SIEMENS

RUGGEDCOM ROS v4.3

User Guide

For RS900

Preface

Introduction 1

Using ROS 2

Device Management 3

System Administration 4

Setup and Configuration 5

Troubleshooting 6

07/2016

RC1275-EN-03

Copyright © 2016 Siemens Canada Ltd

All rights reserved. Dissemination or reproduction of this document, or evaluation and communication of its contents, is not authorized except where expressly permitted. Violations are liable for damages. All rights reserved, particularly for the purposes of patent application or trademark registration.

This document contains proprietary information, which is protected by copyright. All rights are reserved. No part of this document may be photocopied, reproduced or translated to another language without the prior written consent of Siemens Canada Ltd.

Disclaimer Of Liability

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

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

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

Registered Trademarks

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

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

Third Party Copyrights

Siemens recognizes the following third party copyrights:

- Copyright © 2004 GoAhead Software, Inc. All Rights Reserved.

Open Source

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

Security Information

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

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

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

Warranty

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

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

Contacting Siemens

Address

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

Telephone

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

E-mail

ruggedcom.info.i-ia@siemens.com

Web

www.siemens.com/ruggedcom

Table of Contents

Preface xiii
Conventions xiii
Related Documents xiv
System Requirements xiv
Accessing Documentation xiv
Training xv
Customer Support xv

Chapter 1
Introduction 1
1.1 Features and Benefits 1
1.2 Security Recommendations and Considerations 3
1.2.1 Security Recommendations 3
1.2.2 Credential Files 5
1.2.2.1 SSL Certificates 6
1.2.2.2 SSH Key Pairs 8
1.3 Supported Networking Standards 9
1.4 Port Numbering Scheme 9
1.5 Available Services by Port 10
1.6 SNMP Management Interface Base (MIB) Support 12
1.6.1 Supported Standard MIBs 12
1.6.2 Supported Proprietary RUGGEDCOM MIBs 13
1.6.3 Supported Agent Capabilities 13
1.7 SNMP Traps 14
1.8 ModBus Management Support 16
1.8.1 ModBus Function Codes 16
1.8.2 ModBus Memory Map 17
1.8.3 ModBus Memory Formats 22
1.8.3.1 Text 23
1.8.3.2 Cmd 23
1.8.3.3 Uint16 23
1.8.3.4 Uint32 24
1.8.3.5 PortCmd 24
1.8.3.6 Alarm 25
1.8.3.7 PSStatusCmd 25

1.8.3.8 TruthValues 25
1.9 SSH and SSL Keys and Certificates 26
1.9.1 Certificate and Keys Life Cycle 26
1.9.2 Certificate and Key Requirements 27

Chapter 2
Using ROS 29
2.1 Connecting to ROS 29
2.1.1 Connecting Directly 29
2.1.2 Connecting via the Network 30
2.2 Logging In 31
2.3 Logging Out 32
2.4 Using the Web Interface 33
2.5 Using the Console Interface 34
2.6 Using the Command Line Interface 36
2.6.1 Available CLI Commands 36
2.6.2 Tracing Events 39
2.6.3 Executing Commands Remotely via RSH 40
2.6.4 Using SQL Commands 40
2.6.4.1 Finding the Correct Table 41
2.6.4.2 Retrieving Information 41
2.6.4.3 Changing Values in a Table 43
2.6.4.4 Resetting a Table 44
2.6.4.5 Using RSH and SQL 44
2.7 Selecting Ports in RUGGEDCOM ROS 44
2.8 Managing the Flash File System 45
2.8.1 Viewing a List of Flash Files 45
2.8.2 Viewing Flash File Details 45
2.8.3 Defragmenting the Flash File System 46
2.9 Accessing BIST Mode 46
2.10 Managing SSH Public Keys 47
2.10.1 Adding a Public Key 47
2.10.2 Viewing a List of Public Keys 49
2.10.3 Updating a Public Key 49
2.10.4 Deleting a Public Key 50

Chapter 3
Device Management 51
3.1 Viewing Product Information 51
3.2 Viewing CPU Diagnostics 53
3.3 Restoring Factory Defaults 54

3.4 Uploading/Downloading Files 55
3.4.1 Uploading/Downloading Files Using XMODEM 56
3.4.2 Uploading/Downloading Files Using a TFTP Client 57
3.4.3 Uploading/Downloading Files Using a TFTP Server 58
3.4.4 Uploading/Downloading Files Using an SFTP Server 58
3.5 Managing Logs 59
3.5.1 Viewing Local Logs 59
3.5.2 Clearing Local Logs 60
3.5.3 Configuring the Local System Log 60
3.5.4 Managing Remote Logging 61
3.5.4.1 Configuring the Remote Syslog Client 61
3.5.4.2 Viewing a List of Remote Syslog Servers 62
3.5.4.3 Adding a Remote Syslog Server 63
3.5.4.4 Deleting a Remote Syslog Server 64
3.6 Managing Ethernet Ports 65
3.6.1 Controller Protection Through Link Fault Indication (LFI) 66
3.6.2 Viewing the Status of Ethernet Ports 67
3.6.3 Viewing Statistics for All Ethernet Ports 68
3.6.4 Viewing Statistics for Specific Ethernet Ports 68
3.6.5 Clearing Statistics for Specific Ethernet Ports 71
3.6.6 Configuring an Ethernet Port 72
3.6.7 Configuring Port Rate Limiting 74
3.6.8 Configuring Port Mirroring 76
3.6.9 Configuring Link Detection 77
3.6.10 Detecting Cable Faults 79
3.6.10.1 Viewing Cable Diagnostics Results 79
3.6.10.2 Performing Cable Diagnostics 81
3.6.10.3 Clearing Cable Diagnostics 83
3.6.10.4 Determining the Estimated Distance To Fault (DTF) 83
3.6.11 Resetting Ethernet Ports 84
3.7 Managing IP Interfaces 84
3.7.1 Viewing a List of IP Interfaces 85
3.7.2 Adding an IP Interface 85
3.7.3 Deleting an IP Interface 87
3.8 Managing IP Gateways 88
3.8.1 Viewing a List of IP Gateways 88
3.8.2 Adding an IP Gateway 89
3.8.3 Deleting an IP Gateway 90
3.9 Configuring IP Services 91
3.10 Managing Remote Monitoring 93

3.10.1 Managing RMON History Controls 94
3.10.1.1 Viewing a List of RMON History Controls 94
3.10.1.2 Adding an RMON History Control 94
3.10.1.3 Deleting an RMON History Control 96
3.10.2 Managing RMON Alarms 97
3.10.2.1 Viewing a List of RMON Alarms 98
3.10.2.2 Adding an RMON Alarm 99
3.10.2.3 Deleting an RMON Alarm 101
3.10.3 Managing RMON Events 102
3.10.3.1 Viewing a List of RMON Events 103
3.10.3.2 Adding an RMON Event 103
3.10.3.3 Deleting an RMON Event 105
3.11 Upgrading/Downgrading Firmware 105
3.11.1 Upgrading Firmware 106
3.11.2 Downgrading Firmware 106
3.12 Resetting the Device 107
3.13 Decommissioning the Device 108

Chapter 4
System Administration 111
4.1 Configuring the System Information 111
4.2 Customizing the Login Screen 112
4.3 Configuring Passwords 112
4.4 Clearing Private Data 115
4.5 Enabling/Disabling the Web Interface 116
4.6 Managing Alarms 116
4.6.1 Viewing a List of Pre-Configured Alarms 117
4.6.2 Viewing and Clearing Latched Alarms 118
4.6.3 Configuring an Alarm 118
4.6.4 Authentication Related Security Alarms 121
4.6.4.1 Security Alarms for Login Authentication 121
4.6.4.2 Security Messages for Port Authentication 123
4.7 Managing the Configuration File 124
4.7.1 Configuring Data Encryption 124
4.7.2 Updating the Configuration File 126
4.8 Managing an Authentication Server 126
4.8.1 Managing RADIUS Authentication 127
4.8.1.1 Configuring the RADIUS Server 128
4.8.1.2 Configuring the RADIUS Client 128
4.8.2 Managing TACACS+ Authentication 130
4.8.2.1 Configuring TACACS+ 130

4.8.2.2 Configuring User Privileges 131

Chapter 5
Setup and Configuration 133
5.1 Managing Virtual LANs 133
5.1.1 VLAN Concepts 134
5.1.1.1 Tagged vs. Untagged Frames 134
5.1.1.2 Native VLAN 134
5.1.1.3 The Management VLAN 135
5.1.1.4 Edge and Trunk Port Types 135
5.1.1.5 Ingress and Egress Rules 135
5.1.1.6 Forbidden Ports List 136
5.1.1.7 VLAN-Aware and VLAN-Unaware Modes 136
5.1.1.8 GARP VLAN Registration Protocol (GVRP) 137
5.1.1.9 PVLAN Edge 138
5.1.1.10 QinQ 138
5.1.1.11 VLAN Advantages 140
5.1.2 Viewing a List of VLANs 141
5.1.3 Configuring VLANs Globally 141
5.1.4 Configuring VLANs for Specific Ethernet Ports 143
5.1.5 Managing Static VLANs 145
5.1.5.1 Viewing a List of Static VLANs 145
5.1.5.2 Adding a Static VLAN 145
5.1.5.3 Deleting a Static VLAN 147
5.2 Managing Spanning Tree Protocol 148
5.2.1 RSTP Operation 148
5.2.1.1 RSTP States and Roles 149
5.2.1.2 Edge Ports 151
5.2.1.3 Point-to-Point and Multipoint Links 152
5.2.1.4 Path and Port Costs 152
5.2.1.5 Bridge Diameter 153
5.2.1.6 eRSTP 153
5.2.1.7 Fast Root Failover 154
5.2.2 RSTP Applications 154
5.2.2.1 RSTP in Structured Wiring Configurations 155
5.2.2.2 RSTP in Ring Backbone Configurations 156
5.2.2.3 RSTP Port Redundancy 158
5.2.3 MSTP Operation 158
5.2.3.1 MSTP Regions and Interoperability 159
5.2.3.2 MSTP Bridge and Port Roles 160
5.2.3.3 Benefits of MSTP 161

5.2.3.4 Implementing MSTP on a Bridged Network 162
5.2.4 Configuring STP Globally 163
5.2.5 Configuring STP for Specific Ethernet Ports 164
5.2.6 Configuring eRSTP 167
5.2.7 Viewing Global Statistics for STP 169
5.2.8 Viewing STP Statistics for Ethernet Ports 171
5.2.9 Managing Multiple Spanning Tree Instances 173
5.2.9.1 Viewing Statistics for Global MSTIs 173
5.2.9.2 Viewing Statistics for Port MSTIs 175
5.2.9.3 Configuring the MST Region Identifier 176
5.2.9.4 Configuring a Global MSTI 177
5.2.9.5 Configuring an MSTI for an Ethernet Port 178
5.2.10 Clearing Spanning Tree Protocol Statistics 180
5.3 Managing Classes of Service 180
5.3.1 Configuring Classes of Service Globally 181
5.3.2 Configuring Classes of Service for Specific Ethernet Ports 182
5.3.3 Configuring Priority to CoS Mapping 184
5.3.4 Configuring DSCP to CoS Mapping 185
5.4 Managing MAC Addresses 186
5.4.1 Viewing a List of MAC Addresses 187
5.4.2 Configuring MAC Address Learning Options 188
5.4.3 Configuring MAC Address Flooding Options 188
5.4.4 Managing Static MAC Addresses 190
5.4.4.1 Viewing a List of Static MAC Addresses 190
5.4.4.2 Adding a Static MAC Address 190
5.4.4.3 Deleting a Static MAC Address 192
5.4.5 Purging All Dynamic MAC Addresses 193
5.5 Managing Time Services 193
5.5.1 Configuring the Time and Date 194
5.5.2 Managing NTP 195
5.5.2.1 Enabling/Disabling NTP Service 195
5.5.2.2 Configuring NTP Servers 196
5.6 Managing SNMP 197
5.6.1 Managing SNMP Users 198
5.6.1.1 Viewing a List of SNMP Users 198
5.6.1.2 Adding an SNMP User 199
5.6.1.3 Deleting an SNMP User 201
5.6.2 Managing Security-to-Group Mapping 203
5.6.2.1 Viewing a List of Security-to-Group Maps 203
5.6.2.2 Adding a Security-to-Group Map 203

5.6.2.3 Deleting a Security-to-Group Map 205
5.6.3 Managing SNMP Groups 205
5.6.3.1 Viewing a List of SNMP Groups 206
5.6.3.2 Adding an SNMP Group 206
5.6.3.3 Deleting an SNMP Group 208
5.7 Managing Network Discovery 209
5.7.1 Network Discovery Concepts 209
5.7.1.1 Link Layer Discovery Protocol (LLDP) 209
5.7.1.2 RUGGEDCOM Discovery Protocol (RCDP) 210
5.7.2 Configuring LLDP Globally 210
5.7.3 Configuring LLDP for an Ethernet Port 212
5.7.4 Enabling/Disabling RCDP 213
5.7.5 Viewing Global Statistics and Advertised System Information 214
5.7.6 Viewing Statistics for LLDP Neighbors 215
5.7.7 Viewing Statistics for LLDP Ports 216
5.8 Managing Multicast Filtering 217
5.8.1 Managing IGMP 217
5.8.1.1 IGMP Concepts 217
5.8.1.2 Viewing a List of Multicast Group Memberships 221
5.8.1.3 Viewing Forwarding Information for Multicast Groups 222
5.8.1.4 Configuring IGMP 223
5.8.2 Managing GMRP 224
5.8.2.1 GMRP Concepts 225
5.8.2.2 Viewing a Summary of Multicast Groups 227
5.8.2.3 Configuring GMRP Globally 227
5.8.2.4 Configuring GMRP for Specific Ethernet Ports 228
5.8.2.5 Viewing a List of Static Multicast Groups 230
5.8.2.6 Adding a Static Multicast Group 230
5.8.2.7 Deleting a Static Multicast Group 231
5.9 Managing Port Security 232
5.9.1 Port Security Concepts 233
5.9.1.1 Static MAC Address-Based Authentication 233
5.9.1.2 IEEE 802.1x Authentication 233
5.9.1.3 IEEE 802.1X Authentication with MAC Address-Based Authentication 234
5.9.1.4 Assigning VLANS with Tunnel Attributes 235
5.9.2 Viewing a List of Authorized MAC Addresses 235
5.9.3 Configuring Port Security 236
5.9.4 Configuring IEEE 802.1X 238
5.10 Managing Link Aggregation 240
5.10.1 Link Aggregation Concepts 241

5.10.1.1 Rules and Limitations 242
5.10.1.2 Link Aggregation and Layer 2 Features 242
5.10.1.3 Link Aggregation and Physical Layer Features 243
5.10.2 Managing Port Trunks 243
5.10.2.1 Viewing a List of Port Trunks 243
5.10.2.2 Adding a Port Trunk 244
5.10.2.3 Deleting a Port Trunk 245

Chapter 6
Troubleshooting 247
6.1 General 247
6.2 Ethernet Ports 248
6.3 Spanning Tree 248
6.4 VLANs 249

Preface

This guide describes v4.3 of ROS (Rugged Operating System) running on the RUGGEDCOM RS900. 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.

IMPORTANT!
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.

Conventions

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

Alerts

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

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

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

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

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

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

CLI Command Syntax

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

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

Related Documents

Other documents that may be of interest include:

- *RUGGEDCOM RS900 Installation Guide*

System Requirements

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

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

Accessing Documentation

The latest user documentation for RUGGEDCOM ROS v4.3 is available online at www.siemens.com/ruggedcom. 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.

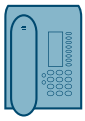
For more information about training services and course availability, visit www.siemens.com/ruggedcom or contact a Siemens Sales representative.

Customer Support

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

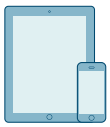
Online

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



Telephone

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



Mobile App

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

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

1 Introduction

Welcome to the RUGGEDCOM ROS v4.3 Software User Guide for the RS900. This Guide describes the wide array of carrier grade features made available by ROS (Rugged Operating System).

CONTENTS

- Section 1.1, “Features and Benefits”
- Section 1.2, “Security Recommendations and Considerations”
- Section 1.3, “Supported Networking Standards”
- Section 1.4, “Port Numbering Scheme”
- Section 1.5, “Available Services by Port”
- Section 1.6, “SNMP Management Interface Base (MIB) Support”
- Section 1.7, “SNMP Traps”
- Section 1.8, “ModBus Management Support”
- Section 1.9, “SSH and SSL Keys and Certificates”

Section 1.1

Features and Benefits

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

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

Section 1.2

Security Recommendations and Considerations

This section describes important security-related recommendations and suggestions that should be considered before implementing the RS900 on any network.

CONTENTS

- Section 1.2.1, “Security Recommendations”
- Section 1.2.2, “Credential Files”

Section 1.2.1

Security Recommendations

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

Authentication

- Replace the default passwords for all user accounts and processes (where applicable) before the device is deployed.
- Use strong passwords with high randomization (i.e. entropy), without repetition of characters. Avoid weak passwords such as *password1*, *123456789*, *abcdefgh*, and any dictionary words or proper names in any combination. For more information about creating strong passwords, refer to the password requirements in Section 4.3, “Configuring Passwords” .

- 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.

Physical/Remote Access

- Do not connect the device to the Internet. Deploy the device only within a secure network perimeter.
- Restrict physical access to the device to only authorized personnel. A person with malicious intent could extract critical information, such as certificates, keys, etc. (user passwords are protected by hash codes), or reprogram the device.
- Control access to the serial console to the same degree as any physical access to the device. Access to the serial console allows for potential access to the RUGGEDCOM ROS boot loader, which includes tools that may be used to gain complete access to the device.
- Only enable services that will be used on the device, including physical ports. Unused physical ports could potentially be used to gain access to the network behind the device.
- If SNMP is enabled, limit the number of IP addresses that can connect to the device and change the community names. Also configure SNMP to raise a trap upon authentication failures. For more information, refer to Section 5.6, “Managing SNMP” .
- 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.
- 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 Section 3.5, “Managing Logs” .
- 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 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 a third-party from launching various attacks that can harm the network or device. For more information, refer to Section 5.9, “Managing Port Security” .

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 [http://www.industry.siemens.com/topics/global/en/industrial-security/news-alerts/Pages/alerts.aspx] or the ProductCERT Security Advisories website [http://www.siemens.com/innovation/en/technology-focus/siemens-cert/cert-security-advisories.htm] . 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.
- Configure port security features on access ports to prevent a third-party from launching various attacks that can harm the network or device. For more information, refer to Section 5.9, “Managing Port Security” .

- 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. Additionally, 1/n-1 record splitting is enabled in the latest web browser versions of Mozilla Firefox, Google Chrome and Internet Explorer, and mitigates against attacks such as SSL/TLS Protocol Initialization Vector Implementation Information Disclosure Vulnerability (BEAST) for Non-Controlled (NC) versions of RUGGEDCOM ROS.
- 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 passwords without repetitive strings (e.g. *abc* or *abcabc*) with this feature. For more information about creating strong passwords, refer to the password requirements in Section 4.3, “Configuring Passwords” .
- Unless required for a particular network topology, the *IP Forward* setting should be set to { Disabled } to prevent the routing of packets.

> **NOTE**
> *For configuration compatibility reasons, the configured setting will not change when upgrading from RUGGEDCOM ROS versions older than v4.2.0 to v4.2.0 and newer. This setting is always enabled and cannot be configured on versions before v4.2.0. For new units with firmware v4.2.0 this setting is configurable and disabled by default.*

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.

Section 1.2.2

Credential Files

RUGGEDCOM ROS uses security keys to establish secure remote logins (SSH) and Web access (SSL).

It is strongly recommended that a unique SSL certificate and SSH keys be created and provisioned. New RUGGEDCOM ROS-based units from Siemens will be shipped with a unique certificate and keys preconfigured in the `ssl.crt` and `ssh.keys` flash files.

The default and auto-generated SSL certificates are self-signed. It is recommended to use an SSL certificate that is either signed by a trusted third-party Certificate Authority (CA) or by an organization's own CA. This technique is described in the Siemens application note: *Creating/Uploading SSH Keys and SSL Certificates to ROS Using Windows*, available from www.siemens.com/ruggedcom.

The sequence of events related to Key Management during an upgrade to RUGGEDCOM ROS v4.3 or later is as follows:

> **NOTE**
> *The auto-generation of SSH keys is not available for Non-Controlled (NC) versions of RUGGEDCOM ROS.*

- On first boot, RUGGEDCOM ROS will start the SSH and SSL services using the *default keys*.

- Immediately after boot, RUGGEDCOM ROS will start to generate a unique SSL certificate and SSH key pair, and save each one to its corresponding flash file. This process may take several minutes to complete. As each one is created, the corresponding service is immediately restarted with the new keys.
- At any time during the key generation process, custom keys can be uploaded. The custom keys will take precedence over both the default and auto-generated keys.
- On subsequent boot, if there is a valid `ssl.crt` file, the default certificate will not be used for SSL. If there is a valid `ssh.keys` file, the default SSH key will not be used.
- At any time, new keys may be uploaded or generated by RUGGEDCOM ROS using the `sslkeygen` or `sshkeygen` CLI commands.

CONTENTS

- Section 1.2.2.1, "SSL Certificates"
- Section 1.2.2.2, "SSH Key Pairs"

Section 1.2.2.1

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 EC 256, 384 or 521 bits
- For RUGGEDCOM ROS Non-Controlled (NC) verions: RSA key pair, 512 to 2048 bits

The RSA key pair used in the default certificate and in those generated by RUGGEDCOM ROS uses a public key of 1024 bits in length.

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

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.

NOTE
RSA key generation times increase depending on the key length. 1024 bit RSA keys may take several minutes to generate, 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 `openssl` command line utility to generate a self-signed X.509 v3 SSL certificate with a 1024 bit RSA key suitable for use in RUGGEDCOM ROS. Note that two standard PEM files are required: the SSL certificate and the RSA private key file. These are concatenated into the resulting `ssl.crt` file, which may then be uploaded to RUGGEDCOM ROS:

```
# RSA key size:
BITS=1024
# 20 years validity:
```

```
DAYS=7305

# Values that will be stored in the Distinguished Name fields:

COUNTRY_NAME=CA                    # Two-letter country code
STATE_OR_PROVINCE_NAME=Ontario     # State or Province
LOCALITY_NAME=Concord              # City
ORGANIZATION=Ruggedcom.com         # Your organization's name
ORGANIZATION_CA=${ORGANIZATION}_CA # Your Certificate Authority
COMMON_NAME=RC                     # The DNS or IP address of the ROS unit
ORGANIZATIONAL_UNIT=ROS            # Organizational unit name

# Variables used in the construction of the certificate
REQ_SUBJ="/C=${COUNTRY_NAME}/ST=${STATE_OR_PROVINCE_NAME}/L=${LOCALITY_NAME}/O=${ORGANIZATION}/OU=
${ORGANIZATIONAL_UNIT}/CN=${COMMON_NAME}/"
REQ_SUBJ_CA="/C=${COUNTRY_NAME}/ST=${STATE_OR_PROVINCE_NAME}/L=${LOCALITY_NAME}/O=${ORGANIZATION_CA}/
OU=${ORGANIZATIONAL_UNIT}/"

#######################################################################
# Make the self-signed SSL certificate and RSA key pair:

openssl req -x509 -newkey rsa:${BITS} -nodes \
 -days ${DAYS} -subj ${REQ_SUBJ} \
 -keyout ros_ssl.key  \
 -out    ros_ssl.crt

# Concatenate Cert and Key into a single file suitable for upload to ROS:
# Note that cert must precede the RSA key:
cat  ros_ssl.crt  ros_ssl.key > ssl.crt
```

For information on creating SSL certificates for use with RUGGEDCOM ROS in a Microsoft Windows environment, refer to the following Siemens application note: *Creating/Uploading SSH Keys and SSL Certificates to ROS Using Windows*.

The following is an example of a self-signed SSL certificate generated by RUGGEDCOM ROS:

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            ca:01:2d:c0:bf:f9:fd:f2
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=CA, ST=Ontario, L=Concord, O=RuggedCom.com, OU=RC, CN=ROS
        Validity
            Not Before: Dec  6 00:00:00 2012 GMT
            Not After : Dec  7 00:00:00 2037 GMT
        Subject: C=CA, ST=Ontario, L=Concord, O=RuggedCom.com, OU=RC, CN=ROS
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):
                    00:83:e8:1f:02:6b:cd:34:1f:01:6d:3e:b6:d3:45:
                    b0:18:0a:17:ae:3d:b0:e9:c6:f2:0c:af:b1:3e:e7:
                    fd:f2:0e:75:8d:6a:49:ce:47:1d:70:e1:6b:1b:e2:
                    fa:5a:1b:10:ea:cc:51:41:aa:4e:85:7c:01:ea:c3:
                    1e:9e:98:2a:a9:62:48:d5:27:1e:d3:18:cc:27:7e:
                    a0:94:29:db:02:5a:e4:03:51:16:03:3a:be:57:7d:
                    3b:d1:75:47:84:af:b9:81:43:ab:90:fd:6d:08:d3:
                    e8:5b:80:c5:ca:29:d8:45:58:5f:e4:a3:ed:9f:67:
                    44:0f:1a:41:c9:d7:62:7f:3f
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                EC:F3:09:E8:78:92:D6:41:5F:79:4D:4B:7A:73:AD:FD:8D:12:77:88
            X509v3 Authority Key Identifier:
                keyid:EC:F3:09:E8:78:92:D6:41:5F:79:4D:4B:7A:73:AD:FD:8D:12:77:88
```

```
                DirName:/C=CA/ST=Ontario/L=Concord/O=RuggedCom.com/OU=RC/CN=ROS
                serial:CA:01:2D:C0:BF:F9:FD:F2
            X509v3 Basic Constraints:
                CA:TRUE
    Signature Algorithm: sha1WithRSAEncryption
        64:cf:68:6e:9f:19:63:0e:70:49:a6:b2:fd:09:15:6f:96:1d:
        4a:7a:52:c3:46:51:06:83:7f:02:8e:42:b2:dd:21:d2:e9:07:
        5c:c4:4c:ca:c5:a9:10:49:ba:d4:28:fd:fc:9d:a9:0b:3f:a7:
        84:81:37:ca:57:aa:0c:18:3f:c1:b2:45:2a:ed:ad:dd:7f:ad:
        00:04:76:1c:f8:d9:c9:5c:67:9e:dd:0e:4f:e5:e3:21:8b:0b:
        37:39:8b:01:aa:ca:30:0c:f1:1e:55:7c:9c:1b:43:ae:4f:cd:
        e4:69:78:25:5a:a5:f8:98:49:33:39:e3:15:79:44:37:52:da:
        28:dd
```

Section 1.2.2.2

SSH Key Pairs

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; or RSA 1024, 2048 or 3072 bits in length

The DSA key pair used in the default key pair and in those generated by RUGGEDCOM ROS uses a public key of 1024 bits in length.

NOTE
DSA or RSA keys smaller than 2048 bits in length are not recommended, and support is only included here for compatibility with legacy equipment.

NOTE
DSA/RSA key generation times increase depending on the key length. 1024 bit RSA keys may take several minutes to generate, 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 1024 bit DSA key suitable for use in RUGGEDCOM ROS. The resulting `ssh.keys` file, which may then be uploaded to RUGGEDCOM ROS:

```
# DSA key size:
BITS=1024

# Make an SSH key pair:
ssh-keygen -t dsa -b 1024 -N '' -f ssh.keys
```

The following is an example of an SSH key generated by RUGGEDCOM ROS:

```
Private-Key: (1024 bit)
priv:
    00:b2:d3:9d:fa:56:99:a5:7a:ba:1e:91:c5:e1:35:
    77:85:e8:c5:28:36
pub:
    6f:f3:9e:af:e6:d6:fd:51:51:b9:fa:d5:f9:0a:b7:
    ef:fc:d7:7c:14:59:52:48:52:a6:55:65:b7:cb:38:
    2e:84:76:a3:83:62:d0:83:c5:14:b2:6d:7f:cc:f4:
    b0:61:0d:12:6d:0f:5a:38:02:67:a4:b7:36:1d:49:
    0a:d2:58:e2:ff:4a:0a:54:8e:f2:f4:c3:1c:e0:1f:
    9b:1a:ee:16:e0:e9:eb:c8:fe:e8:16:99:e9:61:81:
    ed:e4:f2:58:fb:3b:cb:c3:f5:9a:fa:ed:cd:39:51:
```

```
    47:90:5d:6d:1b:27:d5:04:c5:de:57:7e:a7:a3:03:
    e8:fb:0a:d5:32:89:40:12
P:
    00:f4:81:c1:9b:5f:1f:eb:ac:43:2e:db:dd:77:51:
    6e:1c:62:8d:4e:95:c6:e7:b9:4c:fb:39:9c:9d:da:
    60:4b:0f:1f:c6:61:b0:fc:5f:94:e7:45:c3:2b:68:
    9d:11:ba:e1:8a:f9:c8:6a:40:95:b9:93:7c:d0:99:
    96:bf:05:2e:aa:f5:4e:f0:63:02:00:c7:c2:52:c7:
    1a:70:7c:f7:e5:fe:dd:3d:57:02:86:ae:d4:89:20:
    ca:4b:46:80:ea:de:a1:30:11:5c:91:e2:40:d4:a3:
    82:c5:40:3b:25:8e:d8:b2:85:cc:f5:9f:a9:1d:ea:
    0a:ac:77:95:ee:d6:f7:61:e3
Q:
    00:d5:db:48:18:bd:ec:69:99:eb:ff:5f:e1:40:af:
    20:80:6d:5c:b1:23
G:
    01:f9:a1:91:c0:82:12:74:49:8a:d5:13:88:21:3e:
    32:ea:f1:74:55:2b:de:61:6c:fd:dd:f5:e1:c5:03:
    68:b4:ad:40:48:58:62:6c:79:75:b1:5d:42:e6:a9:
    97:86:37:d8:1e:e5:65:09:28:86:2e:6a:d5:3d:62:
    50:06:b8:d3:f9:d4:9c:9c:75:84:5b:db:96:46:13:
    f0:32:f0:c5:cb:83:01:a8:ae:d1:5a:ac:68:fb:49:
    f9:b6:8b:d9:d6:0d:a7:de:ad:16:2b:23:ff:8e:f9:
    3c:41:16:04:66:cf:e8:64:9e:e6:42:9a:d5:97:60:
    c2:e8:9e:f4:bc:8f:6f:e0
```

Section 1.3

Supported Networking Standards

The following networking standards are supported by RUGGEDCOM ROS:

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

Section 1.4

Port Numbering Scheme

For quick identification, each port on a RS900 device is assigned a number. All port numbers are silk-screened on the device.

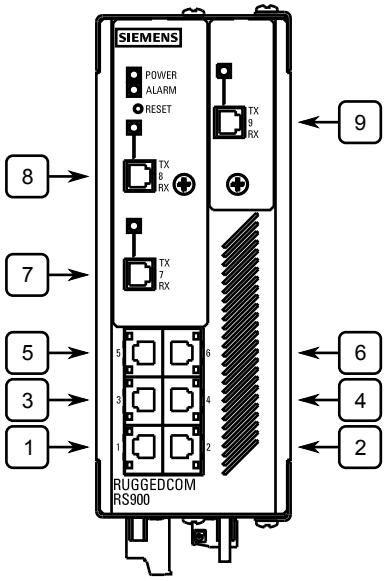


Figure 1: RS900 Port Numbering (Typical)

Use these numbers to configure applicable features on select ports.

Section 1.5

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 two

Services	Port Number	Service Enabled/ Disabled	Access Authorized	Note
				management interfaces.
HTTP	TCP/80	Enabled (configurable), redirects to 443	—	
HTTPS	TCP/443	Enabled (configurable)	Yes	
RSH	TCP/512	Disabled (configurable)	Yes	Only available through two management interfaces.
TFTP	UDP/69	Disabled (configurable)	No	Only available through two management interfaces.
SFTP	TCP/22	Enabled	Yes	Only available through two management interfaces.
SNMP	UDP/161	Disabled (configurable)	Yes	Only available through two management interfaces.
SNTP	UDP/123	Enabled (configurable)	No	Only available through two management interfaces.
SSH	TCP/22	Enabled	Yes	Only available through two management interfaces.
ICMP	—	Enabled	No	
TACACS+	TCP/49 (configurable)	Disabled (configurable)	Yes	
RADIUS	UDP/1812 to send (configurable), opens random port to listen to	Disabled (configurable)	Yes	Only available through two management interfaces.
Remote Syslog	UDP/514 (configurable)	Disabled (configurable)	No	Only available through two management interfaces.
TCP Modbus (Server)	TCP/502	Disabled (configurable)	No	Only available through two management interfaces.
TCP Modbus (Switch)	TCP/502	Disabled (configurable)	No	
DHCP, DHCP Agent	UDP/67, 68 sending msg if enabled - if received, always	Disabled (configurable)	No	

Services	Port Number	Service Enabled/ Disabled	Access Authorized	Note
	come to CPU, dropped if service not configured			
RCDP	—	Disabled (configurable)	Yes	

Section 1.6

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).

CONTENTS

- Section 1.6.1, “Supported Standard MIBs”
- Section 1.6.2, “Supported Proprietary RUGGEDCOM MIBs”
- Section 1.6.3, “Supported Agent Capabilities”

Section 1.6.1

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 Convention s 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 1659	RS-232-MIB	Definitions of Managed Objects for RS-232-like Hardware Devices
RFC 2863	IF-MIB	The Interface Group MIB
RFC 2819	RMON-MIB	Remote Network Monitoring (RMON) management Information base
RFC 4188	BRIDGE-MIB	Definitions of Managed Objects for Bridges

Standard	MIB Name	Title
RFC 4318	RSTP-MIB	Definitions of Managed Objects for Bridges with Rapid Spanning Tree Protocol
RFC 3411	SNMP-FRAMEWORK-MIB	An Architecture for Describing Simple Network Management Protocol (SNMP) Management Framework
RFC 3414	SNMP-USER-BASED-SM-MIB	User-based Security Model (USM) for Version 3 of the Simple Network Management Protocol (SNMPv3)
RFC 3415	SNMP-VIEW-BASED-ACM-MIB	View-bsed 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

Section 1.6.2

Supported Proprietary RUGGEDCOM MIBs

RUGGEDCOM ROS supports the following proprietary RUGGEDCOM MIBs:

File Name	MIB Name	Description
RUGGEDCOM-MIB.mib	RUGGEDCOM-MIB	RUGGEDCOM enterprise SMI
RUGGEDCOM-TRAPS-MIB.mib	RUGGEDCOM-TRAPS-MIB	RUGGEDCOM traps definition
RUGGEDCOM-SYS-INFO-MIB.mib	RUGGEDCOM-SYS-INFO-MIB	General system information about RUGGEDCOM device
RUGGEDCOM-DOT11-MIB.mib	RUGGEDCOM-DOT11-MIB	Managemet for wireless interface on RUGGEDCOM device
RUGGEDCOM-POE-MIB.mib	RUGGEDCOM-POE-MIB	Management for PoE ports on RUGGEDCOM device
RUGGEDCOM-SERIAL-MIB.mib	RUGGEDCOM-SERIAL-MIB	Managemet for seral ports on RUGGEDCOM device
RUGGEDCOM-STP-MIB.mib	RUGGEDCOM-STP-MIB	Management for RSTP protocol

Section 1.6.3

Supported Agent Capabilities

RUGGEDCOM ROS supports the following agent capabilities for the SNMP agent:

NOTE
For information about agent capabilities for SNMPv2, refer to RFC 2580 [http://tools.ietf.org/html/rfc2580].

File Name	MIB Name	Supported MIB
RC-SNMPv2-MIB-AC.mib	RC-SNMPv2-MIB-AC	SNMPv2-MIB
RC-UDP-MIB-AC.mib	RC-UDP-MIB-AC	UDP-MIB
RC-TCP-MIB-AC.mib	RC-TCP-MIB-AC	TCP-MIB
RC-SNMP-USER-BASED-SM-MIB-AC.mib	RC-SNMP-USER-BASED-SM-MIB-AC	SNMP-USER-BASED-SM-MIB-AC
RC-SNMP-VIEW-BASED-ACM-MIB-AC.mib	RC-SNMP-VIEW-BASED-ACM-MIB-AC	SNMP-VIEW-BASED-ACM-MIB-AC
RC-IF-MIB-AC.mib	RC-IF-MIB-AC	IF-MIB
RC-BRIDGE-MIB-AC.mib	RC-BRIDGE-MIB-AC	BRIDGE-MIB
RC-RMON-MIB-AC.mib	RC-RMON-MIB-AC	RMON-MIB
RC-Q-BRIDGE-MIB-AC.mib	RC-Q-BRIDGE-MIB-AC	Q-BRIDGE-MIB
RC-IP-MIB-AC.mib	RC-IP-MIB-AC	IP-MIB
RC-LLDP-MIB-AC.mib	RC-LLDP-MIB-AC	LLDP-MIB
RC-LAG-MIB-AC.mib	RC-LAG-MIB-AC	IEEE8023-LAG-MIB
RC_RSTP-MIB-AC.mib	RC_RSTP-MIB-AC	RSTP-MIB
RC-RUGGEDCOM-DOT11-MIB-AC.mib	RC-RUGGEDCOM-DOT11-MIB-AC	RUGGEDCOM-DOT11- MIB
RC-RUGGEDCOM-POE-MIB-AC.mib	RC-RUGGEDCOM-POE-MIB-AC	RUGGEDCOM-POE-MIB
RC-RUGGEDCOM-STP-AC-MIB.mib	RC-RUGGEDCOM-STP-AC-MIB	RUGGEDCOM-STP-MIB
RC-RUGGEDCOM-SYS-INFO-MIB-AC.mib	RC-RUGGEDCOM-SYS-INFO-MIB-AC	RUGGEDCOM-SYS-INFO-MIB
RC-RUGGEDCOM-TRAPS-MIB-AC.mib	RC-RUGGEDCOM-TRAPS-MIB-AC	RUGGEDCOM-TRAPS-MIB
RUGGEDCOM_RS-232-MIB-AC.mib	RUGGEDCOM_RS-232-MIB-AC	RS-232-MIB
RC-RUGGEDCOM-SERIAL-MIB-AC.mib	RC-RUGGEDCOM-SERIAL-MIB-AC	RUGGEDCOM-SERIAL-MIB

Section 1.7

SNMP Traps

The device generates the following standard traps:

Table: Standard Traps

Trap	MIB
linkDown	IF-MIB
linkUp	
authenticationFailure	SNMPv2-MIB
coldStart	
newRoot	BRIDGE-MIB
topologyChage	
risingAlarm	RMON-MIB

Trap	MIB
fallingAlarm	
lldpRemoteTablesChange	LLDP-MIB

The device also generates the following proprietary traps:

Table: Proprietary Traps

Trap	MIB
genericTrap	RUGGEDCOM-TRAPS-MIB
powerSupplyTrap	
swUpgradeTrap	
cfgChangeTrap	
weakPasswordTrap	
defaultKeysTrap	

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* *Section 2.6.1, "Available CLI Commands"* .

Table: Generic Traps

Trap	Severity
heap error	Alert
NTP server failure	notification
real time clock failure	Error
failed password	Warning
MAC address not learned by switch fabric	Warning
BootP client: TFTP transfer failure	Error
received looped back BPDU	Error
received two consecutive confusing BPDUs on port, forcing down	Error
GVRP failed to learn – too many VLANs	Warning

The device generates the following traps when specific events occur:

Table: Event-Based Traps

Trap	MIB	Event
rcRstpNewTopology	RUGGEDCOM-STP-MIB	This trap is generated when the device topology becomes stable after a topology change occurs on a switch port.

Section 1.8

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 writable registers for operator commands.

The ModBus protocol PDU (Protocol Data Unit) format is as follows:

Function Code	Data

CONTENTS

- Section 1.8.1, “ModBus Function Codes”
- Section 1.8.2, “ModBus Memory Map”
- Section 1.8.3, “ModBus Memory Formats”

Section 1.8.1

ModBus Function Codes

RUGGEDCOM devices support the following ModBus function codes for device management through ModBus:

NOTE

While RUGGEDCOM devices have a variable number of ports, not all registers and bits apply to all products.

Registers that are not applicable to a particular device return a zero (0) value. For example, registers referring to serial ports are not applicable to RUGGEDCOM switch devices.

Read Input Registers or Read Holding Registers — 0x04 or 0x03

Example PDU Request

Function Code	1 Byte	0x04(0x03)
Starting Address	2 Bytes	0x0000 to 0xFFFF (Hexadecimal) 128 to 65535 (Decimal)
Number of Input Registers	2 Bytes	Bytes 0x0001 to 0x007D

Example PDU Response

Function Code	1 Byte	0x04(0x03)
Byte Count	1 Byte	2 x *N* [a]
Number of Input Registers	*N* [a] x 2 Bytes	

[a] *The number of input registers*

Write Multiple Registers — 0x10

Example PDU Request

Function Code	1 Byte	0x10
Starting Address	2 Bytes	0x0000 to 0xFFFF
Number of Input Registers	2 Bytes	Bytes 0x0001 to 0x0079
Byte Count	1 Byte	2 x *N* [b]
Registers Value	*N* [b] x 2 Bytes	Value of the register

[b] *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)

Section 1.8.2

ModBus Memory Map

The following details how ModBus process variable data is mapped.

Product Info

The following data is mapped to the *Productinfo* table:

Address	#Registers	Description (Reference Table in UI)	R/W	Format
0000	16	Product Identification	R	Text
0010	32	Firmware Identification	R	Text
0040	1	Number of Ethernet Ports	R	Uint16
0041	1	Number of Serial Ports	R	Uint16
0042	1	Number of Alarms	R	Uint16
0043	1	Power Supply Status	R	PSStatusCmd
0044	1	FailSafe Relay Status	R	TruthValue
0045	1	ErrorAlarm Status	R	TruthValue

Product Write Register

The following data is mapped to various tables:

Address	#Registers	Description (Reference Table in UI)	R/W	Format
0080	1	Clear Alarms	W	Cmd
0081	2	Reset Ethernet Ports	W	PortCmd

Address	#Registers	Description (Reference Table in UI)	R/W	Format
0083	2	Clear Ethernet Statistics	W	PortCmd
0085	2	Reset Serial Ports	W	PortCmd
0087	2	Clear Serial Port Statistics	W	PortCmd

Alarms

The following data is mapped to the *alarms* table:

Address	#Registers	Description (Reference Table in UI)	R/W	Format
0100	64	Alarm 1	R	Alarm
0140	64	Alarm 2	R	Alarm
0180	64	Alarm 3	R	Alarm
01C0	64	Alarm 4	R	Alarm
0200	64	Alarm 5	R	Alarm
0240	64	Alarm 6	R	Alarm
0280	64	Alarm 7	R	Alarm
02C0	64	Alarm 8	R	Alarm

Ethernet Port Status

The following data is mapped to the *ethPortStats* table:

Address	#Registers	Description (Reference Table in UI)	R/W	Format
03FE	2	Port Link Status	R	PortCmd

Ethernet Statistics

The following data is mapped to the *rmonStats* table:

Address	#Registers	Description (Reference Table in UI)	R/W	Format
0400	2	Port s1/p1 Statistics - Ethernet In Packets	R	Uinst32
0402	2	Port s1/p2 Statistics - Ethernet In Packets	R	Uinst32
0404	2	Port s1/p3 Statistics - Ethernet In Packets	R	Uinst32
0406	2	Port s1/p4 Statistics - Ethernet In Packets	R	Uinst32
0408	2	Port s2/p1 Statistics - Ethernet In Packets	R	Uinst32
040A	2	Port s2/p2 Statistics - Ethernet In Packets	R	Uinst32
040C	2	Port s2/p3 Statistics - Ethernet In Packets	R	Uinst32
040E	2	Port s2/p4 Statistics - Ethernet In Packets	R	Uinst32
0410	2	Port s3/p1 Statistics - Ethernet In Packets	R	Uinst32

Address	#Registers	Description (Reference Table in UI)	R/W	Format
0412	2	Port s3/p2 Statistics - Ethernet In Packets	R	Uinst32
0414	2	Port s3/p3 Statistics - Ethernet In Packets	R	Uinst32
0416	2	Port s3/p4 Statistics - Ethernet In Packets	R	Uinst32
0418	2	Port s4/p1 Statistics - Ethernet In Packets	R	Uinst32
041A	2	Port s4/p2 Statistics - Ethernet In Packets	R	Uinst32
041C	2	Port s4/p3 Statistics - Ethernet In Packets	R	Uinst32
041E	2	Port s4/p4 Statistics - Ethernet In Packets	R	Uinst32
0420	2	Port s5/p1 Statistics - Ethernet In Packets	R	Uinst32
0422	2	Port s5/p2 Statistics - Ethernet In Packets	R	Uinst32
0424	2	Port s5/p3 Statistics - Ethernet In Packets	R	Uinst32
0426	2	Port s5/p4 Statistics - Ethernet In Packets	R	Uinst32
0428	2	Port s6/p1 Statistics - Ethernet In Packets	R	Uinst32
042A	2	Port s6/p2 Statistics - Ethernet In Packets	R	Uinst32
042C	2	Port s6/p3 Statistics - Ethernet In Packets	R	Uinst32
042E	2	Port s6/p4 Statistics - Ethernet In Packets	R	Uinst32
0430	2	Port s7/p1 Statistics - Ethernet In Packets	R	Uinst32
0432	2	Port s7/p2 Statistics - Ethernet In Packets	R	Uinst32
0434	2	Port s8/p1 Statistics - Ethernet In Packets	R	Uinst32
0436	2	Port s8/p2 Statistics - Ethernet In Packets	R	Uinst32
0440	2	Port s1/p1 Statistics - Ethernet Out Packets	R	Uinst32
0442	2	Port s1/p2 Statistics - Ethernet Out Packets	R	Uinst32
0444	2	Port s1/p3 Statistics - Ethernet Out Packets	R	Uinst32
0446	2	Port s1/p4 Statistics - Ethernet Out Packets	R	Uinst32
0448	2	Port s2/p1 Statistics - Ethernet Out Packets	R	Uinst32
044A	2	Port s2/p2 Statistics - Ethernet Out Packets	R	Uinst32
044C	2	Port s2/p3 Statistics - Ethernet Out Packets	R	Uinst32
044E	2	Port s2/p4 Statistics - Ethernet Out Packets	R	Uinst32
0450	2	Port s3/p1 Statistics - Ethernet Out Packets	R	Uinst32
0452	2	Port s3/p2 Statistics - Ethernet Out Packets	R	Uinst32
0454	2	Port s3/p3 Statistics - Ethernet Out Packets	R	Uinst32
0456	2	Port s3/p4 Statistics - Ethernet Out Packets	R	Uinst32
0458	2	Port s4/p1 Statistics - Ethernet Out Packets	R	Uinst32
045A	2	Port s4/p2 Statistics - Ethernet Out Packets	R	Uinst32
045C	2	Port s4/p3 Statistics - Ethernet Out Packets	R	Uinst32

Address	#Registers	Description (Reference Table in UI)	R/W	Format
045E	2	Port s4/p4 Statistics - Ethernet Out Packets	R	Uinst32
0460	2	Port s5/p1 Statistics - Ethernet Out Packets	R	Uinst32
0462	2	Port s5/p2 Statistics - Ethernet Out Packets	R	Uinst32
0464	2	Port s5/p3 Statistics - Ethernet Out Packets	R	Uinst32
0466	2	Port s5/p4 Statistics - Ethernet Out Packets	R	Uinst32
0468	2	Port s6/p1 Statistics - Ethernet Out Packets	R	Uinst32
046A	2	Port s6/p2 Statistics - Ethernet Out Packets	R	Uinst32
046C	2	Port s6/p3 Statistics - Ethernet Out Packets	R	Uinst32
046E	2	Port s6/p4 Statistics - Ethernet Out Packets	R	Uinst32
0470	2	Port s7/p1 Statistics - Ethernet Out Packets	R	Uinst32
0472	2	Port s7/p2 Statistics - Ethernet Out Packets	R	Uinst32
0474	2	Port s8/p1 Statistics - Ethernet Out Packets	R	Uinst32
0476	2	Port s8/p2 Statistics - Ethernet Out Packets	R	Uinst32
0480	2	Port s1/p1 Statistics - Ethernet In Packets	R	Uinst32
0482	2	Port s1/p2 Statistics - Ethernet In Packets	R	Uinst32
0484	2	Port s1/p3 Statistics - Ethernet In Packets	R	Uinst32
0486	2	Port s1/p4 Statistics - Ethernet In Packets	R	Uinst32
0488	2	Port s2/p1 Statistics - Ethernet In Packets	R	Uinst32
048A	2	Port s2/p2 Statistics - Ethernet In Packets	R	Uinst32
048C	2	Port s2/p3 Statistics - Ethernet In Packets	R	Uinst32
048E	2	Port s2/p4 Statistics - Ethernet In Packets	R	Uinst32
0490	2	Port s3/p1 Statistics - Ethernet In Packets	R	Uinst32
0492	2	Port s3/p2 Statistics - Ethernet In Packets	R	Uinst32
0494	2	Port s3/p3 Statistics - Ethernet In Packets	R	Uinst32
0496	2	Port s3/p4 Statistics - Ethernet In Packets	R	Uinst32
0498	2	Port s4/p1 Statistics - Ethernet In Packets	R	Uinst32
049A	2	Port s4/p2 Statistics - Ethernet In Packets	R	Uinst32
049C	2	Port s4/p3 Statistics - Ethernet In Packets	R	Uinst32
049E	2	Port s4/p4 Statistics - Ethernet In Packets	R	Uinst32
04A0	2	Port s5/p1 Statistics - Ethernet In Packets	R	Uinst32
04A2	2	Port s5/p2 Statistics - Ethernet In Packets	R	Uinst32
04A4	2	Port s5/p3 Statistics - Ethernet In Packets	R	Uinst32
04A6	2	Port s5/p4 Statistics - Ethernet In Packets	R	Uinst32
04A8	2	Port s6/p1 Statistics - Ethernet In Packets	R	Uinst32

Address	#Registers	Description (Reference Table in UI)	R/W	Format
04AA	2	Port s6/p2 Statistics - Ethernet In Packets	R	Uinst32
04AC	2	Port s6/p3 Statistics - Ethernet In Packets	R	Uinst32
04AE	2	Port s6/p4 Statistics - Ethernet In Packets	R	Uinst32
04B0	2	Port s7/p1 Statistics - Ethernet In Packets	R	Uinst32
04B2	2	Port s7/p2 Statistics - Ethernet In Packets	R	Uinst32
04B4	2	Port s8/p1 Statistics - Ethernet In Packets	R	Uinst32
04B6	2	Port s8/p2 Statistics - Ethernet In Packets	R	Uinst32
04C0	2	Port s1/p1 Statistics - Ethernet Out Packets	R	Uinst32
04C2	2	Port s1/p2 Statistics - Ethernet Out Packets	R	Uinst32
04C4	2	Port s1/p3 Statistics - Ethernet Out Packets	R	Uinst32
04C6	2	Port s1/p4 Statistics - Ethernet Out Packets	R	Uinst32
04C8	2	Port s2/p1 Statistics - Ethernet Out Packets	R	Uinst32
04CA	2	Port s2/p2 Statistics - Ethernet Out Packets	R	Uinst32
04CC	2	Port s2/p3 Statistics - Ethernet Out Packets	R	Uinst32
04CE	2	Port s2/p4 Statistics - Ethernet Out Packets	R	Uinst32
04D0	2	Port s3/p1 Statistics - Ethernet Out Packets	R	Uinst32
04D2	2	Port s3/p2 Statistics - Ethernet Out Packets	R	Uinst32
04D4	2	Port s3/p3 Statistics - Ethernet Out Packets	R	Uinst32
04D6	2	Port s3/p4 Statistics - Ethernet Out Packets	R	Uinst32
04D8	2	Port s4/p1 Statistics - Ethernet Out Packets	R	Uinst32
04DA	2	Port s4/p2 Statistics - Ethernet Out Packets	R	Uinst32
04DC	2	Port s4/p3 Statistics - Ethernet Out Packets	R	Uinst32
04DE	2	Port s4/p4 Statistics - Ethernet Out Packets	R	Uinst32
04E0	2	Port s5/p1 Statistics - Ethernet Out Packets	R	Uinst32
04E2	2	Port s5/p2 Statistics - Ethernet Out Packets	R	Uinst32
04E4	2	Port s5/p3 Statistics - Ethernet Out Packets	R	Uinst32
04E6	2	Port s5/p4 Statistics - Ethernet Out Packets	R	Uinst32
04E8	2	Port s6/p1 Statistics - Ethernet Out Packets	R	Uinst32
04EA	2	Port s6/p2 Statistics - Ethernet Out Packets	R	Uinst32
04EC	2	Port s6/p3 Statistics - Ethernet Out Packets	R	Uinst32
04EE	2	Port s6/p4 Statistics - Ethernet Out Packets	R	Uinst32
04F0	2	Port s7/p1 Statistics - Ethernet Out Packets	R	Uinst32
04F2	2	Port s7/p2 Statistics - Ethernet Out Packets	R	Uinst32
04F4	2	Port s8/p1 Statistics - Ethernet Out Packets	R	Uinst32

Address	#Registers	Description (Reference Table in UI)	R/W	Format
04F6	2	Port s8/p2 Statistics - Ethernet Out Packets	R	Uinst32

Serial Statistics

The following data is mapped to the *uartPortStatus* table:

Address	#Registers	Description (Reference Table in UI)	R/W	Format
0600	2	Port 1 Statistics – Serial In characters	R	Uint32
0602	2	Port 2 Statistics – Serial In characters	R	Uint32
0604	2	Port 3 Statistics – Serial In characters	R	Uint32
0606	2	Port 4 Statistics – Serial In characters	R	Uint32
0640	2	Port 1 Statistics – Serial Out characters	R	Uint32
0642	2	Port 2 Statistics – Serial Out characters	R	Uint32
0644	2	Port 3 Statistics – Serial Out characters	R	Uint32
0646	2	Port 4 Statistics – Serial Out characters	R	Uint32
0680	2	Port 1 Statistics – Serial In Packets	R	Uint32
0682	2	Port 2 Statistics – Serial In Packets	R	Uint32
0684	2	Port 3 Statistics – Serial In Packets	R	Uint32
0686	2	Port 4 Statistics – Serial In Packets	R	Uint32
06C0	2	Port 1 Statistics – Serial Out Packets	R	Uint32
06C2	2	Port 2 Statistics – Serial Out Packets	R	Uint32
06C4	2	Port 3 Statistics – Serial Out Packets	R	Uint32
06C6	2	Port 4 Statistics – Serial Out Packets	R	Uint32

Section 1.8.3

ModBus Memory Formats

The following ModBus memory formats are supported by Siemens.

CONTENTS

- Section 1.8.3.1, “Text”
- Section 1.8.3.2, “Cmd”
- Section 1.8.3.3, “Uint16”
- Section 1.8.3.4, “Uint32”
- Section 1.8.3.5, “PortCmd”
- Section 1.8.3.6, “Alarm”
- Section 1.8.3.7, “PSStatusCmd”

- Section 1.8.3.8, “TruthValues”

Section 1.8.3.1
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).

Section 1.8.3.2
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

Section 1.8.3.3
Uint16

The Uint16 format describes a Standard ModBus 16 bit register.

Section 1.8.3.4
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.

Section 1.8.3.5
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 locatoin 0x03FE.

0x04	0x03	0xFE	0x00	0x02

The response depends on how many parts 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

Section 1.8.3.6

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.

Section 1.8.3.7

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.

Section 1.8.3.8

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.

Section 1.9

SSH and SSL Keys and Certificates

The following describes the SSH and SSL keys and certificates in RS900, along with the certificate and SSH key requirements.

CONTENTS

- Section 1.9.1, “Certificate and Keys Life Cycle”
- Section 1.9.2, “Certificate and Key Requirements”

Section 1.9.1

Certificate and Keys Life Cycle

Each RUGGEDCOM ROS device is shipped with an SSL certificate and RSA key pair, and a DSA host key pair for SSH, 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
SSH is not supported in Non-Controlled (NC) versions of 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.

- **Default**
  A default certificate and SSL/SSH keys are built in to RUGGEDCOM ROS and are common across all RUGGEDCOM ROS units sharing the same firmware image. In the event that valid SSL certificate or SSL/SSH key files are not available on the device (as is usually only the case when upgrading from an old ROS version that does not support user-configurable keys and therefore does was not shipped with unique, factory-generated keys), the default certificate and keys are put into service *temporarily* so that SSH and SSL (https) sessions can be served until generated or provisioned keys are available.
- **Auto-Generated**
  If a default SSL certificate and SSL/SSH keys are in use, RUGGEDCOM ROS immediately begins to generate a unique certificate and SSL/SSH keys for the device in the background. This process may take several minutes to complete depending on the requested key length and how busy the device is at the time. If a custom certificate and keys are loaded while auto-generated certificates and keys are being generated, the generator will abort and the custom certificate and keys and will be used.
- **User-Generated (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 key pair corresponding to the SSL certificate must be appended to the certificate in the `ssl.crt` *file.*

Section 1.9.2

Certificate and Key Requirements

For SSL, controlled versions of RUGGEDCOM ROS require an X.509 certificate in standard PEM format and an RSA or ECC key pair. The certificate may be self-signed or signed by a separate authority. The RSA key must be 1024, 2048 or 3072 bits in length; the ECC key must be 192, 224, 256, 384 or 521 bits in length.

Non-Controlled (NC) versions of RUGGEDCOM ROS require an X.509 certificate in standard PEM format and an RSA key pair. The RSA key must be between 512 and 2048 bits in length.

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-----
MIICXAIBAAKBgQC3xOHodmmPghN1uWuFs9WdURkT9Ngjh7ded8BRa1PP3xUFzYSp
UIq5QB2zU0UsHE0fGRWqYr8GA4r59KIDhhV5J2D/dIL9qCGklWNPBamZCVu+4N5M
5L//Ga8N5lv3AbGSfEsiiyA38uNNR5B6QzpXuTbEBUq84hlD4wDiL78eKwIDAQAB
AoGBAI2CXHuHg23wuk9zAusoOhw0MN1/M1jYz0k9aajIvvdZT3Tyd29yCADy8GwA
eUmoWXLS/C4CcBqPa9til8ei3rDn/w8dveVHsi9FXjtVSYqN+ilKw+moMAjZy4kN
/kpdpHMohwv/909VWR1AZbr+YTxaG/++tKl5bqXnZl4wHF8xAkEA5vwut8USRg2/
TndOt1e8ILEQNHvHQdQr2et/xNH4ZEo7mqot6skkCD1xmxA6XG64hR3BfxFSZcew
Wr4SOFGCtQJBAMurr5FYPJRFGzPM3HwcpAaaMIUtPwNyTtTjywlYcUI7iZVVfbdx
4B7qOadPybTg7wqUrGVkPSzzQelz9YCSSV8CQFqpIsEYhbqfTLZEl83YjsuaE801
xBivaWLIT0b2TvM2O7zSDOG5fv4I990v+mgrQRtmeXshVmEChtKnBcm7HH0CQE6B
2WUfLArDMJ8hAoRczeU1nipXrIh5kWWCgQsTKmUrafdEQvdpT8ja5GpX2Rp98eaU
NHfI0cP36JpCdome2eUCQDZN9OrTgPfeDIXzyOiUUwFlzS1idkUGL9nH86iuPnd7
WVF3rV9Dse30sVEk63Yky8uKUy7yPUNWldG4U5vRKmY=
-----END RSA PRIVATE KEY-----
```


For SSH, RUGGEDCOM ROS requires a DSA or RSA host key pair in PEM format. The key must be 1024, 2048 or 3072 bits in length for Controlled versions. The key file is uploaded to the `ssh.keys` flash file on the device.

