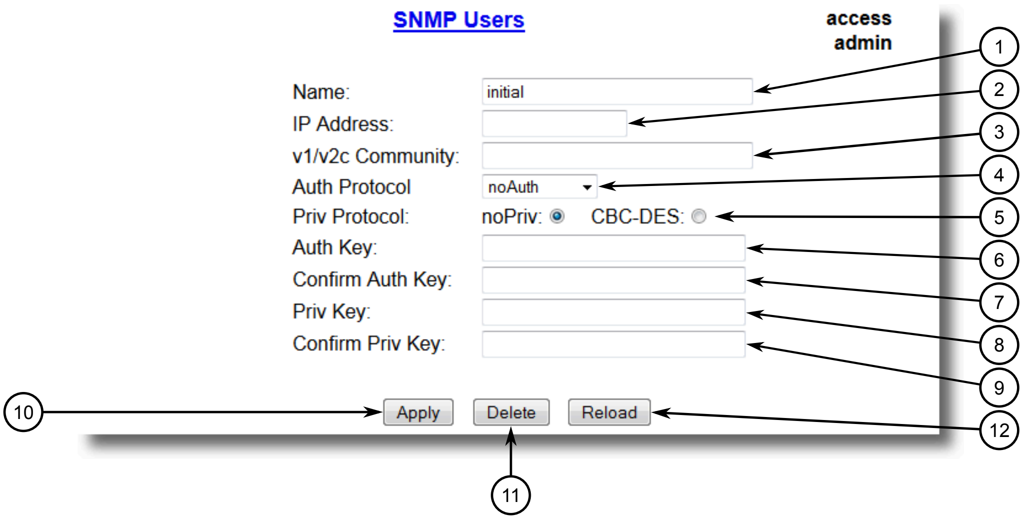


Name	IP Address	v1/v2c Community	Auth Protocol	Priv Protocol	Autl
Manager	192.168.0.100	Manager	HMACMD5	CBC-DES	xxx
common		common	noAuth	noPriv	
public		public	noAuth	noPriv	
read		public	noAuth	noPriv	

① InsertRecord

Figure 12.9 SNMP Users Table

2. Click **InsertRecord**. The **SNMP Users** form appears.



SNMP Users

access
admin

Name: initial
IP Address:
v1/v2c Community:
Auth Protocol noAuth
Priv Protocol: noPriv: ● CBC-DES: ○
Auth Key:
Confirm Auth Key:
Priv Key:
Confirm Priv Key:

① Name Box
② IP Address Box
③ v1/v2c Community Box
④ Auth Protocol Box
⑤ Priv Protocol Box
⑥ Auth Key Box
⑦ Confirm Auth Key Box
⑧ Priv Key Box
⑨ Confirm Priv Key Box
⑩ Apply Button
⑪ Delete Button
⑫ Reload Button

Figure 12.10 SNMP Users Form

Note

RUGGEDCOM ROS requires that all user passwords meet strict guidelines to prevent the use of weak passwords. When creating a new password, make sure it adheres to the following rules:

- Must not be less than 6 characters in length.
- Must not include the username or any 4 continuous alphanumeric characters found in the username. For example, if the username is *Subnet25*, the

password may not be *subnet25admin* or *subnetadmin*. However, *net25admin* or *Sub25admin* is permitted.

- Must have at least one alphabetic character and one number. Special characters are permitted.
- Must not have more than 3 continuously incrementing or decrementing numbers. For example, *Sub123* and *Sub19826* are permitted, but *Sub12345* is not.

An alarm will generate if a weak password is configured. The weak password alarm can be disabled by the user. For more information about disabling alarms, refer to "Managing Alarms (Page 102)".

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

Parameter	Description
`Name`	**Synopsis:** A string 32 characters long **Default:** initial The name of the user. This user name also represents the security name that maps this user to the security group.
`IP Address`	**Synopsis:** ###.###.###.### where ### ranges from 0 to 255 The IP address of the user's SNMP management station. If IP address is configured, SNMP requests from that user will be verified by IP address as well. SNMP Authentication trap will be generated to trap receivers if request was received from this user, but from any other IP address.If IP address is empty, traps can not be generated to this user, but SNMP requests will be served for this user from any IP address.
`v1/v2c Community`	**Synopsis:** A string 32 characters long The community string which is mapped by this user/security name to the security group if security model is SNMPv1 or SNMPv2c. If this string is left empty, it will be assumed to be equal to the same as user name.
`Auth Protocol`	**Synopsis:** [noAuth | HMACMD5 | HMACSHA] **Default:** noAuth An indication of whether messages sent on behalf of this user to/from SNMP engine, can be authenticated, and if so, the type of authentication protocol which is used.
`Priv Protocol`	**Synopsis:** [noPriv | CBC-DES] **Default:** noPriv An Indication of whether messages sent on behalf of this user to/from SNMP engine can be protected from disclosure, and if so, the type of privacy protocol which is used.
`Auth Key`	**Synopsis:** A string 31 characters long The secret authentication key (password) that must be shared with SNMP client. If the key is not an emtpy string, it must be at least 6 characters long.

Parameter	Description
`Confirm Auth Key`	**Synopsis:** A string 31 characters long The secret authentication key (password) that must be shared with SNMP client. If the key is not an emtpy string, it must be at least 6 characters long.
`Priv Key`	**Synopsis:** A string 31 characters long The secret encription key (password) that must be shared with SNMP client. If the key is not an emtpy string, it must be at least 6 characters long.
`Confirm Priv Key`	**Synopsis:** A string 31 characters long The secret encription key (password) that must be shared with SNMP client. If the key is not an emtpy string, it must be at least 6 characters long.

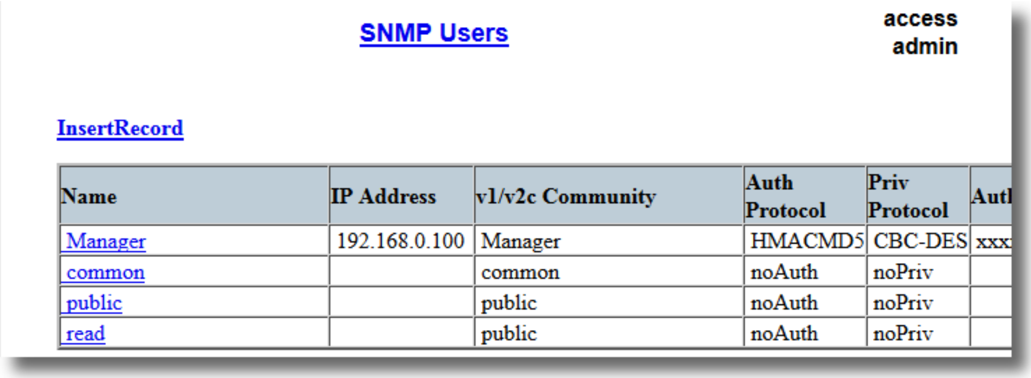
4. Click **Apply**.

12.3.3.3 Deleting an SNMP User

For CLI commands related to deleting an SNMP user, refer to "Available CLI Commands (Page 17)".

