SIEMENS

Edition 12/2025

Configuration Manual

SIMATIC NET

Rugged Ethernet switches

RUGGEDCOM ROS v5.10

For RSL910

https://www.siemens.com/ruggedcom

SIEMENS

SIMATIC NET

Rugged Ethernet switches RUGGEDCOM ROS v5.10

Configuration Manual

For RSL910

Preface

Introduction 1

Using ROS 2

Getting started 3

Device management 4

System administration 5

Security 6

Layer 2 7

Network redundancy 8

Traffic control and classification 9

Time services 10

Network discovery and management 11

IP address assignment 12

Troubleshooting 13

Reference 14

12/2025
C79000-G8976-1651-03

Legal information

Warning notice system

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

⚠ DANGER

Indicates that death or severe personal injury will result if proper precautions are not taken.

⚠ WARNING

Indicates that death or severe personal injury may result if proper precautions are not taken.

⚠ CAUTION

Indicates that minor personal injury can result if proper precautions are not taken.

⚠ NOTICE

Indicates that property damage can result if proper precautions are not taken.

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

Qualified personnel

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

Proper use of Siemens products

Note the following:

⚠ WARNING

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

Trademarks

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

Disclaimer of liability

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

Digital Industries
Process Automation
300 Applewood Crescent
Concord, Ontario, L4K 4E5
Canada

Document order number: C79000-G8976-1651-03
© 12/2025 Subject to change

Copyright © Siemens Canada Ltd. 2025
All rights reserved

Table of contents

Preface ..... **xiii**
Cybersecurity information xiii
Firmware/software support model xiv
CLI command syntax xiv
Supplementary documentation xv
SIMATIC NET glossary xv
System requirements xvi
Accessing documentation xvi
Registered trademarks xvi
Warranty xvi
Training xvii
Customer support xvii
Contacting Siemens xvii

1 Introduction **1**
1.1 Features and benefits 1
1.2 Security recommendations 4
1.3 Logged security events 7
1.4 Controlled vs. non-controlled 10
1.5 Supported networking standards 11
1.6 Internet protocol support 11
1.6.1 Features supported by IPv4 and/or IPv6 11
1.6.2 IPv4 address 12
1.6.3 IPv6 address 12
1.7 Port numbering scheme 12
1.8 Available services 13

2 Using ROS **17**
2.1 Logging in with default settings 17
2.2 Logging in 19
2.3 Logging out 20
2.4 Using the Web interface 20
2.5 Using the console interface 22
2.6 Using the command line interface 24
2.6.1 Available CLI commands 24
2.6.2 Tracing events 31
2.6.3 Executing commands remotely via RSH 32
2.6.4 Using SQL commands 33
2.6.4.1 Finding the correct table 33

2.6.4.2 Retrieving information 34
2.6.4.3 Changing values in a table 36
2.6.4.4 Resetting a table 36
2.6.4.5 Using RSH and SQL 37
2.7 Selecting ports in RUGGEDCOM ROS 37
2.8 Managing the flash file system 37
2.8.1 Viewing a list of flash files 38
2.8.2 Viewing flash file details 38
2.8.3 Defragmenting the flash file system 39
2.9 Accessing BIST mode 39
2.10 Managing access to the boot loader interface 40
2.10.1 Enabling/disabling access to the boot loader interface 40
2.10.2 Accessing the boot loader interface 41
2.11 Enabling/disabling the console service 42
3 Getting started 43
3.1 Connecting to ROS 43
3.1.1 Default IP address 43
3.1.2 Connecting directly 43
3.1.3 Connecting remotely 45
3.2 Installing the RUGGEDCOM USB serial console driver (Windows only) 47
3.3 Configuring a basic network 47
4 Device management 49
4.1 Viewing product information 49
4.2 Viewing CPU diagnostics 50
4.3 Restoring factory defaults 50
4.4 Uploading/downloading files 51
4.4.1 Uploading/downloading files using XMODEM 53
4.4.2 Uploading/downloading files using a TFTP client 54
4.4.3 Uploading/downloading files using a TFTP server 55
4.4.4 Uploading/downloading files using an SFTP server 55
4.5 Managing logs 56
4.5.1 File storage capacity 56
4.5.2 Viewing local and system logs 56
4.5.3 Clearing local and system logs 56
4.5.4 Configuring the local system log 57
4.5.5 Managing remote logging 57
4.5.5.1 Syslog format 57
4.5.5.2 Configuring the remote syslog client 59
4.5.5.3 Viewing a list of remote syslog servers 60
4.5.5.4 Adding a remote syslog server 60
4.5.5.5 Deleting a remote syslog server 61
4.6 Managing Ethernet ports 61

4.6.1 Controller protection through Link Fault Indication (LFI) 62
4.6.2 Viewing the status of Ethernet ports 63
4.6.3 Viewing statistics for all Ethernet ports 64
4.6.4 Viewing statistics for specific Ethernet ports 64
4.6.5 Clearing statistics for specific ethernet ports 67
4.6.6 Configuring an Ethernet port 67
4.6.7 Configuring port rate limiting 70
4.6.8 Configuring link detection 71
4.6.9 Traffic mirroring 72
4.6.9.1 Configuring traffic mirroring 72
4.6.10 Managing SFP transceivers 74
4.6.10.1 SFP transceiver requirements 75
4.6.10.2 Monitoring an SFP port 75
4.6.10.3 Displaying information for an SFP port 76
4.6.10.4 Setting the SFP polling interval 77
4.6.10.5 Viewing SFP diagnostics 78
4.6.11 Managing EoVDSL Ports 81
4.6.11.1 Understanding EoVDSL 81
4.6.11.2 Viewing the status of EoVDSL ports 82
4.6.11.3 Configuring an EoVDSL port 84
4.6.11.4 Adjusting EoVDSL settings 85
4.6.12 Detecting cable faults 86
4.6.12.1 Viewing cable diagnostics results 86
4.6.12.2 Performing cable diagnostics 88
4.6.12.3 Clearing cable diagnostics 89
4.6.12.4 Determining the Estimated Distance To Fault (DTF) 89
4.6.13 Resetting Ethernet ports 89

4.7 Managing IP interfaces 90
4.7.1 Viewing a list of IP interfaces 91
4.7.2 Adding an IP interface 91
4.7.3 Deleting an IP interface 93

4.8 Managing IP gateways 93
4.8.1 Viewing a list of IP gateways 93
4.8.2 Adding an IP gateway 93
4.8.3 Deleting an IP gateway 94

