SIEMENS

Configuration Manual

# SIMATIC NET

## Rugged Ethernet Switches

RUGGEDCOM ROS v5.4

For RST2228, RST2228P

Edition 12/2019

https://www.siemens.com

SIEMENS

# SIMATIC NET

# Rugged Ethernet Switches RUGGEDCOM ROS v5.4

**Configuration Manual**

**For RST2228, RST2228P**




**12/2019**
C79000-G8976-1451-01

# 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

© 12/2019 Subject to Change

# Table of Contents

# Preface

This guide describes v5.4 of ROS (Rugged Operating System) running on the RUGGEDCOM RST2228/RST2228P. 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

This document details CLI commands. A CLI command consists of a key command, parameters, options and/or user variables.

### Elements of a CLI Command

In the following CLI command, `interface` is the key command, { *name* } is a user-defined value, `vlan` and `type` are parameters, and `access` and `trunk` are fixed options.

**`interface`** { *name* } `vlan type [ access | trunk ]`

### Command Formatting

CLI commands are displayed in this document according to the following syntax rules:

| Convention | Description | Example |
| --- | --- | --- |
| Font | All commands, parameters, and options are displayed in a monospace font. | **`command`** `parameter` |
| User-Defined Values | Some parameters require a user-defined value. Values that need to be defined by you are wrapped in braces (curly brackets).<br>The value can be a string, such as a name or description.<br>The value may be a system component, such as an ID or interface. | **`command`** `parameter { value }` |

| Convention | Description | Example |
|---|---|---|
| | In all cases, the key word between the braces indicates the type of value to enter. | |
| Number Ranges | When the value of a parameter is a number within a specific range, the range is enclosed in braces (curly brackets). | **command** parameter { *0 - 10* } |
| Options | When multiple choices are available for the value of a parameter, all choices are wrapped in square brackets.<br>Choices are often comprised of fixed values, but may also include user-defined values and/or number ranges. | **command** parameter [ option1 \| option2 \| { *value* } \| { *0 - 10* } ] |

## Related Documents

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

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

### Product Notes

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

### User/Reference Guides

| Document Title | Link |
|---|---|
| RUGGEDCOM 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 |

### Catalogs

| Document Title | Link |
|---|---|
| RUGGEDCOM Modules Catalog for the RUGGEDCOM RST2228/RST2228P | https://support.industry.siemens.com/cs/ww/en/view/109752858 |
| RUGGEDCOM SFP Transceivers Catalog | https://support.industry.siemens.com/cs/ww/en/view/109482309 |

### 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 Reset Passwords | https://support.industry.siemens.com/cs/ww/en/view/109738242 |
| 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 |
| How to Control Bidirectional Traffic when Using Port Mirroring | https://support.industry.siemens.com/cs/ww/en/view/109759351 |

### Installation Guides

| Document Title | Link |
|---|---|
| RUGGEDCOM RST2228 Installation Guide | https://support.industry.siemens.com/cs/ww/en/view/109752856 |
| RUGGEDCOM RST2228P Installation Guide | https://support.industry.siemens.com/cs/ww/en/view/109757479 |

## 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 v5.4 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.

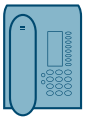
For more information about training services and course availability, visit https://-www.siemens.com or contact a Siemens Sales representative.

## 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:

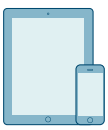
**Online**

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 v5.4 Software Configuration Manual for the RUGGEDCOM RST2228/RST2228P 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.

- **IPv4/IPv6 Support**

  RUGGEDCOM ROS supports both IPv4 and IPv6 addresses (for select features). For more information about support per protocol refer to "Internet Protocol Support (Page 11)".

- **Layer 3 Switching**

  RUGGEDCOM RST2228 can function as a Layer 3 switch. For information about how to configure Layer 3 switching rules in RUGGEDCOM ROS, refer to "*Layer 3* (Page 171)".

## 1.2 Security Recommendations

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

**Note**
Be aware that GPS signals have the potential to be either spoofed or jammed by a malicious third party.

### 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 113)".
- 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 129)".

- Use SSH public key authentication. For more information, refer to "Managing SSH/SSL Keys and Certificates (Page 129)".

**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.
- Unless required, automatic access to removable memory should be disabled to prevent unauthorized access. For more information about disabling access to removable memory, refer to "Enabling/Disabling Automatic Access to Removable Memory (Page 41)".
- 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 unauthorized access to the RUGGEDCOM ROS boot loader, which includes tools that may be used to gain complete access to the device. For more information about restricting access to the boot loader interface, refer to "Managing Access to the Boot Loader Interface (Page 39)".
- 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 70)". For more information about enabling ingress filtering, refer to "Configuring VLANs Globally (Page 147)".
- For increased security, enable ingress filtering on all ports by default. For more information about enabling ingress filtering, refer to "Configuring VLANs Globally (Page 147)".
- 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 280)".
- 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 57)" and the FAQ *How to*

*Implement Secure, Unattended Logging in ROS* (https://support.industry.siemens.com/cs/ww/en/view/109756843).

- 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, MMS, 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 121)".

**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 113)".
- 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 Logged Security Events

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

| Category | Event Message | Facility | Severity | Condition |
|---|---|---|---|---|
| SE_LOCAL_SUCCESSFUL_LOGON | {date} {time} INFO {temperature} Console user '{username}' logged in with admin level | local0 | Info | A user logged in successfully via a local interface to the device. |
| SE_LOCAL_UNSUCCESSFUL_LOGON | {date} {time} INFO {temperature} Failed Console user '{username}' login attempt | local0 | Info | Unsuccessful login attempt via a local interface to the device. |
| SE_NETWORK_SUCCESSFUL_LOGON | {date} {time} INFO {temperature} {protocol} user '{username}' logged in with admin level {ip address} | local0 | Info | A user logged in successful via a network interface to the device. |
| SE_NETWORK_UNSUCCESSFUL_LOGON | {date} {time} INFO {temperature} Failed {protocol} user '{username}' login attempt {ip address} | local0 | Info | Unsuccessful login attempt via a network interface to the device. |
| SE_LOGOFF | {date} {time} INFO {temperature} console user '{username}, cmd: Logged out | local0 | Info | A user logged out either manually or automatically due to a timeout via a local interface. |
| | {date} {time} INFO {temperature} {protocol} user '{username}' ({ip address}), cmd: Logged out | local0 | Info | A user logged out either manually or automatically due to a timeout via a network interface. |
| SE_USER_AUTH_RADIUS_SERVER_NOT_AVAILABLE | {date} {time} INFO {temperature} RADIUS Primary server is unreachable | local0 | Info | Unsuccessful RADIUS server access or no RADIUS response. |
| SE_ACCESS_PWD_CHANGED | {date} {time} INFO {temperature} 'admin' level password changed {date} {time} INFO {temperature} {protocol} user {'username'} {(ip address)} Passwords Admin Password - MODIFIED. | local0 | Info | An authenticated user changed its own password. |

| Category | Event Message | Facility | Severity | Condition |
|---|---|---|---|---|
| | {date} {time} INFO {temperature} 'guest' level password changed {date} {time} INFO {temperature} {protocol} user {'username'} {(ip address)} Passwords Guest Password - MODIFIED. | local0 | Info | An authenticated user changed the password of another user. |
| SE_USER_ACCOUNT_CHANGED | {date> {time} INFO {temperature} {protocol} user {username} {ip address}, Passwords Guest Username, old: {guest}, new: {new username} - MODIFIED. | local0 | Info | User account modified or assigned to another role. |
| SE_USER_ACCOUNT_DELETED | date> {time} INFO {temperature} {protocol} user {username} {ip address}, Passwords Guest Username, old: {username}, new:- MODIFIED. | local0 | Info | User account deleted. |
| SE_ACCOUNT_LOCKED_TEMP | {date} {time} WARN {temperature} Excessive failed {protocol} access/login attempts, service locked. | local0 | Warning | Brute force prevention via temporary locked user account. |
| SE_SESSION_LOCKED_INACTIVITY | {date} {time} INFO 37C Console user 'admin' , cmd: Logged out | local0 | Info | Session was locked after some time of inactivity. |
| SE_RAS_SESSION_TERMINATED_INACTIVITY | {date} {time} INFO 37C HTTPS user 'admin' logged out (IP:192.168.0.200). | local0 | Info | Remote session closed after some time of inactivity. |
| SE_UNSUCCESSFUL_RAS_LOGON | {date} {time} INFO {temperature} Failed {protocol} user '{username}' login attempt {ip address} | local0 | Info | Remote access user failed to log in the remote access device. |
| SE_RAS_LOGOFF | {date} {time} INFO {temperature} {protocol} user '{username}' {ip address}, cmd: loggd out | local0 | Info | Remote access user logged out from the remote access device. |
| SE_RAS_CONNECTION_CLOSED | {date} {time} INFO {protocol} user {'username'} closing connection {(ip address)} | local0 | Info | Remote access connection closed. |
| SE_SUCCESSFUL_DEVICE_IDENTIFICATION | {date} {time} INFO {temperature} {protocol} port 1 authorized addr {MAC address}, {VLAN ID} {date} {time} INFO{temperature} Secure port 1 learned addr {MAC address}, {VLAN ID} | local0 | Info | Device access granted because of successful 802.1X Port authentication. |
| SE_UNSUCCESSFUL_DEVICE_IDENTIFICATION | {date} {time}WARN 43C 802.1X port 1 auth failed, addr {MAC address}, {VLAN ID} | local0 | Warning | Device access denied because of unsuccessful 802.1X Port authentication. |
| SE_SUCCESSFUL_DEVICE_AUTHENTICATION | {date} {time} INFO {temperature}{protocol} user {username} (pub id 1 fingerprint:{value}) logged in with {role} access {ip address} | local0 | Info | Device authenticated successful via certificate-based authentication. |
| SE_AUDIT_LOG_CLEARED | {date} {time}INFO {temperature} Console user 'admin' , cmd: clearlogs {date} {time} INFO {temperature} clearlogs | local0 | Info | The user deleted the device local logging buffer. |

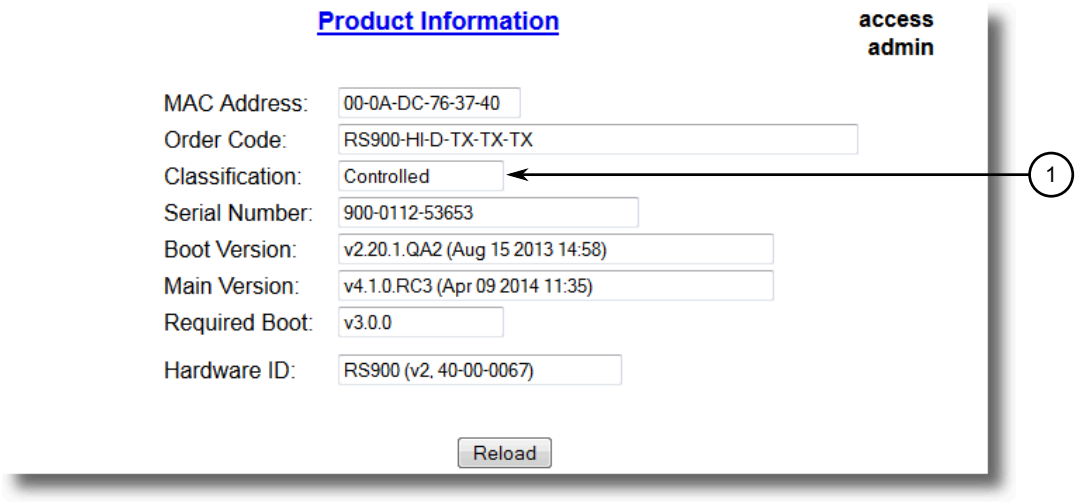
| Category | Event Message | Facility | Severity | Condition |
|---|---|---|---|---|
| SE_CONFIG_CHANGE | {date} {time} INFO {temperature} Console user '{username}', IP Services Inactivity Timeout, old: 5 min, new: Disable - MODIFIED {date} {time} INFO {temperature} Configuration changed | local0 | Info | The user changed defined configuration details. |
| | {date} {time} INFO {temperature} Console user '{username}', Load Factory Defaults Defaults Choice, old: None, new: All - MODIFIED. | local0 | Info | The user initiated a reset to factory defaults. |
| SE_SOFTWARE_INTEGRITY_CHECK_FAILED | {date} {time} NOTE {temperature} SFTP put file main.bin from {ip address} by user {date} {time} INFO Console user '{username}', cmd: xmodem receive main.bin {date} {time} ERRO Downloaded file main.bin is invalid: Bad signature {date} {time} NOTE Downloaded file with invalid signature (-7711) {date} {time} Downloaded file main.bin is invalid: Body CRC invalid | local0 | Error | Firmware/Software integrity verification identified an integrity error. |
| SE_BACKUP_SUCCESSFULLY_DONE | {date} {time} NOTE {temperature} config.csv copied to A:\config.csv | local0 | Notice | The system successfully created a backup when an external memory is mounted. |

## 1.4 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.




① Classification Box

Figure 1.1 Product Information Form (Example)

## 1.5 Supported Networking Standards

The following networking standards are supported by RUGGEDCOM ROS:

| Parameter | 10 Mbps | 100 Mbps | 1000 Mbps | 10000 Mbps | Notes |
|---|---|---|---|---|---|
| IEEE 802.1AB | • | • | • | • | Link Layer Discovery Protocol (LLDP) |
| IEEE 802.1D | • | • | • | • | MAC bridges |
| IEEE 802.1Q | • | • | • | • | VLAN (Virtual LAN) |
| IEEE 802.1p | • | • | • | • | Priority levels |
| IEEE 802.1x | • | • | • | • | Port-based network access control |
| IEEE 802.3 | • | | | | 10Base-T |
| IEEE 802.3u | | • | | | 100Base-TX/100Base-FX |
| IEEE 802.3z | | | • | | 1000Base-SX/LX |
| IEEE 802.3ab | | | • | | 1000Base-TX |
| IEEE 802.3ae | | | | • | 10GBase |
| IEEE 802.3af | • | • | • | | Power over Ethernet ports (RST2228P only) |
| IEEE 802.3at | • | • | • | | PoE+ ports, 4-pair (RST2228P only) |
| IEEE 802.3x | • | • | • | • | Full duplex operation |

## 1.6 Internet Protocol Support

RUGGEDCOM ROS supports both IPv4 addresses and IPv6 global unicast addresses for select features. For more information, refer to "Features Supported by IPv4 and/or IPv6 (Page 11)".

### 1.6.1 Features Supported by IPv4 and/or IPv6

The following table lists the features supported by IPv4 and/or IPv6 addresses.

| Feature | IPv4 | IPv6 |
|---|---|---|
| Ping | • | • |
| Telnet Server | • | • |
| SSH Server | • | • |
| SFTP Server | • | • |
| Web Server Access | • | • |
| SNMP Client (v1, v2c, v3) | • | • |
| Radius Client | • | • |
| TACACS+ Client | • | • |
| TFTP | • | • |
| NTP Server/Client | • | • |
| DHCP Client | • | |
| Remote Syslog Server | • | • |
| RSH | • | • |
| Serial Protocol | • | |
| ARP | • | |
| Network Discovery Messages[a] | | • |

[a] Supports network solicitation and network advertisement.

### 1.6.2 IPv4 Address

An IPv4 address is 32 bits in length and is written in dot-decimal notation consisting of four octets separated by periods. Each number can be zero to 255.

Example: 192.168.0.1

### 1.6.3 IPv6 Address

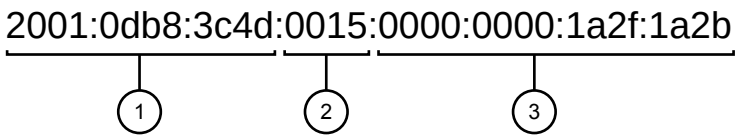
RUGGEDCOM ROS supports IPv6 global unicast addresses for management.

An IPv6 address is 128 bits in length and consists of eight 16-bit octets separated by a colons.

IPv6 addresses often contain consecutive hexadecimal fields of zeros. The double colon *(::)* can be used to compress zeros in an address. For example, IPv6 address FF00:5402:0:0:0:0:0:32 can be represented as FF00:5402::32.

An IPv6 address is formatted as follows:

- The leftmost three fields (48 bits) contain the site prefix. The prefix describes the public topology typically allocated to a site by an ISP.
- The center field is the 16-bit subnet ID, which is allocated to a specific site. The subnet ID describes the private topology, also known as the site topology, as it is internal to the site.
- The rightmost four fields (64 bits) contain the interface ID.




① Site Prefix
② Subnet ID
③ Interface ID

Figure 1.2 IPv6 Global Unicast Address Example

## 1.7 Port Numbering Scheme

For quick identification, each port on a RUGGEDCOM RST2228/RST2228P is assigned a number in the form of [slot]/[position].

- For modular media, the slot represents the location of the parent module in the chassis, while the number represents the location of the port in the module from left to right. Therefore, the fourth port on the module in slot 6 would be identified in RUGGEDCOM ROS as *6/4*.
- For fixed media, the slot number is 0 and ports are labeled left to right, top to bottom. Therefore, port 4 (bottom right) is identified in RUGGEDCOM ROS as 0/4.

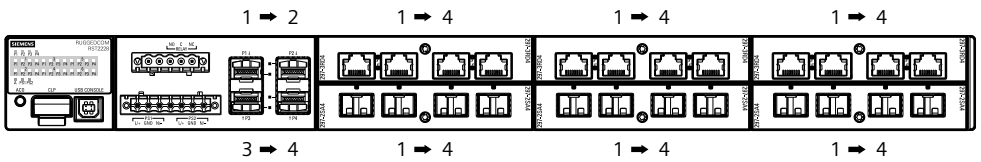



Figure 1.3 RUGGEDCOM RST2228/RST2228P Port Numbering (Typical)

Use these numbers to configure applicable features on select ports.

## 1.8 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. |

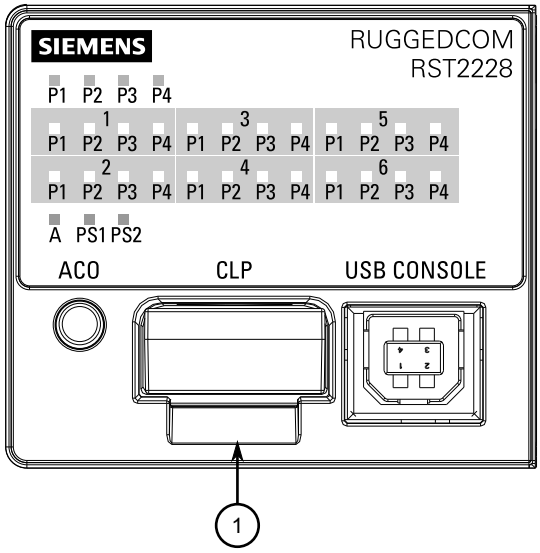
| Services | Port Number | Service Enabled/Disabled | Access Authorized | Note |
|---|---|---|---|---|
| ICMP | — | Enabled | No | |
| TACACS+ | TCP/49 (configurable) | Disabled (configurable) | Yes | |
| RADIUS | UDP/1812 to send (configurable), opens random port to listen to | Disabled (configurable) | 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 | |
| RCDP | — | Enabled (configurable) | Yes | |
| PTP (IEEE 1588) | UDP/319<br>UDP/320 | Disabled (configurable) | No | |

## 1.9 Removable Memory

The RST2228/RST2228P features a user-accessible memory slot that supports a standard ISO/IEC 9293-compatible FAT16 or FAT32 (File Allocation Table) file system on a RUGGEDCOM ROS  RUGGEDCOM CLP, an exchangeable storage medium used for device configuration data.

An important advantage of using a FAT-based file system for the removable memory is that its contents may be modified on any general purpose computer that has a USB Type C interface.

**Note**
The CLP will be automatically formatted to the FAT16 or FAT32 file system if any file system other than FAT16 or FAT32 is loaded on the card.




① CLP

Figure 1.4 Memory Slot

The primary purpose of the removable CLP is to provide a place to automatically backup the main firmware image and device configuration database, along with the ability to automatically restore the firmware image and/or the configuration from the backup. It can also be used to regain access to the device if data in the internal Flash memory is corrupted.

During normal operation, the device will automatically synchronize the files `main.bin` and `config.csv` on the device and the CLP. If a valid firmware file (`main.bin`) exists on the CLP, RUGGEDCOM ROS will load and run the firmware from the card.

When the device is rebooted, it will compare the files `main.bin` and `config.csv` on the device and the CLP. If the files on the device differ from those on the card, the device will upload the files from the card into its file system and apply them.

Other applications for the removable CLP include:

- Quickly recover from a hardware failure in the field
- Backup and restore firmware and configuration data
- Copy the firmware and configuration from one device to another
- Perform an automatic firmware upgrade
- Recover from a failed firmware upgrade or reconfiguration
- Automatically backup system logs

In addition to being able to automatically backup and restore firmware and configuration using the removable memory, RUGGEDCOM ROS supports an extended set of command line utilities for manipulating files on the system. The removable memory presents a disk paradigm, familiar to users of FAT-based file systems, complete with

CLI (Command Line Interface) commands like **`dir`**, **`copy`**, and **`move`**. For a complete list of available CLI commands, refer to "Available CLI Commands (Page 23)".

**Note**
For instructions on how to disable automatic access to the CLP, refer to "Enabling/Disabling Automatic Access to Removable Memory (Page 41)".

# 2 Using ROS

This chapter describes how to use RUGGEDCOM ROS.

## 2.1 Logging In

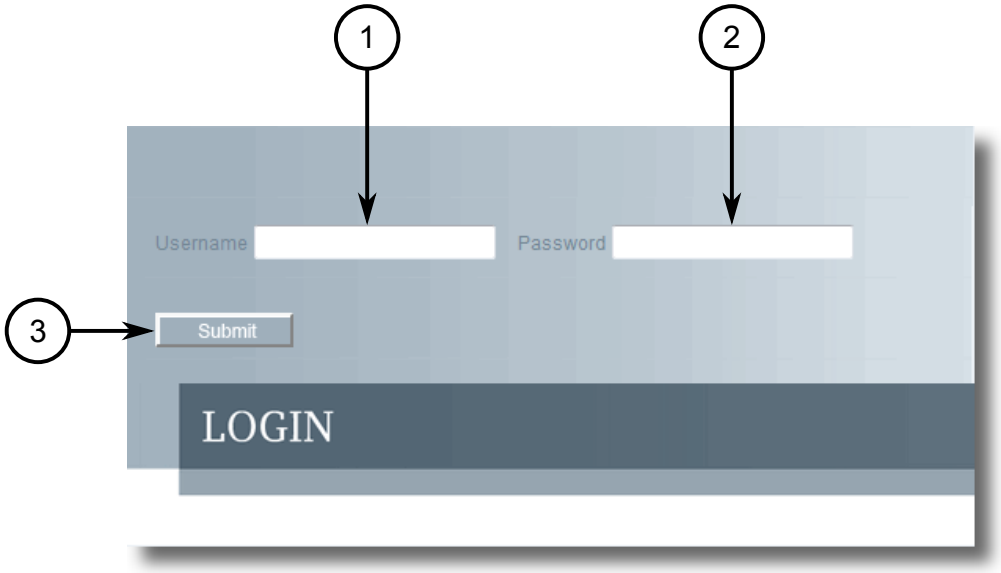
To log in to the device, do the following:

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 43)".

   Once the connection is established, the login form appears.


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 name and password is set on the device:

| User Name | Password |
|---|---|
| admin | admin |

**⚠ CAUTION**

To prevent unauthorized access to the device, make sure to change the default admin password before commissioning the device.

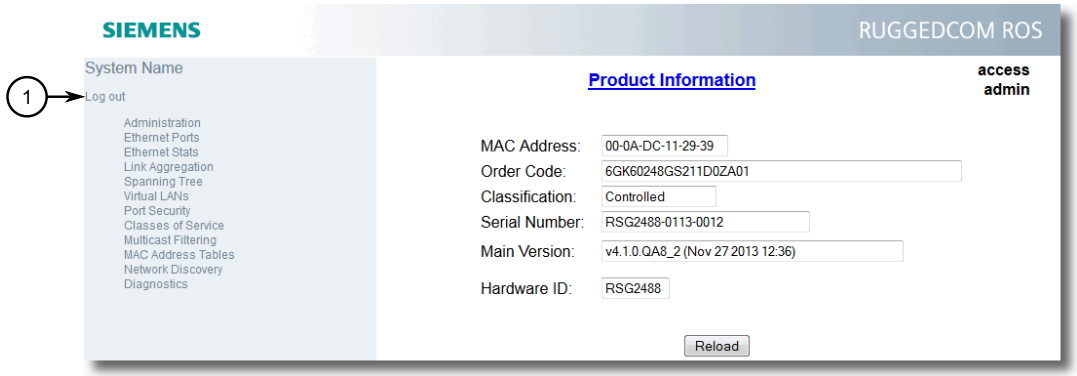
For more information about changing passwords, refer to "Configuring Passwords (Page 113)".

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**.




① Logout

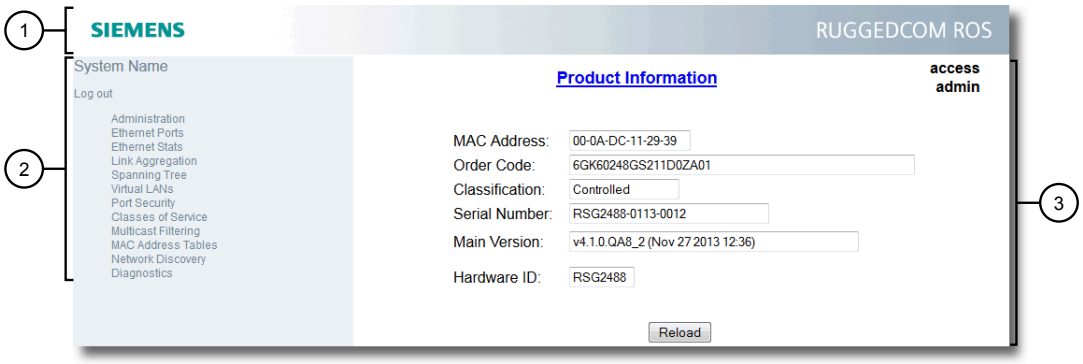
Figure 2.3 Web Interface (Example)

**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.



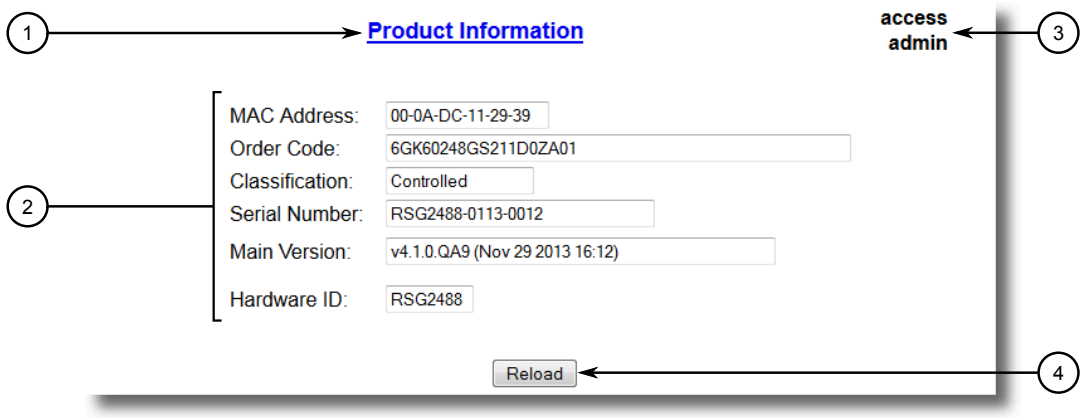

① Top Frame
② Side Frame
③ Main Frame

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 19)". |
| 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 100)".




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

Figure 2.5 Elements of a Typical Screen (Example)

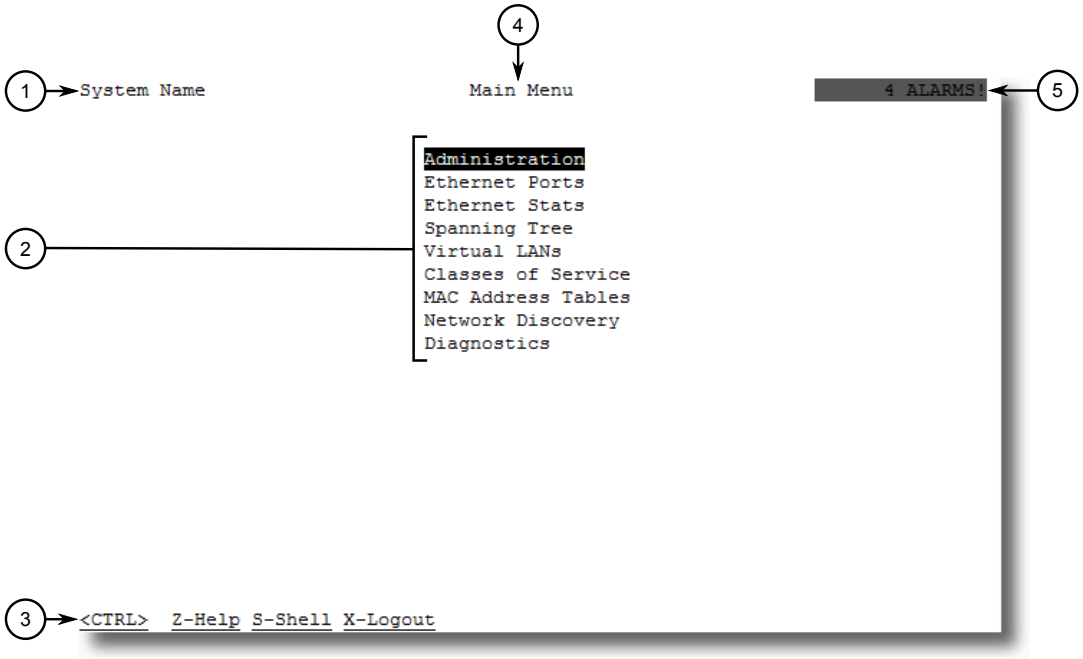
**Note**
If desired, the web interface can be disabled. For more information, refer to "Enabling/Disabling the Web Interface (Page 100)".

## 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 86)".

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 99)".

## 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.<br>**Note**<br>Before exiting a screen, RUGGEDCOM ROS will automatically prompt the user to save any changes that have not been committed.<br>**Note**<br>If removable memory (i.e. CLP) is present, configuration changes will update both `config.csv` on the flash and on the removable memory. |
| **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.<br>Optional and/or required parameters include:<br>• `all` displays all available alarms | Guest, Operator, Admin |
| **arp** | Displays the IP to MAC address resolution table. | Admin |
| **attrib** { *filename* } [ + \| - ] [ W \| H ] | Sets and removes file attributes. | Admin |
| **banner** { *-?* } { *-c* } { *-l* } { *-f* } { -s <enter>{ *text* } \| -s { *text* } } -e { *line_number* } -d { *line_number* } | Modifies the banner file `banner.txt`.<br>Optional and/or required parameters include:<br>• { *-?* } Displays the command options help.<br>• { *-c* } Clears the content of the banner file. | Admin |

| Command | Description | Authorized Users |
|---|---|---|
| | • { *-l* } Displays the banner file with line numbers indexed.<br>• { *-f* } Restores the factory default banner.<br>• `-s <enter> { text }` Inputs text into the banner file. The existing banner text is erased and replaced by the new text. Accepts up to 8190 characters and supports sets of control characters for editing text.<br>• `-s { text }` Inputs text into the banner file. Can be used to modify the file via terminal. The existing banner text is erased and replaced by the new text. Accepts up to 500 characters, maximum 250 words.<br>• `-e { line_number }` Edits the selected line of the banner file.<br>• `-d { line_number }` Deletes the selected line of the banner file. | |
| **chkdsk** | Checks the file system for disk errors. | Admin |
| **clearalarms** | Clears all alarms. | Operator, Admin |
| **clearethstats** `[ all \| { port } ]` | Clears Ethernet statistics for one or more ports.<br>Optional and/or required parameters include:<br>• `all` clears statistics for all ports<br>• { *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.<br>Optional and/or required parameters include:<br>• `all` clears statistics for all ports<br>• { *port* }is a comma separated list of port numbers (e.g. 1,3-5,7) | Admin |
| **clrstpstats** | Clears all spanning tree statistics. | Operator, Admin |
| **cls** | Clears the screen. | Guest, Operator, Admin |
| **copy** | Copies a target file to the internal or removable memory.<br>Examples:<br>• Copying a file from the removable memory to the internal memory<br>`copy a:\config.csv config.csv`<br>• Copying a file from the internal memory to the removable memory<br>`copy config.csv a:\config.csv` | Admin |
| **delete** `{ filename }` | Deletes the specified file on the removable memory card. | Admin |
| **dir** | Prints the directory listing of the internal memory. | Guest, Operator, Admin |
| **dir** `{ A: }` | Prints the directory listing of the removable memory card, if equipped. | 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. | Admin |

| Command | Description | Authorized Users |
|---|---|---|
| | **⚠ CAUTION**<br>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. | |
| **flashfiles** { info { *filename* } \| defrag } | A set of diagnostic commands to display information about the Flash filesystem and to defragment Flash memory.<br>Optional and/or required parameters include:<br>• info { *filename* } displays information about the specified file in the Flash file system<br>• defrag defragments files in the Flash file system<br>For more information about the **flashfiles** command, refer to "Managing the Flash File System (Page 36)". | Admin |
| **flashleds** { *time out* } | Flashes the LED indicators on the device for a specified number of seconds.<br>Optional and/or required parameters include:<br>• { *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 |
| **format** { *disk* } | Formats the specified disk (e.g. A:). | 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.<br>Optional and/or required parameters include:<br>• { *command* }is the command name. | Guest, Operator, Admin |
| **ipconfig** | Displays the current IP address, subnet mask and default gateway. | Guest, Operator, Admin |
| **label** { *disk* } { *string* } | Applies a label to the specified disk (e.g. A:). | Admin |
| **loaddflts** | Loads the factory default configuration. | Admin |
| **logout** | Logs out of the shell. | Guest, Operator, Admin |
| **logs** | Displays syslog entries in CLI shell. | Admin |
| **passwd** { *user_name* } { *new_password* } | Changes the selected user's password.<br>Optional and/or required parameters include:<br>• { *user_name* } is an existing user_name in RUGGEDCOM ROS.<br>• { *new_password* } is the new password that will replace the existing password of the selected user.<br>This command is unavailable in Telnet sessions. | Admin |
| **ping** { *address* } { { *count* } \| { *time out* } } | 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 num- | Guest, Operator, Admin |

| Command | Description | Authorized Users |
|---|---|---|
| | ber of pings with a specified time for which to wait for a response.<br>Optional and/or required parameters include:<br>• { *address* }is the target IP address.<br>• { *count* }is the number of echo requests to send. The default is 4.<br>• { *timeout* }is the time in milliseconds to wait for each reply. The range is 2 to 5000 seconds. The default is 300 milliseconds.<br>**Note**<br>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. | |
| **purgemac** | Purges the MAC Address table. | Operator, Admin |
| **random** | Display seeds or random numbers. | Admin |
| **rename** { *source* } { *destination* } | Renames the specified file. Add a path to new filename to move the file at the same time. | 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.<br>Optional and/or required parameters include:<br>• all resets all ports<br>• { *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 parameter specified } | 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.<br>Optional and/or required parameters include:<br>• { *port* }is the port number for which the data are required<br>• base displays the base information<br>• alarms displays alarms and warning flags<br>• diag displays measured data<br>• calibr displays calibration data for external calibration<br>• thr displays thresholds data<br>• all displays all diagnostic data | Admin |
| **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. | Admin |

| Command | Description | Authorized Users |
|---|---|---|
| | Optional and/or required parameters include:<br>• `default` sets all records in a table(s) to factory defaults<br>• `delete` allows for records to be deleted from a table<br>• `help` provides a brief description for any SQL command or clause<br>• `info` displays a variety of information about the tables in the database<br>• `insert` enables new records to be inserted into a table<br>• `save` saves the database to non-volatile memory storage<br>• `select` queries the database and displays selected records<br>• `update` enable existing records in a table to be updated<br>For more information about the **`sql`** command, refer to "Using SQL Commands (Page 32)". | |
| **`sshdigest`** | Displays the host key fingerprints of the device. | 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`.<br>Optional and/or required parameters include:<br>• { *keytype* }is the type of key, either rsa or ecc<br>• { *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 } } -sm { SecurityModel } -sl { SecurityLevel } -rv { ReadViewName } -wv { WriteViewName } -nv { NotifyViewName }` | Modifies SNMP access groups.<br>Optional and/or required parameters include:<br>• `-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<br>• `-d { GroupName }` deletes a specified access group<br>• `-sm { SecurityModel }` specifies the security model to be used<br>• `-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).<br>• `-rv { ReadViewName }` identifies the MIB tree(s) to which this entry authorizes read access. Allowable values are 'noView', 'V1Mib', or 'allOfMib'.<br>• `-wv { WriteViewName }` identifies the MIB tree(s) to which this entry authorizes write access. Allowable values are 'noView', 'V1Mib', or 'allOfMib'.<br>• `-nv { NotifyViewName }` identifies the MIB tree(s) to which this entry authorizes access for notifications. Allowable values are 'noView', 'V1Mib', or 'allOfMib'. | Admin |

| Command | Description | Authorized Users |
|---|---|---|
| **svcmod** -s { *snmp group* } { -i { *User Name* } \| -d { *User Name* } } -sm { *SecurityModel* } -g { *group* } | Modifies SNMP security-to-group maps.<br>Optional and/or required parameters include:<br>• -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<br>• -d { *UserName* } -sm { *SecurityModel* } deletes a specified user name and security profile<br>• -g { *group* } specifies the group to which the user name and secuirty profile belong | Admin |
| **svcmod** -s { *snmpuser* } { -i { *User Name* } \| -d { *User Name* } } -c { *Community* } -ip { *IP* } -ap { *protocol* } -ak { *key* } -pp { *protocol* } -pk { *key* } | Modifies SNMP users.<br>Optional and/or required parameters include:<br>• -i { *UserName* } creates a new user name as specified or modifies parameters associated with a specified user name, if it already exists<br>• -d { *UserName* } deletes a specified user name<br>• -c { *Community* } specifies the SNMP community string (for SNMPv1 or SNMPv2c).<br>• -ip { *IP* } configures a specified IP address to be used for SNMP authentication<br>• -ap { *protocol* } configures SNMP authetication via a specified authentication protocol. Allowable values are 'noAuth', 'HMACMD5', or 'HMACSHA'.<br>• -ak { *key* } sets a secret key (of 0 or 6+ characters) to be used for SNMP authentication<br>• -pp { *protocol* } configures data encryption via a specified privacy protocol. Allowable values are 'noPriv' or 'CBC-DES.'<br>• -ak { *key* } sets a secret key (of 0 or 6+ characters) to be used for data encyrption | Admin |
| **svcmod** -s { *radius* } { -ip { *1* } \| -ip { *2* } } -ip { *IP* } -ak { *AuthKey* } -pt { *Port* } -ux { *UsernameExtension* } -mr { *MaxRetries* } -to { *timeout* } | Modifies RADIUS security server.<br>Optional and/or required parameters include:<br>• -ip { *1* } sets the specified server as the primary RADIUS server<br>• -ip { *2* } sets the specified server as the backup RADIUS server<br>• -ip { *2* } -ip deletes the primary RADIUS server<br>• -ip { *1* } -ip deletes the backup RADIUS server<br>• -ip { *IP* } specifies the IP address of the RADIUS server<br>• -ak { *AuthKey* } specifies an authentication key to be shared with the RADIUS server<br>• -pt { *Port* } specifies the port number of the IP port on the RADIUS server<br>• -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), '%Sys- | Admin |

| Command | Description | Authorized Users |
|---|---|---|
| | Name%' (i.e. the system name given to the device), and '%SysLocation%' (i.e. the phyiscal location of the device).<br>• `-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.<br>• `-to { timeout }` specifies the number of milliseconds (ms) the authenticator will wait for a response from the RADUS server before reattempting authentication. | |
| **svcmod** `-s { tacacsplus } { -ip { 1 } \| -ip { 2 } } -ip { IP } -ak { AuthKey } -pt { Port } -ux { UsernameExtension } -mr { MaxRetries } -to { timeout } -apl { AdminPrivilege } -opl { OperPrivilege } -gpl { GuestPrivilege }` | Modifies TACACS+ security server.<br>Optional and/or required parameters include:<br>• `-ip { 1 }` sets the specified server as the primary TACACS+ server<br>• `-ip { 2 }` sets the specified server as the backup TACACS+ server<br>• `-ip { 2 } -ip` deletes the primary TACACS+ server<br>• `-ip { 1 } -ip` deletes the backup TACACS+ server<br>• `-ip { IP }` specifies the IP address of the TACACS+ server<br>• `-ak { AuthKey }` specifies an authentication key to be shared with the TACACS+ server<br>• `-pt { Port }` specifies the port number of the IP port on the TACACS+ server<br>• `-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).<br>• `-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.<br>• `-to { timeout }` specifies the number of milliseconds (ms) the authenticator will wait for a response from the TACACS+ server before reattempting authentication.<br>• `-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.<br>• `-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.<br>• `-gpl { GuestPrivilege }` specifies the level to which guest users are able to configure the TACACS+ server. Values must correspond with one or more op- | Admin |

| Command | Description | Authorized Users |
|---|---|---|
| | tion(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.<br>Optional and/or required parameters include:<br>• { *dest* }is the server's IP address | Guest, Operator, Admin |
| **tftp** { *address* } [ put \| get ] { *source* } { *target* } | Opens a TFTP session. Press **Ctrl-C** to close the session.<br>Optional and/or required parameters include:<br>• { *address* }is the IP address of the remote TFTP server<br>• put indicates TFTP will be uploading the source file to replace the destination file<br>• get indicates TFTP will be downloading the source file to replace the destination file<br>• { *source* }is the name of the source file<br>• { *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.<br>Optional and/or required parameters include:<br>• { *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.<br>Optional and/or required parameters include:<br>• -b browses through the existing user names in RUGGEDCOM ROS.<br>• -r { *username* } removes a specified user name to disable the account<br>• { *old_user_name* } and { *new_user_name* } define the user name to be changed<br>This command is unavailable in Telnet sessions. | Admin |
| **version** | Prints the software version. | Guest, Operator, Admin |
| **xmodem** { send \| receive } { *filename* } | Opens an XModem session.<br>Optional and/or required parameters include:<br>• send sends the file to the client.<br>• receive receives the file from the client.<br>• { *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 23)".
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 23)".

**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
   1/1  Port 1          1/1             1000T       Enabled  On    Auto  Auto  Off
   Off On
   1/2  Port 2          1/2             1000T       Enabled  On    Auto  Auto  Off
   Off On
   1/3  Port 3          1/3             1000T       Enabled  On    Auto  Auto  Off
   Off On
   1/4  Port 4          1/4             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
   1/1  Port 1          1/1             1000T       Enabled  On    Auto  Auto  Off
   Off on
   1/2  Port 2          1/2             1000T       Enabled  On    Auto  Auto  Off
   Off On
   1/3  Port 3          1/3             1000T       Enabled  On    Auto  Auto  Off
   Off On
   1/4  Port 4          1/4             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 a port within a specific slot.

Select a single port by specifying the slot and port number:

1/2

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

1/1-1/4

Select multiple ports by defining a comma-separated list:

1/1,1/4

Only ports within the same slot can be selected in a single range. To select a range of ports from different slots, define a comma-separated list of ranges:

1/1-1/4,2/1-2/4,3/1-3/3

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 23)".
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
------------------------------------------------------------------
main.bin                   0xFE959AE0   0x002C5493 (2905235)
syslog.txt                 0xFE100080   0x001BFF80 (1834880)
.
.
.