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


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


For more information about encryption key management, refer to Section 1.2, “Security Recommendations and Considerations” .

2 Using ROS

This chapter describes how to use the RUGGEDCOM ROS interface.

CONTENTS

- Section 2.1, “Connecting to ROS”
- Section 2.2, “Logging In”
- Section 2.3, “Logging Out”
- Section 2.4, “Using the Web Interface”
- Section 2.5, “Using the Console Interface”
- Section 2.6, “Using the Command Line Interface”
- Section 2.7, “Selecting Ports in RUGGEDCOM ROS ”
- Section 2.8, “Managing the Flash File System”
- Section 2.9, “Accessing BIST Mode”
- Section 2.10, “Managing SSH Public Keys”

Section 2.1

Connecting to ROS

This section describes the various methods for connecting the device.

CONTENTS

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

Section 2.1.1

Connecting Directly

RUGGEDCOM ROS can be accessed through a direct RS-232 serial console connection for management and troubleshooting purposes. A console connection provides access to the console interface and CLI.

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 RS-232 serial console port on the device. For more information about the RS-232 serial console port, refer to the *RS900 Installation Guide*.

> **NOTE**
> *The baud rate for the device is printed on the chassis exterior near the RS-232 serial console port.*

2. Configure the workstation as follows:
   - Speed (baud): 57600
   - Data Bits: 8
   - Parity: None
   - Flow Control: Off
   - Terminal ID: VT100
   - Stop Bit: 1
3. Connect to the device. Once the connection is established, the login form appears. For more information about logging in to the device, refer to Section 2.2, "Logging In" .

Section 2.1.2

Connecting via the Network

RUGGEDCOM ROS can be accessed over the network either through a Web browser, terminal or a 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 the section called "System Requirements" .

   IMPORTANT!
   Upon connecting to the device, some Web browsers may report the Web server's certificate cannot be verified against any known certificates. This is expected behavior, and it is safe to instruct the browser to accept the certificate. Once the certificate is accepted, all communications with the Web server through that browser will be secure.
3. In the address bar, type the IP address for the port that is connected to the network. For example, to access the device using its factory default IP address, type **`https://192.168.0.1`** and press **Enter**. Once the connection is established, the login screen for the Web interface appears.

   For more information about logging in to the device, refer to Section 2.2, "Logging In" . For more information about the Web interface, refer to Section 2.4, "Using the Web Interface" .

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* *Section 3.9, "Configuring IP Services"* .

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 Section 2.2, "Logging In" .

Section 2.2

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 Section 2.1, "Connecting to ROS" .

   Once the connection is established, the login form appears.

Figure 2: SSH Login Screen (Console Interface)

1. User Name Box **2.** Password Box

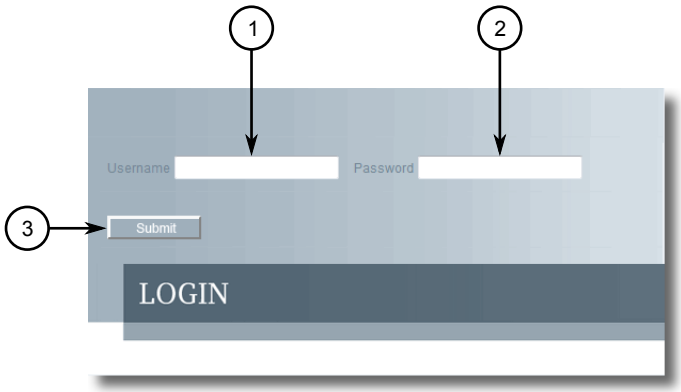


Figure 3: Login Screen (Web Interface)

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

NOTE
The following default usernames and passwords are set on the device for each user type:

Guest	***Operator***	***Admin***
Username: guest	*Username: operator*	*Username: admin*
Password: guest	*Password: operator*	*Password: admin*

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

For more information about changing passwords, refer to *Section 4.3, "Configuring Passwords"*.

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

Section 2.3
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**.

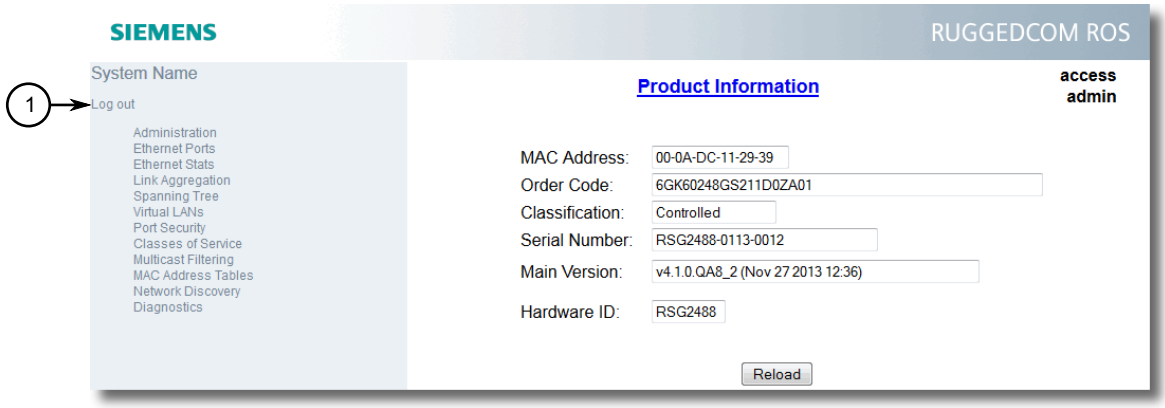


Figure 4: Web Interface (Example)

1. Logout

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.

Section 2.4

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.

Figure 5: Web Interface Layout (Example)

1. Top Frame **2.** Side Frame **3.** Main Frame

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 Section 2.3, "Logging Out" .
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 Section 4.6, "Managing Alarms" .

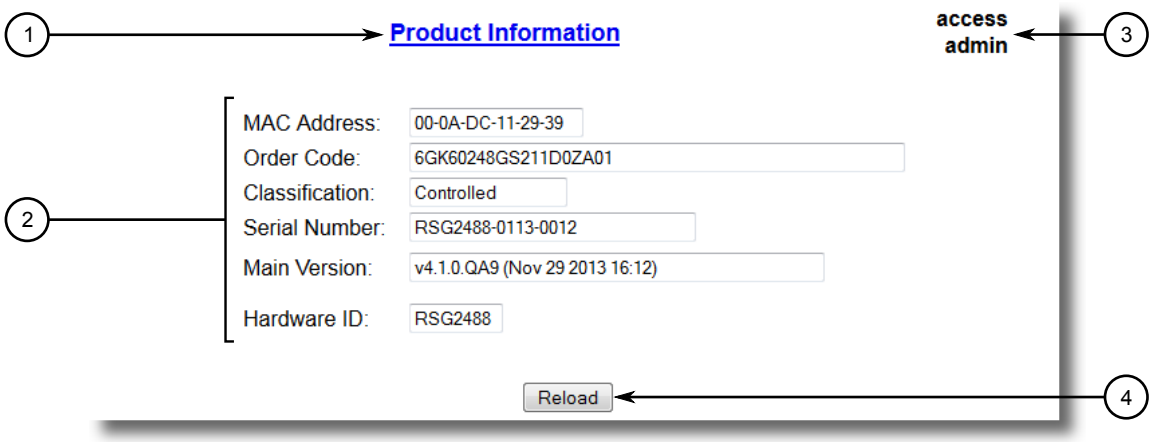


Figure 6: Elements of a Typical Screen (Example)

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

NOTE
If desired, the web interface can be disabled. For more information, refer to *Section 4.5, "Enabling/Disabling the Web Interface"*.

Section 2.5

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 *Section 3.9, "Configuring IP Services"*.

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.

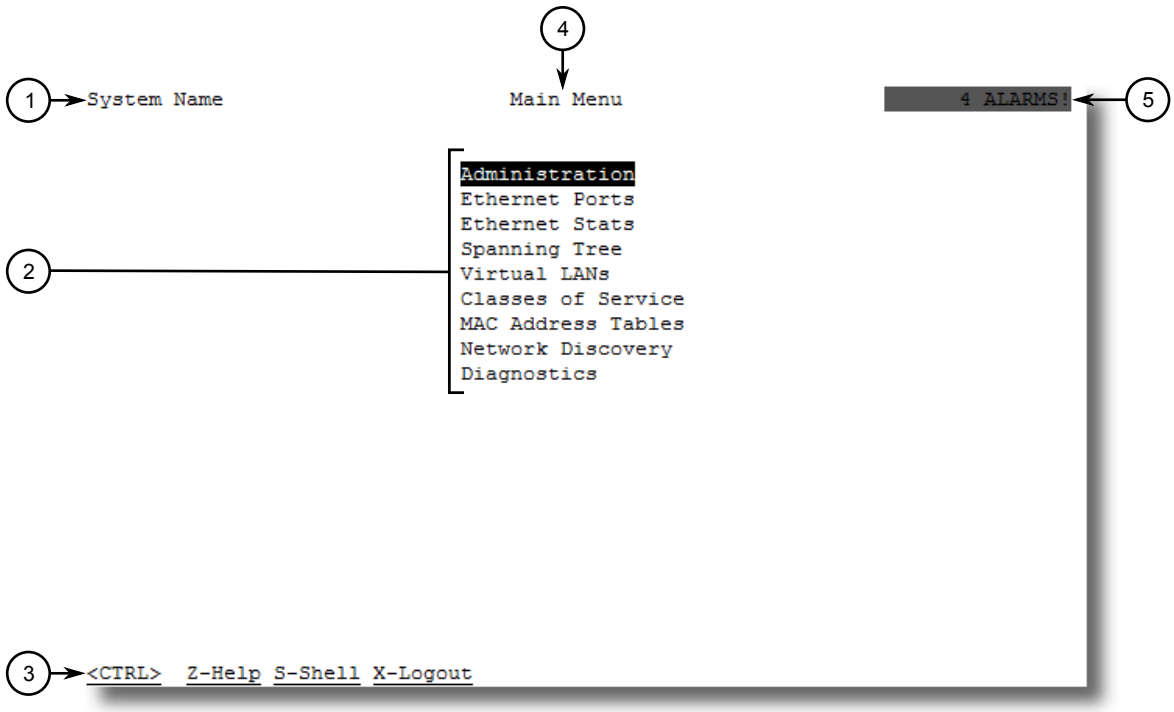


Figure 7: Console Interface (Example)

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

NOTE
The system identifier is user configurable. For more information about setting the system name, refer to *Section 4.1, "Configuring the System Information"*.

Navigating the Interface

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

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

Configuring Parameters

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

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

Commands

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

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

Section 2.6

Using the Command Line Interface

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

CONTENTS

- Section 2.6.1, “Available CLI Commands”
- Section 2.6.2, “Tracing Events”
- Section 2.6.3, “Executing Commands Remotely via RSH”
- Section 2.6.4, “Using SQL Commands”

Section 2.6.1

Available CLI Commands

The following commands are available at the command line:

Command	Description
`alarms` `all`	Displays a list of available alarms. Optional and/or required parameters include: • `all` displays all available alarms
`arp`	Displays the IP to MAC address resolution table.
`clearalarms`	Clears all alarms.
`clearethstats` `[ all |` *`port`* `]`	Clears Ethernet statistics for one or more ports. Optional and/or required parameters include: • `all` clears statistics for all ports

Command	Description
	• *port* is a comma separated list of port numbers (e.g. 1,3-5,7)
clearlogs	Clears the system and crash logs.
clrcblstats [all | *port*]	Clears cable diagnostics statistics for one or more ports. Optional and/or required parameters include: • all clears statistics for all ports • *port* is a comma separated list of port numbers (e.g. 1,3-5,7)
clrstpstats	Clears all spanning tree statistics.
cls	Clears the screen.
dir	Prints the directory listing.
exit	Terminates the session.
factory	Enables factory mode, which includes several factory-level commands used for testing and troubleshooting. Only available to admin users. **CAUTION!** *Misuse of the factory commands may corrupt the operational state of device and/or may permanently damage the ability to recover the device without manufacturer intervention.*
flashfiles { info *filename* | defrag }	A set of diagnostic commands to display information about the Flash filesystem and to defragment Flash memory. Optional and/or required parameters include: • info *filename* displays information about the specified file in the Flash file system • defrag defragments files in the Flash file system For more information about the **flashfiles** command, refer to Section 2.8, "Managing the Flash File System" .
flashleds *timeout*	Flashes the LED indicators on the device for a specified number of seconds. Optional and/or required parameters include: • *timeout* is the number of seconds to flash the LED indicators. To stop the LEDs from flashing, set the timeout period to 0 (zero).
fpgacmd	Provides access to the FPGA management tool for troubleshooting time synchronization.
help *command*	Displays a brief description of the specified command. If no command is specified, it displays a list of all available commands, including a description for each. Optional and/or required parameters include: • *command* is the command name.
ipconfig	Displays the current IP address, subnet mask and default gateway. This command provides the only way of determining these values when DHCP is used.
loaddflts	Loads the factory default configuration.
login	Logs in to the shell.
logout	Logs out of the shell.
logs	Displays syslog entries in CLI shell.
ping *address* { *count* | *timeout* }	Sends an ICMP echo request to a remotely connected device. For each reply received, the round trip time is displayed. Use this command to verify connectivity to the next connected device. It is a useful tool for testing commissioned links. This command also includes the ability to send a specific number of pings with a specified time for which to wait for a response. Optional and/or required parameters include:

Command	Description
	• *address* is the target IP address. • *count* is the number of echo requests to send. The default is 4. • *timeout* is the time in milliseconds to wait for each reply. The range is 2 to 5000 seconds. The default is 300 milliseconds. **NOTE** *The device to be pinged must support ICMP echo. Upon commencing the ping, an ARP request for the MAC address of the device is issued. If the device to be pinged is not on the same network as the device pinging the other device, the default gateway must be programmed.*
purgemac	Purges the MAC Addrtess table.
random	Display seeds or random numbers.
reset	Perform a hard reset of the switch.
resetport { all | *ports* }	Resets one or more Ethernet ports, which may be useful for forcing re-negotiation of speed and duplex, or in situations where the link partner has latched into an inappropriate state. Optional and/or required parameters include: • all resets all ports • *ports* is a comma separated list of port numbers (e.g. 1,3-5,7)
rmon	Displays the names of all RMON alarm eligible objects.
route	Displays the gateway configuration.
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. Optional and/or required parameters include: • *port* is the port number for which the data are required • base displays the base information • alarms displays alarms and warning flags • diag displays measured data • calibr displays calibration data for external calibration • thr displays thresholds data • all displays all diagnostic data
sql { default | delete | help | info | insert | save | select | update }	Provides an SQL-like interface for manipulating all system configuration and status parameters. All commands, clauses, table, and column names are case insensitive. Optional and/or required parameters include: • default sets all records in a table(s) to factory defaults • delete allows for records to be deleted from a table • help provides a brief description for any SQL command or clause • info displays a variety of information about the tables in the database • insert enables new records to be inserted into a table • save saves the database to non-volatile memory storage • select queries the dtabase and displays selected records • update enable existing records in a table to be updated For more information about the **sql** command, refer to Section 2.6.4, "Using SQL Commands" .
sshkeygen *keytype* *N*	Generates new SSH keys in ssh.keys. Optional and/or required parameters include: • *keytype* is the type of key, either rsa or dsa • *N* is the number of bits in length. The allowable sizes are 1024, 2048 or 3072

Command	Description
sshpubkey	List, remove and update key entries in sshpub.keys file.
sslkeygen *keytype* *N*	Generates a new SSL certificate in `ssl.crt`. Optional and/or required parameters include: • *keytype* is the type of key, either rsa or ecc • *N* is the number of bits in length. For RSA keys, the allowable sizes are 1024, 2048 or 3072. For ECC keys, the allowable sizes are 192, 224, 256, 384, or 521.
telnet *dest*	Opens a telnet session. Press **Ctrl-C** to close the session. Optional and/or required parameters include: • *dest* is the server's IP address
tftp { *dest* | *cmd* | *fsource* | *fdest* }	Opens a TFTP session. Press **Ctrl-C** to close the session. Optional and/or required parameters include: • *dest* is the remote TFTP server's IP address • *cmd* is either **put** (upload) or **get** (download) • *fsource* is the source filename • *fdest* is the destination filename
trace	Starts event tracing. Run **trace ?** for more help.
type *filename*	Displays the contents of a text file. Optional and/or required parameters include: • *filename* is the name of the file to be read
version	Prints the software version.
xmodem { send | receive } *filename*	Opens an XModem session. Optional and/or required parameters include: • send sends the file to the client. • receive receives the file from the client. • *filename* is the name of the file to be read.

Section 2.6.2

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 Section 2.6, “Using the Command Line Interface” .
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
```

Section 2.6.3

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.*

Section 2.6.4

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* *Section 2.6.1, "Available CLI Commands"* .

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

CONTENTS

- Section 2.6.4.1, "Finding the Correct Table"
- Section 2.6.4.2, "Retrieving Information"
- Section 2.6.4.3, "Changing Values in a Table"
- Section 2.6.4.4, "Resetting a Table"
- Section 2.6.4.5, "Using RSH and SQL"

Section 2.6.4.1

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
```

Section 2.6.4.2

Retrieving Information

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

Retrieving Information from a Table

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

```
sql select from  table
```

Where:

- *table* is the name of the table

Example:

```
>sql select from ipAddrtable

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

1 records selected
```

Retrieving Information About a Parameter from a Table

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

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

```
sql select  parameter  from  table
```

Where:

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

Example:

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

IP Address
192.168.0.1

1 records selected
```

Retrieving Information from a Table Using the *Where* Clause

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

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

Where:

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

Example:

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

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

4 records selected
```

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

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

Where:

- *`table`* is the name of the table
- *`parameter`* is the name of the parameter
- *`value`* is the value of the parameter

Example:

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

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

4 records selected
```

Section 2.6.4.3

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
```

Section 2.6.4.4
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

Section 2.6.4.5
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:\
```

Section 2.7
Selecting Ports in RUGGEDCOM ROS

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

Select a single port by specifying the port number:

```
2
```

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

```
1-4
```

Select multiple ports by defining a comma-separated list:

```
1,4,6,9
```

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

Section 2.8

Managing the Flash File System

The following section describes how to manage the flash file system.

CONTENTS

- Section 2.8.1, "Viewing a List of Flash Files"
- Section 2.8.2, "Viewing Flash File Details"
- Section 2.8.3, "Defragmenting the Flash File System"

Section 2.8.1

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 Section 2.6, "Using the Command Line Interface" .
2. Type **flashfiles**. A list of files currently in Flash memory is displayed, along with their locations and the amount of memory they consume. For example:

```
>flashfiles
-------------------------------------------------------------------
Filename              Base    Size  Sectors     Used
-------------------------------------------------------------------
boot.bin          00000000 110000    0-16   1095790
main.bin          00110000 140000   17-36   1258403
fpga.xsvf         00250000 010000   37-37     55882
syslog.txt        00260000 140000   38-57     19222
ssh.keys          003A0000 010000   58-58       915
ssl.crt           003B0000 010000   59-59      1970
banner.txt        003C0000 010000   60-60       256
crashlog.txt      003D0000 010000   61-61       256
config.bak        003E0000 010000   62-62     15529
config.csv        003F0000 008000   63-63     15529
factory.txt       003FC000 004000   66-66       407
-------------------------------------------------------------------
```

Section 2.8.2

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 Section 2.6, "Using the Command Line Interface" .
2. Display information about a file by typing:

```
flashfiles info  filename
```

Where:

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

Details, similar to the following, are displayed.

```
>flashfiles info main.bin

Flash file information for main.bin:
Header version   : 4
Platform         : ROS-CF52

File name        : main.bin
Firmware version : v4.3.0
Build date       : Sep 27 2014 15:50
File length      : 2624659
Board IDs        :  3d
Header CRC       : 73b4
Header CRC Calc  : 73b4
Body CRC         : b441
Body CRC Calc    : b441
```

Section 2.8.3

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 Section 2.6, "Using the Command Line Interface" .
2. Defragment the flash memory by typing:

```
flashfiles defrag
```

Section 2.9

Accessing BIST Mode

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

CAUTION!
Mechanical hazard – risk of damage to the device. Excessive use of BIST functions may cause increase wear on the device, which may void the warranty. Avoid using BIST functions unless instructed by a Siemens Customer Support representative.

To access BIST mode, do the following:

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

1. Disconnect the device from the network.
2. Connect to RUGGEDCOM ROS through the RS-232 console connection and a terminal application. For more information, refer to Section 2.1.1, “Connecting Directly” .
3. Reset the device. For more information, refer to Section 3.12, “Resetting the Device” .
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.

Section 2.10

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.

CONTENTS

- Section 2.10.1, “Adding a Public Key”
- Section 2.10.2, “Viewing a List of Public Keys”
- Section 2.10.3, “Updating a Public Key”
- Section 2.10.4, “Deleting a Public Key”

Section 2.10.1

Adding a Public Key

Admin users can add one or more public keys to RUGGEDCOM ROS.

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 or 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/
GR24NrRJa0Lc7scNsWRgi0XulHuGrRLRB5RoQ39+spdig88Y8CqhRI49XJx7uLJe0Su3RvyNYz1jkdSwHq2hSZCpukJxJ6CK95Po/
sVa5Gq2gMaHowiYDSkcx+AJywzK/eM6i/jc125lRxFPdfkj74u+ob3PCvmIWz5z3WAJBrQU1IDPHDets511WMu8O9/
mAPZRwjqrWhRsqmcXZuv5oo54wIopCAZSo20SPzM2VmXFuUsEwDkvYMXLJK1koJPbDjH7yFFC7mwK2eMU/
oMFFn934cbO5N6etsJSvplYQ4pMCw6Ok8Q/bB5cPSOa/rAt bob@work
```

IMPORTANT!
*The content of the **sshaddpub.keys** file must follow the same syntax as the **sshpub.keys** file.*

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

There are two ways to update *sshpub.keys*. Users can either upload a locally-created file directly to the *sshpub.keys* file, which will replace the content in flash with the uploaded content. Or, users can upload a locally-created file to the *sshaddpub.keys* file, which will keep the existing entries in the *sshpub.keys* file and append the new entries.

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 Section 3.4, “Uploading/Downloading Files” .
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 Section 2.6, “Using the Command Line Interface” .

4. Check the system log to make sure the files were properly transferred. For more information about viewing the system log, refer to Section 3.5.1, "Viewing Local Logs" .

Section 2.10.2

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 Section 2.6, "Using the Command Line Interface" .
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.

Section 2.10.3

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 Section 2.6, "Using the Command Line Interface" .
2. At the CLI prompt, type:

```
sshpubkey list
```

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

3. Type the following commands to update the public keys:

Command	Description
sshpubkey update_id *current_ID new_ID*	Updates the ID of user public key. **NOTE** *The user public key ID must be a number between 0 and 9999.* • *current_ID* is the ID currently assigned to the public key • *new_ID* is the ID that will be used to identify the public key going forward
sshpubkey update_al *AL*	Updates the access level of a user public key. • *AL* is the access level (admin, operator or guest) of the public key to be updated
sshpubkey update_rs *RS*	Updates the revocation status (active, inactive) of a user public key. • *RS* is the revocation status of the public key to be updated
sshpubkey update_un *UN*	Updates the user name of a user public key. • *UN* is the user name of the public key to be updated

Section 2.10.4

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 Section 2.6, "Using the Command Line Interface" .
2. At the CLI prompt, type:

```
sshpubkey list
```

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

3. Type the following commands to delete the public key(s):

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

3 Device Management

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

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

CONTENTS

- Section 3.1, “Viewing Product Information”
- Section 3.2, “Viewing CPU Diagnostics”
- Section 3.3, “Restoring Factory Defaults”
- Section 3.4, “Uploading/Downloading Files”
- Section 3.5, “Managing Logs”
- Section 3.6, “Managing Ethernet Ports”
- Section 3.7, “Managing IP Interfaces”
- Section 3.8, “Managing IP Gateways”
- Section 3.9, “Configuring IP Services”
- Section 3.10, “Managing Remote Monitoring”
- Section 3.11, “Upgrading/Downgrading Firmware”
- Section 3.12, “Resetting the Device”
- Section 3.13, “Decommissioning the Device”

Section 3.1

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.

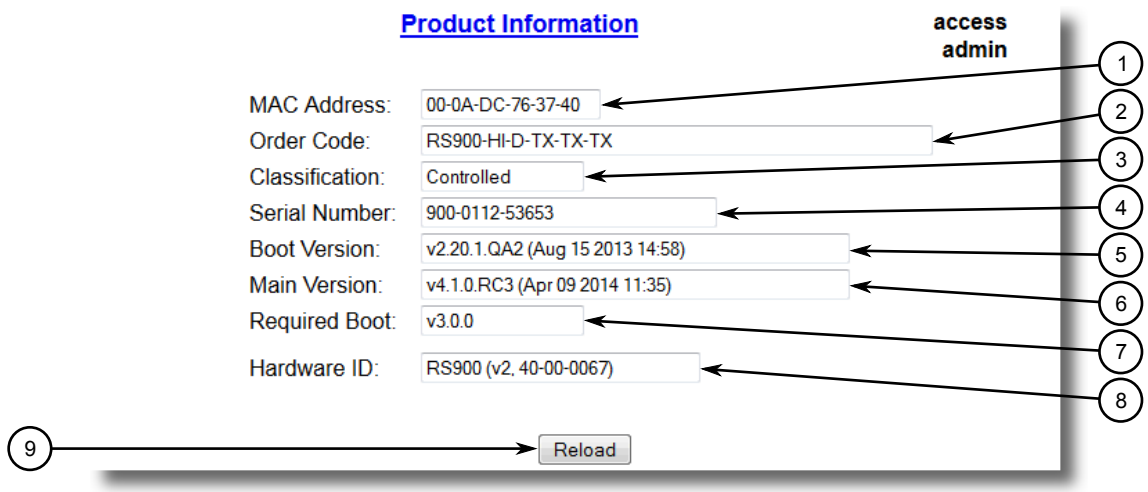


Figure 8: Product Information Form (Example)

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

This screen displays the following information:

Parameter	Description
MAC Address	**Synopsis:** ##-##-##-##-##-## where ## ranges 0 to FF Shows the unique MAC address of the device.
Order Code	**Synopsis:** Any 57 characters Shows the order code of the device.
Classification	**Synopsis:** Any 15 characters Provides system classification. The value *Controlled* indicates the main firmware is a Controlled release. The value *Non-Controlled* indicates the main firmware is a Non-Controlled release. 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:** Any 31 characters Shows the serial number of the device.
Boot Version	**Synopsis:** Any 47 characters Shows the version and the build date of the boot loader software.
Main Version	**Synopsis:** Any 47 characters Shows the version and build date of the main operating system software.
Required Boot	**Synopsis:** Any 15 characters Shows the minimum boot software loader version required by running main.
Hardware ID	**Synopsis:** { RSMCPU (40-00-0008 Rev B1), RSMCPU2 (40-00-0026 Rev A1), RS400 (40-00-0010 Rev B2), RMC30, RS900 (40-00-0025 Rev B1), RS900 (40-00-0032 Rev B1), RS1600M, RS400 (40-00-0010

Parameter	Description
	Rev C1), RSG2100, RS900G, RSG2200, RS969, RS900 (v2, 40-00-0066), RS900 (v2, 40-00-0067), , RS416 (40-00-0078), RMC30 (v2), RS930 (40-00-0089), RS969 (v2, 40-00-0090), RS910 (40-00-0091-001 Rev A), RS920L (40-00-0102-001 Rev A), RS940G (40-00-0097-000 Rev A), RSi80X series CPU board, RSG2300, RS416v2, ... } Shows the type, part number, and revision level of the hardware.

Section 3.2

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.

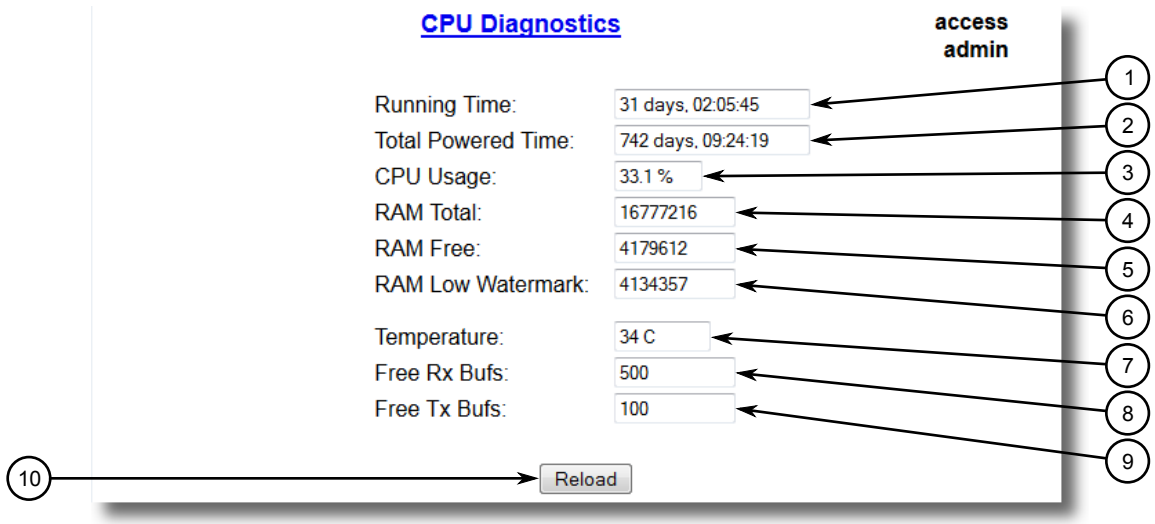


Figure 9: CPU Diagnostics Form

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

This screen displays the following information:

Parameter	Description
Running Time	**Synopsis:** DDDD days, HH:MM:SS The amount of time since the device was last powered on.
Total Powered time	**Synopsis:** DDDD days, HH:MM:SS The cumulative powered up time of the device.
CPU Usage	**Synopsis:** 0.0 to 100.0% The percentage of available CPU cycles used for device operation as measured over the last second.
RAM Total	**Synopsis:** 0 to 4294967295

Parameter	Description
	The total size of RAM in the system.
RAM Free	**Synopsis:** 0 to 4294967295 The total size of RAM still available.
RAM Low Watermark	**Synopsis:** 0 to 4294967295 The size of RAM that have never been used during the system runtime.
Temperature	**Synopsis:** -32768 to 32767 C The temperature on CPU board.
Free Rx Bufs	**Synopsis:** 0 to 4294967295 Free Rx Buffers.
Free Tx Bufs	**Synopsis:** 0 to 4294967295 Free Tx Buffers.

Section 3.3

Restoring Factory Defaults

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

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

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

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

- Time Zone
- DST Offset
- DST Rule

To restore factory defaults, do the following:

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

Figure 10: Load Factory Defaults Form

1. Defaults Choice List **2.** Apply Button **3.** Reload

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

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

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

3. Click **Apply**.

Section 3.4

Uploading/Downloading Files

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

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

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

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

Files that may need to be uploaded or downloaded include:

- `main.bin` – the main RUGGEDCOM ROS application firmware image
- `boot.bin` – the boot loader firmware image
- `fpga.xsvf` – the FPGA firmware binary image
- `config.csv` – the complete configuration database, in the form of a comma-delimited ASCII text file
- `factory.txt` – Contains the MAC address, order code and serial number. Factory data must be signed.
- `banner.txt` – contains text that appears on the login screen

CONTENTS

- Section 3.4.1, "Uploading/Downloading Files Using XMODEM"
- Section 3.4.2, "Uploading/Downloading Files Using a TFTP Client"
- Section 3.4.3, "Uploading/Downloading Files Using a TFTP Server"
- Section 3.4.4, "Uploading/Downloading Files Using an SFTP Server"

Section 3.4.1

Uploading/Downloading Files Using XMODEM

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

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

NOTE
Xmodem transfers can only be performed through the serial console, which is authenticated during login.

1. Establish a direct connection between the device and the host computer. For more information, refer to Section 2.1.1, "Connecting Directly" .
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 Section 2.6, "Using the Command Line Interface" .

   NOTE
   The `send` *option sends files to the host computer, while the* `receive` *option pulls files from the host computer.*

3. At the CLI prompt, type:

   ```
   xmodem [ send | receive ]  filename
   ```

   Where:

   - *`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.

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
```

Section 3.4.2

Uploading/Downloading Files Using a TFTP Client

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

> **IMPORTANT!**
> *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 direct connection between the device and a host computer. For more information, refer to Section 2.1.1, “Connecting Directly” .
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 Section 2.6, “Using the Command Line Interface” .
4. At the CLI prompt, type:

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

Where:

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

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

```
>tftp 10.0.0.1 get ROS-CF52_Main_v3.7.0.bin main.bin
TFTP CMD: main.bin transfer ok. Please wait, closing file ...
```

```
TFTP CMD: main.bin loading succesful.
```

Section 3.4.3

Uploading/Downloading Files Using a TFTP Server

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

IMPORTANT!
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.

IMPORTANT!
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 *Section 3.9, "Configuring IP Services"* .

1. Establish a direct connection between the device and the host computer. For more information, refer to Section 2.1.1, "Connecting Directly" .
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\ROD-CF52_Main_v3.7.0.bin main.bin
Transfer successful: 1428480 bytes in 4 seconds, 375617 bytes/s
```

Section 3.4.4

Uploading/Downloading Files Using an SFTP Server

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

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

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

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

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

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

```
user@host$ sftp admin@ros_ip
Connecting to ros_ip...
admin@ros_ip's password:
sftp> put ROS-CF52_Main_v3-7-0.bin main.bin
Uploading ROS-CF52_Main_v3-7-0.bin to /main.bin
ROS-CF52_Main_v3-7-0.bin 100% 2139KB 48.6KB/s 00:44
sftp>
```

Section 3.5

Managing Logs

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

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

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

CONTENTS

- Section 3.5.1, “Viewing Local Logs”
- Section 3.5.2, “Clearing Local Logs”
- Section 3.5.3, “Configuring the Local System Log”
- Section 3.5.4, “Managing Remote Logging”

Section 3.5.1

Viewing Local 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 Section 3.4, “Uploading/Downloading Files” .

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

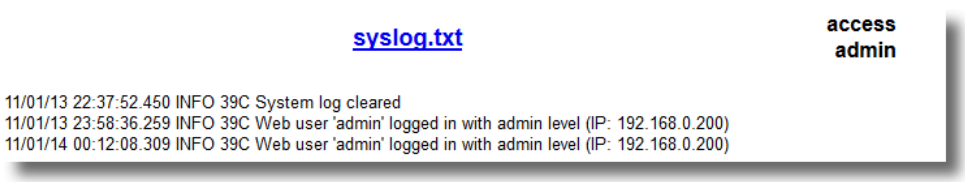


Figure 11: syslog.txt Form

Section 3.5.2

Clearing Local 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.

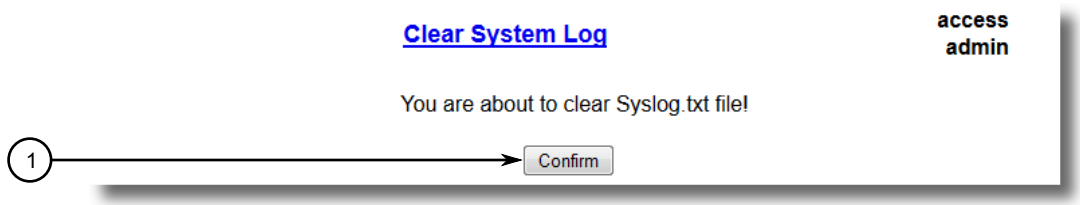


Figure 12: Clear System Log Form

1. Confirm Button

2. Click **Confirm**.

Section 3.5.3

Configuring the Local System Log

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

> **NOTE**
> *For maximum reliability, use remote logging. For more information, refer to* *Section 3.5.4, "Managing Remote Logging"* .

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

Figure 13: Local Syslog Form

1. Local Syslog Level **2.** Apply Button **3.** Reload Button

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

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

3. Click **Apply**.

Section 3.5.4

Managing Remote Logging

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

The remote syslog protocol, defined in RFC 3164, is a UDP/IP-based transport that enables the device to send event notification messages across IP networks to event message collectors, also known as syslog servers. The protocol is designed to simply transport these event messages from the generating device to the collector(s).

CONTENTS

- Section 3.5.4.1, “Configuring the Remote Syslog Client”
- Section 3.5.4.2, “Viewing a List of Remote Syslog Servers”
- Section 3.5.4.3, “Adding a Remote Syslog Server”
- Section 3.5.4.4, “Deleting a Remote Syslog Server”

Section 3.5.4.1

Configuring the Remote Syslog Client

To configure the remote syslog client, do the following:

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

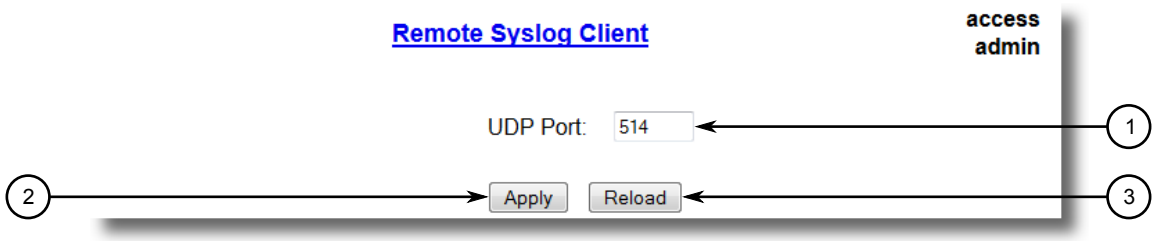


Figure 14: Remote Syslog Client Form

1. UDP Port **2.** Apply Button **3.** Reload Button

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

Parameter	Description
UDP Port	**Synopsis:** 1025 to 65535 or { 514 } **Default:** 514 The local UDP port through which the client sends information to the server(s).

3. Click **Apply**.

Section 3.5.4.2

Viewing a List of Remote Syslog Servers

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

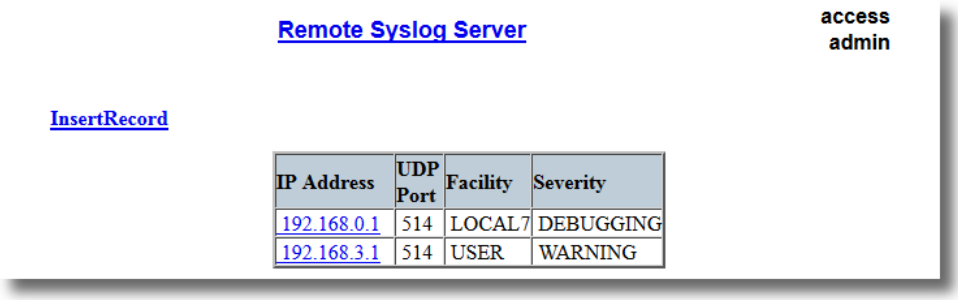


Figure 15: Remote Syslog Server Table

If remote syslog servers have not been configured, add the servers as needed. For more information, refer to Section 3.5.4.3, “Adding a Remote Syslog Server” .

Section 3.5.4.3

Adding a Remote Syslog Server

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

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

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

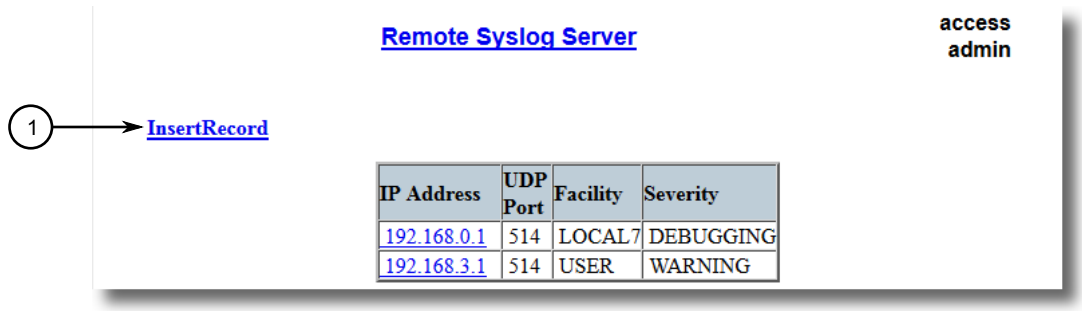


Figure 16: Remote Syslog Server Table

1. InsertRecord

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

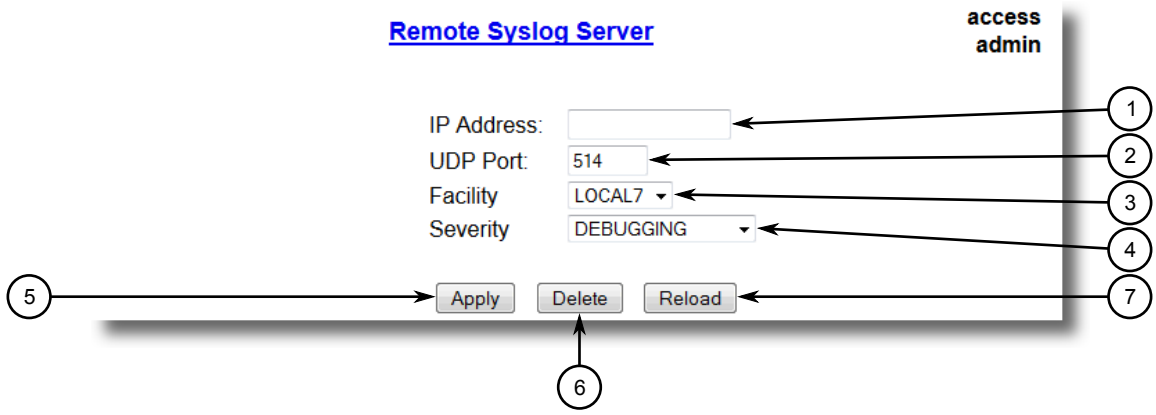


Figure 17: Remote Syslog Server Form

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

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

Parameter	Description
IP Address	**Synopsis:** ###.###.###.### where ### ranges from 0 to 255 Syslog server IP Address.
UDP Port	**Synopsis:** 1025 to 65535 or { 514 }

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

4. Click **Apply**.

Section 3.5.4.4

Deleting a Remote Syslog Server

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

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

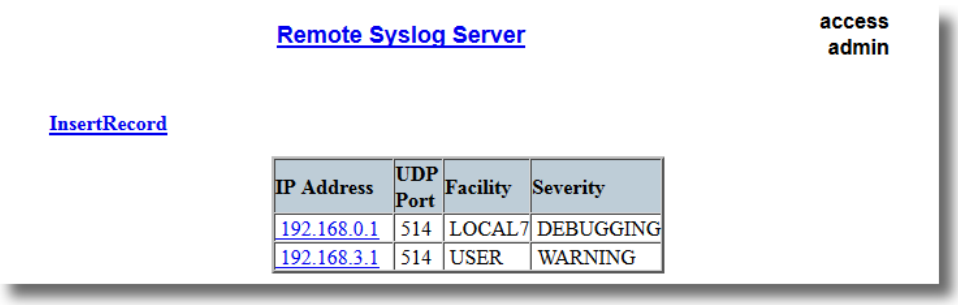


Figure 18: Remote Syslog Server Table

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

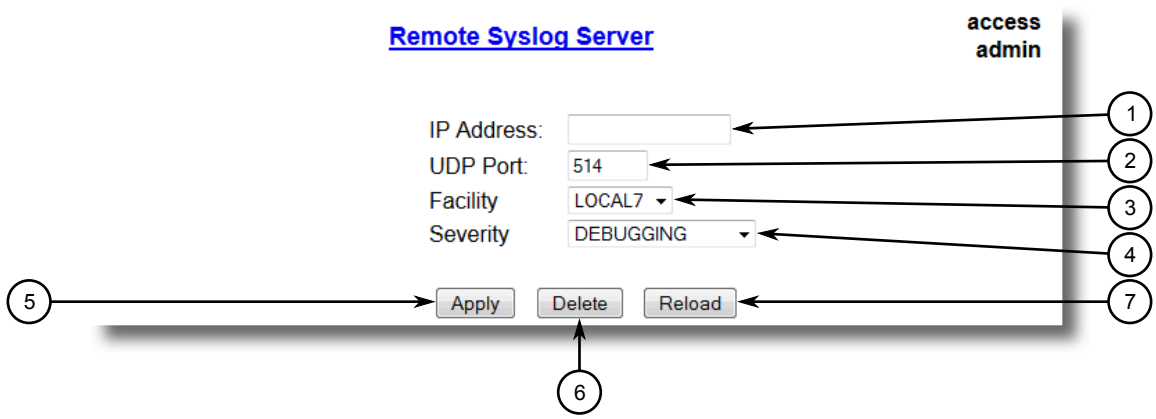


Figure 19: Remote Syslog Server Form

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

3. Click **Delete**.

Section 3.6

Managing Ethernet Ports

The following section describes how to set up and manage Ethernet ports.

> **NOTE**
> *For information about configuring remote monitoring for Ethernet ports, refer to Section 3.10, "Managing Remote Monitoring".*

CONTENTS

- Section 3.6.1, "Controller Protection Through Link Fault Indication (LFI)"
- Section 3.6.2, "Viewing the Status of Ethernet Ports"
- Section 3.6.3, "Viewing Statistics for All Ethernet Ports"
- Section 3.6.4, "Viewing Statistics for Specific Ethernet Ports"
- Section 3.6.5, "Clearing Statistics for Specific Ethernet Ports"
- Section 3.6.6, "Configuring an Ethernet Port"
- Section 3.6.7, "Configuring Port Rate Limiting"
- Section 3.6.8, "Configuring Port Mirroring"
- Section 3.6.9, "Configuring Link Detection"
- Section 3.6.10, "Detecting Cable Faults"

- Section 3.6.11, “Resetting Ethernet Ports”

Section 3.6.1

Controller Protection Through Link Fault Indication (LFI)

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

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

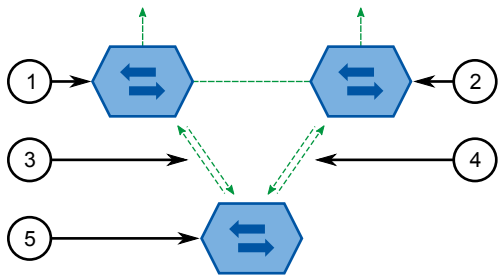


Figure 20: Example

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

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

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

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

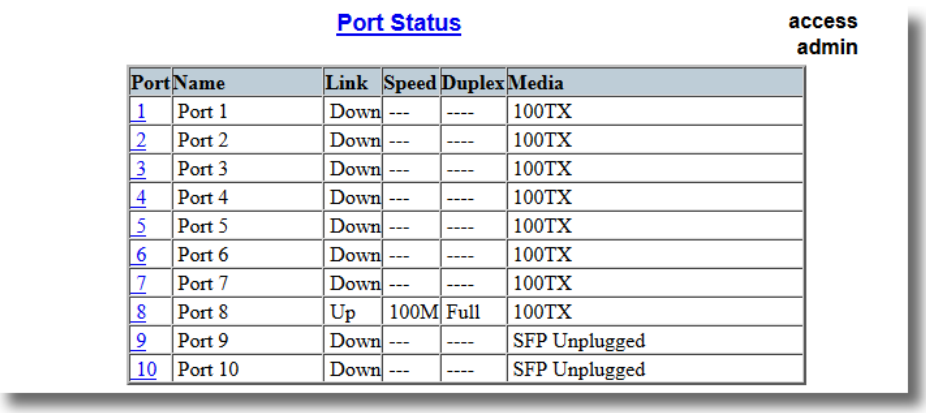
> **IMPORTANT!**
> *If both link partners have the LFI feature, it **must not** be enabled on both sides of the link. If it is enabled on both sides, the link will never be established, as each link partner will be waiting for the other to transmit a link signal.*

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).

Section 3.6.2

Viewing the Status of Ethernet Ports

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



Port Status

access
admin

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

Figure 21: Port Status Table

This table displays the following information:

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

Section 3.6.3

Viewing Statistics for All Ethernet Ports

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

Ethernet Statistics

access admin

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

Figure 22: Ethernet Statistics Table

This table displays the following information:

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

Section 3.6.4

Viewing Statistics for Specific Ethernet Ports

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

Ethernet Port Statistics access admin

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

Figure 23: Ethernet Port Statistics Table

This table displays the following information:

Parameter	Description
Port	**Synopsis:** 1 to maximum port number The port number as seen on the front plate silkscreen of the switch.
InOctets	**Synopsis:** 0 to 18446744073709551615 The number of octets in received good packets (Unicast+Multicast +Broadcast) and dropped packets.
OutOctets	**Synopsis:** 0 to 18446744073709551615 The number of octets in transmitted good packets.
InPkts	**Synopsis:** 0 to 18446744073709551615 The number of received good packets (Unicast+Multicast+Broadcast) and dropped packets.
OutPkts	**Synopsis:** 0 to 18446744073709551615 The number of transmitted good packets.
TotalInOctets	**Synopsis:** 0 to 18446744073709551615 The total number of octets of all received packets. This includes data octets of rejected and local packets which are not forwarded to the switching core for transmission. It should reflect all the data octets received on the line.
TotalInPkts	**Synopsis:** 0 to 18446744073709551615 The number of received packets. This includes rejected, dropped local, and packets which are not forwarded to the switching core for transmission. It should reflect all packets received ont the line.
InBroadcasts	**Synopsis:** 0 to 18446744073709551615 The number of good Broadcast packets received.
InMulticasts	**Synopsis:** 0 to 18446744073709551615 The number of good Multicast packets received.
CRCAlignErrors	**Synopsis:** 0 to 4294967295 The number of packets received which meet all the following conditions:

Parameter	Description
	• Packet data length is between 64 and 1536 octets inclusive. • Packet has invalid CRC. • Collision Event has not been detected. • Late Collision Event has not been detected.
OversizePkts	**Synopsis:** 0 to 4294967295 The number of packets received with data length greater than 1536 octets and valid CRC.
Fragments	**Synopsis:** 0 to 4294967295 The number of packets received which meet all the following conditions: • Packet data length is less than 64 octets, or packet without SFD and is less than 64 octets in length. • Collision Event has not been detected. • Late Collision Event has not been detected. • Packet has invalid CRC.
Jabbers	**Synopsis:** 0 to 4294967295 The number of packets which meet all the following conditions: • Packet data length is greater that 1536 octets. • Packet has invalid CRC.
Collisions	**Synopsis:** 0 to 4294967295 The number of received packets for which Collision Event has been detected.
LateCollisions	**Synopsis:** 0 to 4294967295 The number of received packets for which Late Collision Event has been detected.
Pkt64Octets	**Synopsis:** 0 to 4294967295 The number of received and transmitted packets with size of 64 octets. This includes received and transmitted packets as well as dropped and local received packets. This does not include rejected received packets.
Pkt65to127Octets	**Synopsis:** 0 to 4294967295 The number of received and transmitted packets with size of 65 to 127 octets. This includes received and transmitted packets as well as dropped and local received packets. This does not include rejected received packets.
Pkt128to255Octets	**Synopsis:** 0 to 4294967295 The number of received and transmitted packets with size of 128 to 257 octets. This includes received and transmitted packets as well as dropped and local received packets. This does not include rejected received packets.
Pkt256to511Octets	**Synopsis:** 0 to 4294967295 The number of received and transmitted packets with size of 256 to 511 octets. This includes received and transmitted packets as well as dropped and local received packets. This does not include rejected received packets.
Pkt512to1023Octets	**Synopsis:** 0 to 4294967295 The number of received and transmitted packets with size of 512 to 1023 octets. This includes received and transmitted packets as well

Parameter	Description
	as dropped and local received packets. This does not include rejected received packets.
Pkt1024to1536Octets	**Synopsis:** 0 to 4294967295 The number of received and transmitted packets with size of 1024 to 1536 octets. This includes received and transmitted packets as well as dropped and local received packets. This does not include rejected received packets.
DropEvents	**Synopsis:** 0 to 4294967295 The number of received packets that are droped due to lack of receive buffers.
OutMulticasts	**Synopsis:** 0 to 18446744073709551615 The number of transmitted Multicast packets. This does not include Broadcast packets.
OutBroadcasts	**Synopsis:** 0 to 18446744073709551615 The number of transmitted Broadcast packets.
UndersizePkts	**Synopsis:** 0 to 4294967295 The number of received packets which meet all the following conditions: • Packet data length is less than 64 octets. • Collision Event has not been detected. • Late Collision Event has not been detected. • Packet has valid CRC.

Section 3.6.5

Clearing Statistics for Specific Ethernet Ports

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

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

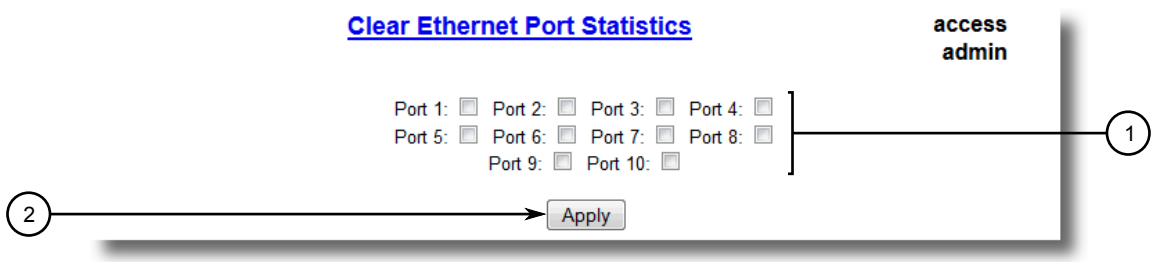


Figure 24: Clear Ethernet Port Statistics Form (Typical)

1. Port Check Boxes **2.** Confirm Button

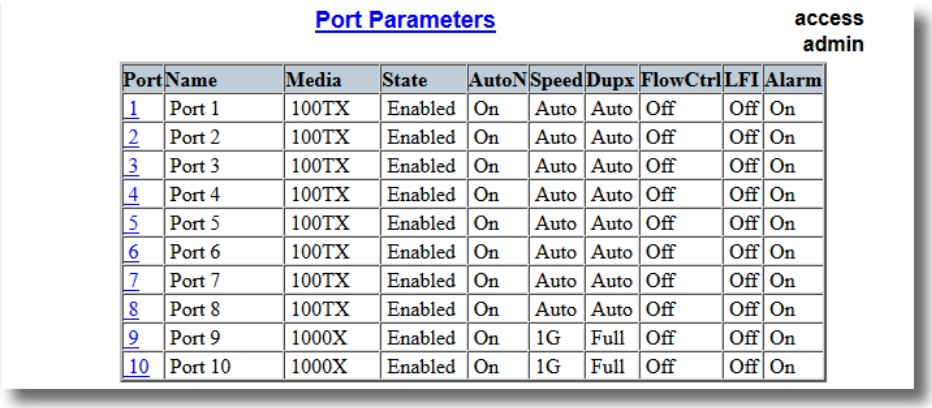
2. Select one or more Ethernet ports.
3. Click **Confirm**.

Section 3.6.6

Configuring an Ethernet Port

To configure an Ethernet port, do the following:

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



Port Parameters

access admin

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

Figure 25: Port Parameters Table

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

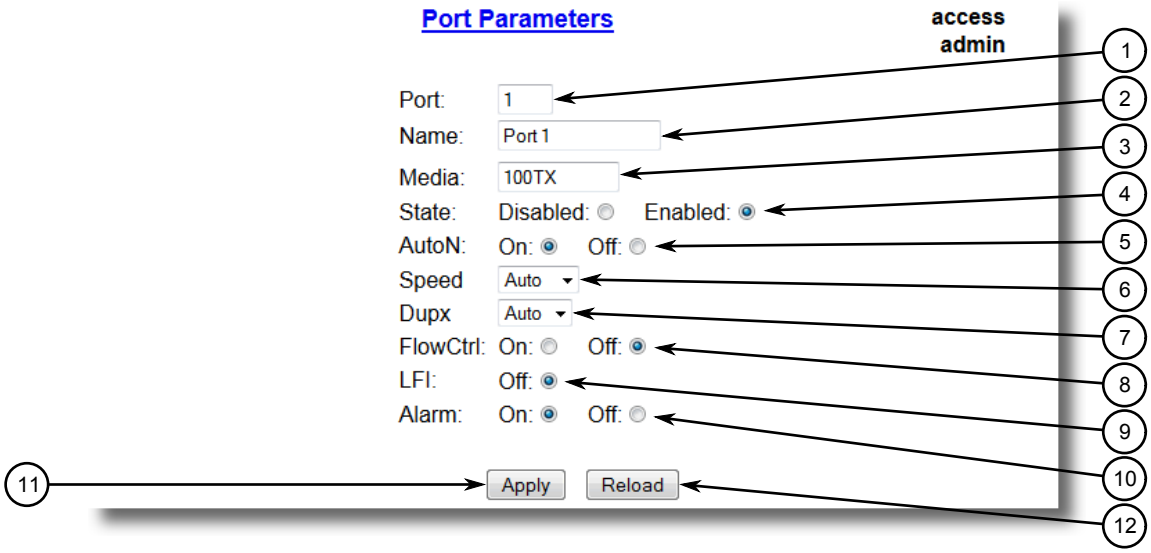


Figure 26: Port Parameters Form

1. Port Box **2.** Name Box **3.** Media Box **4.** State Box **5.** AutoN Box **6.** Speed Box **7.** Dupx Box **8.** FlowCtrl Box **9.** LFI Box **10.** Alarm Box **11.** Apply Button **12.** Reload Button

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

Parameter	Description
Port	**Synopsis:** 1 to maximum port number

Parameter	Description
	Default: 1 The port number as seen on the front plate silkscreen of the switch.
Name	**Synopsis:** Any 15 characters **Default:** Port x 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 } **Default:** 100TX The type of the port media.
State	**Synopsis:** { Disabled, Enabled } **Default:** Enabled Disabling a port will prevent all frames from being sent and received on that port. Also, when disabled link integrity signal is not sent so that the link/activity LED will never be lit. You may want to disable a port for troubleshooting or to secure it from unauthorized connections. **NOTE** *Disabling a port whose media type is set to **802.11g** disables the corresponding wireless module.*
AutoN	**Synopsis:** { Off, On } **Default:** On Enable or disable IEEE 802.3 auto-negotiation. Enabling auto-negotiation results in speed and duplex being negotiated upon link detection; both end devices must be auto-negotiation compliant for the best possible results. 10Mbps and 100Mbps fiber optic media do not support auto-negotiation so these media must be explicitly configured to either half or full duplex. Full duplex operation requires that both ends are configured as such or else severe frame loss will occur during heavy network traffic.
Speed	**Synopsis:** { Auto, 10M, 100M, 1G } **Default:** Auto Speed (in Megabit-per-second or Gigabit-per-second). If auto-negotiation is enabled, this is the speed capability advertised by the auto-negotiation process. If auto-negotiation is disabled, the port is explicitly forced to this speed mode. AUTO means advertise all supported speed modes.
Dupx	**Synopsis:** { Auto, Half, Full } **Default:** Auto Duplex mode. If auto-negotiation is enabled, this is the duplex capability advertised by the auto-negotiation process. If auto-negotiation is disabled, the port is explicitly forced to this duplex mode. AUTO means advertise all supported duplex modes.
Flow Control	**Synopsis:** { Off, On } **Default:** On Flow Control is useful for preventing frame loss during times of severe network traffic. Examples of this include multiple source ports sending to a single destination port or a higher speed port bursting to a lower speed port.