4.9 Configuring IP services 94

4.10 Managing remote monitoring 96
4.10.1 Managing rmon history controls 96
4.10.1.1 Viewing a list of RMON history controls 96
4.10.1.2 Adding an rmon history control 96
4.10.1.3 Deleting an RMON history control 97
4.10.2 Managing RMON alarms 97
4.10.2.1 Viewing a list of RMON alarms 98
4.10.2.2 Adding an RMON alarm 99
4.10.2.3 Deleting an RMON alarm 101
4.10.3 Managing RMON events 101
4.10.3.1 Viewing a list of RMON events 101

4.10.3.2 Adding an RMON event 101
4.10.3.3 Deleting an RMON event 102
4.11 Upgrading/downgrading firmware 102
4.11.1 Verifying the hash checksum 102
4.11.2 Upgrading firmware 103
4.11.3 Downgrading firmware 104
4.12 Rebooting the device 105
4.13 Decommissioning the device 105
5 System administration 109
5.1 Configuring the system information 109
5.2 Customizing the login screen 109
5.3 Enabling/disabling the Web interface 110
5.4 Managing alarms 110
5.4.1 Viewing a list of pre-configured alarms 111
5.4.2 Viewing and clearing latched alarms 111
5.4.3 Configuring an alarm 111
5.4.4 Authentication related security alarms 113
5.4.4.1 Security alarms for login authentication 113
5.4.4.2 Security messages for port authentication 115
5.4.5 List of alarms 116
5.5 Managing the configuration file 120
5.5.1 Configuring data encryption 121
5.5.2 Updating the configuration file 122
5.6 Managing MMS 122
5.6.1 Understanding MMS 123
5.6.1.1 MMS reporting 123
5.6.1.2 Reports/data sets 123
5.6.1.3 Supported logical nodes 124
5.6.2 Viewing a list of preconfigured MMS reports 125
5.6.3 Configuring an MMS report 126
5.6.4 Example: Configuring MMS reports 126
6 Security 129
6.1 Configuring passwords 129
6.2 Clearing private data 131
6.3 Managing user authentication 132
6.3.1 Authentication methods 132
6.3.2 Configuring user name extensions 134
6.3.3 Managing RADIUS authentication 135
6.3.3.1 Configuring the RADIUS server 135
6.3.3.2 Configuring the RADIUS client on the device 136
6.3.4 Managing TACACS+ authentication 138
6.3.4.1 Configuring TACACS+ 138
6.3.4.2 Configuring user privileges 140

6.4 Managing port security 141
6.4.1 Port security concepts 141
6.4.1.1 Static MAC address-based authentication 141
6.4.1.2 Static MAC address-based authentication in an MRP ring 142
6.4.1.3 IEEE 802.1X authentication 142
6.4.1.4 IEEE 802.1X authentication with MAC address-based authentication 144
6.4.1.5 Restricted VLANs 144
6.4.1.6 Assigning VLANS with tunnel attributes 145
6.4.1.7 Example: 802.1X port security on multiple VLANs 146
6.4.2 Viewing a list of authorized MAC addresses 147
6.4.3 Configuring port security 148
6.4.4 Configuring IEEE 802.1X 149

6.5 Managing SSH/TLS keys and certificates 150
6.5.1 TLS certificates 152
6.5.2 SSH host key 153
6.5.3 Managing SSH public keys 153
6.5.3.1 Public key requirements 154
6.5.3.2 Adding a public key 155
6.5.3.3 Viewing a list of public keys 156
6.5.3.4 Updating a public key 156
6.5.3.5 Deleting a public key 157
6.5.4 Certificate and key examples 157

7 Layer 2 159

7.1 Managing Virtual Local Area Networks (VLANs) 159
7.1.1 VLAN concepts 159
7.1.1.1 Tagged vs. untagged frames 159
7.1.1.2 Native VLAN 160
7.1.1.3 The management VLAN 160
7.1.1.4 Auxiliary management VLANs 160
7.1.1.5 Edge and trunk port types 161
7.1.1.6 Ingress and egress rules 162
7.1.1.7 Forbidden ports list 162
7.1.1.8 VLAN-aware and VLAN-unaware modes 162
7.1.1.9 GARP VLAN Registration Protocol (GVRP) 163
7.1.1.10 PVLAN edge 165
7.1.1.11 QinQ 165
7.1.1.12 VLAN advantages 167
7.1.2 Viewing a list of VLANs 168
7.1.3 Configuring VLANs globally 169
7.1.4 Configuring VLANs for specific Ethernet ports 169
7.1.5 Managing static VLANs 170
7.1.5.1 Viewing a list of static VLANs 171
7.1.5.2 Adding a static VLAN 171
7.1.5.3 Deleting a static VLAN 172
7.1.6 Example: Configuring management support on multiple VLANs 172

7.2 Managing MAC addresses 174
7.2.1 Viewing a list of MAC addresses 174

7.2.2 Configuring MAC address learning options 174
7.2.3 Configuring MAC address flooding options 175
7.2.4 Managing static MAC addresses 175
7.2.4.1 Viewing a list of static MAC addresses 176
7.2.4.2 Adding a static MAC address 176
7.2.4.3 Deleting a static MAC address 177
7.2.5 Purging all dynamic MAC addresses 177

7.3 Managing multicast filtering 177
7.3.1 Managing IGMP 177
7.3.1.1 IGMP concepts 178
7.3.1.2 Viewing a list of multicast group memberships 182
7.3.1.3 Viewing forwarding information for multicast groups 183
7.3.1.4 Configuring IGMP 184
7.3.2 Managing GMRP 185
7.3.2.1 GMRP concepts 185
7.3.2.2 Viewing a summary of multicast groups 188
7.3.2.3 Configuring GMRP globally 188
7.3.2.4 Configuring GMRP for specific Ethernet ports 189
7.3.2.5 Viewing a list of static multicast groups 190
7.3.2.6 Adding a static multicast group 190
7.3.2.7 Deleting a static multicast group 191

8 Network redundancy 193

8.1 Managing Spanning Tree Protocol (STP) 193
8.1.1 RSTP operation 193
8.1.1.1 RSTP states and roles 194
8.1.1.2 Edge ports 196
8.1.1.3 Point-to-point and multipoint links 196
8.1.1.4 Path and port costs 196
8.1.1.5 Bridge diameter 197
8.1.1.6 eRSTP 198
8.1.1.7 Fast Root Failover 198
8.1.2 RSTP applications 199
8.1.2.1 RSTP in structured wiring configurations 199
8.1.2.2 RSTP in ring backbone configurations 201
8.1.2.3 RSTP port redundancy 203
8.1.3 MSTP operation 204
8.1.3.1 MSTP regions and interoperability 204
8.1.3.2 MSTP bridge and port roles 205
8.1.3.3 Benefits of MSTP 207
8.1.3.4 Implementing MSTP on a bridged network 208
8.1.4 Configuring STP globally 209
8.1.5 Configuring STP for specific Ethernet ports 210
8.1.6 Configuring eRSTP 212
8.1.7 Viewing global statistics for STP 214
8.1.8 Viewing STP statistics for Ethernet ports 216
8.1.9 Managing multiple spanning tree instances 218
8.1.9.1 Viewing statistics for global MSTIs 218
8.1.9.2 Viewing statistics for port MSTIs 218