Free Space: 19792360
Used Space: 11664720
Fragmented Space: 5830423
------------------------------------------------------------------
```

### 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 23)".
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-MPC83
File name        : main.bin
Firmware version : v5.4.0
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 23)".
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.

**Note**

Access to BIST mode is disabled at the factory by default. All console inputs are ignored and users are directed automatically to the RUGGEDCOM ROS user interface.

To first enable access to BIST mode, do the following:

1. Using a PC/laptop, create a file named `bootoption.txt` and include the following line in the file:

   ```
   Security=no
   ```

2. Upload the file to the device and reboot the device.

**Note**

Access to BIST and the boot loader can be later revoked by changing `no` to `yes`.

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 USB console connection and a terminal application. For more information, refer to "Connecting Directly (Page 43)".
3. Reset the device. For more information, refer to "Resetting the Device (Page 97)".
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.

Alternatively, BIST functions can be accessed via factory mode. For more information about factory mode, refer to "Available CLI Commands (Page 23)".

## 2.9 Managing Access to the Boot Loader Interface

The following sections describe how to enable, disable, and access the boot loader interface in RUGGEDCOM ROS.

**Note**
Access to the boot loader interface is disabled at the factory by default on all devices running RUGGEDCOM ROS v5.4. All console inputs are ignored and users are directed automatically to the RUGGEDCOM ROS user interface.

**Note**
Siemens recommends disabling access to the boot loader interface following an upgrade from an earlier version of RUGGEDCOM ROS to RUGGEDCOM ROS v5.4. For more information about disabling the boot loader, refer to "Enabling/Disabling Access to the Boot Loader Interface (Page 39)".

### 2.9.1 Enabling/Disabling Access to the Boot Loader Interface

To enable or disable access to the boot loader interface, do the following:

#### Create File bootoption.txt

To enable or disable access to the boot loader, the file `bootoption.txt` must be available on the device.

If the file is not available, do the following:

1. Using a PC/laptop, create a file named `bootoption.txt` and include the following line in the file:

   ```
   Security=[no | yes]
   ```

   - *Security=no* enables access to the boot loader.
   - *Security=yes* disables access to the boot loader.
2. Upload the file to the device and reboot the device.

#### Enabling the Boot Loader

To enable access to the boot loader, do the following:

1. Using a PC/laptop, navigate to the file `bootoption.txt`.
2. Locate the following line and change from

   ```
   Security=yes
   ```

   to

   ```
   Security=no
   ```
3. Upload the file to the device and reboot the device.

### Disabling the Boot Loader

To disable access to the boot loader, do the following:

1. Using a PC/laptop, navigate to the file `bootoption.txt`.
2. Locate the following line and change from

   ```
   Security=no
   ```

   to

   ```
   Security=yes
   ```
3. Upload the file to the device and reboot the device.

## 2.9.2 Accessing the Boot Loader Interface

To access the boot loader interface, do the following:

1. Connect to RUGGEDCOM ROS through the RS-232 console connection and a terminal application. For more information, refer to "Connecting Directly (Page 43)".
2. Reset the device. For more information, refer to "Resetting the Device (Page 97)".
3. As soon as the device starts to boot up, press **Ctrl-Z**. The command prompt for Uboot appears.

   ```
   =>
   ```
4. Type **`help`** to view a list of all available options under Uboot.

## 2.9.3 Setting the Boot Source

By default, the device boots up from its internal flash memory. However, RUGGEDCOM ROS supports booting up from the inserted CLP if desired.

To set the boot source, do the following:

| IMPORTANT |
| --- |
| To allow boot up from the CLP, automatic access to the removable memory must be enabled. For more information, refer to "Enabling/Disabling Automatic Access to Removable Memory (Page 41)". |

1. Using a PC/laptop, create a file named `bootoption.txt` and include the following line in the file:

   ```
   BootOrderFirstRemovable=[no | yes]
   ```

   - *BootOrderFirstRemovable=no* boots from internal flash.
   - *BootOrderFirstRemovable=yes* boots from the CLP.
2. Upload the file to the device and reboot the device.

## 2.10 Enabling/Disabling Automatic Access to Removable Memory

RUGGEDCOM ROS can automatically synchronize firmware, configuration, and log files between a device and its RUGGEDCOM ROS CLP.

**⚠ WARNING**

Security hazard – risk of unauthorized access and/or exploitation. Unless required, automatic access to removable memory should be disabled.

To configure automatic access to removable memory, do the following:

1. Using a PC/laptop, create a file named `bootoption.txt`
2. To disable automatic access to removable memory, add the following line to the file:

   ```
   DisableAutoAccessRemovable = yes
   ```

   **Note**
   The **`DisableAutoAccessRemovable`** command only affects automatic actions. Even when automatic access to removable memory is disabled, users can manually copy files between a device and its CLP.

3. To re-enable automatic access to removable memory after having disabled it, add the following line to the file:

   ```
   DisableAutoAccessRemovable = no
   ```

4. Upload the file to the device.
5. Reboot the device.

# 3 Getting Started

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

| NOTICE |
| --- |
| Siemens recommends the following actions before commissioning the device:<br>• Replace the factory-provisioned, self-signed SSL certificate with one signed by a trusted Certificate Authority (CA)<br>• 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 or Ethernet connection for management and troubleshooting purposes. A console connection provides access to the console interface and CLI. An Ethernet connection provides access to the Web interface.

#### Using the USB 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 USB console port on the device. For more information about the USB console port, refer to the *RST2228/RST2228P Installation Guide*.

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 18)".

#### Using an Ethernet Port

To establish a direct Ethernet connection to the device, 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.

| Port | IP Address/Mask |
|---|---|
| All Ethernet ports | 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. Launch the SSH client on the workstation and connect to admin@{ipaddress}, where {ipaddress} is the IP address for the port that is connected to the network. The login prompt appears:

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

3. Log in to RUGGEDCOM ROS. For more information about logging in to RUGGEDCOM ROS, refer to "Logging In (Page 18)".

### 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 xv)".

   **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.

   **NOTICE**

   IPv6 addresses must be wrapped in square brackets (e.g. `https://[2001:db8:123::2228]`).

3. In the address bar, type the IP address for the port that is connected to the network. 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 18)". For more information about the Web interface, refer to "Using the Web Interface (Page 19)".

### 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 86)".

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 18)".

## 3.2 Installing the RUGGEDCOM USB Serial Console Driver (Windows Only)

Workstations running Microsoft Windows must have the RUGGEDCOM USB Serial Console driver installed before connecting to the console interface via the USB Type-B serial console port. This driver can be obtained from Siemens Customer Support.

To install the RUGGEDCOM USB Serial Console driver manually, do the following:

1. Obtain the installer from Siemens Customer Support. For more information about contacting Customer Support, refer to "Customer Support (Page xvi)".
2. Uninstall all previously installed USB-to-serial drivers from the workstation.
3. Make sure the USB serial console port is not connected to the workstation.
4. Double-click `Setup.exe`. The installation wizard appears.
5. Follow the on-screen instructions to install the driver.
6. Connect the workstation to the device using a USB Standard-A to Standard-B cable.
7. Open Device Manager by clicking the **Start** button, clicking **Control Panel**, clicking **System and Security**, and then, under **System**, clicking **Device Manager**.
8. Under **Ports (COM & LPT)**, verify the USB port is recognized.

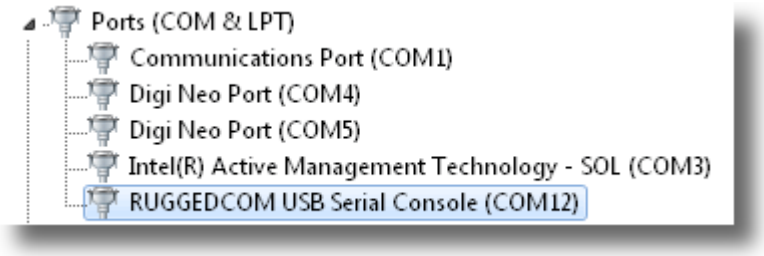



Figure 3.1 RUGGEDCOM USB Serial Console Port

## 3.3 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.

This screen displays the following information:

| Parameter | Description |
|---|---|
| `MAC Address` | **Synopsis:** ##-##-##-##-##-## where ## ranges 0 to FF<br>Shows the unique MAC address of the device. |
| `Order Code` | **Synopsis:** A string 57 characters long<br>Shows the order code of the device. |
| `Classification` | **Synopsis:** A string 15 characters long<br>Provides system classification.<br>The value `Controlled` indicates the main firmware is a Controlled release. The value `Non-Controlled` indicates the main firmware is a Non-Controlled release. The `Controlled` main firmware can run on Controlled units, but it can not run on Non-Controlled units. The `Non-Controlled` main firmware can run on both Controlled and Non-Controlled units. |
| `Serial Number` | **Synopsis:** A string 31 characters long<br>Shows the serial number of the device. |
| `Main Version` | **Synopsis:** A string 47 characters long<br>Shows the version and build date of the main operating system software. |
| `Hardware ID` | Shows the type, part number, and revision level of the hardware.<br>Example: RST2228, RST2228v2 |
| `Descr` | **Synopsis:** A string 57 characters long<br>The description of product based on Hardware ID, order code and classification. |

## 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.

This screen displays the following information:

| Parameter | Description |
|---|---|
| `Running Time` | **Synopsis:** DDDD days, HH:MM:SS<br>The amount of time since the device was last powered on. |
| `CPU Usage` | **Synopsis:** An integer between 0.0 and 100.0<br>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<br>The total size of RAM in the system. |
| `RAM Free` | **Synopsis:** An integer between 0 and 4294967295<br>The total size of RAM still available. |
| `RAM Low Watermark` | **Synopsis:** An integer between 0 and 4294967295<br>The size of RAM that have never been used during the system runtime. |
| `DMA RAM Free` | **Synopsis:** An integer between 0 and 4294967295<br>The total size of DMA RAM still available. |
| `DMA RAM Low Watermark` | **Synopsis:** An integer between 0 and 4294967295<br>The size of DMA RAM that have never been used during the system runtime. |
| `Temperature` | **Synopsis:** An integer between -32768 and 32767<br>The temperature on CPU board. |
| `Free Rx Bufs` | **Synopsis:** An integer between 0 and 4294967295<br>Free Rx Buffers. |
| `Free Tx Bufs` | **Synopsis:** An integer between 0 and 4294967295<br>Free Tx Buffers. |

## 4.3 Viewing the Status of the Power Supplies

To view the current status of the power supplies, navigate to ***Diagnostics » Power Supply Status***. The **Power Supply Status** table appears.

This table displays the following information:

| Parameter | Description |
|---|---|
| `ID` | **Synopsis:** An integer between 1 and 2<br>The ID of the power supply. |

| Parameter | Description |
|---|---|
| `Voltage` | **Synopsis:** An integer between 0 and 4294967295<br>The millivolt output voltage. |
| `Current` | **Synopsis:** An integer between 0 and 4294967295<br>The milliampere output current. |
| `Temperature` | **Synopsis:** An integer between -32768 and 32767<br>The temperature of the power supply. |
| `InStatus` | **Synopsis:** [ ---- \| Out of range \| Good ]<br>Specifies whether or not the power supply input voltage is in range.<br>For dual DC/DC power supplies, the input voltage range is between 36 and 72 V.<br>For dual AC/DC power supplies, the input voltage range for AC is between 85 and 264 VAC and, for DC, 95 and 300 VDC. |
| `OutStatus` | **Synopsis:** [ ---- \| Out of range \| Good ]<br>Specifies whether or not the power supply output voltage is in range. The output voltage range is 12 V +/- 1%. |
| `Calibration` | **Synopsis:** [ ---- \| Bad \| Good ]<br>Indicates whether or not the power supply is calibrated correctly. |

## 4.4 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
- RNA Parameters
- SNMP Users
- SNMP Security to Group Maps
- SNMP Access

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

- Time Zone
- DST Offset
- DST Rule

**Note**
MRMs or MRAs acting as Manager must be either physically disconnected or have the ring port disabled (i.e. MRP ring open) before restoring factory defaults, otherwise default configurations may not be restored for the following parameters:

- Port RSTP Parameters
- Global MRP Parameters
- MRP Instances

For more information about MRP rings, refer to "Managing the Media Redundancy Protocol (MRP) (Page 214)".

For more information about configuring port parameters, refer to "Configuring an Ethernet Port (Page 66)".

To restore factory defaults, do the following:

1. Navigate to ***Diagnostics » Load Factory Defaults***. The **Load Factory Defaults** form appears.
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 ]<br>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**.

## 4.5 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
- `fpga2228.bin` – 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

## 4.5.1 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 43)".
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 23)".

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 RST2228 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 97)"

## 4.5.2 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 43)".

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 23)".
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-MPC83_Main_v5.4.0.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 97)"

## 4.5.3 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 86)". |

1. Establish a connection between the device and the host computer. For more information, refer to "Connecting to ROS (Page 43)".
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-MPC83_Main_v5.4.0.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 97)"

### 4.5.4 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>
```

3. If the file has been uploaded, reset the device. For more information, refer to "Resetting the Device (Page 97)"

### 4.5.5 Uploading/Downloading Files Using the RUGGEDCOM CLP

The removable RUGGEDCOM CLP can be used to transfer files between the device, a host computer, and/or another device for a variety of purposes. For more information about the removable CLP and its uses, refer to "Removable Memory (Page 14)".

**⚠ CAUTION**

Security hazard - risk of unauthorized access and/or exploitation. For increased security, store files on an encrypted CLP. For more information about enabling data encryption, refer to "Configuring Data Encryption (Page 105)".

**⚠ CAUTION**

Configuration hazard - risk of reduced performance. Before sharing an encrypted configuration file with another device, make sure both devices share the same password/passphrase for deciphering encrypted configuration files. For more informa-

tion on how to enable data encryption, refer to "Configuring Data Encryption (Page 105)".

**⚠ CAUTION**

Configuration hazard - risk of data loss. After uploading or downloading a file, allow at least 20 seconds before removing the CLP to make sure the data has been fully transferred.

**Note**

The files on the CLP and the device can be renamed during the transfer. This is useful, for instance, when multiple versions of the firmware binary file are available on the CLP. The correct version can be transferred to the device and renamed `main.bin` to replace the version currently on the device.

To updload a file to the device or download a file from the device, do the following:

1. Insert the CLP in the device. For more information, refer to the *Installation Guide* for the device.
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 23)".
3. At the CLI prompt, type:
   - **Uploading**

     **copy** `a:\{` *sourceFile* `}  {` *destinationFile* `}`

   - **Downloading**

     **copy** `{` *sourceFile* `}  a:\{` *destinationFile* `}`
4. If the file has been uploaded, reset the device. For more information, refer to "Resetting the Device (Page 97)"

## 4.6 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.

**Note**
Syslog files backed up to the CLP are timestamped in the format of year, month and date (e.g. syslog.txt.20140101). This allows for multiple syslog files to be saved on the same card.

## 4.6.1 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 52)".

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

## 4.6.2 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.
2. Click **Confirm**.

## 4.6.3 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 59)".

1. Navigate to ***Administration » Configure Syslog » Configure Local Syslog***. The **Local Syslog** form appears.
2. Configure the following parameter(s) as required:

| Parameter | Description |
|---|---|
| `Local Syslog Level` | **Synopsis:** [ EMERGENCY \| ALERT \| CRITICAL \| ERROR \| WARNING \| NOTICE \| INFORMATIONAL \| DEBUGGING ]<br>**Default:** INFORMATIONAL<br>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 |

| Parameter | Description |
|---|---|
| | system sends any syslog messages generated by Error, Critical, Alert and Emergency. |

3. Click **Apply**.

## 4.6.4 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).

### 4.6.4.1 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.
2. Configure the following parameter(s) as required:

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

3. Click **Apply**.

### 4.6.4.2 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.

If remote syslog servers have not been configured, add the servers as needed. For more information, refer to "Adding a Remote Syslog Server (Page 60)".

### 4.6.4.3 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.
2. Click **InsertRecord**. The **Remote Syslog Server** form appears.
3. Configure the following parameter(s) as required:

| Parameter | Description |
|---|---|
| `IP Address` | **Synopsis:** ###.###.###.### where ### ranges from 0 to 255<br>Syslog server IP Address. |
| `UDP Port` | **Synopsis:** An integer between 1025 and 65535 or [ 514 ]<br>**Default:** 514<br>The UDP port number on which the remote server listens. |
| `Facility` | **Synopsis:** [ USER \| LOCAL0 \| LOCAL1 \| LOCAL2 \| LOCAL3 \| LOCAL4 \| LOCAL5 \| LOCAL6 \| LOCAL7 ]<br>**Default:** LOCAL7<br>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 ]<br>**Default:** DEBUGGING<br>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**.

### 4.6.4.4 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.
2. Select the server from the table. The **Remote Syslog Server** form appears.
3. Click **Delete**.

## 4.7 Managing Ethernet Ports

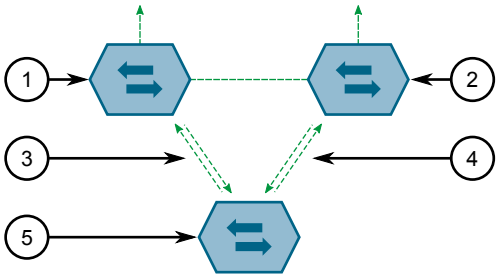
This section describes how to manage Ethernet ports.

**Note**
For information about configuring remote monitoring for Ethernet ports, refer to "Managing Remote Monitoring (Page 88)".

### 4.7.1 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 4.1 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:<br>• **Transmitting FEFI**<br>Transmits a modified link integrity signal in case a link failure is detected (i.e. no link signal is received from the link partner)<br>• **Detecting FEFI**<br>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).

## 4.7.2 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.

This table displays the following information:

| Parameter | Description |
|---|---|
| `Port` | **Synopsis:** 0/1 to maximum port number<br>The port number as seen on the front plate silkscreen of the device. |
| `Name` | **Synopsis:** A string 15 characters long<br>A descriptive name that may be used to identify the device connected on that port. |
| `Link` | **Synopsis:** [ ---- \| Down \| Up ]<br>The port's link status. |
| `Speed` | **Synopsis:** [ --- \| 10M \| 100M \| 1G \| 10G ]<br>The port's current speed. |

| Parameter | Description |
|---|---|
| Duplex | **Synopsis:** [ ---- \| Half \| Full ]<br>The port's current duplex status. |
| Media | **Synopsis:** A string 31 characters long<br>Provides user with the description of installed media type on the port for modular products. Please note that fiber media may be either Single Mode(SM), Multi Mode(MM), may be Short Distance, Long Distance or Very Long Distance with connectors like LC, SC, ST, MTRJ etc. For the modules with SFP/GBICs, media description is displayed as per SFF-8472 specification, if transceiver is plugged into the module. E.g. 10/100/1000TX RJ45, 100FX SM SC, 10FX MM ST, 1000SX SFP LC S SL M5. |

## 4.7.3 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.

This table displays the following information:

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

## 4.7.4 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.

This table displays the following information:

| Parameter | Description |
|---|---|
| `Port` | **Synopsis:** 1/1 to maximum port number<br>The port number as seen on the front plate silkscreen of the device. |
| `InOctets` | **Synopsis:** An integer between 0 and 18446744073709551615<br>The number of octets in received good packets (Unicast+Multicast+Broadcast) and dropped packets. |
| `OutOctets` | **Synopsis:** An integer between 0 and 18446744073709551615<br>The number of octets in transmitted good packets. |
| `InPkts` | **Synopsis:** An integer between 0 and 18446744073709551615<br>The number of received good packets (Unicast+Multicast+Broadcast) and dropped packets. |
| `OutPkts` | **Synopsis:** An integer between 0 and 18446744073709551615<br>The number of transmitted good packets. |
| `TotalInOctets` | **Synopsis:** An integer between 0 and 18446744073709551615<br>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<br>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<br>The number of good Broadcast packets received. |
| `InMulticasts` | **Synopsis:** An integer between 0 and 18446744073709551615<br>The number of good Multicast packets received. |
| `CRCAlignErrors` | **Synopsis:** An integer between 0 and 4294967295<br>The number of packets received which meet all the following conditions:<br>• Packet data length is between 64 and 1536 octets inclusive<br>• Packet has invalid CRC<br>• Collision Event has not been detected<br>• Late Collision Event has not been detected |
| `OversizePkts` | **Synopsis:** An integer between 0 and 4294967295<br>The number of packets received with data length greater than 1536 octets and valid CRC. |
| `Fragments` | **Synopsis:** An integer between 0 and 4294967295<br>The number of packets received which meet all the following conditions:<br>• Packet data length is less than 64 octets, or packet without SFD and is less than 64 octets in length |

| Parameter | Description |
|---|---|
| | • Collision Event has not been detected<br>• Late Collision Event has not been detected<br>• Packet has invalid CRC |
| Jabbers | **Synopsis:** An integer between 0 and 4294967295<br>The number of packets which meet all the following conditions:<br>• Packet data length is greater that 1536 octets<br>• Packet has invalid CRC |
| Collisions | **Synopsis:** An integer between 0 and 4294967295<br>The number of received packets for which Collision Event has been detected. |
| LateCollisions | **Synopsis:** An integer between 0 and 4294967295<br>The number of received packets for which Late Collision Event has been detected. |
| Pkt64Octets | **Synopsis:** An integer between 0 and 4294967295<br>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<br>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<br>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. |
| Pkt256to511Octets | **Synopsis:** An integer between 0 and 4294967295<br>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<br>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<br>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. |

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

## 4.7.5 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.
2. Select one or more Ethernet ports.
3. Click **Apply**.

## 4.7.6 Configuring an Ethernet Port

To configure an Ethernet port, do the following:

**Note**
Depending on the required link media type, an SFP port may require some explicit configuration. Before configuring an SFP port, refer to "SFP Transceiver Requirements (Page 73)".

1. Navigate to ***Ethernet Ports » Configure Port Parameters***. The **Port Parameters** table appears.
2. Select an Ethernet port. The **Port Parameters** form appears.

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

| Parameter | Description |
|---|---|
| `Port` | **Synopsis:** 1/1 to maximum port number<br>**Default:** 1/1<br>The port number as seen on the front plate silkscreen of the device. |
| `Name` | **Synopsis:** A string 15 characters long<br>**Default:** Port x<br>A descriptive name that may be used to identify the device connected on that port. |
| `Media` | **Synopsis:** [ 100TX \| 10FL \| 100FX \| 1000X \| 1000T \| 802.11g \| EoVDSL \| 100TX Only \| 10FL/100SX \| 10GX ]<br>**Default:** 100TX<br>The type of the port media. |
| `State` | **Synopsis:** [ Disabled \| Enabled ]<br>**Default:** Enabled<br>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.<br>**Note**<br>Disabling a port whose media type is set to `802.11g` disables the corresponding wireless module. |
| `AutoN` | **Synopsis:** [ Off \| On ]<br>**Default:** On<br>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 ]<br>**Default:** Auto<br>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.<br>AUTO means advertise all supported speed modes. |

| Parameter | Description |
|---|---|
| `Dupx` | **Synopsis:** [ Auto \| Half \| Full ]<br>**Default:** Auto<br>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.<br>AUTO means advertise all supported duplex modes. |
| `LFI` | **Synopsis:** [ Off \| On ]<br>**Default:** Off<br>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.<br>**Note**<br>This feature must not be enabled at both ends of a fiber link. |
| `Alarm` | **Synopsis:** [ On \| Off ]<br>**Default:** On<br>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 ]<br>**Default:** Do nothing<br>The action to be taken upon a port LinkDown event. Options include:<br>• `Do nothing` – No action is taken.<br>• `Admin Disable` – The port state is disabled. The State parameter must be set to Enabled before the link can be restored. |
| `Downshift` | **Synopsis:** [ Disabled \| Enabled ]<br>**Default:** Enabled<br>Enable or disable auto-negotiation on a gigabit (1000BASE-T) port with a two-pair twisted cable. If this option is enabled, the device is able to auto-negoatiate with another 1000BASE-T link partner using a two-pair cable and establish a link at 100Mbps or 10Mbps. |

**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**.

## 4.7.7 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.
2. Select an Ethernet port. The **Port Rate Limiting** form appears.
3. Configure the following parameter(s) as required:

| Parameter | Description |
|---|---|
| `Port` | **Synopsis:** 1/1 to maximum port number<br>**Default:** 1/1<br>The port number as seen on the front plate silkscreen of the device. |
| `Ingress Limit` | **Synopsis:** An integer between 64 and 1000000 or [ Disabled ]<br>**Default:** 1000<br>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 \| Multicast \| Mcast&FloodUcast \| Bcast&FloodUcast \| FloodUcast \| Bcast&Mcast \| Bcast&Mcast&FloodUcast \| All ]<br>**Default:** Broadcast<br>This parameter specifies the types of frames to be rate-limited on this port. It applies only to received frames:<br>• `Broadcast` – Only broadcast frames are limited<br>• `Multicast` – Only multicast frames are limited<br>• `Bcast&Mcast` – Broadcast and multicast frames are limited<br>• `Bcast&FloodUcast` – Broadcast and flooded unicast frames are limited<br>• `Mcast&FloodUcast` – Multicast and flooded unicast frames are limited<br>• `FloodUcast` – Only flooded unicast frames are limited |
| `Egress Limit` | **Synopsis:** An integer between 64 and 1000000 or [ Disabled ]<br>**Default:** Disabled<br>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**.

## 4.7.8 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 147)".
- 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.
2. Configure the following parameter(s) as required:

| Parameter | Description |
|---|---|
| `Port Mirroring` | **Synopsis:** [ Disabled \| Enabled ]<br>**Default:** Disabled<br>Enabling port mirroring causes all frames received and transmitted by the source port(s) to be transmitted out of the target port. |

| Parameter | Description |
|---|---|
| `Source Ports Egr` | **Synopsis:** Comma-separated list of ports<br>The port(s) being monitored. |
| `Source Ports Ingr` | **Synopsis:** Comma-separated list of ports<br>The port(s) being monitored. |
| `Target Port` | **Synopsis:** 1/1 to maximum port number<br>**Default:** 1/1<br>The port where a monitoring device should be connected. |

3. Click **Apply**.

## 4.7.9 Configuring Link Detection

To configure link detection, do the following:

1. Navigate to ***Ethernet Ports » Configure Link Detection***. The **Link Detection** form appears.
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 ]<br>**Default:** On_withPortGuard<br>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.<br>Three different settings are available for this parameter:<br>• `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.<br>• `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 |

| Parameter | Description |
|---|---|
| | 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.<br>• `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. |
| `Link Detection Time` | **Synopsis:** An integer between 100 and 1000<br>**Default:** 100<br>The time that the link has to continuously stay up before the "link up" decision is made by the device.<br>(The device performs de-bouncing of Ethernet link detection to avoid multiple responses to an occasional link bouncing event, e.g. when a cable is shaking while being plugged-in or unplugged). |

3. Click **Apply**.

## 4.7.10 Managing SFP Transceivers

RUGGEDCOM ROS supports Small Form-factor Pluggable (SFP) transceivers to provide a 1000Base-X, 100Base-FX, 1000Base-T or 100Base-TX link.

**Note**
Since 1000Base-X fiber SFP transceivers are standardized, RUGGEDCOM ROS supports most models of this type. For more information, refer to the RUGGEDCOM SFP Transceivers Catalog [https://support.industry.siemens.com/cs/ww/en/view/109482309].

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

1000Base-T copper SFP transceivers are not standardized. RUGGEDCOM ROS supports only selected models of this type.

**Note**
SFP transceivers are hot swappable.

When an SFP transceiver is inserted in to the SFP cage, the speed and auto-negotiation settings for the port are automatically adjusted to the appropriate values. For example, if a 1 G SFP transceiver is installed, the speed of the port is automatically changed to 1 G and auto-negotiation is set to *On*.

**Note**
Due to the uncertain latency introduced by the built-in PHY, the time accuracy of IEEE 1588 may be significantly degraded on a copper SFP port.

### 4.7.10.1 SFP Transceiver Requirements

RUGGEDCOM ROS supports Smart SFPs, where an SFP port will automatically configure itself to match the installed SFP transceiver. For example, when a 1000Base-X SFP transceiver is installed in a port that supports both 100Base-X and 1000Base-X, the port will automatically configure itself as a 1000Base-X port.

Depending on the required link media type, an SFP port may require some explicit configuration:

- For 10GBase-X links, the speed must be set to 10 Gbps, and auto-negotiation must be *Off* .
- For 100Base-FX links, the speed must be set to 100 Mbps, and auto-negotiation must be *Off* .
- For 1000Base-X links, the speed of the SFP port must be set to 1 Gbps, and auto-negotiation must be *On* .
- For 1000Base-T links via a Copper SFP Transceiver the speed of the SFP port can be set to 10/100/1000Mbps, or *Auto* in the case of Auto-negotiation.
- For 1000Base-T links via a Copper SFP Transceiver, auto-negotiation can be configured to *On* for all speeds. Auto-negotiation cannot be turned off for 1 Gbps speed.
- Duplex mode cannot be configured on the 10G SFP+ Ports and is always forced to full duplex.

For more information about configuring SFP transceiver ports and other Ethernet ports on the device, refer to "Configuring an Ethernet Port (Page 66)".

### 4.7.10.2 Displaying Information for an SFP Port

To display detailed information about an SFP port, do the following:

1. Log in to the device and access the CLI shell. For more information about accessing the CLI shell, refer to "Using the Command Line Interface (Page 23)".

2. Type the following command:

   **sfp** { *port* }

   Where:

   - { *port* } is the port number

   Information about the SFP port is displayed. For example:

```
>sfp
                        1/1

ID: SFP
Extended ID: GBIC/SFP function is defined by serial ID only
Connector: LC
Transceiver:
Gigabit Ethernet Compliance Codes:
1000LX
Fibre Channel link length:
Long Distance (L)
Fibre Channel transmitter technology:
Longwave laser (LC)
Fibre Channel transmission media:
Single Mode (SM)
Fibre Channel speed:
100 MBytes/Sec
Baud Rate, nominal: 1300 MBits/sec
Encoding type: 8B10B
Length(9um): 10 km
Length(9um): 10000 m
Length(50um): 550 m
Length(62.5um): 550 m
Length(Copper): Not specified
Vendor: xxxxxxx
IEEE company ID: xxxxxxx
Part number: xxxxxxxxxx
Revision: 0000
Laser wavelength: 1310 nm
>
```

## 4.7.11 Managing PoE Ports (For RST2228P Only)

The RUGGEDCOM RST2228/RST2228P  RST2228P features up to twenty-four IEEE 802.3at compliant Power over Ethernet (POE) ports powered by an external power supply. Through RUGGEDCOM ROS, these ports can be managed as follows:

- **Overload Protection**

  Prioritize and automatically enable/disable the lowest priority ports depending on power demands.

- **Power Conservation**

  Schedule ports to enable/disable automatically at specific times during the week to conserve power.

For more information about the PoE ports, refer to the *RUGGEDCOM RST2228/ RST2228P  RST2228P Installation Guide*.

### 4.7.11.1 Configuring PoE Ports Globally (For RST2228P Only)

To configure global settings for all Power-over-Ethernet (PoE) ports, do the following:

1. Navigate to ***Ethernet Ports » Configure/View PoE Parameters » Configure/View System PoE Parameters***. The **System PoE Parameters** form appears.
2. Configure the following parameter(s) as required:

| Parameter | Description |
|---|---|
| `Capacity` | **Synopsis:** An integer between 1 and 500 or [ Unlimited ]<br>**Default:** 500<br>The capacity of the PoE power supply source. That is, the maximum total output power can be provided by all PoE ports.<br>When total power consumption reaches this limit, some ports will be shutdown.<br>If set to Unlimited, the total output power is not limited by software. |
| `Capacity Per Module` | **Synopsis:** An integer between 1 and 140<br>**Default:** 120<br>The capacity allowed per PoE module. That is, the maximum output power that can be provided by the four PoE ports of each module.<br>When power consumption of a module reaches this limit, some module ports will be shutdown. |
| `Minimum Voltage` | **Synopsis:** An integer between 39 and 57<br>**Default:** 44<br>The minimum required voltage for PoE ports.<br>If PoE voltage dropped below this threshold, some ports will be shutdown.<br>The IEEE 802.3af standard specifies the PoE voltage range as 44 – 57 V.<br>The IEEE 802.3at standard specifies the PoE voltage range as 50 – 57 V. |
| `Reenable Time` | **Synopsis:** An integer between 10 and 4294967295<br>**Default:** 60<br>The time to wait to turn on PoE ports again after they were shutdown due to overload condition. |
| `Consumption` | **Synopsis:** An integer between 0 and 4294967295<br>Current total power consumption by all PoE devices. |

3. Click **Apply**.

### 4.7.11.2 Configuring a Specific PoE Port (For RST2228P Only)

To configure Power-over-Ethernet (PoE) settings for a specific Ethernet port, do the following:

1. Navigate to ***Ethernet Ports » Configure/View PoE Parameters » Configure/View Port PoE Parameters***. The **Port PoE Parameters** table appears.
2. Select an Ethernet port. The **Port PoE Parameters** form appears.
3. Configure the following parameter(s) as required:

| Parameter | Description |
|---|---|
| `Port` | **Synopsis:** 0/1 to maximum port number<br>**Default:** 0/1<br>The port number as seen on the front plate silkscreen of the device. |
| `Admin` | **Synopsis:** [ Disabled \| Enabled ]<br>**Default:** Enabled<br>This parameter allows to enable or disable supplying power by the port. |
| `Compliant` | **Synopsis:** [ No \| Yes ]<br>**Default:** Yes<br>Set this value to Yes (default) if the attachd powered device is compliant to the IEEE802.3at/IEEE802.3af standard.<br>Set this value to No if the attached device is a non-standard compliant PoE device such as the RUGGEDCOM WiN7200. In this case, power to the port is forced on without performing a signature test. |
| `Priority` | **Synopsis:** [ Normal \| Low ]<br>**Default:** Normal<br>Specify whether this port is of low priority. Low priority ports will be shutdown first if power supply is overloaded. Other ports may be shutdown as well if overload condition still exists after shutting down low priority ports. |
| `TwoPairMode` | **Synopsis:** [ Alt-A \| Alt-B ]<br>**Default:** Alt-A<br>Supported two-pair mode standard (ALT-A/ALT-B). All PoE ports must be off before changing this configuration. |
| `Powered` | **Synopsis:** [ No \| Yes ]<br>Whether or not power is currently supplied by the port. |
| `Class` | **Synopsis:** An integer between 0 and 100<br>PoE Class value that defines the minimum supplied power level. For more information, refer to the IEEE 802.1af and 802.1at standards.<br>0 = 15.4 W (default)<br>1 = 4.0 W<br>2 = 7.0 W |

| Parameter | Description |
|---|---|
| | 3 = 15.4 W<br>4 = 34.2 W |
| `Voltage` | **Synopsis:** An integer between 0 and 100<br>Supplied voltage level. |
| `Current` | **Synopsis:** An integer between 0 and 10000<br>Supplied current level. |

4. Click **Apply**.

### 4.7.11.3 Scheduling PoE Ports (For RST2228P Only)

To save power, Power-over-Ethernet (PoE) ports can be configured to shut down and restart at specific times during the week.

To configure a schedule for when a PoE port should be powered on, do the following:

1. Navigate to ***Ethernet Ports » Configure/View PoE Parameters » Configure PoE Scheduling***. The **PoE Scheduling** table appears.
2. Select an Ethernet port. The **PoE Scheduling** form appears.
3. Configure the following parameter(s) as required:

| Parameter | Description |
|---|---|
| `Port` | **Synopsis:** 0/1 to maximum port number<br>The port number as seen on the front plate silkscreen of the device. |
| `Sunday` | **Synopsis:** HH:MM (start time) hours (number of hours)<br>The time period of the day to power off this PoE port to save power.<br>Example:<br>'17:00 12' means that the port will be shut down at 17:00 (5:00PM) for 12 hours. So it will be turned on again at 5:00AM the next day. |
| `Monday` | **Synopsis:** HH:MM (start time) hours (number of hours)<br>The time period of the day to power off this PoE port to save power.<br>Example:<br>'17:00 12' means that the port will be shut down at 17:00 (5:00PM) for 12 hours. So it will be turned on again at 5:00AM the next day. |
| `Tuesday` | **Synopsis:** HH:MM (start time) hours (number of hours)<br>The time period of the day to power off this PoE port to save power. |

| Parameter | Description |
|---|---|
| | Example:<br>'17:00 12' means that the port will be shut down at 17:00 (5:00PM) for 12 hours. So it will be turned on again at 5:00AM the next day. |
| `Wednesday` | **Synopsis:** HH:MM (start time) hours (number of hours)<br>The time period of the day to power off this PoE port to save power.<br>Example:<br>'17:00 12' means that the port will be shut down at 17:00 (5:00PM) for 12 hours. So it will be turned on again at 5:00AM the next day. |
| `Thursday` | **Synopsis:** HH:MM (start time) hours (number of hours)<br>The time period of the day to power off this PoE port to save power.<br>Example:<br>'17:00 12' means that the port will be shut down at 17:00 (5:00PM) for 12 hours. So it will be turned on again at 5:00AM the next day. |
| `Friday` | **Synopsis:** HH:MM (start time) hours (number of hours)<br>The time period of the day to power off this PoE port to save power.<br>Example:<br>'17:00 12' means that the port will be shut down at 17:00 (5:00PM) for 12 hours. So it will be turned on again at 5:00AM the next day. |
| `Saturday` | **Synopsis:** HH:MM (start time) hours (number of hours)<br>The time period of the day to power off this PoE port to save power.<br>Example:<br>'17:00 12' means that the port will be shut down at 17:00 (5:00PM) for 12 hours. So it will be turned on again at 5:00AM the next day. |

4. Click **Apply**.

## 4.7.12 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.

### 4.7.12.1 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 80)".

This table displays the following information:

| Parameter | Description |
|---|---|
| `Port` | **Synopsis:** 1/1 to maximum port number<br>The port number as seen on the front plate silkscreen of the device. |
| `State` | **Synopsis:** [ Stopped \| Started ]<br>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<br>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<br>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:<br>1. Pick a particular port which calibration is needed.<br>2. Connect an Ethernet cable with a known length (e.g. 50m) to the port.<br>3. DO NOT connect the other end of the cable to any link partner.<br>4. Run cable diagnostics a few times on the port. OPEN fault should be detected.<br>5. 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.<br>6. Enter the calibration value and run cable diagnostics a few more times.<br>7. The distance to OPEN fault should now be at similar distance as the cable length.<br>8. Distance to fault for the selected port is now calibrated. |
| `Good` | **Synopsis:** An integer between 0 and 65535<br>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<br>The number of times OPEN is detected on the cable pairs of the selected port. |

| Parameter | Description |
|---|---|
| `Short` | **Synopsis:** An integer between 0 and 65535<br>The number of times SHORT is detected on the cable pairs of the selected port. |
| `Imped` | **Synopsis:** An integer between 0 and 65535<br>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<br>This field summarizes the results of the cable diagnostics performed so far.<br>• `Pass` – number of times cable diagnostics successfully completed on the selected port.<br>• `Fail` – number of times cable diagnostics failed to complete on the selected port.<br>• `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 58)".

### 4.7.12.2 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.
4. Select an Ethernet port. The **Cable Diagnostics Parameters** form appears.

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 81)".
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 79)".

### 4.7.12.3 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.
2. Select one or more Ethernet ports.
3. Click **Apply**.

### 4.7.12.4 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 80)". 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 58)".
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.

### 4.7.13 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.
2. Select one or more Ethernet ports to reset.
3. Click **Apply**. The selected Ethernet ports are reset.

## 4.8 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 interface must be configured as a management interface. By default,the management interface is the only interface that is able to run IP services such as DHCP, IEEE1588, Serial Server, and LLDP that affect the device. However, RUGGEDCOM ROS can be configured to allow auxiliary management interfaces to run the following services:

- Layer 3 Switching
- MMS
- Modbus
- Radius/TacPlus
- Remote Shell
- Remote Syslog
- SNMP
- SNTP
- SSH
- TFTP
- Telnet
- Web Server

For more information, refer to "Configuring IP Services (Page 86)".

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. |

## 4.8.1 Viewing a List of Switch IP Interfaces

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

If switch IP interfaces have not been configured, add IP interfaces as needed. For more information, refer to "Adding a Switch IP Interface (Page 83)".

## 4.8.2 Adding a Switch IP Interface

To add a switch IP interface, do the following:

1. Navigate to ***Administration » Configure IP Interfaces » Configure Switch IP Interfaces***. The **Switch IP Interfaces Table** appears.
2. Click **InsertRecord**. The **Switch IP Interfaces** form appears.
3. Configure the following parameter(s) as required:

| ⚠ WARNING |
| --- |
| **Security hazard – risk of unauthorized access and/or exploitation** |
| IP interfaces that belong to a management or auxiliary management VLAN must be connected to a trusted network. |

| ⚠ 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. |

**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.

**Note**
For IPv4, if a dotted decimal notation is configured for the subnet prefix (e.g. 255.255.255.0) it will be automatically converted to the equivalent number of bits (e.g. 24 bits).

| Parameter | Description |
|---|---|
| `Type` | **Synopsis:** [ VLAN ]<br>**Default:** VLAN<br>Specifies the type of the interface for which this IP interface is created. |
| `ID` | **Synopsis:** An integer between 1 and 4094<br>**Default:** 1<br>Specifies the the ID of the interface for which this IP interface is created. If interface type is VLAN, represents VLAN ID. |
| `Mgmt` | **Synopsis:** [ No \| Yes \| Aux ]<br>**Default:** No<br>Specifies whether the IP interface can support management functions.<br>• `Aux` – Supports management functions<br>• `Yes` – Supports management functions and dynamic address assignment such as DHCP<br>• `No` – Does not support management functions or dynamic address assignment |
| `IP Address Type` | **Synopsis:** [ Static \| Dynamic \| DHCP \| BOOTP ]<br>**Default:** Static<br>Specifies whether the IP address is static or dynamically assigned via DHCP or BOOTP. Option DYNAMIC is a common case of dynamically assigned IP address. It switches between BOOTP and DHCP until it gets the response from the relevant server.<br>Must be static for non management interfaces. |
| `IP Address` | **Synopsis:** Any valid IP address<br>**Default:** 192.168.0.1<br>Specifies the Internet Protocol address of this interface. An IP address is a 128-bit number that is notated by using eight fields of four hexadecimal digits, for which leading zeros can be omitted, delimited by colons. Consult offline documentation for more information. A version 4 address can be encoded by four decimal numbers from 0 through 255, separated by periods. Only a unicast IP addresses is allowed, which does not begin with "FF", or ranges from 1.0.0.0 to 233.255.255.255 for version 4. |

| Parameter | Description |
|---|---|
| `Subnet Prefix` | **Synopsis:** An integer between 0 and 128<br>**Default:** 24<br>Specifies the number of contiguous highest order bits that comprise the subnet mask for the current interface. For example, 24 would be equivalent to a 255.255.255.0 IPv4 subnet mask, while 64 would specify the subnet mask to consist of the highest order 64 bits (valid for IPv6).<br>**NOTICE**<br>Each IP interface must have a unique network address. |

4. Click **Apply**.

### 4.8.3 Deleting a Switch IP Interface

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

1. Navigate to ***Administration » Configure IP Interfaces » Configure Switch IP Interfaces***. The **Switch IP Interfaces** table appears.
2. Select the IP interface from the table. The **Switch IP Interfaces** form appears.
3. Click **Delete**.

## 4.9 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.

**NOTICE**

The default gateway will not be changed if the selected factory default configuration is reloaded.

### 4.9.1 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.

If IP gateways have not been configured, add IP gateways as needed. For more information, refer to "Adding an IP Gateway (Page 86)".

### 4.9.2 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.
2. Click **InsertRecord**. The **IP Gateways** form appears.
3. Configure the following parameter(s) as required:

| Parameter | Description |
| --- | --- |
| `Destination` | **Synopsis:** Any valid IP address<br>Specifies the IP address of destination network or host. For default gateway, both the destination and subnet are 0. |
| `Subnet` | **Synopsis:** An integer between 0 and 128<br>**Default:** 0<br>Specifies the destination IP subnet mask. For default gateway, both the destination and subnet are 0. |
| `Gateway` | **Synopsis:** Any valid IP address<br>Specifies the gateway to be used to reach the destination. |

4. Click **Apply**.

### 4.9.3 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.
2. Select the IP gateway from the table. The **IP Gateways** form appears.
3. Click **Delete**.