Parameter	Description
	When the port is half-duplex it is accomplished using 'backpressure' where the switch simulates collisions causing the sending device to retry transmissions according to the Ethernet backoff algorithm. When the port is full-duplex it is accomplished using PAUSE frames which causes the sending device to stop transmitting for a certain period of time.
LFI	**Synopsis:** { Off, On } **Default:** Off Enabling Link-Fault-Indication (LFI) inhibits transmitting link integrity signal when the receive link has failed. This allows the device at far end to detect link failure under all circumstances. **NOTE** *This feature must not be enabled at both ends of a fiber link.*
Alarm	**Synopsis:** { On, Off } **Default:** On Disabling link state alarms will prevent alarms and LinkUp and LinkDown SNMP traps from being sent for that port.

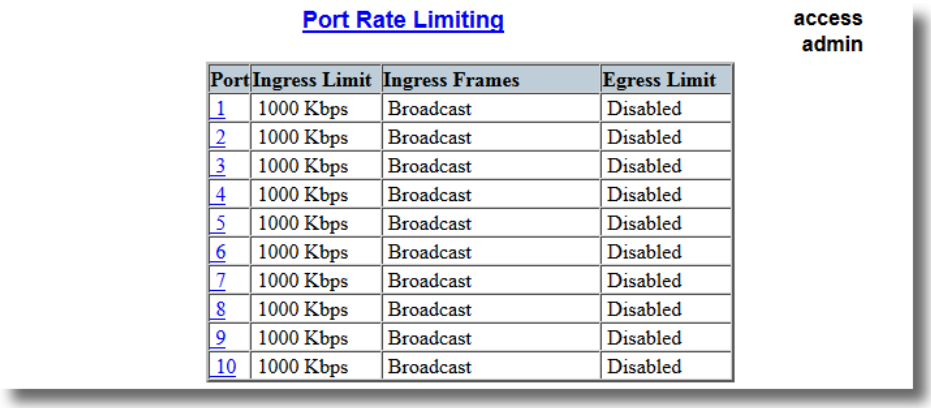
NOTE
If one end of the link is fixed to a specific speed and duplex type and the peer auto-negotiates, there is a strong possibility that the link will either fail to raise, or raise with the wrong settings on the auto-negotiating side. The auto-negotiating peer will fall back to half-duplex operation, 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**.

Section 3.6.7
Configuring Port Rate Limiting

To configure port rate limiting, do the following:

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



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

Figure 27: Port Rate Limiting Table

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

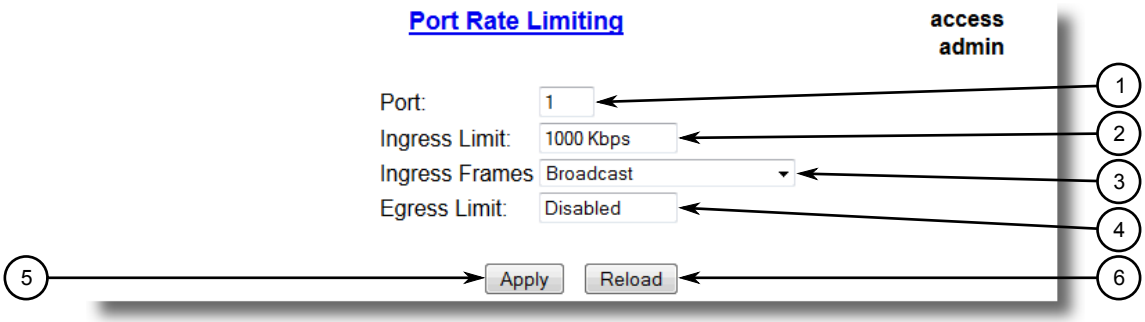


Figure 28: Port Rate Limiting Form

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

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

Parameter	Description
Port	**Synopsis:** 1 to maximum port number **Default:** 1 The port number as seen on the front plate silkscreen of the switch.
Ingress Limit	**Synopsis:** 62 to 256000 Kbps or { Disabled } **Default:** 1000 Kbps The rate after which received frames (of the type described by the ingress frames parameter) will be discarded by the switch.
Ingress Frames	**Synopsis:** { Broadcast, Bcast&Mcast, Bcast&Mcast&FloodUcast, Bcast&FloodUcast, FloodUcast, All } **Default:** Broadcast This parameter specifies the types of frames to be rate-limited on this port. It applies only to received frames: • Broadcast - only broadcast frames

Parameter	Description
	• Bcast&Mcast - broadcast and multicast frames • Bcast&FloodUcast - broadcast and flooded unicast frames • Bcast&Mcast&FloodUcast - broadcast, multicast and flooded unicast frames • FloodUcast - only flooded unicast frames • All - all (multicast, broadcast and unicast) frames
Egress Limit	**Synopsis:** { Broadcast, Multicast, Mcast&FloodUcast, All }">62 to 256000 Kbps or { Disabled } **Default:** Disabled The maximum rate at which the switch will transmit (multicast, broadcast and unicast) frames on this port. The switch will discard frames in order to meet this rate if required.

4. Click **Apply**.

Section 3.6.8

Configuring Port Mirroring

Port mirroring is a troubleshooting tool that copies, or mirrors, all traffic received or transmitted on a designated port to 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.

Select a target port that has a higher speed than the source port. Mirroring a 100 Mbps port onto a 10 Mbps port may result in an improperly mirrored stream.

Frames will be dropped if the full-duplex rate of frames on the source port exceeds the transmission speed of the target port. Since both transmitted and received frames on the source port are mirrored to the target port, frames will be discarded if the sum traffic exceeds the target port's transmission rate. This problem reaches its extreme in the case where traffic on a 100 Mbps full-duplex port is mirrored onto a 10 Mbps half-duplex port.

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.

IMPORTANT!
Before configuring port mirroring, note the following limitations:

- *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.) may not be mirrored*
- *Switch management frames generated by the switch (such as Telnet, HTTP, SNMP, etc.) may not be mirrored*

To configure port mirroring, do the following:

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

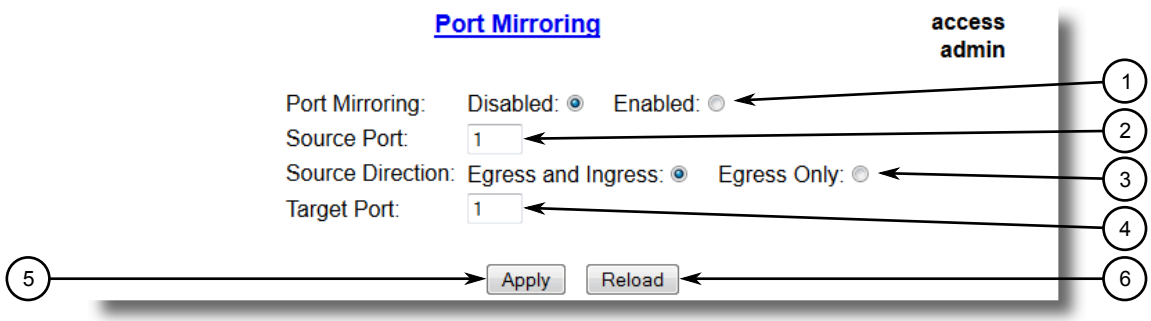


Figure 29: Port Mirroring Form

1. Port Mirroring Box **2.** Source Port Box **3.** Target Port Box **4.** Apply Button **5.** Reload Button

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

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

3. Click **Apply**.

Section 3.6.9

Configuring Link Detection

To configure link detection, do the following:

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

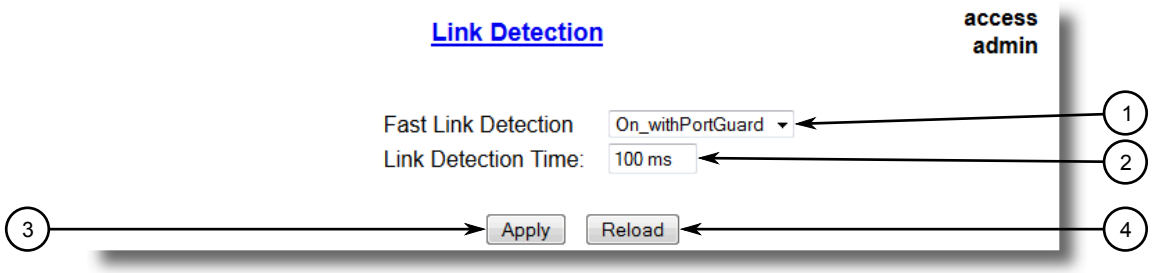


Figure 30: Link Detection Form

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

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

> **NOTE**
> *When Fast Link Detection is enabled, the system prevents link state change processing from consuming all available CPU resources. However, if Port Guard is not used, it is possible for almost all available CPU time to be consumed by frequent link state changes, which could have a negative impact on overall system responsiveness.*

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

Parameter	Description
	could continue affect the system in terms of response time. This setting should be used with caution. • OFF - Turning this parameter OFF will disable FAST LINK DETECTION completely. The switch will need a longer time to detect a link failure. This will result in a longer network recovery time of up to 2s.
Link Detection Time	**Synopsis:** 100 ms to 1000 ms **Default:** 100 ms The time that the link has to continuously stay up before the "link up" decision is made by the device. (The device performs de-bouncing of Ethernet link detection to avoid multiple responses to an occasional link bouncing event, e.g. when a cable is shaking while being plugged-in or unplugged).

3. Click **Apply**.

Section 3.6.10

Detecting Cable Faults

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

CONTENTS

- Section 3.6.10.1, “Viewing Cable Diagnostics Results”
- Section 3.6.10.2, “Performing Cable Diagnostics”
- Section 3.6.10.3, “Clearing Cable Diagnostics”
- Section 3.6.10.4, “Determining the Estimated Distance To Fault (DTF)”

Section 3.6.10.1

Viewing Cable Diagnostics Results

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

NOTE
For information about how to start a diagnostic test, refer to Section 3.6.10.2, “Performing Cable Diagnostics” .

Cable Diagnostics Parameters

access
admin

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

Figure 31: Cable Diagnostics Parameters Table

This table displays the following information:

Parameter	Description
Port	**Synopsis:** 1 to maximum port number The port number as seen on the front plate silkscreen of the switch.
State	**Synopsis:** { Stopped, Started } Control the start/stop of the cable diagnostics on the selected port. If a port does not support cable diagnostics, State will be reported as N/A.
Runs	**Synopsis:** 0 to 65535 The total number of times cable diagnostics to be performed on the selected port. If this number is set to 0, cable diagnostics will be performed forever on the selected port.
Calib.	**Synopsis:** -100.0 to 100.0 m This calibration value can be used to adjust or calibrate the estimated distance to fault. User can take following steps to calibrate the cable diagnostics estimated distance to fault: • Pick a particular port which calibration is needed • Connect an Ethernet cable with a known length (e.g. 50m) to the port • DO NOT connect the other end of the cable to any link partner • Run cable diagnostics a few times on the port. OPEN fault should be detected • Find the average distance to the OPEN fault recorded in the log and compare it to the known length of the cable. The difference can be used as the calibration value • Enter the calibration value and run cable diagnostics a few more times • The distance to OPEN fault should now be at similar distance as the cable length • Distance to fault for the selected port is now calibrated
Good	**Synopsis:** 0 to 65535 The number of times GOOD TERMINATION (no fault) is detected on the cable pairs of the selected port.
Open	**Synopsis:** 0 to 65535

Parameter	Description
	The number of times OPEN is detected on the cable pairs of the selected port.
Short	**Synopsis:** 0 to 65535 The number of times SHORT is detected on the cable pairs of the selected port.
Imped	**Synopsis:** 0 to 65535 The number of times IMPEDANCE MISMATCH is detected on the cable pairs of the selected port.
Pass /Fail /Total	**Synopsis:** Any 19 characters This field summarizes the results of the cable diagnostics performed so far. Pass - number of times cable diagnostics successfully completed on the selected port. Fail - number of times cable diagnostics failed to complete on the selected port. 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 *Section 3.5.1, "Viewing Local Logs"* *.*

Section 3.6.10.2

Performing Cable Diagnostics

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

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

   IMPORTANT!
   *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 ROS, navigate to ***Ethernet Ports » Configure/View Cable Diagnostics Parameters*** . The **Cable Diagnostics Parameters** table appears.

Cable Diagnostics Parameters access admin

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

Figure 32: Cable Diagnostics Parameters Table

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

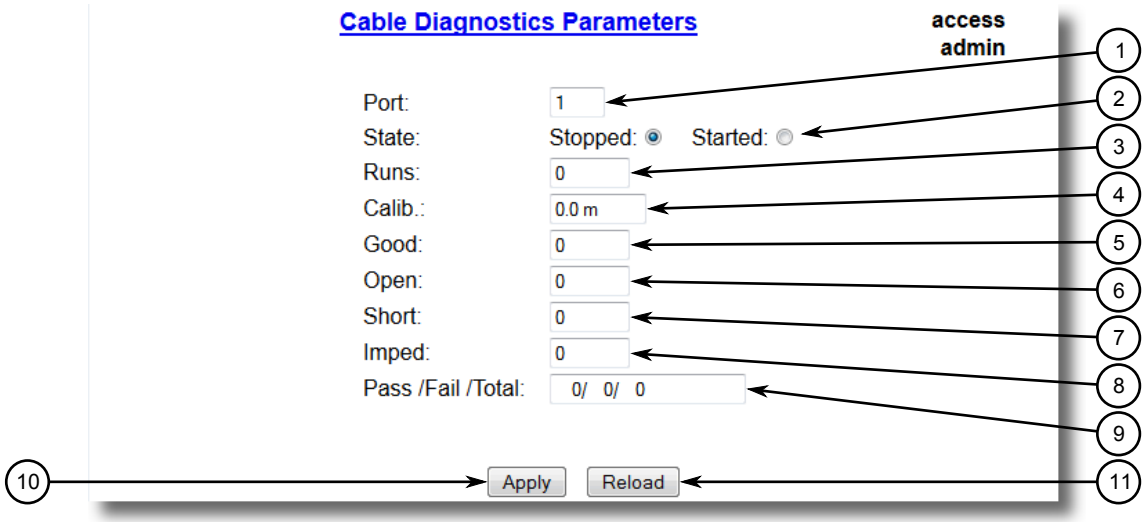


Figure 33: Cable Diagnostics Parameters Form

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

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 Section 3.6.10.4, "Determining the Estimated Distance To Fault (DTF)" .
7. Select **Started**.

IMPORTANT!
*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 Section 3.6.10.1, "Viewing Cable Diagnostics Results" .

Section 3.6.10.3

Clearing Cable Diagnostics

To clear the cable diagnostic results, do the following:

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

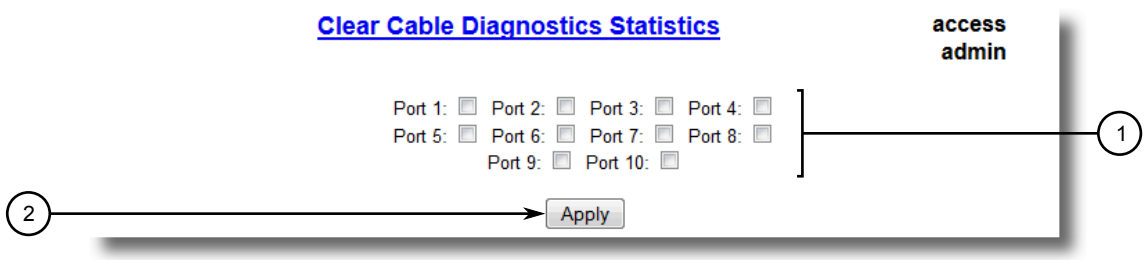


Figure 34: Clear Cable Diagnostics Statistics Form

1. Port Check Boxes **2.** Apply Button

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

Section 3.6.10.4

Determining the Estimated Distance To Fault (DTF)

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

1. Connect a CAT-5 (or better quality) Ethernet cable with a known length to the device. Do not connect the other end of the cable to another port.
2. Configure the cable diagnostic utility to run a few times on the selected Ethernet port and start the test. For more information, refer to Section 3.6.10.2, "Performing Cable Diagnostics" . 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 Section 3.5.1, "Viewing Local Logs" .
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.

Section 3.6.11

Resetting Ethernet Ports

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

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

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

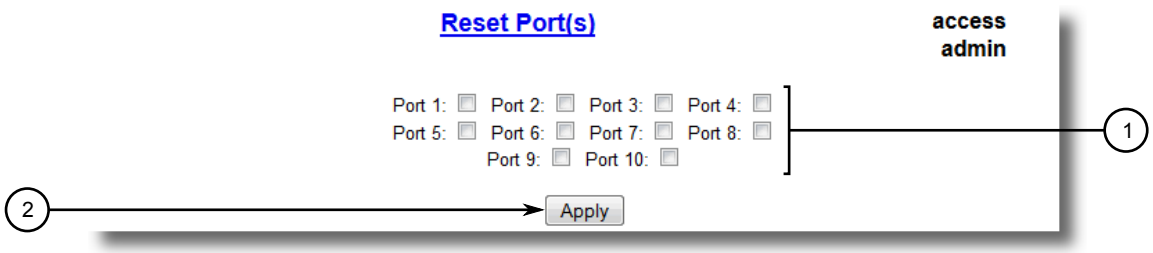


Figure 35: Reset Port(s) Form

1. Ports **2.** Apply Button

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

Section 3.7

Managing IP Interfaces

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

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

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

CONTENTS

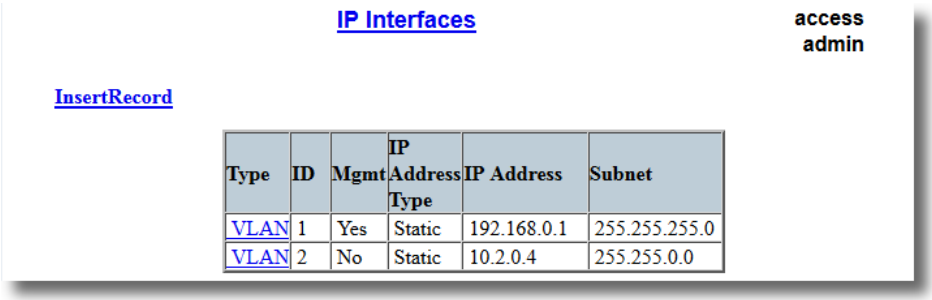
- Section 3.7.1, “Viewing a List of IP Interfaces”
- Section 3.7.2, “Adding an IP Interface”

- Section 3.7.3, “Deleting an IP Interface”

Section 3.7.1

Viewing a List of IP Interfaces

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



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

Figure 36: IP Interfaces Table

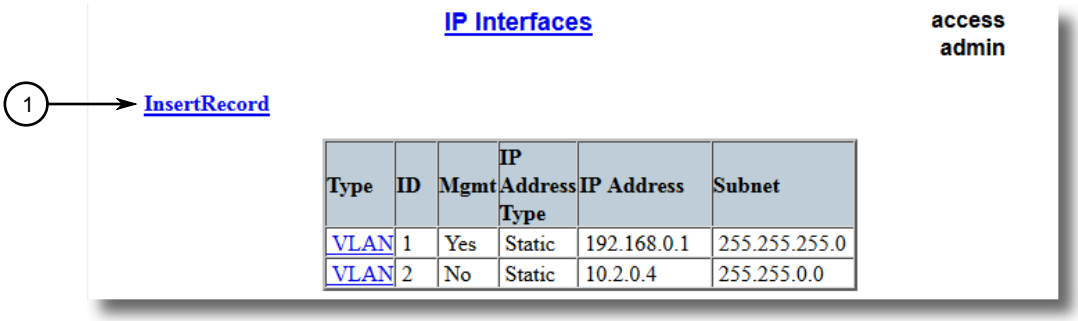
If IP interfaces have not been configured, add IP interfaces as needed. For more information, refer to Section 3.7.2, “Adding an IP Interface” .

Section 3.7.2

Adding an IP Interface

To add an IP interface, do the following:

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



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

Figure 37: IP Interfaces Table

1. InsertRecord

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

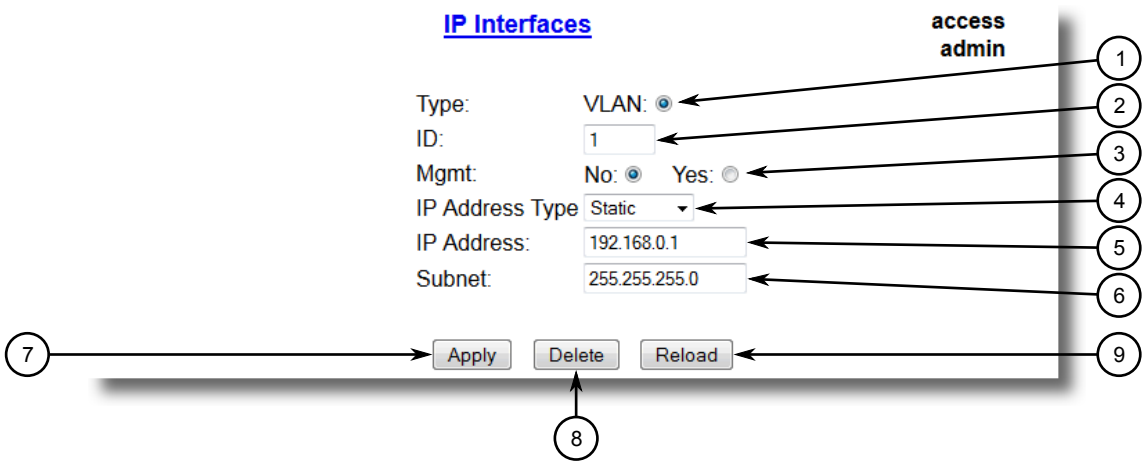


Figure 38: IP Interfaces Form

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

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

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

Parameter	Description
Type	**Synopsis:** { VLAN } **Default:** VLAN Specifies the type of the interface for which this IP interface is created.
ID	**Synopsis:** 1 to 4094 **Default:** 1 Specifies the ID of the interface for which this IP interface is created. If the interface type is VLAN, this represents the VLAN ID.
Mgmt	**Synopsis:** { No, Yes } **Default:** No Specifies whether the IP interface is the device management interface.
IP Address Type	**Synopsis:** { Static, Dynamic, DHCP, BOOTP } **Default:** Static Specifies whether the IP address is static or is dynamically assigned via DHCP or BOOTP>. The Dynamic option automatically switches between BOOTP and DHCP until it receives a response from the relevant server. The Static option must be used for non-management interfaces.
IP Address	**Synopsis:** ###.###.###.### where ### ranges from 0 to 255 **Default:** 192.168.0.1

Parameter	Description
	Specifies the IP address of this device. An IP address is a 32-bit number that is notated by using four numbers from 0 through 255, separated by periods. Only a unicast IP address is allowed, which ranges from 1.0.0.0 to 233.255.255.255.
Subnet	**Synopsis:** ###.###.###.### where ### ranges from 0 to 255 **Default:** 255.255.255.0 Specifies the IP subnet mask of this device. An IP subnet mask is a 32-bit number that is notated by using four numbers from 0 through 255, separated by periods. Typically, subnet mask numbers use either 0 or 255 as values (e.g. 255.255.255.0) but other numbers can appear. **IMPORTANT!** *Each IP interface must have a unique network address.*

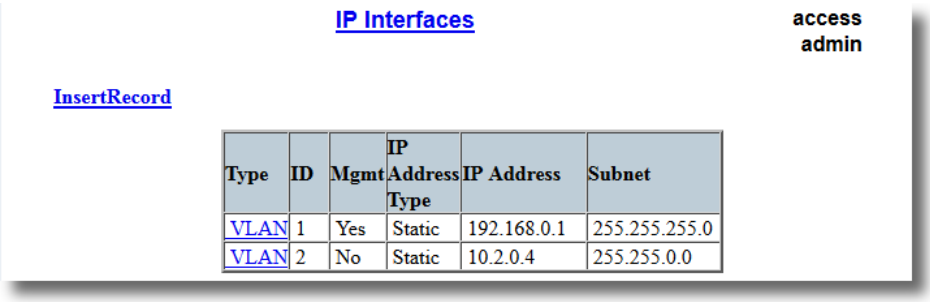
4. Click **Apply**.

Section 3.7.3

Deleting an IP Interface

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

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



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

Figure 39: IP Interfaces Table

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

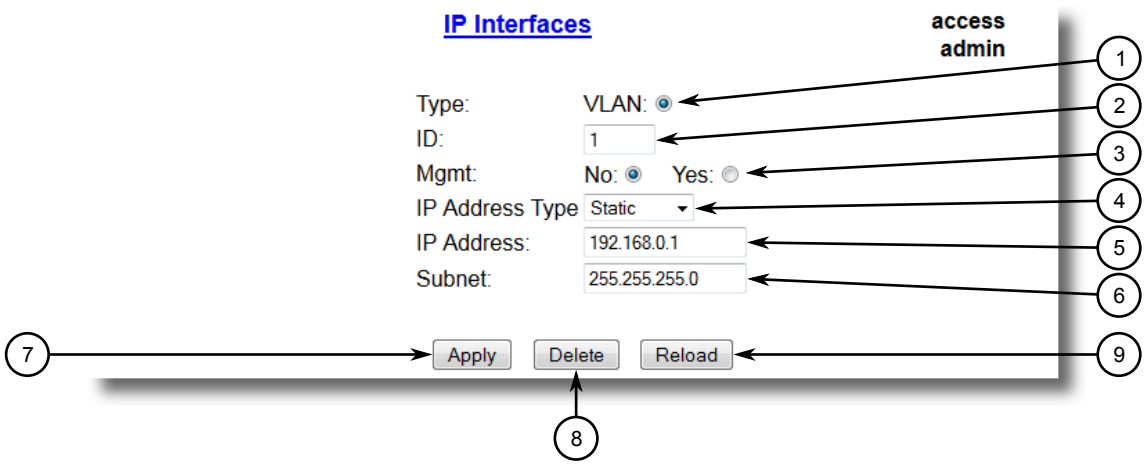


Figure 40: IP Interfaces Form

1. IP Address Type Box **2.** IP Address Box **3.** Subnet Box **4.** Apply Button **5.** Delete Button **6.** Reload Button

3. Click **Delete**.

Section 3.8

Managing IP Gateways

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

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

CONTENTS

- Section 3.8.1, “Viewing a List of IP Gateways”
- Section 3.8.2, “Adding an IP Gateway”
- Section 3.8.3, “Deleting an IP Gateway”

Section 3.8.1

Viewing a List of IP Gateways

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

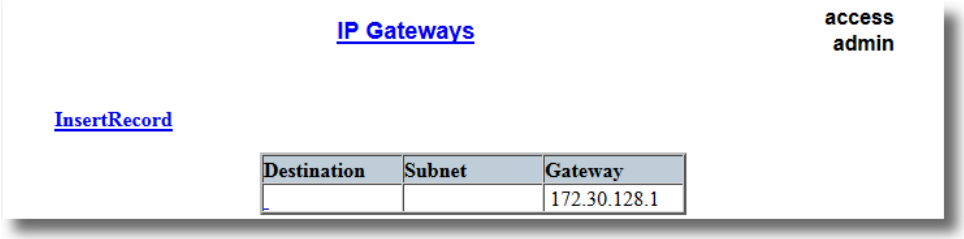


Figure 41: IP Gateways Table

If IP gateways have not been configured, add IP gateways as needed. For more information, refer to Section 3.8.2, "Adding an IP Gateway" .

Section 3.8.2

Adding an IP Gateway

To add an IP gateway, do the following:

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

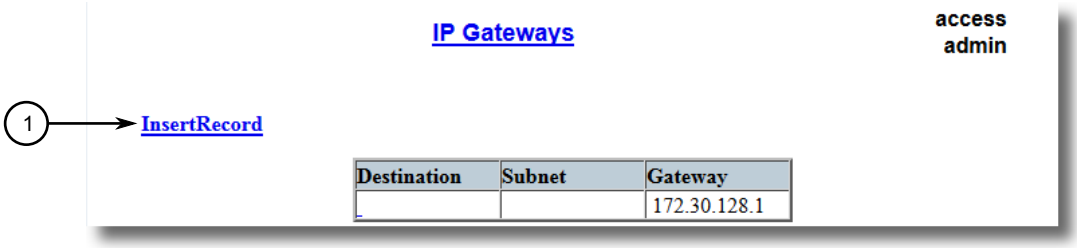


Figure 42: IP Gateways Table

1. InsertRecord

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

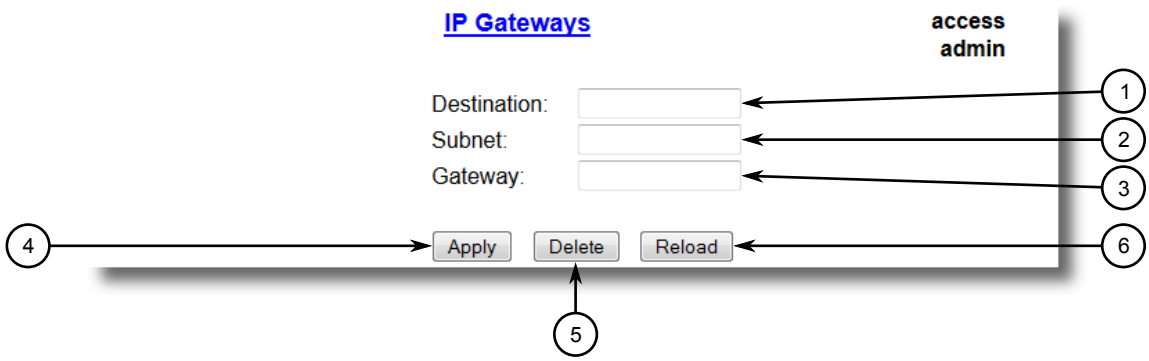


Figure 43: IP Gateways

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

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

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

4. Click **Apply**.

Section 3.8.3

Deleting an IP Gateway

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

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

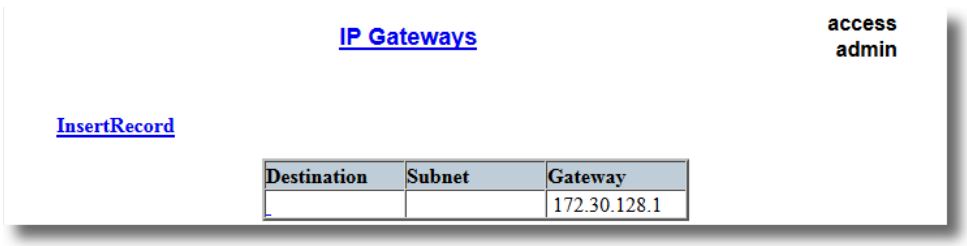


Figure 44: IP Gateways Table

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

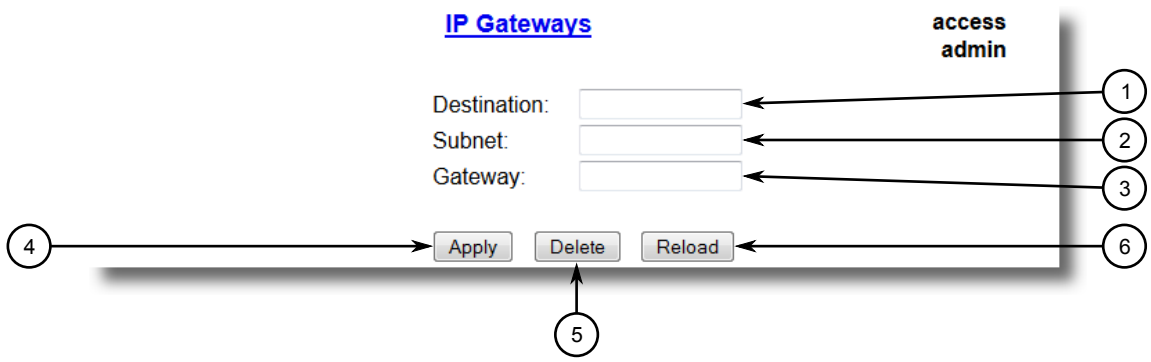


Figure 45: IP Gateways Form

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

3. Click **Delete**.

Section 3.9

Configuring IP Services

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

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

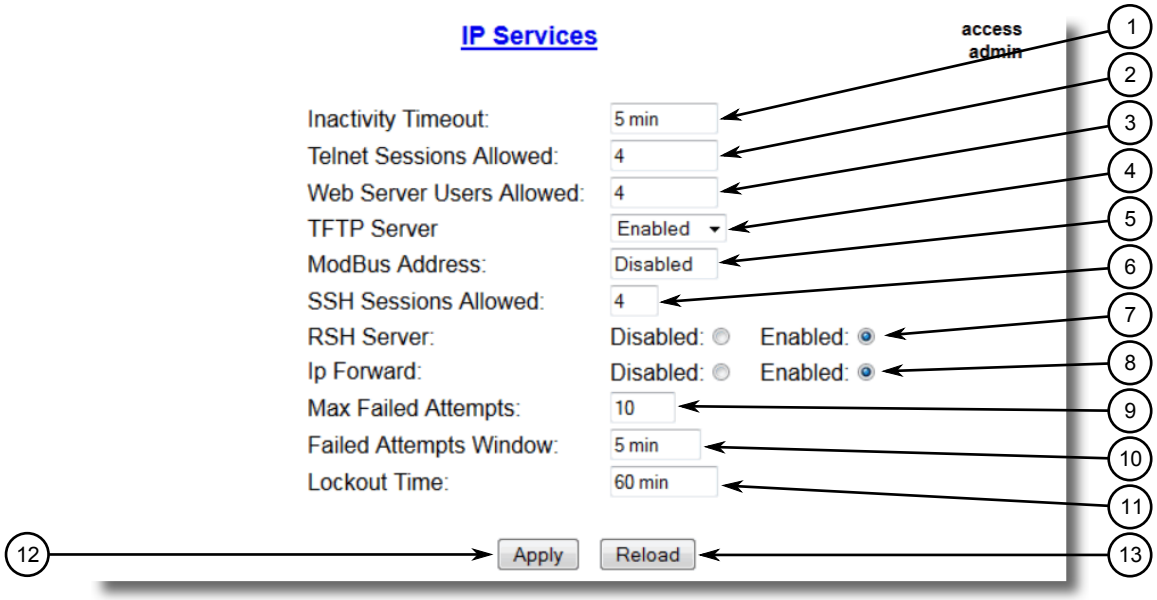


Figure 46: IP Services Form

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

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

Parameter	Description
Inactivity Timeout	**Synopsis:** 1 to 60 or { Disabled } **Default:** 5 min Specifies when the console will timeout and display the login screen if there is no user activity. A value of zero disables timeouts. For Web Server users maximum timeout value is limited to 30 minutes.
Telnet Sessions Allowed	**Synopsis:** 1 to 4 or { Disabled } **Default:** Disabled Limits the number of Telnet sessions. A value of zero prevents any Telnet access.
Web Server Users Allowed	**Synopsis:** 1 to 4 or { Disabled } **Default:** 4 Limits the number of simultaneous web server users.
TFTP Server	**Synopsis:** { Disabled, Get Only, Enabled } **Default:** Disabled As TFTP is a very insecure protocol, this parameter allows user to limit or disable TFTP Server access.. DISABLED - disables read and write access to TFTP Server GET ONLY - only allows reading of files via TFTP Server ENABLED - allows reading and writing of files via TFTP Server
ModBus Address	**Synopsis:** 1 to 255 or { Disabled } **Default:** Disabled

Parameter	Description
	Determines the Modbus address to be used for Management through Modbus.
SSH Sessions Allowed (Controlled Version Only)	**Synopsis:** 1 to 4 **Default:** 4 Limits the number of SSH sessions.
RSH Server	**Synopsis:** { Disabled, Enabled } **Default:** Disabled (controlled version) or Enabled (non-controlled version) Disables/enables Remote Shell access.
IP Forward	**Synopsis:** { Disabled, Enabled } Controls the ability of IP Forwarding between VLANs in Serial Server or IP segments. **NOTE** *When upgrading to ROS v4.3, the default will be set to { Enabled }.*
Max Failed Attempts	**Synopsis:** 1 to 20 **Default:** 10 Maximum number of consecutive failed access attempts on service within Failed Attempts Window before blocking the service.
Failed Attempts Window	**Synopsis:** 1 to 30 min **Default:** 5 min 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.
Lockout Time	**Synopsis:** 1 to 120 min **Default:** 60 min The time in minutes (min) the service remains locked out after the maximum number of failed access attempts has been reached.

3. Click **Apply**.

Section 3.10

Managing Remote Monitoring

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

CONTENTS

- Section 3.10.1, “Managing RMON History Controls”
- Section 3.10.2, “Managing RMON Alarms”

- Section 3.10.3, “Managing RMON Events”

Section 3.10.1

Managing RMON History Controls

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

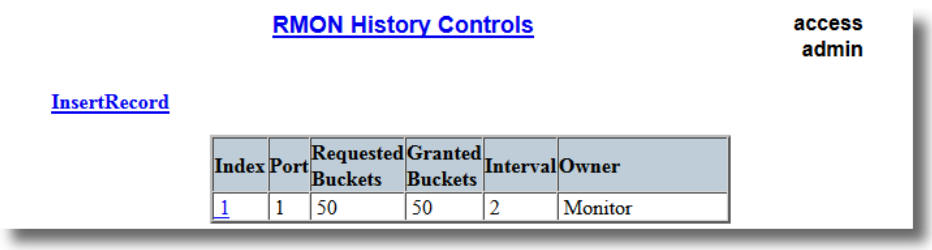
CONTENTS

- Section 3.10.1.1, “Viewing a List of RMON History Controls”
- Section 3.10.1.2, “Adding an RMON History Control”
- Section 3.10.1.3, “Deleting an RMON History Control”

Section 3.10.1.1

Viewing a List of RMON History Controls

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



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

Figure 47: RMON History Controls Table

If history controls have not been configured, add controls as needed. For more information, refer to Section 3.10.1.2, “Adding an RMON History Control” .

Section 3.10.1.2

Adding an RMON History Control

To add an RMON history control, do the following:

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

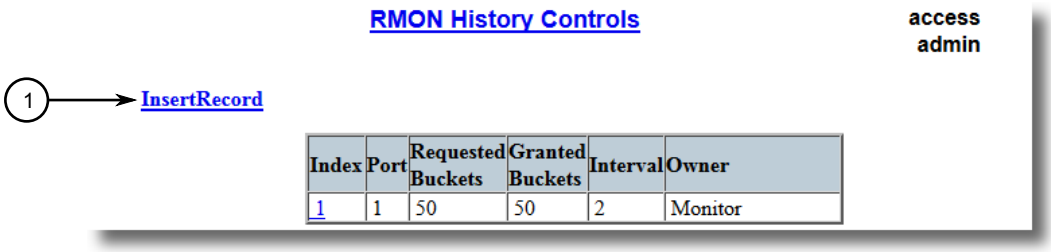


Figure 48: RMON History Controls Table

1. InsertRecord

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

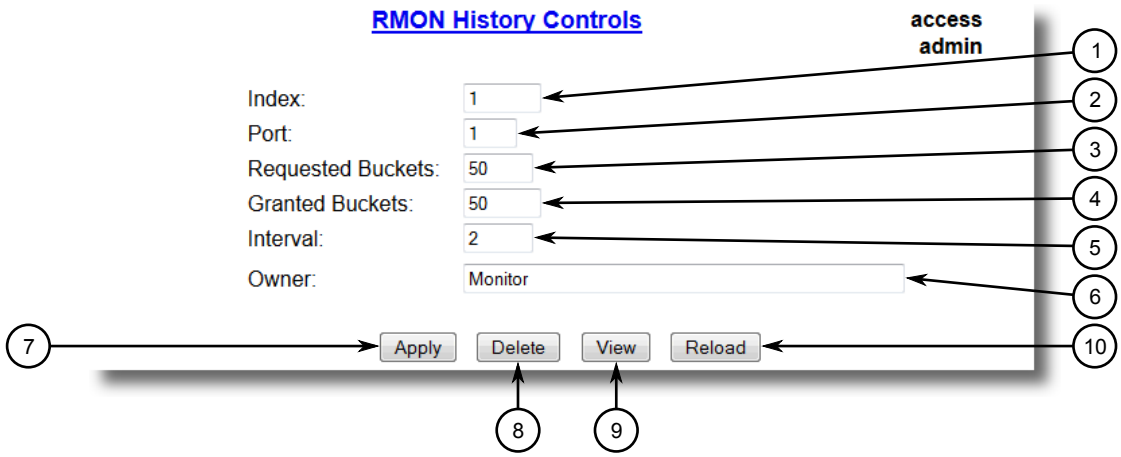


Figure 49: RMON History Controls Form

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

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

Parameter	Description
Index	**Synopsis:** 1 to 65535 **Default:** 1 The index of this RMON History Contol record.
Port	**Synopsis:** 1 to maximum port number **Default:** 1 The port number as seen on the front plate silkscreen of the switch.
Requested Buckets	**Synopsis:** 1 to 4000 **Default:** 50 The maximum number of buckets requested for this RMON collection history group of statistics. The range is 1 to 4000. The default is 50.

Parameter	Description
Granted Buckets	**Synopsis:** 0 to 65535 The number of buckets granted for this RMON collection history. This field is not editable.
Interval	**Synopsis:** 1 to 3600 **Default:** 1800 The number of seconds in over which the data is sampled for each bucket. The range is 1 to 3600. The default is 1800.
Owner	**Synopsis:** Any 127 characters **Default:** Monitor The owner of this record. It is suggested to start this string withword 'monitor'.

4. Click **Apply**.

Section 3.10.1.3

Deleting an RMON History Control

To delete an RMON history control, do the following:

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

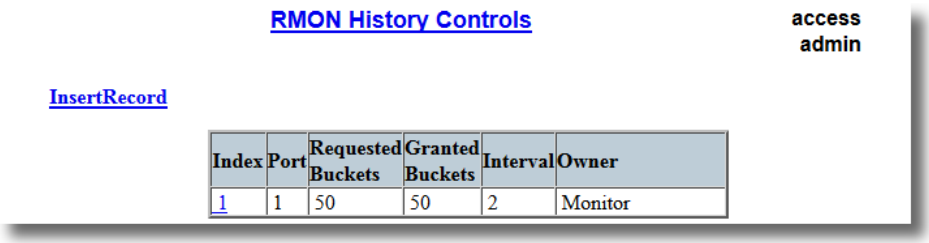


Figure 50: RMON History Controls Table

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

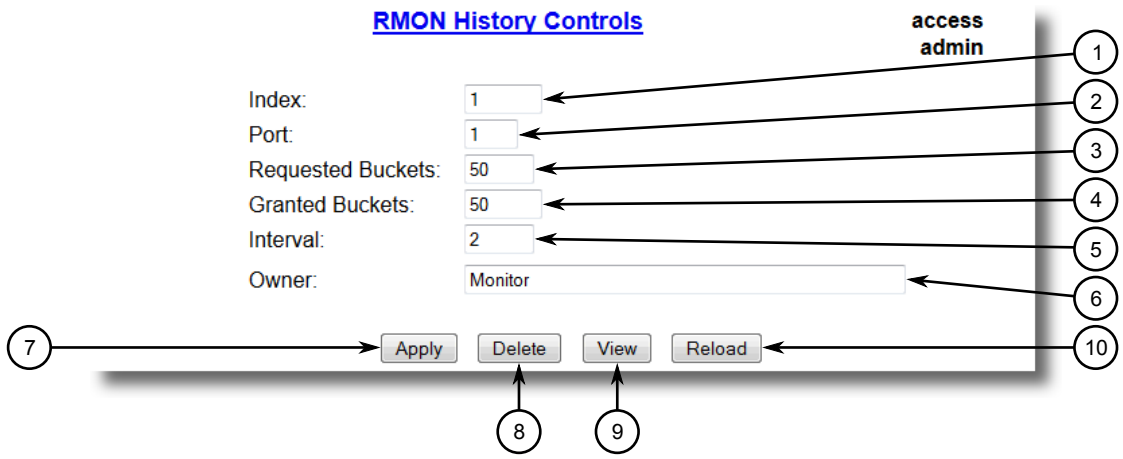


Figure 51: RMON History Controls Form

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

3. Click **Delete**.

Section 3.10.2

Managing RMON Alarms

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

Remote Monitoring (RMON) alarms define upper and lower thresholds for legal values of specific statistical variables in a given interval. This allows RUGGEDCOM ROS to detect events as they occur more quickly than a specified maximum rate or less quckly 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 Section 4.6.2, "Viewing and Clearing Latched Alarms" .

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.

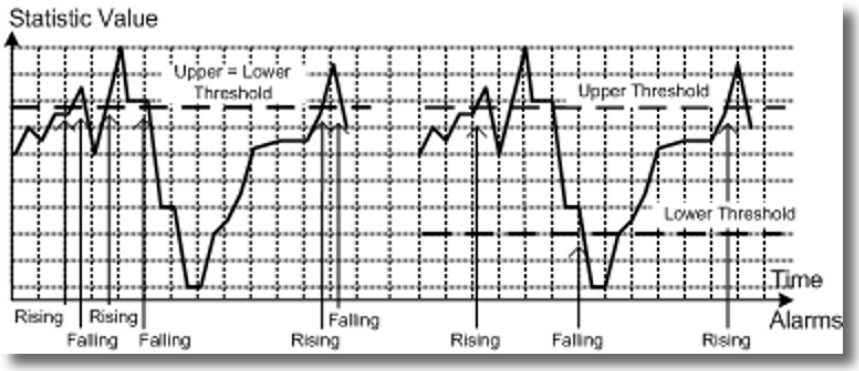


Figure 52: The Alarm Process

There are two methods to evaluate a statistic in order 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*.

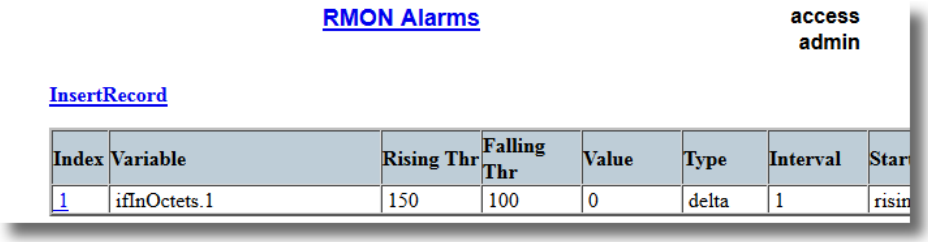
CONTENTS

- Section 3.10.2.1, "Viewing a List of RMON Alarms"
- Section 3.10.2.2, "Adding an RMON Alarm"
- Section 3.10.2.3, "Deleting an RMON Alarm"

Section 3.10.2.1

Viewing a List of RMON Alarms

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



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

Figure 53: RMON Alarms Table

If alarms have not been configured, add alarms as needed. For more information, refer to Section 3.10.2.2, "Adding an RMON Alarm" .

Section 3.10.2.2

Adding an RMON Alarm

To add an RMON alarm, do the following:

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

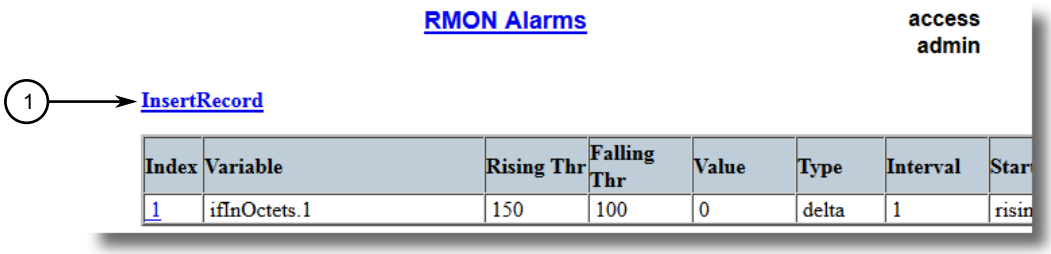


Figure 54: RMON Alarms Table

1. InsertRecord

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

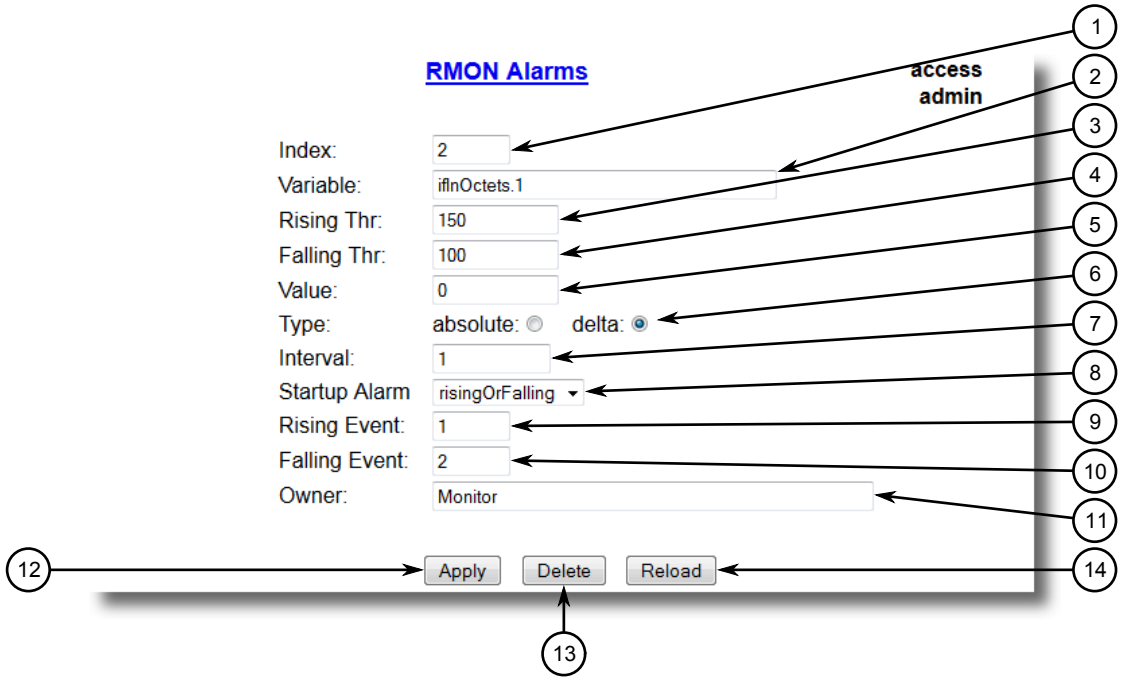


Figure 55: RMON Alarms Form

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

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

Parameter	Description
Index	**Synopsis:** 1 to 65535 **Default:** 1 The index of this RMON Alarm record.
Variable	**Synopsis:** SNMP Object Identifier - up to 39 characters The SNMP object identifier (OID) of the particular variable to be sampled. Only variables that resolve to an ASN.1 primitive type INTEGER (INTEGER, Integer32,Counter32, Counter64, Gauge, or TimeTicks) may be sampled. A list of objects can be printed using shell command 'rmon'. The OID format: objectName.index1.index2... where index format depends on index object type.
Rising Thr	**Synopsis:** -2147483647 to 2147483647 **Default:** 0 A threshold for the sampled variable. When the current sampled variable value is greater than or equal to this threshold, and the value at the last sampling interval was less than this threshold, a single event will be generated. A single event will also be generated if the first sample after this record is created is greater than or equal to this threshold and the associated startup alarm ils equal to 'rising'.After rising alarm is generated, another such event will not be generated until the sampled value falls below this threshold and reaches the value of FallingThreshold.
Falling Thr	**Synopsis:** -2147483647 to 2147483647 **Default:** 0 A threshold for the sampled variable. When the current sampled variable value is less than or equal to this threshold, and the value at the last sampling interval was greater than this threshold, a single event will be generated. A single event will also be generated if the first sample after this record is created is less than or equal to this threshold and the associated startup alarm ils equal to 'falling'.After falling alarm is generated, another such event will not be generated until the sampled value rises above this threshold and reaches the value of RisingThreshold.
Value	**Synopsis:** -2147483647 to 2147483647 The value of monitoring object during the last sampling period. The presentation of value depends of sample type ('absolute' or 'delta').
Type	**Synopsis:** { absolute, delta } **Default:** delta The method of sampling the selected variable and calculating the value to be compared against the thresholds. The value of sample type can be 'absolute' or 'delta'.
Interval	**Synopsis:** 0 to 2147483647 **Default:** 60 The number of seconds in over which the data is sampled and compared with the rising and falling thresholds.
Startup Alarm	**Synopsis:** { rising, falling, risingOrFalling } **Default:** risingOrFalling The alarm that may be sent when this record is first created if condition for raising alarm is met. The value of startup alarm can be 'rising', 'falling' or 'risingOrFalling'.
Rising Event	**Synopsis:** 0 to 65535 **Default:** 0

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

4. Click **Apply**.

Section 3.10.2.3

Deleting an RMON Alarm

To delete an RMON alarm, do the following:

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

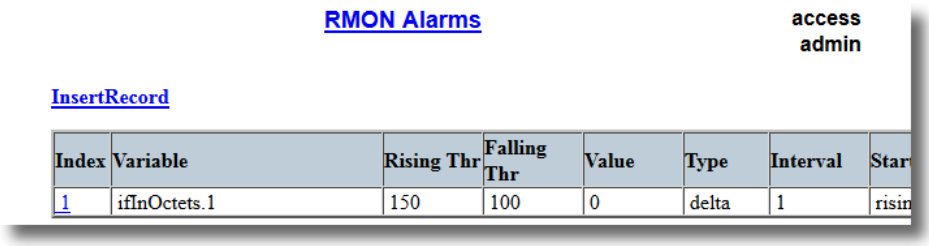


Figure 56: RMON Alarms Table

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

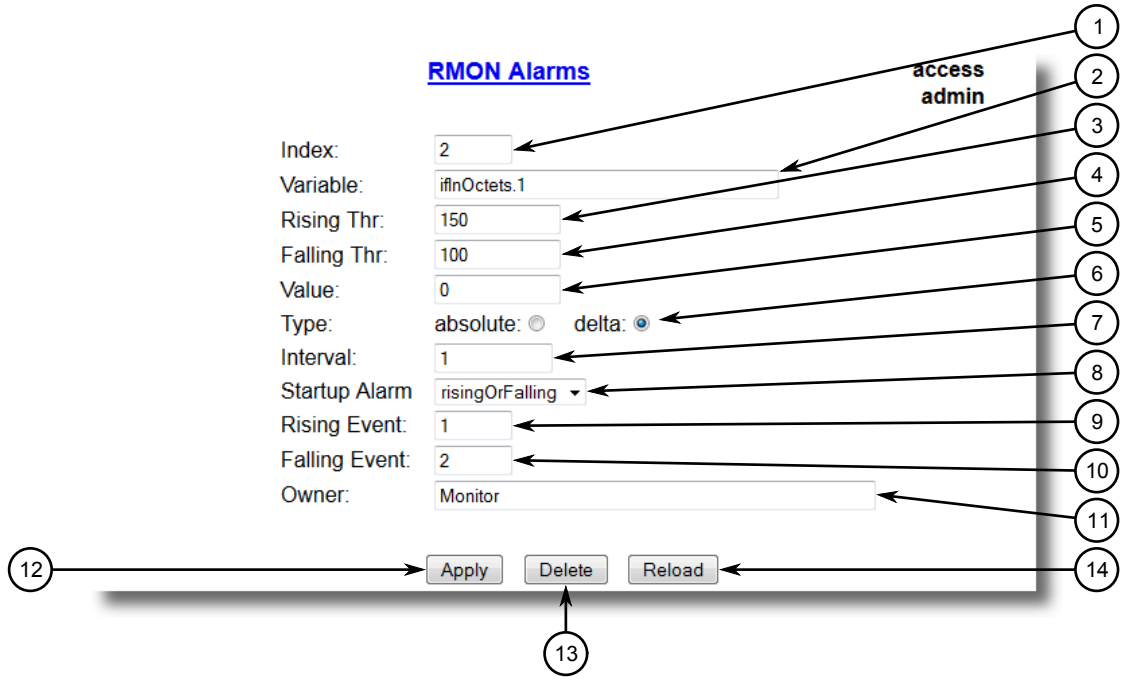


Figure 57: RMON Alarms Form

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

3. Click **Delete**.

Section 3.10.3

Managing RMON Events

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

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

Two traps are defined: risingAlarm and fallingAlarm.