8.1.9.3 Configuring the MST region identifier 220
8.1.9.4 Configuring a global MSTI 220
8.1.9.5 Configuring an MSTI for an Ethernet port 221
8.1.10 Clearing spanning tree protocol statistics 222

8.2 Managing the Media Redundancy Protocol (MRP) 222
8.2.1 Understanding MRP 222
8.2.1.1 MRM vs MRC devices 223
8.2.1.2 MRA devices 223
8.2.1.3 Ring port states 223
8.2.1.4 Ring-closed vs ring-open 224
8.2.2 Configuring MRP globally 225
8.2.3 Viewing the status of MRP instances 225
8.2.4 Adding an MRP instance 226
8.2.5 Deleting an MRP instance 228
8.2.6 Example: Configuring an MRP ring 229

8.3 Managing link aggregation 231
8.3.1 Link aggregation concepts 232
8.3.1.1 Static vs. dynamic link aggregation 232
8.3.1.2 Rules and limitations 233
8.3.1.3 Link aggregation and Layer 2 features 234
8.3.1.4 Link aggregation and physical layer features 234
8.3.2 Configuring link aggregation 234
8.3.3 Managing link aggregation groups 235
8.3.3.1 Viewing a list of link aggregation groups 235
8.3.3.2 Adding a link aggregation group 235
8.3.3.3 Deleting a link aggregation group 236
8.3.3.4 Viewing the status of link aggregation groups 237
8.3.4 Managing the link aggregation control protocol 237
8.3.4.1 Viewing information about the LACP partner 238
8.3.4.2 Configuring global LACP settings 238
8.3.4.3 Configuring LACP per port 239
8.3.4.4 Viewing LACP statistics 240
8.3.5 Clearing link aggregation statistics 241

9 Traffic control and classification 243

9.1 Managing Classes of Service (CoS) 243
9.1.1 Configuring classes of service globally 244
9.1.2 Configuring classes of service for specific ethernet ports 244
9.1.3 Configuring priority to CoS mapping 245
9.1.4 Configuring DSCP to CoS mapping 245

10 Time services 247

10.1 Configuring the time and date 247

10.2 Managing NTP 248
10.2.1 Enabling/disabling NTP service 248
10.2.2 Configuring NTP servers 249

11 Network discovery and management 251

11.1 Enabling/disabling RCDP 251
11.2 Managing LLDP 252
11.2.1 Configuring LLDP globally 253
11.2.2 Configuring LLDP for an Ethernet port 254
11.2.3 Viewing global statistics and advertised system information 255
11.2.4 Viewing statistics for LLDP neighbors 255
11.2.5 Viewing statistics for LLDP ports 256
11.3 Managing SNMP 256
11.3.1 Improving SNMP performance 257
11.3.2 Managing SNMP users 258
11.3.2.1 Viewing a list of SNMP users 258
11.3.2.2 Adding an SNMP user 258
11.3.2.3 Deleting an SNMP user 261
11.3.3 Managing security-to-group mapping 261
11.3.3.1 VIewing a list of security-to-group maps 261
11.3.3.2 Adding a security-to-group map 261
11.3.3.3 Deleting a security-to-group map 262
11.3.4 Managing SNMP groups 262
11.3.4.1 Viewing a list of SNMP groups 262
11.3.4.2 Adding an SNMP group 262
11.3.4.3 Deleting an SNMP group 264
11.4 ModBus management support 264
11.4.1 ModBus function codes 264
11.4.2 ModBus memory map 265
11.4.3 Modbus memory formats 270
11.4.3.1 Text 270
11.4.3.2 Cmd 270
11.4.3.3 Uint16 271
11.4.3.4 Uint32 271
11.4.3.5 PortCmd 271
11.4.3.6 Alarm 272
11.4.3.7 TruthValues 272
12 IP address assignment 275
12.1 Managing DHCP 275
12.1.1 DHCP concepts 275
12.1.1.1 DHCP snooping 275
12.1.1.2 Trusted and untrusted ports 275
12.1.1.3 DHCP relay agent (Option 82) 276
12.1.1.4 DHCP binding table 276
12.1.1.5 Preventable network attacks 277
12.1.2 Configuring the DHCP relay agent 279
12.1.3 Enabling DHCP relay agent information (Option 82) for specific ports 279
12.1.4 Configuring DHCP snooping 280
12.1.5 Configuring trusted/untrusted ports 280
12.1.6 Managing the DHCP binding table 281
12.1.6.1 Adding entries to the DHCP binding table 281
12.1.6.2 Viewing the DHCP binding table 282

12.1.6.3 Saving the DHCP binding table 282
12.1.6.4 Example: Configuring the device as a relay agent 283

13 Troubleshooting 285

13.1 General 285

13.2 Ethernet ports 286

13.3 Spanning tree 286

13.4 VLANs 288

14 Reference 291

14.1 SNMP 291
14.1.1 Supported standard MIBs 291
14.1.2 Supported proprietary RUGGEDCOM MIBs 377
14.1.3 Supported agent capabilities 419
14.1.4 SNMP trap bindings 420
14.1.5 SNMP traps 423

14.2 Cipher suites and algorithms 438

Preface

This manual describes v5.10 of ROS (Rugged Operating System) running on the RUGGEDCOM RSL910. 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.

Note

This document is updated to match the version of RUGGEDCOM ROS v5.10 available at the time of publication, including minor releases (e.g. 5.10.1, 5.10.2, etc.). To determine the current release of RUGGEDCOM ROS v5.10, refer to Siemens Industrial Online Support:

- **Product Notes**
  https://support.industry.siemens.com/cs/search?search=ROS&type=ProductNote&o=0
- **Downloads**
  https://support.industry.siemens.com/cs/search?search=ROS&type=Download&o=0

Users can also set up a daily or weekly e-mail notification to inform of them of recent releases/updates. For more information, refer to Siemens Industrial Online Support [https://support.industry.siemens.com] website.

Note

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 manual should be used as a companion to the Help text included in the software.