## 4.10 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.

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

| Parameter | Description |
|---|---|
| `Inactivity Timeout` | **Synopsis:** An integer between 1 and 60 or [ Disabled ]<br>**Default:** 5<br>Specifies when the console will timeout and display the login screen if there is no user activity. A value of zero disables time-outs. For Web Server users maximum timeout value is limited to 30 minutes. |
| `Telnet Sessions Allowed` | **Synopsis:** An integer between 1 and 4 or [ Disabled ]<br>**Default:** Disabled<br>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 ]<br>**Default:** 4<br>Limits the number of simultaneous web server users. |
| `TFTP Server` | **Synopsis:** [ Disabled \| Get Only \| Enabled ]<br>**Default:** Disabled<br>As this is an insecure protocol, this parameter allows user to limit or disable the service.<br>`Disabled` – disables read and write access through this service<br>`Get Only` – only allows to read files through this service<br>`Enabled` – allows to read and write files through this service |
| `ModBus Address` | **Synopsis:** An integer between 1 and 255 or [ Disabled ]<br>**Default:** Disabled<br>Determines the Modbus address to be used for Management through Modbus. |
| `SSH Sessions Allowed (Controlled Version Only)` | **Synopsis:** An integer between 1 and 4<br>**Default:** 4<br>Limits the number of SSH sessions. |
| `MMS Sessions Allowed` | **Synopsis:** An integer between 1 and 4<br>**Default:** Disabled<br>Limits the number of MMS sessions. A value of zero prevents any MMS access. |
| `RSH Server` | **Synopsis:** [ Disabled \| Enabled ]<br>**Default:** Disabled<br>Disables/enables Remote Shell access. |
| `IP Forward` | **Synopsis:** [ Disabled \| Enabled ]<br>**Default:** Disabled<br>Controls the ability of IP forwarding between VLANs in Serial Server or IP segments. |

| Parameter | Description |
|---|---|
| | **Note**<br>When Layer 3 switching is enabled and **Unicast Mode** is set to "Auto", IP forwarding must be enabled. |
| `Max Failed Attempts` | **Synopsis:** An integer between 1 and 20<br>**Default:** 10<br>Maximum number of failed access attempts per service within the Failed Attempts Window before blocking the service. Each service is allowed the maximum number of attempts before being blocked. This parameter resets to the default value when the factory default configuration is reloaded, however the counter for failed attempts on a particular service will not be reset. |
| `Failed Attempts Window` | **Synopsis:** An integer between 1 and 30<br>**Default:** 5<br>The time in minutes (min) in which the maximum number of failed login attempts must be exceeded before a service is blocked. The counter of failed attempts resets to 0 when the timer expires. This parameter resets to the default value when the factory default configuration is reloaded. |
| `Lockout Time` | **Synopsis:** An integer between 1 and 120<br>**Default:** 60<br>The time in minutes (min) the service remains locked out after the maximum number of failed access attempts has been reached. With the exception of the device management interface, this parameter resets to the default value when the factory default configuration is reloaded. |

3. Click **Apply**.

## 4.11 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.

### 4.11.1 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.

### 4.11.1.1 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.

If history controls have not been configured, add controls as needed. For more information, refer to "Adding an RMON History Control (Page 89)".

### 4.11.1.2 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.
2. Click **InsertRecord**. The **RMON History Controls** form appears.
3. Configure the following parameter(s) as required:

| Parameter | Description |
|---|---|
| `Index` | **Synopsis:** An integer between 1 and 65535<br>**Default:** 1<br>The index of this RMON History Contol record. |
| `Port` | **Synopsis:** 1/1 to maximum port number<br>**Default:** 1/1<br>The port number as seen on the front plate silkscreen of the device. |
| `Requested Buckets` | **Synopsis:** An integer between 1 and 5000<br>**Default:** 50<br>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<br>The number of buckets granted for this RMON collection history. This field is not editable. |
| `Interval` | **Synopsis:** An integer between 1 and 3600<br>**Default:** 1800<br>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<br>**Default:** Monitor<br>The owner of this record. It is suggested to start this string with word 'monitor'. |

4. Click **Apply**.

#### 4.11.1.3 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.
2. Select the history control from the table. The **RMON History Controls** form appears.
3. Click **Delete**.

### 4.11.2 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 101)".

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.

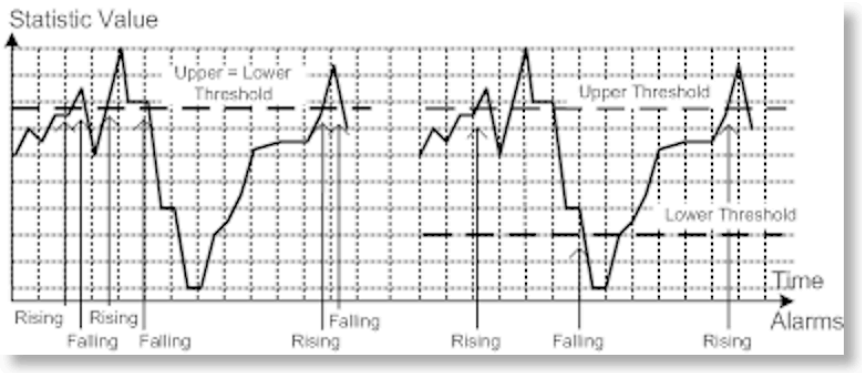



Figure 4.2 The Alarm Process

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*.

### 4.11.2.1 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.

If alarms have not been configured, add alarms as needed. For more information, refer to "Adding an RMON Alarm (Page 91)".

### 4.11.2.2 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.
2. Click **InsertRecord**. The **RMON Alarms** form appears.
3. Configure the following parameter(s) as required:

| Parameter | Description |
|---|---|
| `Index` | **Synopsis:** An integer between 1 and 65535<br>**Default:** 1<br>The index of this RMON Alarm record. |
| `Variable` | **Synopsis:** An integer<br>The SNMP object identifier (OID) of the particular variable to be sampled. Only variables that resolve to an ASN.1 primitive type |

| Parameter | Description |
|---|---|
| | 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.index1.index2... where index format depends on index object type. |
| `Rising Thr` | **Synopsis:** An integer between -2147483647 and 2147483647<br>**Default:** 0<br>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<br>**Default:** 0<br>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<br>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 ]<br>**Default:** delta<br>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<br>**Default:** 60<br>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 ]<br>**Default:** risingOrFalling<br>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'. |

| Parameter | Description |
|---|---|
| `Rising Event` | **Synopsis:** An integer between 0 and 65535<br>**Default:** 0<br>The index of the event that is used when a falling 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. |
| `Falling Event` | **Synopsis:** An integer between 0 and 65535<br>**Default:** 0<br>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<br>**Default:** Monitor<br>The owner of this record. It is suggested to start this string with-word 'monitor'. |

4. Click **Apply**.

#### 4.11.2.3 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.
2. Select the alarm from the table. The **RMON Alarms** form appears.
3. Click **Delete**.

### 4.11.3 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.

#### 4.11.3.1 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.

If events have not been configured, add events as needed. For more information, refer to "Adding an RMON Event (Page 94)".

### 4.11.3.2 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.
2. Click **InsertRecord**. The **RMON Events** form appears.
3. Configure the following parameter(s) as required:

| Parameter | Description |
|---|---|
| `Index` | **Synopsis:** An integer between 1 and 65535<br>**Default:** 3<br>The index of this RMON Event record. |
| `Type` | **Synopsis:** [ none \| log \| snmpTrap \| logAndTrap ]<br>**Default:** logAndTrap<br>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<br>**Default:** public<br>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<br>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. |
| `Description` | **Synopsis:** A string 127 characters long<br>**Default:** EV2-Rise<br>A comment describing this event. |
| `Owner` | **Synopsis:** A string 127 characters long<br>**Default:** Monitor<br>The owner of this event record. It is suggested to start this string withword 'monitor'. |

4. Click **Apply**.

#### 4.11.3.3 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.
2. Select the event from the table. The **RMON Events** form appears.
3. Click **Delete**.

## 4.12 Upgrading/Downgrading Firmware

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

### 4.12.1 Upgrading Firmware

Upgrading RUGGEDCOM ROS firmware, including the main, bootloader and FPGA firmware main 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.

| NOTICE |
| --- |
| RUGGEDCOM ROS devices only accept new firmware digitally-signed by Siemens. |

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

| IMPORTANT |
| --- |
| It is recommended to enable access to the bootloader interface during this procedure in case emergency recovery is needed (e.g. power interruption during the upgrade). For increased security, Siemens recommends disabling bootloader access following the upgrade. For more information about managing bootloader access, refer to "Enabling/Disabling Access to the Boot Loader Interface (Page 39)". |

To upgrade the RUGGEDCOM ROS firmware, do the following:

1. Enable access to the bootloader interface. For more information, refer to "Enabling/Disabling Access to the Boot Loader Interface (Page 39)".
2. Upload a different version of the binary firmware image to the device. For more information, refer to "Uploading/Downloading Files (Page 52)".
3. Reset the device to complete the installation. For more information, refer to "Resetting the Device (Page 97)".

4. 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-MPC83 Main Software v5.4.0 (Jan 01 5.4 00:01)
```

5. Disable access to the bootloader interface. For more information, refer to "Enabling/Disabling Access to the Boot Loader Interface (Page 39)".

### 4.12.2 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 18)".
3. Make a local copy of the current configuration file. For more information, refer to "Uploading/Downloading Files (Page 52)".

| 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 51)".
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 95)".
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.

## 4.13 Resetting the Device

To reset the device, do the following:

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

## 4.14 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 43)".
3. Restore all factory default settings for the device. For more information, refer to "Restoring Factory Defaults (Page 51)".
4. Access the CLI. For more information, refer to "Using the Command Line Interface (Page 23)".
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 52)".
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.

# 5 System Administration

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

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

| Parameter | Description |
|---|---|
| `System Name` | **Synopsis:** A string 24 characters long<br>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<br>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. |
| `Contact` | **Synopsis:** A string 49 characters long<br>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 52)".

Alternatively, the `banner.txt` file can be updated using the **`banner`** CLI command. For more information, refer to "Available CLI Commands (Page 23)".

## 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 86)".

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 23)".
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 90)".

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.

**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 23)".

For information about modifying a pre-configured alarm, refer to "Configuring an Alarm (Page 101)".

## 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.

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

1. Navigate to ***Diagnostics » Clear Latched Alarms***. The **Clear Latched Alarms** form appears.
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.
2. Select an alarm. The **Alarms** form appears.

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

| Parameter | Description |
|---|---|
| `Name` | **Synopsis:** A string 34 characters long or [ sys_alarm ]<br>**Default:** sys_alarm<br>The alarm name, as obtained through the **`alarms`** CLI command. |
| `Level` | **Synopsis:** [ EMRG \| ALRT \| CRIT \| ERRO \| WARN \| NOTE \| INFO \| DEBG ]<br>Severity level of the alarm:<br>• `EMRG` – The device has had a serious failure that caused a system reboot.<br>• `ALRT` – The device has had a serious failure that did not cause a system reboot.<br>• `CRIT` – The device has a serious unrecoverable problem.<br>• `ERRO` – The device has a recoverable problem that does not seriously affect operation.<br>• `WARN` – Possibly serious problem affecting overall system operation.<br>• `NOTE` – Condition detected that is not expected or not allowed.<br>• `INFO` – Event which is a part of normal operation, e.g. cold start, user login etc.<br>• `DEBG` – Intended for factory troubleshooting only.<br>This parameter is not configurable. |
| `Latch` | **Synopsis:** [ On \| Off ]<br>**Default:** Off<br>Enables latching occurrence of this alarm in the Alarms Table. |
| `Trap` | **Synopsis:** [ On \| Off ]<br>**Default:** Off<br>Enables sending an SNMP trap for this alarm. |
| `Log` | **Synopsis:** [ On \| Off ]<br>**Default:** Off<br>Enables logging the occurrence of this alarm in syslog.txt. |
| `LED & Relay` | **Synopsis:** [ On \| Off ]<br>**Default:** Off<br>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<br>**Default:** 60<br>Refreshing time for this alarm. |

4. Click **Apply**.

## 5.4.4 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 101)".

### 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 129)".

**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 |

## 5.5 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 v5.4 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.
2. Configure the following parameter(s) as required:

| Parameter | Description |
|---|---|
| `Encryption` | **Synopsis:** [ On \| Off ]<br>Enable/disable encryption of data in configuration file. |
| `Passphrase` | **Synopsis:** A string 31 characters long<br>This passphrase is used as a secret key to encrypt the configuration data.<br>Encrypted data can be decrypted by any device configured with the same passphrase. |
| `Confirm Passphrase` | **Synopsis:** A string 31 characters long<br>This passphrase is used as a secret key to encrypt the configuration data.<br>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 52)".

- 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,
```

## 5.6 Managing MMS

RUGGEDCOM ROS supports the IEC 61850 Manufacturing Message Specification (MMS) protocol.

### 5.6.1 Understanding MMS

RUGGEDCOM ROS supports the IEC 61850 standard, a management and monitoring protocol for intelligent electronic devices (IEDs) at electrical substations. The standard uses the Manufacturing Message Specification (MMS) as a transport protocol, while the bridge object model defines the objects to be polled or configured.

MMS specifies services for exchange of real-time data between networked devices and computer applications. It provides a generic messaging system for communication between industrial devices.

The data model used by MMS is based on logical nodes containing a set of data objects. These data objects contain a set of data attributes.

#### 5.6.1.1 MMS Reporting

The IEC 61850 report functionality is used to aggregate a group of data objects from logical nodes. These data objects can be sent to the client either as an unsolicited event-driven report or a time-based report initiated by the client.

The MMS Report is based on the *MMS Sessions Allowed* parameter, which controls how many clients can build MMS connections simultaneously to the RUGGEDCOM ROS bridge device. For more information about configuring MMS reporting, refer to "Configuring IP Services (Page 86)".

### 5.6.1.2 Reports/Data Sets

RUGGEDCOM ROS supports the following types of reports/data sets:

- **LLDPStatus**

  A time-based report belonging to the logical node LPLD, indicating the LLDP status of the device. It includes three data objects: LPLD.RemPortId (remote port identifier), LPLD.RemChsId (remote port chassis identifier) and LPLD.RemAddr (remote system management address).

- **PortLinkStatus**

  An event-driven report belonging to the logical node LPCP, indicating the device's physical port MAU status. It includes the data object LPCP.Mau (medium attachment unit link status).

- **PortStatistics**

  A time-based report belonging to the logical node LPCP, indicating the device's physical port working status. It includes four data objects: LPCP.AutoNgt (If true, the port is auto-negotiation), LPCP.RxCnt (Number of messages received since last reset), LPCP.TxCnt (number of messages sent since last reset) and LPCP.FerPort (frame error rate on the port).

- **RSTPStatus**

  An event-driven report belonging to the logical node LBRI, indicating the RSTP status of the device. It includes three data objects: LBRI.RstpRoot (device is RSTP root or not), LBRI.RstpTopoCnt (RSTP topology change count) and LBSP.RstpSt (RSTP port state).

- **SystemStatus**

  An event-driven report belonging to the logical node LPHD, indicating the device's working status. It includes two data objects: LPHD.PhyHealth (device health status) and LPHD.PwrSupAlm (device power supply alarm status).

**Note**
The files `ruggedcom.icd` (IEC61850 IED Capability Description of the device) and `ruggedcom.iid` (IEC61850 Instantiated IED Description of the device) list the logical nodes supported by RUGGEDCOM ROS. For information about downloading these files, refer to "Uploading/Downloading Files (Page 52)".

### 5.6.1.3 Supported Logical Nodes

RUGGEDCOM ROS supports the following logical nodes:

| Logical Node | Description |
|---|---|
| LLN0 | A common logical node providing generic information about the device as a whole, such as the vendor name and software version. |
| LPHD (Physical Device) | A logical node bearing system level information about the physical device, such as the system name and system description. |

| Logical Node | Description |
|---|---|
| LBRI (Bridge) | A logical node providing spanning tree related information when the device functions as a bridge, such as RSTP priority and RSTP hello time. |
| LPCP (Physical Communication Port) | A logical node providing port specific information for each physical interface on the device, such as port admin status and port auto negotiation status. |
| LPLD (Port Link Discovery) | A logical node providing port specific information related to LLDP (Link Layer Discovery Protocol) for each physical interface on the device, such as local port ID and remote port ID. |
| LBSP (Bridge Spanning tree Port) | A logical node providing port specific information related to spanning tree for each physical interface on the device, such as RSTP port state and RSTP edge port status. |
| LCMF (Communication channel MAC Filtering) | A logical node bearing filtering information related to Multicast MAC addresses, such as the white list of multicast MAC addresses and related VLAN IDs. |
| LCVF (Communication channel VLAN Filtering) | A logical node providing port specific information related to VLAN configuration, such as port VLAN ID and CoS priority. |

## 5.6.2 Viewing a List of Preconfigured MMS Reports

To view a list of MMS Reports pre-configured for the device, navigate to ***Administration » Configure MMS***. The **MMS Report Configuration** table appears.

This table displays the following information:

| Parameter | Description |
|---|---|
| `Name` | **Synopsis:** A string 32 characters long or [ SysStatus ]<br>**Default:** SysStatus<br>The MMS report name (i.e.the name of the data set). |
| `Status` | **Synopsis:** [ Disabled \| Enabled ]<br>**Default:** Disabled<br>The MMS reporting status initiated or changed by the client application. If any client application enables a data set's report functionality, the status of this data set is 'Enabled'. If no client application enables the data set's report functionality, the status of this data set is 'Disabled'. |
| `EventDriven` | **Synopsis:** [ False \| True ]<br>**Default:** True<br>The reporting criteria:<br>• `True` – Reporting is event-driven<br>• `False` – Reporting is time-based |
| `Period` | **Synopsis:** An integer between 30 and 1080 or [ Disabled ]<br>**Default:** 300<br>The reporting interval, in seconds, for time-based reports. This parameter is 'Disabled' for event-driven reports. |

For information about modifying an MMS report, refer to "Configuring an MMS Report (Page 110)".

## 5.6.3 Configuring an MMS Report

While all MMS reports are pre-configured on the device, some reports can be modified to suit the application. This includes enabling/disabling certain reports and changing the reporting interval.

To configuring an MMS report, do the following:

1. Navigate to ***Administration » Configure MMS***. The **MMS Report Configuration** table appears.
2. Select a report. The **MMS Report Configuration** form appears.
3. Configure the following parameter(s) as required:

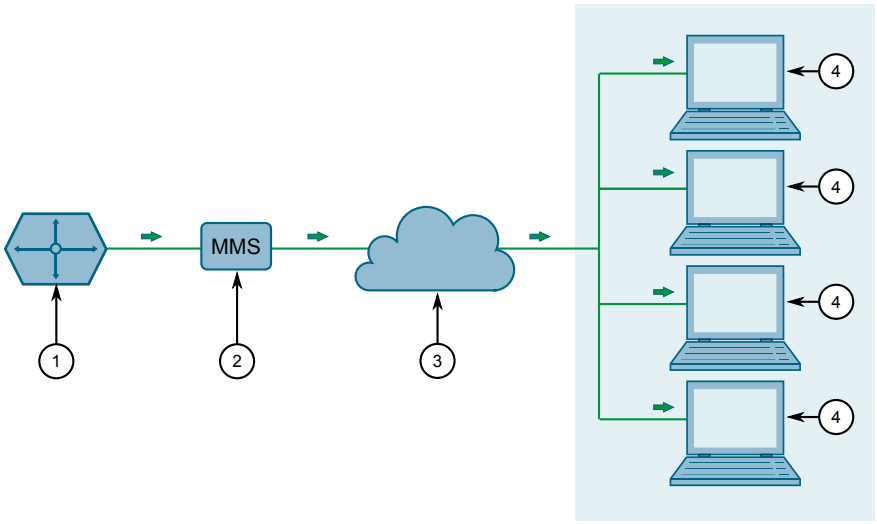
| Parameter | Description |
|---|---|
| `Period` | **Synopsis:** An integer between 30 and 1080 or [ Disabled ]<br>**Default:** 300<br>The reporting interval, in seconds, for time-based reports. This parameter is 'Disabled' for event-driven reports. |

4. Click **Apply**.

## 5.6.4 Example: Configuring MMS Reports

This example demonstrates how to configure the device to generate MMS reports.

The following topology depicts a scenario where four clients on a LAN are being sent MMS reports from RUGGEDCOM ROS:




① RUGGEDCOM ROS
② MMS Report
③ LAN
④ Client

Figure 5.1 Topology – MMS

To configure the device to receive MMS reports, do the following:

1. On the client side, do the following:

   **Note**
   Client configuartion is dependent on the MMS client being used. Refer to the OEM's operating instructions for specific configuration details.

   a. Enable or disable specific MMS reports, as desired. For a list of available reports in RUGGEDCOM ROS, refer to "Reports/Data Sets (Page 108)".

   b. Configure the device to provide either event-based or time-based reports, as desired.

2. In RUGGEDCOM ROS, do the following:

   a. Configure the number of MMS sessions allowed, to specify how many clients will be receiving reports. Per the topology, 4 sessions are allowed. For more information about configuring MMS sessions, refer to "Configuring IP Services (Page 86)".

   b. If time-based reports are selected on the client side, configure the reporing time interval as desired. For more information, refer to "Configuring an MMS Report (Page 110)".

3. To verify the configuration, make sure each client receives MMS reports from the device per the configuration.

# 6 Security

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.

   **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 continous 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 100)".

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

| Parameter | Description |
|---|---|
| `Auth Type` | **Synopsis:** [ Local \| RADIUS \| TACACS+ \| RADIUSorLocal \| TACACS+orLocal ]<br>**Default:** Local<br>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. |

| Parameter | Description |
|---|---|
| | Settings:<br>• `Local` – Authentication from the local Password Table.<br>• `RADIUS` – Authentication using a RADIUS server for network access only (HTTP/HTTPS, SSH, RSH, Telnet). For console access, authenticate from the local Password Table. If local authentication fails, then authenticate using RADIUS server.<br>• `TACACS+` – Authentication using a TACACS+ server for network access only (HTTP/HTTPS, SSH, RSH, Telnet). For console access, authenticate from the local Password Table. If local authentication fails, then authenticate using TACACS+ server.<br>• `RADIUSOrLocal` – Authentication using RADIUS. If the server cannot be reached, authenticate from the local Password Table.<br>• `TACACS+OrLocal` – Authentication using TACACS+. If the server cannot be reached, authenticate from the local Password Table. |
| `Guest Username` | **Synopsis:** A string 15 characters long<br>**Default:** guest<br>Related password is in field Guest Password; view only, cannot change settings or run any commands. |
| `Guest Password` | **Synopsis:** A string 19 characters long<br>Related username is in field Guest Username; view only, cannot change settings or run any commands. |
| `Confirm Guest Password` | **Synopsis:** A string 19 characters long<br>Related username is in field Guest Username; view only, cannot change settings or run any commands. |
| `Operator Username` | **Synopsis:** A string 15 characters long<br>**Default:** operator<br>Related password is in field Oper Password; cannot change settings; can reset alarms, statistics, logs, etc. |
| `Operator Password` | **Synopsis:** A string 19 characters long<br>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<br>Related username is in field Oper Username; cannot change settings; can reset alarms, statistics, logs, etc. |
| `Admin Username` | **Synopsis:** A string 15 characters long<br>**Default:** admin<br>Related password is in field Admin Password; full read/write access to all settings and commands. |
| `Admin Password` | **Synopsis:** A string 19 characters long<br>Related username is in field Admin Username; full read/write access to all settings and commands. |

| Parameter | Description |
|---|---|
| `Confirm Admin Password` | **Synopsis:** A string 19 characters long<br>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<br>**Default:** 1<br>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 43)".
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 121)".

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

| Parameter | Description |
|---|---|
| `Username Extension` | **Synopsis:** A string 127 characters long<br>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.<br>Delimited values include:<br>%Username%: The name associated with the user profile (e.g. admin, oper, etc.)<br>%IPaddr%: The management IP address of the switch that acts as a Network Access Server (NAS).<br>%SysName%: The system name given to the device.<br>%SysLocation%: The system location given to the device.<br>All pre-defined keywords are case-insensitive.<br>Examples:<br>%Username%@ABC.com<br>%Username%_%SysLocation%<br>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<br>Format: String<br>Number: 2<br>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.

For CLI commands related to configuring the RADIUS client on the device, refer to "Available CLI Commands (Page 23)".

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.
2. Select either **Primary** or **Backup** from the table. The **RADIUS Server** form appears.
3. Configure the following parameter(s) as required:

| Parameter | Description |
|---|---|
| `Server` | **Synopsis:** A string 8 characters long or [ Primary ]<br>**Default:** Primary<br>This field tells whether this configuration is for a Primary or a Backup Server. |
| `IP Address` | **Synopsis:** Any valid IP address<br>The Server IP Address. |
| `Auth UDP Port` | **Synopsis:** An integer between 1 and 65535<br>**Default:** 1812<br>The IP Port on server. |
| `Max Retry` | **Synopsis:** An integer between 1 and 10<br>**Default:** 2<br>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<br>**Default:** 10000<br>The amount of time in milliseconds the Authenticator will wait for a response from the authentication server. |
| `Reachable` | **Synopsis:** [ No \| Yes ]<br>The status of the server. |
| `Auth Key` | **Synopsis:** A string 31 characters long<br>The authentication key to be shared with server. |
| `Confirm Auth Key` | **Synopsis:** A string 31 characters long<br>The authentication key to be shared with server. |

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 23)".

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.
2. Select either **Primary** or **Backup** from the table. The **TACACS Plus Server** form appears.
3. Configure the following parameter(s) as required:

| Parameter | Description |
|---|---|
| `Server` | **Synopsis:** A string 8 characters long or [ Primary ]<br>**Default:** Primary<br>This field tells whether this configuration is for a Primary or a Backup Server. |
| `IP Address` | **Synopsis:** Any valid IP address<br>The Server IP Address. |
| `Auth TCP Port` | **Synopsis:** An integer between 1 and 65535<br>**Default:** 49<br>The IP Port on server. |
| `Max Retry` | **Synopsis:** An integer between 1 and 10<br>**Default:** 3<br>The maximum number of times the Authenticator will attempt to contact the authentication server to authenticate the user in case of any failure. |

| Parameter | Description |
|---|---|
| `Timeout` | **Synopsis:** An integer between 1000 and 120000<br>**Default:** 10000<br>The amount of time in milliseconds the Authenticator will wait for a response from the authentication server. |
| `Reachable` | **Synopsis:** [ No \| Yes ]<br>The status of the server. |
| `Auth Key` | **Synopsis:** A string 31 characters long or [ mySecret ]<br>**Default:** mySecret<br>The authentication key to be shared with server. |
| `Confirm Auth Key` | **Synopsis:** A string 31 characters long<br>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 120)".
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 as defined in the TACACS+ configuration file:

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

The *svcmod* CLI command is used to configure user privileges. The values entered must correspond with one or more option(s) defined numerically (between 0 and 15) in the TACACS+ configuration file located on the TACACS+ server.

For more information about the *svcmod* CLI command, refer to "Available CLI Commands (Page 23)".

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

| Parameter | Description |
|---|---|
| `Admin Priv` | **Synopsis:** An integer between 0 and 15 or a range (e.g. 2-14)<br>**Default:** 15<br>Privilege level to be assigned to the user. |

| Parameter | Description |
|---|---|
| `Oper Priv` | **Synopsis:** An integer between 0 and 15 or a range (e.g. 2-14)<br>**Default:** 2-14<br>Privilege level to be assigned to the user. |
| `Guest Priv` | **Synopsis:** An integer between 0 and 15 or a range (e.g. 2-14)<br>**Default:** 1<br>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 insert-

ed into the Static MAC Address Table and remain there until explicitly removed by the user.

### 6.4.1.2 Static MAC Address-Based Authentication in an MRP Ring

When port security is configured on an MRC, the MAC address of the MRM's ring ports must be configured in the **Static MAC Addresses** table for the ring to remain closed.

To allow communication (i.e. ping) between MRP devices in a ring, each device with port security enabled on its MRP ports must contain the MAC addresses of all devices in the ring in its **Static MAC Addresses** table.

For information about configuring MRP, refer to "Managing the Media Redundancy Protocol (MRP) (Page 214)".

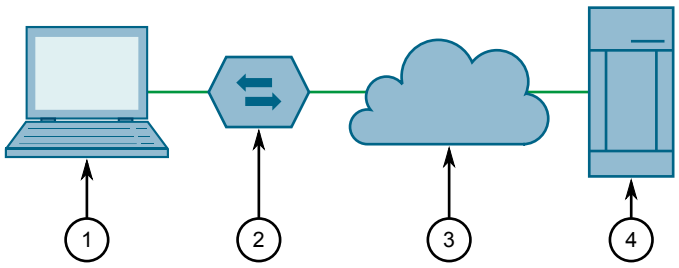
For information about configuring a static MAC address, refer to "Adding a Static MAC Address (Page 155)".

### 6.4.1.3 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 6.1 IEEE 802.1x General Topology

| NOTICE |
| --- |
| RUGGEDCOM ROS supports Protected Extensible Authentication Protocol (PEAP), EAP Transport Layer Security (EAP-TLS) and EAP-MD5. PEAP and EAP-TLS are more secure and are recommended if available in the supplicant. |

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

RUGGEDCOM 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.

#### 6.4.1.4 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.

### 6.4.1.5 Restricted VLANs

RUGGEDCOM ROS allows users to configure 802.1X ports in *Guest VLAN* or *Quarantine VLAN* mode, to limit services to clients when IEEE 802.1x or 802.1x/MAC-Auth authentication fails. For example, an administrator may choose to restrict access to only printers, internet or specific dowloads for unauthenticated users.

When a client fails to authenticate after a specified number of attempts, the configured port will switch automatically to either the Quarantine VLAN or the Guest VLAN, depending on the port security mode and the client's security setup:

- If a connected device supports 802.1x security but has failed authentication, the port will switch to the Quarantine VID.
- If a connected device is 802.1X incompatible and port security is set to 802.1X, the port will become a member of the Guest VLAN after the authentication times out.

An SNMP trap will be generated when a client device is placed in the Quarantine or Guest VLAN. An alarm will warn the user about the change in port status.

When a port is a member of the Quarantine VLAN, ROS will attempt to re-authenticate the client at configured intervals. Clients who fail to authenticate remain in the Quarantine VLAN until successfully re-authenticated, or until the physical link goes down. If re-authentication fails, the port remains a member of the Quarantine VLAN.

There are no re-authentication attempts for clients in Guest VLANs. When an EAPOL Start frame is received from the client, the port will revert to the unauthenticated state, removing the client's access from the Guest VLAN to continue with the authentication process.

The following table outlines Quarantine vs Guest port placement behavior following authentication failure:

| Port Security Mode | Client Security | Placement Following Authentication Failure |
|---|---|---|
| 802.1x | 802.1x Capable | Quarantine VLAN |
| | 802.1x Not Capable | Guest VLAN |
| 802.1x/MAC-Auth | 802.1x Capable | Quarantine VLAN |
| | 802.1x Not Capable | Quarantine VLAN |

For more information about configuring a Guest/Quarantine VLAN, refer to "Configuring Port Security (Page 126)".

### 6.4.1.6 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.

This table displays the following information:

| Parameter | Description |
|---|---|
| `Port` | **Synopsis:** 1/1 to maximum port number<br>Port on which MAC address has been learned. |
| `MAC Address` | **Synopsis:** ##-##-##-##-##-## where ## ranges 0 to FF<br>Authorized MAC address learned by the switch. |
| `VID` | **Synopsis:** An integer between 0 and 65535<br>VLAN Identifier of the VLAN upon which the MAC address operates. |

| Parameter | Description |
|---|---|
| `Sticky` | **Synopsis:** [ No \| Yes ]<br>This describes whether the authorized MAC address/Device can move to another port or not:<br>• `Yes` – authorized MAC address/Device cannot move to a different switch port<br>• `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 126)".
- Configure IEEE 802.1X. For more information, refer to "Configuring IEEE 802.1X (Page 128)".

### 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.
2. Select an Ethernet port. The **Ports Security** form appears.
3. Configure the following parameter(s) as required:

| Parameter | Description |
|---|---|
| `Port` | **Synopsis:** 1/1 to maximum port number<br>**Default:** 1<br>The port number as seen on the front plate silkscreen of the device. |
| `Security` | **Synopsis:** [ Off \| Static MAC \| 802.1X \| 802.1x/MAC-Auth ]<br>**Default:** Off<br>Enables or disables the port's security feature. Two types of port access control are available:<br>• 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.<br>• IEEE 802.1X standard authentication.<br>• 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. |

| Parameter | Description |
|---|---|
| `Quarantine VID` | **Synopsis:** An integer between 1 and 4096 or [ None ]<br>**Default:** None<br>The VLAN identifier for the Quarantine VLAN. Only applicable when the 'Security' field has been set to '802.1x' or '802.1x/MAC-Auth'. The port will be placed in the Quarantine VLAN if a client fails authentication. |
| `Guest VID` | **Synopsis:** An integer between 1 and 4096 or [ None ]<br>**Default:** None<br>The VLAN identifier for the Guest VLAN. Only applicable when the 'Security' field has been set to '802.1x'. The port will be placed in the Guest VLAN if a client does not support the 802.1x standard. |
| `Autolearn` | **Synopsis:** An integer between 1 and 16 or [ None ]<br>**Default:** None<br>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 ]<br>**Default:** Yes<br>Only applicable when the 'Security' field has been set to 'Static MAC'. Change the behaviour of the port to either sticky or non-sticky.<br>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.<br>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 ]<br>**Default:** Don't shutdown<br>Specifies for how long to shut down the port, if a security violation occurs. |

| Parameter | Description |
|---|---|
| `Status` | **Synopsis:** A string 31 characters long<br>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.
2. Select an Ethernet port. The **802.1X Parameters** form appears.
3. Configure the following parameter(s) as required:

| Parameter | Description |
|---|---|
| `Port` | **Synopsis:** 1/1 to maximum port number<br>**Default:** 1<br>The port number as seen on the front plate silkscreen of the device. |
| `txPeriod` | **Synopsis:** An integer between 1 and 65535<br>**Default:** 30<br>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<br>**Default:** 60<br>The period of time not to attempt to acquire a Supplicant after the authorization session failed. |
| `reAuthEnabled` | **Synopsis:** [ No \| Yes ]<br>**Default:** No<br>Enables or disables periodic re-authentication. |

| Parameter | Description |
|---|---|
| reAuthPeriod | **Synopsis:** An integer between 60 and 86400<br>**Default:** 3600<br>The time between periodic re-authentication of the Supplicant. |
| reAuthMax | **Synopsis:** An integer between 1 and 10<br>**Default:** 2<br>The number of re-authentication attempts that are permitted before the port becomes unauthorized. |
| suppTimeout | **Synopsis:** An integer between 1 and 300<br>**Default:** 30<br>The time to wait for the Supplicant's response to the authentication server's EAP packet. |
| serverTimeout | **Synopsis:** An integer between 1 and 300<br>**Default:** 30<br>The time to wait for the authentication server's response to the Supplicant's EAP packet. |
| maxReq | **Synopsis:** An integer between 1 and 10<br>**Default:** 2<br>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 ECC 256 self-signed SSL certificate and an RSA 2048 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. 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 52)".

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 135)".

## 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 52)".
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 23)".

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 58)".

#### 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 23)".
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 23)".
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.<br>**Note**<br>The user public key ID must be a number between 0 and 9999.<br>• { *current_ID* } is the ID currently assigned to the public key<br>• { *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.<br>• { *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.<br>• { *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.<br>• { *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 23)".
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.<br>• { *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 131)".

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 131)".