To delete an SNMP user, do the following:

1. Navigate to ***Administration » Configure SNMP » Configure SNMP Users***. The **SNMP Users Table** appears.



SNMP Users

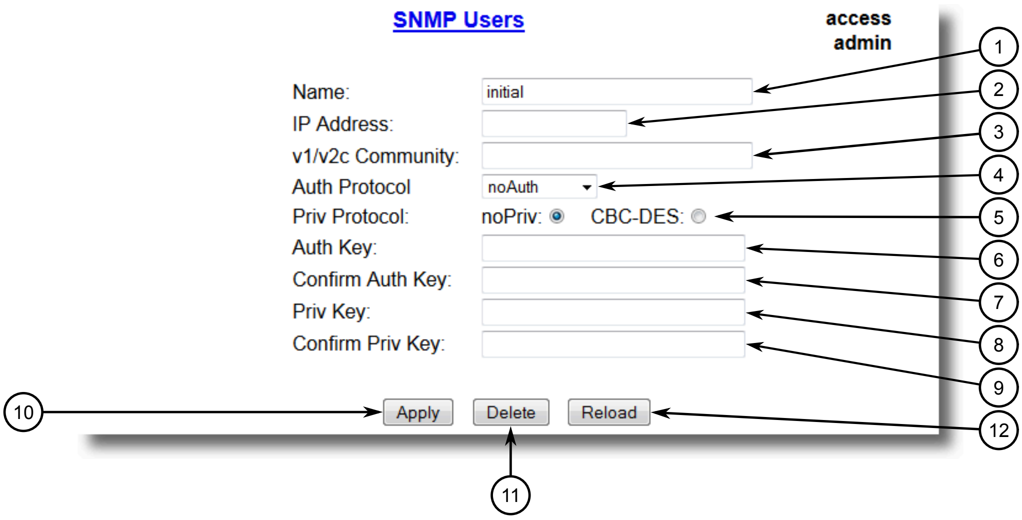
access
admin

InsertRecord

Name	IP Address	v1/v2c Community	Auth Protocol	Priv Protocol	Autl
Manager	192.168.0.100	Manager	HMACMD5	CBC-DES	xxx
common		common	noAuth	noPriv	
public		public	noAuth	noPriv	
read		public	noAuth	noPriv	

Figure 12.11 SNMP Users Table

2. Select the user from the table. The **SNMP Users** form appears.



SNMP Users

access
admin

Name: initial

IP Address:

v1/v2c Community:

Auth Protocol noAuth

Priv Protocol: noPriv: ● CBC-DES: ○

Auth Key:

Confirm Auth Key:

Priv Key:

Confirm Priv Key:

① Name Box
② IP Address Box
③ v1/v2c Community Box
④ Auth Protocol Box
⑤ Priv Protocol Box
⑥ Auth Key Box
⑦ Confirm Auth Key Box
⑧ Priv Key Box
⑨ Confirm Priv Key Box
⑩ Apply Button
⑪ Delete Button
⑫ Reload Button

Figure 12.12 SNMP Users Form

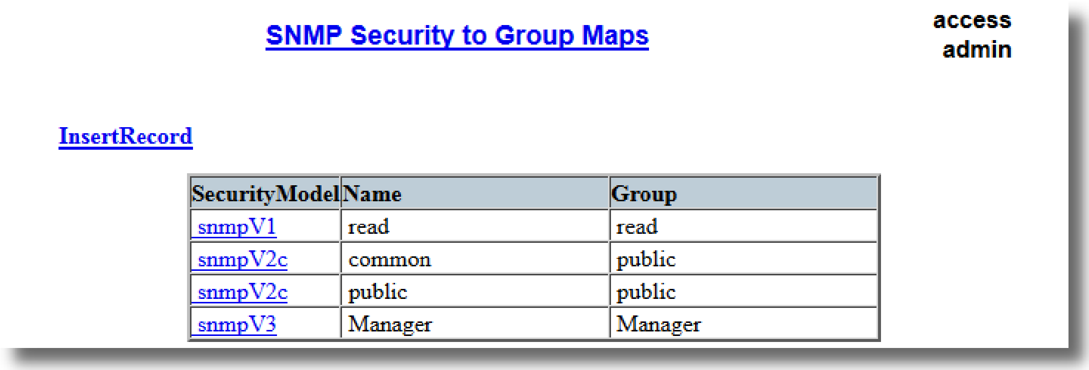
3. Click **Delete**.

12.3.4 Managing Security-to-Group Mapping

This section describes how to configure and manage security-to-group maps.

12.3.4.1 Viewing a List of Security-to-Group Maps

To view a list of security-to-group maps configured on the device, navigate to ***Administration » Configure SNMP » Configure SNMP Security to Group Maps***. The **SNMP Security to Group Maps** table appears.



SecurityModel	Name	Group
snmpV1	read	read
snmpV2c	common	public
snmpV2c	public	public
snmpV3	Manager	Manager

Figure 12.13 SNMP Security to Group Maps Table

If security-to-group maps have not been configured, add maps as needed. For more information, refer to "Adding a Security-to-Group Map (Page 290)".

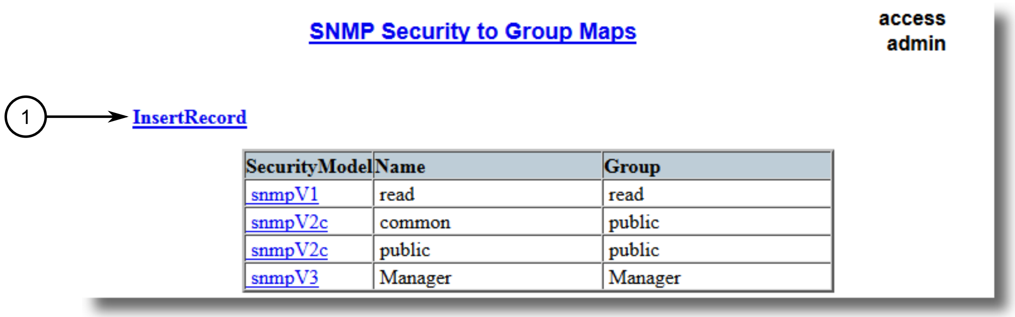
12.3.4.2 Adding a Security-to-Group Map

Multiple combinations of security models and groups can be mapped (up to a maximum of 32) for SNMP.

For CLI commands related to adding an SNMP security-to-group map, refer to "Available CLI Commands (Page 17)".

To add a security-to-group map, do the following:

1. Navigate to ***Administration » Configure SNMP » Configure SNMP Security to Group Maps***. The **SNMP Security to Group Maps Table** appears.