Cybersecurity information

Siemens provides products and solutions with industrial cybersecurity functions that support the secure operation of plants, systems, machines and networks.

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial cybersecurity concept. Siemens' products and solutions constitute one element of such a concept.

Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent

such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place.

For additional information on industrial cybersecurity measures that may be implemented, please visit https://www.siemens.com/cybersecurity-industry.

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customer's exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Cybersecurity RSS Feed under https://www.siemens.com/cert.

Firmware/software support model

Siemens only monitors the latest firmware/software version for security vulnerabilities. Therefore, bug and security fixes are provided only for the latest released firmware/software version.

CLI command syntax

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

Elements of a CLI command

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

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

Command formatting

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

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

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

Supplementary documentation

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

For specific documents, search the following:

Product notes	https://support.industry.siemens.com/cs/ww/en/ps/29749/pm
Manuals	https://support.industry.siemens.com/cs/ww/en/ps/29749/man
FAQs	https://support.industry.siemens.com/cs/ww/en/ps/29749/faq
Application examples	https://support.industry.siemens.com/cs/ww/en/ps/29749/ae
Catalogs/brochures	https://support.industry.siemens.com/cs/ww/en/ps/29749/cat
Certificates	https://support.industry.siemens.com/cs/ww/en/ps/29749/cert
Downloads	https://support.industry.siemens.com/cs/ww/en/ps/29749/dl

Other documents that may be of interest include:

SINEC NMS Operating Instructions	https://support.industry.siemens.com/cs/ww/en/ps/26672
SINEC PNI Operating Instructions	https://support.industry.siemens.com/cs/ww/en/ps/25518/man
Performance of the Rapid Spanning Tree Protocol in Ring Network Topology	https://assets.new.siemens.com/siemens/assets/api/uuid:d4af5d17-728c-493f-b00a-9c4db67b23ed/RSTP-whitepaper-EN-09-2020.pdf

SIMATIC NET glossary

The SIMATIC NET glossary describes special terms that may be used in this document.

The glossary is available online via Siemens Industry Online Support (SIOS) at:

https://support.industry.siemens.com/cs/ww/en/view/50305045

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 Edge 107
  - Mozilla Firefox 107.0
  - Google Chrome 107
- Must have a working Ethernet interface compatible with at least one of the port types on the RUGGEDCOM device
- The ability to configure an IP address and netmask on the computer's Ethernet interface

Accessing documentation

The latest user documentation for RUGGEDCOM ROS v5.10 is available online at https://support.industry.siemens.com. To request or inquire about a user document, contact Siemens Customer Support.

Registered trademarks

The following and possibly other names not identified by the registered trademark sign ® are registered trademarks of Siemens Canada Ltd.:

- RUGGEDCOM
- ROS
- RCDP
- Discovery Protocol

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

Warranty

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

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

Training

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

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

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

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

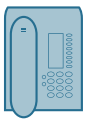
Customer support

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



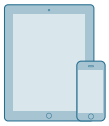
Online

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



Telephone

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



Mobile app

Install the Industry Online Support app by Siemens Aktiengesellschaft 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

Contacting Siemens

Address	Siemens Canada Ltd. Digital Industries Process Automation 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	info.ruggedcom@siemens.com
Web	https://www.siemens.com

1 Introduction

Welcome to the RUGGEDCOM ROS v5.10 Software Configuration Manual for the RUGGEDCOM RSL910 devices. This manual describes the wide array of carrier grade features made available by RUGGEDCOM ROS (Rugged Operating System).

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

1.1 Features and benefits

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

- **Cyber security features**
  Cyber security is an urgent issue in many industries where advanced automation and communications networks play a crucial role in mission critical applications and where high reliability is of paramount importance. Key RUGGEDCOM ROS features that address security issues at the local area network level include:

Passwords	Multi-level user passwords secures against unauthorized configuration
SSH/TLS	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.
- **Remote monitoring and configuration with SINEC NMS**
  SINEC NMS 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.

  SINEC NMS is especially suited for remotely monitoring and configuring Siemens routers, switches, serial servers and WiMAX wireless network equipment. For more information, visit https://www.siemens.com/sinec.
- **Device management with SINEC PNI**
  RUGGEDCOM ROS devices are compatible with SINEC PNI (Primary Network Initialization), a tool for commissioning RUGGEDCOM routers and switches. Use SINEC PNI to quickly add one or more devices to the network.

  Some of the features offered by SINEC PNI include:

  - Bulk device management
  - Change, load, or download device configurations
  - Upgrade or downgrade firmware
  - IP address management
- **Simple Network Management Protocol (SNMP)**
  SNMP provides a standardized method, for network management stations, to interrogate devices from different vendors. Supported SNMP versions include v1, v2c and v3. SNMPv3 in particular provides security features (such as authentication, privacy, and access control) not present in earlier SNMP versions. Numerous standard MIBs (Management Information Base) allow for easy integration with any Network Management System (NMS). A feature of SNMP supported by RUGGEDCOM ROS is the ability to generate *traps* upon system events. SINEC 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.

- **NTP (Network Time Protocol)**
  NTP automatically synchronizes the internal clock of all RUGGEDCOM ROS devices on the network. This allows for correlation of time stamped events for troubleshooting.
- **Port rate limiting**
  RUGGEDCOM ROS supports configurable rate limiting per port to limit unicast and multicast traffic. This can be essential to managing precious network bandwidth for service providers. It also provides edge security for Denial of Service (DoS) attacks.
- **Broadcast storm filtering**
  Broadcast storms wreak havoc on a network and can cause attached devices to malfunction. This could be disastrous on a network with mission critical equipment. RUGGEDCOM ROS limits this by filtering broadcast frames with a user-defined threshold.
- **Link aggregation**
  Ethernet ports can be aggregated into a single logical link either statically or dynamically to increase bandwidth and balance the traffic load.
- **Port mirroring**
  RUGGEDCOM ROS can be configured to duplicate all traffic on one port to a designated mirror port. When combined with a network analyzer, this can be a powerful troubleshooting tool.
- **Port configuration and status**
  RUGGEDCOM ROS allows individual ports to be *hard* configured for speed, duplex, auto-negotiation, flow control and more. This allows proper connection with devices that do not negotiate or have unusual settings. Detailed status of ports with alarm and SNMP trap on link problems aid greatly in system troubleshooting.
- **Port statistics and RMON (Remote Monitoring)**
  RUGGEDCOM ROS provides continuously updating statistics per port that provide both ingress and egress packet and byte counters, as well as detailed error figures.