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
sml/zPSwYQ0SbQ9aOAJnpLc2HUkK0lji/0oKVI7y9MMc4B+bGu4W4OnryP7oFpnp
YYHt5PJY+zvLw/Wa+u3NOVFHkF1tGyfVBMXeV36nowPo+wrVMolAEgIVALLTnfpW
maV6uh6RxeE1d4XoxSg2
-----END DSA PRIVATE KEY-----
```

# 7 Layer 2

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 two ways:

- **Explicitly**

  Static VLANs can be created in the switch. For more information about static VLANs, refer to "Managing Static VLANs (Page 149)".

- **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.

For more information about VLANs, refer to "VLAN Concepts (Page 137)".

### 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

By default, all management traffic belongs to the management VLAN. Auxiliary management VLANs can be configured to move management traffic; however, BOOTP, DHCP, and LLDP traffic can only belong to the management VLAN.

The management VLAN is configurable and always defaults to VLAN 1. This VLAN is also the default native VLAN for all ports. Changing the management VLAN can be used to restrict management access to a specific set of users.

**⚠ WARNING**

Security hazard – risk of unauthorized access and/or exploitation. IP interfaces that belong to the management VLAN must be connected to a trusted network.

#### 7.1.1.4 Auxiliary Management VLANs

In addition to the management VLAN, auxiliary management VLANs can forward management traffic associated with the following services:

- MMS
- Modbus
- Radius/TacPlus
- Remote Shell
- Remote Syslog
- SNMP
- SNTP
- SSH
- TFTP
- Telnet
- Web Server

However, unlike the management VLAN, auxiliary management VLANs cannot forward BOOTP, DHCP, or LLDP traffic.

No auxiliary management VLANs are configured by default. Up to 254 auxiliary management VLANs can be configured. Configuring auxiliary management VLANs can be used to restrict or expand management access across a set of users.

| ⚠ WARNING |
| --- |
| Security hazard – risk of unauthorized access and/or exploitation. IP interfaces that belong to an auxiliary management VLAN must be connected to a trusted network. |

### 7.1.1.5 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 140)".

| 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.<br>*Multiple-VLAN End Devices*: Implement connections to end devices that support multiple VLANs at the same time. |

### 7.1.1.6 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

#### 7.1.1.7 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 149)".

#### 7.1.1.8 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)

#### 7.1.1.9 GARP VLAN Registration Protocol (GVRP)

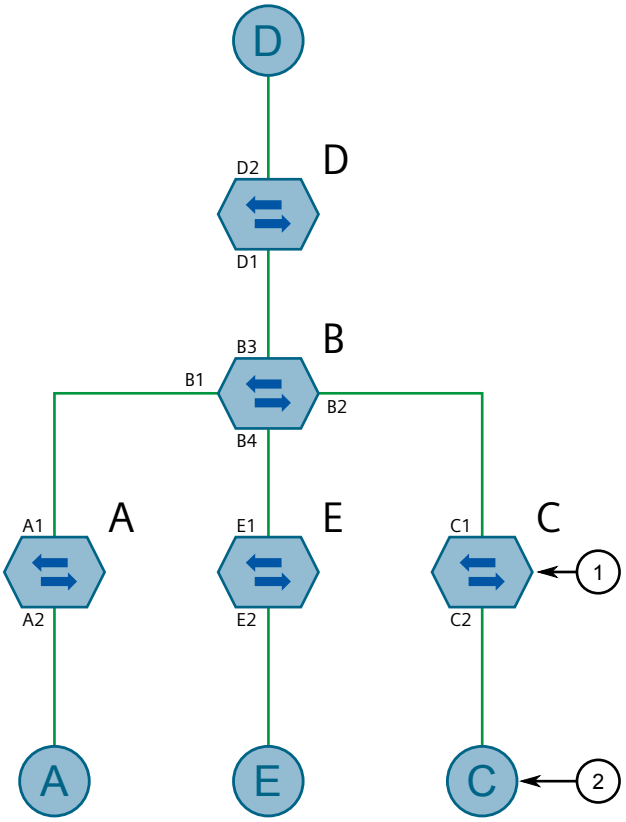
GARP VLAN Registration Protocol (GVRP) is a standard protocol built on GARP (Generic Attribute Registration Protocol) to automatically distribute VLAN configuration information in a network. Each switch in a network needs only to be configured with VLANs it requires locally. VLANs configured elsewhere 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 147)".

#### 7.1.1.10 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 147)".

**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.

#### 7.1.1.11 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.

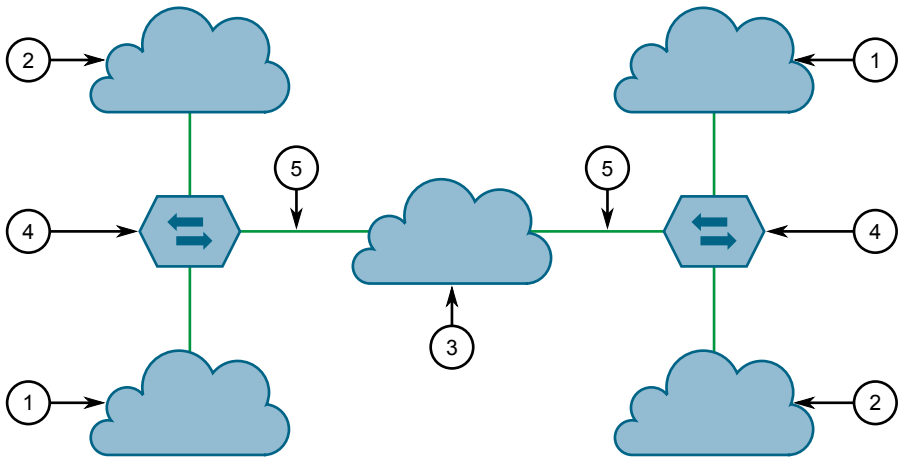
The following figure shows an example of traffic flow using QinQ.

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.

### 7.1.1.12 VLAN Advantages

The following are a few of the advantages offered by VLANs.

#### Traffic Domain Isolation

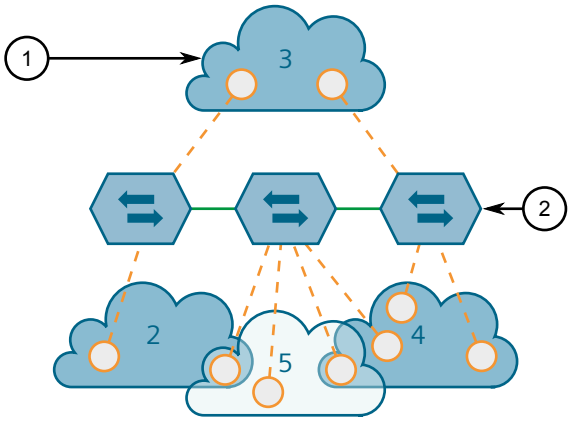
VLANs are most often used for their ability to restrict traffic flows between groups of devices.

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

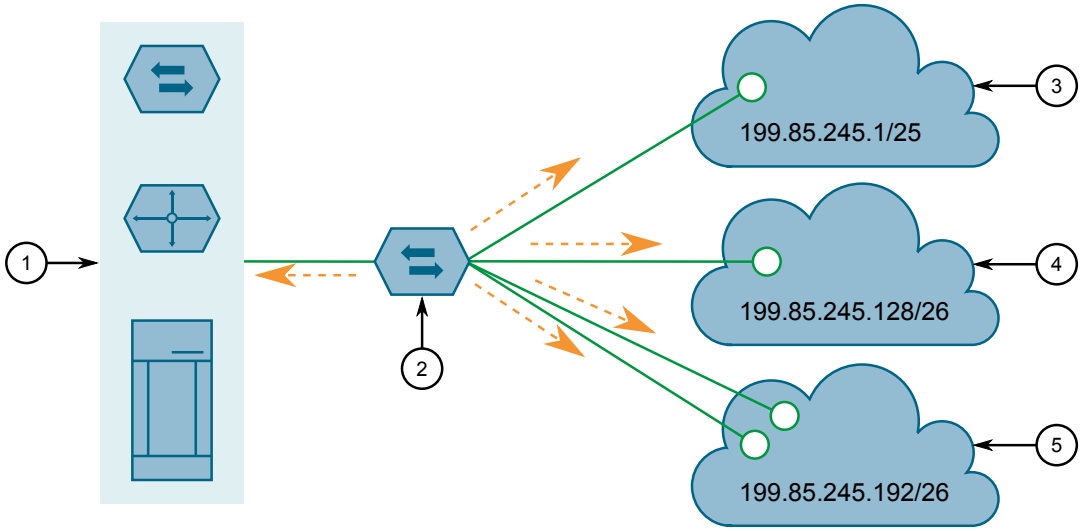
VLANs enable equipment moves to be handled by software reconfiguration instead of by physical cable management. When a host's physical location is changed, its connection point is often changed as well. With VLANs, the host's VLAN membership and priority are simply copied to the new port.

### 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 3
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 or implicitly, navigate to ***Virtual LANs » View VLAN Summary***. The **VLAN Summary** table appears.

If a VLANs are not listed, add static VLANs as needed. For more information, refer to "Adding a Static VLAN (Page 149)".

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

| Parameter | Description |
|---|---|
| `VLAN-aware` | **Synopsis:** [ No \| Yes ]<br>**Default:** Yes<br>Set either VLAN-aware or VLAN-unaware mode of operation. |
| `Ingress Filtering` | **Synopsis:** [ Disabled \| Enabled ]<br>**Default:** Disabled<br>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.<br>**Note**<br>Ingress filtering has no effect when ports are in either VLAN-unaware mode or Q-in-Q mode. |
| `QinQ Outer TPID` | **Synopsis:** [ 0x8100 \| 0x88A8 ]<br>**Default:** 0x8100<br>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.<br>**Note**<br>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.
2. Select a port. The **Port VLAN Parameters** form appears.

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

| Parameter | Description |
|---|---|
| `Port(s)` | **Synopsis:** Any combination of numbers valid for this parameter<br>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 ]<br>**Default:** Edge<br>This parameter specifies how the port determines its membership in VLANs. There are few types of ports:<br>• `Edge` – the port is only a member of one VLAN (its native VLAN specified by the PVID parameter).<br>• `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.<br>• `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.<br>• `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 the PVID of the frame's ingress port. VLAN tag is always stripped from frames ingressing this port.<br>**Note**<br>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<br>**Default:** 1<br>The Port VLAN Identifier specifies the VLAN ID associated with untagged (and 802.1p priority tagged) frames received on this port.<br>Frames tagged with a non-zero VLAN ID will always be associated with the VLAN ID retrieved from the frame tag.<br>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 ]<br>**Default:** Untagged<br>Specifies whether frames transmitted out of the port on its native VLAN (specified by the *`PVID`* parameter) will be tagged or untagged. |

| Parameter | Description |
|---|---|
| | **Note**<br>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 ]<br>**Default:** Disabled<br>Configures GVRP (Generic VLAN Registration Protocol) operation on the port. There are several GVRP operation modes:<br>• `Adv&Learn` – the port will declare all VLANs existing in the switch (configured or learned) and can dynamically learn VLANs.<br>• `Adv Only` – the port will declare all VLANs existing in the switch (configured or learned) but will not learn any VLANs.<br>• `Disabled` – the port is not capable of any GVRP processing.<br>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.

If a static VLAN is not listed, add the VLAN. For more information, refer to "Adding a Static VLAN (Page 149)".

### 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.
2. Click **InsertRecord**. The **Static VLANs** form appears.
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 mem-

ber 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<br>**Default:** 1<br>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<br>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 or [ None ]<br>These are ports that are not allowed to be members of the VLAN.<br>Examples:<br>• None – All ports of the switch are allowed to be members of the VLAN<br>• 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 ]<br>**Default:** Off<br>This parameter enables or disables IGMP Snooping on the VLAN. |
| DHCP | **Synopsis:** [ Off \| On ]<br>**Default:** Off<br>This parameter enables or disables DHCP Snooping on the VLAN. |
| MSTI | **Synopsis:** An integer between 0 and 16<br>**Default:** 0<br>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:

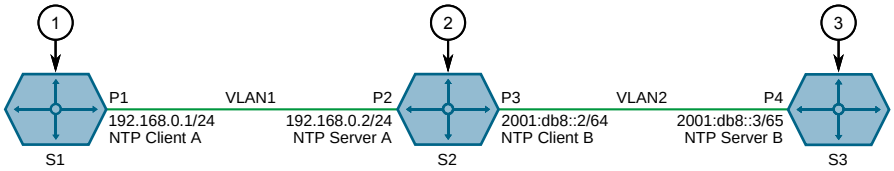
1. Navigate to ***Virtual LANs » Configure Static VLANs***. The **Static VLANs** table appears.
2. Select the static VLAN from the table. The **Static VLANs** form appears.
3. Click **Delete**.

## 7.1.6 Example: Configuring Management Support on Multiple VLANs

This example demonstrates how to move management traffic across multiple VLANs.

The following topology depicts a scenario where system time is synchronized across three RUGGEDCOM ROS devices over two VLANs. SNTP packets are sent back and forth between RUGGEDCOM ROS devices in a client-server model.

| NOTICE |
| --- |
| The values shown are specific to the provided topology. Actual values can vary based on the user's configuration. |




① Switch S1
② Switch S2
③ Switch S3

Figure 7.5 Topology – Management Support on Multiple VLANs

To replicate the topology, do the following:

1. Configure switch S1 as follows:
   a. Connect port P1 to port P2 on switch S2.
   b. Assign IP address *192.168.0.1/24* to port P1.
   c. Configure port P1 as the management interface. For more information, refer to "Adding a Switch IP Interface (Page 83)".
   d. Assign port P1 to VLAN 1. For more information, refer to Section "Configuring VLANs for Specific Ethernet Ports (Page 147)".
   e. Set the time source of switch S1 to *NTP SERVER*. For more information, refer to "Configuring the Time Source (Page 272)".
   f. Configure the NTP server on switch S1 as follows:

| | |
| --- | --- |
| **Server** | Primary |
| **IP Address** | 192.168.0.2 |
| **Update Period** | 1 min |

   For more information, refer to "Configuring NTP Servers (Page 273)".

2. Configure switch S2 as follows:
   a. Connect port P3 to port P4 on switch S3.
   b. Assign IP address *192.168.0.2/24* to port P2.
   c. Assign IP address *2001:db8::2/64* to port P3.
   d. Configure port P2 as an auxiliary management interface. For more information, refer to "Adding a Switch IP Interface (Page 83)".
   e. Configure port P3 as a non-management interface. For more information, refer to "Adding a Switch IP Interface (Page 83)".
   f. Assign port P2 to VLAN 1. For more information, refer to Section "Configuring VLANs for Specific Ethernet Ports (Page 147)".
   g. Assign port P3 to VLAN 2. For more information, refer to Section "Configuring VLANs for Specific Ethernet Ports (Page 147)".
   h. Set the time source of switch S2 to *NTP SERVER*. For more information, refer to "Configuring the Time Source (Page 272)".
   i. Configure the NTP server on switch S2 as follows:

| | |
|---|---|
| **Server** | Primary |
| **IP Address** | 2001:db8::3 |
| **Update Period** | 1 min |

   For more information, refer to "Configuring NTP Servers (Page 273)".
3. Configure switch S3 as follows:
   a. Assign IP address *2001:db8::3/64* to port P4.
   b. Configure port P4 as a non-management interface. For more information, refer to "Adding a Switch IP Interface (Page 83)".
   c. Assign port P4 to VLAN 2. For more information, refer to Section "Configuring VLANs for Specific Ethernet Ports (Page 147)".
   d. Set the time source of switch S3 to *LOCAL CLK*. For more information, refer to "Configuring the Time Source (Page 272)".
   e. Enable SNTP on switch S3. For more information, refer to Section "Enabling/Disabling NTP Service (Page 272)".
4. Verify the following:
   a. The local clock of switch S1 is synchronized with the local clock of switch S2. For more information, refer to "Managing NTP (Page 272)".
   b. The local clock of switch S2 is *not* synchronized with the local clock of switch S3. For more information, refer to "Managing NTP (Page 272)".
   c. The SNTP server on switch S2 is unreachable from the primary NTP server (because VLAN 2 is a non-management VLAN). For more information, refer to "Managing NTP (Page 272)".

## 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.

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 153)".
2. Configure the address on the device as a static MAC address. For more information, refer to "Adding a Static MAC Address (Page 155)".

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

| Parameter | Description |
|---|---|
| `Aging Time` | **Synopsis:** An integer between 15 and 800<br>**Default:** 300<br>This parameter configures the time that a learned MAC address is held before being aged out. |
| `Age Upon Link Loss` | **Synopsis:** [ No \| Yes ]<br>**Default:** Yes<br>When set to Yes, all MAC addresses learned on a failed port will be aged-out immediately upon link failure detection.<br>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.<br>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.
2. Select a port. The **Flooding Options** form appears.
3. Configure the following parameter(s) as required:

| Parameter | Description |
|---|---|
| `Port(s)` | **Synopsis:** Comma-separated list of ports<br>The port number as seen on the front plate silkscreen of the switch (or a list of ports, if aggregated in a port trunk). |
| `Flood Unknown Unicast` | **Synopsis:** [ On \| Off ]<br>**Default:** On<br>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.

If static MAC addresses have not been configured, add addresses as needed. For more information, refer to "Adding a Static MAC Address (Page 155)".

### 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.
2. Click **InsertRecord**. The **Static MAC Addresses** form appears.
3. Configure the following parameter(s) as required:

| Parameter | Description |
|---|---|
| `MAC Address` | **Synopsis:** ##-##-##-##-##-## where ## ranges 0 to FF<br>A MAC address learned by the switch.<br>Maximum of 6 wildcard characters may be used to specify a range of MAC addresses allowed to be learned by the Port Security module (when Port Security is set to 'Static MAC' mode). Wildcard must start from the right hand end and continuous.<br>Examples:<br>• 00-0A-DC-**-**-** means the entire MAC address space of RuggedCom.<br>• 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 ]<br>**Default:** 1<br>VLAN Identifier of the VLAN upon which the MAC address operates.<br>Option ANY allows learning a MAC address through the Port Security module on any VLAN's that are configured on the switch. |
| `Port` | **Synopsis:** 1/1 to maximum port number or [ Learn ]<br>**Default:** Learn<br>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'.<br>If the port should be auto-learned, set this parameter to 'Learn'. The option 'Learn' is applicable for Port Security in 'Static MAC' mode. |
| `Priority` | **Synopsis:** An integer between 0 and 7 or [ N/A ]<br>**Default:** N/A<br>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.
2. Select the MAC address from the table. The **Static MAC Addresses** form appears.
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.
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

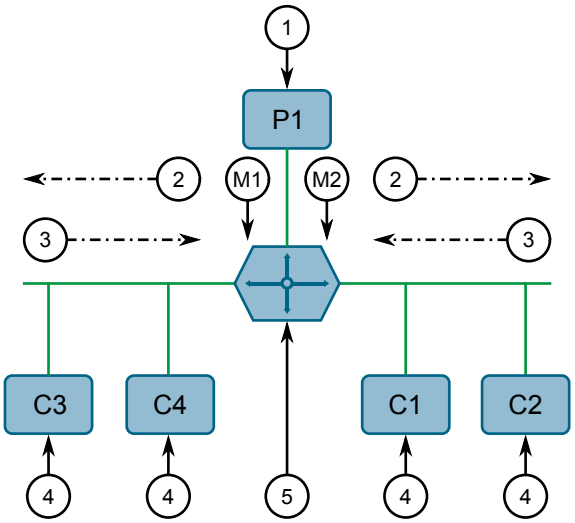
These addresses are reserved for routing protocols and IEEE 1588. If an IGMP membership report contains one of these addresses, the report is forwarded by the switch without learning about the host.

### 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 7.6 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 with-

in 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.

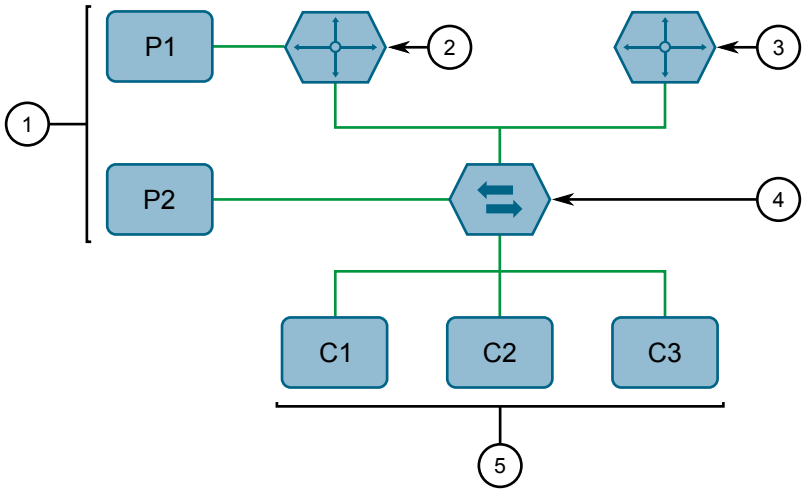
If RSTP detects a change in the network topology, IGMP will take some actions to avoid the loss of multicast connectivity and reduce network convergence time:

- 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 7.7 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 mem-

ber 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.

This table provides the following information:

| Parameter | Description |
|---|---|
| `Port` | **Synopsis:** 1/1 to maximum port number<br>The port number as seen on the front plate silkscreen of the device. |
| `VID` | **Synopsis:** An integer between 0 and 65535<br>VLAN Identifier of the VLAN upon which the multicast group operates. |
| `Group` | **Synopsis:** ###.###.###.### where ### ranges from 0 to 255<br>Multicast Group Address. |
| `Ver` | **Synopsis:** [ v3 \| v2 \| v1 ]<br>Specifies the IGMP version of the learnt multicast group. |
| `Reporter` | **Synopsis:** ###.###.###.### where ### ranges from 0 to 255<br>Specifies the source IP address that is reporting subscription to the multicast group. |
| `Age` | **Synopsis:** An integer between 0 and 7210<br>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 162)".

### 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.

This table provides the following information:

| Parameter | Description |
|---|---|
| `VID` | **Synopsis:** An integer between 0 and 65535<br>VLAN Identifier of the VLAN upon which the multicast group operates. |
| `Group` | **Synopsis:** ###.###.###.### where ### ranges from 0 to 255<br>Multicast Group Address. |
| `Source` | **Synopsis:** ###.###.###.### where ### ranges from 0 to 255 or [ * ]<br>Source Address. * means all possible source addresses. |
| `Joined Ports` | **Synopsis:** Comma-separated list of ports<br>All ports that currently receive multicast traffic for the specified multicast group. |
| `Router Ports` | **Synopsis:** Comma-separated list of ports<br>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 162)".

### 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 149)".
2. Navigate to ***Multicast Filtering » Configure IGMP Parameters***. The **IGMP Parameters** form appears.

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

| Parameter | Description |
|---|---|
| `Mode` | **Synopsis:** [ Passive \| Active ]<br>**Default:** Passive<br>Specifies the IGMP mode. Options include:<br>• `Passive` – the switch passively snoops IGMP traffic and never sends IGMP queries<br>• `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 ]<br>**Default:** v2<br>Specifies the configured IGMP version on the switch. Options include:<br>• `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.<br>• `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<br>**Default:** 60<br>The time interval between IGMP queries generated by the switch.<br>**Note**<br>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<br>**Default:** None<br>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 ]<br>**Default:** On<br>This parameter specifies whether multicast streams will be always forwarded to multicast routers. |
| `RSTP Flooding` | **Synopsis:** [ Off \| On ]<br>**Default:** Off<br>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. |

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.

### 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:

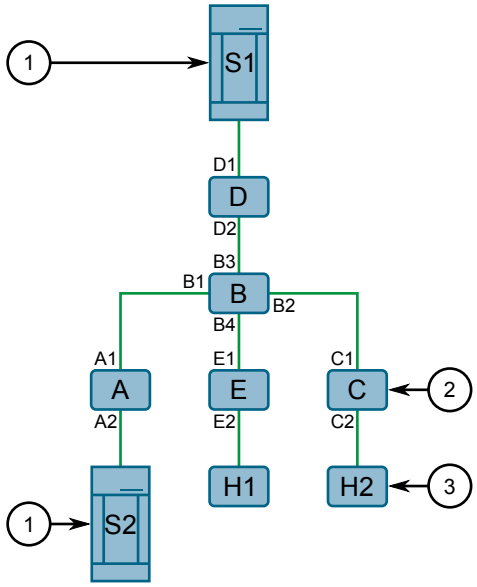
- Forward All Multicast group traffic in the VLAN, or
- Forward All Unknown Traffic (Multicast Groups) for which there are no members registered in the device in a VLAN

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 7.8 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.

This table provides the following information:

| Parameter | Description |
|---|---|
| VID | **Synopsis:** An integer between 0 and 65535<br>VLAN Identifier of the VLAN upon which the multicast group operates. |
| MAC Address | **Synopsis:** ##-##-##-##-##-## where ## ranges 0 to FF<br>Multicast group MAC address. |
| Static Ports | **Synopsis:** Any combination of numbers valid for this parameter<br>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<br>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.
2. Configure the following parameter(s) as required:

| Parameter | Description |
|---|---|
| GMRP Enable | **Synopsis:** [ No \| Yes ]<br>**Default:** No<br>Globally enable or disable GMRP.<br>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 ]<br>**Default:** Off<br>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. |
| Leave Timer | **Synopsis:** An integer between 600 and 300000<br>**Default:** 4000<br>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 167)".
2. Navigate to ***Multicast Filtering » Configure Port GMRP Parameters***. The **Port GMRP Parameters** table appears.
3. Select an Ethernet port. The **Port GMRP Parameters** form appears.
4. Configure the following parameter(s) as required:

| Parameter | Description |
|---|---|
| `Port(s)` | **Synopsis:** Any combination of numbers valid for this parameter<br>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 ]<br>**Default:** Disabled<br>Configures GMRP (GARP Multicast Registration Protocol) operation on the port. There are several GMRP operation modes:<br>• `Disabled` – the port is not capable of any GMRP processing.<br>• `Adv Only` – the port will declare all MCAST addresses existing in the switch (configured or learned) but will not learn any MCAST addresses.<br>• `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.

If a static multicast group is not listed, add the group. For more information, refer to "Adding a Static Multicast Group (Page 168)".

### 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.
2. Click **InsertRecord**. The **Static Multicast Groups** form appears.

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

| Parameter | Description |
|---|---|
| MAC Address | **Synopsis:** ##-##-##-##-##-## where ## ranges 0 to FF<br>**Default:** 00-00-00-00-00-00<br>Multicast group MAC address. |
| VID | **Synopsis:** An integer between 1 and 4094<br>**Default:** 1<br>VLAN Identifier of the VLAN upon which the multicast group operates. |
| Priority | **Synopsis:** An integer between 0 and 7 or [ N/A ]<br>**Default:** N/A<br>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<br>**Default:** None<br>A comma-separated list of ports to which the multicast group traffic is forwarded. If a port is part of a Link Aggregation Group (LAG), or port trunk, specify all ports in the LAG. |

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.
2. Select the group from the table. The **Static Multicast Groups** form appears.
3. Click **Delete**.

# 8 Layer 3

This chapter describes the Layer 3, or network layer, features of RUGGEDCOM ROS.

## 8.1 Managing Layer 3 Switching

This section describes how to manage Layer 3 switching.

**Note**
Layer 3 switching only supports IPv4 addresses (not IPv6 addresses).

**Note**
Layer 3 switching only supports unicast traffic. Layer 3 switching for multicast and broadcast traffic is not supported.

### 8.1.1 Understanding Layer 3 Switching

Traditional switching operates at Layer 2 of the OSI model, where packets are sent to a specific switch port based on destination MAC addresses and VLANs. Routing operates at Layer 3, where packets are sent to a specific next-hop IP address, based on the destination IP address.

RUGGEDCOM ROS supports configuration of Layer 3 switching rules, allowing IP traffic to be switched between two existing VLANs via device hardware.

This section describes some of the concepts important to the implementation of Layer 3 switching in RUGGEDCOM ROS.

#### 8.1.1.1 Layer 3 Switch Forwarding Table

To route a packet with a specific destination IP address, a device needs the following information:

- **Egress interface (subnet)**

  This information is stored in the device's routing table.

  **Note**
  In a Layer 2 switched network segment, a VLAN constitutes an IP subnet.

- **Next-hop or Gateway Media Access Control (MAC) address**

  This information is stored in an ARP table specific to Layer 3 switching.

  **Note**
  If the next hop is the destination subnet itself, then the destination host MAC address is required.

Layer 3 switching translates this routing information into Layer 3 switching rules. These rules are known as the *Layer 3 Switch Forwarding Information Base (FIB)* or the *Layer 3 Switch Forwarding Table*. A Layer 3 switching rule defines how to switch a specific traffic flow.

Layer 3 switching Application-Specific Integrated Circuits (ASICs) store Layer 3 switching rules in seperate Ternary Content Addressable Memory (TCAM) tables for hosts and subnets. Layer 3 switching rules can be statically configured or dynamically learned (or *auto-learned*).

**Note**
Layer 3 switching rules can only be dynamically learned for neighbor hosts. Rules must be statically configured for remote hosts and subnets.

**Note**
The maximum number of Layer 3 switching rules is 3072, including 2048 for hosts and 1024 for subnets.

#### 8.1.1.2 Static Layer 3 Switching Rules

When creating a static route through switch management, hardware acceleration can be explicitly configured. If hardware acceleration is selected, an appropriate Layer 3 switching rule is installed in the ASIC's TCAM and never ages out.

**Note**
Only ICMP, TCP, and UDP traffic flows will be accelerated by the IP/Layer 3 switching ASIC.

**Note**
When using statically configured Layer 3 switching rules, IP forwarding may be enabled or disabled. For information on how to configure IP forwarding, refer to "Configuring IP Services (Page 86)".

#### 8.1.1.3 Dynamic Learning of Layer 3 Switching Rules

For static routes without hardware acceleration or for dynamic routes, Layer 3 switching rules can be dynamically learned based on software-based router decisions.

After a certain amount of traffic for the same flow is successfully routed, the Layer 3 switching ASIC begins switching the rest of the packets belonging to the same flow. A flow is unidirectional traffic between two hosts. For example, traffic flowing between ports from one host to another is considered a flow. Traffic flowing in the opposite direction between the same ports is considered a different flow.

RUGGEDCOM ROS supports the host-oriented auto-learning method, where the device uses the source and destination IP addresses to identify a traffic flow.

Each flow constitutes one rule.

The Layer 3 switch continuously monitors activity (this is, the presence of traffic) for dynamically learned rules. Because of this, dynamically learned rules may be removed after a configurable time due to inactivity.

#### 8.1.1.4 Interaction Between IP Forwarding and Layer 3 Switching

To use static Layer 3 switching rules, IP forwarding can be enabled or disabled. However, to use dynamically learned Layer 3 switching rules, IP forwarding must be enabled. For information about configuring IP forwarding, refer to "Configuring IP Services (Page 86)".

The following shows how IP forwarding interacts with Layer 3 switching in RUGGEDCOM ROS.

| IP Forwarding | L3 Switching Disabled | L3 Switching Static | L3 Switching Dynamic |
|---|---|---|---|
| Disabled | Both features disabled | Static Layer 3 switching | Not possible |
| Enabled | No hardware acceleration | Static Layer 3 switching | Static and Dynamic Layer 3 switching |

#### 8.1.1.5 Layer 3 Switch ARP Table

A router needs to know the destination host or next-hop gateway MAC address for it to forward a packet on another subnet. Therefore, software maintains an Address Resolution Protocol (ARP) table that maps IP addresses to MAC addresses. The same information is also needed by the Layer 3 switching ASIC when it switches IP packets between subnets.

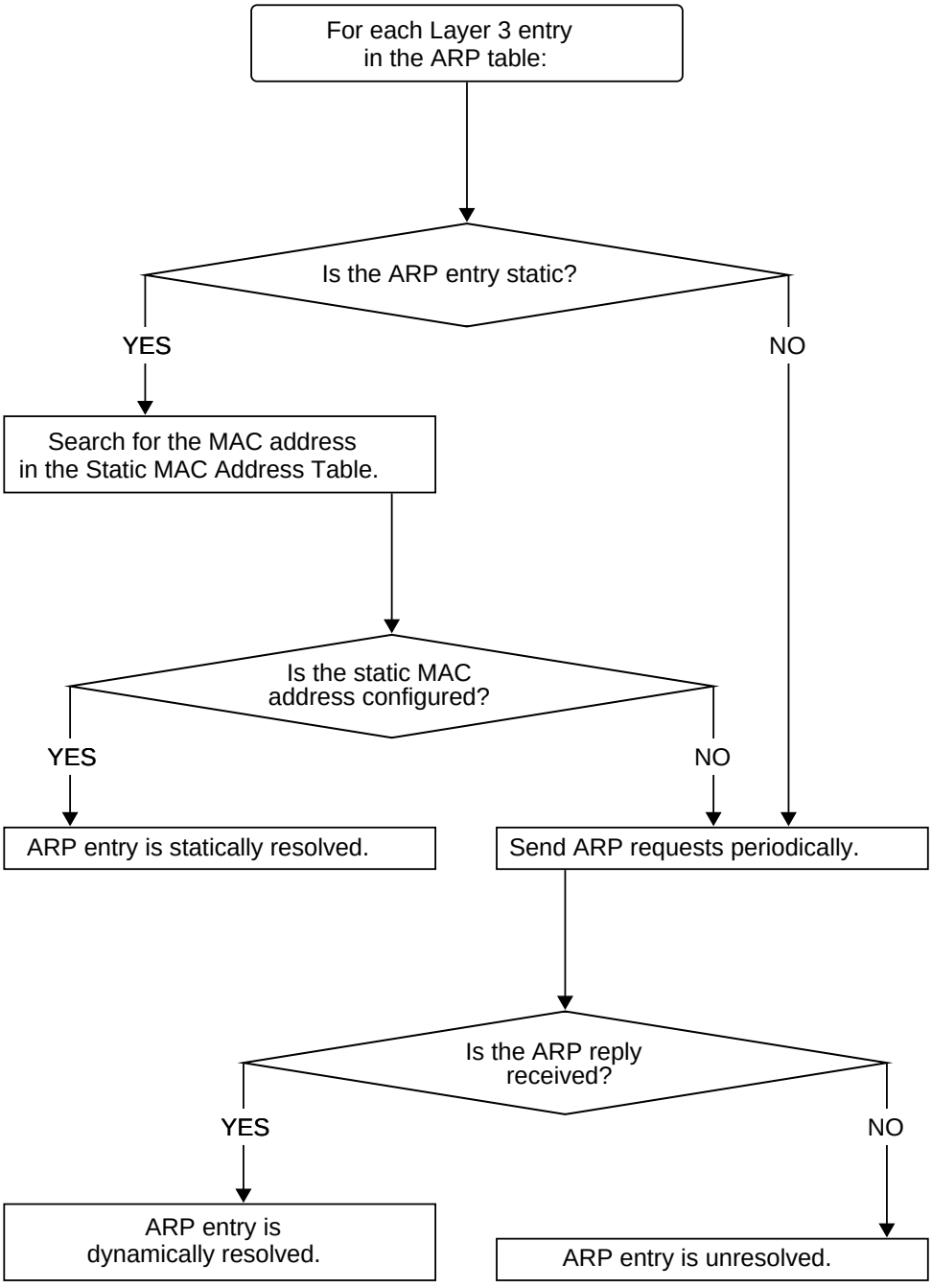
**Note**
ARP entries can be statically configured and resolved if the static MAC addresses to which they correspond are configured in the **Static MAC Address Table**. Otherwise, ARP entries will be dynamically resolved every 60 seconds (s).

The destination or gateway MAC address is usually obtained through ARP. However, ARP entries can also be statically configured in the Layer 3 Switch so they do not time out. When configuring a static ARP entry, if no value is entered for the MAC Address parameter, the address is automatically resolved through ARP and then saved statically. This is preserved across reboots of the device.

If no static ARP entry is configured for a specific destination, a dynamic ARP entry will be created and the destination MAC address will be resolved automatically.

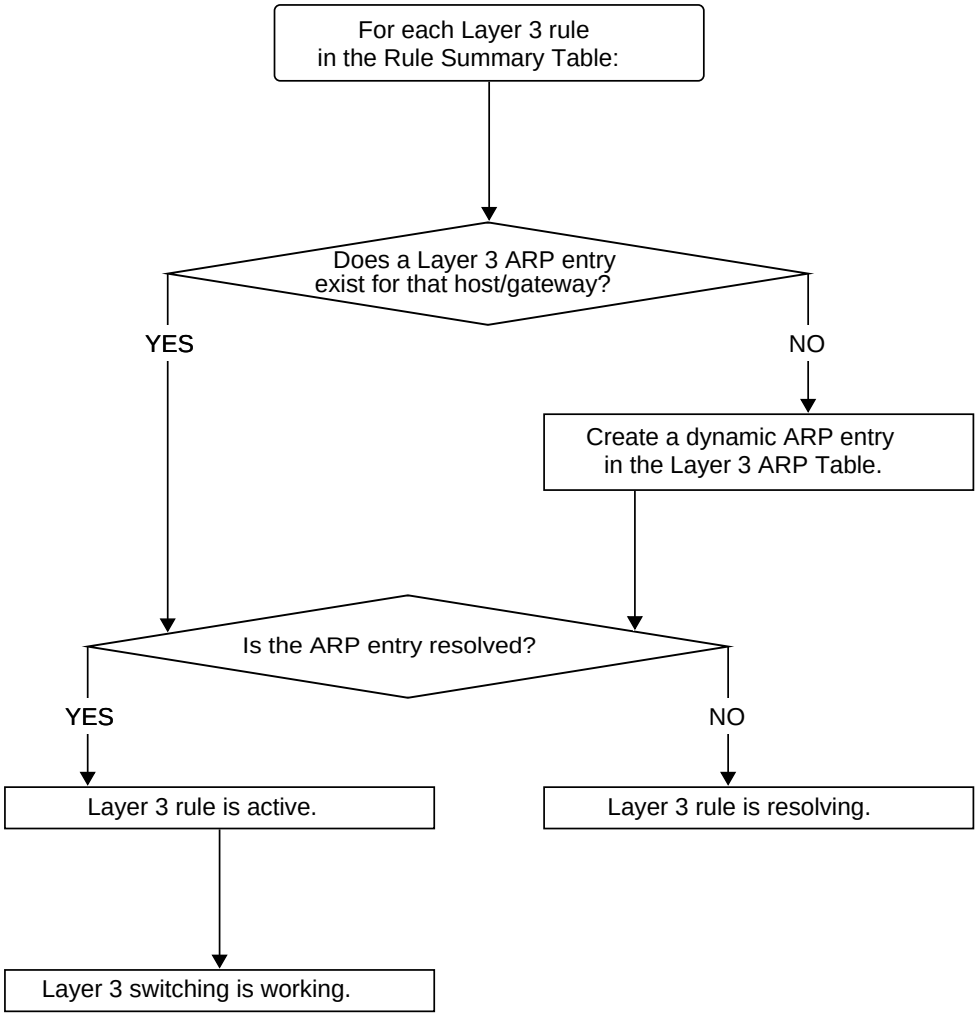
**Layer 3 ARP Resolution Behavior**

The following flowchart shows how ARP entries are resolved in RUGGEDCOM ROS.



### Layer 3 Switching Rule Resolution Behavior

The following flowchart shows how Layer 3 switching rules are resolved in RUGGEDCOM ROS.




## 8.1.1.6 Layer 3 Switch Routable Interfaces

RUGGEDCOM ROS allows up to 255 interfaces (VLANs) to be configured. To make an interface routable for unicast IPv4 traffic, an IPv4 address must be configured statically or assigned via DHCP to the interface. For more information, refer to "Managing IP Interfaces (Page 82)".

### 8.1.2 Configuring Layer 3 Switching

To configure Layer 3 switching, do the following:

**Note**
Avoid configuring Link Aggregation Groups (LAGs) when Layer 3 switching is enabled. For more information, refer to "Managing Link Aggregation Groups (Page 251)".

1. Add VLANs as required. For more information, refer to "Adding a Static VLAN (Page 149)".
2. Assign IP addresses to the configured VLANs. For more information, refer to "Adding a Switch IP Interface (Page 83)".
3. Assign desired ports to the configured VLANs. For more information, refer to "Configuring VLANs for Specific Ethernet Ports (Page 147)".
4. Configure the unicast mode and aging time. For more information, refer to "Configuring Layer 3 Switching Options (Page 176)".
5. If static unicast mode is selected, add destination IP addresses and next hop gateways as needed. For more information, refer to "Managing Static Unicast Rules (Page 177)".
6. If static unicast mode is selected, add static ARP table entries as needed. For more information, refer to "Managing Static ARP Table Entries (Page 178)".
7. Test the configuration by sending traffic and verifying the following:
   a. ARP entries are resolved in the **ARP Table**. For more information, refer to "Viewing a List of ARP Table Entries (Page 178)".
   b. Rules are active in the **Rule Summary Table**. For more information, refer to "Viewing Routing Rules (Page 180)".
   c. Traffic is being sent and received. For more information, refer to "Viewing Statistics for Specific Ethernet Ports (Page 63)".

For configuration examples, refer to "Example: Configuring Layer 3 Switching (Page 181)" and "Example: Configuring Layer 3 Switching Using Multiple Switches (Page 182)".

### 8.1.3 Configuring Layer 3 Switching Options

To configure Layer 3 switching options, do the following:

1. Navigate to ***Layer 3 Switching » Configure Switch Options***. The **Switch Options** form appears.

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

| Parameter | Description |
|---|---|
| `Unicast Mode` | **Synopsis:** [ Disabled \| Static \| Auto ]<br>**Default:** Disabled<br>Disabled – Layer 3 switching is disabled.<br>Static – Only statically configured Layer 3 switching rules will be used.<br>Auto – Both statically configured and dynamically learned Layer 3 switching rules will be used. In this mode, maximum routing hardware acceleration is utilized. |
| `Aging Time` | **Synopsis:** An integer between 16 and 600<br>**Default:** 32<br>This parameter configures the time a dynamically learned rule for a traffic flow, which has become inactive, is held before being removed from the Layer 3 Switch forwarding table. |

3. Click **Apply**.

## 8.1.4 Managing Static Unicast Rules

This section describes how to manage static unicast rules.

### 8.1.4.1 Viewing Static Unicast Rules

To view a list of static unicast rule entries, navigate to ***Layer 3 Switching » Configure Static Unicast Rules***. If table entries have been configured, the **Static Unicast Rules** table appears.

Static unicast rules can be configured as required. For more information about adding static unicast rules, refer to "Adding a Static Unicast Rule (Page 177)".

### 8.1.4.2 Adding a Static Unicast Rule

To add a static unicast rule, do the following:

1. Navigate to ***Layer 3 Switching » Configure Static Unicast Rules***. The **Static Unicast Rules Table** appears.
2. Click **InsertRecord**. The **Static Unicast Rules** form appears.

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

| Parameter | Description |
|---|---|
| `Destination` | **Synopsis:** ###.###.###.###/## where ### ranges from 0 to 255 and ## ranges from 0 to 32<br>**Default:** ANY<br>Destination IP address or subnet. To match the rule, the incoming packet's destination IP address should belong to the subnet. |
| `Gateway` | **Synopsis:** ###.###.###.### where ### ranges from 0 to 255<br>IP address of the next hop to which matching unicast packets will be forwarded<br>**Note**<br>If the **Destination** is a directly connected neighbor, no value should be supplied for the **Gateway** parameter. |

4. Click **Apply**.

#### 8.1.4.3 Deleting a Static Unicast Rule

To delete a static unicast rule, do the following:

1. Navigate to ***Layer 3 Switching » Configure Static Unicast Rules***. The **Static Unicast Rules** table appears.
2. Select the record to be deleted. The **Static Unicast Rules** form appears.
3. Click **Delete**.

### 8.1.5 Managing Static ARP Table Entries

This section describes how to manage static ARP Table entries.

#### 8.1.5.1 Viewing a List of ARP Table Entries

To view a list of Layer 3 switching ARP table entries, navigate to ***Layer 3 Switching » Configure/View ARP Table***. If table entries have been configured, the **ARP Table** appears.

When unicast rules are configured, the Layer 3 switching ARP table will populate as ARP entries are dynamically learned. Static ARP table entries can also be added as needed. For more information about adding static ARP table entries, refer to "Adding a Static ARP Table Entry (Page 179)".

### 8.1.5.2 Adding a Static ARP Table Entry

To add a static ARP table entry, do the following:

1. Navigate to ***Layer 3 Switching » Configure/View ARP Table***. The **ARP Table** form appears.
2. Click **InsertRecord**. The **ARP Table** form appears.
3. Configure the following parameter(s) as required:

| Parameter | Description |
|---|---|
| `IP Address` | **Synopsis:** ###.###.###.### where ### ranges from 0 to 255<br>IP address of the network device the entry describes. |
| `VID` | **Synopsis:** An integer between 0 and 65535<br>**Default:** N/A<br>VLAN Identifier of the VLAN upon which the MAC address operates. |
| `MAC Address` | **Synopsis:** ##-##-##-##-##-## where ## ranges 0 to FF<br>**Default:** 00-00-00-00-00-00<br>MAC address of the network device specified by the IP address. |
| `Static` | **Synopsis:** [ True \| False ]<br>**Default:** True<br>Whether the entry is static or dynamic. Static entries are configured as a result of management activity. Dynamic entries are automatically learned by the device and can be unlearned. |
| `Status` | **Synopsis:** [ Unresolved \| Resolved ]<br>ARP entry resolution status:<br>Resolved – MAC-IP address pair is resolved and operational.<br>Unresolved – the device hasn't resolved the MAC-IP address pair and keeps sending ARP requests periodically. |

4. Click **Apply**.

### 8.1.5.3 Deleting a Static ARP Table Entry

To delete a static ARP table entry, do the following:

1. Navigate to ***Layer 3 Switching » Configure/View ARP Table***. The **ARP Table** form appears.
2. Select the record to be deleted. The **ARP Table** form appears.
3. Click **Delete**.

## 8.1.6 Viewing Routing Rules

To view a list of routing rules, navigate to ***Layer 3 Switching » View Rule Summary***. If any static or dynamic unicast rules are configured, the **Rule Summary Table** appears.

This table provides the following information:

| Parameter | Description |
|---|---|
| `Destination` | **Synopsis:** A string 20 characters long<br>Destination IP address or subnet.<br>To match the rule, the incoming packet's destination IP address should belong to the subnet. |
| `Out-VLAN(s)` | **Synopsis:** Comma separated list of up to 2 numbers ranging from 1 to 4095<br>Egress VLAN(s).<br>Matching unicast or multicast packets will be sent to this one or more VLAN(s). |
| `Gateway` | **Synopsis:** ###.###.###.### where ### ranges from 0 to 255<br>IP address of the next hop to which matching unicast packets will be forwarded. |
| `Static` | **Synopsis:** [ True \| False ]<br>Whether the rule is static or dynamic.<br>Static rules are configured as a result of management activity.<br>Dynamic rules are automatically learned by the device and can be unlearned subject to Aging Time. |
| `Status` | **Synopsis:** [ Active \| Resolving ]<br>Whether the rule is currently operational or not:<br>Active – rule is fully operational and can be applied, so hardware acceleration is performed.<br>Resolving – rule is not operational yet due to some unresolved information, like ARP or gateway's MAC address in the MAC Address Table. Hardware acceleration is not performed. |

## 8.1.7 Flushing Dynamic Hardware Routing Rules

Flushing dynamic hardware routing rules removes all dynamically learned rules from the **Layer 3 Switch Forwarding Table**.

**Note**
Only dynamic rules can be flushed. Static rules, configured in the **Layer 3 Switch Forwarding Table**, never age out. For more information about enabling hardware acceleration, refer to "Understanding Layer 3 Switching (Page 171)".

To flush dynamic hardware routing rules, do the following:

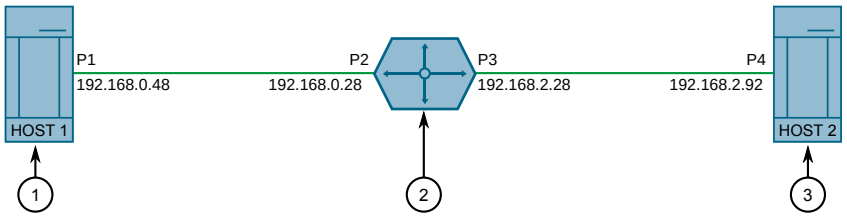
1. Navigate to ***Layer 3 Switching*** and click **Flush Learned Rules**. The **Flush Learned Rules** form appears.
2. Click **Confirm**.

## 8.1.8 Example: Configuring Layer 3 Switching

This example demonstrates how to configure Layer 3 switching.

The following topology depicts a scenario where two hosts on separate networks are connected to a RUGGEDCOM ROS device configured as a Layer 3 switch. Bi-directional traffic is being sent between the two hosts via RUGGEDCOM ROS.

| **NOTICE** |
| --- |
| The values shown are specific to the provided topology. Actual values can vary based on the user's configuration. |




① Host 1
② RUGGEDCOM ROS device
③ Host 2

Figure 8.1 Basic Layer 3 Switching Topology

To replicate the topology, do the following:

**Note**
Host 1 and Host 2 can be either a Layer 2 device or a PC. For specific configuration instructions consult the original equipment manufacturer (OEM) documentation.

1. Configure Host 1 per the topology as follows:
   a. Connect P1 to P2 of the RUGGEDCOM ROS device.
   b. Assign IP address *192.168.0.48* to the P1 interface.
   c. Set the default gateway to *192.168.0.28*.

2. Configure Host 2 per the topology as follows:
   a. Connect P4 to P3 of the RUGGEDCOM ROS device.
   b. Assign IP address *192.168.2.92* to the P4 interface.
   c. Set the default gateway to *192.168.2.28*.
3. Configure the RUGGEDCOM ROS device as a Layer 3 switch:
   a. Add VLAN 1 and VLAN 2. For more information, refer to "Adding a Static VLAN (Page 149)".
   b. Assign IP address *192.168.0.28* to VLAN 1, and IP address *192.168.2.28* to VLAN 2. For more information, refer to "Adding a Switch IP Interface (Page 83)".
   c. Assign P2 to VLAN1 and P3 to VLAN2. Refer to "Configuring VLANs for Specific Ethernet Ports (Page 147)" for more information.
   d. Enable unicast mode. For more information, refer to "Configuring Layer 3 Switching Options (Page 176)".
   e. If *Auto* is selected as the unicast mode, proceed to step Step 4. Otherwise, configure destination and default gateway static unicast rules as follows:

| Destination | Gateway |
|---|---|
| 192.168.0.48 | 0.0.0.0 |
| 192.168.2.92 | 0.0.0.0 |

   For more information about configuring static unicast rules, refer to "Adding a Static Unicast Rule (Page 177)".
   f. Send multiple ARP requests/replies from Host 1 and Host 2 to the RUGGEDCOM ROS device.
4. Send bidirectional traffic (i.e. UDP, TCP, ICMP) between Host 1 and Host 2, and verify the following:
   a. ARP entries are resolved in the **ARP Table**. For more information, refer to "Viewing a List of ARP Table Entries (Page 178)".
   b. Rules are active in the **Rule Summary Table**. For more information, refer to "Viewing Routing Rules (Page 180)".
   c. Traffic is being sent and received between the two end hosts. For more information, refer to "Viewing Statistics for Specific Ethernet Ports (Page 63)".

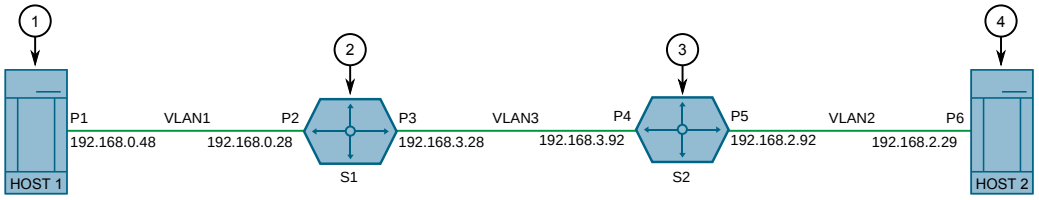
## 8.1.9 Example: Configuring Layer 3 Switching Using Multiple Switches

This example demonstrates how to configure Layer 3 switching using multiple switches.

The following topology depicts a scenario where two hosts on separate networks are connected to two RUGGEDCOM ROS devices configured as a Layer 3 switches. Bi-directional traffic is being sent between the two hosts via the RUGGEDCOM ROS devices.

**NOTICE**

The values shown are specific to the provided topology. Actual values can vary based on the user's configuration.




① Host 1
② S1
③ S2
④ Host 2

Figure 8.2 Topology – Layer 3 Switching Using Two Switches

To replicate the topology, do the following:

**Note**

Host 1 and Host 2 can be either a Layer 2 device or a PC. For specific configuration instructions, consult the OEM documentation.

1. Configure Host 1 per the topology as follows:
   a. Connect P1 to P2 of RUGGEDCOM ROS device 1.
   b. Assign IP address *192.168.0.48* to the P1 interface.
   c. Set the default gateway to *192.168.0.28*.
2. Configure Host 2 per the topology as follows:
   a. Connect P6 to P5 of S2.
   b. Assign IP address *192.168.2.29* to the P6 interface.
   c. Set the default gateway to *192.168.2.92*.

3. Configure S1 as a Layer 3 switch:
   a. Connect P3 to P4 of S2.
   b. Add VLAN 1 and VLAN 3. For more information, refer to "Adding a Static VLAN (Page 149)".
   c. Assign IP address *192.168.0.28* to VLAN 1, and IP address *192.168.3.28* to VLAN 3. For more information, refer to "Adding a Switch IP Interface (Page 83)".
   d. Assign P2 to VLAN1 and P3 to VLAN3. Refer to "Configuring VLANs for Specific Ethernet Ports (Page 147)" for more information.
   e. Set the unicast mode to *Auto*. For more information, refer to "Configuring Layer 3 Switching Options (Page 176)".
   f. Configure destination and default gateway static unicast rules as follows:

| Destination | Gateway |
|---|---|
| 192.168.2.0/24 | 192.168.3.92 |

   For more information about configuring static unicast rules, refer to "Adding a Static Unicast Rule (Page 177)".
4. Configure S2 as a Layer 3 switch:
   a. Add VLAN 3 and VLAN 2. For more information, refer to "Adding a Static VLAN (Page 149)".
   b. Assign IP address *192.168.3.92* to VLAN 3, and IP address *192.168.2.92* to VLAN 2. For more information, refer to "Adding a Switch IP Interface (Page 83)".
   c. Set the unicast mode to *Auto*. For more information, refer to "Configuring Layer 3 Switching Options (Page 176)".
   d. Configure destination and default gateway static unicast rules as follows:

| Destination | Gateway |
|---|---|
| 192.168.0.0/24 | 192.168.3.28 |

   For more information about configuring static unicast rules, refer to "Adding a Static Unicast Rule (Page 177)".
5. Send multiple ARP requests/replies from Host 1 to S1, and from Host 2 to S2.