CONTENTS

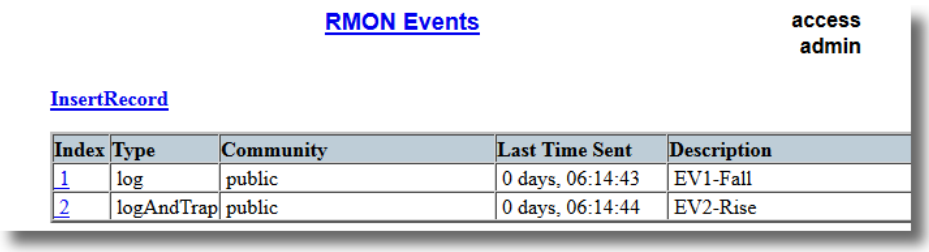
- Section 3.10.3.1, “Viewing a List of RMON Events”
- Section 3.10.3.2, “Adding an RMON Event”

- Section 3.10.3.3, “Deleting an RMON Event”

Section 3.10.3.1

Viewing a List of RMON Events

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



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

Figure 58: RMON Events Table

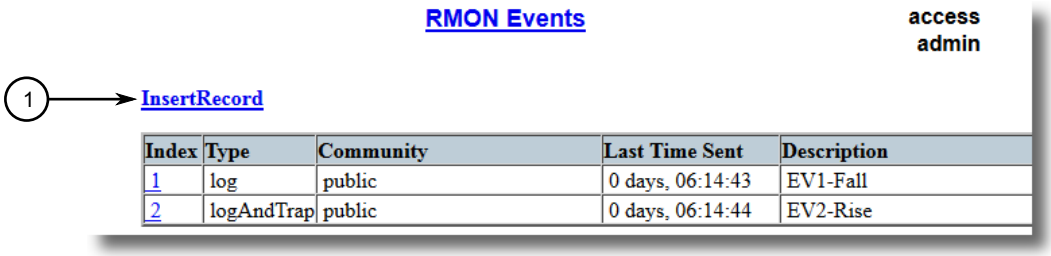
If events have not been configured, add events as needed. For more information, refer to Section 3.10.3.2, “Adding an RMON Event” .

Section 3.10.3.2

Adding an RMON Event

To add an RMON alarm, do the following:

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



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

Figure 59: RMON Events Table

1. InsertRecord

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

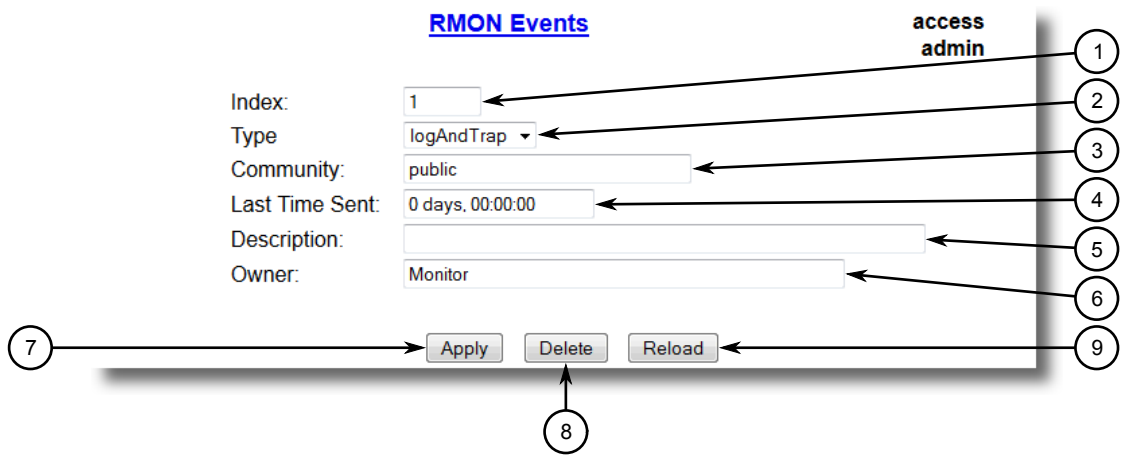


Figure 60: RMON Events Form

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

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

Parameter	Description
Index	**Synopsis:** 1 to 65535 **Default:** 3 The index of this RMON Event record.
Type	**Synopsis:** { none, log, snmpTrap, logAndTrap } **Default:** logAndTrap The type of notification that the probe will make about this event. In the case of 'log', an entry is made in the RMON Log table for each event. In the case of snmp_trap, an SNMP trap is sent to one or more management stations.
Community	**Synopsis:** Any 31 characters **Default:** public If the SNMP trap is to be sent, it will be sent to the SNMP community specified by this string.
Last Time Sent	**Synopsis:** DDDD days, HH:MM:SS The time from last reboot at the time this event entry last generated an event. If this entry has not generated any events, this value will be 0.
Description	**Synopsis:** Any 127 characters **Default:** EV2-Rise A comment describing this event.
Owner	**Synopsis:** Any 127 characters **Default:** Monitor The owner of this event record. It is suggested to start this string withword 'monitor'.

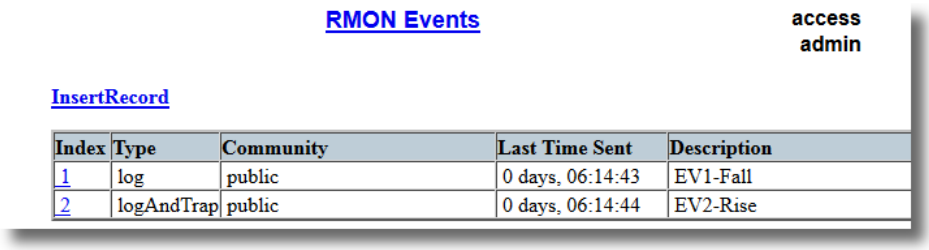
4. Click **Apply**.

Section 3.10.3.3

Deleting an RMON Event

To delete an RMON event, do the following:

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



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

Figure 61: RMON Events Table

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

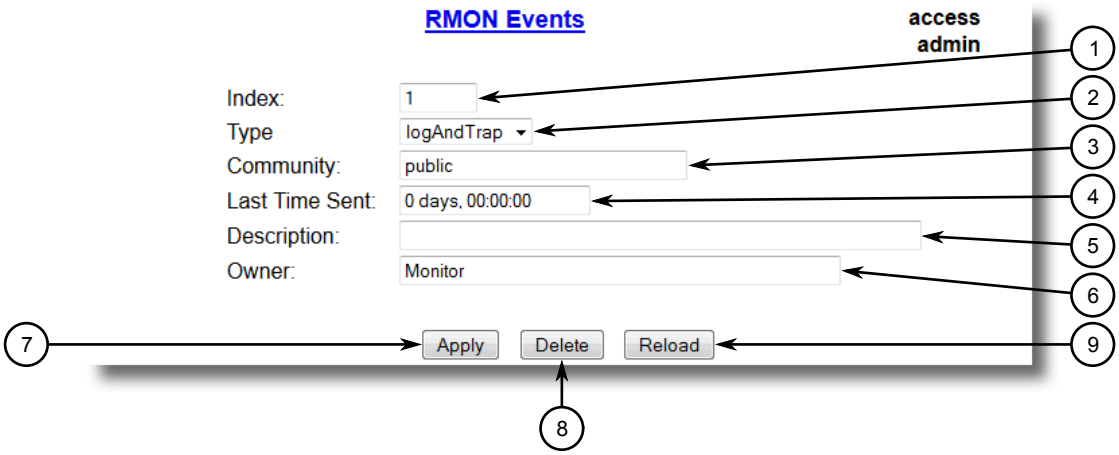


Figure 62: RMON Events Form

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

3. Click **Delete**.

Section 3.11

Upgrading/Downgrading Firmware

The following section describes how to upgrade and downgrade the firmware.

CONTENTS

- Section 3.11.1, "Upgrading Firmware"

- Section 3.11.2, “Downgrading Firmware”

Section 3.11.1

Upgrading Firmware

Upgrading RUGGEDCOM ROS firmware, including the main, bootloader and FPGA firmware, may be necessary to take advantage of new features or bug fixes. Binary firmware images are available from Siemens. Visit www.siemens.com/ruggedcom to determine which versions/updates are available or contact Siemens Customer Support.

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

IMPORTANT!
Non-Controlled (NC) versions of RUGGEDCOM ROS can not be upgraded to Controlled firmware versions. However, Controlled firmware versions can be upgraded to an NC firmware version.

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

To upgrade the RUGGEDCOM ROS firmware, do the following:

1. Upload a different version of the binary firmware image to the device. For more information, refer to Section 3.4, “Uploading/Downloading Files” .
2. Reset the device to complete the installation. For more information, refer to Section 3.12, “Resetting the Device” .
3. Access the CLI shell and verify the new software version has been installed by typing **`version`**. The currently installed versions of the main and boot firmware are displayed.

```
>version
Current ROS-CF52 Boot Software v2.20.0 (Jan 29 2013 13:25)
Current ROS-CF52 Main Software v4.0 (Feb 2 2013 09:33)
```

Section 3.11.2

Downgrading Firmware

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

IMPORTANT!
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.

IMPORTANT!
Non-Controlled (NC) versions of RUGGEDCOM ROS can not be downgraded to Controlled firmware versions. However, Controlled firmware versions can be downgraded to an NC firmware version.

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 Section 2.2, "Logging In" .
3. Make a local copy of the current configuration file. For more information, refer to Section 3.4, "Uploading/ Downloading Files" .

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

4. Restore the device to its factory defaults. For more information, refer to Section 3.3, "Restoring Factory Defaults" .
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 Section 3.11.1, "Upgrading Firmware" .
6. Press **Ctrl-S** to access the CLI.
7. Clear all logs by typing:

   ```
   clearlogs
   ```

8. Clear all alarms by typing:

   ```
   clearalarms
   ```

   IMPORTANT!
   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.

Section 3.12

Resetting the Device

To reset the device, do the following:

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

Figure 63: Reset Device Form

1. Confirm Button

2. Click **Confirm**.

Section 3.13

Decommissioning the Device

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

To decommission the device, do the following:

1. Disconnect all network cables from the device.
2. Connect to the device via the RS-232 serial console port. For more information, refer to Section 2.1.1, "Connecting Directly" .
3. Restore all factory default settings for the device. For more information, refer to Section 3.3, "Restoring Factory Defaults" .
4. Access the CLI. For more information, refer to Section 2.6, "Using the Command Line Interface" .
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 Section 3.4, "Uploading/Downloading Files" .
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.

4 System Administration

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

CONTENTS

- Section 4.1, "Configuring the System Information"
- Section 4.2, "Customizing the Login Screen"
- Section 4.3, "Configuring Passwords"
- Section 4.4, "Clearing Private Data"
- Section 4.5, "Enabling/Disabling the Web Interface"
- Section 4.6, "Managing Alarms"
- Section 4.7, "Managing the Configuration File"
- Section 4.8, "Managing an Authentication Server"

Section 4.1

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.

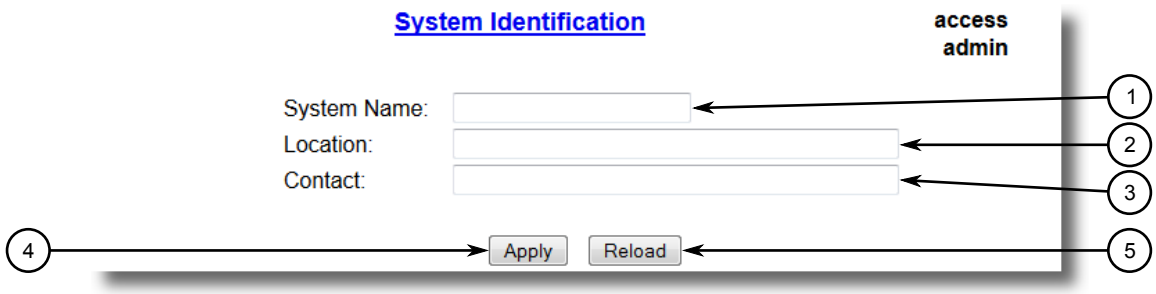


Figure 64: System Identification Form

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

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

Parameter	Description
System Name	**Synopsis:** Any 24 characters

Parameter	Description
	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:** Any 49 characters 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:** Any 49 characters 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**.

Section 4.2

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 Section 3.4, "Uploading/Downloading Files" .

Section 4.3

Configuring Passwords

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

- Guest
- Operator
- Admin

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

Rights	User Type		
	Guest	Operator	Admin
View Settings	✓	✓	✓
Clear Logs	×	✓	✓
Reset Alarms	×	✓	✓
Clear Statistics	×	✓	✓

Rights	User Type		
	Guest	Operator	Admin
Change Basic Settings	×	✓	✓
Change Advanced Settings	×	×	✓
Run Commands	×	×	✓

Default passwords are configured for each user type initially. It is strongly recommended that these be changed before the device is commissioned.

NOTE
Users can also be verified through a RADIUS or TACACS+ server. When enabled for authentication and authorization, the RADIUS or TACACS+ server will be used in the absence of any local settings. For more information about configuring a RADIUS or TACACS+ server, refer to *Section 4.8, "Managing an Authentication Server"* .

CAUTION!
To prevent unauthorized access to the device, make sure to change the default passwords for each profile before commissioning the device.

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.

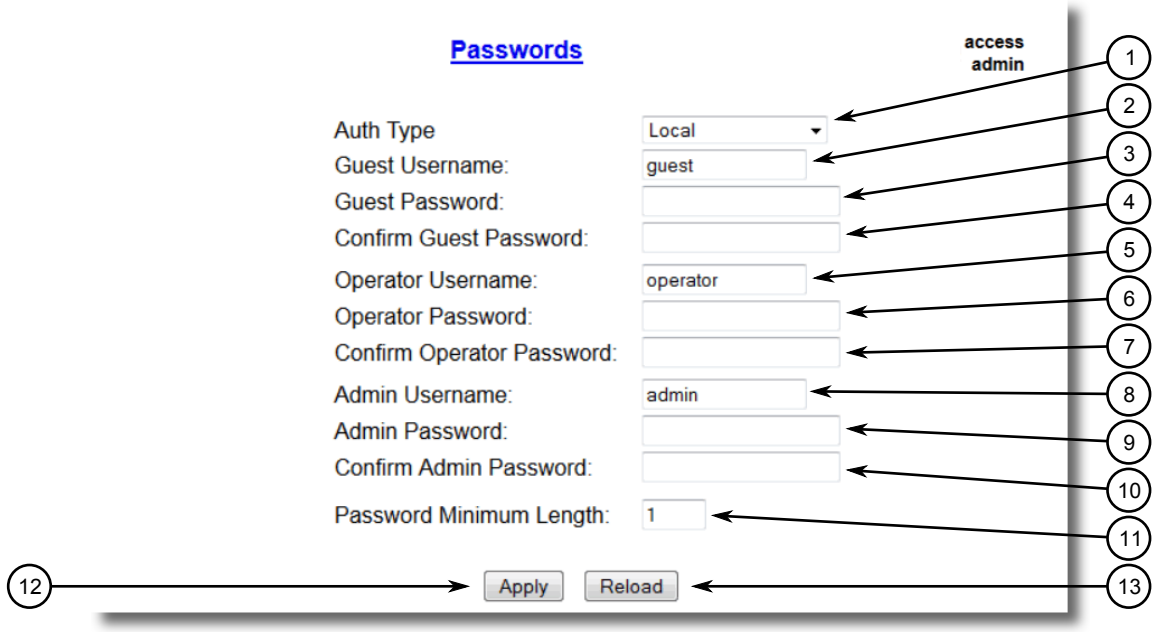


Figure 65: Configure Passwords Form

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

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 *Section 4.6, "Managing Alarms"* *.*

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

Parameter	Description
Auth Type	**Synopsis:** { Local, RADIUS, TACACS+, RADIUSorLocal, TACACS +orLocal } **Default:** Local Password can be authenticated using localy configured values, or remote RADIUS or TACACS+ server. Setting value to any of combinations that involve RADIUS or TACACS+ require Security Server Table to be configured. Settings: • Local - Authentication from the local Password Table. • RADIUS - Authentication using a RADIUS server. • TACACS+ - Authentication using a TACACS+ server. • RADIUSOrLocal - Authentication using RADIUS. If the server cannot be reached, authenticate from the local Password Table. • TACACS+OrLocal - Authentication using TACACS+. If the server cannot be reached, authenticate from the local Password Table **NOTE** *For console access, local credentials will always be checked first regardless of the device configuration. If server authentication is required, requests to the server will be sent only if local authentication fails.*
Guest Username	**Synopsis:** Any 15 characters **Default:** guest Related password is in field Guest Password; view only, cannot change settings or run any commands.
Guest Password	**Synopsis:** 19 character ASCII string Related username is in field Guest Username; view only, cannot change settings or run any commands.
Confirm Guest Password	**Synopsis:** 19 character ASCII string Related username is in field Guest Username; view only, cannot change settings or run any commands.
Operator Username	**Synopsis:** Any 15 characters **Default:** operator

Parameter	Description
	Related password is in field Oper Password; cannot change settings; can reset alarms, statistics, logs, etc.
Operator Password	**Synopsis:** 19 character ASCII string Related username is in field Oper Username; cannot change settings; can reset alarms, statistics, logs, etc
Confirm Operator Password	**Synopsis:** 19 character ASCII string Related username is in field Oper Username; cannot change settings; can reset alarms, statistics, logs, etc.
Admin Username	**Synopsis:** Any 15 characters **Default:** admin Related password is in field Admin Password; full read/write access to all settings and commands.
Admin Password	**Synopsis:** 19 character ASCII string Related username is in field Admin Username; full read/write access to all settings and commands.
Confirm Admin Password	**Synopsis:** 19 character ASCII string Related username is in field Admin Username; full read/write access to all settings and commands.
Password Minimum Length	**Synopsis:** 1 to 17 **Default:** 1 Configure the password string minimum length. The new password shorter than the minimum length will be rejected.

3. Click **Apply**.

Section 4.4

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 Section 2.1.1, “Connecting Directly” .
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.

Section 4.5

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* *Section 3.9, "Configuring IP Services"* .

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 Section 2.6, "Using the Command Line Interface" .
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.

Section 4.6

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 th 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* *Section 3.10.2, "Managing RMON Alarms"* .

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.

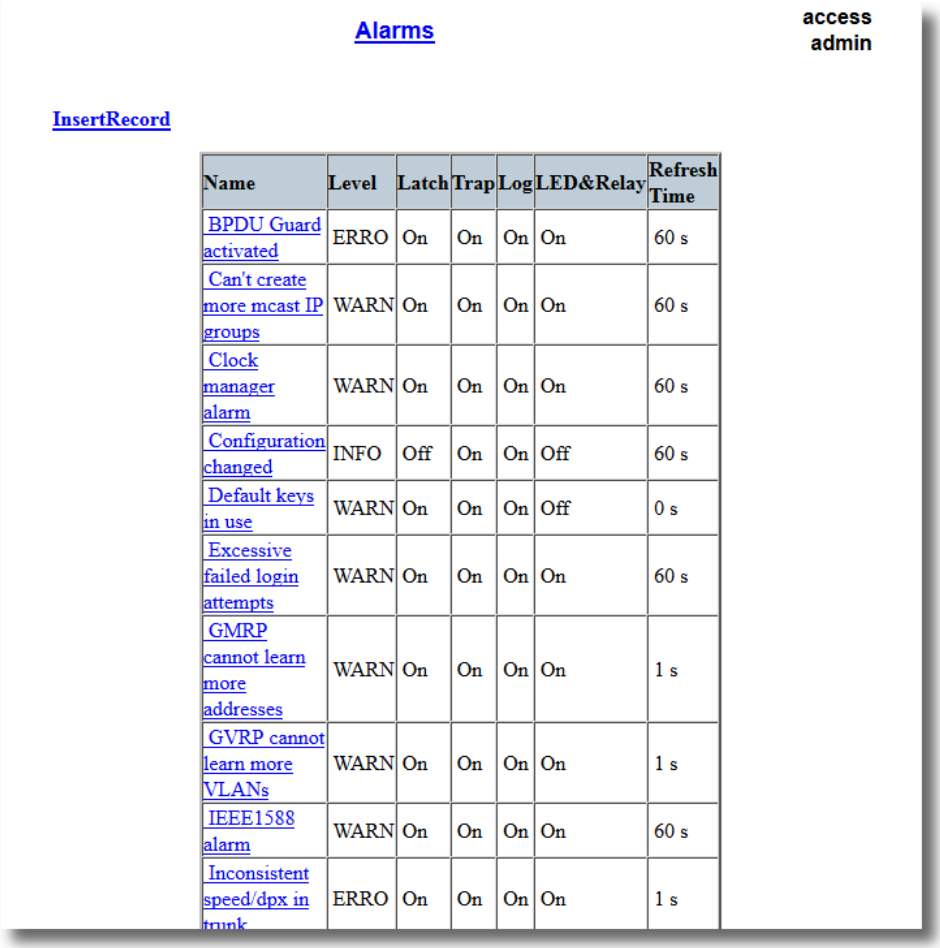
CONTENTS

- Section 4.6.1, "Viewing a List of Pre-Configured Alarms"
- Section 4.6.2, "Viewing and Clearing Latched Alarms"
- Section 4.6.3, "Configuring an Alarm"
- Section 4.6.4, "Authentication Related Security Alarms"

Section 4.6.1

Viewing a List of Pre-Configured Alarms

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



Alarms

access admin

InsertRecord

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

Figure 66: Alarms Table

> **NOTE**
> *This list of alarms (configurable and non-configurable) is accessible through the Command Line Interface (CLI) using the* **`alarms`**. *For more information, refer to* *Section 2.6.1, "Available CLI Commands"* .

For information about modifying a pre-configured alarm, refer to Section 4.6.3, "Configuring an Alarm" .

Section 4.6.2

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.

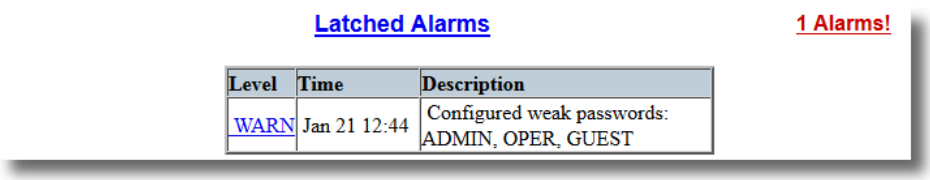


Figure 67: Latched Alarms Table

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

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

Figure 68: Clear Latched Alarms Form

1. Confirm Button

2. Click **Confirm**.

Section 4.6.3

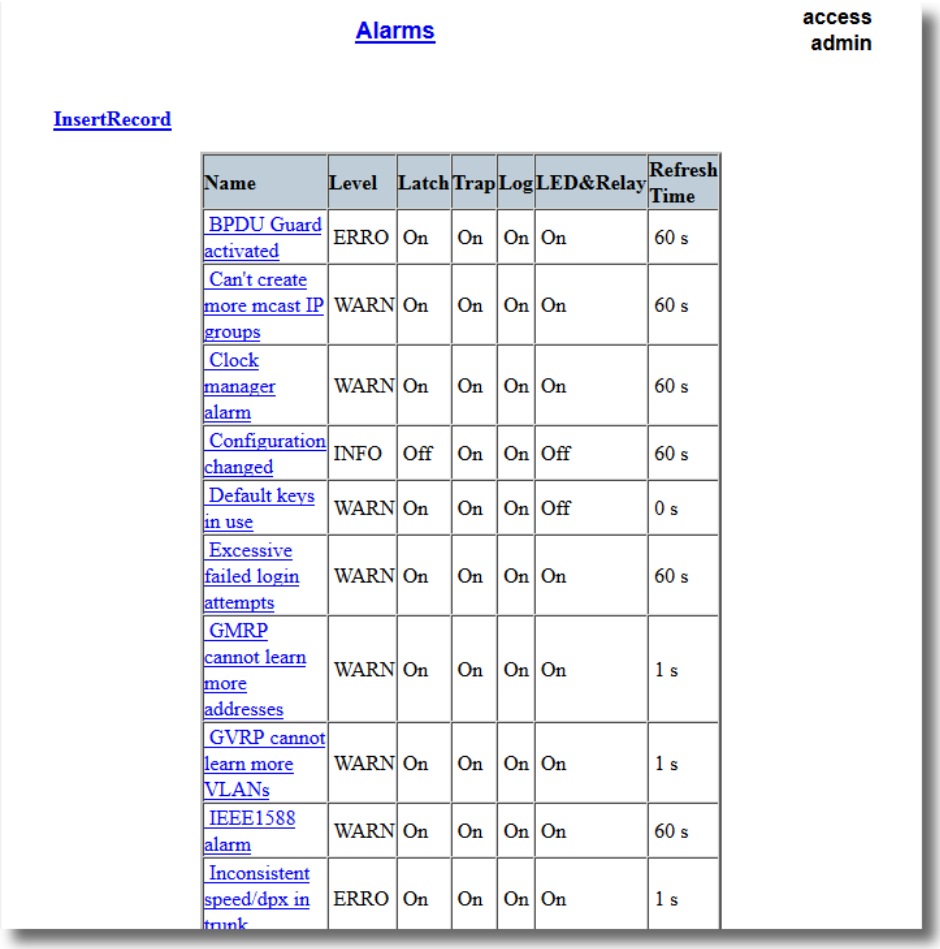
Configuring an Alarm

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

To configuring an alarm, do the following:

IMPORTANT!
Critical and Alert level alarms are not configurable and cannot be disabled.

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



Alarms

access
admin

InsertRecord

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

Figure 69: Alarms Table

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

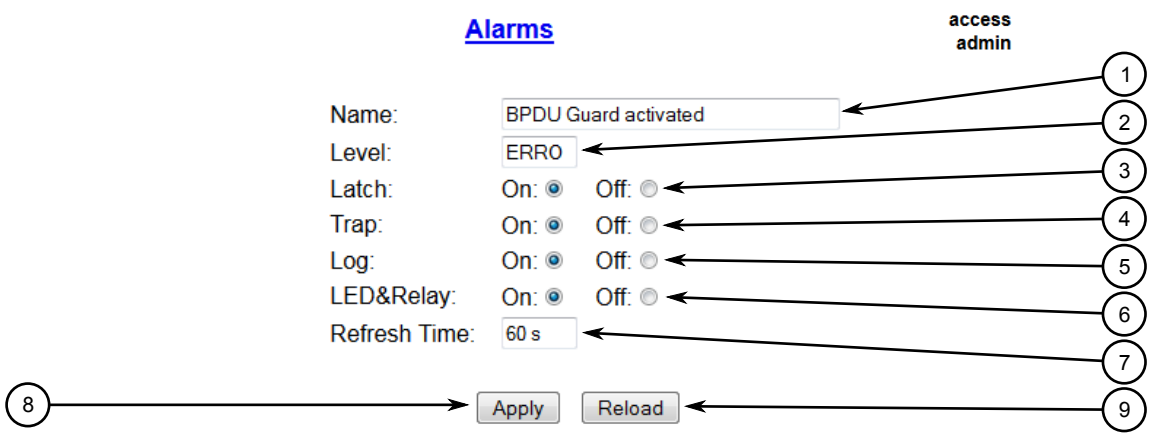


Figure 70: Alarms Form

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

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

Parameter	Description
Name	**Synopsis:** Any 34 characters **Default:** sys_alarm The alarm name, as obtained through the **`alarms`** CLI command.
Level	**Synopsis:** { EMRG, ALRT, CRIT, ERRO, WARN, NOTE, INFO, DEBG } Severity level of the alarm: • EMERG - The device has had a serious failure that caused a system reboot. • ALERT - The device has had a serious failure that did not cause a system reboot. • CRITICAL - The device has a serious unrecoverable problem. • ERROR - The device has a recoverable problem that does not seriously affect operation. • WARNING - Possibly serious problem affecting overall system operation. • NOTIFY - Condition detected that is not expected or not allowed. • INFO - Event which is a part of normal operation, e.g. cold start, user login etc. • DEBUG - Intended for factory troubleshooting only. This parameter is not configurable.
Latch	**Synopsis:** { On, Off } **Default:** Off Enables latching occurrence of this alarm in the Alarms Table.
Trap	**Synopsis:** { On, Off } **Default:** Off Enables sending an SNMP trap for this alarm.
Log	**Synopsis:** { On, Off } **Default:** Off

Parameter	Description
	Enables logging the occurrence of this alarm in syslog.txt.
LED & Relay	**Synopsis:** { On, Off } **Default:** Off Enables LED and fail-safe relay control for this alarm. If latching is not enabled, this field will remain disabled.
Refresh Time	**Synopsis:** 0 s to 60 s **Default:** 60 s Refreshing time for this alarm.

4. Click **Apply**.

Section 4.6.4

Authentication Related Security Alarms

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

CONTENTS

- Section 4.6.4.1, "Security Alarms for Login Authentication"
- Section 4.6.4.2, "Security Messages for Port Authentication"

Section 4.6.4.1

Security Alarms for Login Authentication

RUGGEDCOM ROS provides various logging options related to login authentication. A user can log into a RUGGEDCOM ROS device in three different ways: 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 *Section 4.6.3, "Configuring an Alarm"* .

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 Section 1.9, "SSH and SSL Keys and Certificates" .

> **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

Section 4.6.4.2

Security Messages for Port Authentication

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

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

MAC Address Authorization Failure

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

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

Secure Port X Learned MAC Addr on VLAN X

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

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

Port Security Violated

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

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

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

Section 4.7

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.

CONTENTS

- Section 4.7.1, “Configuring Data Encryption”
- Section 4.7.2, “Updating the Configuration File”

Section 4.7.1

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.

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

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

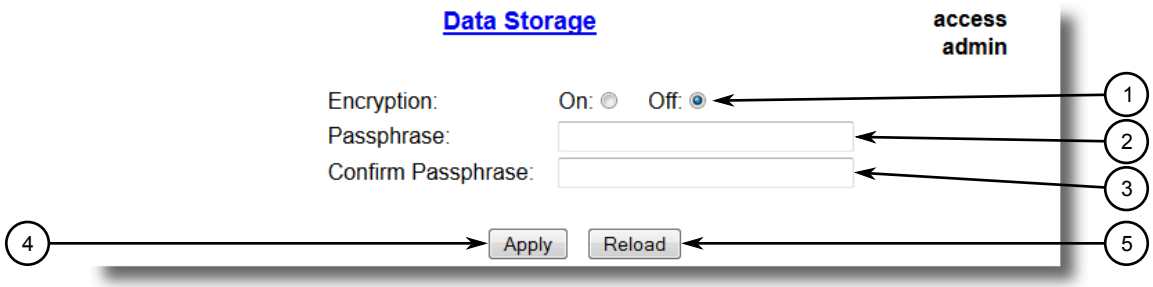


Figure 71: Data Storage Form

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

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

Parameter	Description
Encryption	**Synopsis:** { On, Off } Enable/disable encryption of data in configuration file.
Passphrase	**Synopsis:** 31 character ascii string This passphrase is used as a secret key to encrypt the configuration data. Encrypted data can be decrypted by any device configured with the same passphrase.
Confirm Passphrase	**Synopsis:** 31 character ascii string

Parameter	Description
	This passphrase is used as a secret key to encrypt the configuration data. Encrypted data can be decrypted by any device configured with the same passphrase.

3. Click **Apply**.

Section 4.7.2

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 *Section 3.4, "Uploading/Downloading Files"* .