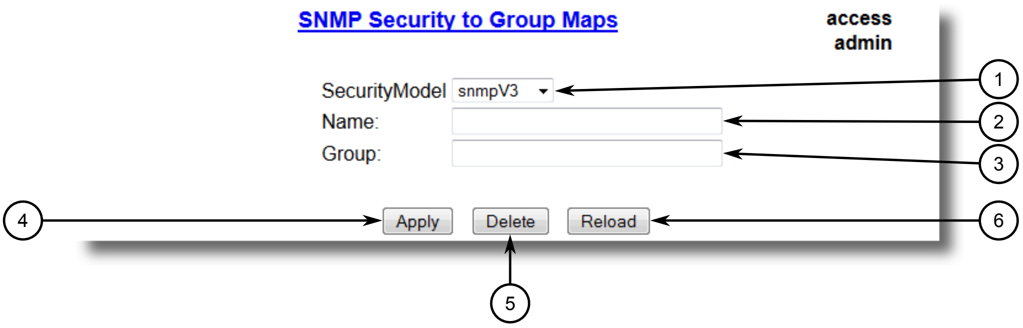


SecurityModel	Name	Group
snmpV1	read	read
snmpV2c	common	public
snmpV2c	public	public
snmpV3	Manager	Manager

① InsertRecord

Figure 12.14 SNMP Security to Group Maps Table

2. Click **InsertRecord**. The **SNMP Security to Group Maps** form appears.



①	Security Model Box
②	Name Box
③	Group Box
④	Apply Button
⑤	Delete Button
⑥	Reload Button

Figure 12.15 SNMP Security to Group Maps Form

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

Parameter	Description
`SecurityModel`	**Synopsis:** [snmpV1 | snmpV2c | snmpV3] **Default:** snmpV3 The Security Model that provides the name referenced in this table.
`Name`	**Synopsis:** A string 32 characters long The user name which is mapped by this entry to the specified group name.
`Group`	**Synopsis:** A string 32 characters long The group name to which the security model and name belong. This name is used as an index to the SNMPv3 VACM Access Table.

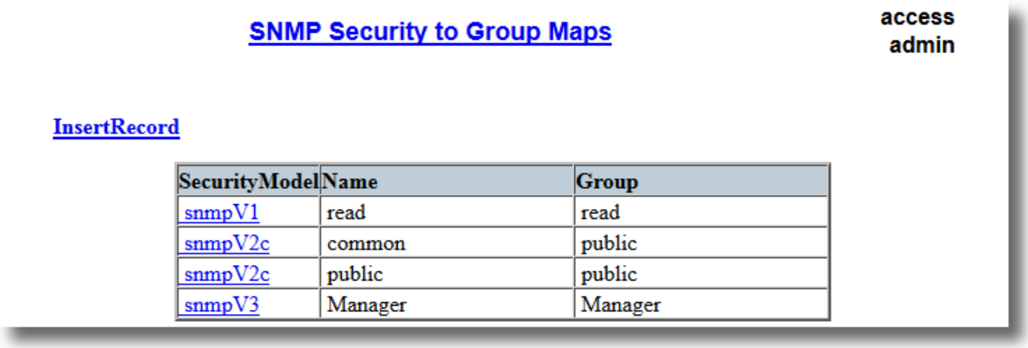
4. Click **Apply**.

12.3.4.3 Deleting a Security-to-Group Map

For CLI commands related to deleting an SNMP security-to-group map, refer to "Available CLI Commands (Page 17)".

To delete a security-to-group map, do the following:

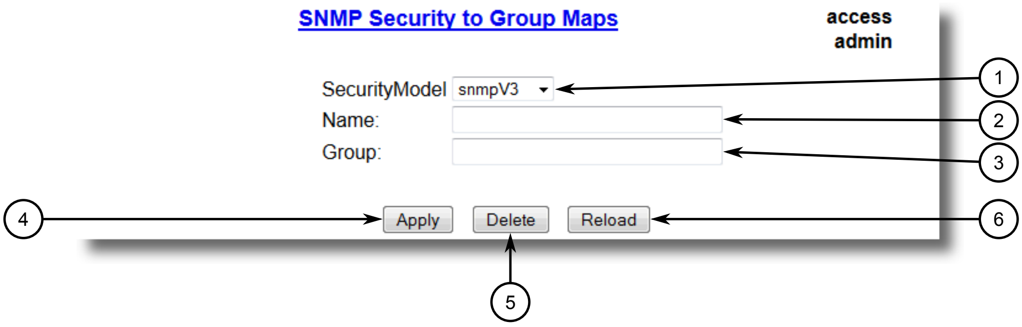
1. Navigate to ***Administration » Configure SNMP » Configure SNMP Security to Group Maps***. The **SNMP Security to Group Maps Table** appears.



SecurityModel	Name	Group
snmpV1	read	read
snmpV2c	common	public
snmpV2c	public	public
snmpV3	Manager	Manager

Figure 12.16 SNMP Security to Group Maps Table

2. Select the map from the table. The **SNMP Security to Group Maps** form appears.



① Security Model Box
② Name Box
③ Group Box
④ Apply Button
⑤ Delete Button
⑥ Reload Button

Figure 12.17 SNMP Security to Group Maps Form

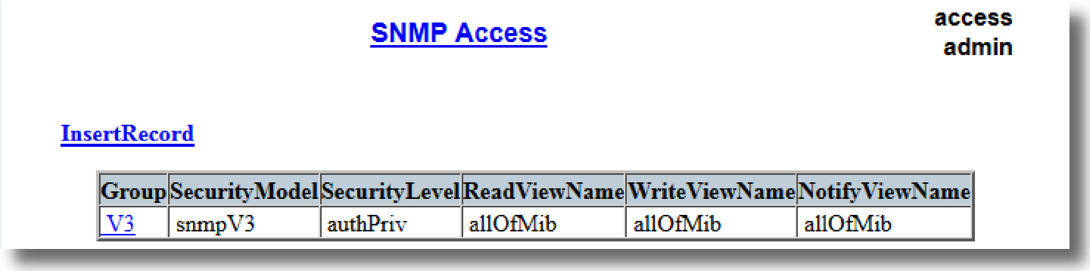
3. Click **Delete**.

12.3.5 Managing SNMP Groups

Multiple SNMP groups (up to a maximum of 32) can be configured to have access to SNMP.

12.3.5.1 Viewing a List of SNMP Groups

To view a list of SNMP groups configured on the device, navigate to ***Administration » Configure SNMP » Configure SNMP Access***. The **SNMP Access** table appears.



SNMP Access

access
admin

InsertRecord

Group	SecurityModel	SecurityLevel	ReadViewName	WriteViewName	NotifyViewName
V3	snmpV3	authPriv	allOfMib	allOfMib	allOfMib

Figure 12.18 SNMP Access Table

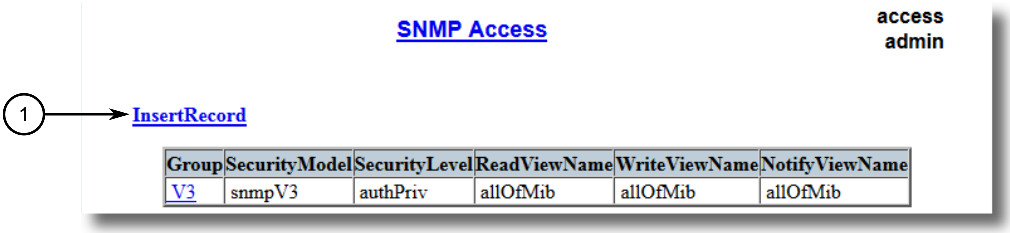
If SNMP groups have not been configured, add groups as needed. For more information, refer to "Adding an SNMP Group (Page 293)".

12.3.5.2 Adding an SNMP Group

For CLI commands related to adding an SNMP group, refer to "Available CLI Commands (Page 17)".