  Also provided is full support for RMON statistics. RMON allows for very sophisticated data collection, analysis and detection of traffic patterns.
- **Multicast filtering**
  RUGGEDCOM ROS supports static multicast groups and the ability to join or leave multicast groups dynamically using IGMP (Internet Group Management Protocol) or GMRP (GARP Multicast Registration Protocol).
- **Event logging and alarms**
  RUGGEDCOM ROS records all significant events to a non-volatile system log allowing forensic troubleshooting. Events include link failure and recovery, unauthorized access, broadcast storm detection, and self-test diagnostics among others. Alarms provide a snapshot of recent events that have yet to be acknowledged by the network administrator. An external hardware relay is de-energized during the presence of critical alarms, allowing an external controller to react if desired.

- **HTML Web browser user interface**
  RUGGEDCOM ROS provides a simple, intuitive user interface for configuration and monitoring via a standard graphical Web browser or via a standard telcom user interface. All system parameters include detailed online help to facilitate setup and configuration. RUGGEDCOM ROS presents a common look and feel and standardized configuration process, allowing easy migration to other managed RUGGEDCOM products.
- **Brute force attack prevention**
  Protection against Brute Force Attacks (BFAs) is standard in RUGGEDCOM ROS. If an external host fails to log in to the Terminal or Web interfaces after a fixed number of attempts, the service will be blocked for one hour.

1.2 Security recommendations

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

Authentication

- Replace the default passwords for all user accounts and processes (where applicable) before the device is deployed.
- Use strong passwords with high randomization (i.e. entropy), without repetition of characters. Avoid weak passwords such as *password1*, *123456789*, *abcdefgh*, and any dictionary words or proper names in any combination. For more information about creating strong passwords, refer to the password requirements in "Configuring passwords" (Page 129).
- 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 in use, make sure the Force Message-Authenticator attribute is enabled to validate message requests.

  For more information about the Force Message-Authenticator attribute, refer to "Configuring the RADIUS client on the device" (Page 136).
- When RADIUS or TACACS+ are utilized for user authentication, make sure all communications are within the security perimeter or protected by a secure channel.

  TACACS+ uses the MD5 algorithm for key encryption. Make sure to follow the security recommendations outlined in this document and configure the environment according to defense in depth best practices.
- Generate and provision a custom TLS certificate and SSH host key pair before commissioning the device. Certificates and keys must be unique and not reused on multiple devices or servers. For more information, refer to "Managing SSH/TLS keys and certificates" (Page 150).

- Use SSH public key authentication. For more information, refer to "Managing SSH public keys" (Page 153).
- Be aware of any link layer protocols that do not provide any inherent authentication between endpoints, such as ARP in IPv4, neighbor discovery/ DAD in IPv6 and Wi-Fi in wireless networks. A malicious entity could exercise weaknesses in these protocols to attack hosts, switches, and routers connected to your Layer 2 network, for example, by poisoning the ARP caches of systems within the subnet and subsequently intercepting traffic. Appropriate safeguards against non-secure L2 protocols, such as securing physical access to the local network and using secure higher layer protocols, should be taken to prevent unauthorized access to the network.

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 unauthorized access to the RUGGEDCOM ROS boot loader, which includes tools that may be used to gain complete access to the device. For more information about restricting access to the boot loader interface, refer to "Managing access to the boot loader interface" (Page 40).
- 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.
- For increased security, enable ingress filtering on all ports by default. For more information about enabling ingress filtering, refer to "Configuring VLANs globally" (Page 169).
- If SNMP is enabled, limit the number of IP addresses that can connect to the device and change the community names. Also configure SNMP to raise a trap upon authentication failures. For more information, refer to "Managing SNMP" (Page 256).
- Limit the number of simultaneous Web Server, Telnet and SSH sessions allowed.
- Configure remote system logging to forward all logs to a central location. For more information, refer to "Managing logs" (Page 56) and the FAQ "How to Implement Secure, Unattended Logging in ROS" (https://support.industry.siemens.com/cs/ww/en/view/109756843).
- Configuration files are provided in the CSV (comma separated values) format for ease of use. Make sure configuration files are properly protected when they exist outside of the device. For instance, encrypt the files, store them in a secure place, and do not transfer them via insecure communication channels.

- Management of the configuration file, certificates and keys is the responsibility of the device owner. Consider using key type Ed25519 256 for SSH and TLS, an ECC key of at least 256 bits in length, and certificates signed with SHA256 or greater 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.

Secure/non-secure protocols

- While some protocols are secure, others were not designed for secure applications. Use of secure protocols is recommended regardless of physical or network protection measures.

  Secure protocols include:

  - SSH and SFTP (TCP/22)
  - SNMPv3 (UDP/161)
  - WebUI HTTPS via TLS1.2 (TCP/443)
  - 802.1X

  All other protocols should be considered insecure and only used in a secure environment.

  For more information about the available protocols or services and their associated ports, refer to "Available services" (Page 13)
- Disable or limit the use of non-secure protocols (e.g. RCDP) not intended for use.

  When a secure alternative is available for a protocol, use the secure version instead. For example, use SNMPv3 instead of SNMPv1/v2c.

  Appropriate safeguards against non-secure protocols should be taken to prevent unauthorized access to the device/network. If non-secure protocols and services are required, make sure the device is operated within a protected network area.
- Avoid or limit use of the following:
  - Non-authenticated and unencrypted protocols
  - Link Layer Discovery Protocol (LLDP)
- For port security, RUGGEDCOM ROS supports Protected Extensible Authentication Protocol (PEAP), EAP Transport Layer Security (EAP-TLS) and EAP-MD5. EAP-MD5 not considered a secure protocol and should not be used by the supplicant. Where possible, the supplicant should be configured to use the certificate-based EAP-TLS authentication protocol to communicate with the RADIUS server.
- Whenever possible, use the SSH File Transfer Protocol (SFTP) to transfer files. While other transfer protocols are available (e.g. TFTP), SFTP is the only protocol that transfers files encrypted. The other protocols are not protected against interception and manipulation.

Hardware/software

- Make sure the latest firmware version is installed, including the latest security-related patches. For the latest information on security patches for Siemens products and security advisories, visit the CERT services website [https://new.siemens.com/global/en/products/services/cert.html]. To stay informed about new product security advisories, consider registering for the Siemens ProductCERT mailing list or subscribing to the RSS feed.
- Enable BPDU Guard on ports where RSTP BPDUs are not expected.
- Use the latest Web browser version compatible with RUGGEDCOM ROS to make sure the most secure Transport Layer Security (TLS) versions and ciphers available are employed.
- Modbus can be deactivated if not required by the user. If Modbus activation is required, then it is recommended to follow the security recommendations outlined in this manual and to configure the environment according to defense-in-depth best practices.
- Prevent access to external, untrusted Web pages while accessing the device via a Web browser. This can assist in preventing potential security threats, such as session hijacking.
- For optimal security, use SNMPv3 whenever possible. Use strong authentication keys and private keys without repetitive strings (e.g. *abc* or *abcabc*) with this feature. For more information about creating strong passwords, refer to the password requirements in "Configuring passwords" (Page 129).
- Unless required for a particular network topology, the *IP Forward* setting should be set to **Disabled** to prevent the routing of packets.