- 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,
```

Section 4.8

Managing an Authentication Server

The following section describes how to setup and configure an authentication server.

CONTENTS

- Section 4.8.1, "Managing RADIUS Authentication"

- Section 4.8.2, “Managing TACACS+ Authentication”

Section 4.8.1

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).

NOTE
For more information about the RADIUS protocol, refer to RFC 2865.

For more information about the Extensible Authentication Protocol (EAP), refer to RFC 3748.

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

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

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

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

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

Attribute	Value
User-Name	{ The username as derived from the client's EAP identity response }
NAS-IP-Address	{ The Network Access Server IP address }
Service-Type	2
Frame-MTU	1500

Attribute	Value
EAP-Message[a]	{ A message(s) received from the authenticating peer }

[a] *EAP-Message is an extension attribute for RADIUS, as defined by RFC 2869.*

CONTENTS

- Section 4.8.1.1, "Configuring the RADIUS Server"
- Section 4.8.1.2, "Configuring the RADIUS Client"

Section 4.8.1.1

Configuring the RADIUS Server

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

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

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

Section 4.8.1.2

Configuring the RADIUS Client

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

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

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

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

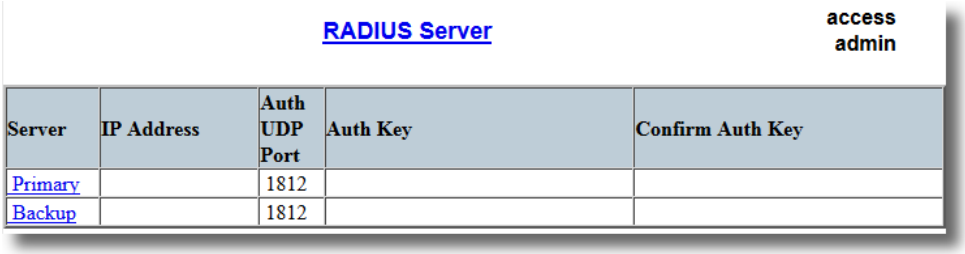


Figure 72: RADIUS Server Table

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

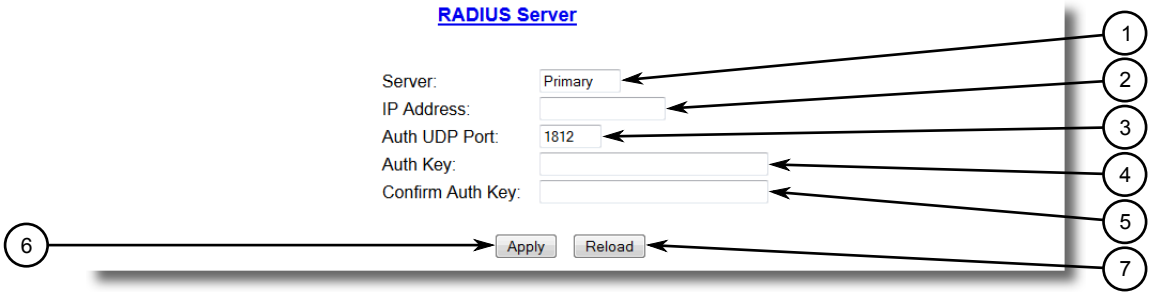


Figure 73: RADIUS Server Form

1. Server Box **2.** IP Address Box **3.** Auth UDP Port Box **4.** Auth Key Box **5.** Confirm Auth Key Box **6.** Apply Button **7.** Reload Button

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

Parameter	Description
Server	**Synopsis:** Any 8 characters **Default:** Primary This field tells whether this configuration is for a Primary or a Backup Server.
IP Address	**Synopsis:** ###.###.###.### where ### ranges from 0 to 255 The Server IP Address.
Auth UDP Port	**Synopsis:** 1 to 65535 **Default:** 1812 The IP Port on server.
Auth Key	**Synopsis:** 31 character ASCII string The authentication key to be shared with server.
Confirm Auth Key	**Synopsis:** 31 character ASCII string The authentication key to be shared with server.

4. Click **Apply**.

Section 4.8.2

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.

The following section describes how to configure TACACs+ authentication.

CONTENTS

- Section 4.8.2.1, “Configuring TACACS+”
- Section 4.8.2.2, “Configuring User Privileges”

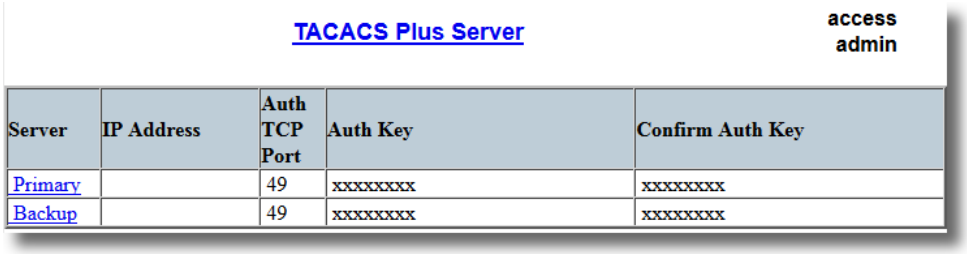
Section 4.8.2.1

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.

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

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



TACACS Plus Server

access admin

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

Figure 74: TACACS Plus Server Table

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

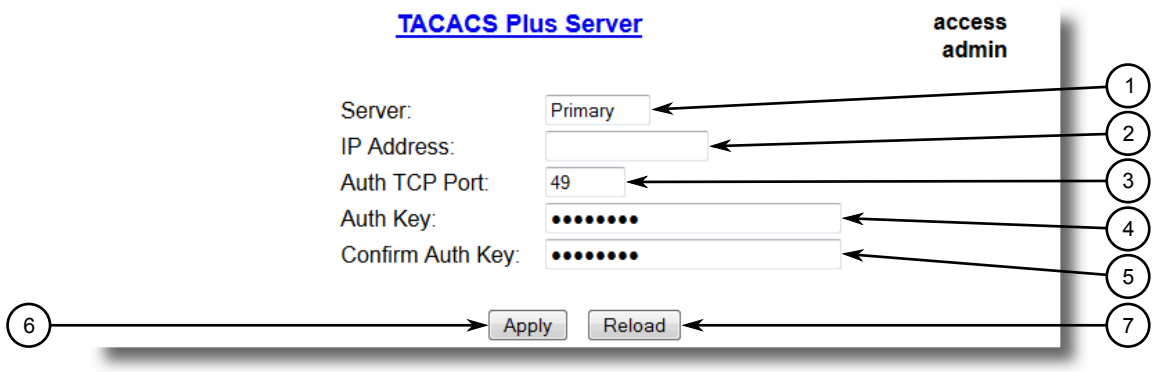


Figure 75: TACACS Plus Server Form

1. Server Box **2.** IP Address Box **3.** Auth TCP Port Box **4.** Auth Key Box **5.** Confirm Key Box **6.** Apply Button **7.** Reload Button

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

Parameter	Description
Server	**Synopsis:** Any 8 characters **Default:** Primary This field tells whether this configuration is for a Primary or a Backup Server.
IP Address	**Synopsis:** ###.###.###.### where ### ranges from 0 to 255 The Server IP Address.
Auth TCP Port	**Synopsis:** 1 to 65535 **Default:** 49 The IP Port on server.
Auth Key	**Synopsis:** 31 character ascii string **Default:** mySecret The authentication key to be shared with server.
Confirm Auth Key	**Synopsis:** 31 character ascii string 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 Section 4.8.2.2, "Configuring User Privileges" .
5. Click **Apply**.

Section 4.8.2.2

Configuring User Privileges

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

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

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.

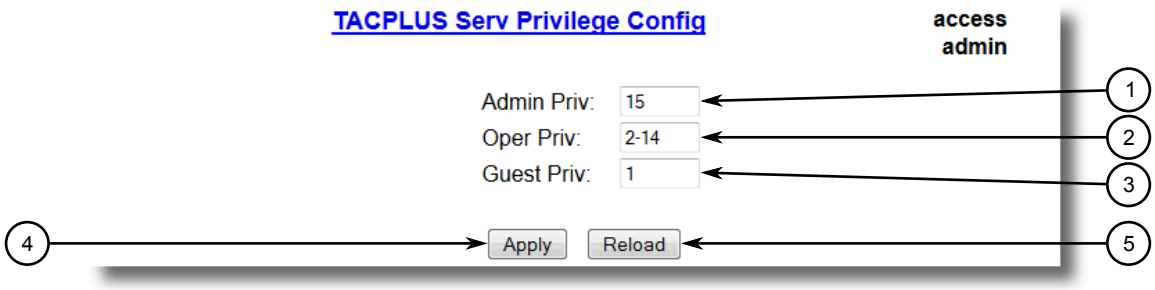


Figure 76: TACPLUS Serv Privilege Config Form

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

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

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

3. Click **Apply**.

5 Setup and Configuration

This chapter describes how to setup and configure the device for use on a network using the various features available in RUGGEDCOM ROS.

CONTENTS

- Section 5.1, "Managing Virtual LANs"
- Section 5.2, "Managing Spanning Tree Protocol"
- Section 5.3, "Managing Classes of Service"
- Section 5.4, "Managing MAC Addresses"
- Section 5.5, "Managing Time Services"
- Section 5.6, "Managing SNMP"
- Section 5.7, "Managing Network Discovery"
- Section 5.8, "Managing Multicast Filtering"
- Section 5.9, "Managing Port Security"
- Section 5.10, "Managing Link Aggregation"

Section 5.1

Managing Virtual LANs

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

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

VLANs are created in three ways:

- **Explicitly**
  Static VLANs can be created in the switch. For more information about static VLANs, refer to Section 5.1.5, "Managing Static VLANs" .
- **Implicitly**
  When a VLAN ID (VID) is set for a port-based VLAN, static MAC address or IP interface, an appropriate VLAN is automatically created if it does not yet exist.
- **Dynamically**
  VLANs can be learned through GVRP. For more information about GVRP, refer to Section 5.1.1.8, "GARP VLAN Registration Protocol (GVRP)"

For more information about VLANs, refer to Section 5.1.1, "VLAN Concepts" .

CONTENTS

- Section 5.1.1, "VLAN Concepts"

- Section 5.1.2, “Viewing a List of VLANs”
- Section 5.1.3, “Configuring VLANs Globally”
- Section 5.1.4, “Configuring VLANs for Specific Ethernet Ports”
- Section 5.1.5, “Managing Static VLANs”

Section 5.1.1

VLAN Concepts

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

CONTENTS

- Section 5.1.1.1, “Tagged vs. Untagged Frames”
- Section 5.1.1.2, “Native VLAN”
- Section 5.1.1.3, “The Management VLAN”
- Section 5.1.1.4, “Edge and Trunk Port Types”
- Section 5.1.1.5, “Ingress and Egress Rules”
- Section 5.1.1.6, “Forbidden Ports List”
- Section 5.1.1.7, “VLAN-Aware and VLAN-Unaware Modes”
- Section 5.1.1.8, “GARP VLAN Registration Protocol (GVRP)”
- Section 5.1.1.9, “PVLAN Edge”
- Section 5.1.1.10, “QinQ”
- Section 5.1.1.11, “VLAN Advantages”

Section 5.1.1.1

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.

Section 5.1.1.2

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.

Section 5.1.1.3

The Management VLAN

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

Section 5.1.1.4

Edge and Trunk Port Types

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

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

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

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

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

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

For more information about the Forbidden Ports list, refer to *Section 5.1.1.6, "Forbidden Ports List"* .

Port Type	VLANs Supported	PVID Format	Usage
Edge	1 (Native) Configured	Untagged	*VLAN Unaware Networks*: All frames are sent and received without the need for VLAN tags.
		Tagged	*VLAN Aware Networks*: VLAN traffic domains are enforced on a single VLAN.
Trunk	All Configured	Tagged or Untagged	*Switch-to-Switch Connections*: VLANs must be manually created and administered, or can be dynamically learned through GVRP. *Multiple-VLAN End Devices*: Implement connections to end devices that support multiple VLANs at the same time.

Section 5.1.1.5

Ingress and Egress Rules

Ingress and egress rules determine how traffic is received and transmitted by the switch.

Ingress rules are applied as follows to all frame when they are received by the switch:

Frame Received[a]	Untagged	Priority Tagged (VID = 0)	Tagged (Valid VID)
VLAN ID associated with the frame	PVID	PVID	VID in the Tag
Frame dropped due to its tagged/untagged format	No	No	No
Frame dropped if the ingress port is not a member of the VLAN the frame is associated with and ingress filtering is enabled			Yes

[a] *Does not depend on the ingress port's VLAN configuration parameters.*

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

Egress Port Type	On Egress Port's Native VLAN	On Other VLAN	
		Port Is a Member Of the VLAN	Port Is Not a Member Of the VLAN
Edge	According to the egress port's **PVID Format** parameter	Dropped	
Trunk		Tagged	Dropped

Section 5.1.1.6

Forbidden Ports List

Each VLAN can be configured to exclude ports from membership in the VLAN using the forbidden ports list. For more information, refer to Section 5.1.5.2, “Adding a Static VLAN” .

Section 5.1.1.7

VLAN-Aware and VLAN-Unaware Modes

The native operation mode for an IEEE 802.1Q compliant switch is VLAN-aware. Even if a specific network architecture does not use VLANs, RUGGEDCOM ROS's default VLAN settings allow the switch to still operate in a VLAN-aware mode, while providing functionality required for almost any network application. However, the IEEE 802.1Q standard defines a set of rules that must be followed by all VLAN-aware switches:

- Valid VIDs are within the range of 1 to 4094. VIDs equal to 0 or 4095 are invalid.
- Each frame ingressing a VLAN-aware switch is associated with a valid VID.
- Each frame egressing a VLAN-aware switch is either untagged or tagged with a valid VID. Priority-tagged frames with an invalid VID will never sent out by a VLAN-aware switch.

NOTE

Some applications have requirements conflicting with IEEE 802.Q1 native mode of operation. For example, some applications explicitly require priority-tagged frames to be received by end devices.

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

In that mode:

- *Frames ingressing a VLAN-unaware device are not associated with any VLAN*
- *Frames egressing a VLAN-unaware device are sent out unmodified (i.e. in the same untagged, 802.1Q-tagged or priority-tagged format as they were received)*

Section 5.1.1.8

GARP VLAN Registration Protocol (GVRP)

GARP VLAN Registration Protocol (GVRP) is a standard protocol built on GARP (Generic Attribute Registration Protocol) to automatically distribute VLAN configuration information in a network. Each switch in a network needs only to be configured with VLANs it requires locally. VLANs configured elsewhere in the network are learned through GVRP. A GVRP-aware end station (i.e. PC or Intelligent Electronic Device) configured for a particular VID can be connected to a trunk on a GVRP-aware switch and automatically become part of the desired VLAN.

When a switch sends GVRP bridge protocol data units (BPDUs) out of all GVRP-enabled ports, GVRP BPDUs advertise all the VLANs known to that switch (configured manually or learned dynamically through GVRP) to the rest of the network.

When a GVRP-enabled switch receives a GVRP BPDU advertising a set of VLANs, the receiving port becomes a member of those advertised VLANs and the switch begins advertising those VLANs through all the GVRP-enabled ports (other than the port on which the VLANs were learned).

To improve network security using VLANs, GVRP-enabled ports may be configured to prohibit the learning of any new dynamic VLANs but at the same time be allowed to advertise the VLANs configured on the switch.

The following is an example of how to use GVRP:

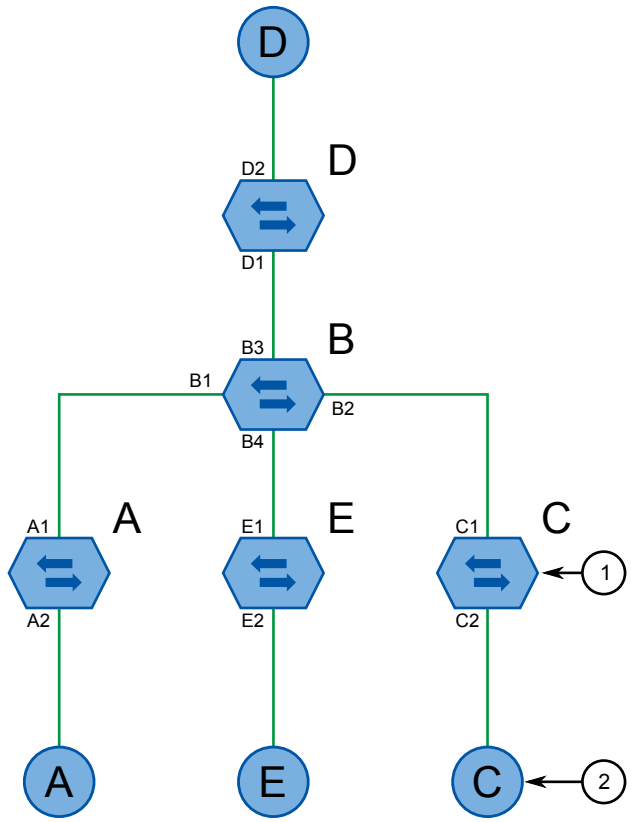


Figure 77: Using GVRP

1. Switch **2.** End Node

- Switch B is the core switch, all others are edge switches
- Ports A1, B1 to B4, C1, D1, D2 and E1 are GVRP aware

- Ports B1 to B4, D1 and D2 are set to advertise and learn
- Ports A1, C1 and E1 are set to advertise only
- Ports A2, C2 and E2 are edge ports
- End node D is GVRP aware
- End nodes A, E and C are GVRP unaware
- Ports A2 and C2 are configured with PVID 7
- Port E2 is configured with PVID 20
- End node D is interested in VLAN 20, hence VLAN 20 is advertised by it towards switch D
- D2 becomes a member of VLAN 20
- Ports A1 and C1 advertise VID 7
- Ports B1 and B2 become members of VLAN 7
- Ports 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 Section 5.1.4, “Configuring VLANs for Specific Ethernet Ports” .

Section 5.1.1.9

PVLAN Edge

Private VLAN (PVLAN) Edge isolates multiple VLAN Edge ports from each other on a single device. When VLAN Edge ports are configured as *protected*, they are prohibited from sending frames to one another, but are still permitted to send frames to other, non-protected ports within the same VLAN. This protection extends to all traffic on the VLAN, including unicast, multicast and broadcast traffic.

For more information about how to configure a port as *protected*, refer to Section 5.1.4, “Configuring VLANs for Specific Ethernet Ports” .

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.

Section 5.1.1.10

QinQ

QinQ, also referred to as Stacked VLANs, port bridging, double VLAN-tagging and Nested VLANs, is used to overlay a private Layer 2 network over a public Layer 2 network.

A large network service provider, for example, might have several clients whose networks each use multiple VLANs. It is likely the VLAN IDs used by these different client networks would conflict with one another, were they mixed together in the provider's network. Using double QinQ, each client network could be further tagged using a client-specific VID at the edges where the clients' networks are connected to the network service provider's infrastructure.

Any tagged frames ingressing an edge port of the service provider's switch are tagged with VIDs of the customer’s private network. When those frames egress the switch's QinQ-enabled port into the service provider network, the switch always adds an extra tag (called an *outer tag*) on top of the frame's original VLAN tag (called an *inner tag*).

The outer tag VID is the PVID of the frame's ingress edge port. This means that traffic from an individual customer is tagged with their unique VID and is thus segregated from other customer's 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.

When double-tagged frames leave the service provider network, they egress a QinQ-enabled port of another switch. The switch strips the outer tag while associating the frames with the VID extracted from it before stripping. Thus, the frames are switched to appropriate edge ports (i.e. customers).

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.

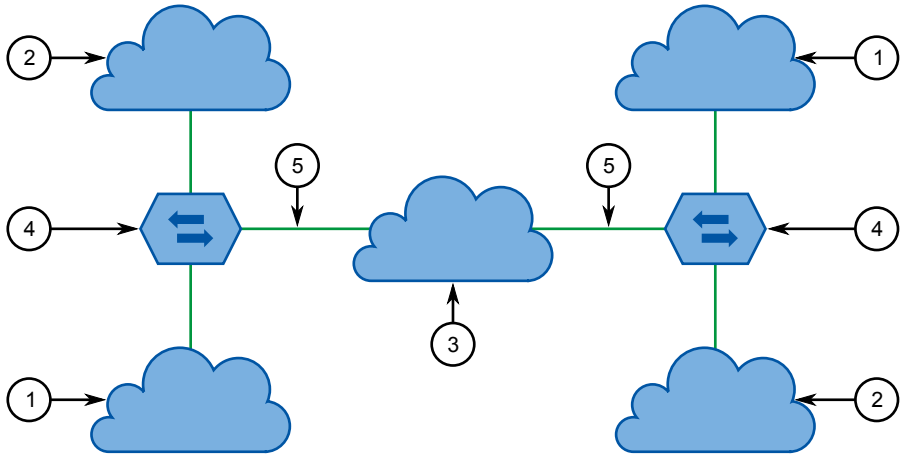


Figure 78: Using QinQ

1. Customer 1 (PVID is X) **2.** Customer 2 (PVID is Y) **3.** Network Service Provider Infrastructure **4.** Switch **5.** 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.

Section 5.1.1.11

VLAN Advantages

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

Traffic Domain Isolation

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

Unnecessary broadcast traffic can be restricted to the VLAN that requires it. Broadcast storms in one VLAN need not affect users in other VLANs.

Hosts on one VLAN can be prevented from accidentally or deliberately assuming the IP address of a host on another VLAN.

The use of creative bridge filtering and multiple VLANs can carve seemingly unified IP subnets into multiple regions policed by different security/access policies.

Multi-VLAN hosts can assign different traffic types to different VLANs.

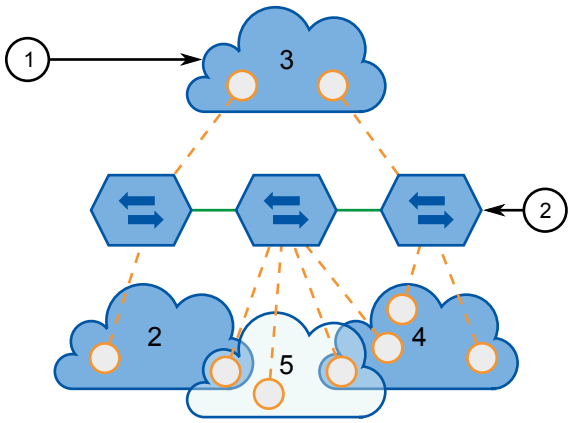


Figure 79: Multiple Overlapping VLANs

1. VLAN **2.** Switch

Administrative Convenience

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

Reduced Hardware

Without VLANs, traffic domain isolation requires the use of separate bridges for separate networks. VLANs eliminate the need for separate bridges.

The number of network hosts may often be reduced. Often, a server is assigned to provide services for independent networks. These hosts may be replaced by a single, multi-horned host supporting each network on its own VLAN. This host can perform routing between VLANs.

Multi-VLAN hosts can assign different traffic types to different VLANs.

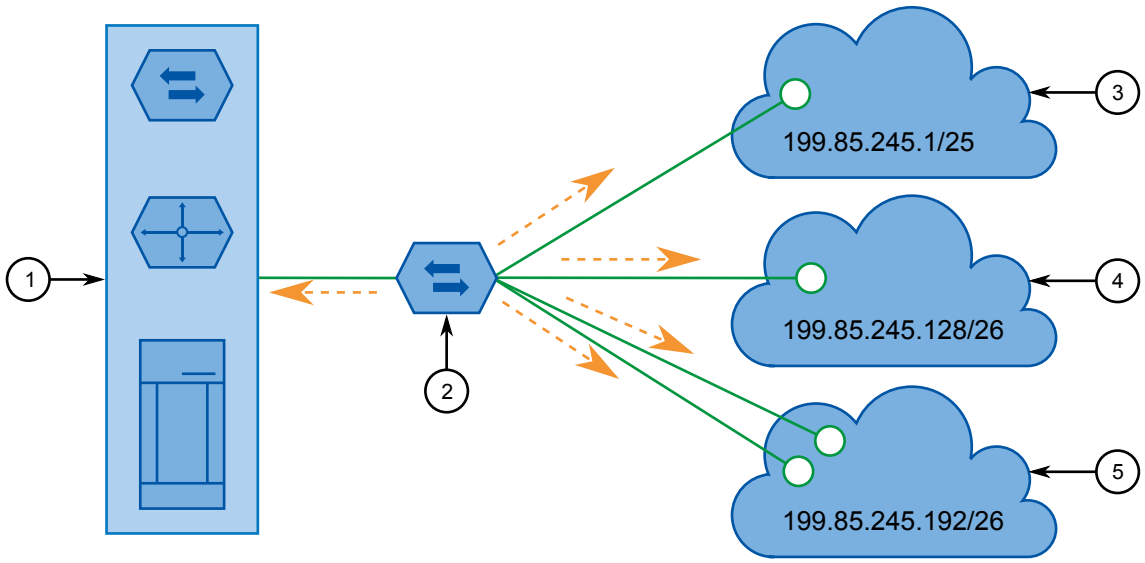


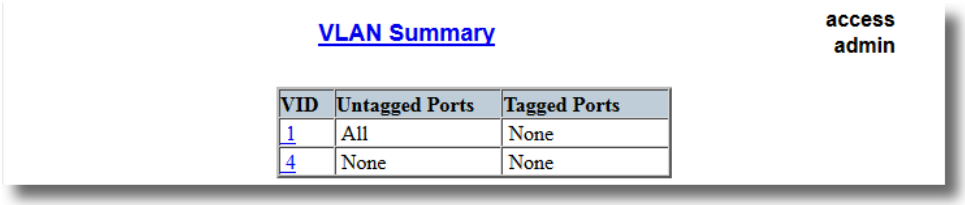
Figure 80: Inter-VLAN Communications

1. Server, Router or Layer 3 Switch **2.** Switch **3.** VLAN 2 **4.** VLAN 3 **5.** VLAN 4

Section 5.1.2

Viewing a List of VLANs

To view a list of all VLANs, whether they were created statically, implicitly or dynamically , navigate to ***Virtual LANs » View VLAN Summary*** . The **VLAN Summary** table appears.



VID	Untagged Ports	Tagged Ports
1	All	None
4	None	None

Figure 81: VLAN Summary Table

If a VLANs are not listed, add static VLANs as needed. For more information, refer to Section 5.1.5.2, “Adding a Static VLAN” .

Section 5.1.3

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.

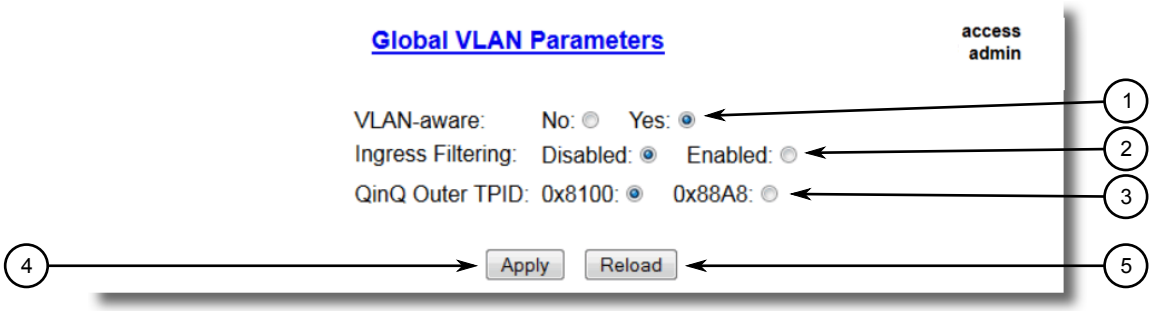


Figure 82: Global VLAN Parameters Form

1. VLAN-aware Options **2.** Ingress Filtering Options **3.** QinQ Outer TPID options **4.** Apply Button **5.** Reload Button

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

Parameter	Description
VLAN-aware	**Synopsis:** { No, Yes } **Default:** Yes Set either VLAN-aware or VLAN-unaware mode of operation.
Ingress Filtering	**Synopsis:** { Disabled, Enabled } **Default:** Disabled Enables or disables VLAN ingress filtering on all ports. When enabled, any tagged packet arriving at a port, which is not a member of a VLAN with which that packet is associated, is dropped. When disabled, packets are not dropped. **NOTE** *Ingress filtering has no effect when ports are in either VLAN-unaware mode or Q-in-Q mode.*
QinQ Outer TPID	**Synopsis:** { 0x8100, 0x88A8 } **Default:** 0x8100 Selects an Ethertype to be used as the Tag Protocol Identifier (TPID) on VLAN QinQ ports when QinQ is enabled. Frames that ingress a VLAN QinQ port will be identified as outer VLAN tagged if the first Ethertype matches this value; an outer VLAN tag with the TPID field assigned to this value will be inserted to frames that egress a VLAN QinQ port. **NOTE** *When QinQ is enabled, all non-QinQ ports will be untagged and cannot be changed, and all QinQ ports will be tagged, and cannot be changed.*

3. Click **Apply**.

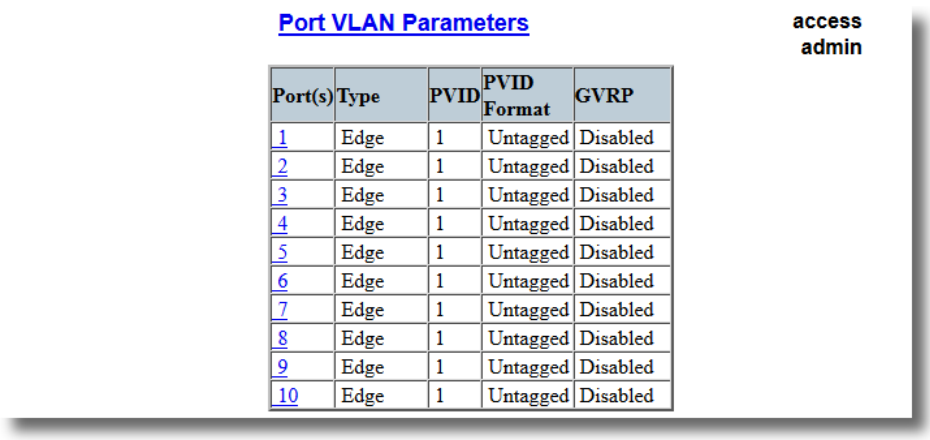
Section 5.1.4

Configuring VLANs for Specific Ethernet Ports

When a VLAN ID is assigned to an Ethernet port, the VLAN appears in the VLAN Summary table where it can be further configured.

To configure a VLAN for a specific Ethernet port, do the following:

1. Navigate to ***Virtual LANs » Configure Port VLAN Parameters*** . The **Port VLAN Parameters** table appears.



Port(s)	Type	PVID	PVID Format	GVRP
1	Edge	1	Untagged	Disabled
2	Edge	1	Untagged	Disabled
3	Edge	1	Untagged	Disabled
4	Edge	1	Untagged	Disabled
5	Edge	1	Untagged	Disabled
6	Edge	1	Untagged	Disabled
7	Edge	1	Untagged	Disabled
8	Edge	1	Untagged	Disabled
9	Edge	1	Untagged	Disabled
10	Edge	1	Untagged	Disabled

Figure 83: Port VLAN Parameters Table

2. Select a port. The **Port VLAN Parameters** form appears.

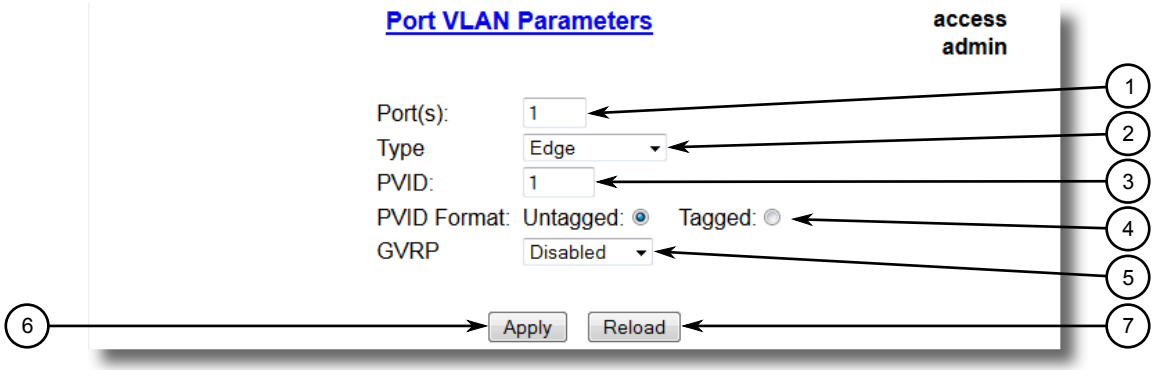


Figure 84: Port VLAN Parameters Form

1. Port(s) Box **2.** Type List **3.** PVID Box **4.** PVID Format Options **5.** GVRP List **6.** Apply Button **7.** Reload Button

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

Parameter	Description
Port(s)	**Synopsis:** Any combination of numbers valid for this parameter The port number as seen on the front plate silkscreen of the switch (or a list of ports, if aggregated in a port trunk).
Type	**Synopsis:** { Edge, Trunk, PVLANEdge, QinQ }

Parameter	Description
	Default: Edge This parameter specifies how the port determines its membership in VLANs. There are few types of ports: • Edge - the port is only a member of one VLAN (its native VLAN specified by the *PVID* parameter). • Trunk - the port is automatically a member of all configured VLANs. Frames transmitted out of the port on all VLANs except the port's native VLAN will be always tagged. It can also be configured to use GVRP for automatic VLAN configuration. • PVLANEdge - the port is only a member of one VLAN (its native VLAN specified by the *PVID* parameter), and does not forward traffic to other PVLANedge ports within the same VLAN. • QinQ - the port is a trunk port using double-VLAN tagging, or nested VLANs. An extra VLAN tag is always added to all frames egressing this port. VID in the added extra tag is the PVID of the frame's ingress port. VLAN tag is always stripped from frames ingressing this port. **NOTE** *Depending on the hardware installed, some switch models allow only one switch port be configured to QinQ mode at a time.*
PVID	**Synopsis:** 1 to 4094 **Default:** 1 The Port VLAN Identifier specifies the VLAN ID associated with untagged (and 802.1p priority tagged) frames received on this port. Frames tagged with a non-zero VLAN ID will always be associated with the VLAN ID retrieved from the frame tag. Modify this parameter with care! By default, the switch is programmed to use VLAN 1 for management and every port on the switch is programmed to use VLAN 1. If you modify a switch port to use a VLAN other than the management VLAN, devices on that port will not be able to manage the switch.
PVID Format	**Synopsis:** { Untagged, Tagged } **Default:** Untagged Specifies whether frames transmitted out of the port on its native VLAN (specified by the *PVID* parameter) will be tagged or untagged. **NOTE** *When QinQ is enabled, all non-QinQ ports will be untagged and cannot be changed, and all QinQ ports will be tagged, and cannot be changed.*
GVRP	**Synopsis:** { Adv&Learn, Adv Only, Disabled } **Default:** Disabled Configures GVRP (Generic VLAN Registration Protocol) operation on the port. There are several GVRP operation modes: • DISABLED - the port is not capable of any GVRP processing. • ADVERTISE ONLY - the port will declare all VLANs existing in the switch (configured or learned) but will not learn any VLANs. • ADVERTISE & LEARN - the port will declare all VLANs existing in the switch (configured or learned) and can dynamically learn VLANs. Only Trunk ports are GVRP-capable.

4. Click **Apply**.

Section 5.1.5

Managing Static VLANs

The following section describes how to configure and manage static VLANs.

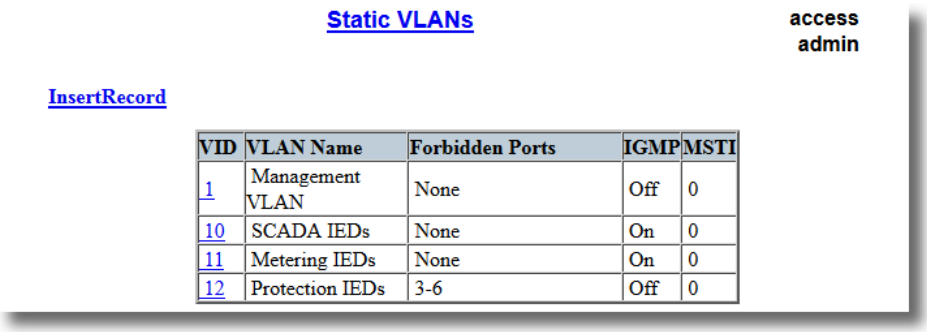
CONTENTS

- Section 5.1.5.1, "Viewing a List of Static VLANs"
- Section 5.1.5.2, "Adding a Static VLAN"
- Section 5.1.5.3, "Deleting a Static VLAN"

Section 5.1.5.1

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.



VID	VLAN Name	Forbidden Ports	IGMP	MSTI
1	Management VLAN	None	Off	0
10	SCADA IEDs	None	On	0
11	Metering IEDs	None	On	0
12	Protection IEDs	3-6	Off	0

Figure 85: Static VLANs Table

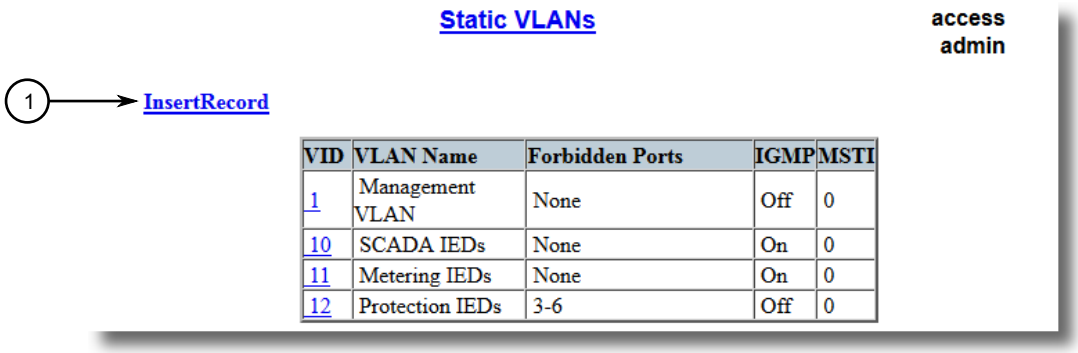
If a static VLAN is not listed, add the VLAN. For more information, refer to Section 5.1.5.2, "Adding a Static VLAN" .

Section 5.1.5.2

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.



VID	VLAN Name	Forbidden Ports	IGMP	MSTI
1	Management VLAN	None	Off	0
10	SCADA IEDs	None	On	0
11	Metering IEDs	None	On	0
12	Protection IEDs	3-6	Off	0

Figure 86: Static VLANs Table

1. InsertRecord

2. Click **InsertRecord**. The **Static VLANs** form appears.

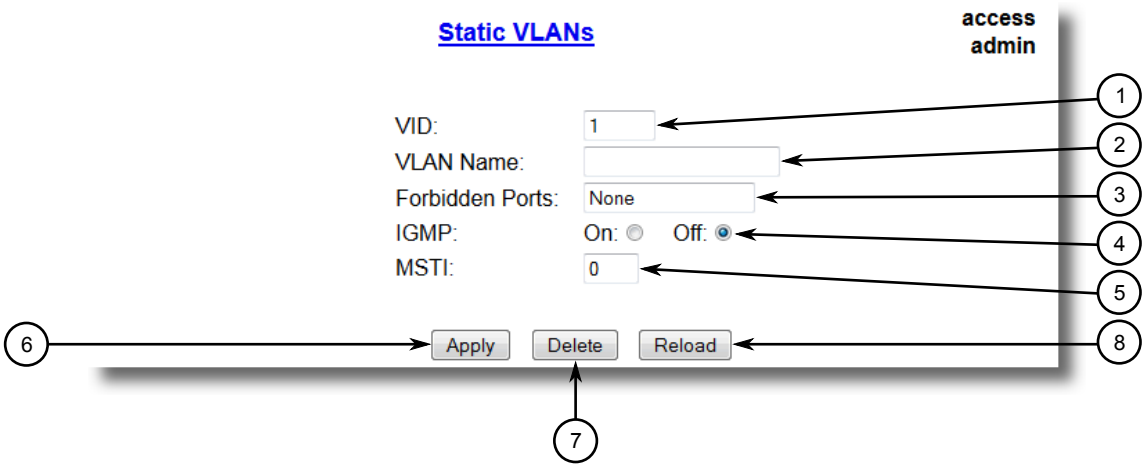


Figure 87: Static VLANs Form

1. VID Box **2.** VLAN Name Box **3.** Forbidden Ports Box **4.** IGMP Options **5.** MSTI Box **6.** Apply Button **7.** Delete Button **8.** Reload Button

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

> **NOTE**
> *If **IGMP Options** is not enabled for the VLAN, both IGMP messages and multicast streams will be forwarded directly to all members of the VLAN. If any one member of the VLAN joins a multicast group, then all members of the VLAN will receive the multicast traffic.*

Parameter	Description
VID	**Synopsis:** 1 to 4094 **Synopsis:** 1 to 4094 **Default:** 1

Parameter	Description
	The VLAN Identifier is used to identify the VLAN in tagged Ethernet frames according to IEEE 802.1Q.
VLAN Name	**Synopsis:** Any 19 characters The VLAN name provides a description of the VLAN purpose (for example, Engineering VLAN).
Forbidden Ports	**Synopsis:** Any combination of numbers valid for this parameter These are ports that are not allowed to be members of the VLAN. Examples: • None - all ports of the switch are allowed to be members of the VLAN • 2,4-6,8 - all ports except ports 2, 4, 6, 7 and 8 are allowed to be members of the VLAN
IGMP	**Synopsis:** { Off, On } **Default:** Off This parameter enables or disables IGMP Snooping on the VLAN.
MSTI	**Synopsis:** 0 to 16 **Default:** 0 This parameter is only valid for Multiple Spanning Tree Protocol (MSTP) and has no effect if MSTP is not used. The parameter specifies the Multiple Spanning Tree Instance (MSTI) to which the VLAN should be mapped.

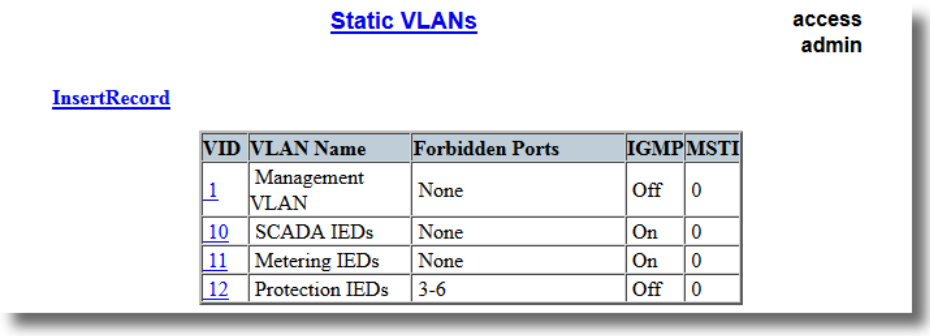
4. Click **Apply**.

Section 5.1.5.3

Deleting a Static VLAN

To delete a static VLAN, do the following:

1. Navigate to ***Virtual LANs » Configure Static VLANs*** . The **Static VLANs** table appears.



VID	VLAN Name	Forbidden Ports	IGMP	MSTI
1	Management VLAN	None	Off	0
10	SCADA IEDs	None	On	0
11	Metering IEDs	None	On	0
12	Protection IEDs	3-6	Off	0

Figure 88: Static VLANs Table

2. Select the static VLAN from the table. The **Static VLANs** form appears.

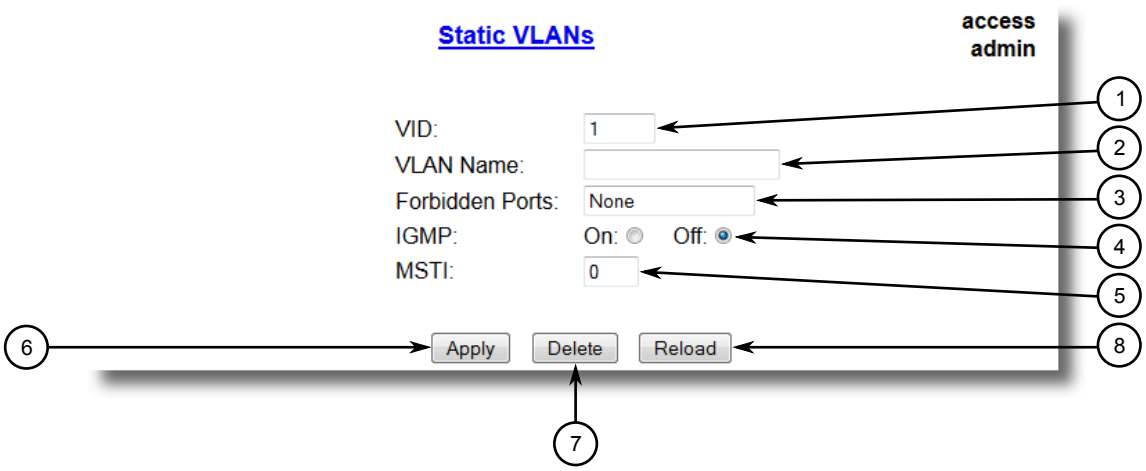


Figure 89: Static VLANs Form

1. VID Box **2.** VLAN Name Box **3.** Forbidden Ports Box **4.** IGMP Options **5.** MSTI Box **6.** Apply Button **7.** Delete Button **8.** Reload Button

3. Click **Delete**.

Section 5.2

Managing Spanning Tree Protocol

CONTENTS

- Section 5.2.1, “RSTP Operation”
- Section 5.2.2, “RSTP Applications”
- Section 5.2.3, “MSTP Operation”
- Section 5.2.4, “Configuring STP Globally”
- Section 5.2.5, “Configuring STP for Specific Ethernet Ports”
- Section 5.2.6, “Configuring eRSTP”
- Section 5.2.7, “Viewing Global Statistics for STP”
- Section 5.2.8, “Viewing STP Statistics for Ethernet Ports”
- Section 5.2.9, “Managing Multiple Spanning Tree Instances”
- Section 5.2.10, “Clearing Spanning Tree Protocol Statistics”

Section 5.2.1

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.

CONTENTS

- Section 5.2.1.1, “RSTP States and Roles”
- Section 5.2.1.2, “Edge Ports”
- Section 5.2.1.3, “Point-to-Point and Multipoint Links”
- Section 5.2.1.4, “Path and Port Costs”
- Section 5.2.1.5, “Bridge Diameter”
- Section 5.2.1.6, “eRSTP”
- Section 5.2.1.7, “Fast Root Failover”

Section 5.2.1.1

RSTP States and Roles

RSTP bridges have roles to play, either root or designated. One bridge - the Root Bridge - is the logical center of the network. All other bridges in the network are Designated bridges. RSTP also assigns each port of the bridge a state and a role. The RSTP state describes what is happening at the port in relation to address learning and frame forwarding. The RSTP role basically describes whether the port is facing the center or the edges of the network and whether it can currently be used.

State

There are three RSTP states: Discarding, Learning and Forwarding.

The discarding state is entered when the port is first put into service. The port does not learn addresses in this state and does not participate in frame transfer. The port looks for RSTP traffic in order to determine its role in the network. When it is determined that the port will play an active part in the network, the state will change to learning.

The learning state is entered when the port is preparing to play an active part in the network. The port learns addresses in this state but does not participate in frame transfer. In a network of RSTP bridges, the time spent in this state is usually quite short. RSTP bridges operating in STP compatibility mode will spend six to 40 seconds in this state.

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

IMPORTANT!
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.

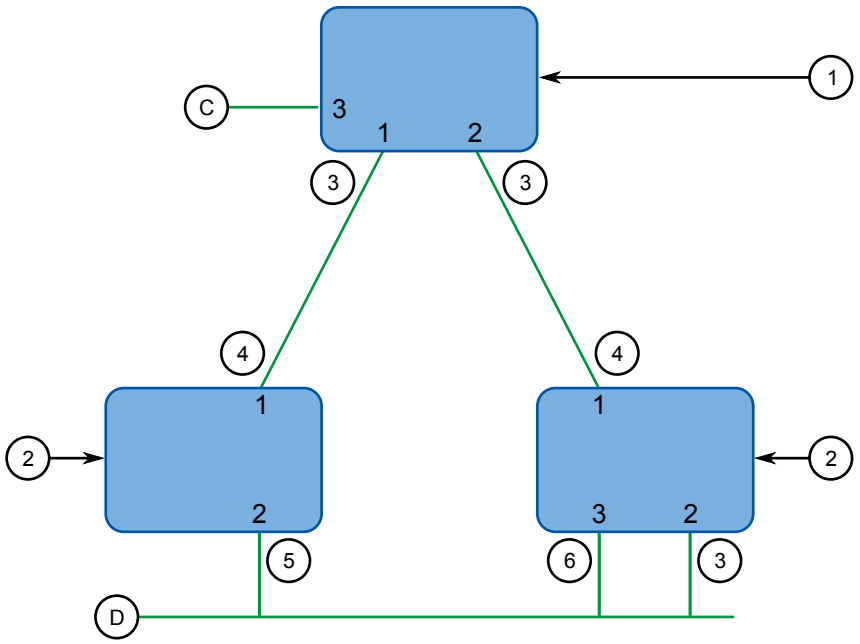


Figure 90: Bridge and Port Roles

1. Root Bridge **2.** Designated Bridge **3.** Designated Port **4.** Root Port **5.** Alternate Port **6.** Backup Port

A port is alternate when it receives a better message from another bridge on the LAN segment it is connected to. The message that an Alternate Port receives is better than the port itself would generate, but not good enough to convince it to become the Root Port. The port becomes the alternate to the current Root Port and will become the new Root Port should the current Root Port fail. The Alternate Port does not participate in the network.

A port is a Backup Port when it receives a better message from the LAN segment it is connected to, originating from another port on the same bridge. The port is a backup for another port on the bridge and will become active if that port fails. The Backup Port does not participate in the network.

Section 5.2.1.2

Edge Ports

A port may be designated as an Edge Port if it is directly connected to an end station. As such, it cannot create bridging loops in the network and can thus directly transition to forwarding, skipping the listening and learning stages.

Edge ports that receive configuration messages immediately lose their Edge Port status and become normal spanning tree ports. A loop created on an improperly connected edge port is thus quickly repaired.

Because an Edge Port services only end stations, topology change messages are not generated when its link toggles.

Section 5.2.1.3

Point-to-Point and Multipoint Links

RSTP uses a peer-peer protocol called Proposing-Agreeing to ensure transitioning in the event of a link failure. This protocol is point-to-point and breaks down in multipoint situations, i.e. when more than two bridges operate on a shared media link.

If RSTP detects this circumstance (based upon the port's half duplex state after link up) it will switch off Proposing-Agreeing. The port must transition through the learning and forwarding states, spending one forward delay in each state.

There are circumstances in which RSTP will make an incorrect decision about the point-to-point state of the link simply by examining the half-duplex status, namely:

- The port attaches only to a single partner, but through a half-duplex link.
- The port attaches to a shared media hub through a full-duplex link. The shared media link attaches to more than one RSTP enabled bridge.

In such cases, the user may configure the bridge to override the half-duplex determination mechanism and force the link to be treated in the proper fashion.

Section 5.2.1.4

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.

Section 5.2.1.5

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.*

IMPORTANT!
Raise the value of the maximum age parameter if implementing very large bridged networks or rings.

Section 5.2.1.6

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 80 switches)

eRSTP is also compatible with standard RSTP for interoperability with commercial switches.

For example, in a network comprised of 15 RUGGEDCOM hardened Ethernet switches in a ring topology, the expected fault recovery time would be less than 75 ms (i.e. 5 ms x 15). However, with eRSTP, the worst case fault recovery time is less than 26 ms.

Section 5.2.1.7

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.

IMPORTANT!
In networks mixing RUGGEDCOM and non-RUGGEDCOM switches, or in those mixing Fast Root Failover algorithms, RSTP Fast Root Failover will not function properly and root bridge failure will result in an unpredictable failover time. To avoid potential issues, note the following:

- *When using the Robust algorithm, all switches must be RUGGEDCOM switches*
- *When using the Relaxed algorithm, all switches must be RUGGEDCOM switches, with the exception of the root switch*
- *All RUGGEDCOM switches in the network must use the same Fast Root Failover algorithm*

Two Fast Root Failover algorithms are available:

- **Robust** – Guarantees a deterministic root failover time, but requires support from all switches in the network, including the root switch
- **Relaxed** – Ensures a deterministic root failover time in most network configurations, but allows the use of a standard bridge in the root role

NOTE
The minimum interval for root failures is one second. Multiple, near simultaneous root failures (within less than one second of each other) are not supported by Fast Root Failover.

Fast Root Failover and RSTP Performance

- Running RSTP with Fast Root Failover disabled has no impact on RSTP performance 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.

Section 5.2.2

RSTP Applications

The following section describes various applications of RSTP.

CONTENTS

- Section 5.2.2.1, "RSTP in Structured Wiring Configurations"

- Section 5.2.2.2, "RSTP in Ring Backbone Configurations"
- Section 5.2.2.3, "RSTP Port Redundancy"

Section 5.2.2.1

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 91 would leave all the ports of bridges 555 through 888 connected to the network.

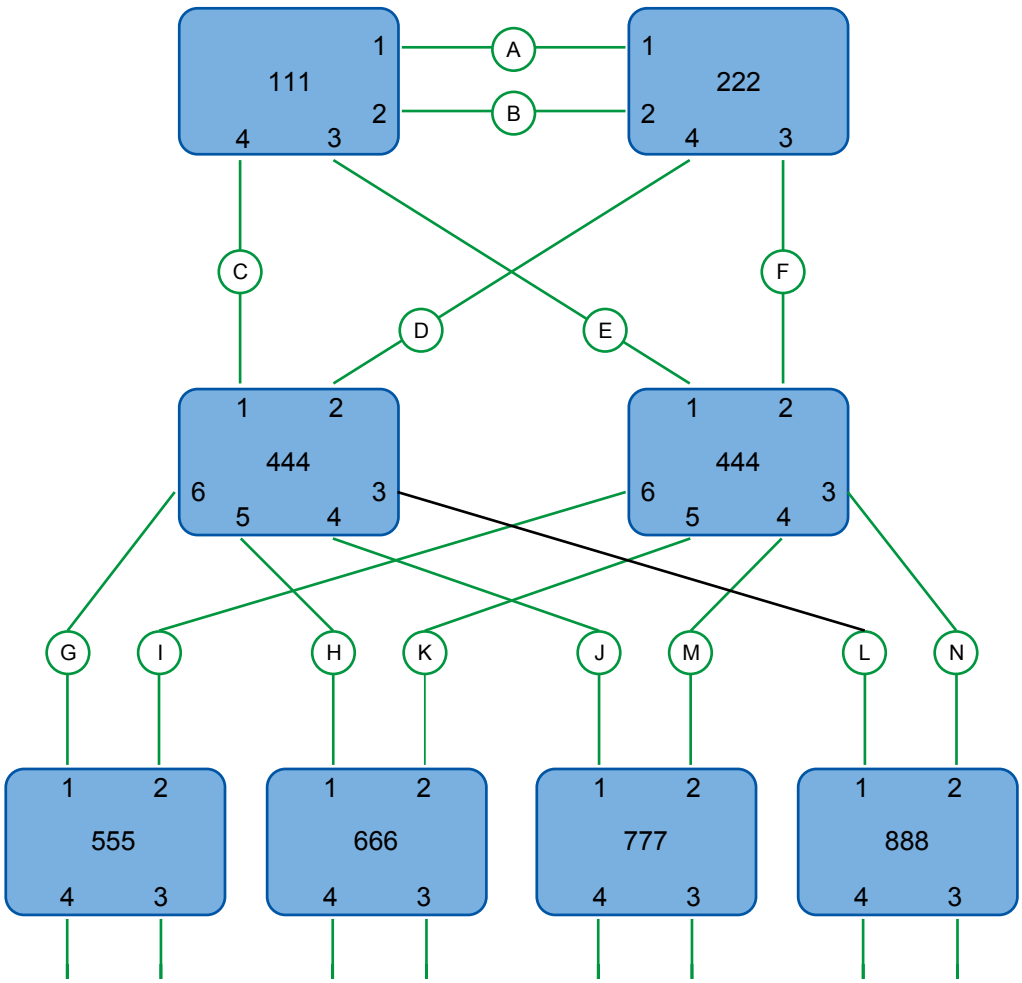


Figure 91: Example - Structured Wiring Configuration

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 in order to guarantee rapid transitioning to forwarding as well as to reduce the number of topology change notifications in the network. Ports with half-duplex/shared media restrictions require special attention in order to guarantee that they do not cause extended fail-over/recovery times.

4. **Choose the root bridge and backup root bridge carefully.**

   The root bridge should be selected to be at the concentration point of network traffic. Locate the backup root bridge adjacent to the root bridge. One strategy that may be used is to tune the bridge priority to establish the root bridge and then tune each bridge's priority to correspond to its distance from the root bridge.

5. **Identify desired steady state topology.**

   Identify the desired steady state topology taking into account link speeds, offered traffic and QOS. Examine of the effects of breaking selected links, taking into account network loading and the quality of alternate links.

6. **Decide upon a port cost calculation strategy.**

   Select whether fixed or auto-negotiated costs should be used? It is recommended to use the auto-negotiated cost style, unless it is necessary for the network design to change the auto-negotiated cost style. Select whether the STP or RSTP cost style should be used. Make sure to configure the same cost style on all devices on the network.

7. **Enable RSTP Fast Root Failover option.**

   This is a proprietary feature of Siemens. In a mesh network with only RUGGEDCOM devices in the core of the network, it is recommended to enable the RSTP Fast Root Failover option to minimize the network downtime in the event of a Root bridge failure.

8. Calculate and configure priorities and costs.
9. Implement the network and test under load.

Section 5.2.2.2

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 92 . 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.

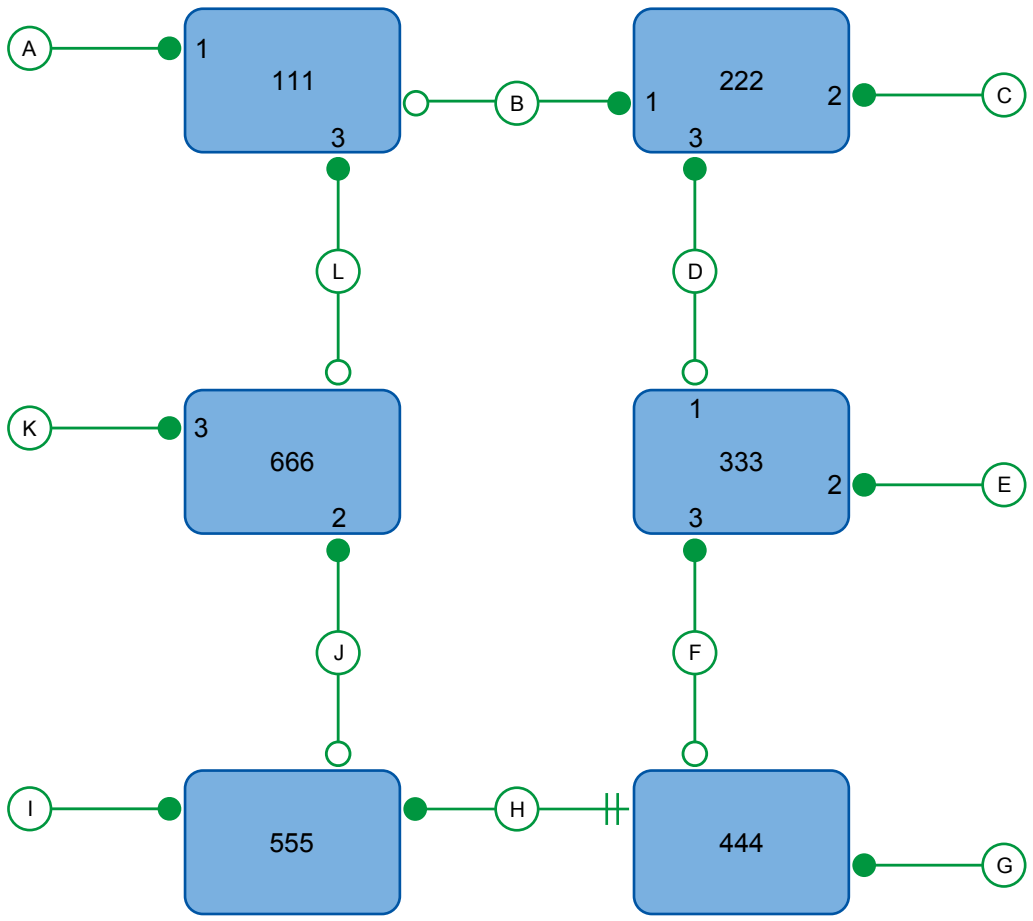


Figure 92: Example - Ring Backbone Configuration

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 in order to guarantee rapid transitioning to forwarding as well as to reduce the number of topology change notifications in the network.

4. **Choose the root bridge.**

   The root bridge can be selected to equalize either the number of bridges, number of stations or amount of traffic on either of its legs. It is important to realize that the ring will always be broken in one spot and that traffic always flows through the root.

5. **Assign bridge priorities to the ring.**

   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.

Section 5.2.2.3

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.

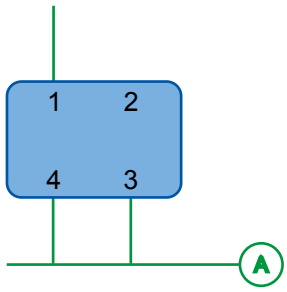


Figure 93: Example - Port Redundancy

Section 5.2.3

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.

CONTENTS

- Section 5.2.3.1, "MSTP Regions and Interoperability"
- Section 5.2.3.2, "MSTP Bridge and Port Roles"
- Section 5.2.3.3, "Benefits of MSTP"
- Section 5.2.3.4, "Implementing MSTP on a Bridged Network"

Section 5.2.3.1

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.

Section 5.2.3.2

MSTP Bridge and Port Roles

MSTP supports the following bridge and port roles:

Bridge Roles

Role	Description
CIST Root	The CIST Root is the elected root bridge of the CIST (Common and Internal Spanning Tree), which spans all connected STP and RSTP bridges and MSTP regions.
CIST Regional Root	The root bridge of the IST within an MSTP region. The CIST Regional Root is the bridge within an MSTP region with the lowest cost path to the CIST Root. Note that the CIST Regional Root will be at the boundary of an MSTP region. Note also that it is possible for the CIST Regional Root to be the CIST Root.
MSTI Regional Root	The root bridge for an MSTI within an MSTP region. A root bridge is independently elected for each MSTI in an MSTP region.

Port Roles

Each port on an MSTP bridge may have more than one CIST role depending on the number and topology of spanning tree instances defined on the port.

Role	Description
CIST Port Roles	• The Root Port provides the minimum cost path from the bridge to the CIST Root via the CIST Regional Root. If the bridge itself happens to be the CIST Regional Root, the Root Port is also the Master Port for all MSTIs, and provides the minimum cost path to a CIST Root located outside the region. • A Designated Port provides the minimum cost path from an attached LAN, via the bridge to the CIST Regional Root.

Role	Description
	• Alternate and Backup Ports function the same as they do in RSTP, but relative to the CIST Regional Root.
MSTI Port Roles	For each MSTI on a bridge: • The Root Port provides the minimum cost path from the bridge to the MSTI Regional Root, if the bridge itself is not the MSTI Regional Root. • A Designated Port provides the minimum cost path from an attached LAN, via the bridge to the MSTI Regional Root. • Alternate and Backup Ports function the same as they do in RSTP, but relative to the MSTI Regional Root. The Master Port, which is unique in an MSTP region, is the CIST Root Port of the CIST Regional Root, and provides the minimum cost path to the CIST Root for all MSTIs.
Boundary Ports	A Boundary Port is a port on a bridge in an MSTP region that connects to either: a bridge belonging to a different MSTP region, or a bridge supporting only RSTP or legacy STP. A Boundary Port blocks or forwards all VLANs from all MSTIs and the CIST alike. A Boundary Port may be: • The CIST Root Port of the CIST Regional Root (and therefore also the MSTI Master Port). • A CIST Designated Port, CIST Alternate/Backup Port, or Disabled. At the MSTP region boundary, the MSTI Port Role is the same as the CIST Port Role. A Boundary Port connected to an STP bridge will send only STP BPDUs. One connected to an RSTP bridge need not refrain from sending MSTP BPDUs. This is made possible by the fact that the MSTP carries the CIST Regional Root Identifier in the field that RSTP parses as the Designated Bridge Identifier.