To add an SNMP group, do the following:

1. Navigate to ***Administration » Configure SNMP » Configure SNMP Access***. The **SNMP Access Table** appears.



SNMP Access

access
admin

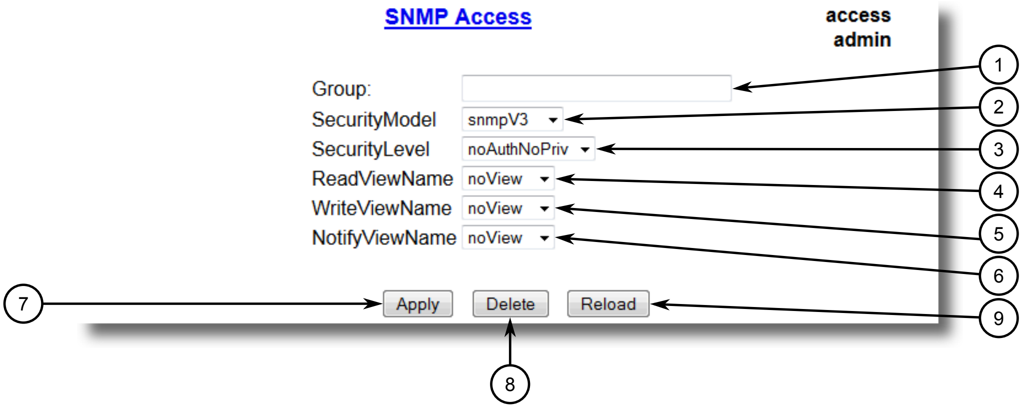
InsertRecord

Group	SecurityModel	SecurityLevel	ReadViewName	WriteViewName	NotifyViewName
V3	snmpV3	authPriv	allOfMib	allOfMib	allOfMib

① InsertRecord

Figure 12.19 SNMP Access Table

2. Click **InsertRecord**. The **SNMP Access** form appears.



① Group Box
② Security Model Box
③ Security Level Box
④ ReadViewName Box
⑤ WriteViewName Box
⑥ NotifyViewName Box
⑦ Apply Button
⑧ Delete Button
⑨ Reload Button

Figure 12.20 SNMP Access Form

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

Parameter	Description
`Group`	**Synopsis:** A string 32 characters long The group name to which the security model and name belong. This name is used as an index to the SNMPv3 VACM Access Table.
`SecurityModel`	**Synopsis:** [snmpV1 | snmpV2c | snmpV3] **Default:** snmpV3 In order to gain the access rights allowed by this entry, configured security model must be in use.
`SecurityLevel`	**Synopsis:** [noAuthNoPriv | authNoPriv | authPriv] **Default:** noAuthNoPriv The minimum level of security required in order to gain the access rights allowed by this entry. A security level of noAuthNoPriv is less than authNoPriv, which is less than authPriv.
`ReadViewName`	**Synopsis:** [noView | V1Mib | allOfMib] **Default:** noView This parameter identifies the MIB tree(s) to which this entry authorizes read access. If the value is noView, then no read access is granted.

Parameter	Description
`WriteViewName`	**Synopsis:** [noView | V1Mib | allOfMib] **Default:** noView This parameter identifies the MIB tree(s) to which this entry authorizes write access. If the value is noView, then no write access is granted.
`NotifyViewName`	**Synopsis:** [noView | V1Mib | allOfMib] **Default:** noView This parameter identifies the MIB tree(s) to which this entry authorizes access for notifications. If the value is noView, then no access for notifications is granted.

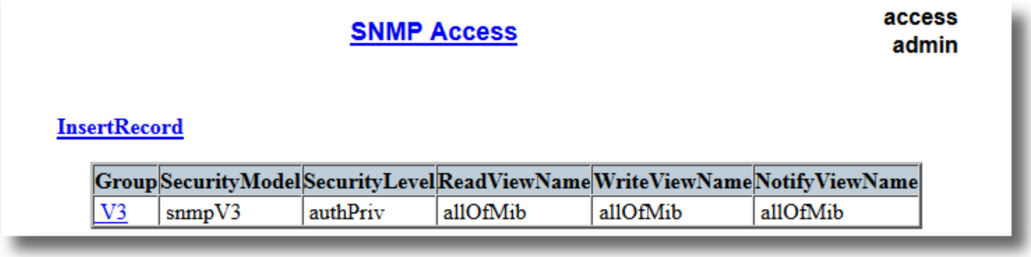
4. Click **Apply**.

12.3.5.3 Deleting an SNMP Group

For CLI commands related to deleting an SNMP group, refer to "Available CLI Commands (Page 17)".

To delete an SNMP group, do the following:

1. Navigate to ***Administration » Configure SNMP » Configure SNMP Access***. The **SNMP Access Table** appears.



SNMP Access

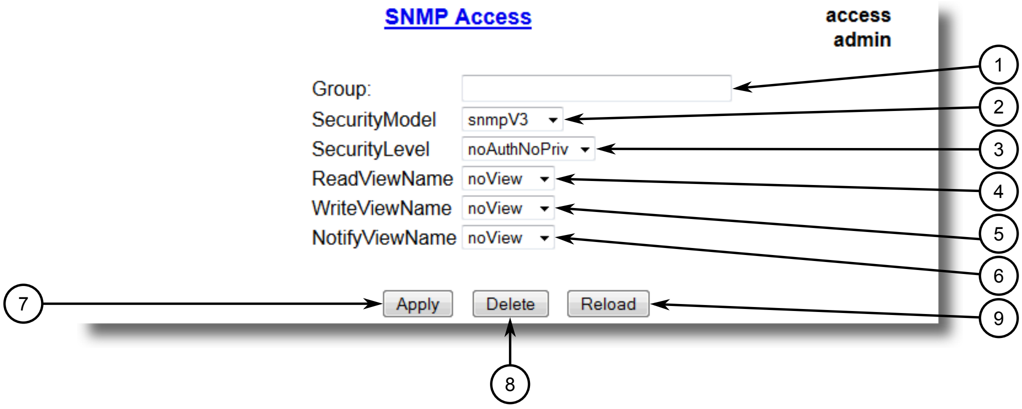
access
admin

InsertRecord

Group	SecurityModel	SecurityLevel	ReadViewName	WriteViewName	NotifyViewName
V3	snmpV3	authPriv	allOfMib	allOfMib	allOfMib

Figure 12.21 SNMP Access Table

2. Select the group from the table. The **SNMP Access** form appears.



① Group Box
② Security Model Box
③ Security Level Box
④ ReadViewName Box
⑤ WriteViewName Box
⑥ NotifyViewName Box
⑦ Apply Button
⑧ Delete Button
⑨ Reload Button

Figure 12.22 SNMP Access Form

3. Click **Delete**.

12.4 ModBus Management Support

Modbus management support in RUGGEDCOM devices provides a simple interface for retrieving basic status information. ModBus support simplifies the job of SCADA (Supervisory Control and Data Acquisition) system integrators by providing familiar protocols for retrieving RUGGEDCOM device information. ModBus provides mostly read-only status information, but there are some writeable registers for operator commands.

The ModBus protocol PDU (Protocol Data Unit) format is as follows:

Function Code	Data

12.4.1 ModBus Function Codes

RUGGEDCOM devices support the following ModBus function codes for device management through ModBus:

Note

While RUGGEDCOM devices have a variable number of ports, not all registers and bits apply to all products.