Policy

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

1.3 Logged security events

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

Category	Event message	Facility	Severity	Condition
SE_LOCAL_SUCCESSFUL_LOGON	{date} {time} INFO {temperature} Console user '{username}' logged in with admin level	Local0	Info	A user logged in successfully via a local interface to the device.
SE_LOCAL_UNSUCCESSFUL_LOGON	{date} {time} INFO {temperature} Failed Console user '{username}' login attempt	Local0	Info	Unsuccessful login attempt via a local interface to the device.

Category	Event message	Facility	Severity	Condition
SE_NETWORK_SUCCESSFUL_LOGON	{date} {time} INFO {temperature} {protocol} user '{username}' logged in with admin level {ip address}	Local0	Info	A user logged in successful via a network interface to the device.
SE_NETWORK_UNSUCCESSFUL_LOGON	{date} {time} INFO {temperature} Failed {protocol} user '{username}' login attempt {ip address}	Local0	Info	Unsuccessful login attempt via a network interface to the device.
SE_LOGOFF	{date} {time} INFO {temperature} console user '{username}, cmd: Logged out	Local0	Info	A user logged out either manually or automatically due to a timeout via a local interface.
	{date} {time} INFO {temperature} {protocol} user '{username}' ({ip address}), cmd: Logged out	Local0	Info	A user logged out either manually or automatically due to a timeout via a network interface.
SE_USER_AUTH_RADIUS_SERVER_NOT_AVAILABLE	{date} {time} INFO {temperature} RADIUS Primary server is unreachable	Local0	Info	Unsuccessful RADIUS server access or no RADIUS response.
SE_ACCESS_PWD_CHANGED	{date} {time} INFO {temperature} 'admin' level password changed {date} {time} INFO {temperature} {protocol} user {'username'} {(ip address)} Passwords Admin Password - MODIFIED.	Local0	Info	An authenticated user changed its own password.
	{date} {time} INFO {temperature} 'guest' level password changed {date} {time} INFO {temperature} {protocol} user {'username'} {(ip address)} Passwords Guest Password - MODIFIED.	Local0	Info	An authenticated user changed the password of another user.
SE_USER_ACCOUNT_CHANGED	{date> {time} INFO {temperature} {protocol} user {username} {ip address}, Passwords Guest Username, old: {guest}, new: {new username} - MODIFIED.	Local0	Info	User account modified or assigned to another role.
SE_USER_ACCOUNT_DELETED	Date> {time} INFO {temperature} {protocol} user {username} {ip address}, Passwords Guest Username, old: {username}, new:- MODIFIED.	Local0	Info	User account deleted.
SE_ACCOUNT_LOCKED_TEMP	{date} {time} WARN {temperature} Excessive failed {protocol} access/login attempts, service locked.	Local0	Warning	Brute force prevention via temporary locked user account.
SE_SESSION_LOCKED_INACTIVITY	{date} {time} INFO 37C Console user 'admin' , cmd: Logged out	Local0	Info	Session was locked after some time of inactivity.

Category	Event message	Facility	Severity	Condition
SE_RAS_SESSION_TERMINATED_INACTIVITY	{date} {time} INFO 37C HTTPS user 'admin' logged out (IP:192.168.0.200).	Local0	Info	Remote session closed after some time of inactivity.
SE_UNSUCCESSFUL_RAS_LOGON	{date} {time} INFO {temperature} Failed {protocol} user '{username}' login attempt {ip address}	Local0	Info	Remote access user failed to log in the remote access device.
SE_RAS_LOGOFF	{date} {time} INFO {temperature} {protocol} user '{username}' {ip address}, cmd: loggd out	Local0	Info	Remote access user logged out from the remote access device.
SE_RAS_CONNECTION_CLOSED	{date} {time} INFO {protocol} user {'username'} closing connection {(ip address)}	Local0	Info	Remote access connection closed.
SE_SUCCESSFUL_DEVICE_IDENTIFICATION	{date} {time} INFO {temperature} {protocol} port 1 authorized addr {MAC address}, {VLAN ID} {date} {time} INFO{temperature} Secure port 1 learned addr {MAC address}, {VLAN ID}	Local0	Info	Device access granted because of successful 802.1X Port authentication.
SE_UNSUCCESSFUL_DEVICE_IDENTIFICATION	{date} {time}WARN 43C 802.1X port 1 auth failed, addr {MAC address}, {VLAN ID}	Local0	Warning	Device access denied because of unsuccessful 802.1X Port authentication.
SE_SUCCESSFUL_DEVICE_AUTHENTICATION	{date} {time} INFO {temperature}{protocol} user {username} (pub id 1 fingerprint:{value}) logged in with {role} access {ip address}	Local0	Info	Device authenticated successful via certificate-based authentication.
SE_AUDIT_LOG_CLEARED	{date} {time}INFO {temperature} Console user 'admin' , cmd: clearlogs {date} {time} INFO {temperature} clearlogs	Local0	Info	The user deleted the device local logging buffer.
SE_CONFIG_CHANGE	{date} {time} INFO {temperature} Console user '{username}', IP Services Inactivity Timeout, old: 5 min, new: Disable - MODIFIED {date} {time} INFO {temperature} Configuration changed	Local0	Info	The user changed defined configuration details.
	{date} {time} INFO {temperature} Console user '{username}', Load Factory Defaults Defaults Choice, old: None, new: All - MODIFIED.	Local0	Info	The user initiated a reset to factory defaults.
SE_SOFTWARE_INTEGRITY_CHECK_FAILED	{date} {time} NOTE {temperature} SFTP put file main.bin from {ip address} by user {date} {time} INFO Console user '{username}', cmd: xmodem receive main.bin {date} {time} ERRO Downloaded	Local0	Error	Firmware/Software integrity verification identified an integrity error.