Section 5.2.3.3

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, in order 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 versus PVST

An advantage of MSTP over the Cisco Systems Inc. proprietary 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 in order to arrive at an optimal network.

Section 5.2.3.4

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 Section 5.2.4, “Configuring STP Globally” or Section 5.2.5, “Configuring STP for Specific Ethernet Ports” .

   > **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 Section 5.1.5.2, “Adding a Static VLAN” .

   > **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 Section 5.2.9.3, “Configuring the MST Region Identifier” .
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 Section 5.2.9.4, “Configuring a Global MSTI” .

6. Configure the Port Cost and Priority per Port for each MSTI. For more information, refer to Section 5.2.9.5, "Configuring an MSTI for an Ethernet Port" .
7. Set the STP Protocol Version to MSTP and enable STP. For more information, refer to Section 5.2.4, "Configuring STP Globally"

Section 5.2.4

Configuring STP Globally

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

1. Navigate to ***Spanning Tree*** » ***Configure Bridge RSTP Parameters*** . The **Bridge RSTP Parameters** form appears.

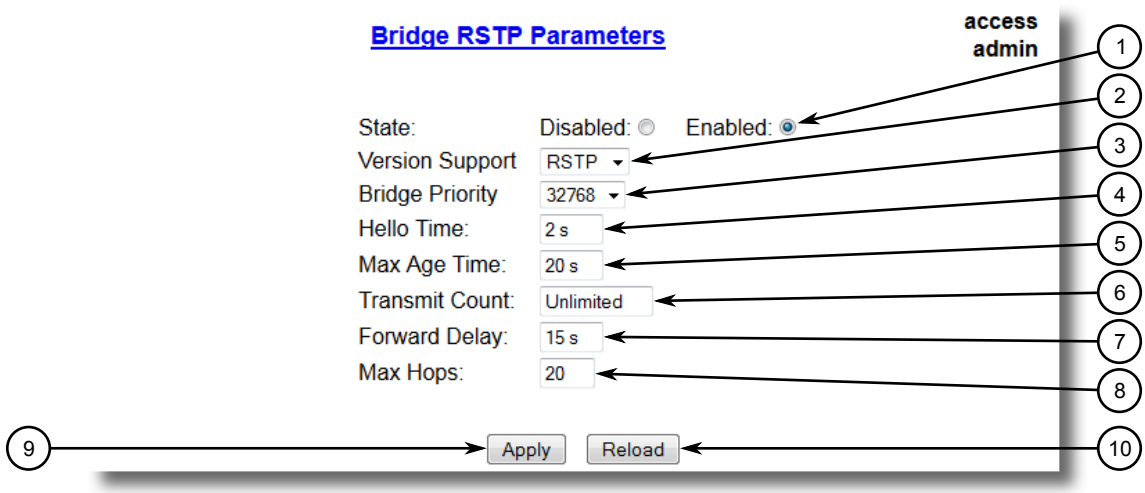


Figure 94: Bridge RSTP Parameters Form

1. State Options **2.** Version Support List **3.** Bridge Priority List **4.** Hello Time Box **5.** Max Age Time Box **6.** Transmit Count Box **7.** Forward Delay Box **8.** Max Hops Box **9.** Apply Button **10.** Reload Button

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

Parameter	Description
State	**Synopsis:** { Disabled, Enabled } **Default:** Enabled Enable STP/RSTP/MSTP for the bridge globally. Note that STP/RSTP/MSTP is enabled on a port when it is enabled globally and along with enabling per port setting.
Version Support	**Synopsis:** { STP, RSTP, MSTP } **Default:** RSTP Selects the version of Spanning Tree Protocol to support, either only STP or Rapid STP or Multiple STP.
Bridge Priority	**Synopsis:** { 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440 } **Default:** 32768

Parameter	Description
	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:** 1 to 10 s **Default:** 2 s 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:** 6 to 40 s **Default:** 20 s The time for which a configuration message remains valid after being issued by the root bridge. Configure this parameter with care when many tiers of bridges exist, or slow speed links (such as those used in WANs) are part of the network
Transmit Count	**Synopsis:** 3 to 100 or { Unlimited } **Default:** Unlimited Maximum number of BPDUs on each port that may be sent in one second. Larger values allow the network to recover from failed links/bridges more quickly.
Forward Delay	**Synopsis:** 4 to 30 s **Default:** 15 s 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:** 6 to 40 **Default:** 20 Only applicable to MSTP. The maximum possible bridge diameter inside an MST region. MSTP BPDUs propagating inside an MST region specify a time-to-live that is decremented by every switch that propagates the BPDU. If the maximum number of hops inside the region exceeds the configured maximum, BPDUs may be discarded due to their time-to-live setting.

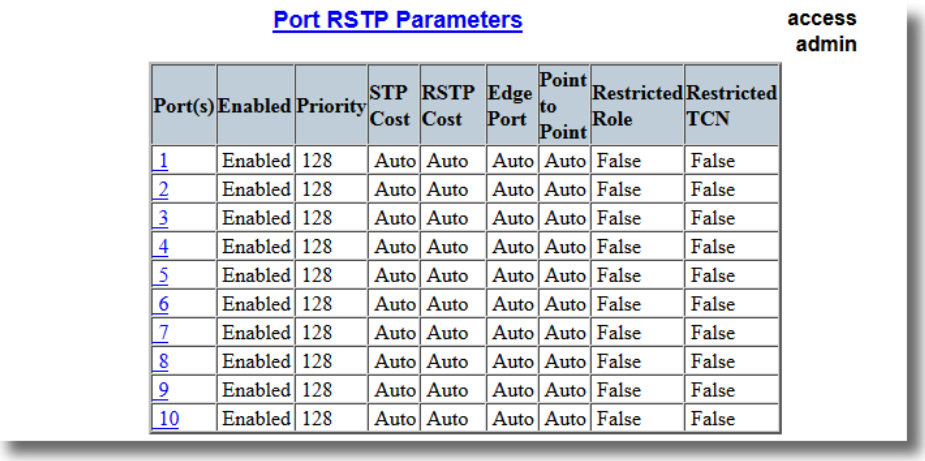
3. Click **Apply**.

Section 5.2.5

Configuring STP for Specific Ethernet Ports

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

1. Navigate to ***Spanning Tree*** » ***Configure Port RSTP Parameters*** . The **Port RSTP Parameters** table appears.



Port(s)	Enabled	Priority	STP Cost	RSTP Cost	Edge Port	Point to Point	Restricted Role	Restricted TCN
1	Enabled	128	Auto	Auto	Auto	Auto	False	False
2	Enabled	128	Auto	Auto	Auto	Auto	False	False
3	Enabled	128	Auto	Auto	Auto	Auto	False	False
4	Enabled	128	Auto	Auto	Auto	Auto	False	False
5	Enabled	128	Auto	Auto	Auto	Auto	False	False
6	Enabled	128	Auto	Auto	Auto	Auto	False	False
7	Enabled	128	Auto	Auto	Auto	Auto	False	False
8	Enabled	128	Auto	Auto	Auto	Auto	False	False
9	Enabled	128	Auto	Auto	Auto	Auto	False	False
10	Enabled	128	Auto	Auto	Auto	Auto	False	False

Figure 95: Port RSTP Parameters Table

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

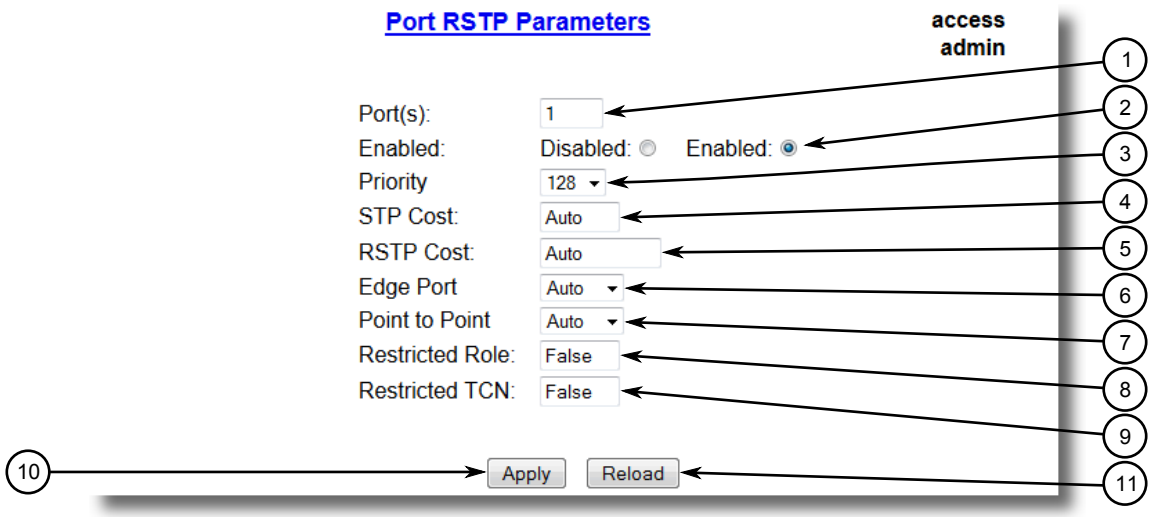


Figure 96: Port RSTP Parameters Form

1. Port(s) Box **2.** Enabled Options **3.** Priority List **4.** STP Cost Box **5.** RSTP Cost Box **6.** Edge Port List **7.** Point to Point List **8.** Restricted Role Box **9.** Restricted TCN Box **10.** Apply Button **11.** Reload Button

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

Parameter	Description
Port(s)	**Synopsis:** Any combination of numbers valid for this parameter The port number as seen on the front plate silkscreen of the switch (or a list of ports, if aggregated in a port trunk).
Enabled	**Synopsis:** { Disabled, Enabled } **Default:** Enabled

Parameter	Description
	Enabling STP activates the STP or RSTP protocol for this port per the configuration in the STP Configuration menu. STP may be disabled for the port ONLY if the port does not attach to an STP enabled bridge in any way. Failure to meet this requirement WILL result in an undetectable traffic loop in the network. A better alternative to disabling the port is to leave STP enabled but to configure the port as an edge port. A good candidate for disabling STP would be a port that services only a single host computer.
Priority	**Synopsis:** { 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 194, 208, 224, 240 } **Default:** 128 Selects the STP port priority. Ports of the same cost that attach to a common LAN will select the port to be used based upon the port priority.
STP Cost	**Synopsis:** 0 to 65535 or { Auto } **Default:** Auto Selects the cost to use in cost calculations, when the Cost Style parameter is set to STP in the Bridge RSTP Parameters configuration. Setting the cost manually provides the ability to preferentially select specific ports to carry traffic over others. Leave this field set to "auto" to use the standard STP port costs as negotiated (4 for 1Gbps, 19 for 100 Mbps links and 100 for 10 Mbps links). For MSTP, this parameter applies to both external and internal path cost.
RSTP Cost	**Synopsis:** 0 to 2147483647 or { Auto } **Default:** Auto Selects the cost to use in cost calculations, when the Cost Style parameter is set to RSTP in the Bridge RSTP Parameters configuration. Setting the cost manually provides the ability to preferentially select specific ports to carry traffic over others. Leave this field set to "auto" to use the standard RSTP port costs as negotiated (20,000 for 1Gbps, 200,000 for 100 Mbps links and 2,000,000 for 10 Mbps links). For MSTP, this parameter applies to both external and internal path cost.
Edge Port	**Synopsis:** { False, True, Auto } **Default:** Auto Edge ports are ports that do not participate in the Spanning Tree, but still send configuration messages. Edge ports transition directly to frame forwarding without any listening and learning delays. The MAC tables of Edge ports do not need to be flushed when topology changes occur in the STP network. Unlike an STP disabled port, accidentally connecting an edge port to another port in the spanning tree will result in a detectable loop. The "Edgeness" of the port will be switched off and the standard RSTP rules will apply (until the next link outage).
Point to Point	**Synopsis:** { False, True, Auto } **Default:** Auto RSTP uses a peer-to-peer protocol that provides rapid transitioning on point-to-point links. This protocol is automatically turned off in situations where multiple STP bridges communicate over a shared (non point-to-point) LAN. The bridge will automatically take point-to-point to be true when the link is found to be operating in full-duplex mode. The point-to-point parameter allows this behavior or overrides it, forcing point-to-point to be true or false. Force the parameter true when the port operates a point-to-point link but

Parameter	Description
	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 or False } **Default:** False A boolean value set by management. If TRUE, causes the Port not to be selected as the Root Port for the CIST or any MSTI, even if it has the best spanning tree priority vector. Such a Port will be selected as an Alternate Port after the Root Port has been selected. This parameter should be FALSE by default. If set, it can cause a lack of spanning tree connectivity. It is set by a network administrator to prevent bridges that are external to a core region of the network from influencing the spanning tree active topology. This may be necessary, for example, if those bridges are not under the full control of the administrator.
Restricted TCN	**Synopsis:** { True or False } **Default:** False A boolean value set by management. If TRUE, it causes the Port not to propagate received topology change notifications and topology changes to other Ports. If set, it can cause temporary loss of connectivity after changes in a spanning tree's active topology as a result of persistent, incorrectly learned, station location information. It is set by a network administrator to prevent bridges that are external to a core region of the network from causing address flushing in that region. This may be necessary, for example, if those bridges are not under the full control of the administrator or if the MAC_Operational status parameter for the attached LANs transitions frequently.

4. Click **Apply**.

Section 5.2.6

Configuring eRSTP

To configure eRSTP, do the following:

1. Navigate to ***Spanning Tree » Configure eRSTP Parameters*** . The **eRSTP Parameters** form appears.

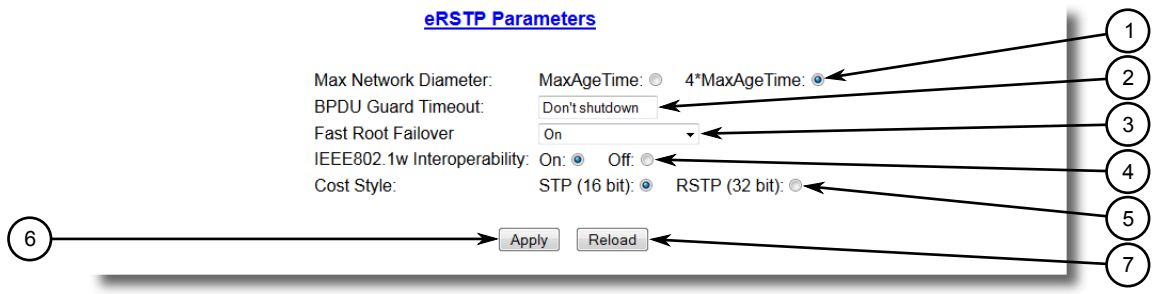


Figure 97: eRSTP Parameters Form

1. Max Network Diameter Options **2.** BPDU Guart Timeout Box **3.** Fast Root Failover List **4.** IEEE802.1w Interoperability Options **5.** Cost Style Options **6.** Apply Button **7.** Reload Button

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

Parameter	Description
Max Network Diameter	**Synopsis:** { MaxAgeTime, 4*MaxAgeTime } **Default:** 4*MaxAgeTime The RSTP standard puts a limit on the maximum network size that can be controlled by the RSTP protocol. The network size is described by the term 'maximum network diameter', which is the number of switches that comprise the longest path that RSTP BPDUs have to traverse. The standard supported maximum network diameter is equal to the value of the 'MaxAgeTime' RSTP configuration parameter. eRSTP offers an enhancement to RSTP which allows it to cover networks larger than ones defined by the standard. This configuration parameter selects the maximum supported network size.
BPDU Guard Timeout	**Synopsis:** 1 to 86400 s or { Until reset, Don't shutdown } **Default:** Don't shutdown The RSTP standard does not address network security. RSTP must process every received BPDU and take an appropriate action. This opens a way for an attacker to influence RSTP topology by injecting RSTP BPDUs into the network. BPDU Guard is a feature that protects the network from BPDUs received by a port where RSTP capable devices are not expected to be attached. If a BPDU is received by a port for which 'Edge' parameter is set to 'TRUE' or RSTP is disabled, the port will be shutdown for the time period specified by this parameter. • DON'T SHUTDOWN - BPDU Guard is disabled • UNTIL RESET - port will remain shutdown until the port reset command is issued by the user
Fast Root Failover	**Synopsis:** { On, On with standard root, Off } **Default:** On In mesh network topologies, the standard RSTP algorithm does not guarantee deterministic network recovery time in the case of a root switch failure. Such a recovery time is hard to calculate and it can be different (and may be relatively long) for any given mesh topology. This configuration parameter enables Siemens's enhancement to RSTP which detects a failure of the root switch and performs some extra RSTP processing steps, significantly reducing the network recovery time and making it deterministic. **NOTE** • *This feature is only available in RSTP mode. In MSTP mode, the configuration parameter is ignored.* • *In a single ring topology, this feature is not needed and should be disabled to avoid longer network recovery times due to extra RSTP processing.* The Fast Root Failover algorithm must be supported by all switches in the network, including the root, to guarantee optimal performance. However, it is not uncommon to assign the root role to a switch from a vendor different from the rest of the switches in the network. In other words, it is possible that the root might not suport the Fast Root Failover algorithm. In such a scenario, a "relaxed" algorithm should be used, which tolerates the lack of support in the root switch.

Parameter	Description
	These are the supported configuration options: • Off - Fast Root Failover algorithm is disabled and hence a root switch failure may result in excessive connectivity recovery time. • On - Fast Root Failover is enabled and the most robust algorithm is used, which requires the appropriate support in the root switch. • On with standard root - Fast Root Failover is enabled but a "relaxed" algorithm is used, allowing the use of a standard switch in the root role.
IEEE802.1w Interoperability	**Synopsis:** { On, Off } **Default:** On The original RSTP protocol defined in the IEEE 802.1w standard has minor differences from more recent, enhanced, standard(s). Those differences cause interoperability issues which, although they do not completely break RSTP operation, can lead to a longer recovery time from failures in the network. eRSTP offers some enhancements to the protocol which make the switch fully interoperable with other vendors' switches, which may be running IEEE 802.2w RSTP. The enhancements do not affect interoperability with more recent RSTP editions. This configuration parameter enables the aforementioned interoperability mode.
Cost Style	**Synopsis:** { STP (16 bit), RSTP (32 bit) } **Default:** STP (16 bit) The RSTP standard defines two styles of a path cost value. STP uses 16-bit path costs based upon 1x10E9/link speed (4 for 1Gbps, 19 for 100 Mbps and 100 for 10 Mbps) whereas RSTP uses 32-bit costs based upon 2x10E13/link speed (20,000 for 1Gbps, 200,000 for 100 Mbps and 2,000,000 for 10 Mbps). However, switches from some vendors keep using the STP path cost style even in RSTP mode, which can cause confusion and interoperability problems. This configuration parameter selects the style of link costs to employ. Note that RSTP link costs are used only when the bridge version support is set to allow RSTP and the port does not migrate to STP.

3. Click **Apply**.

Section 5.2.7

Viewing Global Statistics for STP

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

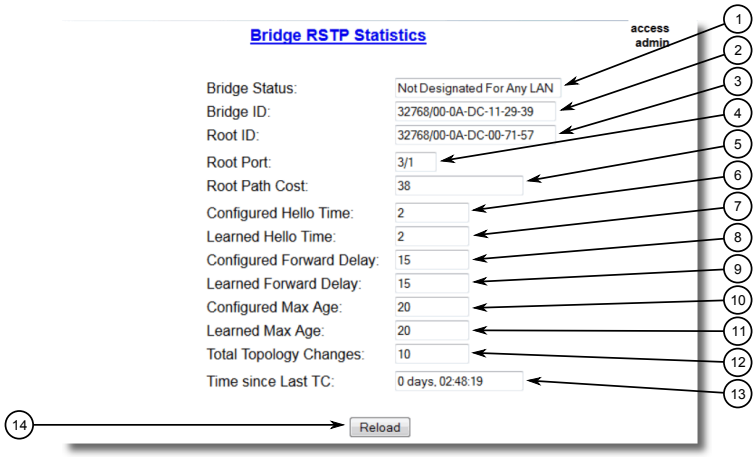


Figure 98: Bridge RSTP Statistics Form

1. Bridge Status Box **2.** Bridge ID Box **3.** Root ID Box **4.** Root Port Box **5.** Root Path Cost Box **6.** Configure Hello Time Box **7.** Learned Hello Time Box **8.** Configured Forward Delay Box **9.** Learned Forward Delay Box **10.** Configured Max Age Box **11.** Learned Max Age Box **12.** Total Topology Changes Box **13.** Time Since Last TC Box **14.** Reload Button

This table displays the following information:

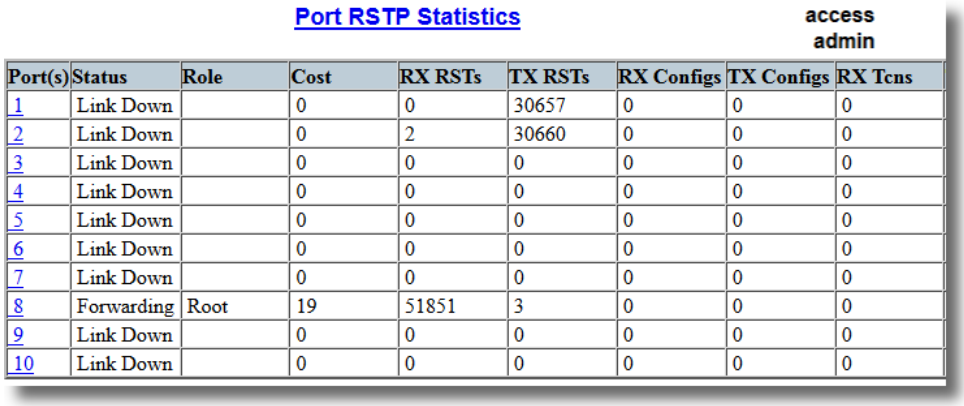
Parameter	Description
Bridge Status	**Synopsis:** { , Designated Bridge, Not Designated For Any LAN, Root Bridge } Spanning Tree status of the bridge. The status may be root or designated. This field may show text saying not designated for any LAN if the bridge is not designated for any of its ports.
Bridge ID	**Synopsis:** $$ / ##-##-##-##-##-## where $$ is 0 to 65535, ## is 0 to FF Bridge Identifier of this bridge.
Root ID	**Synopsis:** $$ / ##-##-##-##-##-## where $$ is 0 to 65535, ## is 0 to FF Bridge Identifier of the root bridge.
Root Port	**Synopsis:** 1 to maximum port number or { <empty string> } If the bridge is designated, this is the port that provides connectivity towards the root bridge of the network.
Root Path Cost	**Synopsis:** 0 to 4294967295 Total cost of the path to the root bridge composed of the sum of the costs of each link in the path. If custom costs have not been configured. 1Gbps ports will contribute 4, 100 Mbps ports will contribute 19 and 10 Mbps ports will contribute a cost of 100 to this figure. For the CIST instance of MSTP, this is an external root path cost, which is the cost of the path from the IST root (i.e. regional root) bridge to the CST root (i.e. network "global" root) bridge.
Configured Hello Time	**Synopsis:** 0 to 65535 The configured Hello time from the Bridge RSTP Parameters menu.
Learned Hello Time	**Synopsis:** 0 to 65535

Parameter	Description
	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:** 0 to 65535 The configured Forward Delay time from the Bridge RSTP Parameters menu.
Learned Forward Delay	**Synopsis:** 0 to 65535 The actual Forward Delay time provided by the root bridge as learned in configuration messages. This time is used in designated bridges.
Configured Max Age	**Synopsis:** 0 to 65535 The configured Maximum Age time from the Bridge RSTP Parameters menu.
Learned Max Age	**Synopsis:** 0 to 65535 The actual Maximum Age time provided by the root bridge as learned in configuration messages. This time is used in designated bridges.
Total Topology Changes	**Synopsis:** 0 to 65535 A count of topology changes in the network, as detected on this bridge through link failures or as signaled from other bridges. Excessively high or rapidly increasing counts signal network problems.
Time since Last TC	**Synopsis:** DDDD days, HH:MM:SS The time since the last time a topology change was detected by the bridge.

Section 5.2.8

Viewing STP Statistics for Ethernet Ports

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



Port RSTP Statistics

access admin

Port(s)	Status	Role	Cost	RX RSTs	TX RSTs	RX Configs	TX Configs	RX Tcns
1	Link Down		0	0	30657	0	0	0
2	Link Down		0	2	30660	0	0	0
3	Link Down		0	0	0	0	0	0
4	Link Down		0	0	0	0	0	0
5	Link Down		0	0	0	0	0	0
6	Link Down		0	0	0	0	0	0
7	Link Down		0	0	0	0	0	0
8	Forwarding	Root	19	51851	3	0	0	0
9	Link Down		0	0	0	0	0	0
10	Link Down		0	0	0	0	0	0

Figure 99: Port RSTP Statistics Table

This table displays the following information:

Parameter	Description
Port(s)	**Synopsis:** Any combination of numbers valid for this parameter The port number as seen on the front plate silkscreen of the switch (or a list of ports, if aggregated in a port trunk).
Status	**Synopsis:** { Disabled, Listening, Learning, Forwarding, Blocking, Link Down, Discarding } Status of this port in Spanning Tree. This may be one of the following: • **Disabled** - STP is disabled on this port. • **Link Down** - STP is enabled on this port but the link is down. • **Discarding** - The link is not used in the STP topology but is standing by. • **Learning** - The port is learning MAC addresses in order to prevent flooding when it begins forwarding traffic. • **Forwarding** - The port is forwarding traffic.
Role	**Synopsis:** { , Root, Designated, Alternate, Backup, Master } Role of this port in Spanning Tree. This may be one of the following: • **Designated** - The port is designated for (i.e. carries traffic towards the root for) the LAN it is connected to. • **Root** - The single port on the bridge, which provides connectivity towards the root bridge. • **Backup** - The port is attached to a LAN that is serviced by another port on the bridge. It is not used but is standing by. • **Alternate** - The port is attached to a bridge that provides connectivity to the root bridge. It is not used but is standing by. • **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:** 0 to 4294967295 Cost offered by this port. If the Bridge RSTP Parameters Cost Style is set to STP, 1Gbps ports will contribute 4, 100 Mbps ports will contribute 19 and 10 Mbps ports contribute a cost of 100. If the Cost Style is set to RSTP, 1Gbps will contribute 20,000, 100 Mbps ports will contribute a cost of 200,000 and 10 Mbps ports contribute a cost of 2,000,000. Note that even if the Cost style is set to RSTP, a port that migrates to STP will have its cost limited to a maximum of 65535.
RX RSTs	**Synopsis:** 0 to 4294967295 The count of RSTP configuration messages received on this port.
TX RSTs	**Synopsis:** 0 to 4294967295 The count of RSTP configuration messages transmitted on this port.
RX Configs	**Synopsis:** 0 to 4294967295 The count of STP configuration messages received on this port.
TX Configs	**Synopsis:** 0 to 4294967295 The count of STP configuration messages transmitted on this port.
RX Tcns	**Synopsis:** 0 to 4294967295

Parameter	Description
	The count of STP topology change notification messages received on this port. Excessively high or rapidly increasing counts signal network problems.
TX Tcns	**Synopsis:** 0 to 4294967295 The count of STP topology change notification messages transmitted on this port.
Desig Bridge ID	**Synopsis:** $$ / ##-##-##-##-##-## where $$ is 0 to 65535, ## is 0 to FF Provided on the root ports of designated bridges, the Bridge Identifier of the bridge this port is connected to.
operEdge	**Synopsis:** True or False The port is operating as an edge port or not.

Section 5.2.9

Managing Multiple Spanning Tree Instances

The following section describes how to configure and manage Multiple Spanning Tree Instances.

CONTENTS

- Section 5.2.9.1, “Viewing Statistics for Global MSTIs”
- Section 5.2.9.2, “Viewing Statistics for Port MSTIs”
- Section 5.2.9.3, “Configuring the MST Region Identifier”
- Section 5.2.9.4, “Configuring a Global MSTI”
- Section 5.2.9.5, “Configuring an MSTI for an Ethernet Port”

Section 5.2.9.1

Viewing Statistics for Global MSTIs

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

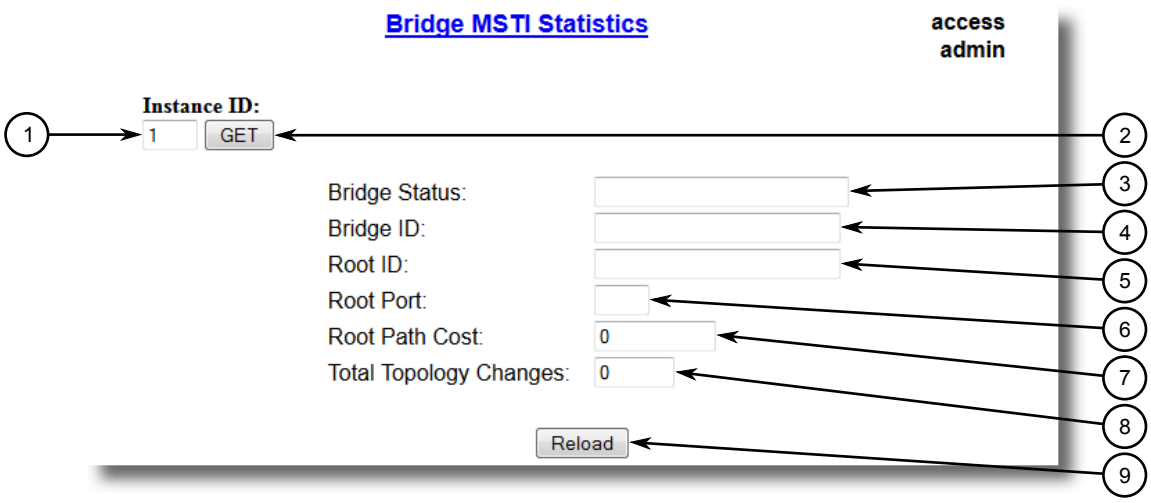


Figure 100: Bridge MSTI Statistics Form

1. Instance Box **2.** Get Button **3.** Bridge Status Box **4.** Bridge ID Box **5.** Root ID Box **6.** Root Port Box **7.** Root Path Cost Box **8.** Total Topology Changes Box **9.** Reload Button

This table displays the following information:

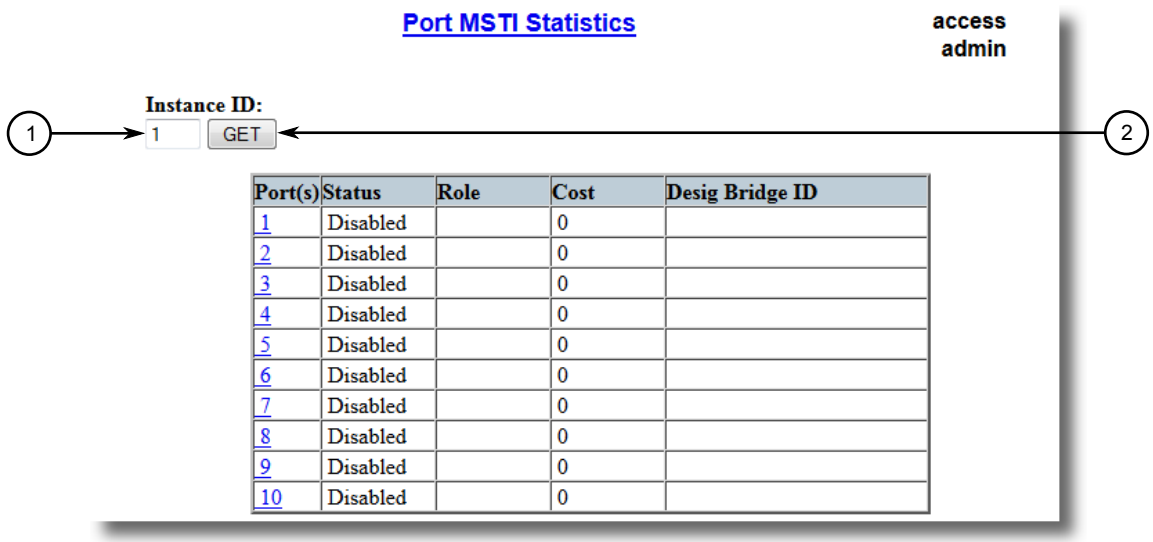
Parameter	Description
Bridge Status	**Synopsis:** { , Designated Bridge, Not Designated For Any LAN, Root Bridge } Spanning Tree status of the bridge. The status may be root or designated. This field may show text saying not designated for any LAN if the bridge is not designated for any of its ports.
Bridge ID	**Synopsis:** $$ / ##-##-##-##-##-## where $$ is 0 to 65535, ## is 0 to FF Bridge Identifier of this bridge.
Root ID	**Synopsis:** $$ / ##-##-##-##-##-## where $$ is 0 to 65535, ## is 0 to FF Bridge Identifier of the root bridge.
Root Port	**Synopsis:** 1 to maximum port number or { <empty string> } If the bridge is designated, this is the port that provides connectivity towards the root bridge of the network.
Root Path Cost	**Synopsis:** 0 to 4294967295 Total cost of the path to the root bridge composed of the sum of the costs of each link in the path. If custom costs have not been configured. 1Gbps ports will contribute 4, 100 Mbps ports will contribute 19 and 10 Mbps ports will contribute a cost of 100 to this figure. For the CIST instance of MSTP, this is an external root path cost, which is the cost of the path from the IST root (i.e. regional root) bridge to the CST root (i.e. network "global" root) bridge.
Total Topology Changes	**Synopsis:** 0 to 65535 A count of topology changes in the network, as detected on this bridge through link failures or as signaled from other bridges.

Parameter	Description
	Excessively high or rapidly increasing counts signal network problems.

Section 5.2.9.2

Viewing Statistics for Port MSTIs

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



Port(s)	Status	Role	Cost	Desig Bridge ID
1	Disabled		0	
2	Disabled		0	
3	Disabled		0	
4	Disabled		0	
5	Disabled		0	
6	Disabled		0	
7	Disabled		0	
8	Disabled		0	
9	Disabled		0	
10	Disabled		0	

Figure 101: Port MSTI Statistics Form

1. Instance ID Box **2.** Get Button

This table displays the following information:

Parameter	Description
Port(s)	**Synopsis:** Any combination of numbers valid for this parameter The port number as seen on the front plate silkscreen of the switch (or a list of ports, if aggregated in a port trunk).
Status	**Synopsis:** { Disabled, Listening, Learning, Forwarding, Blocking, Link Down, Discarding } tatus of this port in Spanning Tree. This may be one of the following: • **Disabled** - STP is disabled on this port. • **Link Down** - STP is enabled on this port but the link is down. • **Discarding** - The link is not used in the STP topology but is standing by. • **Learning** - The port is learning MAC addresses in order to prevent flooding when it begins forwarding traffic. • **Forwarding** - The port is forwarding traffic.
Role	**Synopsis:** { , Root, Designated, Alternate, Backup, Master }

Parameter	Description
	Role of this port in Spanning Tree. This may be one of the following: • **Designated** - The port is designated for (i.e. carries traffic towards the root for) the LAN it is connected to. • **Root** - The single port on the bridge, which provides connectivity towards the root bridge. • **Backup** - The port is attached to a LAN that is serviced by another port on the bridge. It is not used but is standing by. • **Alternate** - The port is attached to a bridge that provides connectivity to the root bridge. It is not used but is standing by. • **Master** - Only exists in MSTP. The port is an MST region boundary port and the single port on the bridge, which provides connectivity for the Multiple Spanning Tree Instance towards the Common Spanning Tree root bridge (i.e. this port is the root port for the Common Spanning Tree Instance).
Cost	**Synopsis:** 0 to 4294967295 Cost offered by this port. If the Bridge RSTP Parameters Cost Style is set to STP, 1Gbps ports will contribute 4, 100 Mbps ports will contribute 19 and 10 Mbps ports contribute a cost of 100. If the Cost Style is set to RSTP, 1Gbps will contribute 20,000, 100 Mbps ports will contribute a cost of 200,000 and 10 Mbps ports contribute a cost of 2,000,000. Note that even if the Cost style is set to RSTP, a port that migrates to STP will have its cost limited to a maximum of 65535.
Desig Bridge ID	**Synopsis:** $$ / ##-##-##-##-##-## where $$ is 0 to 65535, ## is 0 to FF Provided on the root ports of designated bridges, the Bridge Identifier of the bridge this port is connected to.

Section 5.2.9.3

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 Section 5.2.3.1, "MSTP Regions and Interoperability" .

To configure the Multiple Spanning Tree (MST) region identifier, do the following:

1. Navigate to ***Spanning Tree*** » ***Configure MST Region Identifier*** . The **MST Region Identifier** form appears.

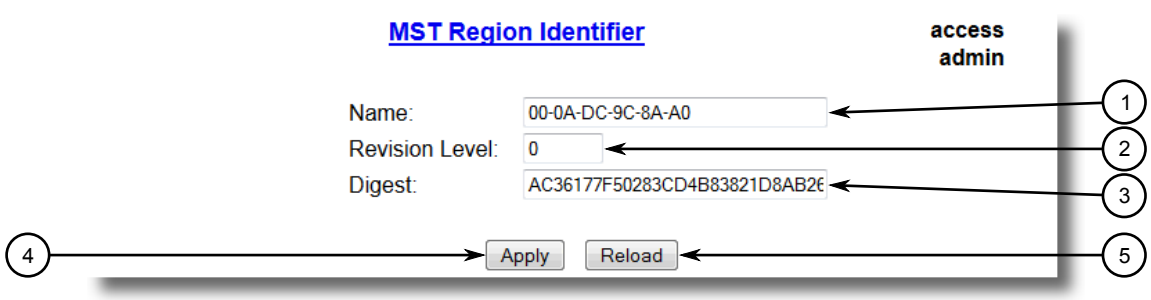


Figure 102: MST Region Identifier Form

1. Name Box **2.** Revision Level Box **3.** Digest Box **4.** Apply Button **5.** Reload Button

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

Parameter	Description
Name	**Synopsis:** Any 32 characters **Default:** 00-0A-DC-92-00-00 The name of the MST region. All devices in the same MST region must have the same region name configured.
Revision Level	**Synopsis:** 0 to 65535 **Default:** 0 The revision level for MST configuration. Typically, all devices in the same MST region are configured with the same revision level. However, different revision levels can be used to create sub-regions under the same region name.
Digest	**Synopsis:** Any 32 characters **Default:** 0 This is a read-only parameter and should be only used for network troubleshooting. In order to ensure consistent VLAN-to-instance mapping, it is necessary for the protocol to be able to exactly identify the boundaries of the MST regions. For that pupose, the characteristics of the region are included in BPDUs. There is no need to propagate the exact VLAN-to-instance mapping in the BPDUs because switches only need to know whether they are in the same region as a neighbor. Therefore, only this 16-octet digest created from the VLAN-to-instance mapping is sent in BPDUs.

3. Click **Apply**.

Section 5.2.9.4

Configuring a Global MSTI

To configure a global Multiple Spanning Tree Instance (MSTI) for the Spanning Tree Protocol (STP), do the following:

1. Navigate to ***Spanning Tree » Configure Bridge MSTI Parameters*** . The **Bridge MSTI Parameters** form appears.

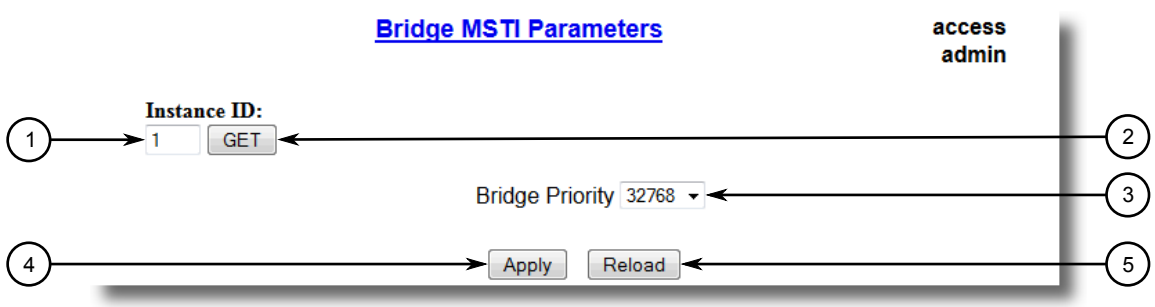


Figure 103: Bridge MSTI Parameters Form

1. Instance ID Box **2.** Get Button **3.** Bridge Priority List **4.** Apply Button **5.** Reload Button

2. Under **Instance ID**, type an ID number for a Multiple Spanning Tree Instance (MSTI) and click **GET**. The settings for the MSTI are displayed. Any changes made to the configuration will be applied specifically to this instance ID.
3. Configure the following parameter(s) as required:

Parameter	Description
Bridge Priority	**Synopsis:** { 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440 } **Default:** 32768 Bridge Priority provides a way to control the topology of the STP connected network. The desired Root and Designated bridges can be configured for a particular topology. The bridge with the lowest priority will become root. In the event of a failure of the root bridge, the bridge with the next lowest priority will then become root. Designated bridges that (for redundancy purposes) service a common LAN also use priority to determine which bridge is active. In this way careful selection of Bridge Priorities can establish the path of traffic flows in normal and abnormal conditions.

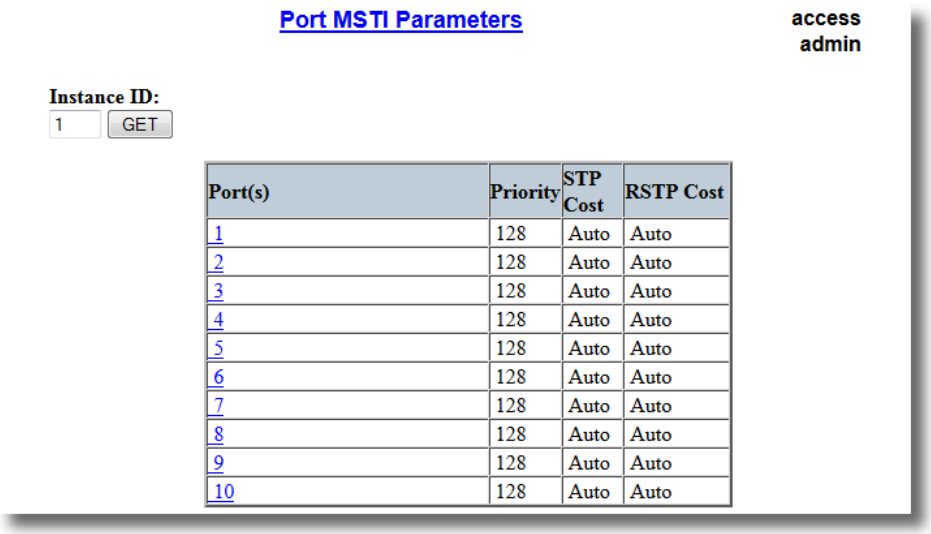
4. Click **Apply**.

Section 5.2.9.5

Configuring an MSTI for an Ethernet Port

To configure a Multiple Spanning Tree Instance (MSTI) for an Ethernet port, do the following

1. Navigate to ***Spanning Tree*** » ***Configure Port MSTI Parameters*** . The **Port MSTI Parameters** table appears.



Port(s)	Priority	STP Cost	RSTP Cost
1	128	Auto	Auto
2	128	Auto	Auto
3	128	Auto	Auto
4	128	Auto	Auto
5	128	Auto	Auto
6	128	Auto	Auto
7	128	Auto	Auto
8	128	Auto	Auto
9	128	Auto	Auto
10	128	Auto	Auto

Figure 104: Port MSTI Parameters Table

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

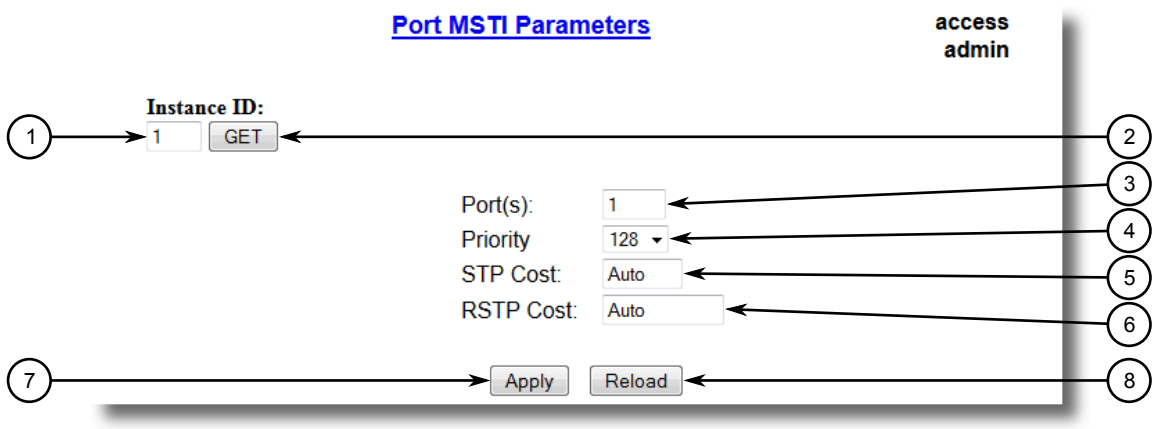


Figure 105: Port MSTI Parameters Form

1. Instance ID Box **2.** Get Button **3.** Port(s) Box **4.** Priority List **5.** STP Cost Box **6.** RSTP Cost Box **7.** Apply Button **8.** Reload Button

3. Under **Instance ID**, type an ID number for a Multiple Spanning Tree Instance (MSTI) and click **GET**. The settings for the MSTI are displayed. Any changes made to the configuration will be applied specifically to this instance ID.
4. Configure the following parameter(s) as required:

Parameter	Description
Port(s)	**Synopsis:** Any combination of numbers valid for this parameter The port number as seen on the front plate silkscreen of the switch (or a list of ports, if aggregated in a port trunk).
Priority	**Synopsis:** { 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, 240 } **Default:** 128 Selects the STP port priority. Ports of the same cost that attach to a common LAN will select the port to be used based upon the port priority.
STP Cost	**Synopsis:** 0 to 65535 or { Auto } **Default:** Auto Selects the cost to use in cost calculations, when the Cost Style parameter is set to STP in the Bridge RSTP Parameters configuration. Setting the cost manually provides the ability to preferentially select specific ports to carry traffic over others. Leave this field set to "auto" to use the standard STP port costs as negotiated (4 for 1Gbps, 19 for 100 Mbps links and 100 for 10 Mbps links). For MSTP, this parameter applies to both external and internal path cost.
RSTP Cost	**Synopsis:** 0 to 2147483647 or { Auto } **Default:** Auto Selects the cost to use in cost calculations, when the Cost Style parameter is set to RSTP in the Bridge RSTP Parameters configuration. Setting the cost manually provides the ability to preferentially select specific ports to carry traffic over others. Leave this field set to "auto" to use the standard RSTP port costs

Parameter	Description
	as negotiated (20,000 for 1Gbps, 200,000 for 100 Mbps links and 2,000,000 for 10 Mbps links). For MSTP, this parameter applies to both external and internal path cost.

5. Click **Apply**.

Section 5.2.10

Clearing Spanning Tree Protocol Statistics

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

1. Navigate to ***Spanning Tree*** » ***Clear Spanning Tree Statistics*** . The **Clear Spanning Tree Statistics** form appears.

Figure 106: Clear Spanning Tree Statistics Form

1. Confirm Button

2. Click **Confirm**.

Section 5.3

Managing Classes of Service

Classes of Service (CoS) provides the ability to expedite the transmission of certain frames and port traffic over others. The CoS of a frame can be set to Normal, Medium, High, or Critical. By default, other than the control frames, RUGGEDCOM ROS enforces Normal CoS for all incoming traffic received without a priority tag.

IMPORTANT!
Use the highest supported CoS with caution, as it is always used by the switch for handling network management traffic, such as RSTP BPDUs.

If this CoS is used for regular network traffic, upon traffic bursts, it may result in the loss of some network management frames, which in turn may result in the loss of connectivity over the network.

The process of controlling traffic based on CoS occurs over two phases:

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* *Section 5.3.2, "Configuring Classes of Service for Specific Ethernet Ports"* .

Received frames are first examined to determine if their destination or source MAC address is found in the Static MAC Address Table. If they are, the CoS configured for the static MAC address is used. If neither destination or source MAC address is in the Static MAC Address Table, the frame is then examined for IEEE 802.1Q tags and the priority field is mapped to a CoS. If a tag is not present, the frame is examined to determine if it is an IP frame. If the frame is an IP frame and **Inspect TOS** is enabled in RUGGEDCOM ROS, the CoS is determined from the DSCP field. If the frame is not an IP frame or **Inspect TOS** is disabled, the default CoS for the port is used.

After inspection, the frame is forwarded to the egress port for transmission.

2. **Forwarding Phase**
   Once the CoS of the frame is determined, the frame is forwarded to the egress port, where it is collected into one of the priority queues according to the assigned CoS.

   CoS weighting selects the degree of preferential treatment that is attached to different priority queues. The ratio of the number of higher CoS to lower CoS frames transmitted can be configured. If desired, lower CoS frames can be transmitted only after all higher CoS frames have been serviced.

CONTENTS

- Section 5.3.1, "Configuring Classes of Service Globally"
- Section 5.3.2, "Configuring Classes of Service for Specific Ethernet Ports"
- Section 5.3.3, "Configuring Priority to CoS Mapping"
- Section 5.3.4, "Configuring DSCP to CoS Mapping"

Section 5.3.1

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.

Figure 107: Global CoS Parameters Form

1. CoS Weighting Options **2.** Apply Button **3.** Reload Button

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

Parameter	Description
CoS Weighting	**Synopsis:** { 8:4:2:1, Strict } **Default:** 8:4:2:1 During traffic bursts, frames queued in the switch pending transmission on a port may have different CoS priorities. This parameter specifies weighting algorithm for transmitting different priority CoS frames. Examples: • 8:4:2:1 - 8 Critical, 4 High, 2 Medium and 1 Normal priority CoS frame • Strict - lower priority CoS frames will be only transmitted after all higher priority CoS frames have been transmitted

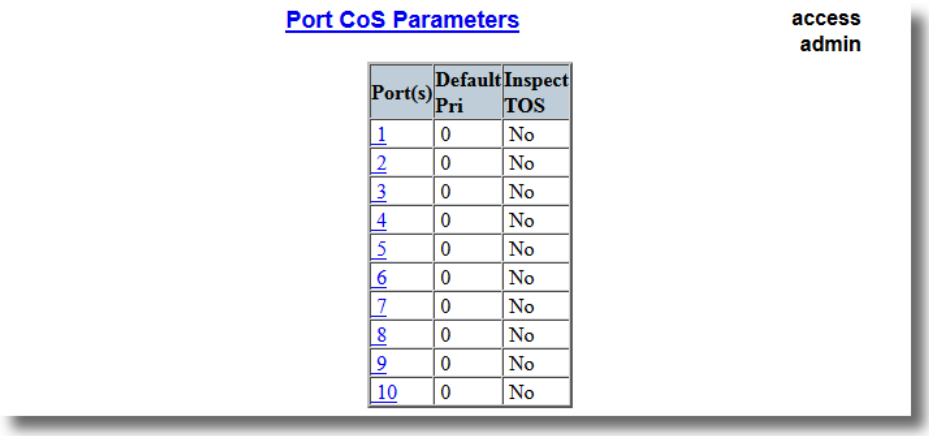
3. Click **Apply**.
4. If necessary, configure CoS mapping based on either the IEEE 802.1p priority or Differentiated Services (DS) field set in the IP header for each packet. For more information, refer to Section 5.3.3, "Configuring Priority to CoS Mapping" or Section 5.3.4, "Configuring DSCP to CoS Mapping" .

Section 5.3.2

Configuring Classes of Service for Specific Ethernet Ports

To configure Classes of Service (CoS) for one or more Ethernet ports, do the following:

1. Navigate to ***Classes of Service » Configure Port CoS Parameters*** . The **Port CoS Parameters** table appears.



Port(s)	Default Pri	Inspect TOS
1	0	No
2	0	No
3	0	No
4	0	No
5	0	No
6	0	No
7	0	No
8	0	No
9	0	No
10	0	No

Figure 108: Port CoS Parameters Table

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

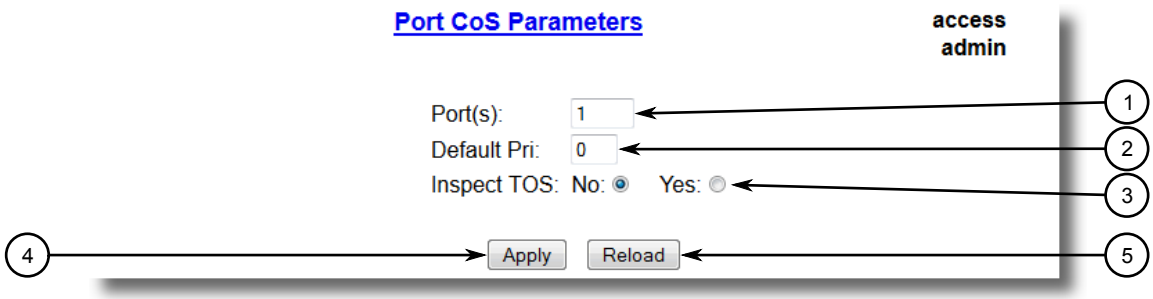


Figure 109: Port CoS Parameters Form

1. Port(s) Box **2.** Default Pri Box **3.** Inspect TOS Options **4.** Apply Button **5.** Reload Button

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

Parameter	Description
Port(s)	**Synopsis:** Any combination of numbers valid for this parameter The port number as seen on the front plate silkscreen of the switch (or a list of ports, if aggregated in a port trunk).
Default Pri	**Synopsis:** 0 to 7 **Default:** 0 This parameter allows to prioritize frames received on this port that are not prioritized based on the frames contents (e.g. priority field in the VLAN tag, DiffServ field in the IP header, prioritized MAC address).
Inspect TOS	**Synopsis:** { No, Yes } **Default:** No This parameters enables or disables parsing of the Type-Of-Service (TOS) field in the IP header of the received frames to determine what Class of Service they should be assigned. When TOS parsing

Parameter	Description
	is enabled the switch will use the Differentiated Services bits in the TOS field.

4. Click **Apply**.

Section 5.3.3

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.

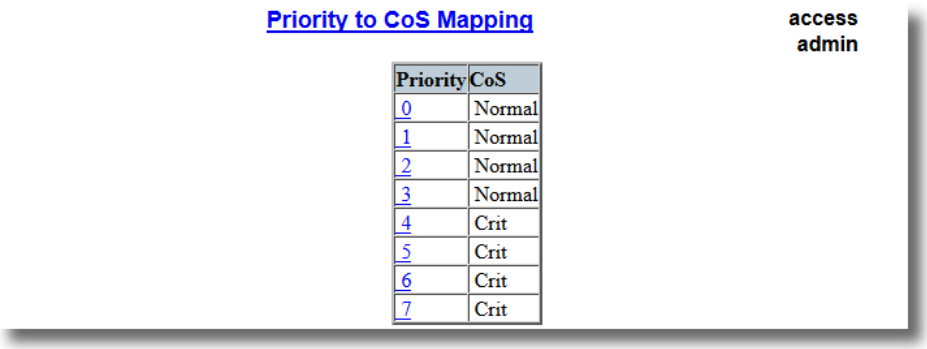


Figure 110: Priority to CoS Mapping Table

2. Select a priority level. The **Priority to CoS Mapping** form appears.

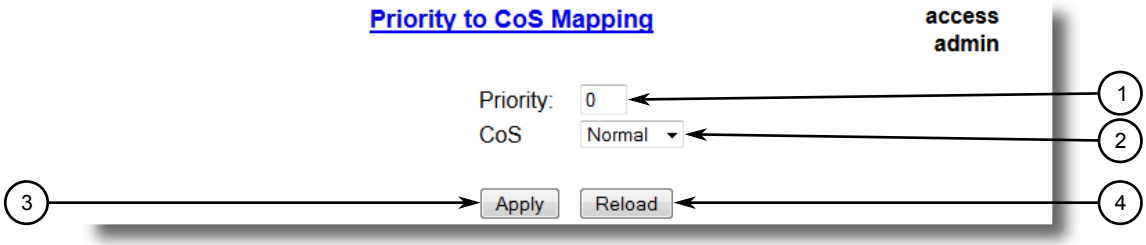


Figure 111: Priority to CoS Mapping Form

1. Priority Box **2.** CoS List **3.** Apply Button **4.** Reload Button

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

Parameter	Description
Priority	**Synopsis:** 0 to 7 **Default:** 0

Parameter	Description
	Value of the IEEE 802.1p priority.
CoS	**Synopsis:** { Normal, Medium, High, Crit } **Default:** Normal CoS assigned to received tagged frames with the specified IEEE 802.1p priority value.

4. Click **Apply**.

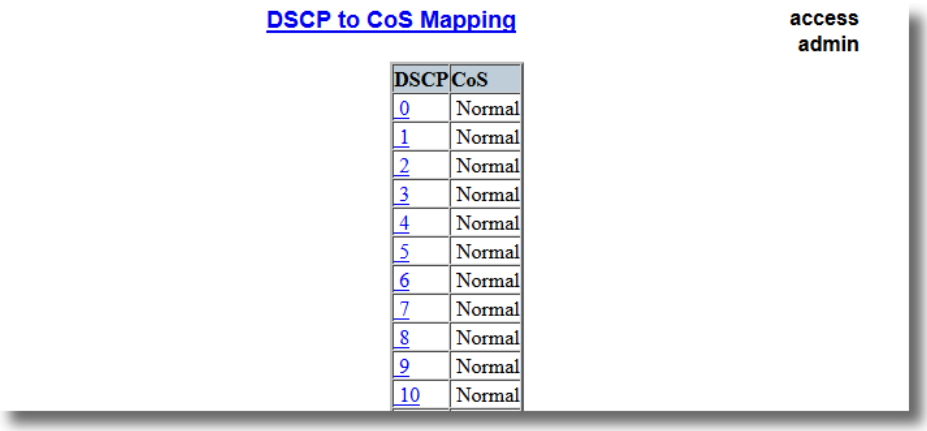
Section 5.3.4