6. Send bidirectional traffic (i.e. UDP, TCP, ICMP) between Host 1 and Host 2, and verify the following:
   a. ARP entries are resolved in the **ARP Table**. For more information, refer to "Viewing a List of ARP Table Entries (Page 178)".
   b. Rules are active in the **Rule Summary Table**. For more information, refer to "Viewing Routing Rules (Page 180)".
   c. Traffic is being sent and received between the two end hosts. For more information, refer to "Viewing Statistics for Specific Ethernet Ports (Page 63)".

# 9 Redundancy

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

## 9.1 Managing Spanning Tree Protocol

This section describes how to manage the spanning tree protocol.

### 9.1.1 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.

#### 9.1.1.1 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.

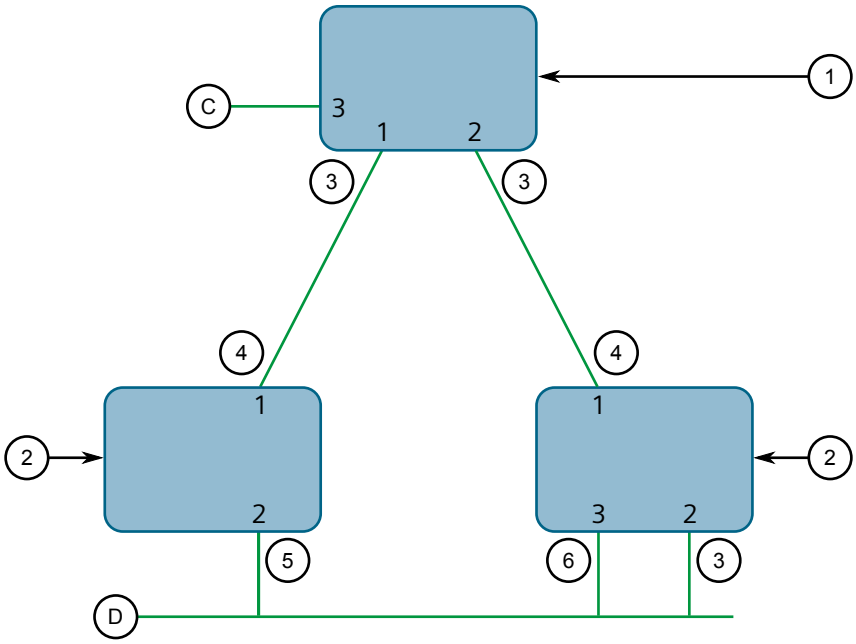
After *learning*, the bridge will place the port in the forwarding state. The port both learns addresses and participates in frame transfer while in this state.

| **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 9.1 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 back-up for another port on the bridge and will become active if that port fails. The Backup Port does not participate in the network.

#### 9.1.1.2 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.

#### 9.1.1.3 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.

#### 9.1.1.4 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.

## 9.1.1.5 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. |

#### 9.1.1.6 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.

#### 9.1.1.7 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.

## 9.1.2 RSTP Applications

This section describes various applications of RSTP.

### 9.1.2.1 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 9.2, “Example - Structured Wiring Configuration” would leave all the ports of bridges 555 through 888 connected to the network.

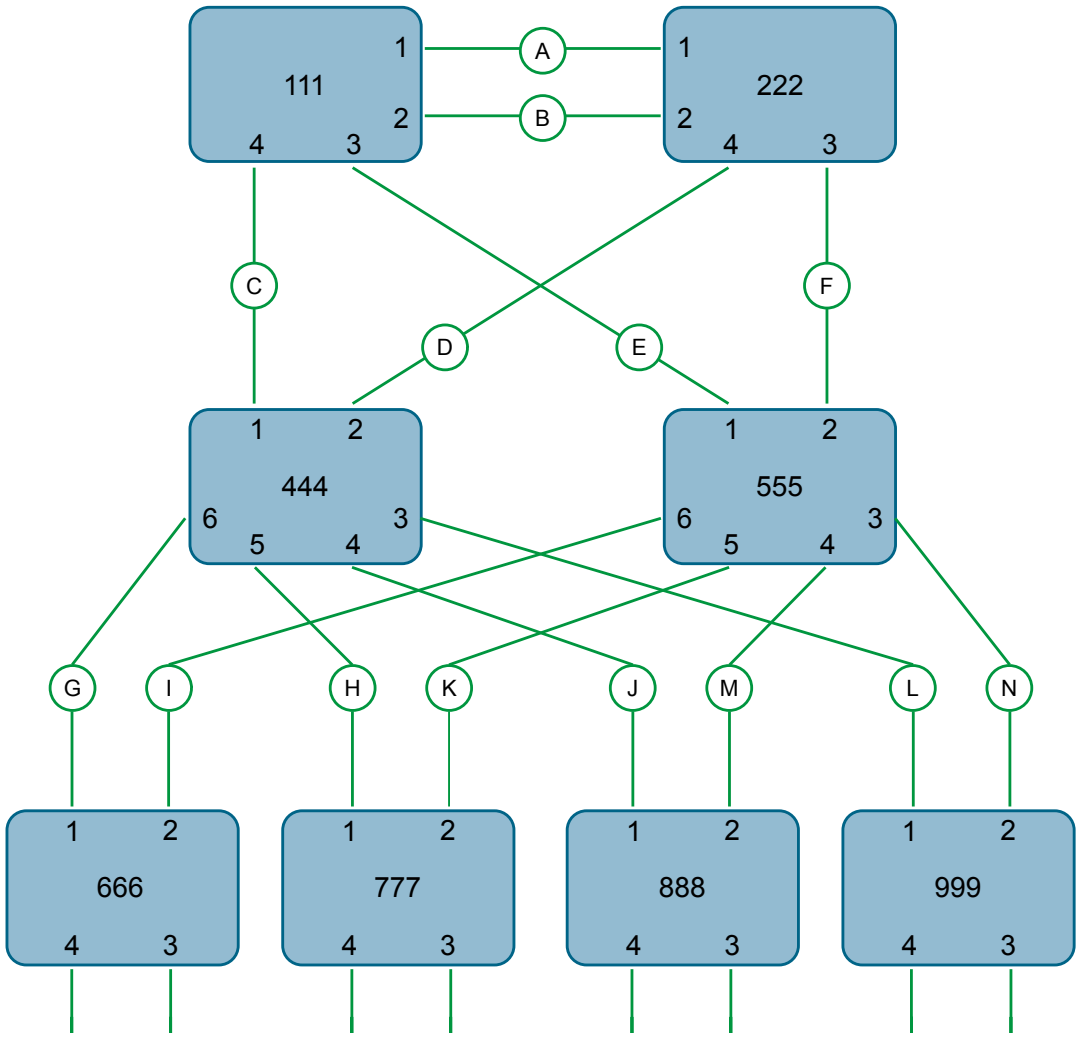



Figure 9.2 Example - Structured Wiring Configuration

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 net-

work. 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.**

### 9.1.2.2 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 9.3, "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.

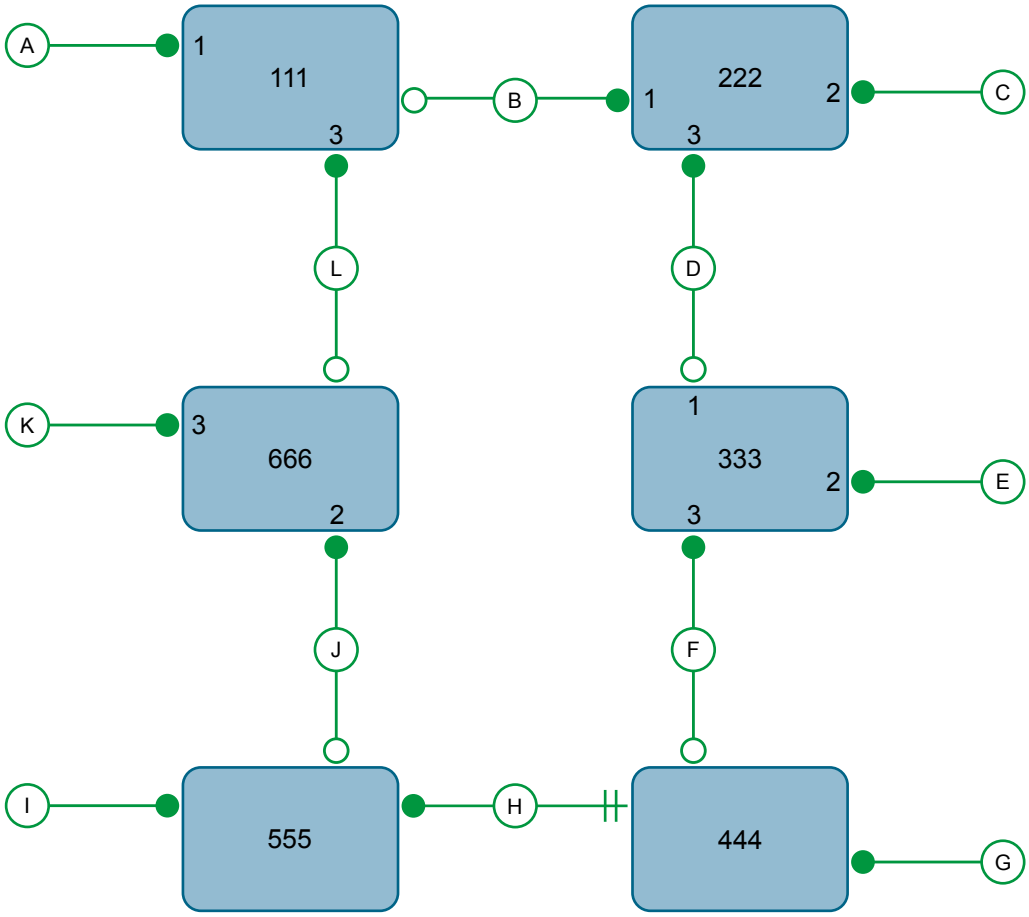



Figure 9.3 Example - Ring Backbone Configuration

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.**

### 9.1.2.3 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.

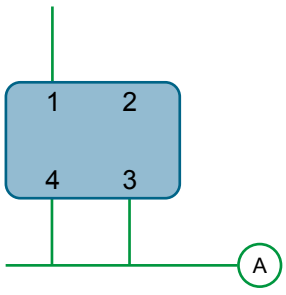



Figure 9.4 Example - Port Redundancy

## 9.1.3 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.

### 9.1.3.1 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.

### 9.1.3.2 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.<br>• A Designated Port provides the minimum cost path from an attached LAN, via the bridge to the CIST Regional Root.<br>• 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:<br>• 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.<br>• A Designated Port provides the minimum cost path from an attached LAN, via the bridge to the MSTI Regional Root.<br>• Alternate and Backup Ports function the same as they do in RSTP, but relative to the MSTI Regional Root.<br>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.<br>A Boundary Port may be:<br>• 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.<br>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. |

#### 9.1.3.3 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.

### 9.1.3.4 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 202)".

   **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 149)".

   **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 212)".
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 212)".
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 213)".

7. Set the STP Protocol Version to MSTP and enable STP. For more information, refer to "Configuring STP Globally (Page 201)"

## 9.1.4 Configuring STP Globally

To configure global settings for the Spanning Tree Protocol (STP), do the following:

1. Navigate to ***Network Redundancy » Spanning Tree » Configure Bridge RSTP Parameters***. The **Bridge RSTP Parameters** form appears.
2. Configure the following parameter(s) as required:

| Parameter | Description |
|---|---|
| `State` | **Synopsis:** [ Disabled \| Enabled ]<br>**Default:** Enabled<br>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 ]<br>**Default:** RSTP<br>Selects the version of Spanning Tree Protocol to support, either only STP or Rapid STP or Multiple STP. |
| `Bridge Priority` | **Synopsis:** [ 0 \| 4096 \| 8192 \| 12288 \| 16384 \| 20480 \| 24576 \| 28672 \| 32768 \| 36864 \| 40960 \| 45056 \| 49152 \| 53248 \| 57344 \| 61440 ]<br>**Default:** 32768<br>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<br>**Default:** 2<br>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<br>**Default:** 20<br>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 |

| Parameter | Description |
|---|---|
| `Transmit Count` | **Synopsis:** An integer between 3 and 100 or [ Unlimited ]<br>**Default:** Unlimited<br>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<br>**Default:** 15<br>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<br>**Default:** 20<br>Only applicable to MSTP. The maximum possible bridge diameter inside an MST region.<br>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**.

## 9.1.5 Configuring STP for Specific Ethernet Ports

To configure the Spanning Tree Protocol (STP) for a specific Ethernet port, do the following:

1. Navigate to ***Network Redundancy » Spanning Tree » Configure Port RSTP Parameters***. The **Port RSTP Parameters** table appears.
2. Select an Ethernet port. The **Port RSTP Parameters** form appears.
3. Configure the following parameter(s) as required:

| Parameter | Description |
|---|---|
| `Port(s)` | **Synopsis:** Comma-separated list of ports<br>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 ]<br>**Default:** Enabled<br>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 dis- |

| Parameter | Description |
|---|---|
| | abling STP would be a port that services only a single host computer. |
| Priority | **Synopsis:** [ 0 \| 16 \| 32 \| 48 \| 64 \| 80 \| 96 \| 112 \| 128 \| 144 \| 160 \| 176 \| 194 \| 208 \| 224 \| 240 ]<br>**Default:** 128<br>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 ]<br>**Default:** Auto<br>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).<br>For MSTP, this parameter applies to both external and internal path cost. |
| RSTP Cost | **Synopsis:** An integer between 0 and 2147483647 or [ Auto ]<br>**Default:** Auto<br>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).<br>For MSTP, this parameter applies to both external and internal path cost. |
| Edge Port | **Synopsis:** [ False \| True \| Auto ]<br>**Default:** Auto<br>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 ]<br>**Default:** Auto<br>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 al- |

| Parameter | Description |
|---|---|
| | lows this behavior or overrides it, forcing point-to-point to be true or false. Force the parameter true when the port operates a point-to-point link but cannot run the link in full-duplex mode. Force the parameter false when the port operates the link in full-duplex mode, but is still not point-to-point (e.g. a full-duplex link to an unmanaged bridge that concentrates two other STP bridges). |
| `Restricted Role` | **Synopsis:** [ True \| False ]<br>**Default:** False<br>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 ]<br>**Default:** False<br>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**.

## 9.1.6 Configuring eRSTP

To configure eRSTP, do the following:

1. Navigate to ***Network Redundancy » Spanning Tree » Configure eRSTP Parameters***. The **eRSTP Parameters** form appears.
2. Configure the following parameter(s) as required:

| Parameter | Description |
|---|---|
| `Max Network Diameter` | **Synopsis:** [ MaxAgeTime \| 4*MaxAgeTime ]<br>**Default:** 4*MaxAgeTime<br>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 |

| Parameter | Description |
|---|---|
| | RSTP BPDUs have to traverse. The standard supported maximum network diameter is equal to the value of the 'MaxAgeTime' RSTP configuration parameter.<br>eRSTP offers an enhancement to RSTP which allows it to cover networks larger than ones defined by the standard.<br>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 ]<br>**Default:** Don't shutdown<br>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.<br>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 is set to 'TRUE' or RSTP is disabled, the port will be shutdown for the time period specified by this parameter.<br>• `Don't shutdown` – BPDU Guard is disabled<br>• `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 ]<br>**Default:** On<br>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.<br>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.<br>**Note**<br>• This feature is only available in RSTP mode. In MSTP mode, the configuration parameter is ignored.<br>• 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.<br>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. |

| Parameter | Description |
|---|---|
| | These are the supported configuration options:<br>• `Off` – Fast Root Failover algorithm is disabled and hence a root switch failure may result in excessive connectivity recovery time.<br>• `On` – Fast Root Failover is enabled and the most robust algorithm is used, which requires the appropriate support in the root switch.<br>• `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 ]<br>**Default:** On<br>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.<br>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.<br>This configuration parameter enables the aforementioned interoperability mode. |
| `Cost Style` | **Synopsis:** [ STP (16 bit) \| RSTP (32 bit) ]<br>**Default:** STP (16 bit)<br>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.<br>This configuration parameter selects the style of link costs to employ.<br>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**.

## 9.1.7 Viewing Global Statistics for STP

To view global statistics for STP, Navigate to ***Network Redundancy » Spanning Tree » View Bridge RSTP Statistics***. The **Bridge RSTP Statistics** form appears.

This table displays the following information:

| Parameter | Description |
|---|---|
| `Bridge Status` | **Synopsis:** [ Designated Bridge \| Not Designated For Any LAN \| Root Bridge ]<br>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<br>Bridge Identifier of this bridge. |
| `Root ID` | **Synopsis:** $$ / ##-##-##-##-##-## where $$ is 0 to 65535, ## is 0 to FF<br>Bridge Identifier of the root bridge. |
| `Root Port` | **Synopsis:** 1/1 to maximum port number or [ <empty string> ]<br>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<br>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.<br>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<br>The configured Hello time from the Bridge RSTP Parameters menu. |
| `Learned Hello Time` | **Synopsis:** An integer between 0 and 65535<br>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<br>The configured Forward Delay time from the Bridge RSTP Parameters menu. |
| `Learned Forward Delay` | **Synopsis:** An integer between 0 and 65535<br>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<br>The configured Maximum Age time from the Bridge RSTP Parameters menu. |
| `Learned Max Age` | **Synopsis:** An integer between 0 and 65535<br>The actual Maximum Age time provided by the root bridge as learned in configuration messages. This time is used in designated bridges. |

| Parameter | Description |
|---|---|
| `Total Topology Changes` | **Synopsis:** An integer between 0 and 65535<br>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<br>The time since the last time a topology change was detected by the bridge. |

## 9.1.8 Viewing STP Statistics for Ethernet Ports

To view STP statistics for Ethernet ports, Navigate to ***Network Redundancy » Spanning Tree » View Port RSTP Statistics***. The **Port RSTP Statistics** table appears.

This table displays the following information:

| Parameter | Description |
|---|---|
| `Port(s)` | **Synopsis:** Comma-separated list of ports<br>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 ]<br>Status of this port in Spanning Tree. This may be one of the following:<br>• `Disabled` – STP is disabled on this port.<br>• `Listening` – This state is not used by .<br>• `Learning` – The port is learning MAC addresses to prevent flooding when it begins forwarding traffic.<br>• `Forwarding` – The port is forwarding traffic.<br>• `Blocking` – The port is blocking traffic.<br>• `Link Down` – STP is enabled on this port but the link is down.<br>• `Discarding` – The link is not used in the STP topology but is standing by. |
| `Role` | **Synopsis:** [ Root \| Designated \| Alternate \| Backup \| Master ]<br>Role of this port in Spanning Tree. This may be one of the following:<br>• `Designated` – The port is designated for (i.e. carries traffic towards the root for) the LAN it is connected to.<br>• `Root` – The single port on the bridge, which provides connectivity towards the root bridge.<br>• `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.<br>• `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<br>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<br>The count of RSTP configuration messages received on this port. |
| `TX RSTs` | **Synopsis:** An integer between 0 and 4294967295<br>The count of RSTP configuration messages transmitted on this port. |
| `RX Configs` | **Synopsis:** An integer between 0 and 4294967295<br>The count of STP configuration messages received on this port. |
| `TX Configs` | **Synopsis:** An integer between 0 and 4294967295<br>The count of STP configuration messages transmitted on this port. |
| `RX Tcns` | **Synopsis:** An integer between 0 and 4294967295<br>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<br>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<br>Provided on the root ports of designated bridges, the Bridge Identifier of the bridge this port is connected to. |
| `operEdge` | **Synopsis:** [ True \| False ]<br>The port is operating as an edge port or not. |

## 9.1.9 Managing Multiple Spanning Tree Instances

This section describes how to configure and manage Multiple Spanning Tree Instances (MSTIs).

### 9.1.9.1 Viewing Statistics for Global MSTIs

To view statistics for global MSTIs, Navigate to ***Network Redundancy » Spanning Tree » View Bridge MSTI Statistics***. The **Bridge MSTI Statistics** form appears.

To view statistics for global MSTIs, Navigate to ***Spanning Tree » View Bridge MSTI Statistics***. The **Bridge MSTI Statistics** form appears.

This table displays the following information:

| Parameter | Description |
|---|---|
| `Bridge Status` | **Synopsis:** [ Designated Bridge \| Not Designated For Any LAN \| Root Bridge ]<br>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<br>Bridge Identifier of this bridge. |
| `Root ID` | **Synopsis:** $$ / ##-##-##-##-##-## where $$ is 0 to 65535, ## is 0 to FF<br>Bridge Identifier of the root bridge. |
| `Root Port` | **Synopsis:** 1/1 to maximum port number or [ <empty string> ]<br>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<br>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.<br>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<br>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. |

### 9.1.9.2 Viewing Statistics for Port MSTIs

To view statistics for port MSTIs, Navigate to ***Network Redundancy » Spanning Tree » View Port MSTI Statistics***. The **Port MSTI Statistics** form appears.

This table displays the following information:

| Parameter | Description |
|---|---|
| `Port(s)` | **Synopsis:** Comma-separated list of ports<br>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 ]<br>Status of this port in Spanning Tree. This may be one of the following:<br>• `Disabled` – STP is disabled on this port.<br>• `Listening` – This state is not used by .<br>• `Learning` – The port is learning MAC addresses in order to prevent flooding when it begins forwarding traffic.<br>• `Forwarding` – The port is forwarding traffic.<br>• `Blocking` – The port is blocking traffic.<br>• `Link Down` – STP is enabled on this port but the link is down.<br>• `Discarding` – The link is not used in the STP topology but is standing by. |
| `Role` | **Synopsis:** [ Root \| Designated \| Alternate \| Backup \| Master ]<br>Role of this port in Spanning Tree. This may be one of the following:<br>• `Designated` – The port is designated for (i.e. carries traffic towards the root for) the LAN it is connected to.<br>• `Root` – The single port on the bridge, which provides connectivity towards the root bridge.<br>• `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.<br>• `Alternate` – The port is attached to a bridge that provides connectivity to the root bridge. It is not used but is standing by.<br>• `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<br>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<br>Provided on the root ports of designated bridges, the Bridge Identifier of the bridge this port is connected to. |

### 9.1.9.3 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 ***Network Redundancy » Spanning Tree » Configure MST Region Identifier***. The **MST Region Identifier** form appears.
2. Configure the following parameter(s) as required:

| Parameter | Description |
|---|---|
| `Name` | **Synopsis:** A string 32 characters long<br>**Default:** 00-0A-DC-92-00-00<br>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<br>**Default:** 0<br>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 sub-regions under the same region name. |
| `Digest` | **Synopsis:** A string 32 characters long<br>**Default:** 0<br>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**.

### 9.1.9.4 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 ***Network Redundancy » Spanning Tree » Configure Bridge MSTI Parameters***. The **Bridge MSTI Parameters** form appears.
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 ]<br>**Default:** 32768<br>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**.

### 9.1.9.5 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 ***Network Redundancy » Spanning Tree » Configure Port MSTI Parameters***. The **Port MSTI Parameters** table appears.
2. Select an Ethernet port. The **Port MSTI Parameters** form appears.
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:** Comma-separated list of ports<br>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 ]<br>**Default:** 128<br>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 ]<br>**Default:** Auto<br>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 preferen- |

| Parameter | Description |
|---|---|
| | tially 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).<br>For MSTP, this parameter applies to both external and internal path cost. |
| `RSTP Cost` | **Synopsis:** An integer between 0 and 2147483647 or [ Auto ]<br>**Default:** Auto<br>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).<br>For MSTP, this parameter applies to both external and internal path cost. |

5. Click **Apply**.

### 9.1.10 Clearing Spanning Tree Protocol Statistics

To clear all spanning tree protocol statistics, do the following:

1. Navigate to ***Network Redundancy » Spanning Tree » Clear Spanning Tree Statistics***. The **Clear Spanning Tree Statistics** form appears.
2. Click **Confirm**.

## 9.2 Managing the Media Redundancy Protocol (MRP)

RUGGEDCOM ROS supports the Media Redundancy Protocol (MRP).

### 9.2.1 Understanding MRP

The Media Redundancy Protocol (MRP) is a networking protocol designed to implement redundancy and recovery in a ring topology of up to 50 devices. It allows rings of Ethernet switches to quickly overcome any single failure of an inter-switch link or switch in the MRP ring or interconnection topology.

MRP operates between Layer 2 and the application layer and uses the functions of ISO/IEC/IEEE 8802-3 (IEEE 802.3) and IEEE 802.1Q, including the Filtering Database (FDB).

MRP is standardized by the International Electrotechnical Commission as IEC 62439-2.

#### 9.2.1.1 MRM vs MRC Devices

In an MRP ring, the Media Redundancy Manager (MRM) acts as the ring manager, while Media Redundancy Clients (MRCs) act as member nodes of the ring.

The MRM periodically sends out MRP Test messages through both of its ring ports. These messages are forwarded by the MRCs between their ring ports. As the switches are connected in a ring, the MRP test messages circulate through the ring and return to the MRM. This allows the MRM to determine the state of the ring.

When the MRP test messages are returned to the MRM, redundancy is present and the ring is declared closed. If the MRP test messages fail to return, redundancy is lost and the ring is declared open.

When the ring is closed, the MRM drops (blocks) all packets on one of its two designated ring ports, while the other port forwards packets. When a link failure occurs, the MRCs sends a link failure notification to the MRM, which will then unblock its blocked port, enabling communication between all of the devices.

#### 9.2.1.2 MRA Devices

Media Redundancy Manager Auto (MRA) devices automatically decide which device will take on the role of manager in the ring. This is done through an election process between all MRAs in the ring. Once the manager is elected, the rest of the MRAs act as clients.

When an MRA is present in a ring, all other devices in the ring must be either MRA or MRC (not MRM).

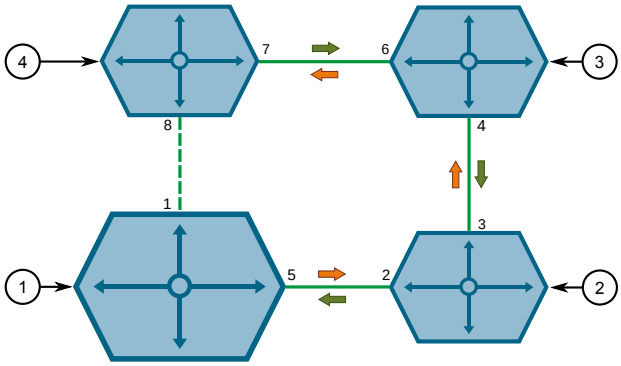
#### 9.2.1.3 Ring Port States

MRM and MRC ring ports support three states: *disabled*, *blocked*, and *forwarding*:

- **Disabled** ring ports drop all received packets.
- **Blocked** ring ports drop all received packets except the MRP control packets.
- **Forwarding** ring ports forward all received packets.

#### 9.2.1.4 Ring-Closed vs Ring-Open

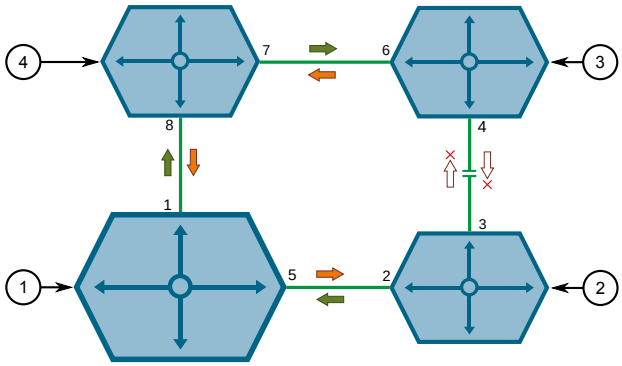
During normal operation, the network works in the ring-closed state. In this state, one of the MRM ring ports is blocked, while the other is forwarding. Both ring ports of all MRCs are forwarding.




① MRM or MRA acting as Manager
② MRP Client 1
③ MRP Client 2
④ MRP Client 3

Figure 9.5 MRP Ring-Closed State

In case of failure, the network works in the ring-open state. In this state, when a link connecting two devices fails, both ring ports of the MRM are now forwarding. The MRCs adjacent to the failure have a blocked and a forwarding ring port and the other MRCs have both ring ports forwarding.




① MRM or MRA acting as Manager
② MRP Client 1
③ MRP Client 2
④ MRP Client 3

Figure 9.6 MRP Ring-Open State

### 9.2.2 Configuring MRP Globally

To configure the Media Redundancy Protocol globally, do the following:

1. Navigate to ***Network Redundancy » Ring Redundancy » Configure Global MRP Parameters***. The **Global MRP Parameters** form appears.
2. Configure the following parameter(s) as required:

| Parameter | Description |
|---|---|
| `State` | **Synopsis:** [ Disabled \| Enabled ]<br>**Default:** Disabled<br>Enables/disables MRP globally. Note that MRP can be disabled on a per port basis. |
| `Auto Generate UUID` | **Synopsis:** [ Disabled \| Enabled ]<br>**Default:** Enabled<br>Enables/disables the automatic generation of the MRP UUID (Universal Unique Identifier). If enabled, any existing user-configured domain ID will be overwritten by the UUID generated. The generated UUID is the MD5 hash of the domain name. |

3. Click **Apply**.

### 9.2.3 Viewing the Status of MRP Instances

To view the status of MRP instances, navigate to ***Network Redundancy » Ring Redundancy » View MRP Instance Status***. The **MRP Instance Status** table appears.

This table displays the following information:

| Parameter | Description |
|---|---|
| `Index` | The MRP instance number. |
| `Name` | **Synopsis:** A string 24 characters long or [ default-mrpdomain ]<br>**Default:** default-mrpdomain<br>The name of the MRP domain/ring. All MRP instances belonging to the same ring must have the same domain name. |
| `Role` | The role assigned to the MRP instance:<br>• `Disabled` – No role is assigned. The MRP instance is disabled.<br>• `Client` – MRP Client.<br>• `Manager` – MRP Manager.<br>• `ManagerAuto` – MRP instance automatically determines the role. |
| `Ring Status` | The status of the MRP ring. Possible values include:<br>• `N/A` – The status of the ring is unknown. This is displayed when the device is an MRC.<br>• `Open` – The MRP ring is open. Both ring ports are forwarding packets. |

| Parameter | Description |
|---|---|
| | • `Closed` – The MRP ring is closed. One ring port is forwarding packets, while the other is blocking packets. |
| `PRM Port` | The port number and state of the MRP ring port. Possible values include:<br>• `{ port }-OFF` – MRP not running.<br>• `{ port }-DWN` – The ring port is down.<br>• `{ port }-BLK` – The ring port is blocking packets.<br>• `{ port }-FWD` – The ring port is forwarding packets. |
| `SEC Port` | The port number and state of the MRP ring port. Possible values include:<br>• `{ port }-OFF` – MRP not running.<br>• `{ port }-DWN` – The ring port is down.<br>• `{ port }-BLK` – The ring port is blocking packets.<br>• `{ port }-FWD` – The ring port is forwarding packets. |
| `Multi-MRM Err` | Error indicated by an MRM when more than one MRM are active in the MRP ring. Possible values include:<br>• `false` – No Multi-MRM error.<br>• `true` – More than one MRM present in the ring. |
| `One Side Rx Err` | Error indicated by an MRM when the test frames of an MRM have been seen, but only on one ring port. Possible values include:<br>• `false` – No One Side Rx error.<br>• `true` – Test frame received only on one ring port. |

## 9.2.4 Adding an MRP Instance

To configure an MRP instance, do the following:

1. Navigate to ***Network Redundancy » Ring Redundancy » Configure MRP Instances***. The **MRP Instances** table appears.
2. Click **InsertRecord**. The **MRP Instances** form appears.

**NOTICE**

RUGGEDCOM ROS only allows multiple MRP instances if all instances are Managers. A device can have up to four Manager instances.

**NOTICE**

MRMs or MRAs acting as Manager must be either physically disconnected or have the ring port disabled (i.e. MRP ring open) before the MRM instance configuration can be changed.

For more information about configuring port parameters, refer to "Configuring an Ethernet Port (Page 66)".

For more information about open and closed MRP rings, refer to "Managing the Media Redundancy Protocol (MRP) (Page 214)".

**Note**
To avoid potential misconfiguration issues which can result in loss of network access, Siemens recommends disabling the ring port of an MRC before configuring it. For more information about configuring port parameters, refer to "Configuring an Ethernet Port (Page 66)".

**Note**
When using port security in an MRP ring, the MAC addresses of devices in the ring must be configured to allow communication between them. Also, the MRM's ring port must be configured in the **Static MAC Addresses** table for the ring to remain in a closed state. For more information, refer to "Static MAC Address-Based Authentication in an MRP Ring (Page 122)".

3. Configure the following parameters:

| Parameter | Description |
|---|---|
| `Index` | **Synopsis:** An integer between 1 and 4<br>**Default:** 1<br>The MRP instance number. |
| `Name` | **Synopsis:** A string 24 characters long<br>**Default:** default-mrpdomain<br>The name of the MRP domain/ring. All MRP instances belonging to the same ring must have the same domain name. |
| `Role` | **Synopsis:** [ Disabled \| Client \| Manager \| ManagerAuto ]<br>**Default:** Client<br>The role assigned to the MRP instance:<br>• `Disabled` – No role is assigned. The MRP instance is disabled.<br>• `Client` – MRP Client.<br>• `Manager` – MRP Manager.<br>• `ManagerAuto` – MRP instance automatically determines the role. |
| `PRM Port` | **Synopsis:** 1 to maximum port number<br>**Default:** 1<br>MRP ring port number. The port number as seen on the silkscreen of the switch. |
| `SEC Port` | **Synopsis:** 1 to maximum port number<br>**Default:** 1<br>MRP ring port number. The port number as seen on the silkscreen of the switch. |

| Parameter | Description |
|---|---|
| `Priority` | **Synopsis:** A string 4 characters long<br>**Default:** 8000<br>The priority assigned to the MRP instance. This is used when negotiating with other MRP devices to determine which is the MRP Manager. Possible values include:<br>• `0000` – Highest priority (Manager)<br>• `1000` – 7000 – High priority (Manager)<br>• `8000` – Default priority (Manager)<br>• `9000` – `E000` – Low priority (ManagerAuto)<br>• `F000` – Lowest priority (ManagerAuto)<br>The priority only applies when Role is set to Manager or ManagerAuto. |
| `ID` | **Synopsis:** A string 32 characters long<br>**Default:** FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF<br>128-bit domain UUID unique to a domain/ring. All MRP instances belonging to the same ring must have the same domain ID. If the Auto Generate UUID parameter is enabled, ROS automatically generates the domain ID as an MD5 hash of the domain name. In this case, any attempt to modify the domain ID will be rejected. If the Auto Generate UUID parameter is disabled, the domain ID can be modified by the user. |

4. Click **Apply**.

## 9.2.5 Deleting an MRP Instance

To delete an MRP instance, do the following:

1. Navigate to ***Network Redundancy » Ring Redundancy » Configure MRP Instances***. The **MRP Instances** table appears.
2. Click the desired record. The **MRP Instances** form appears.

**NOTICE**

MRMs or MRAs acting as Manager must be either physically disconnected or have the ring port disabled (i.e. MRP ring open) before the MRM instance configuration can be changed.

For more information about configuring port parameters, refer to "Configuring an Ethernet Port (Page 66)".

For more information about open and closed MRP rings, refer to "Managing the Media Redundancy Protocol (MRP) (Page 214)".

**Note**

To avoid potential misconfiguration issues which can result in loss of network access, Siemens recommends disabling the ring port of an MRC before configur-

ing it. For more information about configuring port parameters, refer to "Configuring an Ethernet Port (Page 66)".

3. Click **Delete**.

## 9.2.6 Example: Configuring an MRP Ring

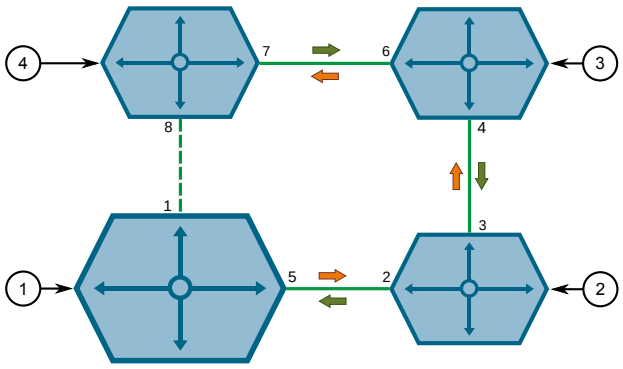
This example demonstrates how to configure an MRP ring using four RUGGEDCOM ROS devices.

In the following topology, the MRP ring is operating in the ring-closed state. The MRP Manager (MRM) device serves as the ring manager, while the MRP Client (MRC) devices act as member nodes of the ring. Each MRM or MRC node has two ports participating in the ring.

The MRM blocks all packets forwarding on one of its two designated ring ports. If one of two links on any other ring nodes detects a failure, the MRP ring will change to the ring-open state. In this state, the MRC sends a message to the MRM which then unblocks its blocked port, enabling communication between all of the switches.

For more information about ring-closed and ring-open states, refer to "Managing the Media Redundancy Protocol (MRP) (Page 214)".

| NOTICE |
| --- |
| The values shown are specific to the provided topology. Actual values can vary based on the user's configuration. |




① MRP Manager
② MRP Client 1
③ MRP Client 2
④ MRP Client 3

Figure 9.7 Topology – MRP Ring

To configure an MRP ring per the topology, do the following:

1. Make sure RSTP is disabled on ports acting as PRM and SEC ports in the ring. For more information, refer to "Configuring an Ethernet Port (Page 66)".
2. Enable MRP on the MRP Manager and all MRP Client devices. For more information, refer to "Configuring MRP Globally (Page 217)".
3. Configure an MRP instance for the MRP Manager device as follows:

| Parameter | Value |
|---|---|
| Name | { name } |
| Role | Manager |
| PRM Port | 5 |
| SEC Port | 1 |
| Priority | 1000 |

   For more information about configuring MRP instances, refer to "Adding an MRP Instance (Page 218)".
4. Configure an MRP instance for each MRP Client device as follows:

   **Note**
   In this example, three devices are being used. MRP is supported in ring topologies with up to 50 devices.

| Device | Parameter | Value |
|---|---|---|
| MRP Client 1 | Name | { name } |
| | Role | Client |
| | PRM Port | 2 |
| | SEC Port | 3 |
| | Priority | A000 |
| MRP Client 2 | Name | { name } |
| | Role | Client |
| | PRM Port | 4 |
| | SEC Port | 6 |
| | Priority | A000 |
| MRP Client 3 | Name | { name } |
| | Role | Client |
| | PRM Port | 7 |
| | SEC Port | 8 |
| | Priority | A000 |

   For more information about configuring MRP instances, refer to "Adding an MRP Instance (Page 218)".
5. To verify the configuration, make sure the MRP Instance ID is generated automatically on the MRP Manager device and each MRP client device. For more information about the MRP Instance ID, refer to "Adding an MRP Instance (Page 218)".

# 9.3 Managing Redundant Network Access (RNA)

This section describes how to configure Redundant Network Access (RNA).

RNA aides in the deployment of network redundancy by duplicating all frames bound for the redundant network domain. It provides a means of network failover should a device or path become unavailable.

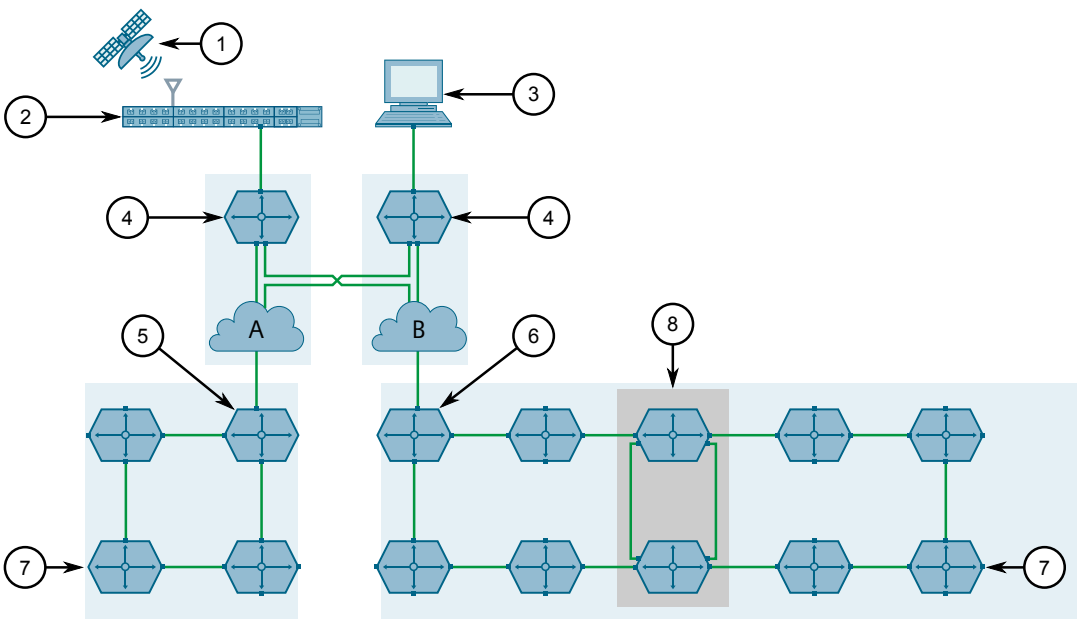
RNA is designed for mission-critical, time-sensitive applications (i.e. IEC 61850 substations) that require zero downtime.

## 9.3.1 Understanding Redundant Network Access

Layer 2 protocols – such as the Rapid Spanning Tree Protocol (RSTP), Resilient Ethernet Protocol (REP) and Media Redundancy Protocol (MRP) – help networks recover from failures by automatically changing the network configuration to allow the flow of traffic to resume, typically by opening a blocked port. However, this is a two-step process (fault detection followed by network reconfiguration) that can take a few milliseconds or a few seconds to complete based on implementation and topology, resulting in a noticeable network delay.

Redundant Network Access (RNA) provides instead *zero downtime* network recovery by duplicating frames using one of the following mechanisms:

- Parallel Redundancy Protocol (PRP)
- High-Availability Seamless Redundancy (HSR)
- HSR to PRP
- HSR QuadBox




① Satellite

② IEEE1588 Grandmaster Clock
③ HMI
④ PRP RedBox
⑤ HSR/PRP-A RedBox
⑥ HSR/PRP-B RedBox
⑦ HSR RedBox
⑧ HSR QuadBox

Figure 9.8 HSR, PRP and HSR QuadBox Applications

#### 9.3.1.1 RNA Definitions

In an RNA network, there are *Double Attached Nodes (DANs)*, *Singly Attached Nodes (SANs)*, *Virtual DANs (VDANs)* and *RedBox* devices.

- **DANP**

  A DANP is a PRP-aware device that has a network port connected to LAN A and a network port connected to LAN B. DANPs duplicate each received data packet and assign them both a Redundancy Check Trailer (RCT) before sending them simultaneously to their destination nodes. An RCT contains a sequence number that helps the destination node identify which packets are duplicates. Destination nodes remove the RCT from the first packet they receive and then consume them. If a second packet is received, the destination node knows to discard it.

- **DANH**

  A DANH is an HSR-aware device that is doubly attached to an HSR ring. DANHs duplicate each received data packet and assign them both an HSR tag before sending them simultaneously to their destination nodes. An HSR tag contains a sequence number that helps the destination node identify which packets are duplicates. Destination nodes remove the HSR tag from the first packet they receive and then consume them. If a second packet is received, the destination node knows to discard it.

- **SAN**

  Singly Attached Nodes (SANs) are PRP-unaware devices connected to either LAN A or LAN B.

- **RedBox**

  RedBox devices, or PRP/HSR Redundancy Boxes, function similarly to DANs, except they also act as proxies on behalf of other devices that are PRP/HSR-unaware and have only one network port.

- **VDAN**

  A Virtual DAN (VDAN) is any device that sits behind a RedBox. While these devices are unable to connect directly to the redundant network like other devices, they can function like a DAN through the RedBox.

### 9.3.1.2 Logical Interlink Configuration

Either one or two RNA modules are required to configure RNA, depending on the application. Each module can be independently configured as an HSR RedBox, PRP RedBox, HSR-PRP-A RedBox, HSR-PRP-B RedBox or HSR-HSR RedBox. Two modules can be configured to create an HSR QuadBox.

Each RNA module has an A port and a B port and acts as a RedBox. For more information about the RNA module, refer to the *RUGGEDCOM Modules Catalog* for the RUGGEDCOM RST2228/RST2228P.

Each RedBox contains a *Switch Interlink* and a *Second Interlink*:

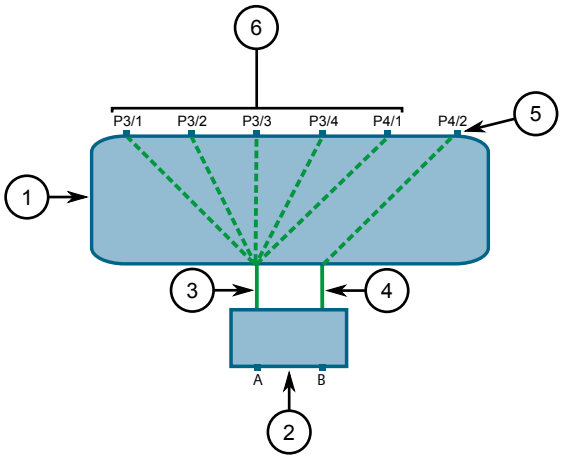
- **Switch Interlink**

  The Switch Interlink provides an internal link between the RedBox and the switch ports. It may be enabled or disabled based on the configured mode.

- **Second Interlink**

  Any switch port can be configured as the Second Interlink port. Once configured, the Second Interlink port belongs only to the RedBox and is isolated from the switch. It may be enabled or disabled based on the configured mode.

In the following scenario, a RUGGEDCOM RST2228 is equipped with one RNA module (i.e. RedBox). Switch ports 3/1 through 4/1 are acting as Virtual DANs (VDANs) while port 4/2 is acting as an isolated VDAN.




① Switch
② RedBox
③ Switch Interlink - Interlink between the RedBox and Switch Ports
④ Second Interlink - Interlink between the RedBox and one designated Switch Port
⑤ Switch port configured as the Second Interlink Port
⑥ Switch ports connected to the Switch Interlink

Figure 9.9 Example: Logical Interlink Configuration

#### 9.3.1.3 RedBox Configuration

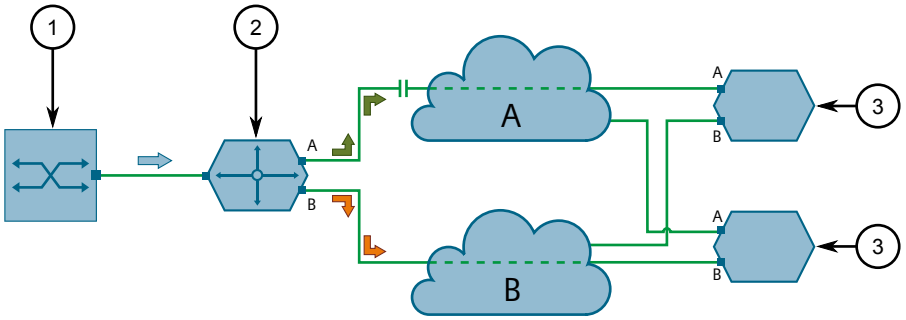
The following table shows the various RedBox configuration possibilities and their associated use cases.

| RedBox Type | Switch Interlink Mode | Second Interlink Mode | Use Case |
|---|---|---|---|
| PRP | VDAN | None | All switch ports are VDANP |
| | None | VDAN | Only the second interlink port is VDANP, isolated from switch |
| HSR | VDAN | None | All switch ports are VDANH |
| | None | VDAN | Only the second interlink port is VDANH, isolated from switch |
| HSR-PRP-A | None | PRP-A | The second interlink Port is coupled to PRP-A LAN, isolated from switch. No port is VDANH. |
| | PRP-A | None | No Port is VDANH, all switch ports are redundant connections to PRP-A LAN |
| | VDAN | PRP-A | The second interlink port is coupled to PRP-A LAN, all other switch ports are VDANH |
| | PRP-A | VDAN | The second interlink port is VDANH, all other switch ports are redundant connections to PRP-A LAN |
| HSR-PRP-B | None | PRP-B | The second interlink port is coupled to PRP-B LAN, isolated from switch. No port is VDANH. |
| | PRP-B | None | No port is VDANH, all switch ports are redundant connections to PRP-B LAN |
| | VDAN | PRP-B | The second interlink port is coupled to PRP-B LAN, all other switch ports are VDANH |
| | PRP-B | VDAN | The second interlink port is VDANH, all other switch ports are redundant connections to PRP-B LAN |
| HSR-HSR | None | HSR | The second interlink port is coupled between the two HSR Rings, isolated from switch. No port is VDANH. |
| | VDAN | HSR | The second interlink port is coupled between the two HSR Rings, all other switch ports are VDANH to both HSR Rings |
| QuadBox | None | HSR | The second interlink port is connected internally to a paired Redbox, no port is VDANH |
| | VDAN | HSR | Second interlink port is connected internally to a paired Redbox, all switch ports are VDANH to both HSR Rings |

#### 9.3.1.4 Parallel Redundancy Protocol (PRP)

Defined by the IEC 62439-3 standard, the Parallel Redundancy Protocol (PRP) replicates each data packet over two physically independent Ethernet networks (LAN A and LAN B) to guarantee the delivery of at least one of the packets should one network fail.

In a PRP redundant network, RUGGEDCOM RST2228 devices are configured as RedBox devices.




① VDAN
② RedBox (RUGGEDCOM RST2228)
③ DANP

Figure 9.10 Parallel Redundancy Protocol (PRP)

### PRP Tag

To detect duplicates, the sender PRP RedBox appends a six-octet Redundancy Control Trailer (RCT) field that contains a sequence number. The receiver PRP RedBox uses the sequence number of the RCT and the source MAC address to detect duplicates. It forwards only the first frame of a pair to its upper layers.

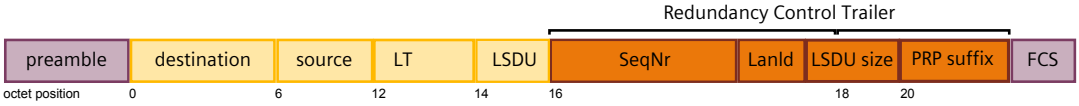



Figure 9.11 Frame Format with PRP Tag

The the Redundancy Control Trailer consists of the following fields:

- 16-bit sequence number (SeqNr)
- 4-bit LAN identifier (LanId)
- 12 bit frame size (LSDU size)
- 16-bit suffix (PRPsuffix)

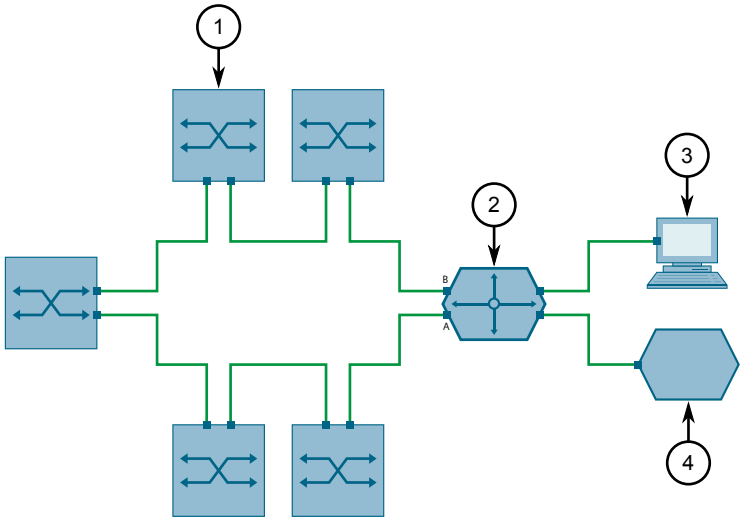
### 9.3.1.5 High-Availability Seamless Redundancy (HSR)

High-availability Seamless Redundancy (HSR) is a redundancy approach designed specifically for ring topologies. HSR is similar to PRP in that it duplicates each frame. However, rather than distribute the duplicate frames to separate networks, it sends each frame in opposite directions through the ring. Should a network link in the ring

fail, the frame on that path will not reach its destination. The frame traveling in the opposite direction however will reach the destination.

HSR connects to a ring network using the **A** and **B** ports. Both ports are connected internally using a DANH (Double Attached Node for HSR). This allows network traffic received by one port to be forwarded through the other. HSR will also send duplicate frames bound for the same destination through both of these ports. Port **A** sends traffic in the counter-clockwise direction and **B** sends traffic in the clockwise direction.

**Note**
Ports **A** and **B** are referred to as port **1/RNA** or **2/RNA** in RUGGEDCOM ROS, depending on whether slot 1 or slot 2 is being used.




① DANH
② HSR RedBox (RUGGEDCOM RST2228)
③ HSR-Unaware Device
④ VDANH

Figure 9.12 A Basic HSR Ring Topology

## HSR Tag

Each egress frame is assigned an HSR tag that defines the length of the user data, its source port and its sequence number. This information is used by other HSR-aware devices to identify duplicate frames. If a frame with the same tag is received, the duplicate frame is dropped.

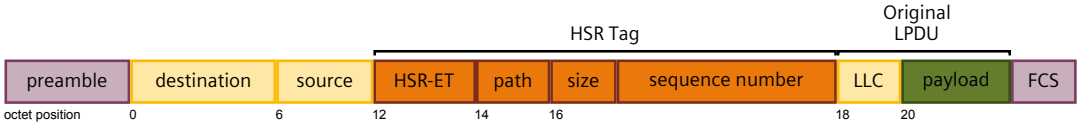


Figure 9.13 Frame Format with HSR Tag

#### Fast Identification and Forwarding

Unlike PRP, which appends a Redundancy Check Trailer to the header of each duplicate frame, HSR encapsulates each Ethernet frame in an HSR header. This enables HSR-aware devices to identify HSR frames immediately. If the frame is not for the device itself, the device will forward the frame to the next device in the ring as soon as the full header is received and the duplicate recognition process is completed. This allows for a seamless flow of traffic through the ring.