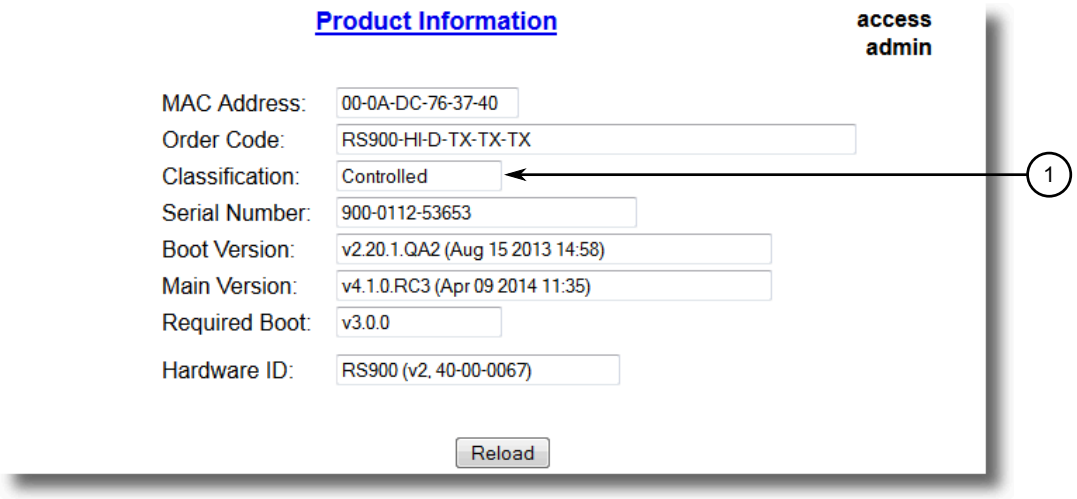
Category	Event message	Facility	Severity	Condition
	file main.bin is invalid: Bad signature {date} {time} NOTE Downloaded file with invalid signature (-7711) {date} {time} Downloaded file main.bin is invalid: Body CRC invalid			
SE_BACKUP_SUCCESSFULLY_DONE	{date} {time} NOTE {temperature} config.csv copied to A:\config.csv	Local0	Notice	The system successfully created a backup when an external memory is mounted.

1.4 Controlled vs. non-controlled

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

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

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



① Classification box

Figure 1.1 Product information form (example)

1.5 Supported networking standards

The following networking standards are supported by RUGGEDCOM ROS:

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

1.6 Internet protocol support

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

1.6.1 Features supported by IPv4 and/or IPv6

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

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

[a] Supports network solicitation and network advertisement.

1.6.2 IPv4 address

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

Example: 192.168.0.1

1.6.3 IPv6 address

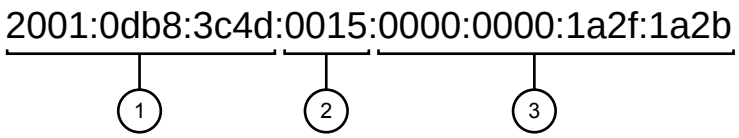
RUGGEDCOM ROS supports IPv6 global unicast addresses for management.

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

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

An IPv6 address is formatted as follows:

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



① Site Prefix
② Subnet ID
③ Interface ID

Figure 1.2 IPv6 Global Unicast Address Example

1.7 Port numbering scheme

For quick identification, each port on a RUGGEDCOM RSL910 device is assigned a number. All port numbers are silk-screened on the device.

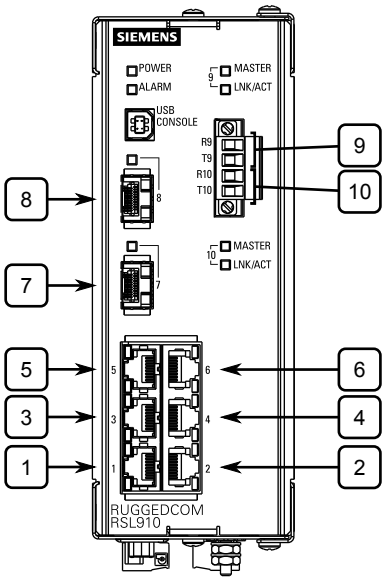


Figure 1.3 RUGGEDCOMRSL910 Port Numbering (Typical)

Use these numbers to configure applicable features on select ports.

1.8 Available services

The following is a list of all available protocols or services and their ports through which the device can be accessed, including the following information:

Note

All services are configurable, unless otherwise noted.

- **Service**
  The service supported by the device
- **Protocol**
  The protocol used by the service.
- **Default port number**
  The default port number assigned to the client/service.
- **Default status**
  The default state of the service.
- **Status**
  The state of the service when active.
- **Configurable port number**
  Specifies whether the port number is configurable.
- **Authentication**
  Specifies whether an authentication of the communication partner takes place or whether an authentication can be configured.

- **Encryption**
  Specifies whether the transfer is encrypted or whether the encryption is configurable.

Interfaces and Layer 3 services

Service	Protocol	Default port number	Default status	Status	Configurable port number	Authentication	Encryption
Telnet server	TCP	23	Closed	Open if configured with login	×	✓	×
MMS server	TCP	102	Closed	Open if configured	×	×	×
TFTP server	UDP	69	Closed	Open if configured	×	×	×
TFTP client	UDP	69	Closed	Open if configured	×	×	×
SNTP client	UDP	123	Open	Open if configured	×	×	×
RSH server	TCP	514	Closed	Open if configured with login	×	✓	×
SFTP	TCP	22	Open	Open with login	×	✓	✓
DHCP client/ BOOTP	UDP	68	Closed	Open if configured	×	×	×
DHCP relay agent	UDP	67	Closed	Open if configured	×	×	×
HTTP server	TCP	80	Open, redirects to HTTPS	Open with login	×	✓	×
HTTPS server	TCP	443	Open	Open with login	×	✓	✓
ICMP[a]	-	-	Open	Open	×	×	×
RADIUS client	UDP	Random port in range 1024 - 49151	Closed	Open if configured	×	✓	×
Syslog client	UDP	514	Closed	Only outgoing open if configured	✓	×	×
SNMPv3 server	UDP	161	Closed	Open if configured	×	✓	✓
SNMP v1/v2c server	UDP	161	Closed	Open if configured	×	×	×
SNMP Trap v1/ v2c	UDP	162	Closed	Only outgoing, open if configured	×	×	×
SNMP Trap v3	UDP	162	Closed	Only outgoing,	×	✓	✓

Service	Protocol	Default port number	Default status	Status	Configurable port number	Authentication	Encryption
				open if configured			
SSH server	TCP	22	Open	Open with login	×	✓	✓
TACACS+ client	TCP	Random port in range 1024 - 49151	Closed	Open if configured	×	✓	✓
TCP Modbus server	TCP	502	Closed	Open if configured	×	×	×

[a] Not configurable

Layer 2 services

Service	Default status	Configurable service
802.1X	Closed	✓
ARP	Open	×
GMRP	Closed	✓
GVRP	Closed	✓
LLDP	Open	✓
Spanning Tree (STP, MSTP, eRSTP)	Closed	✓
RSTP	Open	✓
RCDP	Open	✓
IGMP	Closed	✓
MRP	Closed	✓
QinQ	Closed	✓

2 Using ROS

This chapter describes how to use RUGGEDCOM ROS.