Configuring DSCP to CoS Mapping

Mapping CoS to the Differentiated Services (DS) field set in the IP header for each packet is done by defining Differentiated Services Code Points (DSCPs) in the CoS configuration.

To map a DSCP to a Class of Service, do the following:

1. Navigate to ***Classes of Service » Configure DSCP to CoS Mapping*** . The **DSCP to CoS Mapping** table appears.



DSCP	CoS
0	Normal
1	Normal
2	Normal
3	Normal
4	Normal
5	Normal
6	Normal
7	Normal
8	Normal
9	Normal
10	Normal

Figure 112: DSCP to CoS Mapping Table

2. Select a DSCP level. The **DSCP to CoS Mapping** form appears.

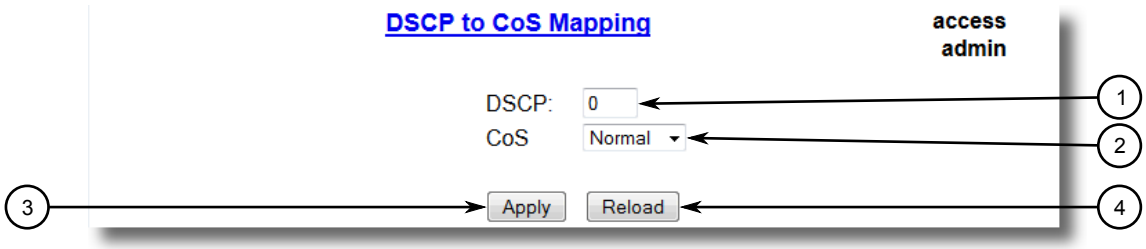


Figure 113: DSCP to CoS Mapping Form

1. DSCP Box **2.** CoS List **3.** Apply Button **4.** Reload Button

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

Parameter	Description
DSCP	**Synopsis:** 0 to 63 **Default:** 0 Differentiated Services Code Point (DSCP) - a value of the 6 bit DiffServ field in the Type-Of-Service (TOS) field of the IP header.
CoS	**Synopsis:** { Normal, Medium, High, Crit } **Default:** Normal Class of Service assigned to received frames with the specified DSCP.

4. Click **Apply**.
5. Configure the CoS parameters on select switched Ethernet ports as needed. For more information, refer to Section 5.3.2, “Configuring Classes of Service for Specific Ethernet Ports” .

Section 5.4

Managing MAC Addresses

The following section describes how to configure and manage MAC addresses.

CONTENTS

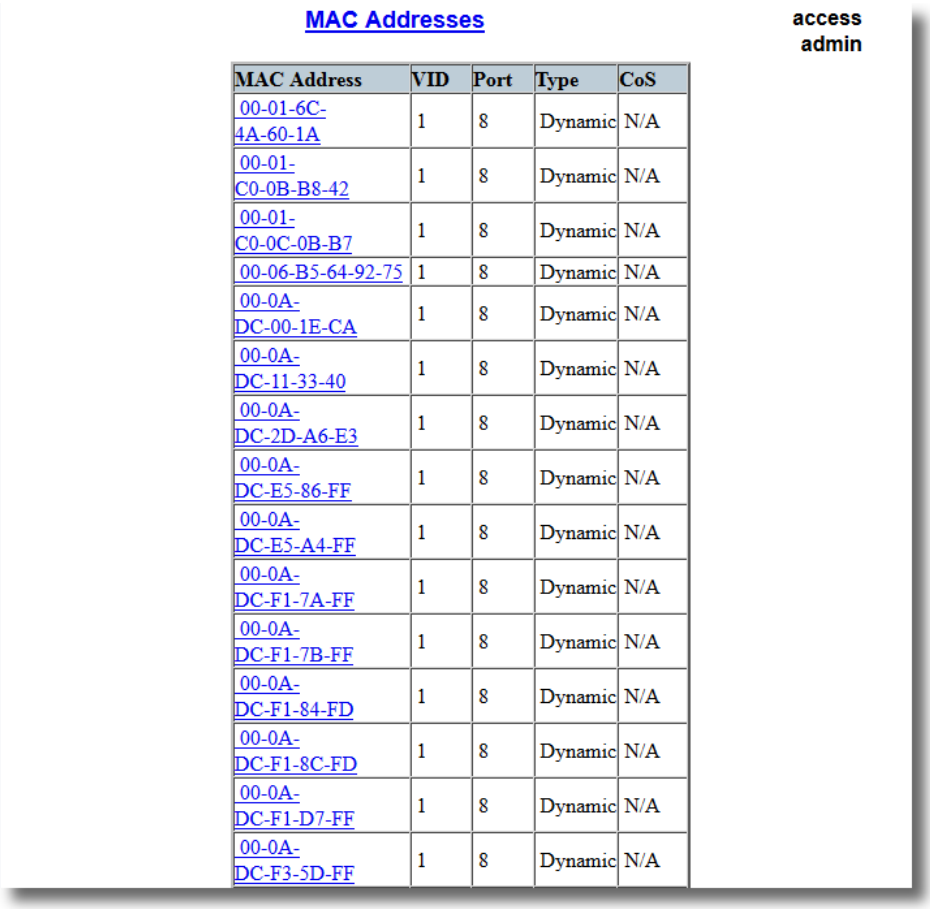
- Section 5.4.1, “Viewing a List of MAC Addresses”
- Section 5.4.2, “Configuring MAC Address Learning Options”
- Section 5.4.3, “Configuring MAC Address Flooding Options”
- Section 5.4.4, “Managing Static MAC Addresses”

- Section 5.4.5, “Purging All Dynamic MAC Addresses”

Section 5.4.1

Viewing a List of MAC Addresses

To view a list of all static and dynamically learned MAC addresses, navigate to ***MAC Address Tables*** » ***View MAC Addresses*** . The **MAC Addresses** table appears.



MAC Addresses

access
admin

MAC Address	VID	Port	Type	CoS
00-01-6C-4A-60-1A	1	8	Dynamic	N/A
00-01-C0-0B-B8-42	1	8	Dynamic	N/A
00-01-C0-0C-0B-B7	1	8	Dynamic	N/A
00-06-B5-64-92-75	1	8	Dynamic	N/A
00-0A-DC-00-1E-CA	1	8	Dynamic	N/A
00-0A-DC-11-33-40	1	8	Dynamic	N/A
00-0A-DC-2D-A6-E3	1	8	Dynamic	N/A
00-0A-DC-E5-86-FF	1	8	Dynamic	N/A
00-0A-DC-E5-A4-FF	1	8	Dynamic	N/A
00-0A-DC-F1-7A-FF	1	8	Dynamic	N/A
00-0A-DC-F1-7B-FF	1	8	Dynamic	N/A
00-0A-DC-F1-84-FD	1	8	Dynamic	N/A
00-0A-DC-F1-8C-FD	1	8	Dynamic	N/A
00-0A-DC-F1-D7-FF	1	8	Dynamic	N/A
00-0A-DC-F3-5D-FF	1	8	Dynamic	N/A

Figure 114: MAC Address Table

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

- 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 Section 5.4.2, “Configuring MAC Address Learning Options” .
- Configure the address on the device as a static MAC address. For more information, refer to Section 5.4.4.2, “Adding a Static MAC Address” .

Section 5.4.2

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 addressees 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.

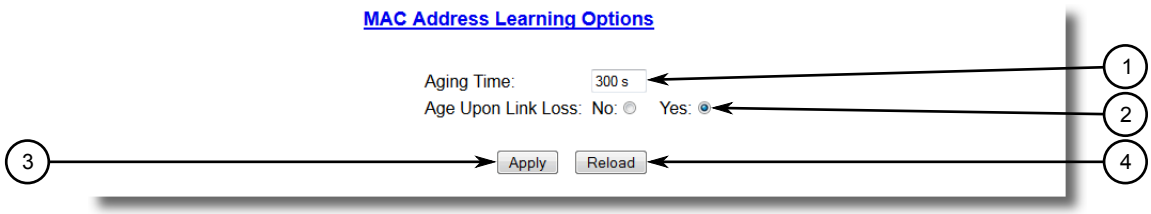


Figure 115: MAC Address Learning Options Form

1. Aging Time Box **2.** Age Upon Link Loss Options **3.** Apply Button **4.** Reload Button

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

Parameter	Description
Aging Time	**Synopsis:** 15 to 800 **Default:** 300 s This parameter configures the time that a learned MAC address is held before being aged out.
Age Upon Link Loss	**Synopsis:** { No, Yes } **Default:** Yes When set to Yes, all MAC addresses learned on a failed port will be aged-out immediately upon link failure detection. When link failure occurs the switch may have some MAC addresses previously learned on the failed port. As long as those addresses are not aged-out the switch will still be forwarding traffic to that port, thus preventing that traffic from reaching its destination via the new network topology. Note that when a network redundancy protocol, e.g. RSTP/MSTP, is enabled on the switch, that redundancy protocol may, upon a link failure, flush MAC addresses learned on the failed port regardless of the setting of this parameter.

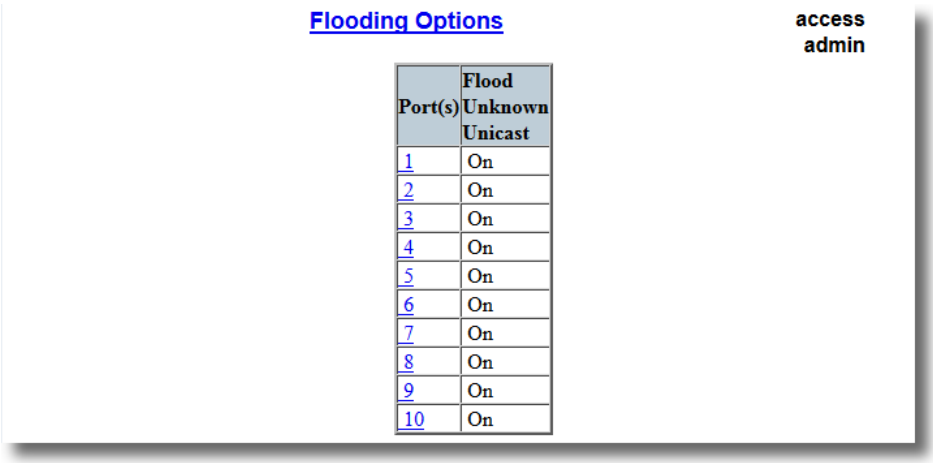
3. Click **Apply**.

Section 5.4.3

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.



Port(s)	Flood Unknown Unicast
1	On
2	On
3	On
4	On
5	On
6	On
7	On
8	On
9	On
10	On

Figure 116: Flooding Options Table

2. Select a port. The **Flooding Options** form appears.

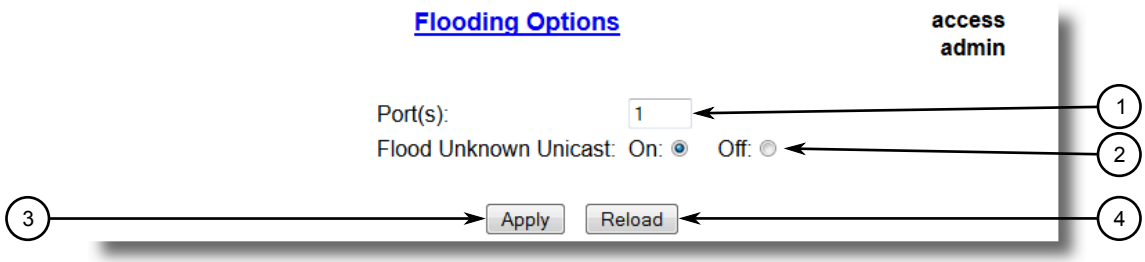


Figure 117: Flooding Options Form

1. Port(s) Box **2.** Flood Unknown Unicast Options **3.** Apply Button **4.** Reload Button

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

Parameter	Description
Port(s)	**Synopsis:** Comma-separated list of ports The port number as seen on the front plate silkscreen of the switch (or a list of ports, if aggregated in a port trunk).
Flood Unknown Unicast	**Synopsis:** { On, Off } **Default:** On Normally, unicast traffic with an unknown destination address is flooded out of all ports. When a port is configured to turn off this kind of flooding, the unknown unicast traffic is not sent out from the selected port.

4. Click **Apply**.

Section 5.4.4

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 ROS will generate a port security alarm.

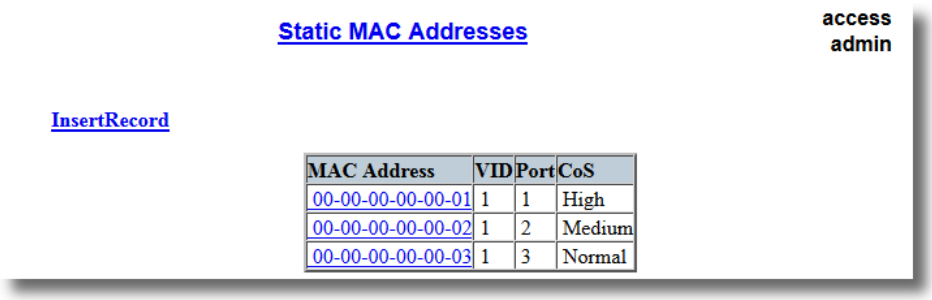
CONTENTS

- Section 5.4.4.1, “Viewing a List of Static MAC Addresses”
- Section 5.4.4.2, “Adding a Static MAC Address”
- Section 5.4.4.3, “Deleting a Static MAC Address”

Section 5.4.4.1

Viewing a List of Static MAC Addresses

To view a list of static MAC addresses configured on the device, navigate to ***MAC Address Tables » Configure Static MAC Addresses*** . The **Static MAC Addresses** table appears.



MAC Address	VID	Port	CoS
00-00-00-00-00-01	1	1	High
00-00-00-00-00-02	1	2	Medium
00-00-00-00-00-03	1	3	Normal

Figure 118: Static MAC Address Table

If static MAC addresses have not been configured, add addresses as needed. For more information, refer to Section 5.4.4.2, “Adding a Static MAC Address” .

Section 5.4.4.2

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.

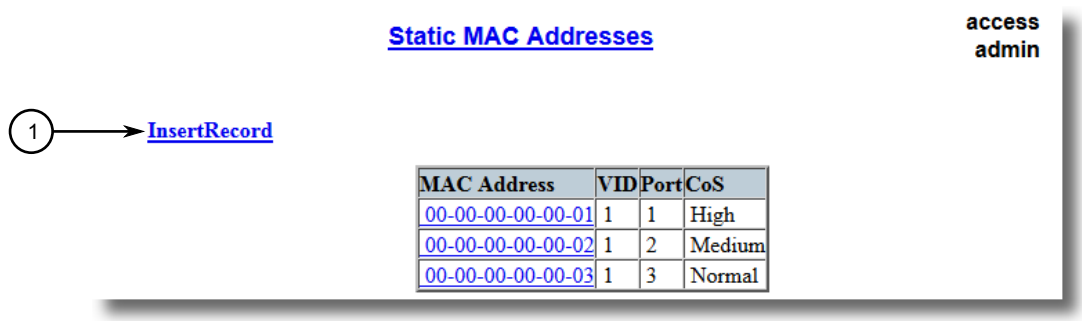


Figure 119: Static MAC Addresses Table

1. InsertRecord

2. Click **InsertRecord**. The **Static MAC Addresses** form appears.

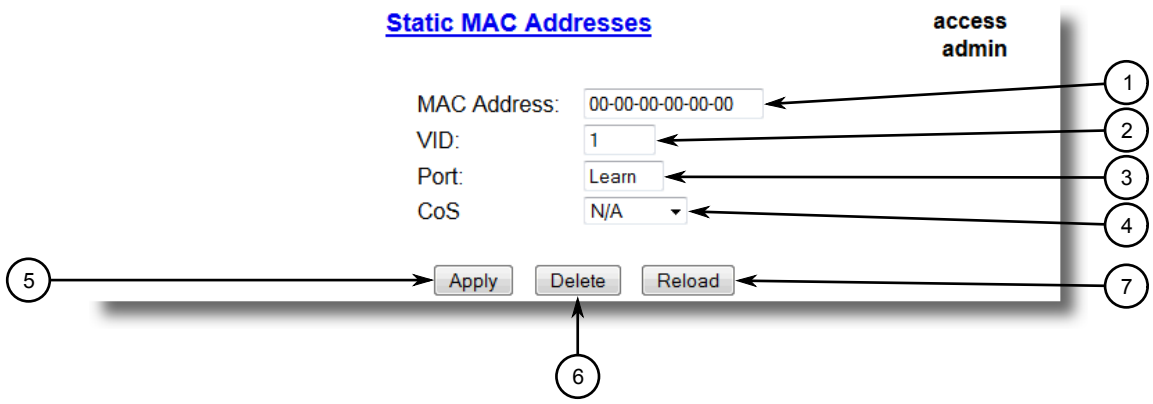


Figure 120: Static MAC Addresses Form

1. MAC Address Box **2.** VID Box **3.** Port Box **4.** CoS List **5.** Apply Button **6.** Delete Button **7.** Reload Button

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

Parameter	Description
MAC Address	**Synopsis:** ##-##-##-##-##-## where ## ranges 0 to FF A MAC address learned by the switch. Maximum of 6 wildcard characters may be used to specify a range of MAC addresses allowed to be learned by the Port Security module (when Port Security is set to 'Static MAC' mode). Wildcard must start from the right hand end and continuous. Examples: • *00-0A-DC-**-**-*** means the entire MAC address space of RuggedCom. • *00-0A-DC-12-3*-*** means the range 00-0A-DC-12-30-00 to 00-0A-DC-12-3F-FF.
VID	**Synopsis:** 1 to 4094 or { ANY } **Default:** 1

Parameter	Description
	VLAN Identifier of the VLAN upon which the MAC address operates. Option ANY allows learning a MAC address through the Port Security module on any VLAN's that are configured on the switch.
Port	**Synopsis:** 1 to maximum port number or { Learn } **Default:** Learn Enter the port number upon which the device with this address is located. The security mode of the port being selected should not be '802.1X'. If the port should be auto-learned, set this parameter to 'Learn'. The option 'Learn' is applicable for Port Security in 'Static MAC' mode.
CoS	**Synopsis:** { N/A, Normal, Medium, High, Crit } **Default:** N/A Prioritizes traffic for the specified MAC address. To not prioritize traffic based on the address, select N/A.

4. Click **Apply**.

Section 5.4.4.3

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.

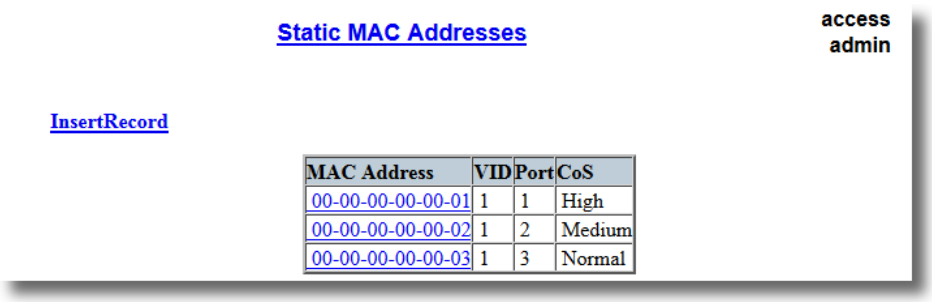


Figure 121: Static MAC Addresses Table

2. Select the MAC address from the table. The **Static MAC Addresses** form appears.

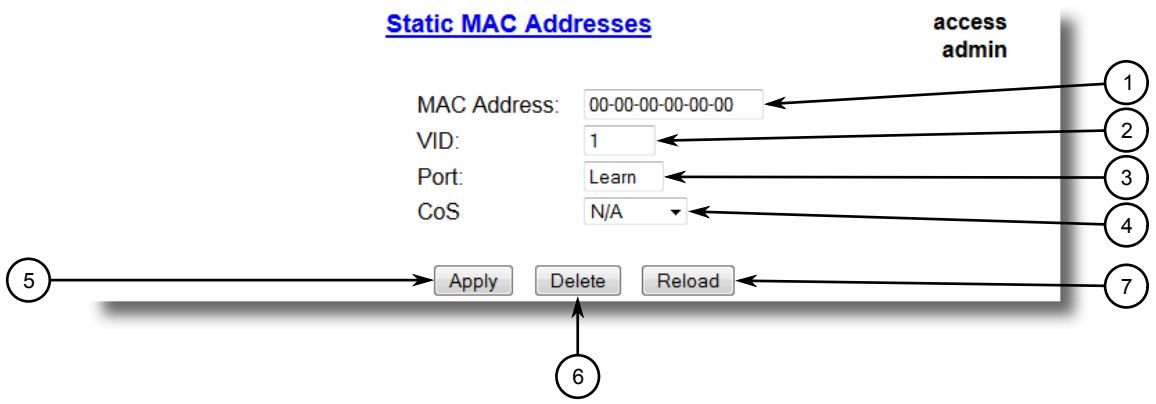


Figure 122: Static MAC Addresses Form

1. MAC Address Box **2.** VID Box **3.** Port Box **4.** CoS List **5.** Apply Button **6.** Delete Button **7.** Reload Button

3. Click **Delete**.

Section 5.4.5

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.

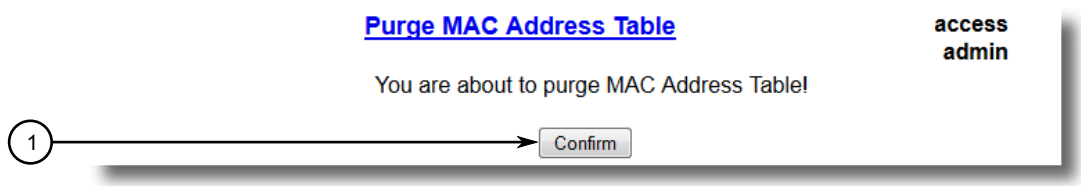


Figure 123: Purge MAC Address Table Form

1. Confirm Button

2. Click **Confirm**.

Section 5.5

Managing Time Services

The System Time Manager offers the following time-keeping and time synchronization features:

- Local hardware time keeping and time zone management

- SNTP (Simple Network Time Protocol) client and server

CONTENTS

- Section 5.5.1, "Configuring the Time and Date"
- Section 5.5.2, "Managing NTP"

Section 5.5.1

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.

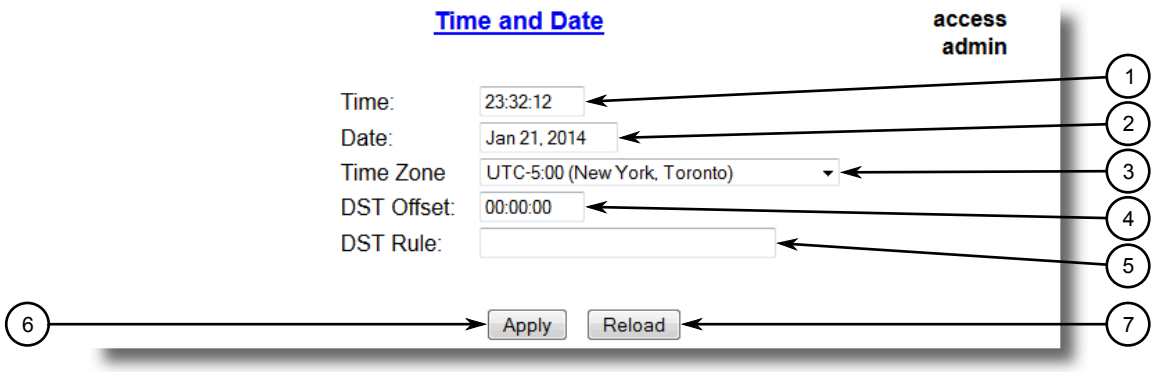


Figure 124: Time and Date Form

1. Time **2.** Date **3.** Time Zone **4.** DST Offset **5.** DST Rule **6.** Apply Button **7.** Reload Button

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

Parameter	Description
Time	**Synopsis:** HH:MM:SS This parameter allows for both the viewing and setting of the local time.
Date	**Synopsis:** MMM DD, YYYY This parameter allows for both the viewing and setting of the local date.
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), ... } **Default:** UTC-5:00 (New York, Toronto)

Parameter	Description
	This setting allows for the conversion of UTC (Universal Coordinated Time) to local time.
DST Offset	**Synopsis:** HH:MM:SS **Default:** 00:00:00 This parameter specifies the amount of time to be shifted forward/backward when DST begins and ends. For example for most part of USA and Canada, DST time shift is 1 hour (01:00:00) forward when DST begins and 1 hour backward when DST ends.
DST Rule	**Synopsis:** mm.n.d/HH:MM:SS mm.n.d/HH:MM:SS This parameter specifies a rule for time and date when the transition between Standard and Daylight Saving Time occurs. • mm - Month of the year (01 - January, 12 - December) • n - nth d-day in the month (1 - 1st d-day, 5 - 5th/last d-day) • d - day of the week (0 - Sunday, 6 - Saturday) • HH - hour of the day (0 - 24) • MM - minute of the hour (0 - 59) • SS - second of the minute (0 - 59) Example: The following rule applies in most part of USA and Canada: `03.2.0/02:00:00 11.1.0/02:00:00` DST begins on March's 2nd Sunday at 2:00am. DST ends on November's 1st Sunday at 2:00am.

Section 5.5.2

Managing NTP

RUGGEDCOM ROS may be configured to refer periodically to a specified NTP server to correct any accumulated drift in the on-board clock. RUGGEDCOM ROS will also serve time via the Simple Network Time Protocol (SNTP) to hosts that request it.

Two NTP servers (primary and backup) may be configured for the device. The primary server is contacted first for each attempt to update the system time. If the primary server fails to respond, the backup server is contacted. If either the primary or backup server fails to respond, an alarm is raised.

CONTENTS

• Section 5.5.2.1, “Enabling/Disabling NTP Service”
• Section 5.5.2.2, “Configuring NTP Servers”

Section 5.5.2.1

Enabling/Disabling NTP Service

To enable or disable NTP Service, do the following:

1. **NOTE**
   If the device is running as an NTP server, NTP service must be enabled.

   Navigate to ***Administration*** » ***System Time Manager*** » ***Configure NTP*** » ***Configure NTP Service*** . The **SNTP Parameters** form appears.

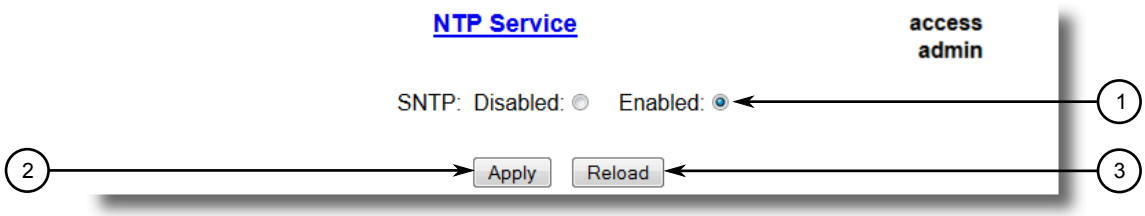


Figure 125: SNTP Parameters Form

1. SNTP Options **2.** Apply Button **3.** Reload Button

2. Select **Enabled** to enable SNTP, or select **Disabled** to disable SNTP.
3. Click **Apply**.

Section 5.5.2.2

Configuring NTP Servers

To configure either the primary or backup NTP server, do the following:

1. Navigate to ***Administration*** » ***System Time Manager*** » ***Configure NTP*** » ***Configure NTP Servers*** . The **NTP Servers** table appears.

Figure 126: NTP Servers Table

2. Select either **Primary** or **Backup**. The **NTP Servers** form appears.

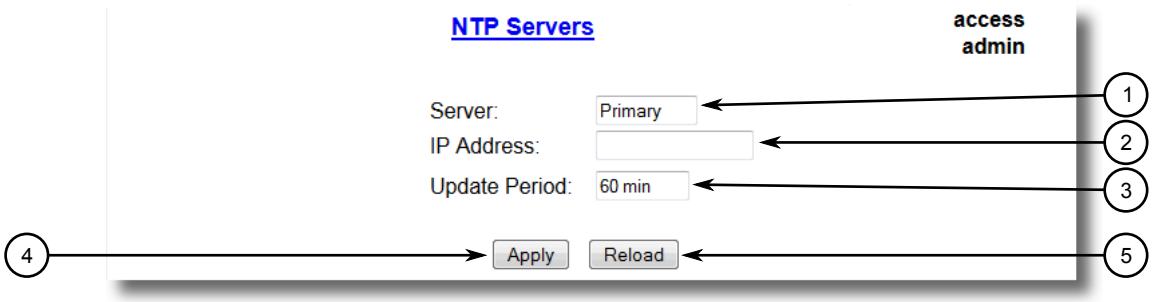


Figure 127: NTP Servers Form

1. Server Box **2.** IP Address Box **3.** Update Period Box **4.** Apply Button **5.** Reload Button

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

Parameter	Description
Server	**Synopsis:** Any 8 characters **Default:** Primary This field tells whether this configuration is for a Primary or a Backup Server.
IP Address	**Synopsis:** ###.###.###.### where ### ranges from 0 to 255 The Server IP Address.
Update Period	**Synopsis:** 1 to 1440 min **Default:** 60 min 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**.

Section 5.6

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**.

CONTENTS

- Section 5.6.1, “Managing SNMP Users”
- Section 5.6.2, “Managing Security-to-Group Mapping”
- Section 5.6.3, “Managing SNMP Groups”

Section 5.6.1

Managing SNMP Users

The following section describes how to configure and manage SNMP users.

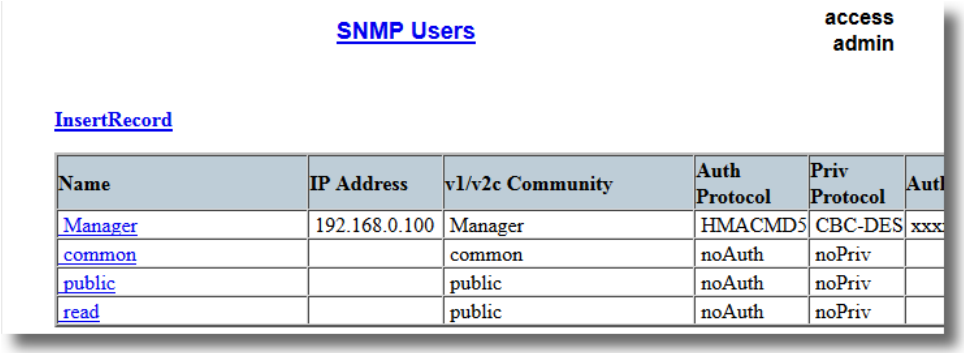
CONTENTS

- Section 5.6.1.1, “Viewing a List of SNMP Users”
- Section 5.6.1.2, “Adding an SNMP User”
- Section 5.6.1.3, “Deleting an SNMP User”

Section 5.6.1.1

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.



Name	IP Address	v1/v2c Community	Auth Protocol	Priv Protocol	Autl
Manager	192.168.0.100	Manager	HMACMD5	CBC-DES	xxx
common		common	noAuth	noPriv	
public		public	noAuth	noPriv	
read		public	noAuth	noPriv	

Figure 128: SNMP Users Table

If users have not been configured, add users as needed. For more information, refer to Section 5.6.1.2, "Adding an SNMP User" .

Section 5.6.1.2

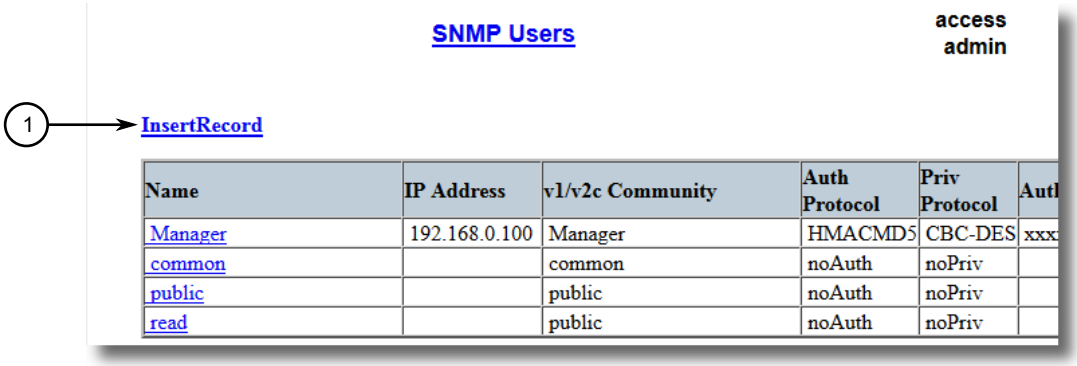
Adding an SNMP User

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.*

To add a new SNMP user, do the following:

1. Navigate to ***Administration*** » ***Configure SNMP*** » ***Configure SNMP Users*** . The **SNMP Users** table appears.



Name	IP Address	v1/v2c Community	Auth Protocol	Priv Protocol	Autl
Manager	192.168.0.100	Manager	HMACMD5	CBC-DES	xxx
common		common	noAuth	noPriv	
public		public	noAuth	noPriv	
read		public	noAuth	noPriv	

Figure 129: SNMP Users Table

1. InsertRecord

2. Click **InsertRecord**. The **SNMP Users** form appears.

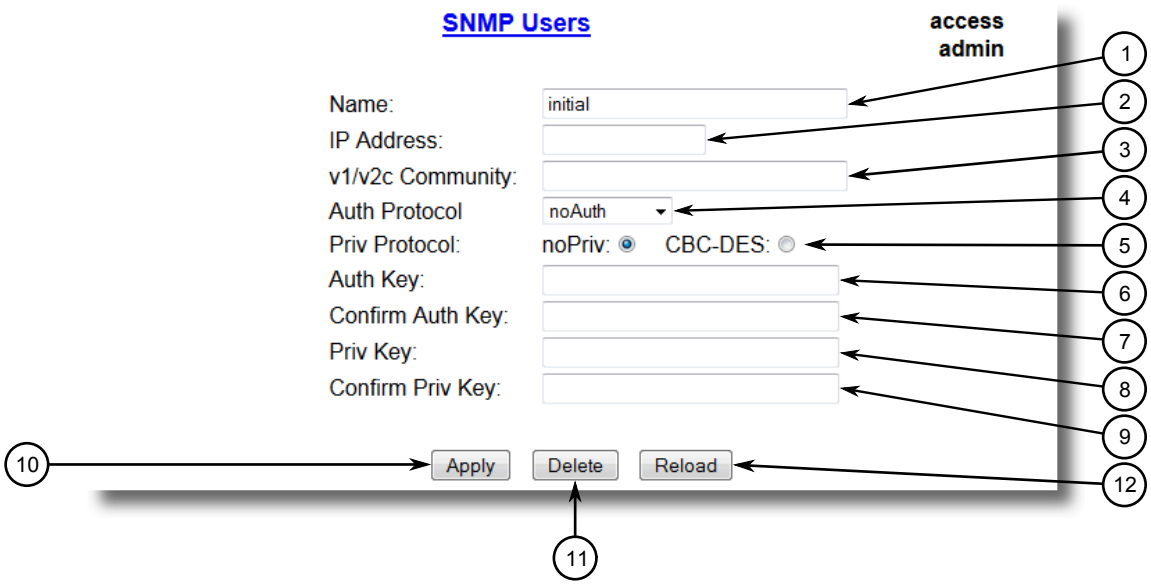


Figure 130: SNMP Users Form

1. Name Box **2.** IP Address Box **3.** v1/v2c Community Box **4.** Auth Protocol Box **5.** Priv Protocol Box **6.** Auth Key Box **7.** Confirm Auth Key Box **8.** Priv Key Box **9.** Confirm Priv Key Box **10.** Apply Button **11.** Delete Button **12.** Reload Button

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 *Section 4.6, "Managing Alarms"*.

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

Parameter	Description
Name	**Synopsis:** Any 32 characters **Default:** initial The name of the user. This user name also represents the security name that maps this user to the security group.
IP Address	**Synopsis:** ###.###.###.### where ### ranges from 0 to 255 The IP address of the user's SNMP management station. If IP address is configured, SNMP requests from that user will be verified by IP address as well. SNMP Authentication trap will be

Parameter	Description
	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:** Any 32 characters The community string which is mapped by this user/security name to the security group if security model is SNMPv1 or SNMPv2c. If this string is left empty, it will be assumed to be equal to the same as user name.
Auth Protocol	**Synopsis:** { noAuth, HMACMD5, HMACSHA } **Default:** noAuth An indication of whether messages sent on behalf of this user to/from SNMP engine, can be authenticated, and if so, the type of authentication protocol which is used.
Priv Protocol	**Synopsis:** { noPriv, CBC-DES } **Default:** noPriv An Indication of whether messages sent on behalf of this user to/from SNMP engine can be protected from disclosure, and if so, the type of privacy protocol which is used.
Auth Key	**Synopsis:** 31 character ASCII string 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:** 31 character ASCII string 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:** 31 character ASCII string 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:** 31 character ASCII string 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.

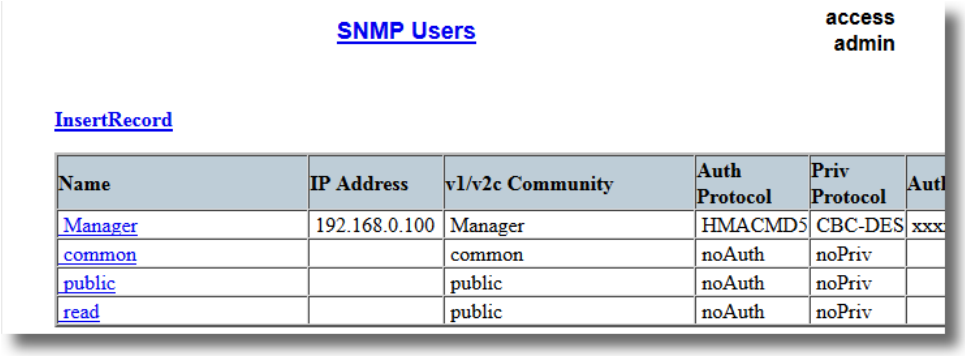
4. Click **Apply**.

Section 5.6.1.3

Deleting an SNMP User

To delete an SNMP user, do the following:

1. Navigate to ***Administration*** » ***Configure SNMP*** » ***Configure SNMP Users*** . The **SNMP Users** table appears.



Name	IP Address	v1/v2c Community	Auth Protocol	Priv Protocol	Autl
Manager	192.168.0.100	Manager	HMACMD5	CBC-DES	xxx
common		common	noAuth	noPriv	
public		public	noAuth	noPriv	
read		public	noAuth	noPriv	

Figure 131: SNMP Users Table

2. Select the user from the table. The **SNMP Users** form appears.

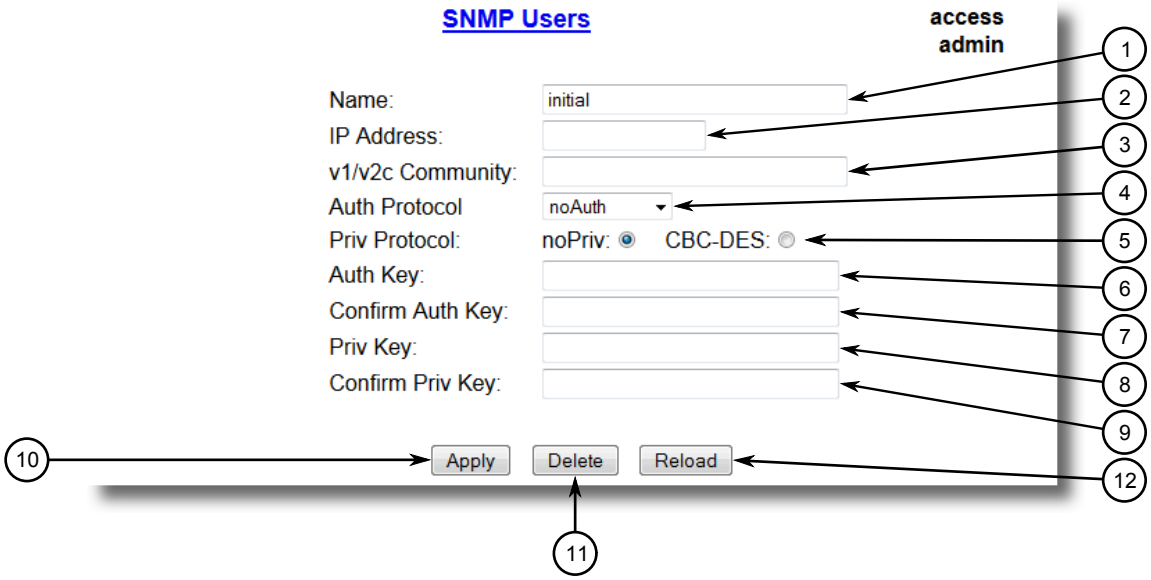


Figure 132: SNMP Users Form

1. Name Box **2.** IP Address Box **3.** v1/v2c Community Box **4.** Auth Protocol Box **5.** Priv Protocol Box **6.** Auth Key Box **7.** Confirm Auth Key Box **8.** Priv Key Box **9.** Confirm Priv Key Box **10.** Apply Button **11.** Delete Button **12.** Reload Button

3. Click **Delete**.

Section 5.6.2

Managing Security-to-Group Mapping

The following section describes how to configure and manage security-to-group maps.

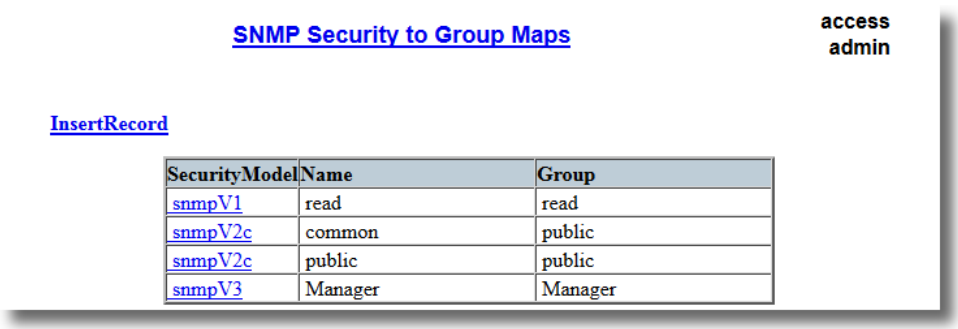
CONTENTS

- Section 5.6.2.1, “Viewing a List of Security-to-Group Maps”
- Section 5.6.2.2, “Adding a Security-to-Group Map”
- Section 5.6.2.3, “Deleting a Security-to-Group Map”

Section 5.6.2.1

Viewing a List of Security-to-Group Maps

To view a list of security-to-group maps configured on the device, navigate to ***Administration » Configure SNMP » Configure SNMP Security to Group Maps*** . The **SNMP Security to Group Maps** table appears.



SecurityModel	Name	Group
snmpV1	read	read
snmpV2c	common	public
snmpV2c	public	public
snmpV3	Manager	Manager

Figure 133: SNMP Security to Group Maps Table

If security-to-group maps have not been configured, add maps as needed. For more information, refer to Section 5.6.2.2, “Adding a Security-to-Group Map” .

Section 5.6.2.2

Adding a Security-to-Group Map

Multiple combinations of security models and groups can be mapped (up to a maximum of 32) for SNMP.

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.

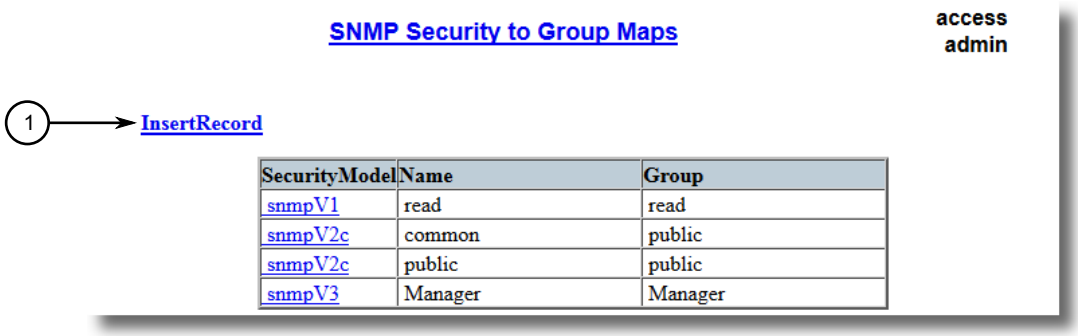


Figure 134: SNMP Security to Group Maps Table

1. InsertRecord

2. Click **InsertRecord**. The **SNMP Security to Group Maps** form appears.

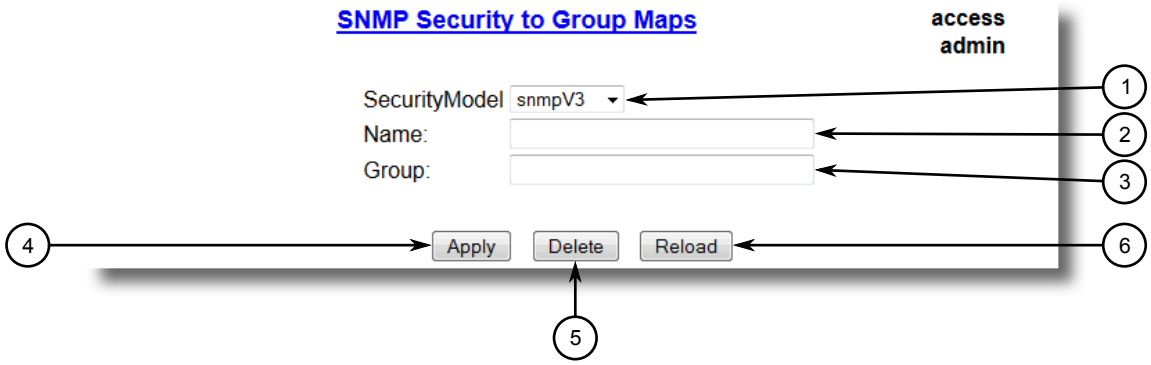


Figure 135: SNMP Security to Group Maps Form

1. Security Model Box **2.** Name Box **3.** Group Box **4.** Apply Button **5.** Delete Button **6.** Reload Button

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

Parameter	Description
SecurityModel	**Synopsis:** { snmpV1, snmpV2c, snmpV3 } **Default:** snmpV3 The Security Model that provides the name referenced in this table.
Name	**Synopsis:** Any 32 characters The user name which is mapped by this entry to the specified group name.
Group	**Synopsis:** Any 32 characters The group name to which the security model and name belong. This name is used as an index to the SNMPv3 VACM Access Table.

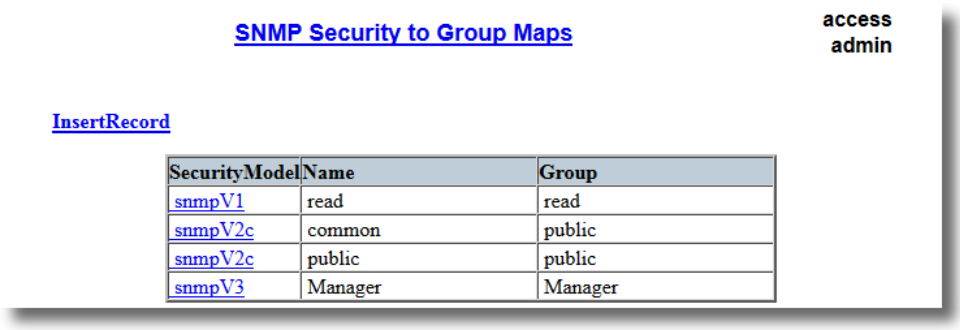
4. Click **Apply**.

Section 5.6.2.3

Deleting a Security-to-Group Map

To delete a security-to-group map, do the following:

1. Navigate to ***Administration » Configure SNMP » Configure SNMP Security to Group Maps*** . The **SNMP Security to Group Maps** table appears.



SecurityModel	Name	Group
snmpV1	read	read
snmpV2c	common	public
snmpV2c	public	public
snmpV3	Manager	Manager

Figure 136: SNMP Security to Group Maps Table

2. Select the map from the table. The **SNMP Security to Group Maps** form appears.

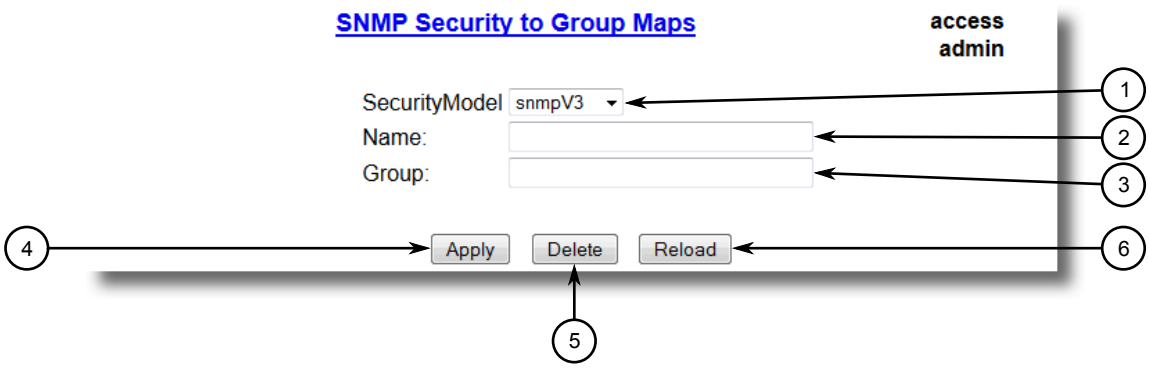


Figure 137: SNMP Security to Group Maps Form

1. Security Model Box **2.** Name Box **3.** Group Box **4.** Apply Button **5.** Delete Button **6.** Reload Button

3. Click **Delete**.

Section 5.6.3

Managing SNMP Groups

Multiple SNMP groups (up to a maximum of 32) can be configured to have access to SNMP.

CONTENTS

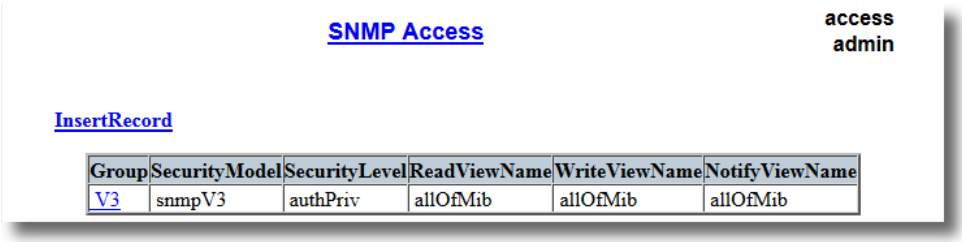
- Section 5.6.3.1, “Viewing a List of SNMP Groups”
- Section 5.6.3.2, “Adding an SNMP Group”

- Section 5.6.3.3, “Deleting an SNMP Group”

Section 5.6.3.1

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.



Group	SecurityModel	SecurityLevel	ReadViewName	WriteViewName	NotifyViewName
V3	snmpV3	authPriv	allOfMib	allOfMib	allOfMib

Figure 138: SNMP Access Table

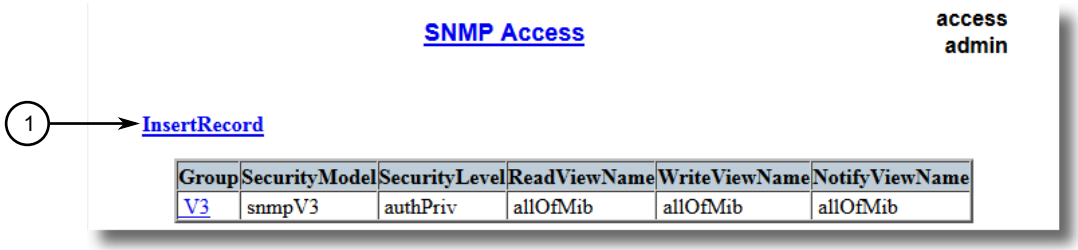
If SNMP groups have not been configured, add groups as needed. For more information, refer to Section 5.6.3.2, “Adding an SNMP Group” .

Section 5.6.3.2

Adding an SNMP Group

To add an SNMP group, do the following:

1. Navigate to ***Administration*** » ***Configure SNMP*** » ***Configure SNMP Access*** . The **SNMP Access** table appears.



Group	SecurityModel	SecurityLevel	ReadViewName	WriteViewName	NotifyViewName
V3	snmpV3	authPriv	allOfMib	allOfMib	allOfMib

Figure 139: SNMP Access Table

1. InsertRecord

2. Click **InsertRecord**. The **SNMP Access** form appears.

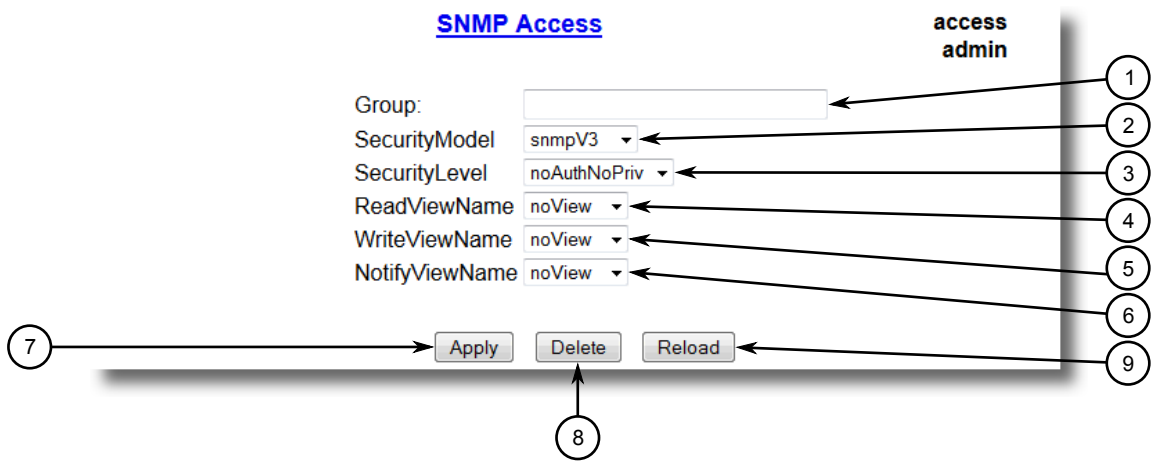


Figure 140: SNMP Access Form

1. Group Box **2.** Security Model Box **3.** Security Level Box **4.** ReadViewName Box **5.** WriteViewName Box **6.** NotifyViewName Box **7.** Apply Button **8.** Delete Button **9.** Reload Button

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

Parameter	Description
Group	**Synopsis:** Any 32 characters The group name to which the security model and name belong. This name is used as an index to the SNMPv3 VACM Access Table.
SecurityModel	**Synopsis:** { snmpV1, snmpV2c, snmpV3 } **Default:** snmpV3 In order to gain the access rights allowed by this entry, configured security model must be in use.
SecurityLevel	**Synopsis:** { noAuthNoPriv, authNoPriv, authPriv } **Default:** noAuthNoPriv The minimum level of security reqwuired in order to gain the access rights allowed by this entry. A security level of noAuthNoPriv is less than authNoPriv, which is less than authPriv.
ReadViewName	**Synopsis:** { noView, V1Mib, allOfMib } **Default:** noView This parameter identifies the MIB tree(s) to which this entry authorizes read access. If the value is noView, then no read access is granted.
WriteViewName	**Synopsis:** { noView, V1Mib, allOfMib } **Default:** noView This parameter identifies the MIB tree(s) to which this entry authorizes write access. If the value is noView, then no write access is granted.
NotifyViewName	**Synopsis:** { noView, V1Mib, allOfMib } **Default:** noView This parameter identifies the MIB tree(s) to which this entry authorizes access for notifications. If the value is noView, then no access for notifications is granted.

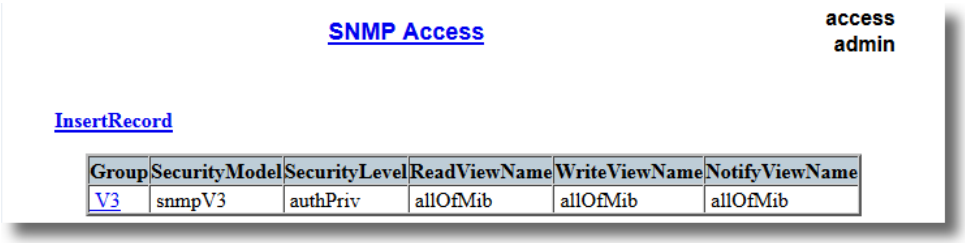
4. Click **Apply**.

Section 5.6.3.3

Deleting an SNMP Group

To delete an SNMP group, do the following:

1. Navigate to ***Administration » Configure SNMP » Configure SNMP Access*** . The **SNMP Access** table appears.



Group	SecurityModel	SecurityLevel	ReadViewName	WriteViewName	NotifyViewName
V3	snmpV3	authPriv	allOfMib	allOfMib	allOfMib

Figure 141: SNMP Access Table

2. Select the group from the table. The **SNMP Access** form appears.

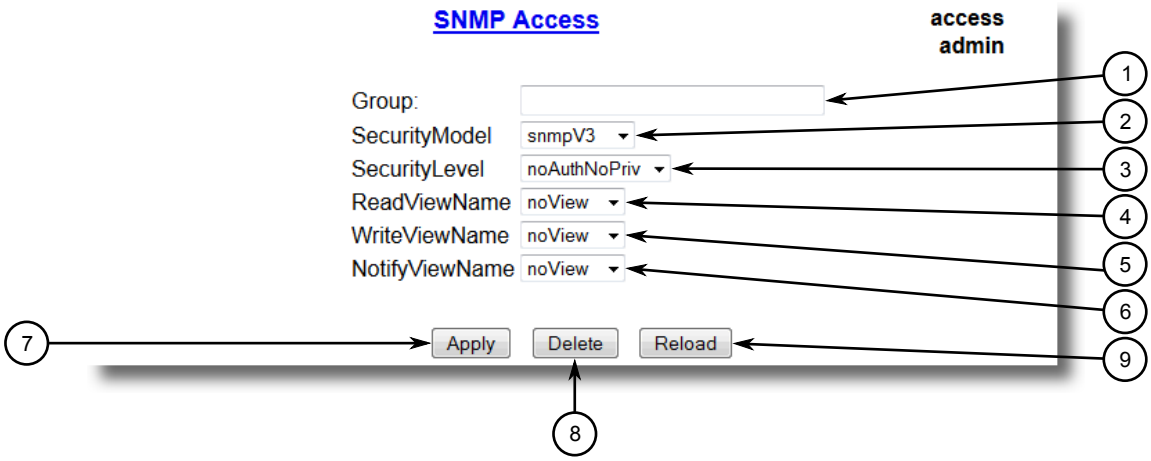


Figure 142: SNMP Access Form

1. Group Box **2.** Security Model Box **3.** Security Level Box **4.** ReadViewName Box **5.** WriteViewName Box **6.** NotifyViewName Box **7.** Apply Button **8.** Delete Button **9.** Reload Button

3. Click **Delete**.

Section 5.7

Managing Network Discovery

RUGGEDCOM ROS supports the Link Layer Discovery Protocol (LLDP) and RUGGEDCOM Discovery Protocol (RCDP), both Layer 2 protocols for automated network discovery.

CONTENTS

- Section 5.7.1, "Network Discovery Concepts"
- Section 5.7.2, "Configuring LLDP Globally"
- Section 5.7.3, "Configuring LLDP for an Ethernet Port"
- Section 5.7.4, "Enabling/Disabling RCDP"
- Section 5.7.5, "Viewing Global Statistics and Advertised System Information"
- Section 5.7.6, "Viewing Statistics for LLDP Neighbors"
- Section 5.7.7, "Viewing Statistics for LLDP Ports"

Section 5.7.1

Network Discovery Concepts

The following section describes some of the concepts important to the implementation of network discovery in RUGGEDCOM ROS.

CONTENTS

- Section 5.7.1.1, "Link Layer Discovery Protocol (LLDP)"
- Section 5.7.1.2, " RUGGEDCOM Discovery Protocol (RCDP)"

Section 5.7.1.1

Link Layer Discovery Protocol (LLDP)

LLDP is an IEEE standard protocol, IEEE 802.11AB, that 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.

Section 5.7.1.2
RUGGEDCOM Discovery Protocol (RCDP)

RUGGEDCOM Discovery Protocol (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 on all devices when Explorer is shut down. If RUGGEDCOM Explorer is unable to disable RCDP on a device, RUGGEDCOM ROS will automatically disable RCDP after approximately one hour of inactivity.

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.

Section 5.7.2
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.

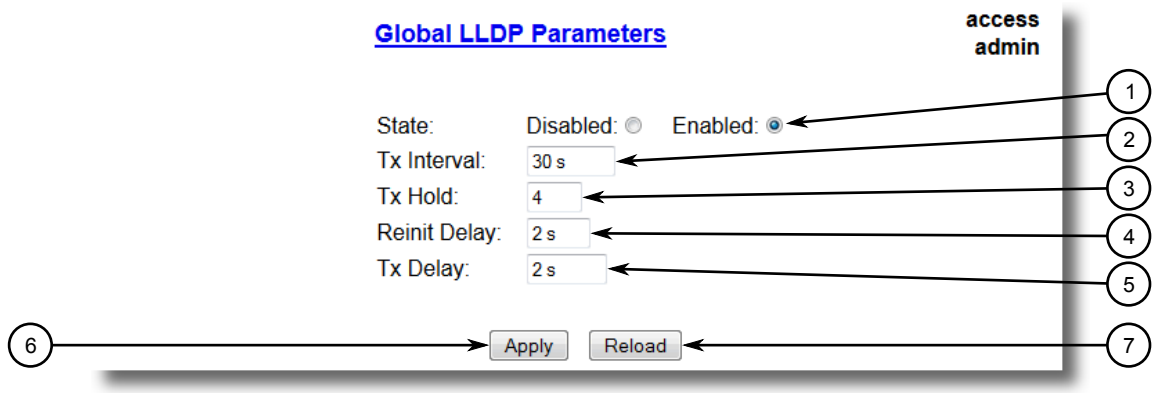


Figure 143: Global LLDP Parameters Form

1. State Options **2.** Tx Interval Box **3.** Tx Hold Box **4.** Reinit Delay Box **5.** Tx Delay Box **6.** Apply Button **7.** Reload Button

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

Parameter	Description
State	**Synopsis:** { Disabled, Enabled } **Default:** Enabled Enables LLDP protocol. Note that LLDP is enabled on a port when LLDP is enabled globally and along with enabling per port setting in Port LLDP Parameters menu.
Tx Interval	**Synopsis:** 5 to 32768 s **Default:** 30 s The interval at which LLDP frames are transmitted on behalf of this LLDP agent.
Tx Hold	**Synopsis:** 2 to 10 **Default:** 4 The multiplier of the Tx Interval parameter that determines the actual time-to-live (TTL) value used in a LLDPDU. The actual TTL value can be expressed by the following formula: `TTL = MIN(65535, (Tx Interval * Tx Hold))`
Reinit Delay	**Synopsis:** 1 to 10 s **Default:** 2 s The delay in seconds from when the value of Admin Status parameter of a particular port becomes 'Disbled' until re-initialization will be lattempted.
Tx Delay	**Synopsis:** 1 to 8192 s **Default:** 2 s The delay in seconds between successive LLDP frame transmissions initiated by value or status changed. The recommended value is set by the following formula: `1 <= txDelay <= (0.25 * Tx Interval)`

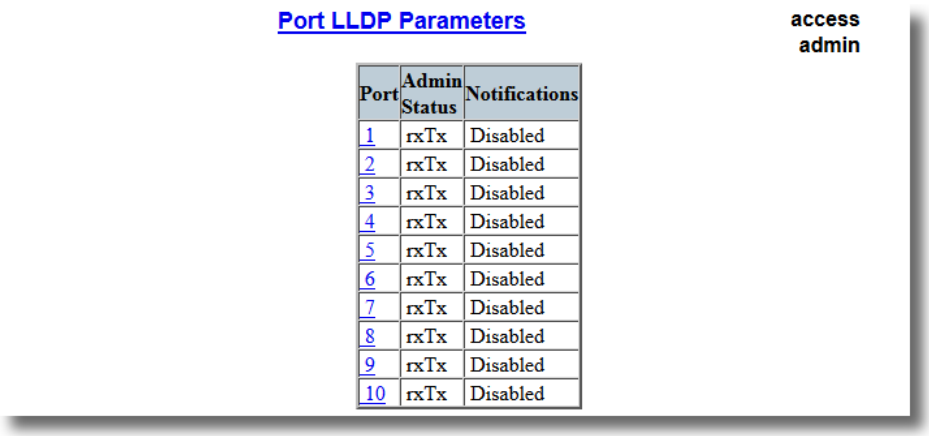
3. Click **Apply**.

Section 5.7.3

Configuring LLDP for an Ethernet Port

To configure LLDP for a specific Ethernet Port, do the following:

1. Navigate to ***Network Discovery » Link Layer Discovery Protocol » Configure Port LLDP Parameters*** . The **Port LLDP Parameters** table appears.



Port	Admin Status	Notifications
1	rxTx	Disabled
2	rxTx	Disabled
3	rxTx	Disabled
4	rxTx	Disabled
5	rxTx	Disabled
6	rxTx	Disabled
7	rxTx	Disabled
8	rxTx	Disabled
9	rxTx	Disabled
10	rxTx	Disabled

Figure 144: Port LLDP Parameters Table

2. Select a port. The **Port LLDP Parameters** form appears.

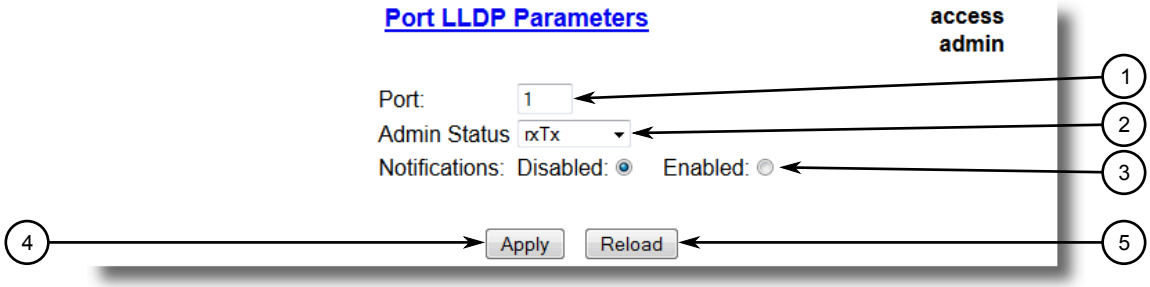


Figure 145: Port LLDP Parameters Form

1. Port Box **2.** Admin Status List **3.** Notifications Options **4.** Apply Button **5.** Reload Button

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

Parameter	Description
Port	**Synopsis:** 1 to maximum port number **Default:** 1 The port number as seen on the front plate silkscreen of the switch.
Admin Status	**Synopsis:** { rxTx, txOnly, rxOnly, Disabled } **Default:** rxTx

Parameter	Description
	rxTx: the local LLDP agent can both transmit and receive LLDP frames through the port. txOnly: the local LLDP agent can only transmit LLDP frames. rxOnly: the local LLDP agent can only receive LLDP frames. disabled: the local LLDP agent can neither transmit or receive LLDP frames.
Notifications	**Synopsis:** { Disabled, Enabled } **Default:** Disabled Disabling notifications will prevent sending notifications and generating alarms for particular port from the LLDP agent.

4. Click **Apply**.

Section 5.7.4

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 on all devices when Explorer is shut down. If RUGGEDCOM Explorer is unable to disable RCDP on a device, RUGGEDCOM ROS will automatically disable RCDP after approximately one hour of inactivity.

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.

Figure 146: RCDP Parameters Form

1. RCDP Discovery Options **2.** Apply Button **3.** Reload Button

2. Select **Enabled** to enable RCDP, or select **Disabled** to disable RCDP.
3. Click **Apply**.

Section 5.7.5

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.

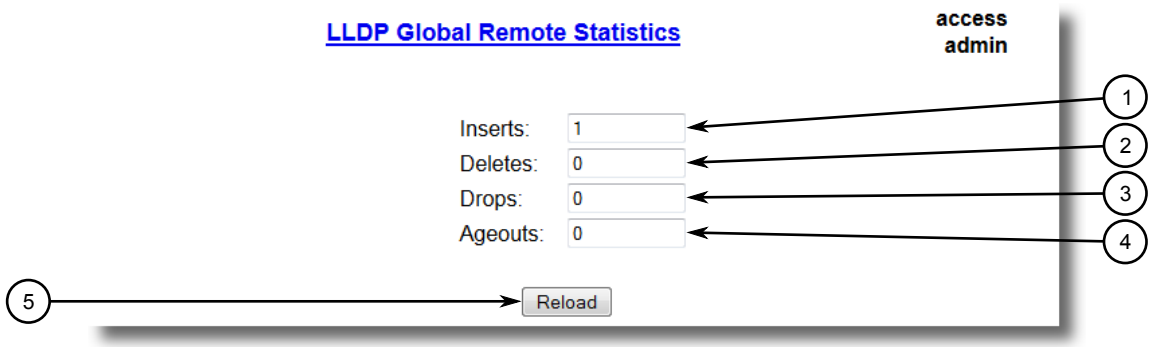


Figure 147: LLDP Global Remote Statistics Form

1. Inserts Box **2.** Deletes Box **3.** Drops Box **4.** Ageouts Box **5.** Reload Button

This form displays the following information:

Parameter	Description
Inserts	**Synopsis:** 0 to 4294967295 A number of times the entry in LLDP Neighbor Information Table was inserted.
Deletes	**Synopsis:** 0 to 4294967295 A number of times the entry in LLDP Neighbor Information Table was deleted.
Drops	**Synopsis:** 0 to 4294967295

Parameter	Description
	A number of times an entry was deleted from LLDP Neighbor Information Table because the information timeliness interval has expired.
Ageouts	**Synopsis:** 0 to 4294967295 A counter of all TLVs discarded.

Section 5.7.6

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.

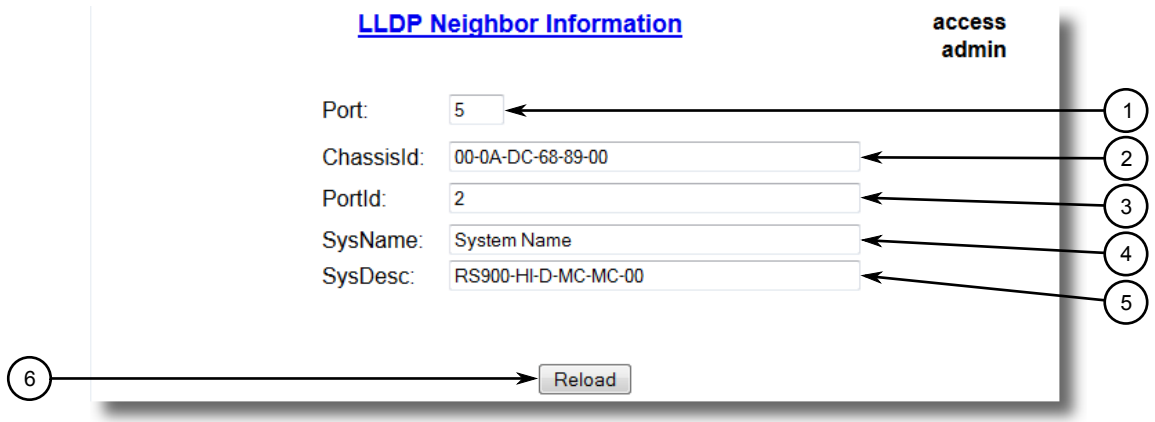


Figure 148: LLDP Neighbor Information Table

1. Port Box **2.** ChassisId Box **3.** PortId Box **4.** SysName Box **5.** SysDesc Box **6.** Reload Button

This form displays the following information:

Parameter	Description
Port	**Synopsis:** 1 to maximum port number The local port associated with this entry.
ChassisId	**Synopsis:** Any 45 characters Chassis Id information received from remote LLDP agent.
PortId	**Synopsis:** Any 45 characters Port Id information received from remote LLDP agent.
SysName	**Synopsis:** Any 45 characters System Name information received from remote LLDP agent.
SysDesc	**Synopsis:** Any 45 characters System Descriptor information received from remote LLDP agent.

Section 5.7.7

Viewing Statistics for LLDP Ports

To view statistics for LLDP ports, navigate to ***Network Discovery » Link Layer Discovery Protocol » View LLDP Statistics*** . The **LLDP Statistics** table appears.

LLDP Statistics

access admin

Port	FrmDrop	ErrFrm	FrmIn	FrmOut	Ageouts	TLVsDrop	TLVsUnknown
1	0	0	12274	2041	1	0	36822
2	0	0	2046	2041	1	0	0
3	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0
8	0	0	1435	1433	0	0	0
9	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0

Figure 149: LLDP Statistics Table

This table displays the following information:

Parameter	Description
Port	**Synopsis:** 1 to maximum port number The port number as seen on the front plate silkscreen of the switch.
FrmDrop	**Synopsis:** 0 to 4294967295 A counter of all LLDP frames discarded.
ErrFrm	**Synopsis:** 0 to 4294967295 A counter of all LLDPDUs received with detectable errors.
FrmIn	**Synopsis:** 0 to 4294967295 A counter of all LLDPDUs received.
FrmOut	**Synopsis:** 0 to 4294967295 A counter of all LLDPDUs transmitted.
Ageouts	**Synopsis:** 0 to 4294967295 A counter of the times that a neighbor's information has been deleted from the LLDP remote system MIB because the txinfoTTL timer has expired.
TLVsDrop	**Synopsis:** 0 to 4294967295 A counter of all TLVs discarded.
TLVsUnknown	**Synopsis:** 0 to 4294967295 A counter of all TLVs received on the port that are not recognized by the LLDP local agent.

Section 5.8

Managing Multicast Filtering

Multicast traffic can be filtered using IGMP (Internet Group Management Protocol) snooping or GMRP (GARP Multicast Registration Protocol).

CONTENTS

- Section 5.8.1, “Managing IGMP”
- Section 5.8.2, “Managing GMRP”

Section 5.8.1

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.

IMPORTANT!

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.

CONTENTS

- Section 5.8.1.1, “IGMP Concepts”
- Section 5.8.1.2, “Viewing a List of Multicast Group Memberships”
- Section 5.8.1.3, “Viewing Forwarding Information for Multicast Groups”
- Section 5.8.1.4, “Configuring IGMP”

Section 5.8.1.1

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.

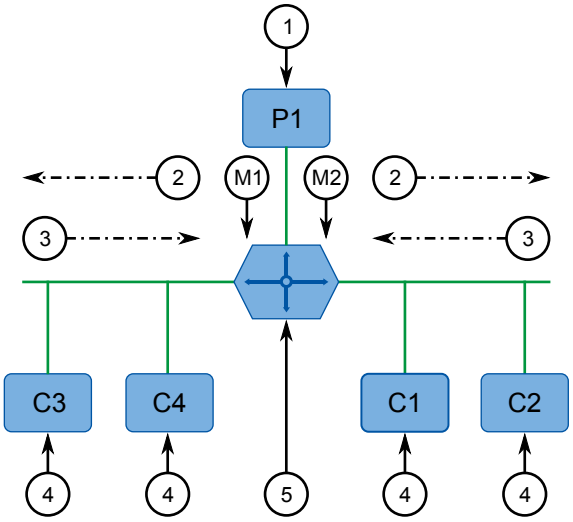


Figure 150: Example – IGMP In Operation

1. Producer **2.** Membership Queries **3.** Membership Reports **4.** Consumer **5.** Multicast Router

One *producer* IP host (P1) is generating two IP multicast streams, M1 and M2. There are four potential *consumers* of these streams, C1 through C4. The multicast router discovers which host wishes to subscribe to which stream by sending general membership queries to each segment.

In this example, the general membership query sent to the C1-C2 segment is answered by a membership report (or *join*) indicating the desire to subscribe to stream M2. The router will forward the M2 stream to the C1-C2 segment. In a similar fashion, the router discovers that it must forward stream M1 to segment C3-C4.

A *consumer* may join any number of multicast groups, issuing a membership report for each group. When a host issues a membership report, other hosts on the same network segment that also require membership to the same group suppress their own requests, since they would be redundant. In this way, the IGMP protocol guarantees the segment will issue only one membership report for each group.

The router periodically queries each of its segments in order to determine whether at least one consumer still subscribes to a given stream. If it receives no responses within a given time period (usually two query intervals), the router will prune the multicast stream from the given segment.

A more common method of pruning occurs when consumers wishing to unsubscribe issue an IGMP *leave group* message. The router will immediately issue a group-specific membership query to determine whether there are any remaining subscribers of that group on the segment. After the last consumer of a group has unsubscribed, the router will prune the multicast stream from the given segment.

Switch IGMP Operation

The IGMP Snooping feature provides a means for switches to snoop (i.e. watch) the operation of routers, respond with joins/leaves on the behalf of consumer ports, and prune multicast streams accordingly. There are two modes of IGMP the switch can be configured to assume: active and passive.

- **Active Mode**
  IGMP supports a *routerless* mode of operation.

  When such a switch is used without a multicast router, it is able to function as if it is a multicast router sending IGMP general queries.

- **Passive Mode**
  When such a switch is used in a network with a multicast router, it can be configured to run Passive IGMP. This mode prevents the switch from sending the queries that can confuse the router causing it to stop issuing IGMP queries.

> **NOTE**
> *A switch running in passive mode requires the presence of a multicast router or it will be unable to forward multicast streams at all if no multicast routers are present.*

> **NOTE**
> *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.

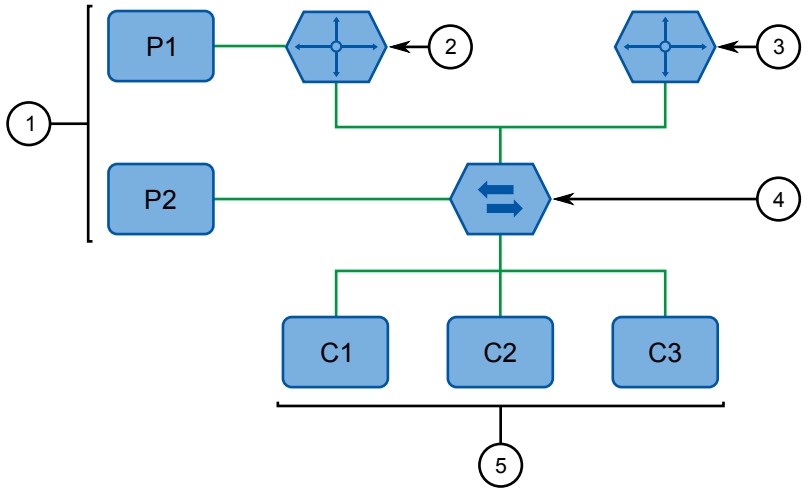


Figure 151: Example – Combined Router and Switch IGMP In Operation

1. Producer **2.** Multicast Router 1 **3.** Multicast Router 2 **4.** Switch **5.** Host

In this example:

- P1, Router 1, Router 2 and C3 are on VLAN 2
- P2 and C2 are on VLAN 3
- C1 is on both VLAN 2 and 3

Assuming that router 1 is the querier for VLAN 2 and router 2 is simply a non-querier, the switch will periodically receive queries from router 1 and maintain the information concerning which port links to the multicast router. However, the switch port that links to router 2 must be manually configured as a *router port*. Otherwise, the switch will send neither multicast streams nor joins/leaves to router 2.

Note that VLAN 3 does not have an external multicast router. The switch should be configured to operate in its *routerless* mode and issue general membership queries as if it is the router.

- **Processing Joins**
  If host C1 wants to subscribe to the multicast streams for both P1 and P2, it will generate two membership reports. The membership report from C1 on VLAN 2 will cause the switch to immediately initiate its own membership report to multicast router 1 (and to issue its own membership report as a response to queries).

The membership report from host C1 for VLAN 3 will cause the switch to immediately begin forwarding multicast traffic from producer P2 to host C2.

- **Processing Leaves**
  When host C1 decides to leave a multicast group, it will issue a leave request to the switch. The switch will poll the port to determine if host C1 is the last member of the group on that port. If host C1 is the last (or only) member, the group will immediately be pruned from the port.

  Should host C1 leave the multicast group without issuing a leave group message and then fail to respond to a general membership query, the switch will stop forwarding traffic after two queries.

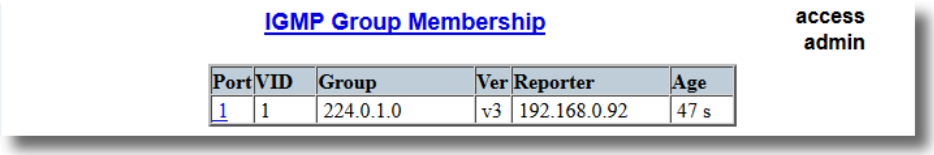
  When the last port in a multicast group leaves the group (or is aged-out), the switch will issue an IGMP leave report to the router.

Section 5.8.1.2

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.



Port	VID	Group	Ver	Reporter	Age
1	1	224.0.1.0	v3	192.168.0.92	47 s

Figure 152: IGMP Group Membership Table

This table provides the following information:

Parameter	Description
Port	**Synopsis:** 1 to maximum port number The port number as seen on the front plate silkscreen of the switch.
VID	**Synopsis:** 0 to 65535 VLAN Identifier of the VLAN upon which the multicast group operates.
Group	**Synopsis:** ###.###.###.### where ### ranges from 0 to 255 Multicast Group Address.
Ver	**Synopsis:** { v3, v2, v1 } Specifies the IGMP version of the learnt multicast group.
Reporter	**Synopsis:** ###.###.###.### where ### ranges from 0 to 255 Specifies the source IP address that is reporting subscription to the multicast group.
Age	**Synopsis:** 0 to 7210 s Specifies the current age of the IP multicast group learned on the port in seconds.

If the table is empty, do the following:

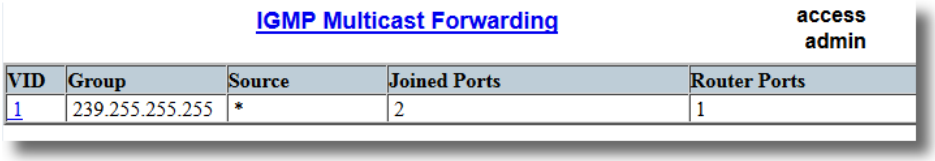
- Make sure traffic is being sent to the device.
- Make sure IGMP is properly configured on the device. For more information, refer to Section 5.8.1.4, "Configuring IGMP" .

Section 5.8.1.3

Viewing Forwarding Information for Multicast Groups

Multicast forwarding information for every source, group and VLAN combination learned by RUGGEDCOM ROS is recorded in the IGMP Multicast Forwarding table.

To view the IGMP Multicast Forwarding table, navigate to ***Multicast Filtering*** » ***View IGMP Multicast Forwarding*** . The **IGMP Multicast Forwarding** table appears.



IGMP Multicast Forwarding