Registers that are not applicable to a particular device return a zero (0) value. For example, registers referring to serial ports are not applicable to RUGGEDCOM switch devices.

Read Input Registers or Read Holding Registers – 0x04 or 0x03

Example PDU Request

Function Code	1 Byte	0x04(0x03)
Starting Address	2 Bytes	0x0000 to 0xFFFF (Hexadecimal) 128 to 65535 (Decimal)
Number of Input Registers	2 Bytes	Bytes 0x0001 to 0x007D

Example PDU Response

Function Code	1 Byte	0x04(0x03)
Byte Count	1 Byte	2 x *N* [a]
Number of Input Registers	*N*[a] x 2 Bytes	

[a] The number of input registers

Write Multiple Registers – 0x10

Example PDU Request

Function Code	1 Byte	0x10
Starting Address	2 Bytes	0x0000 to 0xFFFF
Number of Input Registers	2 Bytes	Bytes 0x0001 to 0x0079
Byte Count	1 Byte	2 x *N* [a]
Registers Value	*N*[a] x 2 Bytes	Value of the register

[a] The number of input registers

Example PDU Response

Function Code	1 Byte	0x10
Starting Address	2 Bytes	0x0000 to 0xFFFF
Number of Registers	2 Bytes	1 to 121 (0x79)

12.4.2 ModBus Memory Map

The following details how ModBus process variable data is mapped.

Product Info

The following data is mapped to the *Productinfo* table:

Address	#Registers	Description (Reference Table in UI)	R/W	Format
0000	16	Product Identification	R	Text
0010	32	Firmware Identification	R	Text
0040	1	Number of Ethernet Ports	R	Uint16
0041	1	Number of Serial Ports	R	Uint16
0042	1	Number of Alarms	R	Uint16
0043	1	Power Supply Status	R	PSStatusCmd
0044	1	FailSafe Relay Status	R	TruthValue
0045	1	ErrorAlarm Status	R	TruthValue

Product Write Register

The following data is mapped to various tables:

Address	#Registers	Description (Reference Table in UI)	R/W	Format
0080	1	Clear Alarms	W	Cmd
0081	2	Reset Ethernet Ports	W	PortCmd
0083	2	Clear Ethernet Statistics	W	PortCmd
0085	2	Reset Serial Ports	W	PortCmd
0087	2	Clear Serial Port Statistics	W	PortCmd

Alarms

The following data is mapped to the *alarms* table:

Address	#Registers	Description (Reference Table in UI)	R/W	Format
0100	64	Alarm 1	R	Alarm
0140	64	Alarm 2	R	Alarm
0180	64	Alarm 3	R	Alarm
01C0	64	Alarm 4	R	Alarm
0200	64	Alarm 5	R	Alarm
0240	64	Alarm 6	R	Alarm
0280	64	Alarm 7	R	Alarm
02C0	64	Alarm 8	R	Alarm

Ethernet Port Status

The following data is mapped to the *ethPortStats* table:

Address	#Registers	Description (Reference Table in UI)	R/W	Format
03FE	2	Port Link Status	R	PortCmd

Ethernet Statistics

The following data is mapped to the *rmonStats* table:

Address	#Registers	Description (Reference Table in UI)	R/W	Format
0400	2	Port 1 Statistics - Ethernet In Packets	R	Uint32
0402	2	Port 2 Statistics - Ethernet In Packets	R	Uint32
0404	2	Port 3 Statistics - Ethernet In Packets	R	Uint32
0406	2	Port 4 Statistics - Ethernet In Packets	R	Uint32
0408	2	Port 5 Statistics - Ethernet In Packets	R	Uint32
040A	2	Port 6 Statistics - Ethernet In Packets	R	Uint32
040C	2	Port 7 Statistics - Ethernet In Packets	R	Uint32
040E	2	Port 8 Statistics - Ethernet In Packets	R	Uint32
0410	2	Port 9 Statistics - Ethernet In Packets	R	Uint32
0412	2	Port 10 Statistics - Ethernet In Packets	R	Uint32
0414	2	Port 11 Statistics - Ethernet In Packets	R	Uint32
0416	2	Port 12 Statistics - Ethernet In Packets	R	Uint32
0418	2	Port 13 Statistics - Ethernet In Packets	R	Uint32
041A	2	Port 14 Statistics - Ethernet In Packets	R	Uint32
041C	2	Port 15 Statistics - Ethernet In Packets	R	Uint32
041E	2	Port 16 Statistics - Ethernet In Packets	R	Uint32
0420	2	Port 17 Statistics - Ethernet In Packets	R	Uint32
0422	2	Port 18 Statistics - Ethernet In Packets	R	Uint32
0424	2	Port 19 Statistics - Ethernet In Packets	R	Uint32
0426	2	Port 20 Statistics - Ethernet In Packets	R	Uint32
0440	2	Port 1 Statistics - Ethernet Out Packets	R	Uint32
0442	2	Port 2 Statistics - Ethernet Out Packets	R	Uint32
0444	2	Port 3 Statistics - Ethernet Out Packets	R	Uint32
0446	2	Port 4 Statistics - Ethernet Out Packets	R	Uint32
0448	2	Port 5 Statistics - Ethernet Out Packets	R	Uint32
044A	2	Port 6 Statistics - Ethernet Out Packets	R	Uint32

Address	#Registers	Description (Reference Table in UI)	R/W	Format
044C	2	Port 7 Statistics - Ethernet Out Packets	R	Uint32
044E	2	Port 8 Statistics - Ethernet Out Packets	R	Uint32
0450	2	Port 9 Statistics - Ethernet Out Packets	R	Uint32
0452	2	Port 10 Statistics - Ethernet Out Packets	R	Uint32
0454	2	Port 11 Statistics - Ethernet Out Packets	R	Uint32
0456	2	Port 12 Statistics - Ethernet Out Packets	R	Uint32
0458	2	Port 13 Statistics - Ethernet Out Packets	R	Uint32
045A	2	Port 14 Statistics - Ethernet Out Packets	R	Uint32
045C	2	Port 15 Statistics - Ethernet Out Packets	R	Uint32
045E	2	Port 16 Statistics - Ethernet Out Packets	R	Uint32
0460	2	Port 17 Statistics - Ethernet Out Packets	R	Uint32
0462	2	Port 18 Statistics - Ethernet Out Packets	R	Uint32
0464	2	Port 19 Statistics - Ethernet Out Packets	R	Uint32
0466	2	Port 20 Statistics - Ethernet Out Packets	R	Uint32
0480	2	Port 1 Statistics - Ethernet In Octets	R	Uint32
0482	2	Port 2 Statistics - Ethernet In Octets	R	Uint32
0484	2	Port 3 Statistics - Ethernet In Octets	R	Uint32
0486	2	Port 4 Statistics - Ethernet In Octets	R	Uint32
0488	2	Port 5 Statistics - Ethernet In Octets	R	Uint32
048A	2	Port 6 Statistics - Ethernet In Octets	R	Uint32
048C	2	Port 7 Statistics - Ethernet In Octets	R	Uint32
048E	2	Port 8 Statistics - Ethernet In Octets	R	Uint32
0490	2	Port 9 Statistics - Ethernet In Octets	R	Uint32
0492	2	Port 10 Statistics - Ethernet In Octets	R	Uint32
0494	2	Port 11 Statistics - Ethernet In Octets	R	Uint32
0496	2	Port 12 Statistics - Ethernet In Octets	R	Uint32
0498	2	Port 13 Statistics - Ethernet In Octets	R	Uint32