#### Multicast and Broadcast Frames

Each node in an HSR ring will receive and forward multicast and broadcast frames. However, to prevent multicast and broadcast frames from cycling endlessly, the source node will remove them once they have completed a full cycle.

#### HSR Nodes Only

Only HSR-aware nodes and RedBox devices are permitted in the HSR ring topology. This is due in part to the requirement of a secondary network interface (which devices such as Singly Attached Nodes do not have), but also due to frame encapsulation. The HSR header applied to each duplicate frame is only readable by HSR-aware devices. Non HSR-aware devices interpret the frame as a valid Layer 2 frame due to the position of the HSR tag and therefore are unable to read the user data properly.

HSR-unaware nodes can only be connected to an HSR ring via an HSR-aware RedBox.

#### HSR-PRP/HSR-HSR Coupling

RUGGEDCOM ROS supports the coupling of an HSR ring to a PRP network or to another HSR ring. Coupling increases availability by chaining multiple redundancy networks into one network.

#### HSR QuadBox

Two RNA modules can be used in a single device to create an HSR QuadBox.

#### HSR-RSTP Interworking

RUGGEDCOM ROS supports the coupling of an HSR ring to a Rapid Spanning Tree Protocol (RSTP) network to form a single RSTP domain.

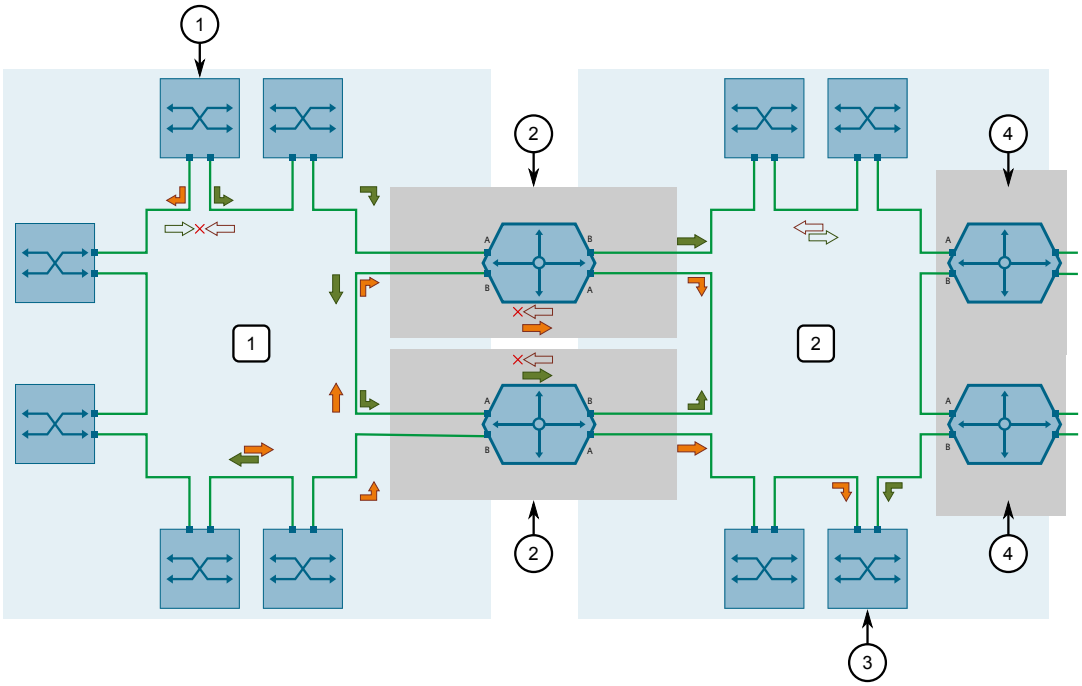
### 9.3.1.6 HSR QuadBox

An HSR QuadBox, or Quadruple Port device, is two HSR/HSR RedBoxes interlinked to combine two separate HSR rings into one redundancy network. HSR traffic travers-

es both HSR rings as normal, but traffic can now be forwarded seamlessly between them via the HSR QuadBox.

A basic HSR QuadBox implementation consists of two HSR rings (Ring 1 and 2) coupled together by two HSR QuadBoxes.

| NOTICE |
| --- |
| Two HSR QuadBoxes are required to avoid any single point of failure between the rings. |




① Source DANH
② HSR QuadBox RUGGEDCOM RST2228
③ Destination DANH
④ Next HSR Ring (partially shown)

Figure 9.14 HSR QuadBox Topology

In this example, two RUGGEDCOM RST2228 devices are being used, each containing two RNA modules to create an HSR QuadBox.

When a DANH forwards a frame, it duplicates the frame as normal and sends both copies in different directions around the HSR ring. If the frame is destined for a DANH in the other ring, the first HSR QuadBox to receive one of the duplicate packets forwards the frame to the second ring. The other duplicate is dropped if/when it is received.

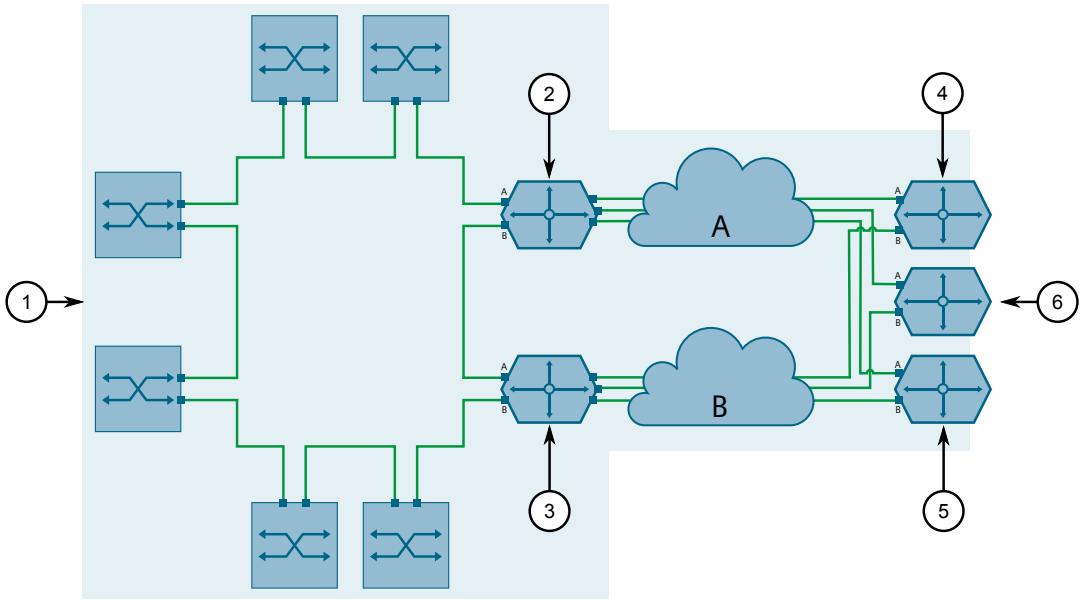
When forwarded to the second HSR ring, the HSR QuadBox duplicates the frame as the source DANH and sends both copies in different directions around the second HSR ring. The destination DANH receives the first copy of the frame and discards the second if/when it is received.

### 9.3.1.7 HSR/PRP Coupling

HSR rings and PRP networks can be coupled together to form a single redundancy network, despite their different approaches to redundant network access.

Using the Second Interlink port , a RUGGEDCOM RST2228 configured as an HSR/PRP RedBox can be connected to either LAN A or LAN B. A companion HSR/PRP RedBox is connected to the other network.

**Note**
HSR/PRP RedBoxes are referred to as either an HSR-PRP-A or HSR-PRP-B RedBox depending on which LAN they are connected to.




① HSR Ring
② HSR-PRP-A RedBox
③ HSR-PRP-B RedBox
④ DANP
⑤ DANP
⑥ PRP Network

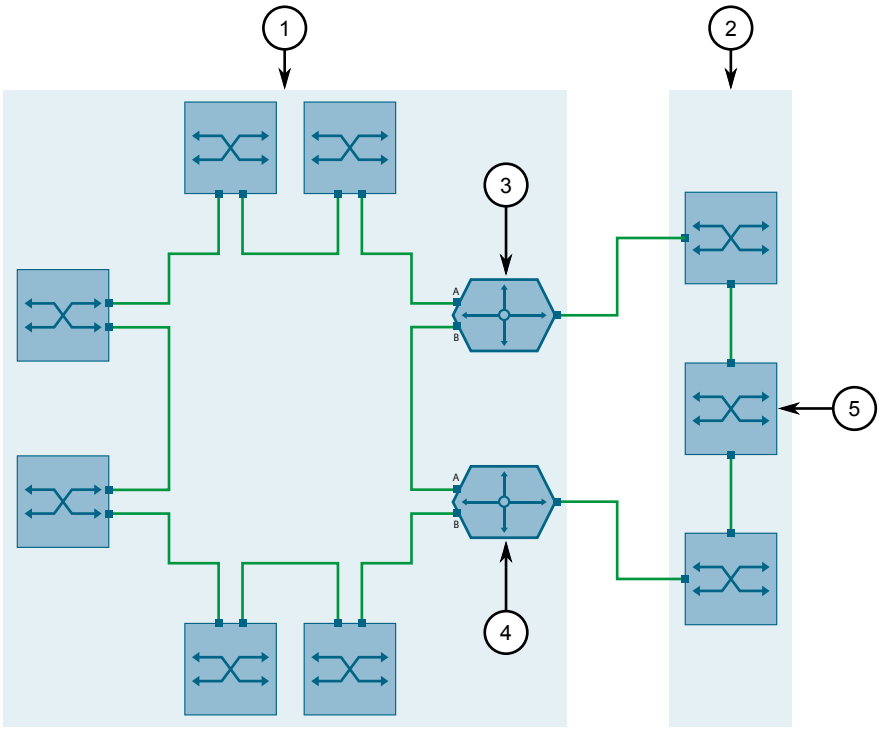
Figure 9.15 HSR Ring to PRP Network Topology

When a DANH on the HSR ring forwards a frame, the HSR/PRP RedBox duplicates the frame as normal and sends both copies in different directions on the HSR ring. If the frame is destined for a DAN on the PRP network, both HSR/PRP RedBoxes forward the first duplicate frame they receive to their respective PRP networks (LAN A or LAN B). The other duplicate is dropped if/when it is received. The destination DAN receives the first frame and discards the duplicate if/when it is received.

### 9.3.1.8 HSR/RSTP Interworking

An HSR ring can be connected to a Rapid Spanning Tree (RSTP) network to form a single RSTP domain. In this configuration, the HSR RedBox is a virtual interlink or *live wire* that acts as a point-to-point link.

**Note**
To avoid a single point of failure, two HSR RedBoxes are recommended.




① HSR Ring as a Virtual Wire
② RSTP Network
③ RUGGEDCOM RST2228
④ RUGGEDCOM RST2228
⑤ Root Bridge

Figure 9.16 HSR/RSTP Topology

When traffic is forward from an RSTP bridge to the HSR ring, the destination MAC address of the BPDU is replaced to allow normal frame forwarding.

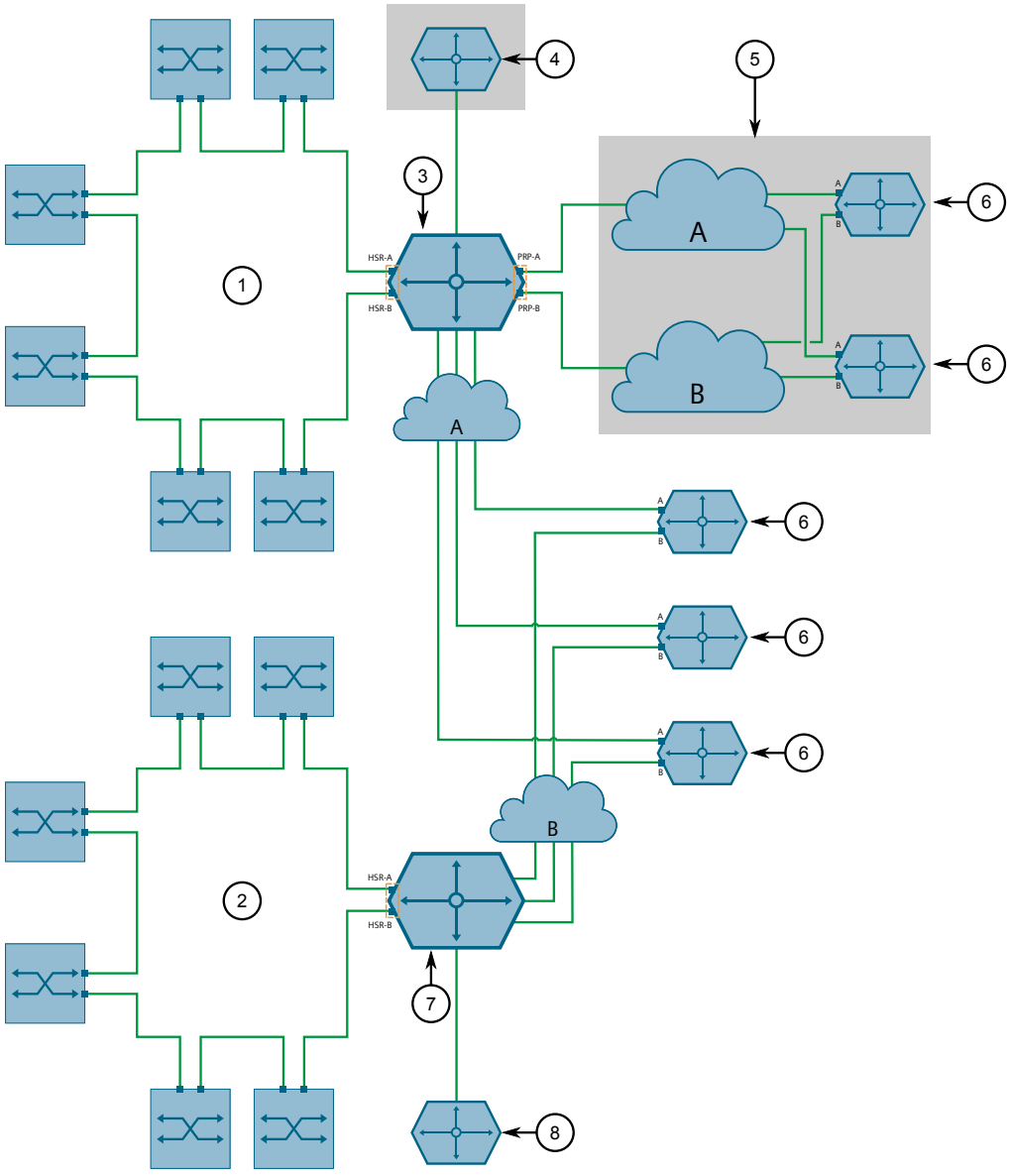
### 9.3.1.9 Two Isolated RedBoxes

An RST2228 equipped with two RNA modules can have each module configured independently.

To configure isolated RedBoxes, only one module can be configured with the Switch Interlink Port enabled (i.e. VDAN, PRP A, PRP B, HSR). The other module must be isolated from the switch.

In the following example, two RST2228 devices are being used. The top device contains two RNA modules. The first module is configured as an HSR-PRP RedBox using ports A and B. The second module is configured as a PRP RedBox, isolated from the switch. A VDANP is connected via a device switch port. Other device switch ports connect to DANPs on LAN A.

The bottom device contains a module configured as an HSR-PRP RedBox using ports A and B. A VDANH is connected via a device switch port. Other device switch ports connect to DANPs on LAN B.




① HSR Ring 1
② HSR Ring 2
③ RST2228 with two RNA Modules

④ VDANP (isolated from the switch)
⑤ PRP Network (isolated from the switch)
⑥ DANP
⑦ RST2228 with one RNA Module
⑧ VDANH

Figure 9.17 Two Isolated RedBoxes Topology

#### 9.3.1.10 Nodes and Proxy Nodes

RUGGEDCOM ROS maintains a separate Node Table and Proxy Node Table to track nodes accessible by the device. These nodes may be Virtual Dual Attached Nodes (VDANs), Dual Attached Nodes (DANs) or other RedBox devices.

- The **Node Table** lists all DANs and RedBoxes connected to the HSR ring or PRP network. The table supports up to 512 entries, each of which defines the node's MAC address and type.

  Nodes learned dynamically are discovered based on the supervision frames they send. These entries are subject to ageing and will expire if a supervision frame is not received within 60 seconds of the last received frame.
- The **Proxy Node Table** lists all VDANs connected to the device via a non-RNA port. The table supports up to 128 dynamic entries, each of which defines the node's MAC address, sequence number, and the time since the node was last seen.

**Note**
In HSR/RSTP applications, the Proxy Node Table is cleared following each topology change to prevent the HSR RedBox from sending unicast frames to proxy nodes that are no longer available, or supervision frames on behalf of proxy nodes that are no longer available. This includes all static entries.

**Operation**

An entry is added automatically to a RedBox's proxy node table when it receives traffic from each connected VDAN. A supervision frame is also sent per the configured interval to advertise this node to all other RedBoxes in the ring (for HSR) or the network A/B (for PRP). Upon receipt of the supervision frame, an entry is created in the node tables of these RedBoxes.

Unknown traffic is flooded to all ports in the ring or network momentarily until it becomes known. If there is an entry in the proxy node table for a specific destination MAC address, the RedBox forwards the traffic through its switch interlink port to the node. If there is no entry in the proxy node table, the packet is not forwarded through its switch interlink port but is instead sent back to the ring or network and discarded by the source.

#### 9.3.1.11 Before Deploying RNA

Before deploying the device on a PRP- or HSR-aware redundancy network, note the following requirements:

- Redundancy Check Trailer (RCT) and HSR tag sequence numbers expand each Ethernet frame by 6 octets. Make sure the redundancy network supports these extended frames.
- Supervisory frames, common to both PRP and HSR, also consume bandwidth. Make sure to consider the overhead introduced by RNA when calculating network capacity requirements.

### 9.3.2 Configuring RNA

To configure Redundant Network Access (RNA), do the following:

1. Navigate to ***Network Redundancy » Seamless Redundancy » Configure RNA Parameters***. The **RNA Parameters** form appears.
2. Configure the following parameter(s) as required:

| Parameter | Description |
|---|---|
| `Redundancy Mode` | **Synopsis:** [ PRP RedBox \| HSR RedBox \| HSR-PRP-A RedBox \| HSR-PRP-B RedBox \| HSR-HSR RedBox HSR Quadbox ]<br>**Default:** PRP RedBox<br>The operational mode of the device. Options include:<br>• `PRP RedBox` – PRP redundancy mode.<br>• `HSR RedBox` – HSR redundancy mode.<br>• `HSR-PRP-A RedBox` – HSR-PRP coupler mode, where PRP LAN A is coupled with HSR ring.<br>• `HSR-PRP-B RedBox` – HSR-PRP coupler mode, where PRP LAN B is coupled with HSR ring.<br>• `HSR-HSR RedBox` – HSR to HSR redundancy mode.<br>• `HSR QuadBox` – HSR QuadBox mode. Two RedBoxes needs to be in this mode (and paired) to configure an HSR QuadBox. |
| `Switch Interlink Mode` | **Synopsis:** [ None \| VDAN \| PRP A \| PRP B ]<br>**Default:** VDAN<br>The Switch Interlink port operational mode. Options include:<br>• `None` – Port is disabled – Available in every Networking Mode.<br>• `VDAN` – Virtual Doubly Attached Node (SAN as visible through a RedBox) Port for RedBox – Available in every Networking Mode.<br>• `PRP A` – PRP LAN A that is coupled with HSR ring – Available in HSR-PRP-A Mode.<br>• `PRP B` – PRP LAN B that is coupled with HSR ring – Available in HSR-PRP-B Mode. |

| Parameter | Description |
|---|---|
| `Switch Interlink Port` | **Synopsis:** 0/1 to 6/4<br>**Default:** 1/RNA<br>The Switch Interlink port of an RNA Redbox. This port is the internal interlink between the RedBox and switch. |
| `Second Interlink Mode` | **Synopsis:** [ None \| VDAN \| PRP A \| PRP B \| HSR ]<br>**Default:** None<br>The Second Interlink port operational mode. Options include:<br>• `None` – Port is disabled – Available in every Networking Mode.<br>• `VDAN` – Virtual Doubly Attached Node (SAN as visible through a RedBox) Port for RedBox – Available in every Networking Mode.<br>• `PRP A` – PRP LAN A that is coupled with HSR ring – Available in HSR-PRP-A Mode.<br>• `PRP B` – PRP LAN B that is coupled with HSR ring – Available in HSR-PRP-B Mode.<br>• `HSR` – HSR-HSR coupler port mode to create a QuadBox – Available in HSR-HSR RedBox and HSR QuadBox Modes. |
| `Second Interlink Port` | **Synopsis:** 0/1 to 6/4<br>**Default:** 0/1<br>The Second Interlink port of an RNA Redbox. |
| `Paired RedBox ID` | **Synopsis:** An integer between 0 and 6<br>**Default:** 0<br>The paired RedBox ID for HSR QuadBox. |
| `Net ID` | **Synopsis:** An integer between 1 and 7<br>**Default:** 1<br>The PRP network identifier (NetId) of the PRP network attached to the HSR ring. Available in HSR-PRP-A/B RedBox modes. |
| `Life Check Interval` | **Synopsis:** An integer between 0 and 300 or [ Disabled ]<br>**Default:** 2<br>The time interval in seconds in which a node sends a supervision frame. |
| `Node Forget Time` | **Synopsis:** An integer<br>**Default:** 60<br>The time in seconds after which a node entry is cleared from the node table. |
| `Proxy Node Forget Time` | **Synopsis:** An integer<br>**Default:** 60<br>The time in seconds after which a proxy node entry is cleared from the proxy node table. |

| Parameter | Description |
|---|---|
| `Entry Forget Time` | **Synopsis:** An integer<br>**Default:** 40<br>The time in milliseconds after which a duplicate entry is cleared from the duplicate removal table. |
| `Max Proxy Node Entries` | **Synopsis:** An integer between 0 and 128<br>**Default:** 128<br>The maximum number of proxy nodes handled by the device. |

3. Click **Apply**.

## 9.3.3 Enabling/Disabling HSR/RSTP Interworking

For an HSR RedBox to participate in an RSTP domain as an interlink or *live wire*, HSR-to-RSTP must first be enabled. For more information about HSR-to-RSTP coupling, refer to "HSR/RSTP Interworking (Page 232)".

To enable or disable HSR-to-RSTP coupling, do the following:

1. Navigate to ***Network Redundancy » Interworking Function » Configure RNA STP Coupler***. The **RNA STP Coupler** form appears.
2. Configure the following parameter(s) as required:

| Parameter | Description |
|---|---|
| `Mode` | **Synopsis:** [ Disabled \| HSR-STP ]<br>**Default:** Disabled<br>Select what redundancy technologies are configured to inter-work. |
| `STP Domain` | **Synopsis:** An integer between 1 and 255<br>**Default:** 255<br>Selects STP domain identifier to identify an instance of STP network attached to HSR ring. |

3. Click **Apply**.

## 9.3.4 Viewing RNA Status

To view the RNA status, navigate to ***Network Redundancy » Seamless Redundancy » View RNA Status***. The **RNA Status** form appears.

This table displays the following information:

| Parameter | Description |
|---|---|
| `Port A` | **Synopsis:** [ ---- \| Down \| Up ]<br>The link status of the port. |

| Parameter | Description |
|---|---|
| Port B | **Synopsis:** [ ---- \| Down \| Up ]<br>The link status of the port. |
| Number Of Nodes | **Synopsis:** An integer between 0 and 512<br>Number of entries in the node table. |
| Number Of Proxy Nodes | **Synopsis:** An integer between 0 and 128<br>Number of entries in the proxy node table. |
| Device MAC Address | **Synopsis:** ##-##-##-##-##-## where ## ranges 0 to FF<br>Device MAC address. |
| PortA PeerDelay | **Synopsis:** An integer between 0 and 2147483647<br>Shows peer delay in nanoseconds. The peer delay mechanism measures the port-to-port propagation time, such as the link delay, between two communicating ports supporting the peer delay mechanism. |
| PortB PeerDelay | **Synopsis:** An integer between 0 and 2147483647<br>Shows peer delay in nanoseconds. The peer delay mechanism measures the port-to-port propagation time, such as the link delay, between two communicating ports supporting the peer delay mechanism. |

## 9.3.5 Viewing RNA Statistics

To view the RNA Statistics table, navigate to ***Network Redundancy » Seamless Redundancy » View RNA Statistics***. The **RNA Statistics** table appears.

This table displays the following information:

| Parameter | Description |
|---|---|
| Port | **Synopsis:** [ A \| B \| Switch Interlink \| Second Interlink ]<br>The RNA port name. |
| OutPkts | **Synopsis:** An integer between 0 and 4294967295<br>**Synopsis:** [ ]<br>The number of transmitted good packets. |
| InPkts | **Synopsis:** An integer between 0 and 4294967295<br>The number of received good packets (Unicast+Multicast+Broadcast). |
| InTagPkts | **Synopsis:** An integer between 0 and 4294967295<br>Number of packets received with PRP tag. |
| InDuplicatePkts | **Synopsis:** An integer between 0 and 4294967295<br>Number of packets detected as duplicate. |

| Parameter | Description |
|---|---|
| InWrongLan | **Synopsis:** An integer between 0 and 4294967295<br>Number of packets that were received with the wrong LAN identifier |
| InErrors | **Synopsis:** An integer between 0 and 4294967295<br>The number of any type of erroneous packet. |
| InCRCErrors | **Synopsis:** An integer between 0 and 4294967295<br>Number of packets received with failed CRC validation. |

## 9.3.6 Clearing RNA Statistics

To clear the RNA Statistics table, navigate to ***Network Redundancy » Seamless Redundancy » Clear RNA Statistics***. The **Clear RNA Statistics** dialog appears.

Click **Confirm** to delete RNA statistics.

## 9.3.7 Viewing the Node Table

Nodes are Dual Attached Nodes (DANs) or other RedBoxes accessible to the device on the RNA network. RUGGEDCOM ROS supports up to 512 nodes, all of which are listed in the Nodes Table.

Each entry in the Nodes Table lists node's MAC address and type.

Nodes learned dynamically are discovered based on the supervision frames they send. These entries are subject to aging and will expire if a supervision frame is not received within 60 seconds of the last received frame.

To view the node table, navigate to ***Network Redundancy » Seamless Redundancy » View Node Table***. The **Node Table** appears.

This table displays the following information for each node.

| Parameter | Description |
|---|---|
| MAC | **Synopsis:** ##-##-##-##-##-## where ## ranges 0 to FF<br>The MAC address of a remote node. |
| Node Type | **Synopsis:** [ DANP \| REDBOXP \| VDANP \| DANH \| REDBOXH \| VDANH ]<br>Node type as indicated in the received supervision frame. |
| TimeLastSeenA | **Synopsis:** An integer between 0 and 4294967295<br>Time elapsed in Time ticks (1/100 s) since the latest frame was received from that node over LAN_A. |
| TimeLastSeenB | **Synopsis:** An integer between 0 and 4294967295<br>Time elapsed in Time ticks (1/100 s) since the latest frame was received from that node over LAN_B. |

| Parameter | Description |
|---|---|
| TimeLastSeenInterlink | **Synopsis:** An integer between 0 and 4294967295<br>Time elapsed in Time ticks (1/100 s) since the latest frame was received from that node over Interlink. |

## 9.3.8 Viewing the Proxy Node Table

Proxy nodes are Virtual Dual Attached Nodes (VDANs) connected to the device via a non-RNA port. These nodes are HSR/PRP-unaware. As such, the device acts as their proxy, managing traffic to and from the RNA network, and sending supervision frames to DANs on their behalf.

The Proxy Node Table lists all current proxy nodes up to a total of 128 dynamic entries. Each entry defines node's MAC address, sequence number, and the time since the node was list seen.

To view the Proxy Node Table, navigate to ***Network Redundancy » Seamless Redundancy » View Proxy Node Table***. The **Proxy Node Table** appears.

This table displays the following information:

| Parameter | Description |
|---|---|
| MAC | **Synopsis:** ##-##-##-##-##-## where ## ranges 0 to FF<br>The MAC address of a remote node. |
| SeqNum | **Synopsis:** An integer between 0 and 65535<br>Sequence number of supervision frame. Supervision frame allows checking the integrity of the network and the presence of the DANP nodes. |
| TimeLastSeen | **Synopsis:** An integer between 0 and 4294967295<br>Time elapsed in Time ticks (1/100 s) since the latest frame was received from that node. |

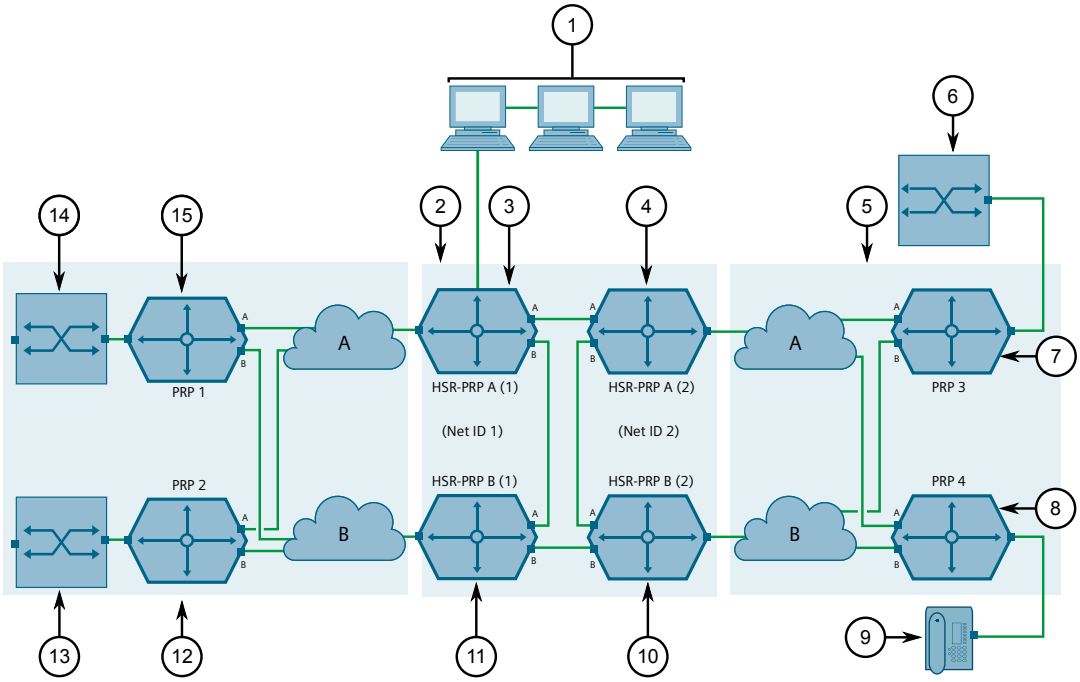
## 9.3.9 Example: Configuring an HSR-to-PRP Network

This example demonstrates how to configure an HSR Ring to work with a PRP network, using RNA-supported RUGGEDCOM ROS devices.

In the following topology, an HSR Ring is coupled to two PRP networks via LAN A and LAN B.

For more information about HSR-to-PRP coupling, refer to "HSR/PRP Coupling (Page 231)".

| NOTICE |
|---|
| The values shown are specific to the provided topology. Actual values can vary based on the user's configuration. |




① HMI
② HSR Ring
③ HSR-PRP A RedBox
④ HSR-PRP A RedBox
⑤ PRP Network 1
⑥ VDAN
⑦ PRP RedBox
⑧ PRP RedBox
⑨ IP Phone
⑩ HSR-PRP B RedBox
⑪ HSR-PRP B RedBox
⑫ PRP RedBox
⑬ VDAN
⑭ VDAN
⑮ PRP RedBox
⑯ PRP Network 2

Figure 9.18 Topology – HSR-to-PRP Network

To configure an HSR-to-PRP network per the topology, do the following:

1. Configure and connect HSR-to-PRP redboxes:

**Note**
To allow communication between external devices (VDANs, SANs, IP phones, etc.) attached to the ring, make sure the Net ID is different on each set of HSR-

to-PRP RedBoxes connected to a PRP network. For more information about configuring RNA, refer to "Configuring RNA (Page 235)".

a. Configure two RUGGEDCOM ROS devices as HSR-PRP A RedBoxes.
b. Connect port A of HSR-PRP A (1) RedBox to port B of HSR-PRP A (2) RedBox.
c. Assign a Net ID of *1* to HSR-PRP A (1).
d. Assign a Net ID of *2* to HSR-PRP A (2).
e. Configure two RUGGEDCOM ROS devices as HSR-PRP B RedBoxes.
f. Connect port A of HSR-PRP B (1) RedBox to port B of HSR-PRP B (2) RedBox.
g. Assign a Net ID of *1* to HSR-PRP B (1).
h. Assign a Net ID of *2* to HSR-PRP B (2).
i. Connect the HSR-PRP A RedBoxes to the HSR-PRP-B RedBoxes as shown.

2. Configure four RUGGEDCOM ROS devices (PRP1, PRP2, PRP3 and PRP4) as PRP RedBoxes as shown.
3. Connect the HSR ring to PRP network 1:

**Note**
For more information about configuring VLANs, refer to "Configuring VLANs for Specific Ethernet Ports (Page 147)".

a. Connect the configured second interlink port of the HSR-PRP A (1) RedBox to LAN A.
b. Connect the configured second interlink port of the HSR-PRP B (1) RedBox to LAN B.
c. Connect port A of PRP1 to LAN A, and connect Port B to LAN B.
d. Connect port A of PRP2 to LAN A, and connect Port B to LAN B.

4. Connect the HSR ring to PRP network 2:

**Note**
For more information about configuring VLANs, refer to "Configuring VLANs for Specific Ethernet Ports (Page 147)".

a. Connect the configured second interlink port of the HSR-PRP A (2) RedBox to LAN A.
b. Connect the configured second interlink port of the HSR-PRP B RedBox (2) to LAN B.
c. Connect port A of PRP3 to LAN A, and connect Port B to LAN B.
d. Connect port A of PRP4 to LAN A, and connect Port B to LAN B.

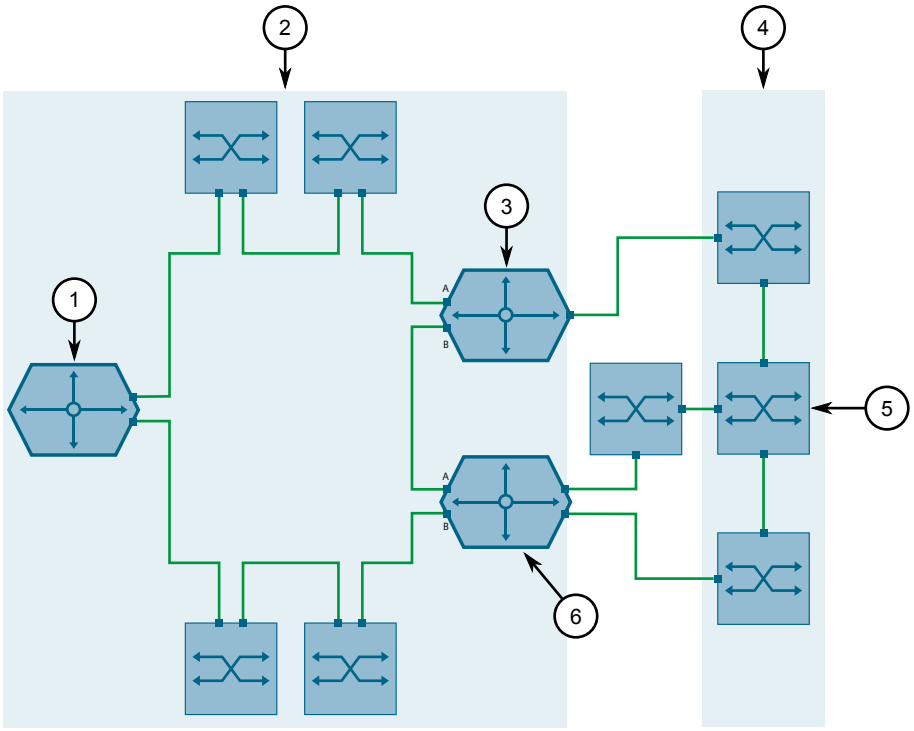
5. Connect external devices (VDANs, SANs, IP phones, etc.) to the ring as desired.

## 9.3.10 Example: Configuring an HSR-to-RSTP Ring

This example demonstrates how to configure an HSR Ring to work with a RSTP ring, using three RNA-supported RUGGEDCOM ROS devices.

For more information about HSR-to-RSTP coupling, refer to "HSR/RSTP Interworking (Page 232)".

| NOTICE |
| --- |
| The values shown are specific to the provided topology. Actual values can vary based on the user's configuration. |




① HSR1
② HSR Ring
③ HSR2
④ RSTP Ring
⑤ Root Bridge
⑥ HSR3

Figure 9.19 Topology – HSR-to-RSTP Ring

To configure an HSR-to-RSTP ring per the topology, do the following:

1. Configure and connect an RSTP ring. If RUGGEDCOM ROS devices are being used, refer to "Managing Spanning Tree Protocol (Page 185)" for more information about configuring RSTP.

2. Configure and connect HSR Redboxes:

**Note**
For more information about configuring RNA, refer to "Configuring RNA (Page 235)".

| NOTICE |
| --- |
| Make sure all devices in the HSR ring have the same STP Domain number. |

   a. Configure the three RUGGEDCOM ROS devices shown in the topology (HSR1, HSR2 and HSR3) as HSR Redboxes. For more information about configuring RNA, refer to "Configuring RNA (Page 235)".

   b. Connect the three RUGGEDCOM ROS devices in the ring, along with the desired number of external devices.

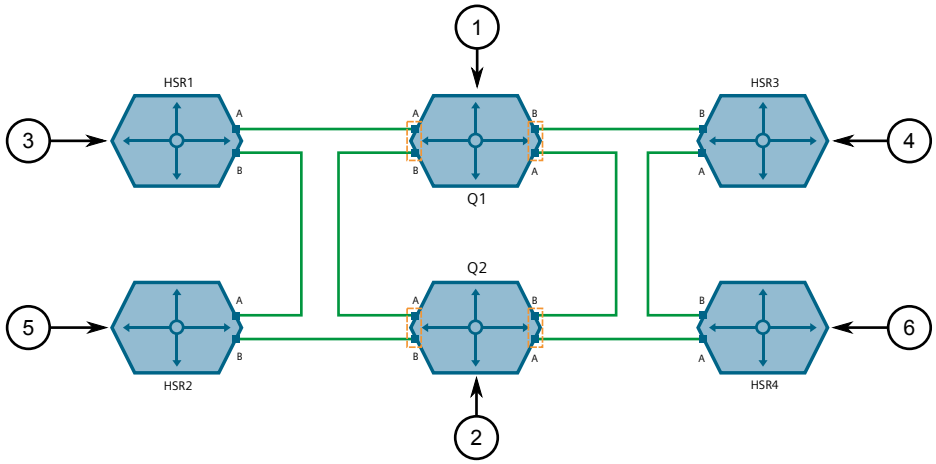
3. Couple the HSR ring to the RSTP ring by enabling HSR-to-RSTP coupling on devices HSR2 and HSR3. For more information about configuring HSR-to-RSTP coupling, refer to "Enabling/Disabling HSR/RSTP Interworking (Page 237)".

## 9.3.11 Example: Configuring an HSR QuadBox Ring

This example demonstrates how to configure an HSR QuadBox ring using two RUGGEDCOM ROS devices, each equipped with two RNA modules configured as HSR QuadBoxes, and four RUGGEDCOM ROS devices configured as HSR RedBoxes.

For more information about HSR QuadBoxes, refer to "HSR QuadBox (Page 229)".

| NOTICE |
| --- |
| The values shown are specific to the provided topology. Actual values can vary based on the user's configuration. |




① RST2228 with two RNA Modules (HSR QuadBox 1)
② RST2228 with two RNA Modules (HSR QuadBox 2)
③ HSR RedBox1

④ HSR RedBox3
⑤ HSR RedBox2
⑥ HSR RedBox4

Figure 9.20 Topology – HSR QuadBox Ring

To configure an HSR QuadBox ring per the topology, do the following:

For more information about configuring RNA, refer to "Configuring RNA (Page 235)".

1. Configure device Q1 as an HSR QuadBox:
   a. On device Q1, configure the Redundancy Mode of two RNA modules as *HSR QuadBox*.
   b. Configure the Second Interlink Port of each module as *HSR*.
   c. Configure the Switch Interlink Mode of one module as *None* and the other module as *VDAN*.
   d. Configure the Paired RedBox ID of one module as *1* and the other module as *2*.
2. Configure device Q2 as an HSR QuadBox:
   a. On device Q2, configure the Redundancy Mode of two RNA modules as *HSR QuadBox*.
   b. Configure the Second Interlink Port of each module as *HSR*.
   c. Configure the Switch Interlink Mode of one module as *None* and the other module as *VDAN*.
   d. Configure the Paired RedBox ID of one module as *1* and the other module as *2*.
3. Connect HSR QuadBoxes Q1 and Q2:
   a. Connect port A of Q1 to port B of Q2.
   b. Connect port B of Q1 to port A of Q2.
4. Configure RUGGEDCOM ROS devices as HSR RedBoxes:
   a. Configure the four RUGGEDCOM ROS devices shown in the topology (HSR1, HSR2, HSR3 and HSR4) as HSR RedBoxes.
   b. Configure the Switch Interlink Mode of each as *VDAN*.
   c. Configure the Second Interlink Mode of each as *None*.

5. Connect the devices as shown:

**Note**
Multiple HSR devices may be connected. Four devices are shown in the topology for simplicity.

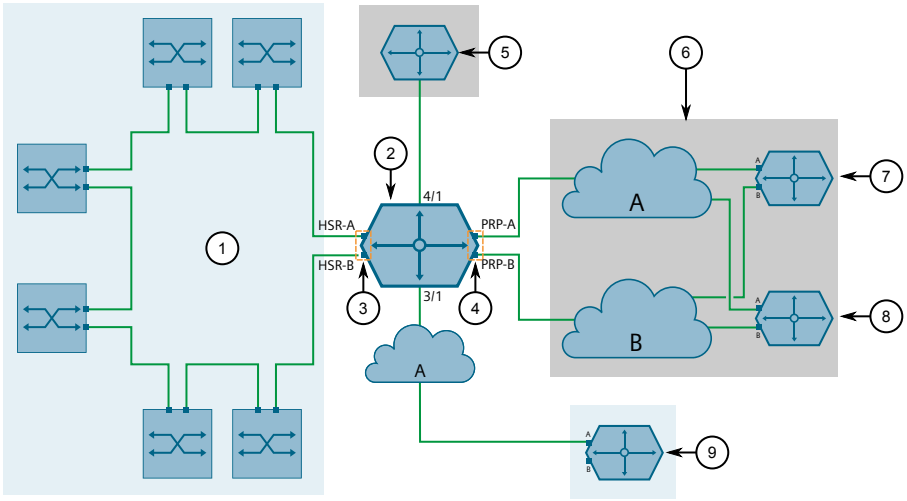
a. Connect port A of device HSR1 to port A of device Q1.
b. Connect port B of device HSR1 to port A of device HSR2.
c. Connect port B of device HSR2 to port B of device Q2.
d. Connect port B of device HSR3 to port B of device Q1.
e. Connect port A of device HSR3 to port B of device HSR4.
f. Connect port A of device HSR4 to port A of device Q2.

## 9.3.12 Example: Configuring Two Isolated RedBoxes

This example demonstrates how to configure an HSR-PRP RedBox and a PRP RedBox on a single RST2228 device. Both RedBoxes are isolated from the device, and work as if they are physically separated.

For more information about two isolated RedBoxes, refer to "Two Isolated RedBoxes (Page 232)".

| NOTICE |
| --- |
| The values shown are specific to the provided topology. Actual values can vary based on the user's configuration. |




① HSR Ring
② RST2228 with two RNA Modules
③ RNA Module 1/RNA
④ RNA Module 2/RNA

⑤ VDANP (isolated from the switch)
⑥ PRP Network (isolated from the switch)
⑦ DANP
⑧ DANP
⑨ DANP

Figure 9.21 Topology – Two Isolated RedBoxes

To configure two isolated RedBoxes per the topology, do the following:

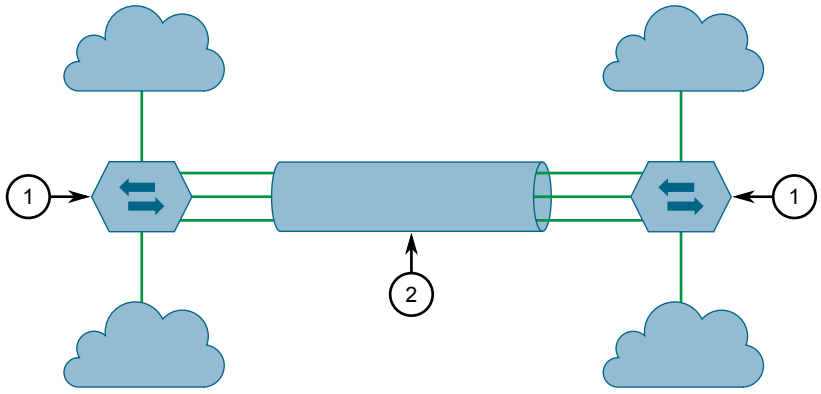
1. Configure RedBox 1 (1/RNA) as an HSR-PRP A RedBox:
   a. Configure the Switch Interlink Mode as *None*.
   b. Configure the Second Interlink Mode as *PRP-A*.
   c. Configure the Second Interlink Port as *3/1*.
2. Configure RedBox 2 (2/RNA) as a PRP RedBox:
   a. Configure the Switch Interlink Mode as *None*.
   b. Configure the Second Interlink Mode as *VDAN*.
   c. Configure the Second Interlink Port as *4/1*.
3. Connect 1/RNA ports A and B to the HSR ring.
4. Connect switch port 3/1 to LAN A.
5. Connect 2/RNA ports A and B to the PRP network.
6. Connect switch port 4/1 to the VDANP.

## 9.4 Managing Link Aggregation

Link aggregation, also referred to as *port trunking* or *port bundling*, provides the ability to aggregate or combine several Ethernet ports into one logical link (Link Aggregation Group) 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 Device
② Link Aggregation Group (LAG)

Figure 9.22 Basic Link Aggregation Topography

## 9.4.1 Link Aggregation Concepts

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

### 9.4.1.1 Static vs. Dynamic Link Aggregation

RUGGEDCOM ROS supports either static or dynamic link aggregation. In **static** link aggregation, a device is paired with a specific partner device that shares the same capabilities and configuration. The same is required for dynamic link aggregation, but with less involvement by the user. In **dynamic** link aggregation, the Link Aggregation Control Protocol (LACP) seeks a suitable partner on its own after negotiating with its peers to determine the best match.

Static link aggregation is ideal for switch-to-switch configurations, but lacks the following key features offered by dynamic link aggregation:

- **Failover**

  In static link aggregation, devices are unable to communicate the status of their LAGs. Should all ports in a LAG go down and there is a media converter between both devices, the device at the other end will not know and continue to send traffic to its partner. Dynamic link aggregation, however, will detect the failed link and stop sending traffic to the other device.

- **Renegotiation**

  Should all ports on the partner device go down and/or the Signal-to-Noise Ratio (SNR) be too high, LACP will automatically seek another LACP-enabled device on the network with which to form a new port channel.

- **Standby**

  If more ports are added to a LAG than the device supports, LACP will automatically put the excess ports on standby. It determines which ports to put on standby based on criteria defined by the user. These standby ports will wait until an active port fails and then take its place.

- **Link Verification**

  In dynamic link aggregation, both partners can mutually verify the port channel between them, making it easy for users to confirm the configuration. Static link aggregation offers no such verification.

Choosing between static or dynamic link aggregation is dependent on the capabilities of the devices available on the network.

#### 9.4.1.2 Rules and Limitations

The implementation of link aggregation must adhere to the following rules and limitations:

- A port can only belong to one Link Aggregation Group (LAG) or *port trunk* at a time.
- A port that is being mirrored (the target port) cannot belong to a LAG. However, any port that receives the mirrored traffic (the source port) can belong to a LAG.
- If only one QinQ port is supported by the device, the port working in QinQ mode cannot be a secondary member of a LAG.
- A DHCP relay agent client port cannot be a member of a LAG.
- Load balancing between the links of a bundle is randomized and may not be ideal. For instance, if three 100 Mbps links are aggregated, the resulting bandwidth of the LAG may not be precisely 300 Mbps.
- 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 LAG.
- The IEEE 802.1AX (formerly IEEE 802.3ad) Link Aggregation standard requires all physical links in the LAG to run at the same speed and in full-duplex mode. If this requirement is violated, the performance of the LAG will drop.

  The switch will raise an appropriate alarm, if such a speed/duplex mismatch is detected.

- The Spanning Tree Protocol (STP) dynamically calculates the path cost of the LAG 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, as it may lead to a longer fail-over time.

#### 9.4.1.3 Link Aggregation and Layer 2 Features

Layer 2 features (e.g. STP, VLAN, CoS, Multicast Filtering) treat a Link Aggregation Group (LAG) as a single link.

- If the Spanning Tree Protocol (STP) sets the status of an aggregated port to `Blocking` or `Forwarding`, it does it for the whole LAG.
- If one of the aggregated ports joins or leaves a multicast group (e.g. via GMRP), all other ports in the LAG will join or leave too.
- Any port configuration parameter (e.g. VLAN, CoS) change will be automatically applied to all ports in the LAG.
- 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 user interface sessions.
- When a secondary port is added to a LAG, it inherits all the configuration settings of the primary port. When this secondary port is removed from the LAG, the settings it had previous to the aggregation are restored.

#### 9.4.1.4 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 Link Aggregation Group (LAG) and will be displayed for each port as usual.
- Make sure 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 LAG.
- To get a value of an Ethernet statistics counter for the LAG, add the values of the counters for all ports in the LAG.

### 9.4.2 Configuring Link Aggregation

To configure static or dynamic link aggregation, do the following:

1. Disconnect or disable each port to be aggregated. For information about disabling a port, refer to "Configuring an Ethernet Port (Page 66)".
2. Create one or more Link Aggregation Groups (LAGs) consisting of two or more ports. For more information, refer to "Adding a Link Aggregation Group (Page 251)".
3. Connect or enable each port in the LAG. For information about enabling a port, refer to "Configuring an Ethernet Port (Page 66)".

4. If dynamic link aggregation is required, configure the global and per port LACP settings. For more information, refer to "Configuring Global LACP Settings (Page 254)" and "Configuring LACP Per Port (Page 255)".
5. Repeat Step 1 to Step 4 for a neighboring device that has the same capabilities (i.e. port speed, media type, etc.), making sure to refer to the device's user documentation for details.

## 9.4.3 Managing Link Aggregation Groups

RUGGEDCOM ROS allows up to 15 Link Aggregation Groups (LAGs), or *port trunks*, to be configured on a single device, with each consisting of up to eight ports.

**Note**
Avoid configuring LAGs when Layer 3 switching is enabled. For more information on enabling or disabling Layer 3 switching, refer to "*Layer 3* (Page 171)".

**Note**
The maximum number of LAGs for each device depends on the number of ports available. At least two ports are required to configure a LAG.

**Note**
The aggregated port with the lowest port number is called the *Primary* port. Other ports in the LAG are called *Secondary* ports.

### 9.4.3.1 Viewing a List of Link Aggregation Groups

To view a list of Link Aggregation Groups (LAGs), or *port trunks*, configured on the device, navigate to ***Link Aggregation » Configure Port Trunks***. The **Port Trunks** table appears.

If LAGs have not been configured, add LAGs as needed. For more information, refer to "Adding a Link Aggregation Group (Page 251)".

### 9.4.3.2 Adding a Link Aggregation Group

To add a LInk Aggregation Group (LAG), or *port trunk*, do the following:

**NOTICE**

The LAG must be properly configured on both sides of the port channel. 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 LAG:

1. Disconnect or disable all the ports involved in the configuration, i.e. either being added to or removed from the LAG.

2. Configure the LAG on both switches.
3. Double-check the LAG configuration on both switches.
4. Reconnect or re-enable the ports.

If the LAG is being configured while the ports are not disconnected or disabled, the port will be automatically disabled for a few seconds.

**NOTICE**

Make sure 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 LAG.

1. Navigate to ***Link Aggregation » Configure Port Trunks***. The **Port Trunks** table appears.
2. Click **InsertRecord**. The **Port Trunks** form appears.
3. Configure the following parameter(s) as required:

| Parameter | Description |
|---|---|
| `Trunk ID` | **Synopsis:** An integer between 1 and 5<br>**Default:** 1<br>The ID for the Link Aggregation Group (LAG), or port trunk. |
| `Trunk Name` | **Synopsis:** A string 19 characters long<br>The name of the Link Aggregation Group (LAG), or port trunk. Whenever possible, include details that identify the purpose of the aggregated links. |
| `Mode` | **Synopsis:** [ LACP \| Static ]<br>**Default:** Static<br>Defines how link aggregation is performed. Options include:<br>• `LACP` – Link aggregation is done dynamically using LACP for both sides of the link aggregation partnership.<br>• `Static` – Link aggregation settings are configured manually on both sides of the link aggregation partnership. LACP is not used. |
| `Ports` | A comma-separated list or range of ports to be aggregated in the Link Aggregation Group (LAG), or port trunk. |

4. Click **Apply**.

### 9.4.3.3 Deleting a Link Aggregation Group

To delete a Link Aggregation Group (LAG), or *port trunk*, do the following:

1. Navigate to ***Link Aggregation » Configure Port Trunks***. The **Port Trunks** table appears.
2. Select the desired LAG from the table. The **Port Trunks** form appears.

3. Click **Delete**.

#### 9.4.3.4 Viewing the Status of Link Aggregation Groups

To view the status of each Link Aggregation Group (LAG), or *port trunk*, configured on the device, navigate to ***Link Aggregation » View Port Trunk Statistics***. The **Port Trunk Statistics** table appears.

This table displays the following information about each LAG:

| Parameter | Description |
|---|---|
| `Trunk ID` | The ID for the Link Aggregation Group (LAG), or port trunk. |
| `Mode` | The link aggregation mode. Options include:<br>• `LACP` – Link aggregation is done dynamically using LACP for both sides of the link aggregation partnership.<br>• `Static` – Link aggregation settings are configured manually on both sides of the link aggregation partnership. LACP is not used. |
| `State` | The operational state of the Link Aggregation Group (LAG), or port trunk.. |
| `Ports Aggregated` | A comma-separated list or range of ports that are aggregated and operational in the Link Aggregation Group (LAG), or port trunk. |

### 9.4.4 Managing the Link Aggregation Control Protocol

The Link Aggregation Control Protocol (LACP) allows LACP-enabled devices to dynamically learn about each other's capabilities and automatically create port channels based on the maximum port speed and trunking state. The capabilities and configuration of each device do not need to be expressly controlled, as it would be with static link aggregation.

The capabilities of LACP-enabled devices are learned through the exchange of LACP Data Units (LACPDU). LACPDUs are distributed initially by ports configured to run LACP in `Active` mode. When these LAPDUs are received by a neighboring LACP-enabled device, an LACPDU is returned and both devices negotiate the creation of the port channel. The channel is created only if the capabilities of each device align.

**Note**
Avoid configuring LACP when Layer 3 switching is enabled. For more information on enabling or disabling Layer 3 switching, refer to "*Layer 3* (Page 171)".

**NOTICE**

At least one LACP-enabled device must have a port configured to run LACP in `Active` mode. Ports configured to run in `Passive` mode participate in the negotiation process, but will not initiate it.

Configure LACP when the *`Mode`* parameter for any port trunk is set to `LACP`.

### 9.4.4.1 Viewing Information About the LACP Partner

To view details about the LACP partner system, navigate to ***Link Aggregation » View Partner LACP Information***. The **Partner LACP Information** table appears.

This table displays the following information:

| Parameter | Description |
|---|---|
| `Port` | The port number as seen on the front plate silkscreen of the device. |
| `System Priority` | The LACP system priority of the partner system. |
| `System ID` | The MAC address of the partner system. |
| `Port Priority` | The LACP port priority of the partner port. |
| `Port Number` | The LACP port number of the partner port. |
| `Key` | The LACP key assigned to the partner port by the partner system. |
| `State` | The LACP operational state of the partner port. The state is expressed as an eight character string. For example:<br>`ASAO----`<br>From left to right, each character in the string has the following meaning:<br>1. LACP Activity: A=Active LACP, P=Passive LACP<br>2. LACP Timeout: S=Short Timeout, L=Long Timeout<br>3. Aggregation: A=Aggregateable, I=Individual<br>4. Synchronization: S=In Sync, O=Out Of Sync<br>5. Collecting: C=Collecting, -=Not Collecting<br>6. Distributing: D=Distributing, -=Not Distributing<br>7. Defaulted: D=Defaulted Info, -=Received Info<br>8. Expired: E=Expired, -=Not Expired |
| `Version` | **Synopsis:** An integer between 0 and 255<br>The version number of LACP packets sent by the partner system. |

### 9.4.4.2 Configuring Global LACP Settings

To configure the global settings for the Link Aggregation Control Protocol (LACP), do the following:

1. Navigate to ***Link Aggregation » Configure Global LACP Parameters***. The **Global LACP Parameters** form appears.

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

| Parameter | Description |
|---|---|
| `Bridge LACP Priority` | **Synopsis:** An integer between 0 and 65535<br>**Default:** 32768<br>The LACP system priority. This is combined with the device's MAC address to form the LACP system ID, which is used in negotiations with other LACP-enabled devices. |
| `LAG Ports Selection Rule` | **Synopsis:** [ ActivePartner \| LinkSpeed \| LinkPriority ]<br>**Default:** ActivePartner<br>Defines the order in which ports in the Link Aggregation Group (LAG), or port trunk, are selected by LACP for aggregation. This parameter applies when ports in the LAG are connected to two or more other LAGs.<br>Options include:<br>• `ActivePartner` – Select ports based on when partner ports become active.<br>• `LinkSpeed` – Select ports based on link speed. The port with the higher link speed has precedence.<br>• `LinkPriority` – Select ports based on LACP link priority. The port with the higher LACP link priority has precedence. |

3. Click **Apply**.

### 9.4.4.3 Configuring LACP Per Port

To configure the Link Aggregation Control Protocol (LACP) settings for a specific port, do the following:

1. Navigate to ***Link Aggregation » Configure Port LACP Parameters***. The **Port LACP Parameters** table appears.
2. Select the desired port. The **Port LACP Parameters** form appears.
3. Configure the following parameter(s) as required:

| Parameter | Description |
|---|---|
| `Port` | **Synopsis:** 1/1 to maximum port number<br>The port number as seen on the front plate silkscreen of the device. |
| `Mode` | **Synopsis:** [ Active \| Passive ]<br>**Default:** Passive<br>Defines the LACP mode for the port. Options include::<br>• `Active` – The port actively sends LACP packets, regardless of the mode of the partner port.<br>• `Passive` – The port does not send LACP packets unless the partner port is in Active mode. |

| Parameter | Description |
|---|---|
| | **Note**<br>For each physical link in the Link Aggregation Group (LAG), or port trunk, one partner port must be in Active mode. |
| `Timeout` | **Synopsis:** [ Short \| Long ]<br>**Default:** Short<br>Defines the time in seconds (s) to wait for LACP packets from the partner port. If an LACP packet is not received within the required time frame, the partner port's information is invalidated. Options include:<br>Options include:<br>• `Short` – 3 s<br>• `Long` – 90 s<br>**Note**<br>The Timeout setting should be the same for all ports in a Link Aggregation Group (LAG), or port trunk. |
| `Individual` | **Synopsis:** [ False \| True ]<br>**Default:** False<br>Enables or disables Individual mode for the port. Ports in Individual mode can not be aggregated in a Link Aggregation Group (LAG), or port trunk. |
| `Priority` | **Synopsis:** An integer between 0 and 65535<br>**Default:** 32768<br>The LACP port priority. This is combined with the port number to form the LACP port identifier.<br>The port priority is considered when determining if the port should be in standby. |