access admin

VID	Group	Source	Joined Ports	Router Ports
1	239.255.255.255	*	2	1

Figure 153: IGMP Multicast Forwarding Table

This table provides the following information:

Parameter	Description
VID	**Synopsis:** 0 to 65535 VLAN Identifier of the VLAN upon which the multicast group operates.
Group	**Synopsis:** ###.###.###.### where ### ranges from 0 to 255 Multicast Group Address.
Source	**Synopsis:** ###.###.###.### where ### ranges from 0 to 255 or { * } Source Address. * means all possible source addresses.
Joined Ports	**Synopsis:** Comma-separated list of ports All ports that currently receive multicast traffic for the specified multicast group.
Router Ports	**Synopsis:** Comma-separated list of ports All ports that have been manually configured or dynamically discovered (by observing router specific traffic) as ports that link to multicast routers.

If the table is empty, do the following:

- Make sure traffic is being sent to the device.
- Make sure IGMP is properly configured on the device. For more information, refer to Section 5.8.1.4, "Configuring IGMP" .

Section 5.8.1.4

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 Section 5.1.5, "Managing Static VLANs" .
2. Navigate to ***Multicast Filtering*** » ***Configure IGMP Parameters*** . The **IGMP Parameters** form appears.

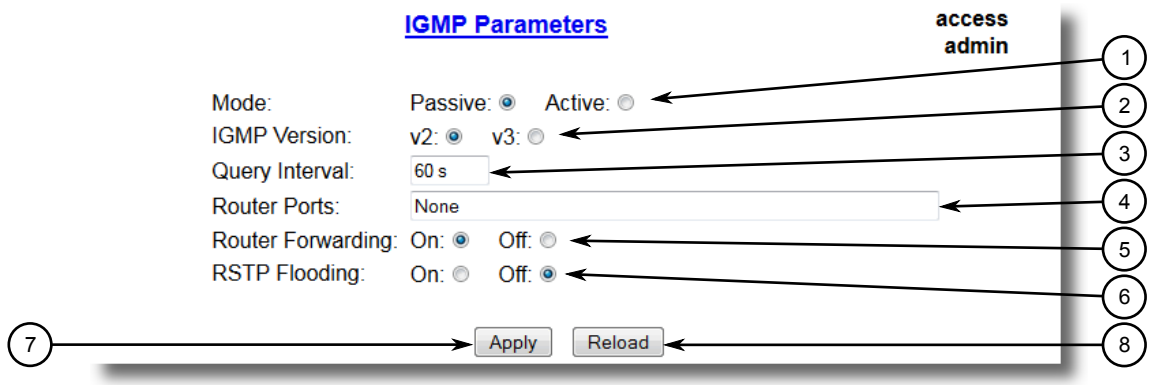


Figure 154: IGMP Parameters Form

1. Mode Options **2.** IGMP Version **3.** Query Interval Box **4.** Router Ports Box **5.** Router Forwarding Options **6.** RSTP Flooding Options **7.** Apply Button **8.** Reload Button

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

Parameter	Description
Mode	**Synopsis:** { Passive, Active } **Default:** Passive Specifies the IGMP mode. Options include: • `PASSIVE` – the switch passively snoops IGMP traffic and never sends IGMP queries • `ACTIVE` – the switch generates IGMP queries, if no queries from a better candidate for being the querier are detected for a while.
IGMP Version	**Synopsis:** { v2, v3 } **Default:** v2 Specifies the configured IGMP version on the switch. Options include: • `v2` – Sets the IGMP version to version 2. When selected for a snooping switch, all IGMP reports and queries greater than v2 are forwarded, but not added to the IGMP Multicast Forwarding table. • `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:** 10 to 3600 **Default:** 60 s The time interval between IGMP queries generated by the switch.

Parameter	Description
	NOTE *This parameter also affects the Group Membership Interval (i.e. the group subscriber aging time), therefore, it takes effect even in PASSIVE mode.*
Router Ports	**Synopsis:** Comma-separated list of ports **Default:** None This parameter specifies ports that connect to multicast routers. If you do not configure known router ports, the switch may be able to detect them, however it is advisable to pre-configure them.
Router Forwarding	**Synopsis:** { Off, On } **Default:** On This parameter specifies whether multicast streams will be always forwarded to multicast routers.
RSTP Flooding	**Synopsis:** { Off, On } **Default:** Off This parameter specifies whether multicast streams will be flooded out of all RSTP non-edge ports upon topology change detection. Such flooding is desirable, if guaranteed multicast stream delivery after topology change is most important.

4. Click **Apply**.

Section 5.8.2

Managing GMRP

The GMRP is an application of the Generic Attribute Registration Protocol (GARP) that provides a Layer 2 mechanism for managing multicast group memberships in a bridged Layer 2 network. It allows Ethernet switches and end stations to register and unregister membership in multicast groups with other switches on a LAN, and for that information to be disseminated to all switches in the LAN that support Extended Filtering Services.

GMRP is an industry-standard protocol first defined in IEEE 802.1D-1998 and extended in IEEE 802.1Q-2005. GARP was defined in IEEE 802.1D-1998 and updated in 802.1D-2004.

NOTE
GMRP provides similar functionality at Layer 2 to what IGMP provides at Layer 3.

CONTENTS

- Section 5.8.2.1, “GMRP Concepts”
- Section 5.8.2.2, “Viewing a Summary of Multicast Groups”
- Section 5.8.2.3, “Configuring GMRP Globally”
- Section 5.8.2.4, “Configuring GMRP for Specific Ethernet Ports”
- Section 5.8.2.5, “Viewing a List of Static Multicast Groups”
- Section 5.8.2.6, “Adding a Static Multicast Group”

- Section 5.8.2.7, “Deleting a Static Multicast Group”

Section 5.8.2.1

GMRP Concepts

The following describes some of the concepts important to the implementation of multicast filtering using GMRP:

Joining a Multicast Group

In order to join a multicast group, an end station transmits a GMRP *join* message. The switch that receives the *join* message adds the port through which the message was received to the multicast group specified in the message. It then propagates the *join* message to all other hosts in the VLAN, one of which is expected to be the multicast source.

When a switch transmits GMRP updates (from GMRP-enabled ports), all of the multicast groups known to the switch, whether configured manually or learned dynamically through GMRP, are advertised to the rest of network.

As long as one host on the Layer 2 network has registered for a given multicast group, traffic from the corresponding multicast source will be carried on the network. Traffic multicast by the source is only forwarded by each switch in the network to those ports from which it has received join messages for the multicast group.

Leaving a Multicast Group

Periodically, the switch sends GMRP queries in the form of a *leave all* message. If a host (either a switch or an end station) wishes to remain in a multicast group, it reasserts its group membership by responding with an appropriate *join* request. Otherwise, it can either respond with a *leave* message or simply not respond at all. If the switch receives a *leave* message or receives no response from the host for a timeout period, the switch removes the host from the multicast group.

Notes About GMRP

Since GMRP is an application of GARP, transactions take place using the GARP protocol. GMRP defines the following two Attribute Types:

- The Group Attribute Type, used to identify the values of group MAC addresses
- The Service Requirement Attribute Type, used to identify service requirements for the group

Service Requirement Attributes are used to change the receiving port's multicast filtering behavior to one of the following:

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

If GMRP is disabled on the RS900, GMRP packets received will be forwarded like any other traffic. Otherwise, GMRP packets will be processed by the RS900, 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.

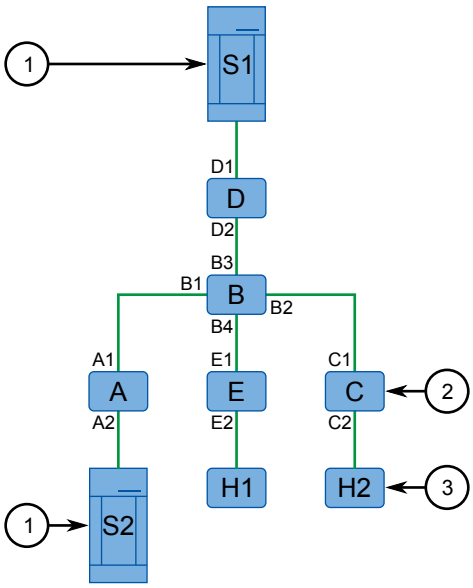


Figure 155: Example – Establishing Membership with GMRP

1. Multicast Source **2.** Switch **3.** Multicast Host

The hosts and switches establish membership with the Multicast Group 1 and 2 as follows:

1. Host H1 is GMRP unaware, but needs to see traffic for Multicast Group 1. Therefore, Port E2 on Switch E is statically configured to forward traffic for Multicast Group 1.
2. Switch E advertises membership in Multicast Group 1 to the network through Port E1, making Port B4 on Switch B a member of Multicast Group 1.
3. Switch B propagates the *join* message, causing Ports A1, C1 and D1 to become members of Multicast Group 1.
4. Host H2 is GMRP-aware and sends a *join* request for Multicast Group 2 to Port C2, which thereby becomes a member of Multicast Group 2.
5. Switch C propagates the *join* message, causing Ports A1, B2, D1 and E1 to become members of Multicast Group 2.

Once GMRP-based registration has propagated through the network, multicast traffic from S1 and S2 can reach its destination as follows:

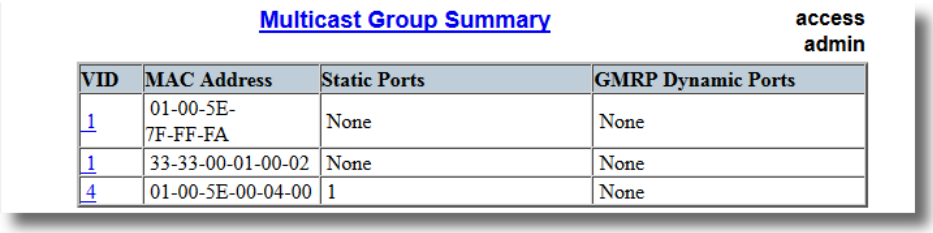
- Source S1 transmits multicast traffic to Port D2 which is forwarded via Port D1, which has previously become a member of Multicast Group 1.
- Switch B forwards the Group 1 multicast via Port B4 towards Switch E.
- Switch E forwards the Group 1 multicast via Port E2, which has been statically configured for membership in Multicast Group 1.
- Host H1, connected to Port E2, thus receives the Group 1 multicast.
- Source S2 transmits multicast traffic to Port A2, which is then forwarded via port A1, which has previously become a member of Multicast Group 2.
- Switch B forwards the Group 2 multicast via Port B2 towards Switch C.

- Switch C forwards the Group 2 multicast via Port C2, which has previously become a member of Group 2.
- Ultimately, Host H2, connected to Port C2, receives the Group 2 multicast.

Section 5.8.2.2

Viewing a Summary of Multicast Groups

To view a summary of all multicast groups, navigate to ***Multicast Filtering » View Multicast Group Summary*** . The **Multicast Group Summary** table appears.



Multicast Group Summary

access admin

VID	MAC Address	Static Ports	GMRP Dynamic Ports
1	01-00-5E-7F-FF-FA	None	None
1	33-33-00-01-00-02	None	None
4	01-00-5E-00-04-00	1	None

Figure 156: Multicast Group Summary Table

This table provides the following information:

Parameter	Description
VID	**Synopsis:** 0 to 65535 VLAN Identifier of the VLAN upon which the multicast group operates.
MAC Address	**Synopsis:** ##-##-##-##-##-## where ## ranges 0 to FF Multicast group MAC address.
Static Ports	**Synopsis:** Any combination of numbers valid for this parameter Ports that joined this group statically through static configuration in Static MAC Table and to which the multicast group traffic is forwarded.
GMRP Dynamic Ports	**Synopsis:** Any combination of numbers valid for this parameter Ports that joined this group dynamically through GMRP Application and to which the multicast group traffic is forwarded.

Section 5.8.2.3

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.

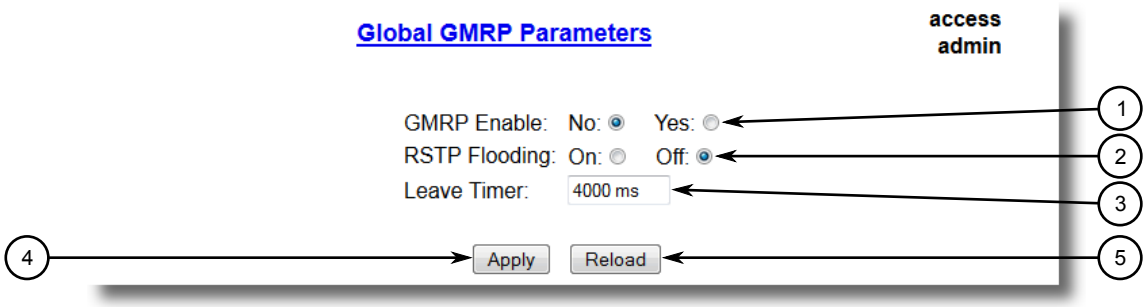


Figure 157: Global GMRP Parameters Form

1. GMRP Enable Options **2.** RSTP Flooding Options **3.** Leave Timer Box **4.** Apply Button **5.** Reload Button

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

Parameter	Description
GMRP Enable	**Synopsis:** { No, Yes } **Default:** No Globally enable or disable GMRP. When GMRP is globally disabled, GMRP configurations on individual ports are ignored. When GMRP is globally enabled, each port can be individually configured.
RSTP Flooding	**Synopsis:** { On, Off } **Default:** Off This parameter specifies whether multicast streams will be flooded out of all RSTP non-edge ports upon topology change detection. Such flooding is desirable, if guaranteed multicast stream delivery after topology change is most important.
Leave Timer	**Synopsis:** 600 to 300000 ms **Default:** 4000 ms 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**.

Section 5.8.2.4

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 Section 5.8.2.3, "Configuring GMRP Globally" .
2. Navigate to ***Multicast Filtering » Configure Port GMRP Parameters*** . The **Port GMRP Parameters** table appears.

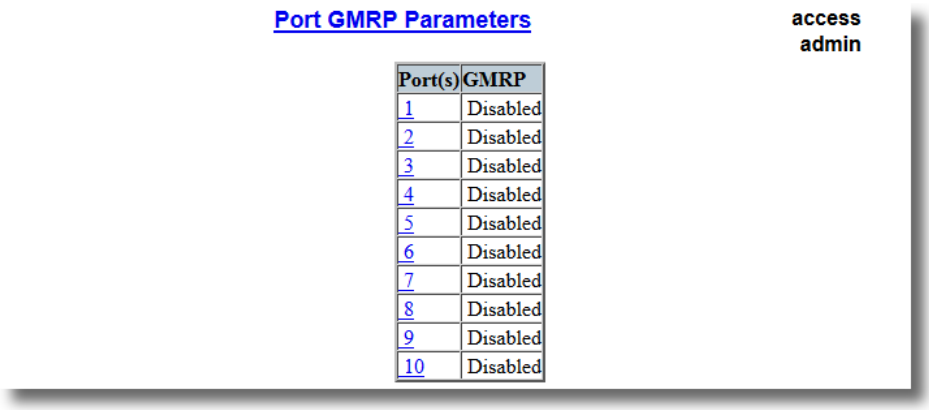


Figure 158: Port GMRP Parameters Table

3. Select an Ethernet port. The **Port GMRP Parameters** form appears.

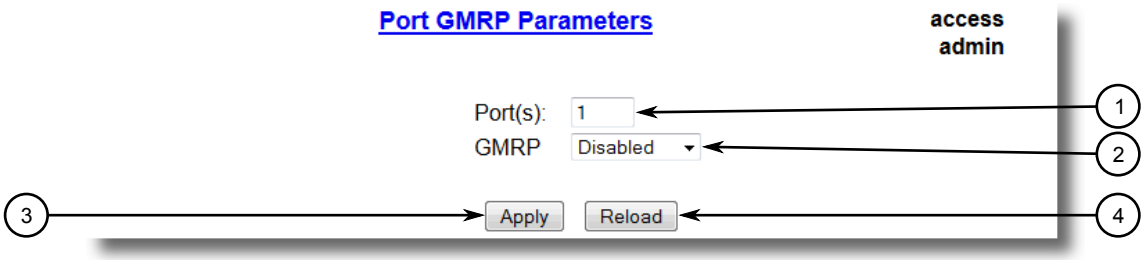


Figure 159: Port GMRP Parameters Form

1. Port(s) Box **2.** GMRP List **3.** Apply Button **4.** Reload Button

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

Parameter	Description
Port(s)	**Synopsis:** Any combination of numbers valid for this parameter The port number as seen on the front plate silkscreen of the switch (or a list of ports, if aggregated in a port trunk).
GMRP	**Synopsis:** { Disabled, Adv Only, Adv&Learn } **Default:** Default: Disabled Configures GMRP (GARP Multicast Registration Protocol) operation on the port. There are several GMRP operation modes: • DISABLED - the port is not capable of any GMRP processing. • ADVERTISE ONLY - the port will declare all MCAST addresses existing in the switch (configured or learned) but will not learn any MCAST addresses. • ADVERTISE & LEARN - the port will declare all MCAST Addresses existing in the switch (configured or learned) and can dynamically learn MCAST addresses.

5. Click **Apply**.

Section 5.8.2.5

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.

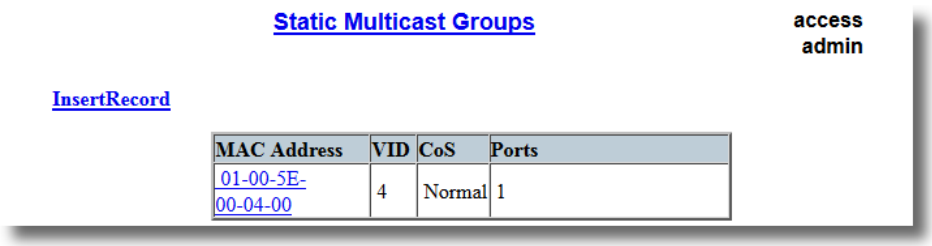


Figure 160: Static Multicast Groups Table

If a static multicast group is not listed, add the group. For more information, refer to Section 5.8.2.6, "Adding a Static Multicast Group" .

Section 5.8.2.6

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.

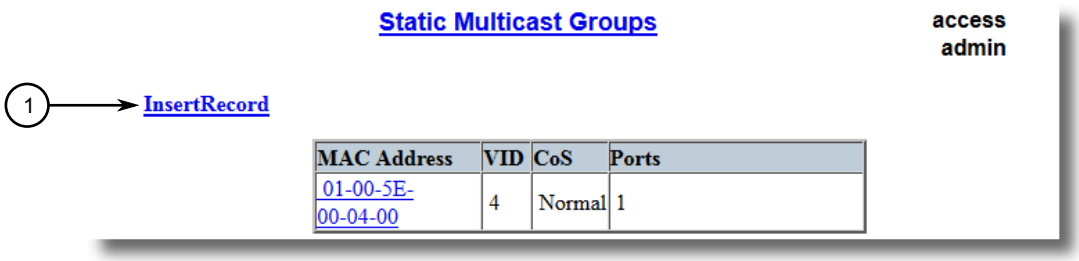


Figure 161: Static Multicast Groups Table

1. InsertRecord

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

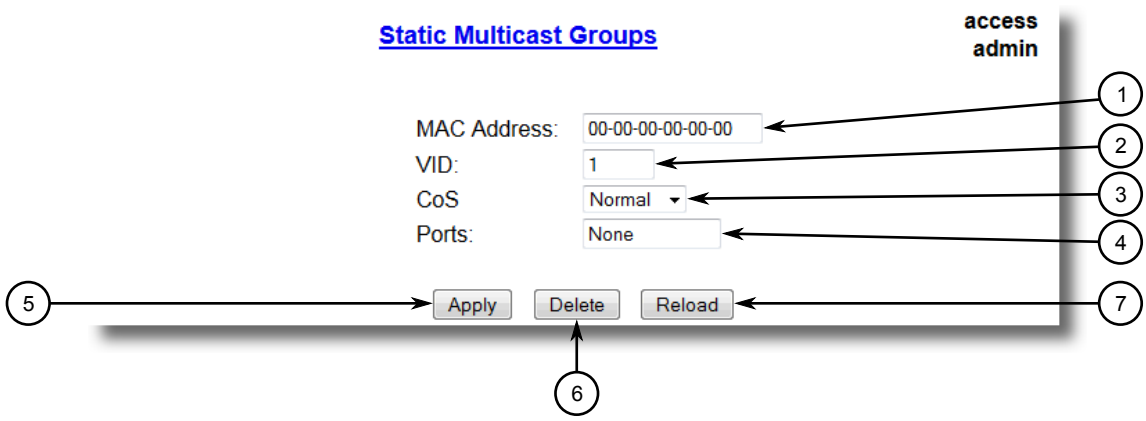


Figure 162: Static Multicast Groups Form

1. MAC Address Box **2.** VID Box **3.** CoS List **4.** Ports Box **5.** Apply Button **6.** Delete Button **7.** Reload Button

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

Parameter	Description
MAC Address	**Synopsis:** ##-##-##-##-##-## where ## ranges 0 to FF **Default:** 00-00-00-00-00-00 Multicast group MAC address.
VID	**Synopsis:** 1 to 4094 **Default:** 1 VLAN Identifier of the VLAN upon which the multicast group operates.
CoS	**Synopsis:** { N/A, Normal, Medium, High, Crit } **Default:** N/A Prioritizes traffic for the specified MAC address. To not prioritize traffic based on the address, select N/A.
Ports	**Synopsis:** Any combination of numbers valid for this parameter **Default:** None Ports to which the multicast group traffic is forwarded.

4. Click **Apply**.

Section 5.8.2.7

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.

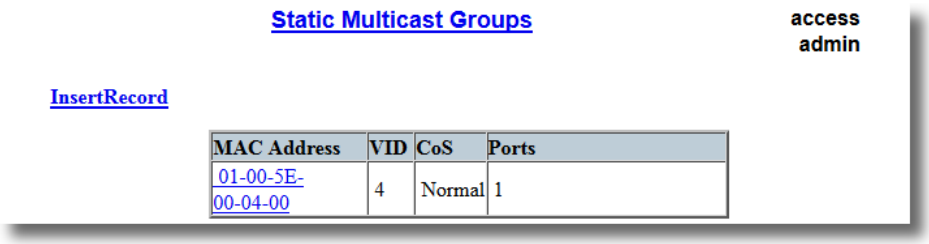


Figure 163: Static Multicast Groups Table

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

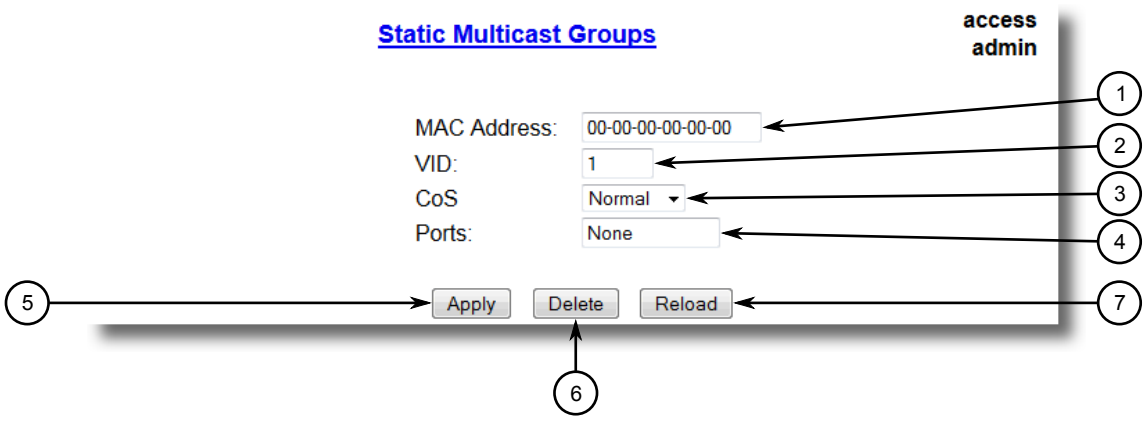


Figure 164: Static Multicast Groups Form

1. MAC Address Box **2.** VID Box **3.** Priority Box **4.** Ports Box **5.** Apply Button **6.** Delete Button **7.** Reload Button

3. Click **Delete**.

Section 5.9

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.

CONTENTS

- Section 5.9.1, “Port Security Concepts”
- Section 5.9.2, “Viewing a List of Authorized MAC Addresses”
- Section 5.9.3, “Configuring Port Security”

- Section 5.9.4, “Configuring IEEE 802.1X”

Section 5.9.1

Port Security Concepts

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

CONTENTS

- Section 5.9.1.1, “Static MAC Address-Based Authentication”
- Section 5.9.1.2, “IEEE 802.1x Authentication”
- Section 5.9.1.3, “IEEE 802.1X Authentication with MAC Address-Based Authentication”
- Section 5.9.1.4, “Assigning VLANS with Tunnel Attributes”

Section 5.9.1.1

Static MAC Address-Based Authentication

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

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

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

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

Section 5.9.1.2

IEEE 802.1x Authentication

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

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

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

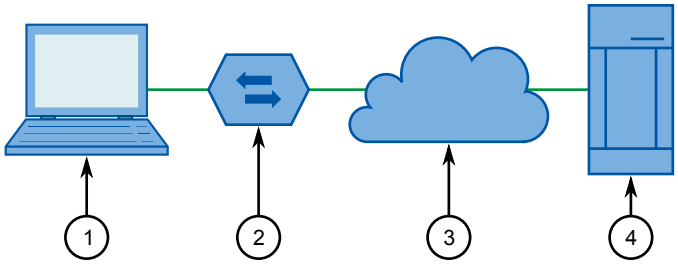


Figure 165: IEEE 802.1x General Topology

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

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

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

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

NOTE
The switch supports authentication of one host per port.

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

Section 5.9.1.3

IEEE 802.1X Authentication with MAC Address-Based Authentication

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

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

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

Section 5.9.1.4

Assigning VLANS with Tunnel Attributes

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

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

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

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

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

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

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

Section 5.9.2

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.*

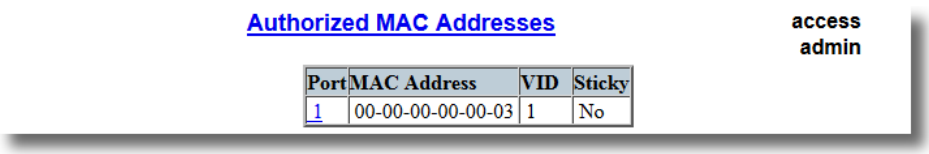


Figure 166: Authorized MAC Addresses Table

This table displays the following information:

Parameter	Description
Port	**Synopsis:** 1 to maximum port number Port on which MAC address has been learned.

Parameter	Description
MAC Address	**Synopsis:** ##-##-##-##-##-## where ## ranges 0 to FF Authorized MAC address learned by the switch.
VID	**Synopsis:** 0 to 65535 VLAN Identifier of the VLAN upon which the MAC address operates.
Sticky	**Synopsis:** { No, Yes } This describes whether the authorized MAC address/Device can move to another port or not: • YES - authorized MAC address/Device cannot move to a different switch port • NO - authorized MAC address/Device may move to another switch port

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

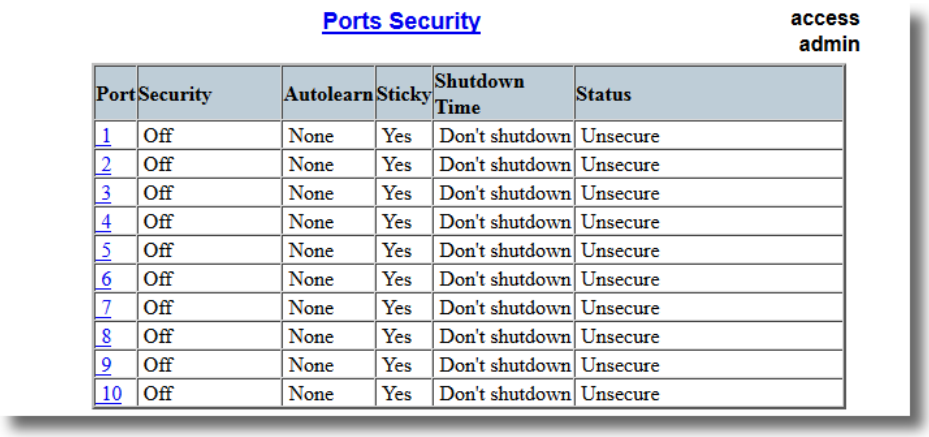
- Configure port security. For more information, refer to Section 5.9.3, "Configuring Port Security" .
- Configure IEEE 802.1X. For more information, refer to Section 5.9.4, "Configuring IEEE 802.1X" .

Section 5.9.3

Configuring Port Security

To configure port security, do the following:

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



Ports Security

access admin

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

Figure 167: Ports Security Table

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

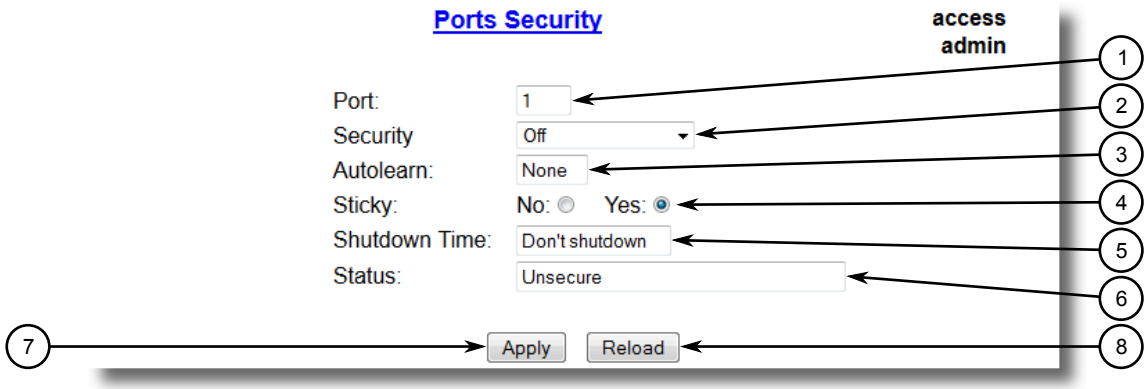


Figure 168: Ports Security Form

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

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

Parameter	Description
Port	**Synopsis:** 1 to maximum port number **Default:** 1 The port number as seen on the front plate silkscreen of the switch.
Security	**Synopsis:** { Off, Static MAC, 802.1X, 802.1x/MAC-Auth } **Default:** Off Enables or disables the port's security feature. Two types of port access control are available: • Static MAC address-based. With this method, authorized MAC address(es) should be configured in the Static MAC Address table. If some MAC addresses are not known in advance (or it is not known to which port they will be connected), there is still an option to configure the switch to auto-learn certain number of MAC addresses. Once learned, they do not age out until the unit is reset or the link goes down. • IEEE 802.1X standard authentication. • IEEE 802.1X with MAC-Authentication, also known as MAC-Authentication Bypass. With this option, the device can authenticate clients based on the client's MAC address if IEEE 802.1X authentication times out.
Autolearn	**Synopsis:** 1 to 16 or { None } **Default:** None Only applicable when the 'Security' field has been set to 'Static MAC'. It specifies maximum number of MAC addresses that can be dynamically learned on the port. If there are static addresses configured on the port, the actual number of addresses allowed to be learned is this number minus the number of the static MAC addresses.
Sticky	**Synopsis:** { No, Yes } **Default:** Yes

Parameter	Description
	Only applicable when the 'Security' field has been set to 'Static MAC'. Change the behaviour of the port to either sticky or non-sticky. If Sticky is 'Yes', MACs/Devices authorized on the port 'stick' to the port and the switch will not allow them to move to a different port. If Sticky is 'No', MACs/Devices authorized on the port may move to another port.
Shutdown Time	**Synopsis:** 1 to 86400 s or { Until reset, Don't shutdown } **Default:** Don't shutdown Specifies for how long to shut down the port, if a security violation occurs.
Status	**Synopsis:** Any 31 characters 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**.

Section 5.9.4

Configuring IEEE 802.1X

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

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

802.1X Parameters access admin

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

Figure 169: 802.1X Parameters Table

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

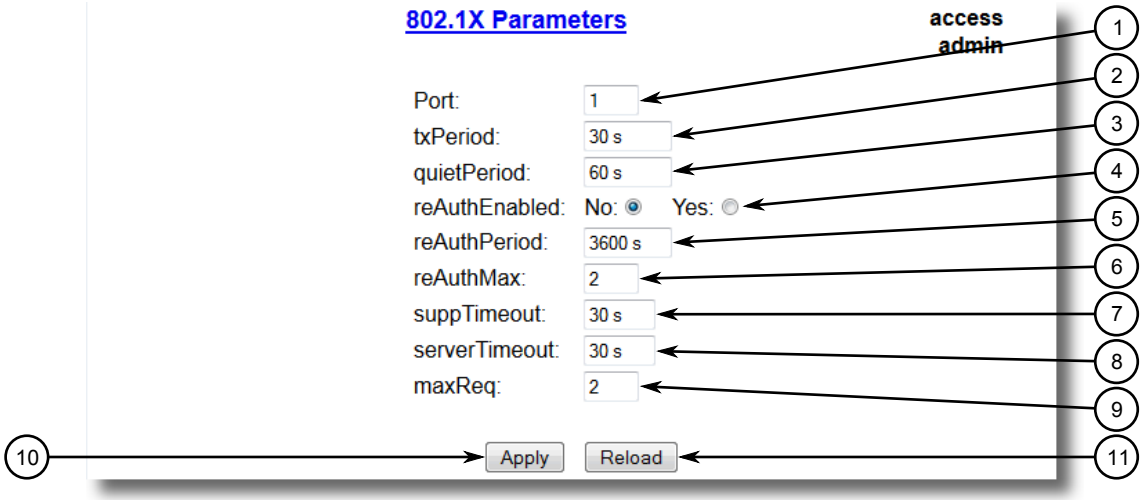


Figure 170: 802.1X Parameters Form

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

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

Parameter	Description
Port	**Synopsis:** 1 to maximum port number **Default:** 1 The port number as seen on the front plate silkscreen of the switch.
txPeriod	**Synopsis:** 1 to 65535 **Default:** 30 s The time to wait for the Supplicant's EAP Response/Identity packet before retransmitting an EAP Request/Identity packet.

Parameter	Description
quietPeriod	**Synopsis:** 0 to 65535 **Default:** 60 s The period of time not to attempt to acquire a Supplicant after the authorization session failed.
reAuthEnabled	**Synopsis:** { No, Yes } **Default:** No Enables or disables periodic re-authentication.
reAuthPeriod	**Synopsis:** 60 to 86400 **Default:** 3600 s The time between periodic re-authentication of the Supplicant.
reAuthMax	**Synopsis:** 1 to 10 **Default:** 2 The number of re-authentication attempts that are permitted before the port becomes unauthorized.
suppTimeout	**Synopsis:** 1 to 300 **Default:** 30 s The time to wait for the Supplicant's response to the authentication server's EAP packet.
serverTimeout	**Synopsis:** 1 to 300 **Default:** 30 s The time to wait for the authentication server's response to the Supplicant's EAP packet.
maxReq	**Synopsis:** 1 to 10 **Default:** 2 The maximum number of times to retransmit the authentication server's EAP Request packet to the Supplicant before the authentication session times out.

4. Click **Apply**.

Section 5.10

Managing Link Aggregation

Link aggregation, also referred to as port trunking or port bundling, provides the ability to aggregate or gather several Ethernet ports into one logical link (port trunk) with higher bandwidth. This allows for highly randomized load balancing between the aggregated links based on both the source and destination MAC addresses of the forwarded frames.

Link Aggregation can be used for two purposes:

- To obtain increased, linearly incremental link bandwidth.
- To improve network reliability by creating link redundancy. If one of the aggregated links fails, the switch will balance the traffic between the remaining links.

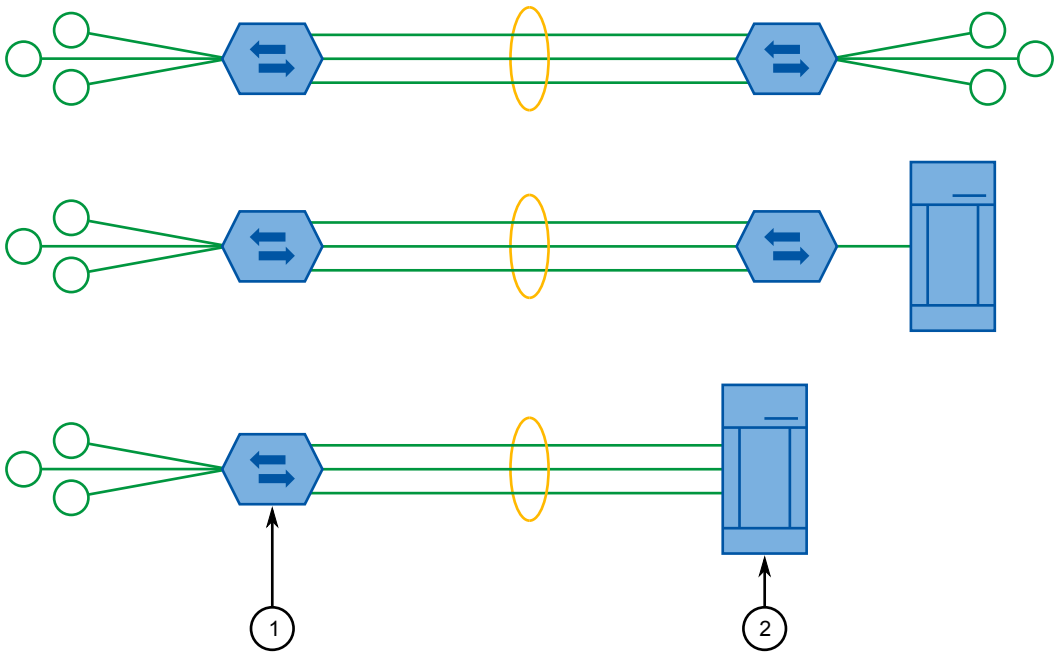


Figure 171: Examples of Link Aggregation

1. Switch **2.** Server

RUGGEDCOM ROS allows up to 15 port trunks to be configured on a single device, with each consisting of up to 8 ports.

NOTE
The maximum number of port trunks for each device depends on the number of ports available. At least two ports are required to configure a port trunk.

NOTE
The aggregated port with the lowest port number is called the Port Trunk Primary Port. Other ports in the trunk are called Secondary Ports.

CONTENTS

- Section 5.10.1, “Link Aggregation Concepts”
- Section 5.10.2, “Managing Port Trunks”

Section 5.10.1

Link Aggregation Concepts

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

CONTENTS

- Section 5.10.1.1, “Rules and Limitations”

- Section 5.10.1.2, "Link Aggregation and Layer 2 Features"
- Section 5.10.1.3, "Link Aggregation and Physical Layer Features"

Section 5.10.1.1

Rules and Limitations

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

- Each port can belong to only one port trunk at a time.
- A port mirroring target port can not be member of a port trunk. However, a port mirroring source port can be member of a port trunk.
- If only one QinQ port is supported by the switch, the port working in QinQ mode cannot be a secondary member of a port trunk.
- DHCP Relay Agent Client port cannot be a member of a port trunk.
- Load balancing between the links of a bundle is randomized and may not be ideal. For instance, if three 100 Mbs links are aggregated, the resulting bandwidth of the port trunk may not be precisely 300 Mbs.
- A Static MAC Address should not be configured to reside on an aggregated port – it may cause some frames destined for that address to be dropped.
- A secure port cannot be a member of a port trunk.
- The IEEE 802.3ad Link Aggregation standard requires all physical links in the port trunk to run at the same speed and in full-duplex mode. If this requirement is violated, the performance of the port trunk will drop.

  The switch will raise an appropriate alarm, if such a speed/duplex mismatch is detected.
- STP dynamically calculates the path cost of the port trunk based on its aggregated bandwidth. However, if the aggregated ports are running at different speeds, the path cost may not be calculated correctly.
- Enabling STP is the best way for handling link redundancy in switch-to-switch connections composed of more than one physical link. If STP is enabled and increased bandwidth is not required, Link Aggregation should not be used because it may lead to a longer fail-over time.

Section 5.10.1.2

Link Aggregation and Layer 2 Features

Layer 2 features (e.g. STP, VLAN, CoS, Multicast Filtering) treat a port trunk as a single link.

- If the Spanning Tree Protocol (STP) puts an aggregated port in blocking/forwarding, it does it for the whole port trunk.
- If one of the aggregated ports joins/leaves a multicast group (e.g. via IGMP or GMRP), all other ports in the trunk will join/leave too.
- Any port configuration parameter (e.g. VLAN, CoS) change will be automatically applied to all ports in the trunk.
- Configuration/status parameters of the secondary ports will not be shown and their port numbers will be simply listed next to the primary port number in the appropriate configuration/status UI sessions.
- When a secondary port is added to a port trunk, it inherits all the configuration settings of the primary port. When this secondary port is removed from the port trunk, the settings it had previous to the aggregation are restored.

Section 5.10.1.3

Link Aggregation and Physical Layer Features

Physical layer features (e.g. physical link configuration, link status, rate limiting, Ethernet statistics) will still treat each aggregated port separately.

- Physical configuration/status parameters will NOT be automatically applied to other ports in the trunk and will be displayed for each port as usual.
- Make sure that only ports with the same speed and duplex settings are aggregated. If auto-negotiation is used, make sure it is resolved to the same speed for all ports in the port trunk.
- To get a value of an Ethernet statistics counter for the port trunk, add the values of the counters for all ports in the port trunk.

Section 5.10.2

Managing Port Trunks

The following section describes how to configure and manage port trunks.

CONTENTS

- Section 5.10.2.1, "Viewing a List of Port Trunks"
- Section 5.10.2.2, "Adding a Port Trunk"
- Section 5.10.2.3, "Deleting a Port Trunk"

Section 5.10.2.1

Viewing a List of Port Trunks

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

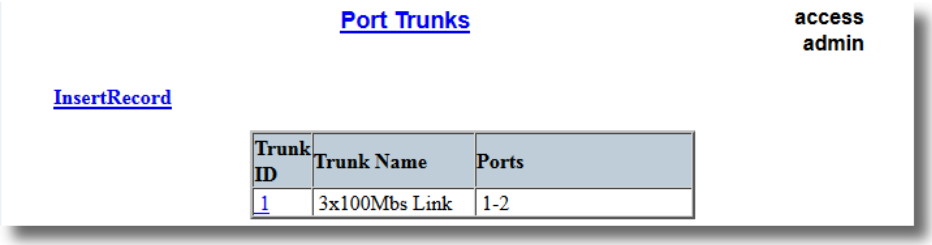


Figure 172: Port Trunks Table

If port trunks have not been configured, add trunks as needed. For more information, refer to Section 5.10.2.2, "Adding a Port Trunk" .

Section 5.10.2.2

Adding a Port Trunk

To add a port trunk, do the following:

IMPORTANT!
The port trunk must be properly configured on both sides of the aggregated link. In switch-to-switch connections, if the configuration of both sides does not match (i.e. some ports are mistakenly not included in the port trunk), it will result in a loop. Therefore, the following procedure is strongly recommended to configure a port trunk:

a. Disconnect or disable all the ports involved in the configuration, i.e. either being added to or removed from the port trunk.

b. Configure the port trunk on both switches.

c. Double-check the port trunk configuration on both switches.

d. Reconnect or re-enable the ports.

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

1. Navigate to ***Link Aggregation*** » ***Configure Port Trunks*** . The **Port Trunks** table appears.

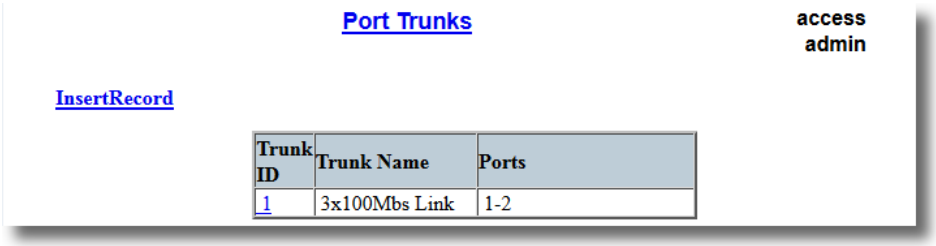


Figure 173: Port Trunks Table

1. InsertRecord

2. Click **InsertRecord**. The **Port Trunks** form appears.

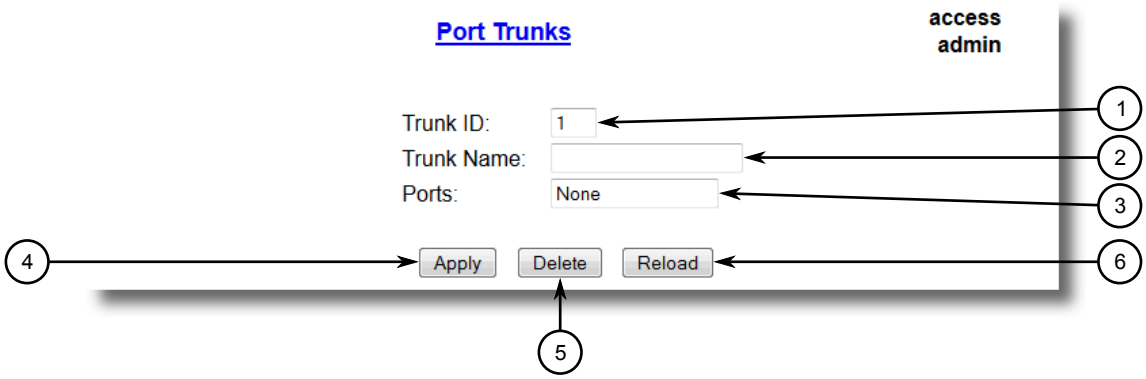


Figure 174: Port Trunks

1. Trunk ID Box **2.** Trunk Name Box **3.** Ports Box **4.** Apply Button **5.** Delete Button **6.** Reload Button

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

Parameter	Description
Trunk ID	**Synopsis:** 1 to 2 **Default:** 1 Trunk number. It doesn't affect port trunk operation in any way and is only used for identification.
Trunk Name	**Synopsis:** Any 19 characters Provides a description of the aggregated link purpose.
Ports	**Synopsis:** Any combination of numbers valid for this parameter **Default:** None List of ports aggregated in the trunk.

4. Click **Apply**.

Section 5.10.2.3

Deleting a Port Trunk

To delete a port trunk, do the following:

1. Navigate to ***Link Aggregation*** » ***Configure Port Trunks*** . The **Port Trunks** table appears.

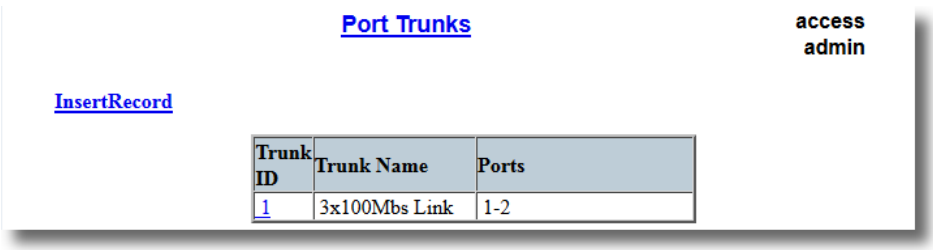


Figure 175: Port Trunks Table

2. Select the port trunk from the table. The **Port Trunks** form appears.

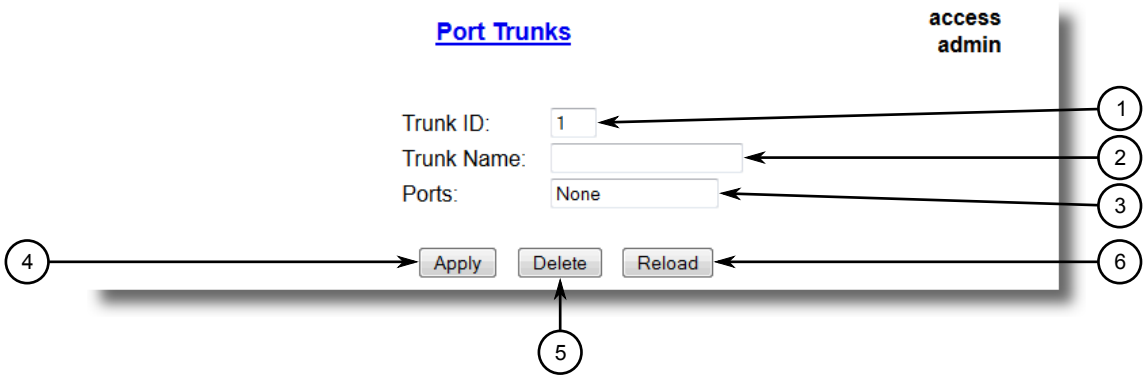


Figure 176: Port Trunks Form

1. Trunk ID Box **2.** Trunk Name Box **3.** Ports Box **4.** Apply Button **5.** Delete Button **6.** Reload Button

3. Click **Delete**.

6 Troubleshooting

This chapter describes troubleshooting steps for common issues that may be encountered when using RUGGEDCOM ROS or designing a network.

IMPORTANT!
For further assistance, contact a Customer Service representative.

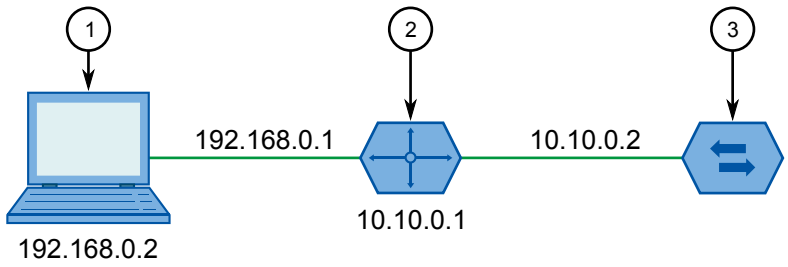
CONTENTS

- Section 6.1, "General"
- Section 6.2, "Ethernet Ports"
- Section 6.3, "Spanning Tree"
- Section 6.4, "VLANs"

Section 6.1

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.  **Figure 177: Using a Router As a Gateway** **1.** Work Station **2.** Router **3.** Switch 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 in order to reach the workstation and will drop the response. Programming a gateway of 10.0.0.1 will cause the switch to forward unresolvable frames to the router. This problem will also occur if the gateway address is not configured and the switch tries to raise an SNMP trap to a host that is not on the local subnet.

Section 6.2

Ethernet Ports

The following describes common problems related to Ethernet ports.

Problem	Solution
A link seems fine when traffic levels are low, but fails as traffic rates increase OR a link can be pinged but has problems with FTP/SQL/HTTP/etc.	A possible cause of intermittent operation is that of a 'duplex mismatch'. If one end of the link is fixed to full-duplex and the peer auto-negotiates, the auto-negotiating end falls back to half-duplex operation. At lower traffic volumes, the link may display few if any errors. As the traffic volume rises, the fixed negotiation side will begin to experience dropped packets while the auto-negotiating side will experience collisions. Ultimately, as traffic loads approach 100%, the link will become entirely unusable. The ping command with flood options is a useful tool for testing commissioned links. The command **`ping`** `192.168.0.1 500 2` can be used to issue 500 pings each separated by two milliseconds to the next switch. If the link used is of high quality, then no pings should be lost and the average round trip time should be small.
Links are inaccessible, even when using the Link Fault Indication (LFI) protection feature.	Make sure LFI is not enabled on the peer as well. If both sides of the link have LFI enabled, then both sides will withhold link signal generation from each other.

Section 6.3

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 port status LEDs are flashing rapidly.	Is it possible that one of the switches in the network or one of the ports on a switch in the network has STP disabled and accidentally connects to another switch? If this has occurred, then a traffic loop has been formed.
Occasionally, the ports seem to experience significant flooding for a brief period of time.	If the problem appears to be transient in nature, it is possible that ports that are part of the spanning tree have been configured as edge ports. After the link layers have come up on edge ports, STP will directly transition them (perhaps improperly) to the forwarding state. If an RSTP configuration message is then received, the port will be returned to blocking. A traffic loop may be formed for the length of time the port was in forwarding.
A switch displays a strange behavior where the root port hops back and forth between two switch ports and never settles down.	If one of the switches appears to flip the root from one port to another, the problem may be one of traffic prioritization. For more information refer to "The network becomes unstable when a specific application is started." Another possible cause of intermittent operation is that of an auto-negotiation mismatch. If one end of the link is fixed to full-duplex mode and the peer auto-negotiates, the auto-negotiating end will fall back to half-duplex operation. At lower traffic, the volumes the link may display few if any errors. As the traffic volume rises, the fixed negotiation side will begin to experience dropped packets while the auto-negotiating side will experience collisions. Ultimately, as traffic loads approach 100%, the link will become entirely unusable. At this point, RSTP will not be able to transmit configuration messages over the link and the spanning tree topology will break down. If an alternate trunk exists, RSTP will activate it in the place of the congested port. Since activation of the alternate port often relieves the congested port of its traffic, the congested port will once again become reliable. RSTP will promptly enter it back into service, beginning the cycle once again. The root port will flip back and forth between two ports on the switch.
A computer or device is connected to a switch. After the switch is reset, it takes a long time for it to come up.	Is it possible that the RSTP edge setting for this port is set to false? If Edge is set to false, the bridge will make the port go through two forward delay times before the port can send or receive frames. If Edge is set to true, the bridge will transition the port directly to forwarding upon link up.

Problem	Solution
	Another possible explanation is that some links in the network run in half-duplex mode. RSTP uses a peer-to-peer protocol called Proposal-Agreement to ensure transitioning in the event of a link failure. This protocol requires full-duplex operation. When RSTP detects a non-full duplex port, it cannot rely on Proposal-Agreement protocol and must make the port transition the slow (i.e. STP) way. If possible, configure the port for full-duplex operation. Otherwise, configure the port's point-to-point setting to true. Either one will allow the Proposal-Agreement protocol to be used.
When the switch is tested by deliberately breaking a link, it takes a long time before devices beyond the switch can be polled.	Is it possible that some ports participating in the topology have been configured to STP mode or that the port's point-to-point parameter is set to false? STP and multipoint ports converge slowly after failures occur. Is it possible that the port has migrated to STP? If the port is connected to the LAN segment by shared media and STP bridges are connected to that media, then convergence after link failure will be slow. Delays on the order of tens or hundreds of milliseconds can result in circumstances where the link broken is the sole link to the root bridge and the secondary root bridge is poorly chosen. The worst of all possible designs occurs when the secondary root bridge is located at the farthest edge of the network from the root. In this case, a configuration message will have to propagate out to the edge and then back in order to reestablish the topology.
The network is composed of a ring of bridges, of which two (connected to each other) are managed and the rest are unmanaged. Why does the RSTP protocol work quickly when a link is broken between the managed bridges, but not in the unmanaged bridge part of the ring?	A properly operating unmanaged bridge is transparent to STP configuration messages. The managed bridges will exchange configuration messages through the unmanaged bridge part of the ring as if it is non-existent. When a link in the unmanaged part of the ring fails however, the managed bridges will only be able to detect the failure through timing out of hello messages. Full connectivity will require three hello times plus two forwarding times to be restored.
The network becomes unstable when a specific application is started. The network returns to normal when the application is stopped.	RSTP sends its configuration messages using the highest possible priority level. If CoS is configured to allow traffic flows at the highest priority level and these traffic flows burst continuously to 100% of the line bandwidth, STP may be disrupted. It is therefore advised not to use the highest CoS.
When a new port is brought up, the root moves on to that port instead of the port it should move to or stay on.	Is it possible that the port cost is incorrectly programmed or that auto-negotiation derives an undesired value? Inspect the port and path costs with each port active as root.
An Intelligent Electronic Device (IED) or controller does not work with the device.	Certain low CPU bandwidth controllers have been found to behave less than perfectly when they receive unexpected traffic. Try disabling STP for the port. If the controller fails around the time of a link outage, there is the remote possibility that frame disordering or duplication may be the cause of the problem. Try setting the root port of the failing controller's bridge to STP.
Polls to other devices are occassionally 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.

Section 6.4

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.
On a network of 30 switches, management traffic needs to be restricted to a separate domain. What is the best method for doing this while staying in contact with these switches?	At the switch where the management station is located, configure a port to use the new management VLAN as its native VLAN. Configure a host computer to act as a temporary management station. At each switch, configure the management VLAN to the new value. Contact with each individual switch will be lost immediately as they are being configured, but it should be possible re-establish communication from the temporary management station. After all switches have been taken to the new management VLAN, configure the ports of all attached management devices to use the new VLAN. **NOTE** *Establishing a management domain is often accompanied with the establishment of an IP subnet specifically for the managed devices.*