Address	#Registers	Description (Reference Table in UI)	R/W	Format
049A	2	Port 14 Statistics - Ethernet In Octets	R	Uint32
049C	2	Port 15 Statistics - Ethernet In Octets	R	Uint32
049E	2	Port 16 Statistics - Ethernet In Octets	R	Uint32
04A0	2	Port 17 Statistics - Ethernet In Octets	R	Uint32
04A2	2	Port 18 Statistics - Ethernet In Octets	R	Uint32
04A4	2	Port 19 Statistics - Ethernet In Octets	R	Uint32
04A6	2	Port 20 Statistics - Ethernet In Octets	R	Uint32
04C0	2	Port 1 Statistics - Ethernet Out Octets	R	Uint32
04C2	2	Port 2 Statistics - Ethernet Out Octets	R	Uint32
04C4	2	Port 3 Statistics - Ethernet Out Octets	R	Uint32
04C6	2	Port 4 Statistics - Ethernet Out Octets	R	Uint32
04C8	2	Port 5 Statistics - Ethernet Out Octets	R	Uint32
04CA	2	Port 6 Statistics - Ethernet Out Octets	R	Uint32
04CC	2	Port 7 Statistics - Ethernet Out Octets	R	Uint32
04CE	2	Port 8 Statistics - Ethernet Out Octets	R	Uint32
04D0	2	Port 9 Statistics - Ethernet Out Octets	R	Uint32
04D2	2	Port 10 Statistics - Ethernet Out Octets	R	Uint32
04D4	2	Port 11 Statistics - Ethernet Out Octets	R	Uint32
04D6	2	Port 12 Statistics - Ethernet Out Octets	R	Uint32
04D8	2	Port 13 Statistics - Ethernet Out Octets	R	Uint32
04DA	2	Port 14 Statistics - Ethernet Out Octets	R	Uint32
04DC	2	Port 15 Statistics - Ethernet Out Octets	R	Uint32
04DE	2	Port 16 Statistics - Ethernet Out Octets	R	Uint32
04E0	2	Port 17 Statistics - Ethernet Out Octets	R	Uint32

Address	#Registers	Description (Reference Table in UI)	R/W	Format
04E2	2	Port 18 Statistics - Ethernet Out Octets	R	Uint32
04E4	2	Port 19 Statistics - Ethernet Out Octets	R	Uint32
04E6	2	Port 20 Statistics - Ethernet Out Octets	R	Uint32

Serial Statistics

The following data is mapped to the *uartPortStatus* table:

Address	#Registers	Description (Reference Table in UI)	R/W	Format
0600	2	Port 1 Statistics – Serial In characters	R	Uint32
0602	2	Port 2 Statistics – Serial In characters	R	Uint32
0604	2	Port 3 Statistics – Serial In characters	R	Uint32
0606	2	Port 4 Statistics – Serial In characters	R	Uint32
0640	2	Port 1 Statistics – Serial Out characters	R	Uint32
0642	2	Port 2 Statistics – Serial Out characters	R	Uint32
0644	2	Port 3 Statistics – Serial Out characters	R	Uint32
0646	2	Port 4 Statistics – Serial Out characters	R	Uint32
0680	2	Port 1 Statistics – Serial In Packets	R	Uint32
0682	2	Port 2 Statistics – Serial In Packets	R	Uint32
0684	2	Port 3 Statistics – Serial In Packets	R	Uint32
0686	2	Port 4 Statistics – Serial In Packets	R	Uint32
06C0	2	Port 1 Statistics – Serial Out Packets	R	Uint32
06C2	2	Port 2 Statistics – Serial Out Packets	R	Uint32
06C4	2	Port 3 Statistics – Serial Out Packets	R	Uint32
06C6	2	Port 4 Statistics – Serial Out Packets	R	Uint32

12.4.3 Modbus Memory Formats

This section defines the Modbus memory formats supported by RUGGEDCOM ROS.

12.4.3.1 Text

The Text format provides a simple ASCII representation of the information related to the product. The most significant register byte of an ASCII characters comes first.

For example, consider a *Read Multiple Registers* request to read Product Identification from location 0x0000.

0x04	0x00	0x00	0x00	0x08

The response may look like:

0x04	0x10	0x53	0x59	0x53	0x54	0x45	0x4D	0x20	0x4E	0x41	0x4D	0x45
0x00	0x00	0x00	0x00	0x00								

In this example, starting from byte 3 until the end, the response presents an ASCII representation of the characters for the product identification, which reads as *SYSTEM NAME*. Since the length of this field is smaller than eight registers, the rest of the field is filled with zeros (0).

12.4.3.2 Cmd

The Cmd format instructs the device to set the output to either *true* or *false*. The most significant byte comes first.

- FF 00 hex requests output to be True
- 00 00 hex requests output to be False
- Any value other than the suggested values does not affect the requested operation

For example, consider a *Write Multiple Registers* request to clear alarms in the device.

0x10	0x00	0x80	0x00	0x01	2	0xFF	0x00

- FF 00 for register 00 80 clears the system alarms
- 00 00 does not clear any alarms

The response may look like:

0x10	0x00	0x80	0x00	0x01

12.4.3.3 Uint16

The Uint16 format describes a Standard ModBus 16 bit register.

12.4.3.4 Uint32

The Uint32 format describes Standard 2 ModBus 16 bit registers. The first register holds the most significant 16 bits of a 32 bit value. The second register holds the least significant 16 bits of a 32 bit value.

12.4.3.5 PortCmd

The PortCmd format describes a bit layout per port, where 1 indicates the requested action is true, and 0 indicates the requested action is false.

PortCmd provides a bit layout of a maximum of 32 ports. Therefore, it uses two ModBus regsiters:

- The first ModBus register corresponds to ports 1 – 16
- The second ModBus register corresponds to ports 17 – 32 for a particular action

Bits that do not apply to a particular product are always set to zero (0).

A bit value of 1 indicates that the requested action is true. For example, the port is *up*.

A bit value of 0 indicates that the requested action is false. For example, the port is *down*.

Reading Data Using PortCmd

To understand how to read data using PortCmd, consider a ModBus Request to read multiple registers from location 0x03FE.

0x04	0x03	0xFE	0x00	0x02

The response depends on how many ports are available on the device. For example, if the maximum number of ports on a connected RUGGEDCOM device is 20, the response would be similar to the following:

0x04	0x04	0xF2	0x76	0x00	0x05

In this example, bytes 3 and 4 refer to register 1 at location 0x03FE, and represent the status of ports 1 – 16. Bytes 5 and 6 refer to register 2 at location 0x03FF, and represent the status of ports 17 – 32. The device only has 20 ports, so byte 6 contains the status for ports 17 – 20 starting from right to left. The rest of the bites in register 2 corresponding to the non-existing ports 21 – 31 are zero (0).