4. Click **Apply**.

### 9.4.4.4 Viewing LACP Statistics

To view statistics collected on ports managed by the Link Aggregation Control Protocol (LACP), navigate to ***Link Aggregation » View Port LACP Statistics***. The **Port LACP Statistics** table appears.

This table displays the following information:

| Parameter | Description |
|---|---|
| `Port` | The port number as seen on the front plate silkscreen of the device. |
| `Link` | The link status of the port. |

| Parameter | Description |
|---|---|
| State | **Synopsis:** An integer between 0 and 255<br>The LACP operational state of the port. The state is expressed as an eight character string. For example:<br>ASAO----<br>From left to right, each character in the string has the following meaning:<br>1. LACP Activity: A=Active LACP, P=Passive LACP<br>2. LACP Timeout: S=Short Timeout, L=Long Timeout<br>3. Aggregation: A=Aggregateable, I=Individual<br>4. Synchronization: S=In Sync, O=Out Of Sync<br>5. Collecting: C=Collecting, -=Not Collecting<br>6. Distributing: D=Distributing, -=Not Distributing<br>7. Defaulted: D=Defaulted Info, -=Received Info<br>8. Expired: E=Expired, -=Not Expired |
| Tx | The number of LACP packets transmitted by the port. |
| Rx | The number of good LACP packets received by the port. |
| RxUnknown | The number of unknown LACP packets received by the port. |
| RxIllegal | The number of illegal LACP packets received by the port. |

## 9.4.5 Clearing Link Aggregation Statistics

To clear all link aggregation statistics from the device, do the following:

1. Navigate to ***Link Aggregation » Clear Link Aggregation Statistics***. The **Clear Link Aggregation Statistics** form appears.
2. Click **Confirm**.

# 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.<br>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)".

   The header of each received frame is first examined to determine if the frame is an IP packet and if **Inspect TOS** is enabled in RUGGEDCOM ROS. The CoS is determined from the DSCP field.

   If the frame is not an IP packet or if **Inspect TOS** is disabled, the frame is examined to determine if its destination or source MAC address is found in the Static MAC address table. If it is, the CoS configured for the static Mac address is used. If neither destination or source MAC address is in the Static MAC Address table, the frame is then examined for 802.1Q tags and the priority field is mapped to a CoS. If a tag is not present, the 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.

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

| Parameter | Description |
|---|---|
| `CoS Weighting` | **Synopsis:** [ 8:4:2:1 \| Strict ]<br>**Default:** 8:4:2:1<br>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.<br>Examples:<br>• `8:4:2:1` – 8 Critical, 4 High, 2 Medium and 1 Normal priority CoS frame<br>• `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 262)".

## 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.
2. Select an Ethernet port. The **Port CoS Parameters** form appears.
3. Configure the following parameter(s) as required:

| Parameter | Description |
|---|---|
| `Port(s)` | **Synopsis:** Any combination of numbers valid for this parameter<br>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<br>**Default:** 0<br>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 ]<br>**Default:** No<br>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 |

| Parameter | Description |
|---|---|
| | 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.
2. Select a priority level. The **Priority to CoS Mapping** form appears.
3. Configure the following parameter(s) as required:

| Parameter | Description |
|---|---|
| `Priority` | **Synopsis:** An integer between 0 and 7<br>**Default:** 0<br>Value of the IEEE 802.1p priority. |
| `CoS` | **Synopsis:** [ Normal \| Medium \| High \| Crit ]<br>**Default:** Normal<br>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.
2. Select a DSCP level. The **DSCP to CoS Mapping** form appears.

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

| Parameter | Description |
|---|---|
| `DSCP` | **Synopsis:** An integer between 0 and 63<br>**Default:** 0<br>Differentiated Services Code Point (DSCP) – a value of the 6 bit DiffServ field in the Type-Of-Service (TOS) field of the IP header. |
| `Priority` | **Synopsis:** An integer between 0 and 7<br>**Default:** 0<br>Priority 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.
2. Configure the following parameter(s) as required:

| Parameter | Description |
|---|---|
| `Time` | **Synopsis:** HH:MM:SS<br>This parameter allows for both the viewing and setting of the local time. |
| `Date` | **Synopsis:** MMM DD, YYYY<br>This parameter allows for both the viewing and setting of the local date. |
| `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) \| UTC+2:00 (Athens, Cairo, Helsinki) \| ... ]<br>**Default:** UTC-5:00 (New York, Toronto)<br>This setting allows for the conversion of UTC (Universal Coordinated Time) to local time. |
| `DST Offset` | **Synopsis:** HH:MM:SS<br>**Default:** 00:00:00<br>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<br>This parameter specifies a rule for time and date when the transition between Standard and Daylight Saving Time occurs. |

| Parameter | Description |
|---|---|
| | • `mm` – Month of the year (01 = January, 12 = December)<br>• `n` – nth d-day in the month (1 = 1st d-day, 5 = 5th/last d-day)<br>• `d` – day of the week (0 = Sunday, 6 = Saturday)<br>• `HH` – hour of the day (0 - 24)<br>• `MM` – minute of the hour (0- 59)<br>• `SS` – second of the minute (0 - 59)<br>Example: The following rule applies in most part of USA and Canada:<br>`03.2.0/02:00:00 11.1.0/02:00:00`<br>DST begins on March's 2nd Sunday at 2:00am.<br>DST ends on November's 1st Sunday at 2:00am. |
| `Current UTC Offset` | **Synopsis:** An integer between 0 and 1000<br>**Default:** 36<br>Coordinated Universal Time (UTC) is a time standard based on International Atomic Time (TAI) with leap seconds added at irregular intervals to compensate for the Earth's slowing rotation. Current UTC offset parameter allows user to adjust the difference between UTC and TAI. The International Earth Rotation and Reference System Service (IERS) observes the Earth's rotation and nearly six months in advance (January and July) a Bulletin-C message is sent out, which reports whether or not to add a leap second in the end of June and December.<br>Please note that change in current UTC offset parameter will result in temporally disruption in the timing network. |
| `Leap Second Pending` | **Synopsis:** [ No \| Yes ]<br>**Default:** No<br>This parameter allows user to manage the leap second event. A leap second is a second added to Coordinated Universal Time (UTC) in order to keep it synchronized with astronomical time. The International Earth Rotation and Reference System Service (IERS) observes the Earth's rotation and nearly six months in advance (January and July) a Bulletin-C message is sent out, which reports whether or not to add a leap second in the end of June and December. This parameter must set at least 5 minutes in advance before the occurrence of leap second event. |

## 11.2 Managing the Precision Time Protocol (PTP)

The Precision Time Protocol (PTP) is a standard method of synchronizing network clocks over Ethernet. RUGGEDCOM ROS supports PTP v2, which is defined by the IEEE 1588 working group in the IEEE 1588-2008 standard.

PTP is a distributed protocol that allows multiple clocks in a network to synchronize with one another. These clocks are organized into a master-slave synchronization hierarchy with a *grandmaster* clock at the top of the hierarchy, which determines the

reference time for the entire system. Synchronization is achieved via the exchange of PTP timing messages. *Slave* clocks use the timing information in PTP messages to adjust their time to that of the *master* in their part of the hierarchy.

The PTP protocol executes within a logical scope called a *domain*. The time established via the protocol within one domain is independent of the time in other domains.

A PTP v2 system may consist of a combination of both PTP-aware and PTP-unaware devices. There are five basic PTP device types defined in the IEEE 1588-2008 standard:

- Ordinary Clocks
- Boundary Clocks
- End-to-End Transparent Clocks
- Peer-to-Peer Transparent Clocks
- Management Nodes

RUGGEDCOM ROS supports *Peer-to-Peer Transparent Clock* and *End-to-End Transparent Clock* modes:

- A *Peer-to-Peer Transparent Clock* forwards all messages just as a normal bridge, router, or repeater does. The difference is that a Peer-to-Peer Transparent Clock also computes the residence time (message departure time - message arrival time) and link delay (packet propagation delay between peer ports) and adds this information in PTP event messages (which carry timestamps). Ethernet ports on a Peer-to-Peer Transparent Clock use the peer delay mechanism to compute the packet propagation delay between peer ports.
- The *End-to-End Transparent Clock* supports the use of the end-to-end delay measurement mechanism between slave clocks and the master clock. It forwards all messages just as a normal bridge, router or repeater does. The difference is that an End-to-End Transparent Clock computes the residence time (message departure time - message arrival time) and adds this information to PTP event messages (messages that carry a time-stamp).

## 11.2.1 Configuring PTP Globally

To configure the global settings for PTP, do the following:

1. Navigate to ***Administration » System Time Manager » Precision Time Protocol » Configure Global Parameters***. The **Global Parameters** form appears.

| **NOTICE** |
| --- |
| Before performing SNMP get or SNMP set operations for MIBs IEEE C37.238-2011 and RUGGEDCOM-PTP1588-MIB.mib, make sure the PTP Enable parameter is set to *Yes*. For more information about supported MIBs, refer to "SNMP Management Interface Base (MIB) Support (Page 281)". |

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

| Parameter | Description |
|---|---|
| `PTP Enable` | **Synopsis:** [ No \| Yes ]<br>**Default:** No<br>Enables PTP (Precision Time Protocol) protocol. |
| `Clock Type` | **Synopsis:** [ P2P TClock \| E2E TClock ]<br>**Default:** P2P TClock<br>Selects the PTP (Precision Time Protocol) clock type. |
| `PTP Profile` | **Synopsis:** [ Power Profile \| Default P2P Profile \| Utility Profile Level 1 \| Default E2E Profile \| Custom Profile \| Power Profile v2 ]<br>**Default:** Power Profile<br>Selects the PTP (Precision Time Protocol) clock profile. PTP profile represents a set of allowed PTP features applicable to specific industry.<br>**Note**<br>`Power Profile` represents C37.238.2011.<br>**Note**<br>`Power Profile v2` represents C37.238.2017.<br>**Note**<br>`Utility Profile Level 1` represents IEC/IEEE 61850-9-3 Ed.1. |
| `Ethernet Ports` | **Synopsis:** Comma-separated list of ports or [ All ]<br>**Default:** All<br>Selects Ethernet port(s) which take part in PTP (Precision Time Protocol) message exchanges. |
| `VLAN ID` | **Synopsis:** An integer between 1 and 4094 or [ Disable ]<br>**Default:** 1<br>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. Frames tagged with a zero VLAN ID will always be associated with the VLAN ID 1 unless this parameter is configured. |
| `Class Of Service` | **Synopsis:** An integer between 1 and 7 or [ Disable ]<br>**Default:** 4<br>Selects the PTP (Precision Time Protocol) message priority based on the IEEE 802.1p specification. IEEE 802.1p defines eight different classes of service, usually expressed using the 3-bit priority field in an IEEE 802.1Q header added to the Ethernet frame. If the VLAN option is enabled and the Class Of Service option is set to 'Disable' then it represents priority '0' in terms of the IEEE 802.1p specification. |

| Parameter | Description |
|---|---|
| `Transport Protocol` | **Synopsis:** [ Layer 2 Multicast \| Layer 3 Multicast ]<br>**Default:** Layer 2 Multicast<br>Selects network transport protocol for PTP (Precision Time Protocol) messages. |
| `Grandmaster ID` | **Synopsis:** An integer between 3 and 255<br>**Default:** 255<br>This parameter is specific to the Power Profile (IEEE C37.238-2011) or Power Profile v2 (IEEE C37.238-2017), as selected. All PTP master capable devices must configure a network-wide, unique instance of this parameter in the range of 3 to 254 for proper operation. |

3. Click **Apply**.
4. Reset the device. For more information, refer to "Resetting the Device (Page 97)".

## 11.2.2 Configuring a Transparent Clock

To configure settings for a PTP transparent clock, do the following:

1. Navigate to ***Administration » System Time Manager » Precision Time Protocol » Configure Clock Parameters***. The **Clock Parameters** form appears.
2. Configure the following parameter(s) as required:

| Parameter | Description |
|---|---|
| `Domain Number` | **Synopsis:** An integer between 0 and 127<br>**Default:** 0<br>Selects the PTP (Precision Time Protocol) domain number. A PTP domain is a logical grouping of PTP clocks that synchronize to each other using the PTP protocol. |
| `Path Delay Mechanism` | **Synopsis:** [ Disabled \| Peer-to-Peer \| End-to-End ]<br>**Default:** Peer-to-Peer<br>Selects the PTP (Precision Time Protocol) delay mechanism. There are two mechanisms used in PTP to measure the propagation delay between PTP ports: The P2P (Peer-to-Peer) delay mechanism measures the port to port propagation time such as link delay and frame residence time. The P2P mechanism is independent of whether the PTP port is acting as Master or Slave.<br>The E2E (End-to-End) delay mechanism measures the message propagation time between Master and Slave clocks across the whole intervening network.<br>Note that the P2P mechanism does not inter-operate with path delay measurements based on the E2E (also called request-response) delay mechanism. |

3. Click **Apply**.

4. Reset the device. For more information, refer to "Resetting the Device (Page 97)".

### 11.2.3 Configuring the PTP Delay Request Interval

To configure the PTP delay request interval, do the following:

1. Navigate to ***Administration » System Time Manager » Precision Time Protocol » Configure Path Delay***. The **Path Delay** form appears.
2. Configure the following parameter(s) as required:

| Parameter | Description |
|---|---|
| `P2P Request Interval` | **Synopsis:** [ 1 s \| 2 s \| 4 s \| 8 s \| 16 s \| 32 s ]<br>**Default:** 1 s<br>Selects PTP delay request interval (mean time interval between successive delay request messages) in seconds. The peer delay mechanism measures the port-to-port propagation time, such as the link delay, between two communicating ports supporting the peer delay mechanism. |
| `E2E Request Interval` | **Synopsis:** [ 1 s \| 2 s \| 4 s \| 8 s \| 16 s \| 32 s ]<br>**Default:** 1<br>Selects PTP delay request interval (mean time interval between successive delay request messages) in seconds. The E2E (also called request-response) delay mechanism measures the message propagation time between master and slave clocks. |

3. Click **Apply**.
4. Reset the device. For more information, refer to "Resetting the Device (Page 97)".

### 11.2.4 Configuring a VLAN for PTP Traffic

To configure a VLAN specifically for PTP traffic, do the following:

1. Assign a VLAN ID to all PTP traffic. For more information, refer to "Configuring PTP Globally (Page 267)".
2. Add a static VLAN with the same ID. For more information about configuring a static VLAN, refer to "Adding a Static VLAN (Page 149)".
3. For each Ethernet port that will transport PTP traffic, configure the PVID to match the VLAN ID configured in Step 1. For more information, refer to "Configuring VLANs for Specific Ethernet Ports (Page 147)".
4. Configure the PVID format for each affected Ethernet port to control whether PTP traffic is transported as tagged or untagged frames. Or, if necessary, configure the port to be a VLAN trunk. For more information, refer to "Configuring VLANs for Specific Ethernet Ports (Page 147)".

### 11.2.5 Viewing PTP Clock Statistics

To view statistics for the Precision Time Protocol (PTP) clock, navigate to ***Administration » System Time Manager » Precision Time Protocol » View PTP Statistics » View PTP Clock Stats***. The **PTP Clock Stats** form appears.

This form displays the following information:

**Note**
Parameters are available dependent on the status of the device.

| Parameter | Description |
|---|---|
| `Status` | **Synopsis:** A string 31 characters long<br>Shows the status of PTP (Precision Time Protocol) node, if device is configured as an ordinary clock then this field will show the status of the PTP state such as MASTER, SLAVE, LISTENING. If the device is configured as a Transparent Clock then this field simply reflects configuration setting. |

### 11.2.6 Viewing Peer Delay Statistics

To view statistics for the Precision Time Protocol (PTP) peer delay, do the following:

1. Navigate to ***Administration » System Time Manager » Precision Time Protocol » View PTP Statistics » View Peer Delay Stats***. The **PTP Delay Stats** table appears.
2. Select an Ethernet port. The **PTP Delay Stats** form appears.

This table displays the following information:

| Parameter | Description |
|---|---|
| `Port` | **Synopsis:** 1/1 to maximum port number<br>The port number as seen on the front plate silkscreen of the device. |
| `State` | **Synopsis:** [ On \| Off ]<br>Shows the status of PTP port with respect to P2P (Peer To Peer) delay mechanism. |
| `PeerDelay` | **Synopsis:** An integer between 0 and 2147483647<br>Shows peer delay in nanoseconds. The peer delay mechanism measures the port-to-port propagation time, such as the link delay, between two communicating ports supporting the peer delay mechanism. |

## 11.3 Configuring the Time Source

To configure a reference time source to be used by the device for the local clock and for all served time synchronization outputs, do the following:

1. Navigate to ***Administration » System Time Manager » Configure Time Source***. The **Time Source** form appears.
2. Configure the following parameter(s) as required:

| Parameter | Description |
|---|---|
| `Primary Time Source` | **Synopsis:** [ LOCAL CLK \| IEEE1588 \| NTP Server ]<br>**Default:** LOCAL CLK<br>To select time source that will discipline the local clock. Note that changing the time source may produce a step change in the time seen via any of the clock outputs. |

3. Click **Apply**.

## 11.4 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.

### 11.4.1 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.
2. Select **Enabled** to enable SNTP, or select **Disabled** to disable SNTP.
3. Click **Apply**.

### 11.4.2 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.
2. Select either **Primary** or **Backup**. The **NTP Servers** form appears.
3. Configure the following parameter(s) as required:

| Parameter | Description |
|---|---|
| `Server` | **Synopsis:** A string 8 characters long<br>**Default:** Primary<br>This field tells whether this configuration is for a Primary or a Backup Server. |
| `IP Address` | **Synopsis:** Any valid IP address<br>The Server IP Address. |
| `Reachable` | **Synopsis:** [ No \| Yes ]<br>The status of the server. |
| `Update Period` | **Synopsis:** An integer between 1 and 1440<br>**Default:** 60<br>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**.

## 11.5 Viewing the Status of Time Synchronization Subsystems

To view the current status of each time synchronization subsystem, navigate to ***Administration » System Time Manager » View Time Sync Status***. The **Time Sync Status** form appears. This form varies based on the time source configured.

This table displays the following information:

| Parameter | Description |
|---|---|
| `Time Source` | **Synopsis:** [ LOCAL CLK \| IRIGB \| IEEE1588 \| NTP Server \| GPS ]<br>A time source that is driving the local clock. |
| `Frequency Adjustment` | **Synopsis:** An integer between -2147483647 and 2147483646<br>Shows the current amount of discipline applied to the local frequency reference (TCXO); i.e. the amount of correction on this system required to synchronize to the current reference. |

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

| Parameter | Description |
|---|---|
| `State` | **Synopsis:** [ Disabled \| Enabled ]<br>**Default:** Enabled<br>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<br>**Default:** 30<br>The interval at which LLDP frames are transmitted on behalf of this LLDP agent. |
| `Tx Hold` | **Synopsis:** An integer between 2 and 10<br>**Default:** 4<br>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:<br>`TTL = MIN(65535, (Tx Interval * Tx Hold)` |
| `Reinit Delay` | **Synopsis:** An integer between 1 and 10<br>**Default:** 2<br>The delay in seconds from when the value of Admin Status parameter of a particular port becomes 'Disbled' until re-initialization will be lattempted. |

| Parameter | Description |
|---|---|
| `Tx Delay` | **Synopsis:** An integer between 1 and 8192<br>**Default:** 2<br>The delay in seconds between successive LLDP frame transmissions initiated by value or status changed. The recommended value is set by the following formula:<br>`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.
2. Select a port. The **Port LLDP Parameters** form appears.
3. Configure the following parameter(s) as required:

| Parameter | Description |
|---|---|
| `Port` | **Synopsis:** 1/1 to maximum port number<br>**Default:** 1/1<br>The port number as seen on the front plate silkscreen of the device. |
| `Admin Status` | **Synopsis:** [ rxTx \| txOnly \| rxOnly \| Disabled ]<br>**Default:** rxTx<br>rxTx: the local LLDP agent can both transmit and receive LLDP frames through the port.<br>txOnly: the local LLDP agent can only transmit LLDP frames.<br>rxOnly: the local LLDP agent can only receive LLDP frames.<br>disabled: the local LLDP agent can neither transmit or receive LLDP frames. |
| `Notifications` | **Synopsis:** [ Disabled \| Enabled ]<br>**Default:** Disabled<br>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.

This form displays the following information:

| Parameter | Description |
|---|---|
| `Inserts` | **Synopsis:** An integer between 0 and 4294967295<br>A number of times the entry in LLDP Neighbor Information Table was inserted. |
| `Deletes` | **Synopsis:** An integer between 0 and 4294967295<br>A number of times the entry in LLDP Neighbor Information Table was deleted. |
| `Drops` | **Synopsis:** An integer between 0 and 4294967295<br>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<br>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.

This form displays the following information:

| Parameter | Description |
|---|---|
| `Port` | **Synopsis:** 1/1 to maximum port number<br>The local port associated with this entry. |
| `ChassisId` | **Synopsis:** A string 45 characters long<br>Chassis Id information received from remote LLDP agent. |
| `PortId` | **Synopsis:** A string 45 characters long<br>Port Id information received from remote LLDP agent. |
| `SysName` | **Synopsis:** A string 45 characters long<br>System Name information received from remote LLDP agent. |
| `SysDesc` | **Synopsis:** A string 45 characters long<br>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.

This table displays the following information:

| Parameter | Description |
|---|---|
| `Port` | **Synopsis:** 1/1 to maximum port number<br>The port number as seen on the front plate silkscreen of the device. |
| `FrmDrop` | **Synopsis:** An integer between 0 and 4294967295<br>A counter of all LLDP frames discarded. |
| `ErrFrm` | **Synopsis:** An integer between 0 and 4294967295<br>A counter of all LLDPDUs received with detectable errors. |
| `FrmIn` | **Synopsis:** An integer between 0 and 4294967295<br>A counter of all LLDPDUs received. |
| `FrmOut` | **Synopsis:** An integer between 0 and 4294967295<br>A counter of all LLDPDUs transmitted. |
| `Ageouts` | **Synopsis:** An integer between 0 and 4294967295<br>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<br>A counter of all TLVs discarded. |
| `TLVsUnknown` | **Synopsis:** An integer between 0 and 4294967295<br>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 |
| 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 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 |

| Standard | MIB Name | Title |
|---|---|---|
| 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 |
| IEEE C37.238-2011 | IEEEC37.238-MIB | IEEE Standard Profile for use of IEEE 1588 Precision Time Protocol in power system applications |
| 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-STP-MIB.mib | RUGGEDCOM-STP-MIB | Management for RSTP protocol |
| RUGGEDCOM-GPS-MIB.mib | RUGGEDCOM-GPS-MIB | RUGGEDCOM proprietary MIB to control and monitor GPS module |
| RUGGEDCOM-IRIGB-MIB.mib | RUGGEDCOM-IRIGB-MIB | RUGGEDCOM proprietary MIB to control and monitor IRIG-B module |
| RUGGEDCOM-NTP-MIB.mib | RUGGEDCOM-NTP-MIB | RUGGEDCOM proprietary MIB to control and monitor NTP module |
| RUGGEDCOM-PTP1588-MIB.mib | RUGGEDCOM-PTP1588-MIB | RUGGEDCOM proprietary MIB to control and monitor PTP1588 module |
| RUGGEDCOM-TIMECONFIG-MIB.mib | RUGGEDCOM-TIMECONFIG-MIB | RUGGEDCOM proprietary MIB to control and monitor TIMECONFIG 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_RSTP-MIB-AC.mib | RC_RSTP-MIB-AC | RSTP-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 |
| RC-GPS-MIB-AC.mib | RC-GPS-MIB-AC | GPS-MIB |
| RC-IRIGB-MIB-AC.mib | RC-IRIGB-MIB-AC | IRIGB-MIB |
| RC-NTP-MIB-AC.mib | RC-NTP-MIB-AC | NTP-MIB |
| RC-PTP1588-MIB-AC.mib | RC-PTP1588-MIB-AC | PTP1588-MIB |
| RC-TIMECONFIG-MIB-AC.mib | RC-TIMECONFIG-MIB-AC | TIMECONFIG-MIB |

## 12.3.2 SNMP Traps

The device generates the following traps.

### Standard Traps

| Trap | MIB |
|---|---|
| linkDown | IF-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 | |
| rcChgPswdAdminTrap | |
| rcChgPswdOperTrap | |
| rcChgPswdGuestTrap | |
| rcChgPswdRadiusTrap | |
| rcChgPswdTacplusTrap | |
| rcChgPswdDataStoreTrap | |
| rcChgPswdSnmpCommunityTrap | |
| rcChgPswdSnmpAuthKeyTrap | |
| rcChgPswdSnmpPrivKeyTrap | |
| rcGpsStatusChange | RUGGEDCOM-GPS-MIB.mib |
| rcIrigbStatusChange | RUGGEDCOM-IRIGB-MIB.mib |

| Trap | MIB |
|---|---|
| rcNTPServiceAvailableChange | RUGGEDCOM-NTP-MIB.mib |

### 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 23)".

| Trap | Severity |
|---|---|
| TACACS+ response invalid | Warning |
| Unable to obtain IP address | Critical |
| SPP is rejected on Port 1 | 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.

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 23)".

To add a new SNMP user, do the following:

1. Navigate to ***Administration » Configure SNMP » Configure SNMP Users***. The **SNMP Users Table** appears.
2. Click **InsertRecord**. The **SNMP Users** form appears.

**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 100)".

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

| Parameter | Description |
|---|---|
| `Name` | **Synopsis:** A string 32 characters long<br>**Default:** initial<br>The name of the user. This user name also represents the security name that maps this user to the security group. |
| `IP Address` | **Synopsis:** Any valid IP address<br>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<br>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. |

| Parameter | Description |
|---|---|
| `Auth Protocol` | **Synopsis:** [ noAuth \| HMACMD5 \| HMACSHA ]<br>**Default:** noAuth<br>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 ]<br>**Default:** noPriv<br>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<br>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. |
| `Confirm Auth Key` | **Synopsis:** A string 31 characters long<br>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<br>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<br>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 23)".

To delete an SNMP user, do the following:

1. Navigate to ***Administration » Configure SNMP » Configure SNMP Users***. The **SNMP Users Table** appears.
2. Select the user from the table. The **SNMP Users** form appears.
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.

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 288)".

### 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 23)".

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.
2. Click **InsertRecord**. The **SNMP Security to Group Maps** form appears.
3. Configure the following parameter(s) as required:

| Parameter | Description |
|---|---|
| `SecurityModel` | **Synopsis:** [ snmpV1 \| snmpV2c \| snmpV3 ]<br>**Default:** snmpV3<br>The Security Model that provides the name referenced in this table. |
| `Name` | **Synopsis:** A string 32 characters long<br>The user name which is mapped by this entry to the specified group name. |
| `Group` | **Synopsis:** A string 32 characters long<br>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 23)".

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.

2. Select the map from the table. The **SNMP Security to Group Maps** form appears.
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.

If SNMP groups have not been configured, add groups as needed. For more information, refer to "Adding an SNMP Group (Page 289)".

### 12.3.5.2 Adding an SNMP Group

For CLI commands related to adding an SNMP group, refer to "Available CLI Commands (Page 23)".

To add an SNMP group, do the following:

1. Navigate to ***Administration » Configure SNMP » Configure SNMP Access***. The **SNMP Access Table** appears.
2. Click **InsertRecord**. The **SNMP Access** form appears.
3. Configure the following parameter(s) as required:

| Parameter | Description |
|---|---|
| `Group` | **Synopsis:** A string 32 characters long<br>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 ]<br>**Default:** snmpV3<br>In order to gain the access rights allowed by this entry, configured security model must be in use. |
| `SecurityLevel` | **Synopsis:** [ noAuthNoPriv \| authNoPriv \| authPriv ]<br>**Default:** noAuthNoPriv<br>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. |

| Parameter | Description |
|---|---|
| ReadViewName | **Synopsis:** [ noView \| V1Mib \| allOfMib ]<br>**Default:** noView<br>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. |
| WriteViewName | **Synopsis:** [ noView \| V1Mib \| allOfMib ]<br>**Default:** noView<br>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 ]<br>**Default:** noView<br>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 23)".

To delete an SNMP group, do the following:

1. Navigate to ***Administration » Configure SNMP » Configure SNMP Access***. The **SNMP Access Table** appears.
2. Select the group from the table. The **SNMP Access** form appears.
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)<br>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 |
| 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 |

### 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 s0/p1 Statistics - Ethernet In Packets | R | Uinst32 |
| 0402 | 2 | Port s0/p2 Statistics - Ethernet In Packets | R | Uinst32 |
| 0404 | 2 | Port s0/p3 Statistics - Ethernet In Packets | R | Uinst32 |
| 0406 | 2 | Port s0/p4 Statistics - Ethernet In Packets | R | Uinst32 |
| 0408 | 2 | Port s1/p1 Statistics - Ethernet In Packets | R | Uinst32 |
| 040A | 2 | Port s1/p2 Statistics - Ethernet In Packets | R | Uinst32 |
| 040C | 2 | Port s1/p3 Statistics - Ethernet In Packets | R | Uinst32 |
| 040E | 2 | Port s1/p4 Statistics - Ethernet In Packets | R | Uinst32 |
| 0410 | 2 | Port s2/p1 Statistics - Ethernet In Packets | R | Uinst32 |
| 0412 | 2 | Port s2/p2 Statistics - Ethernet In Packets | R | Uinst32 |
| 0414 | 2 | Port s2/p3 Statistics - Ethernet In Packets | R | Uinst32 |
| 0416 | 2 | Port s2/p4 Statistics - Ethernet In Packets | R | Uinst32 |
| 0418 | 2 | Port s3/p1 Statistics - Ethernet In Packets | R | Uinst32 |
| 041A | 2 | Port s3/p2 Statistics - Ethernet In Packets | R | Uinst32 |
| 041C | 2 | Port s3/p3 Statistics - Ethernet In Packets | R | Uinst32 |
| 041E | 2 | Port s3/p4 Statistics - Ethernet In Packets | R | Uinst32 |
| 0420 | 2 | Port s4/p1 Statistics - Ethernet In Packets | R | Uinst32 |
| 0422 | 2 | Port s4/p2 Statistics - Ethernet In Packets | R | Uinst32 |
| 0424 | 2 | Port s4/p3 Statistics - Ethernet In Packets | R | Uinst32 |
| 0426 | 2 | Port s4/p4 Statistics - Ethernet In Packets | R | Uinst32 |
| 0428 | 2 | Port s5/p1 Statistics - Ethernet In Packets | R | Uinst32 |
| 042A | 2 | Port s5/p2 Statistics - Ethernet In Packets | R | Uinst32 |

| Address | #Registers | Description (Reference Table in UI) | R/W | Format |
|---|---|---|---|---|
| 042C | 2 | Port s5/p3 Statistics - Ethernet In Packets | R | Uinst32 |
| 042E | 2 | Port s5/p4 Statistics - Ethernet In Packets | R | Uinst32 |
| 0430 | 2 | Port s6/p1 Statistics - Ethernet In Packets | R | Uinst32 |
| 0432 | 2 | Port s6/p2 Statistics - Ethernet In Packets | R | Uinst32 |
| 0434 | 2 | Port s6/p3 Statistics - Ethernet In Packets | R | Uinst32 |
| 0436 | 2 | Port s6/p4 Statistics - Ethernet In Packets | R | Uinst32 |
| 0440 | 2 | Port s0/p1 Statistics - Ethernet Out Packets | R | Uinst32 |
| 0442 | 2 | Port s0/p2 Statistics - Ethernet Out Packets | R | Uinst32 |
| 0444 | 2 | Port s0/p3 Statistics - Ethernet Out Packets | R | Uinst32 |
| 0446 | 2 | Port s0/p4 Statistics - Ethernet Out Packets | R | Uinst32 |
| 0448 | 2 | Port s1/p1 Statistics - Ethernet Out Packets | R | Uinst32 |
| 044A | 2 | Port s1/p2 Statistics - Ethernet Out Packets | R | Uinst32 |
| 044C | 2 | Port s1/p3 Statistics - Ethernet Out Packets | R | Uinst32 |
| 044E | 2 | Port s1/p4 Statistics - Ethernet Out Packets | R | Uinst32 |
| 0450 | 2 | Port s2/p1 Statistics - Ethernet Out Packets | R | Uinst32 |
| 0452 | 2 | Port s2/p2 Statistics - Ethernet Out Packets | R | Uinst32 |
| 0454 | 2 | Port s2/p3 Statistics - Ethernet Out Packets | R | Uinst32 |
| 0456 | 2 | Port s2/p4 Statistics - Ethernet Out Packets | R | Uinst32 |
| 0458 | 2 | Port s3/p1 Statistics - Ethernet Out Packets | R | Uinst32 |
| 045A | 2 | Port s3/p2 Statistics - Ethernet Out Packets | R | Uinst32 |
| 045C | 2 | Port s3/p3 Statistics - Ethernet Out Packets | R | Uinst32 |
| 045E | 2 | Port s3/p4 Statistics - Ethernet Out Packets | R | Uinst32 |
| 0460 | 2 | Port s4/p1 Statistics - Ethernet Out Packets | R | Uinst32 |
| 0462 | 2 | Port s4/p2 Statistics - Ethernet Out Packets | R | Uinst32 |

| Address | #Registers | Description (Reference Table in UI) | R/W | Format |
|---|---|---|---|---|
| 0464 | 2 | Port s4/p3 Statistics - Ethernet Out Packets | R | Uinst32 |
| 0466 | 2 | Port s4/p4 Statistics - Ethernet Out Packets | R | Uinst32 |
| 0468 | 2 | Port s5/p1 Statistics - Ethernet Out Packets | R | Uinst32 |
| 046A | 2 | Port s5/p2 Statistics - Ethernet Out Packets | R | Uinst32 |
| 046C | 2 | Port s5/p3 Statistics - Ethernet Out Packets | R | Uinst32 |
| 046E | 2 | Port s5/p4 Statistics - Ethernet Out Packets | R | Uinst32 |
| 0470 | 2 | Port s6/p1 Statistics - Ethernet Out Packets | R | Uinst32 |
| 0472 | 2 | Port s6/p2 Statistics - Ethernet Out Packets | R | Uinst32 |
| 0474 | 2 | Port s6/p3 Statistics - Ethernet Out Packets | R | Uinst32 |
| 0476 | 2 | Port s6/p4 Statistics - Ethernet Out Packets | R | Uinst32 |
| 0480 | 2 | Port s0/p1 Statistics - Ethernet In Packets | R | Uinst32 |
| 0482 | 2 | Port s0/p2 Statistics - Ethernet In Packets | R | Uinst32 |
| 0484 | 2 | Port s0/p3 Statistics - Ethernet In Packets | R | Uinst32 |
| 0486 | 2 | Port s0/p4 Statistics - Ethernet In Packets | R | Uinst32 |
| 0488 | 2 | Port s1/p1 Statistics - Ethernet In Packets | R | Uinst32 |
| 048A | 2 | Port s1/p2 Statistics - Ethernet In Packets | R | Uinst32 |
| 048C | 2 | Port s1/p3 Statistics - Ethernet In Packets | R | Uinst32 |
| 048E | 2 | Port s1/p4 Statistics - Ethernet In Packets | R | Uinst32 |
| 0490 | 2 | Port s2/p1 Statistics - Ethernet In Packets | R | Uinst32 |
| 0492 | 2 | Port s2/p2 Statistics - Ethernet In Packets | R | Uinst32 |
| 0494 | 2 | Port s2/p3 Statistics - Ethernet In Packets | R | Uinst32 |
| 0496 | 2 | Port s2/p4 Statistics - Ethernet In Packets | R | Uinst32 |
| 0498 | 2 | Port s3/p1 Statistics - Ethernet In Packets | R | Uinst32 |
| 049A | 2 | Port s3/p2 Statistics - Ethernet In Packets | R | Uinst32 |

| Address | #Registers | Description (Reference Table in UI) | R/W | Format |
|---|---|---|---|---|
| 049C | 2 | Port s3/p3 Statistics - Ethernet In Packets | R | Uinst32 |
| 049E | 2 | Port s3/p4 Statistics - Ethernet In Packets | R | Uinst32 |
| 04A0 | 2 | Port s4/p1 Statistics - Ethernet In Packets | R | Uinst32 |
| 04A2 | 2 | Port s4/p2 Statistics - Ethernet In Packets | R | Uinst32 |
| 04A4 | 2 | Port s4/p3 Statistics - Ethernet In Packets | R | Uinst32 |
| 04A6 | 2 | Port s4/p4 Statistics - Ethernet In Packets | R | Uinst32 |
| 04A8 | 2 | Port s5/p1 Statistics - Ethernet In Packets | R | Uinst32 |
| 04AA | 2 | Port s5/p2 Statistics - Ethernet In Packets | R | Uinst32 |
| 04AC | 2 | Port s5/p3 Statistics - Ethernet In Packets | R | Uinst32 |
| 04AE | 2 | Port s5/p4 Statistics - Ethernet In Packets | R | Uinst32 |
| 04B0 | 2 | Port s6/p1 Statistics - Ethernet In Packets | R | Uinst32 |
| 04B2 | 2 | Port s6/p2 Statistics - Ethernet In Packets | R | Uinst32 |
| 04B4 | 2 | Port s6/p3 Statistics - Ethernet In Packets | R | Uinst32 |
| 04B6 | 2 | Port s6/p4 Statistics - Ethernet In Packets | R | Uinst32 |
| 04C0 | 2 | Port s0/p1 Statistics - Ethernet Out Packets | R | Uinst32 |
| 04C2 | 2 | Port s0/p2 Statistics - Ethernet Out Packets | R | Uinst32 |
| 04C4 | 2 | Port s0/p3 Statistics - Ethernet Out Packets | R | Uinst32 |
| 04C6 | 2 | Port s0/p4 Statistics - Ethernet Out Packets | R | Uinst32 |
| 04C8 | 2 | Port s1/p1 Statistics - Ethernet Out Packets | R | Uinst32 |
| 04CA | 2 | Port s1/p2 Statistics - Ethernet Out Packets | R | Uinst32 |
| 04CC | 2 | Port s1/p3 Statistics - Ethernet Out Packets | R | Uinst32 |
| 04CE | 2 | Port s1/p4 Statistics - Ethernet Out Packets | R | Uinst32 |
| 04D0 | 2 | Port s2/p1 Statistics - Ethernet Out Packets | R | Uinst32 |
| 04D2 | 2 | Port s2/p2 Statistics - Ethernet Out Packets | R | Uinst32 |

| Address | #Registers | Description (Reference Table in UI) | R/W | Format |
|---|---|---|---|---|
| 04D4 | 2 | Port s2/p3 Statistics - Ethernet Out Packets | R | Uinst32 |
| 04D6 | 2 | Port s2/p4 Statistics - Ethernet Out Packets | R | Uinst32 |
| 04D8 | 2 | Port s3/p1 Statistics - Ethernet Out Packets | R | Uinst32 |
| 04DA | 2 | Port s3/p2 Statistics - Ethernet Out Packets | R | Uinst32 |
| 04DC | 2 | Port s3/p3 Statistics - Ethernet Out Packets | R | Uinst32 |
| 04DE | 2 | Port s3/p4 Statistics - Ethernet Out Packets | R | Uinst32 |
| 04E0 | 2 | Port s4/p1 Statistics - Ethernet Out Packets | R | Uinst32 |
| 04E2 | 2 | Port s4/p2 Statistics - Ethernet Out Packets | R | Uinst32 |
| 04E4 | 2 | Port s4/p3 Statistics - Ethernet Out Packets | R | Uinst32 |
| 04E6 | 2 | Port s4/p4 Statistics - Ethernet Out Packets | R | Uinst32 |
| 04E8 | 2 | Port s5/p1 Statistics - Ethernet Out Packets | R | Uinst32 |
| 04EA | 2 | Port s5/p2 Statistics - Ethernet Out Packets | R | Uinst32 |
| 04EC | 2 | Port s5/p3 Statistics - Ethernet Out Packets | R | Uinst32 |
| 04EE | 2 | Port s5/p4 Statistics - Ethernet Out Packets | R | Uinst32 |
| 04F0 | 2 | Port s6/p1 Statistics - Ethernet Out Packets | R | Uinst32 |
| 04F2 | 2 | Port s6/p2 Statistics - Ethernet Out Packets | R | Uinst32 |
| 04F4 | 2 | Port s6/p3 Statistics - Ethernet Out Packets | R | Uinst32 |
| 04F6 | 2 | Port s6/p4 Statistics - Ethernet Out Packets | R | Uinst32 |

## 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 IP Address Assignment

This chapter describes features related to the assignment of IP addresses.

## 13.1 Managing DHCP

Dynamic Host Configuration Protocol (DHCP) is a communications protocol that allows network administrators to centrally manage and automate the network configuration of devices attached to an Internet Protocol (IP) network.

### 13.1.1 DHCP Concepts

The following section describes concepts important to the configuration and application of DHCP.

#### 13.1.1.1 DHCP Snooping

DHCP snooping is a network security feature that protects the network from untrusted DHCP servers and untrusted clients by keeping track of ports where DHCP clients and servers reside. This information is tracked by building a DHCP binding table that contains all MAC-IP associations the switch has learned by snooping client and server DHCP communications. The binding table contains MAC-IP information which can be further utilized by DHCP snooping applications. RUGGEDCOM ROS will log messages in the syslog and/or raise an alarm when DHCP violations are detected.

**Note**
DHCP Snooping is enabled on the device on a per-VLAN basis. For more information about enabling DHCP snooping on individual VLANs, refer to "Managing Static VLANs (Page 149)".

#### 13.1.1.2 Trusted and Untrusted Ports

DHCP Snooping classifies ports as trusted and untrusted. This port classification determines how a DHCP message is handled by the switch. DHCP messages received on trusted ports are forwarded without any further checking, while messages received from untrusted ports are verified to determine if the message is legitimate. The user is expected to configure the ports as trusted or untrusted.

From a deployment perspective, it is also expected the user configures network ports as trusted. Network ports typically connect to another switch or a router. This is necessary because a DHCP server may not be directly connected to a switch port.

For more information about configuring ports as trusted or untrusted, refer to "Configuring Trusted/Untrusted Ports (Page 310)".

#### 13.1.1.3 DHCP Relay Agent (Option 82)

A DHCP Relay Agent is a device that forwards DHCP packets between clients and servers when they are not on the same physical LAN segment or IP subnet. The feature is enabled if the DHCP server IP address and a set of ethernet ports are configured.

DHCP Option 82 provides a mechanism for assigning an IP Address based on the location of the client device in the network. Information about the client's location can be sent along with the DHCP request to the server. Based on this information, the DHCP server makes a decision about an IP Address to be assigned.

The DHCP Relay Agent takes the broadcast DHCP requests from clients received on the configured port and inserts the relay agent information option (Option 82) into the packet. Option 82 contains the VLAN ID (2 bytes) and the port number of the client port (2 bytes: the circuit ID sub-option) and the relay agent's MAC address (the remote ID sub-option). This information uniquely defines the client's position in the network.

For example, using the following formula, the Circuit ID for a client which is connected to VLAN 1 on port 3/1 is `00:01:00:09`.