Performing Write Actions Using PortCmd

To understand how data is written using PortCmd, consider a Write Multiple Register request to clear Ethernet port statistics:

0x10	0x00	0x83	0x00	0x01	2	0x55	0x76	0x00	0x50

A bit value of 1 clears Ethernet statistics on the corresponding port. A bit value of 0 does not clear the Ethernet statistics.

0x10	0x00	0x81	0x00	0x02

12.4.3.6 Alarm

The Alarm format is another form of text description. Alarm text corresponds to the alarm description from the table holding all of the alarms. Similar to the Text format, this format returns an ASCII representation of alarms.

Note

Alarms are stacked in the device in the sequence of their occurence (i.e. Alarm 1, Alarm 2, Alarm 3, etc.).

The first eight alarms from the stack can be returned, if they exist. A zero (0) value is returned if an alarm does not exist.

12.4.3.7 PSStatusCmd

The PSStatusCmd format describes a bit layout for providing the status of available power supplies. Bits 0-4 of the lower byte of the register are used for this purpose.

- Bits 0-1: Power Supply 1 Status
- Bits 2-3: Power Supply 2 Status

Other bits in the register do not provide any system status information.

Bit Value	Description
01	Power Supply not present (01 = 1)
10	Power Supply is functional (10 = 2)
11	Power Supply is not functional (11 = 3)

The values used for power supply status are derived from the RUGGEDCOM-specific SNMP MIB.

Reading the Power Supply Status from a Device Using PSStatusCmd

To understand how to read the power supply status from a device using PSStatusCmd, consider a ModBus Request to read multiple registers from location 0x0043.

0x04	0x00	0x43	0x00	0x01

The response may look like:

0x04	0x02	0x00	0x0A

The lower byte of the register displays the power supply's status. In this example, both power supplies in the unit are functional.

12.4.3.8 TruthValues

The Truthvalues format represents a true or false status in the device:

- 1 indicates the corresponding status for the device to be true
- 2 indicates the corresponding status for the device to be false

Reading the FailSafe Relay Status From a Device Using TruthValue

To understand how to use the TruthValue format to read the FailSafe Relay status from a device, consider a ModBus request to read multiple registers from location 0x0044.

0x04	0x00	0x44	0x00	0x01

The response may look like:

0x04	0x02	0x00	0x01

The register's lower byte shows the FailSafe Relay status. In this example, the FailSafe Relay is energized.

Reading the ErrorAlarm Status From a Device Using TruthValue

To understand how to use the TruthValue format to read the ErrorAlarm status from a device, conside a ModBus request to read mulitple registers from location 0x0045.

0x04	0x00	0x45	0x00	0x01

The response may look like:

0x04	0x02	0x00	0x01

The register's lower byte shows the ErrorAlarm status. In this example, there is no active ERROR, ALERT or CRITICAL alarm in the device.

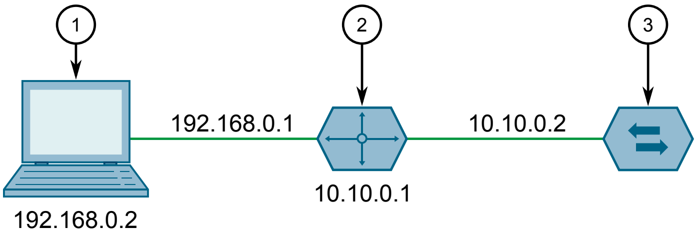
13 Troubleshooting

This chapter describes troubleshooting steps for common issues that may be encountered when using RUGGEDCOM ROS or designing a network.

⚠ NOTICE
For further assistance, contact a Customer Service representative.

13.1 General

The following describes common problems.

Problem	Solution
The switch is not responding to ping attempts, even though the IP address and gateway have been configured. The switch is receiving the ping because the LEDs are flashing and the device statistics are logging the pings. What is going on?	Is the switch being pinged through a router? If so, the switch gateway address must be configured as well. The following figure illustrates the problem.  1 2 3 192.168.0.1 10.10.0.2 10.10.0.1 192.168.0.2 ① Work Station ② Router ③ Switch Figure 13.1 Using a Router As a Gateway The router is configured with the appropriate IP subnets and will forward the ping from the workstation to the switch. When the switch responds, however, it will not know which of its interfaces to use to reach the workstation and will drop the response. Programming a gateway of 10.0.0.1 will cause the switch to forward unresolvable frames to the router. This problem will also occur if the gateway address is not configured and the switch tries to raise an SNMP trap to a host that is not on the local subnet.

13.2 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 with auto-negotiation off 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`** `{destination} {count} {timeout}` can be used to ping the next switch by a specified number of echo requests, separated by the defined number of milliseconds. For example, **`ping`** `192.168.0.1 500 2` issues 500 pings each separated by two milliseconds to the next switch. If the link used is of high quality, then no pings should be lost and the average round trip time should be small.
Links are inaccessible, even when using the Link Fault Indication (LFI) protection feature.	Make sure LFI is not enabled on the peer as well. If both sides of the link have LFI enabled, then both sides will withhold link signal generation from each other.
Previously stable port links experience up/down events when new media is introduced.	This is normal behavior when fiber optic devices are introduced. When a newly inserted fiber optic device is booting up, the fiber ports are in a transitional state and therefore adjacent systems that are live (i.e. functional and stable) will observe port up/down events until the device has completed the boot up sequence. This is due to the fact that fiber transceiver power levels are changing during the boot up transition, thereby toggling the connected link up or down. Installing fiber optic cables in a live network will also cause these effects, especially for connectors that are designed to be keyed and locked, such as ST connectors.
The remote syslog appears to skip events or log them out of sequence.	This is normal behavior when a new Ethernet switch is introduced into a network. In RUGGEDCOM ROS, system and network stability is the highest priority. When a new Ethernet switch is introduced into a network, network reconfiguration occurs so as to prevent loops from occurring and causing broadcast storms. When such reconfiguration takes place, a higher priority is given to RSTP messages and reconfiguration activities than to event logging activities.

13.3 Spanning Tree

The following describes common problems related to the Spanning Tree Protocol (STP).

Problem	Solution
The network locks up when a new port is connected and the	Is it possible that one of the switches in the network or one of the ports on a switch in the network has STP disabled and accidentally

Problem	Solution
port status LEDs are flashing rapidly.	connects to another switch? If this has occurred, then a traffic loop has been formed.
Occasionally, the ports seem to experience significant flooding for a brief period of time.	If the problem appears to be transient in nature, it is possible that ports that are part of the spanning tree have been configured as edge ports. After the link layers have come up on edge ports, STP will directly transition them (perhaps improperly) to the forwarding state. If an RSTP configuration message is then received, the port will be returned to blocking. A traffic loop may be formed for the length of time the port was in forwarding. If one of the switches appears to flip the root from one port to another, the problem may be one of traffic prioritization. For more information refer to "The network becomes unstable when a specific application is started." (Page 310). Another possible cause of intermittent operation is that of an auto-negotiation mismatch. If one end of the link is fixed to full-duplex mode and the peer auto-negotiates, the auto-negotiating end will fall back to half-duplex operation. At lower traffic, the volumes the link may display few if any errors. As the traffic volume rises, the fixed negotiation side will begin to experience dropped packets while the auto-negotiating side will experience collisions. Ultimately, as traffic loads approach 100%, the link will become entirely unusable. At this point, RSTP will not be able to transmit configuration messages over the link and the spanning tree topology will break down. If an alternate trunk exists, RSTP will activate it in the place of the congested port. Since activation of the alternate port often relieves the congested port of its traffic, the congested port will once again become reliable. RSTP will promptly enter it back into service, beginning the cycle once again. The root port will flip back and forth between two ports on the switch.
A switch displays a strange behavior where the root port hops back and forth between two switch ports and never settles down.	
A computer or device is connected to a switch. After the switch is reset, it takes a long time for it to come up.	Is it possible that the RSTP edge setting for this port is set to false? If Edge is set to false, the bridge will make the port go through two forward delay times before the port can send or receive frames. If Edge is set to true, the bridge will transition the port directly to forwarding upon link up. Another possible explanation is that some links in the network run in half-duplex mode. RSTP uses a peer-to-peer protocol called Proposal-Agreement to ensure transitioning in the event of a link failure. This protocol requires full-duplex operation. When RSTP detects a non-full duplex port, it cannot rely on Proposal-Agreement protocol and must make the port transition the slow (i.e. STP) way. If possible, configure the port for full-duplex operation. Otherwise, configure the port’s point-to-point setting to true. Either one will allow the Proposal-Agreement protocol to be used.
When the switch is tested by deliberately breaking a link, it takes a long time before devices beyond the switch can be polled.	Is it possible that some ports participating in the topology have been configured to STP mode or that the port’s point-to-point parameter is set to false? STP and 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 locat-

Problem	Solution
	ed 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 to reestablish the topology.
The network is composed of a ring of bridges, of which two (connected to each other) are managed and the rest are unmanaged. Why does the RSTP protocol work quickly when a link is broken between the managed bridges, but not in the unmanaged bridge part of the ring?	A properly operating unmanaged bridge is transparent to STP configuration messages. The managed bridges will exchange configuration messages through the unmanaged bridge part of the ring as if it is non-existent. When a link in the unmanaged part of the ring fails however, the managed bridges will only be able to detect the failure through timing out of hello messages. Full connectivity will require three hello times plus two forwarding times to be restored.
The network becomes unstable when a specific application is started. The network returns to normal when the application is stopped.	RSTP sends its configuration messages using the highest possible priority level. If CoS is configured to allow traffic flows at the highest priority level and these traffic flows burst continuously to 100% of the line bandwidth, STP may be disrupted. It is therefore advised not to use the highest CoS.
When a new port is brought up, the root moves on to that port instead of the port it should move to or stay on.	Is it possible that the port cost is incorrectly programmed or that auto-negotiation derives an undesired value? Inspect the port and path costs with each port active as root.
An Intelligent Electronic Device (IED) or controller does not work with the device.	Certain low CPU bandwidth controllers have been found to behave less than perfectly when they receive unexpected traffic. Try disabling STP for the port. If the controller fails around the time of a link outage, there is the remote possibility that frame disordering or duplication may be the cause of the problem. Try setting the root port of the failing controller’s bridge to STP.
Polls to other devices are occasionally lost.	Review the network statistics to determine whether the root bridge is receiving Topology Change Notifications (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.

13.4 VLANs

The following describes common problems related to the VLANs.

Problem	Solution
VLANs are not needed on the network. Can they be turned off?	Yes. Simply leave all ports set to type *edge* and leave the native VLAN set to 1. This is the default configuration for the switch.
Two VLANs were created and a number of ports were made members of them. Now some of the devices in one VLAN need to send messages to devices in the other VLAN.	If the devices need to communicate at the physical address layer, they must be members of the same VLAN. If they can communicate in a Layer 3 fashion (i.e. using a protocol such as IP or IPX), use a router. The router will treat each VLAN as a separate interface, which will have its own associated IP address space.

Problem	Solution
On a network of 30 switches, management traffic needs to be restricted to a separate domain. What is the best method for doing this while staying in contact with these switches?	At the switch where the management station is located, configure a port to use the new management VLAN as its native VLAN. Configure a host computer to act as a temporary management station. At each switch, configure the management VLAN to the new value. Contact with each individual switch will be lost immediately as they are being configured, but it should be possible re-establish communication from the temporary management station. After all switches have been taken to the new management VLAN, configure the ports of all attached management devices to use the new VLAN. **Note** Establishing a management domain is often accompanied with the establishment of an IP subnet specifically for the managed devices.

13.5 WLANs

The following describes common problems related to the WLANs.

Problem	Solution
Unable to wirelessly ping *any* devices located on the wired side of the client/bridge	The WDS must be enabled on the Access Point (AP) device to support a wireless station(s) configured for client/bridging functionality. For more information about enabling WDS on the RS900W, refer to "Configuring Advanced Settings (Page 249)".
Unable to apply *any* WLAN configuration changes	WLAN must be running before any configuration changes are made. Configuration changes will be ignored in any other state. For more information about determining the status of WLAN, refer to "Viewing the Status of the Wireless LAN (Page 235)".
The WLAN becomes unresponsive after modifying the configuration.	The WLAN must be resetting/restarting after one or more settings are modified. Typically, only a quick reset of the RF interface is required. However, a full reset of the RF and Ethernet interfaces may be necessary. For more information about resetting/restarting WLAN, refer to "Resetting/Restarting the Wireless LAN (Page 256)".
During the association phase, the station(s) status switches between *association* and *disassociation* states.	This is likely due to a mismatch in the pre-shared keys between the Access Point (AP) and station(s). Make sure the pre-shared key (Passphrase or WEP key) used is the same on both the AP and the station(s).
WPA2 authentication options are not supported in Windows XP.	This is by default. To add support for WPA2 functionality to Windows XP, install the following: • Windows XP Service Pack 2 • Windows XP WPA2 patch Visit http://www.microsoft.com for more information.
Association problems occur during the IP address assignment phase when using a Windows Vista client.	IPv6 is enabled by default in Windows Vista, which may create station association problems. Make sure the Distribution System is IPv6 capable. For example, it must support DHCPv6 if the Vista client is configured for dynamic address assignment. If association problems occur during the IP address assignment phase, disable IPv6, reboot Windows Vista, enable IPv4 and try again. Configuration of WPA2 authentication options is not supported in Windows Vista. Visit http://www.microsoft.com for more information.

Problem	Solution
Windows 2000 does not support IEEE 802.1x functionality.	For Windows 2000 to support 802.1X functionality, a subset of features was taken from Windows XP. Computers running Windows 2000 only support IEEE 802.1x authentication for wired and wireless network adapters using the Microsoft 802.1x Authentication Client, a utility included with Service Pack 4 [https:// www.microsoft.com/windows2000/downloads/servicepacks/default.mspx]. To configure a wireless client computer running Windows 2000, use the wireless configuration tool provided by the manufacturer of the wireless network adapter. **Note** WPA/WPA2 options are not supported in Windows 2000. Visit http://www.microsoft.com for more information.

Further Information

Siemens RUGGEDCOM
https://www.siemens.com/ruggedcom

Industry Online Support (service and support)
https://support.industry.siemens.com

Industry Mall
https://mall.industry.siemens.com

Siemens AG
Digital Industry
Process Automation
Postfach 48 48
90026 NÜRNBERG
GERMANY