```
({slot} - 1)*4 + {port}
```

The DHCP Server supporting DHCP Option 82 sends a unicast reply and echoes Option 82. The DHCP Relay Agent removes the Option 82 field and forwards the packet to the port from which the original request was received.

These parameters provide the ability to configure the information based DHCP relay agent (Option 82).

For more information about configuring the DHCP Relay Agent, refer to "Configuring the DHCP Relay Agent (Page 308)".

#### 13.1.1.4 Dynamic ARP Inspection

Dynamic ARP Inspection (DAI) is a DHCP snooping application that validates Address Resolution Protocol (ARP) packets in a network. DAI filters ARP packets with invalid IP-to-MAC address bindings. This protects the network from some man-in-the-middle attacks. Dynamic ARP inspection makes sure only valid ARP requests and responses are relayed.

**Note**
Dynamic ARP Inspection can only be enabled if DHCP snooping is enabled on the device.

ARP request and reply packets ingressing on untrusted ports are intercepted by the device and subject to validation. ARP packets are not intercepted on ports that are configured as trusted. The user is expected to configure the network ports as *trusted*, so that ARP traffic between devices is not subject to inspection.

The sender MAC and sender IP address fields in an ARP request/reply packets are validated against the MAC-IP binding entry present in the DHCP snooping binding table. If a binding entry is not present in the table, or if the information in the entry does not match, the ARP request/reply packet is dropped.

For more information about ARP inspection statistics, refer to "Viewing ARP Inspection Statistics (Page 311)".

#### 13.1.1.5 DHCP Binding Table

DHCP snooping dynamically builds and maintains a binding table using information extracted from intercepted DHCP messages. The table contains an entry for each untrusted host with a leased IP address from the DHCP server. The table does not contain entries for hosts connected through trusted interfaces. The DHCP snooping feature updates the table when the switch receives specific DHCP messages.

When the device is reset, all the MAC-IP binding information learned by the switch will be lost, unless the learned bindings are saved in the switch configuration file.

If a switch port link goes down, all the dynamically-learned binding table entries on that particular port are removed from the table.

Manually-entered records can also be configured using a static binding table. For more information about configuring the static DHCP binding table, refer to "Adding Entries to the DHCP Binding Table (Page 311)".

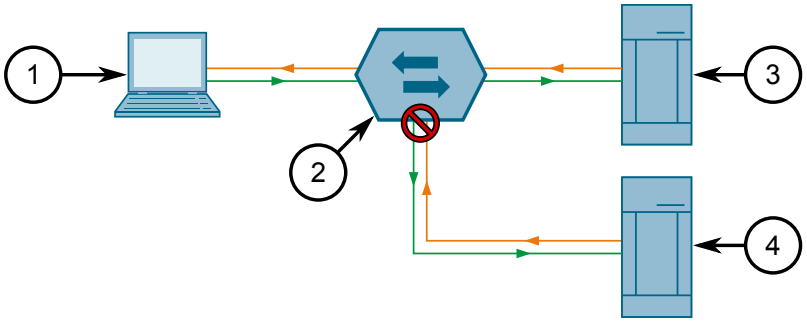
#### 13.1.1.6 Preventable Network Attacks

The following network attacks can be prevented by enabling DHCP snooping and Dynamic ARP Inspection on the switch. For more information, refer to "Configuring DHCP Snooping (Page 309)".

- **Host Misconfiguration by a Rogue DHCP Server**

  A rogue DHCP server can assign an incorrect IP address, default gateway and/or DNS server parameters to the client. A misconfigured client is susceptible to a potential network attack. Switches that support DHCP snooping can identify DHCP

messages from a rogue DHCP server and block these messages in the switch itself.



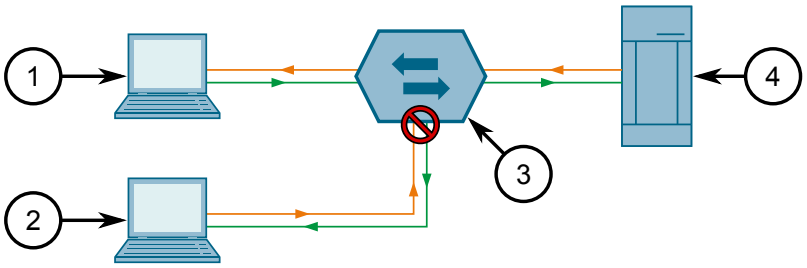

① DHCP Client
② Switch
③ DHCP Server
④ Rogue DHCP Server

Figure 13.1 Misconfiguration by a Rogue DHCP Server

- **DHCP Client Attack**

  A roque DHCP client, or attacker host, can cancel the lease for an IP address assigned to another client by sending a DHCPRELEASE message to the DHCP server. It can also decline the IP address for another client by sending a DHCPDECLINE message.

  DHCP snooping builds a DHCP binding table to validate the legitimacy of DHCPRELEASE and DHCPDECLINE messages. If validation of these messages fail, they are dropped by the device.

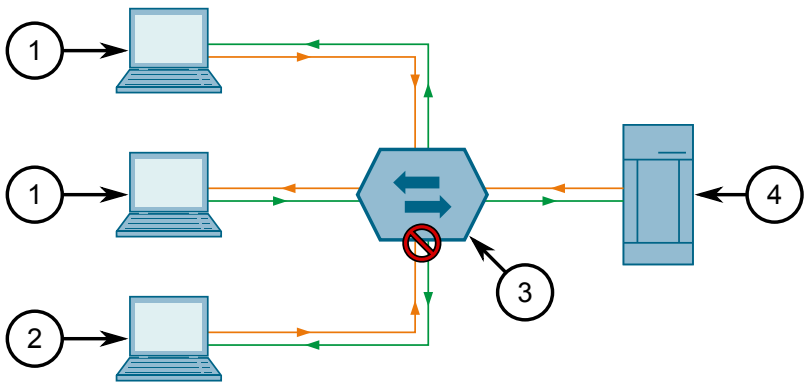



① DHCP Client
② Attacker Host
③ Switch
④ DHCP Server

Figure 13.2 DHCP Client Attack

- **DHCP Starvation Attack**

  DHCP starvation occurs when a DHCP server is flooded with DHCP requests from a single rogue DHCP client that has spoofed the client hardware addresses of other clients. This exhausts the DHCP server's IP address pool, after which the server is unable to respond and provide new leases to legitimate DHCP clients. DHCP snooping provides users an option to verify the client hardware address in the DHCP-REQUEST message, thus preventing a starvation attack.




① DHCP Client
② Attacker
③ Switch
④ DHCP Server

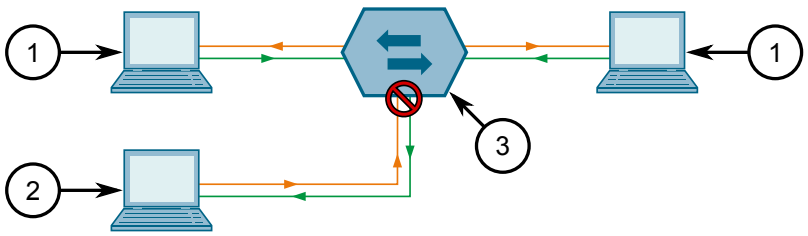
Figure 13.3 DHCP Starvation/Consumption Attack

- **ARP Spoofing Attack/Cache Poisoning**

  ARP spoofing attacks and cache poisoning can occur because ARP allows a gratuitous reply from a host even if an ARP request was not received. After the attack, all traffic from the device under attack flows to the attacker's computer. An ARP spoofing attack can target hosts, switches, and routers connected to a Layer 2

network by poisoning the ARP caches of systems connected to the subnet and by intercepting traffic intended for other hosts on the subnet.

An ARP spoofing attack can be prevented by enabling Dynamic ARP Inspection on the switch. For more information about enabling Dynamic ARP Inspection, refer to "Configuring DHCP Snooping (Page 309)".




① Host
② Attacker
③ Switch

Figure 13.4 ARP Cache Poisoning

## 13.1.2 Configuring the DHCP Relay Agent

To configure the device as a DHCP Relay Agent (Option 82), do the following:

1. Navigate to ***Network Access Control » DHCP Snooping » Configure DHCP Parameters***. The **DHCP Parameters** form appears.
2. Configure the following parameter(s) as required:

| Parameter | Description |
|---|---|
| `DHCP Server Address` | **Synopsis:** Any valid IP address<br>IP address of the DHCP server to which DHCP requests will be forwarded. DHCP server IP must be configured for Relay Agent to work. |

3. Click **Apply**.
4. Enable DHCP Relay Agent (Option 82) on ports connected to a DHCP client. For more information, refer to "Enabling DHCP Relay Agent Information (Option 82) for Specific Ports (Page 308)".

## 13.1.3 Enabling DHCP Relay Agent Information (Option 82) for Specific Ports

DHCP Relay Agent (Option 82) can be enabled for any Ethernet port connected to a DHCP client.

To enable DHCP Relay Agent (Option 82) for a specific port, do the following:

1. Navigate to ***Network Access Control » DHCP Snooping » Configure DHCP Port Parameters***. The **DHCP Port Parameters** table appears.
2. Select a port. The **DHCP Port Parameters** form appears.

**Note**
The *Trusted* parameter is configured as part of the DHCP snooping feature. For more information, refer to "Configuring Trusted/Untrusted Ports (Page 310)".

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

| Parameter | Description |
|---|---|
| Port | **Synopsis:** 1/1 to maximum port number<br>The port number as seen on the front plate silkscreen of the device. |
| Option-82 | **Synopsis:** [ Disabled \| Enabled ]<br>**Default:** Disabled<br>Insert DHCP Option 82. |

4. Click **Apply**.

## 13.1.4 Configuring DHCP Snooping

To configure DHCP snooping, do the following:

**Note**
DHCP Snooping is enabled on the device on a per-VLAN basis. For more information about enabling DHCP snooping on individual VLANs, refer to "Managing Static VLANs (Page 149)".

1. Navigate to ***Network Access Control » DHCP Snooping » Configure DHCP Parameters***. The **DHCP Parameters** form appears.
2. Configure the following parameter(s) as required:

| Parameter | Description |
|---|---|
| DHCP Server Address | **Synopsis:** Any valid IP address<br>IP address of the DHCP server to which DHCP requests will be forwarded. DHCP server IP must be configured for Relay Agent to work. |

3. Click **Apply**.
4. Configure individual ports as *trusted* or *untrusted*. For more information, refer to "Configuring Trusted/Untrusted Ports (Page 310)".

### 13.1.5 Configuring Trusted/Untrusted Ports

Once DHCP Snooping has been enabled, individual ports need to be marked as *trusted* or *untrusted*. Ports connected to the DHCP server should be *trusted*, whereas ports connected to the client or an untrusted DHCP server should be considered *untrusted*.

To configure a port as *trusted* or *untrusted*, do the following:

1. Navigate to ***Network Access Control » DHCP Snooping » Configure DHCP Port Parameters***. The **DHCP Port Parameters** table appears.
2. Select an Ethernet port. The **DHCP Port Parameters** form appears.

**Note**
The *Option-82* parameter is configured as part of the DHCP Relay Agent feature. For more information, refer to "Enabling DHCP Relay Agent Information (Option 82) for Specific Ports (Page 308)".

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

| Parameter | Description |
|---|---|
| Trusted | **Synopsis:** [ No \| Yes ]<br>**Default:** No<br>DHCP trust setting for the port. |

4. Click **Apply**.

### 13.1.6 Managing Dynamic ARP Inspection

This section describes how to configure and manage dynamic Address Resolution Protocol (ARP) inspection.

#### 13.1.6.1 Enabling/Disabling Dynamic ARP Inspection

To enable or disable Dynamic ARP Inspection, do the following:

1. Navigate to ***Network Access Control » DHCP Snooping » Configure DHCP Parameters***. The **DHCP Parameters** form appears.
2. Configure the following parameter(s) as required:

| Parameter | Description |
|---|---|
| ARP Inspection | **Synopsis:** [ Disabled \| Enabled ]<br>**Default:** Disabled<br>Enable or Disable Dynamic ARP Inspection. |

3. Click **Apply**.

#### 13.1.6.2 Viewing ARP Inspection Statistics

To view ARP Inspection Statistics, do the following:

1. Navigate to ***Network Access Control » DHCP Snooping » View ARP Inspection Statistics***. The **ARP Inspection Statistics** table appears.
2. Select an Ethernet port. The **ARP Inspection Statistics** form appears.
3. Configure the following parameter(s) as required:

| Parameter | Description |
|---|---|
| `Port` | **Synopsis:** 1/1 to maximum port number<br>The port number as seen on the front plate silkscreen of the device. |
| `In Packets` | **Synopsis:** An integer between 0 and 4294967295<br>Total number of incoming ARP packets that were processed by Dynamic ARP Inspection on this port. |
| `Dropped Packets` | **Synopsis:** An integer between 0 and 4294967295<br>Total number of incoming ARP packets that were dropped by Dynamic ARP Inspection on this port. |

4. Click **Apply**.

#### 13.1.6.3 Clearing ARP Inspection Statistics

To clear ARP Inspection Statistics, do the following:

1. Navigate to ***Network Access Control » DHCP Snooping » Clear ARP Inspection Statistics***. The **Clear ARP Inspection Statistics** form appears.
2. Click **Confirm**.

### 13.1.7 Managing the DHCP Binding Table

This section describes how to configure and manage the DHCP binding table.

#### 13.1.7.1 Adding Entries to the DHCP Binding Table

The DHCP binding table is populated automatically with information RUGGEDCOM ROS learns about untrusted hosts. Specific hosts can also be added to the table. Static entries do not expire and will not be removed when DHCP snooping is disabled or the device is reset.

To add a static entry to the DHCP binding table, do the following:

1. Navigate to ***Network Access Control » DHCP Snooping » Configure Static DHCP Binding Table***. The **Configure Static DHCP Binding Table** appears.
2. Click **InsertRecord**. The **Static DHCP Binding Table** form appears.

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

| Parameter | Description |
|---|---|
| MAC Address | **Synopsis:** ##-##-##-##-##-## where ## ranges 0 to FF<br>**Default:** 00-00-00-00-00-00<br>MAC Address of the DHCP Host. |
| IP Address | **Synopsis:** ##-##-##-##-##-## where ## ranges 0 to 255<br>IP Address assigned to the DHCP Host. |
| VID | **Synopsis:** An integer between 0 and 65535<br>**Default:** 1<br>VLAN where in the IP-MAC binding entry was registered. |
| Port | **Synopsis:** 1/1 to maximum port number<br>**Default:** 1/1<br>Port on which IP-MAC binding entry was regsitered. |

4. Click **Apply**.

#### 13.1.7.2 Viewing the DHCP Binding Table

To view the DHCP binding table, do the following:

1. Navigate to ***Network Access Control » DHCP Snooping » View DHCP Binding Table***. The **View DHCP Binding Table** appears.
2. Select an Ethernet port. The **DHCP Binding Table** form appears.

The DHCP binding table displays the following information:

To refresh the table, click **Reload**.

#### 13.1.7.3 Saving the DHCP Binding Table

Information learned dynamically and added to the DHCP binding table is removed automatically when the following occurs:

- The lease expires
- DHCP snooping is disabled
- The device is reset

However, this information can be saved to the configuration file for future reference/use.

To save the DHCP binding table, do the following:

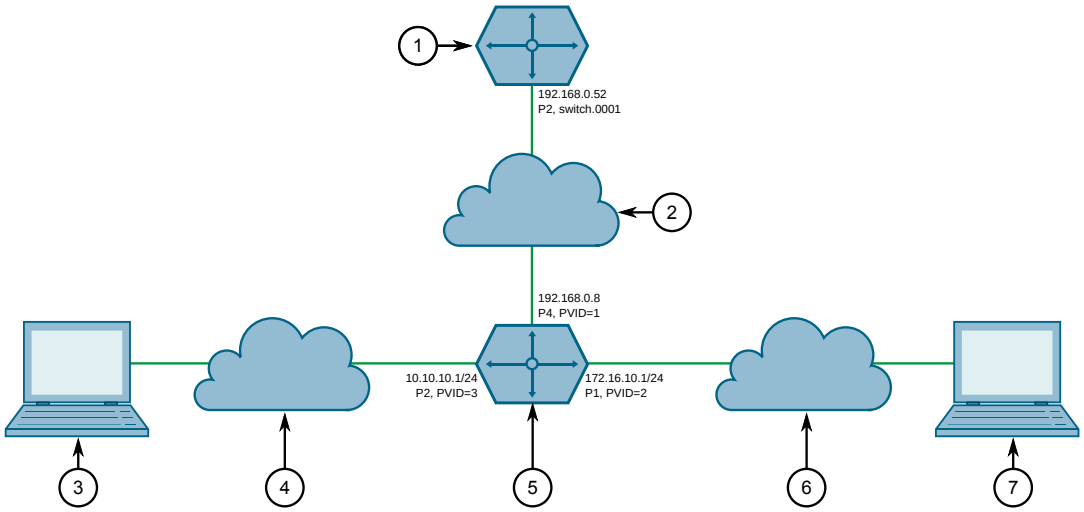
1. Navigate to ***Network Access Control » DHCP Snooping » Save DHCP Binding Table***. The **Save DHCP Binding Table** table appears.
2. Click **Confirm**.

### 13.1.7.4 Example: Configuring the Device as a Relay Agent

This example demonstrates how to configure the device as a DHCP relay agent.

The following topology depicts a scenario where two clients on separate LANs require IP addresses on different subnets from a DHCP server. Each client connects to the DHCP relay agent using different VLANs. The DHCP relay agent manages the requests and responses between the clients and the DHCP server.

| NOTICE |
| --- |
| The values shown are specific to the provided topology. Actual values can vary based on the user's configuration. |




① DHCP Server
② LAN A
③ Client 2
④ LAN B
⑤ DHCP Relay Agent (RUGGEDCOM ROS Device)
⑥ LAN C
⑦ Client 1

Figure 13.5 Topology – Device as a Relay Agent

To configure the device as a DHCP relay agent per the topology, do the following:

1. Configure a separate device as the DHCP Server. If the DHCP server being used is a RUGGEDCOM ROX II device, refer to the device-specific *RUGGEDCOM ROX II User Guide* for more information.

2. Configure the RUGGEDCOM ROS device as a DHCP relay agent:
   a. Add VLAN 2 and VLAN 3. For more information, refer to "Adding a Static VLAN (Page 149)".
   b. Assign IP address *192.168.0.8* to VLAN 1. For more information, refer to "Adding a Switch IP Interface (Page 83)".
   c. Change the PVID of port 1 to PVID 2, and change the PVID of port 2 to PVID 3. Refer to "Configuring VLANs for Specific Ethernet Ports (Page 147)" for more information.
   d. Configure *192.168.0.52* as the DHCP server address. Refer to "Configuring the DHCP Relay Agent (Page 308)" for more information.
   e. Configure DHCP client and server ports as follows:

| Port | Option 82 |
|---|---|
| 1 | Enabled |
| 2 | Enabled |
| 4 | Disabled |

   For more information about configuring the DHCP relay agent (Option 82) for a specific port, refer to "Enabling DHCP Relay Agent Information (Option 82) for Specific Ports (Page 308)".
   f. To verify the configuration, make sure Client 1 has IP address 172.16.10.1/24 and Client 2 has IP address 10.10.10.1/24.
3. [Optional] Configure DHCP snooping:
   a. Enable DHCP snooping on the DHCP server. If the DHCP server being used is a RUGGEDCOM ROX II device, refer to the device-specific *RUGGEDCOM ROX II User Guide* for more information.
   b. Make sure DHCP option is enabled on VLANs 1, 2, and 3. For more information about enabling DHCP for a specific VLAN, refer to "Adding a Static VLAN (Page 149)".
   c. Configure DHCP client and server ports:

      For more information about configuring DHCP port parameters, refer to "Configuring Trusted/Untrusted Ports (Page 310)".

| Port | Trusted |
|---|---|
| 1 | No |
| 2 | No |
| 4 | Yes |

      To verify the configuration, make sure Client 1 has the IP address 172.16.10.1/24 and Client 2 has the IP address 10.10.10.1/24.

      In the relay agent binding table, make sure records have been added for Port 1 and Port 2, and make sure no record exists for Port 4. For more information, refer to "Viewing the DHCP Binding Table (Page 312)".

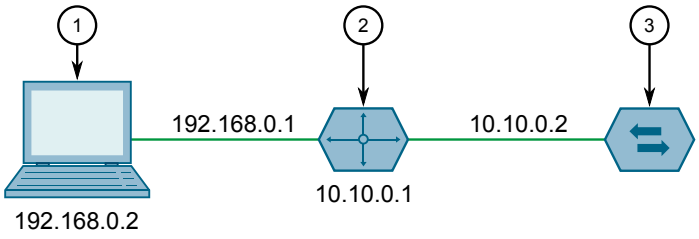
# 14 Troubleshooting

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. |

## 14.1 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.<br>  <br><br>① Work Station<br>② Router<br>③ Switch<br>Figure 14.1 Using a Router As a Gateway<br>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.<br>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. |

## 14.2 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.<br>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.<br>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.<br>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.<br>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.<br>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. |

## 14.3 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.<br>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 318).<br>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.<br>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.<br>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.<br>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.<br>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.<br>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. |

## 14.4 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.<br><br>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.<br><br>**Note**<br>Establishing a management domain is often accompanied with the establishment of an IP subnet specifically for the managed devices. |

## Further Information

Siemens
**https://www.siemens.com**

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