2.1 Logging in with default settings

A device with default settings is either newly commissioned or has been reset to factory defaults.

On first admin login using the default credentials, the user is authenticated but will not be granted access to the device's shell or Web interface. Instead, the user will immediately be redirected to change the password, and cannot proceed until the password is successfully updated.

The interface will present prompts requiring the user to set a new password. Once the admin default password has been changed, the user will be logged out by the system and must log in again using the newly configured password.

While the admin password is in its default state, access for other users and protocols is blocked as follows:

User/protocol	Behavior/action
Guest/Operator	Login is blocked at authentication. The admin password must be changed before other accounts can log in.
Telnet/RSH	Connection is refused after the authentication attempt until the admin password is changed.
SFTP/TFTP	Connection is refused. Access is disabled until the password is changed.

To log in to a device that has default settings, do the following:

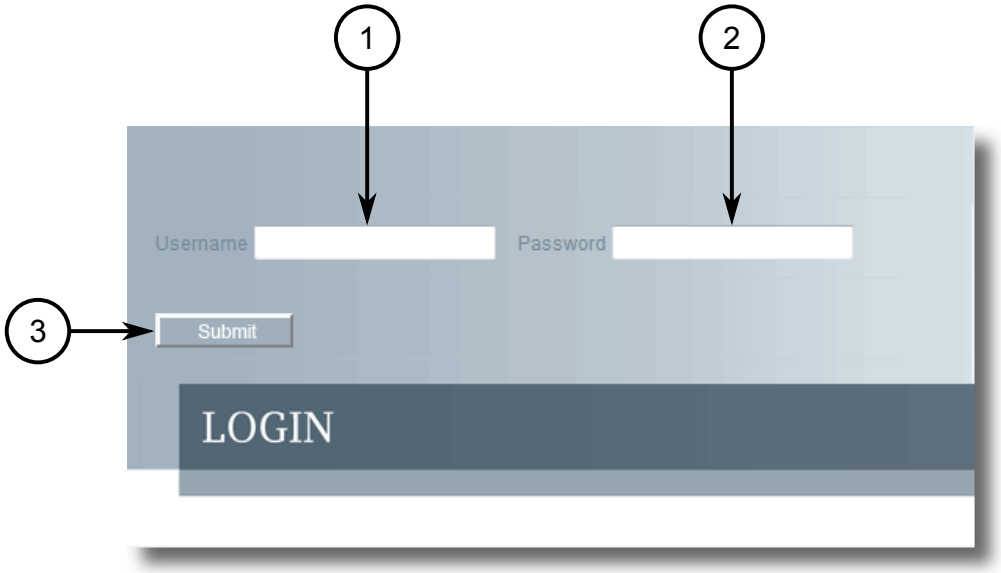
1. Connect to the device either directly or through a Web browser. For more information about how to connect to the device, refer to "Connecting to ROS" (Page 43).

   Once the connection is established, the login form appears.



① User Name box
② Password box

Figure 2.1 SSH login screen (console interface)



① Username box
② Password box
③ Submit button

Figure 2.2 Login screen (web interface)

Note

The following default user name and password is set on the device:

User name	Password
admin	admin

2. In the **User Name** field, type the default user name.
3. In the **Password** field, type the default password, then click **Enter** or click **Submit** (Web interface only). A notification will appear requiring you to change the password.

   For information about creating strong passwords, refer to "Configuring passwords" (Page 129).
4. Follow the prompts to change the password. Once the password is changed, you will automatically be logged out by the system.
5. Log in again using the new credentials.
6. Click **Enter** or click **Submit** (Web interface only).

2.2 Logging in

To log in to the device, do the following:

Note

The default password must be changed at the initial login or following a factory reset.

For more information, refer to "Logging in with default settings" (Page 17).

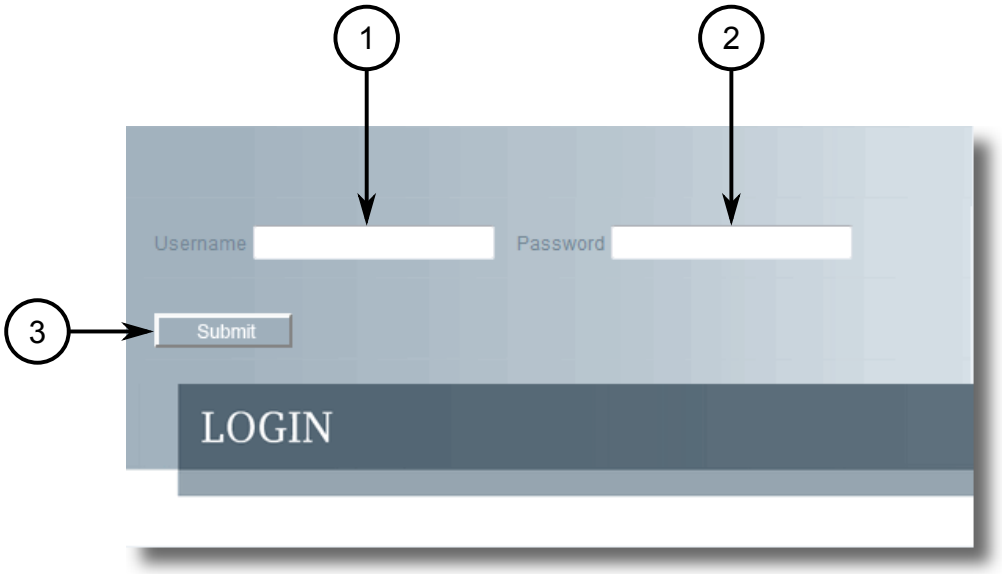
1. Connect to the device either directly or through a Web browser. For more information about how to connect to the device, refer to "Connecting to ROS" (Page 43).

   Once the connection is established, the login form appears.



① User Name box
② Password box

Figure 2.3 SSH login screen (console interface)



① Username box
② Password box
③ Submit button

Figure 2.4 Login screen (web interface)

2. In the **User Name** field, type the user name for an account setup on the device.
3. In the **Password** field, type the password for the account.

4. Click **Enter** or click **Submit** (Web interface only).

2.3 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**.



① Logout

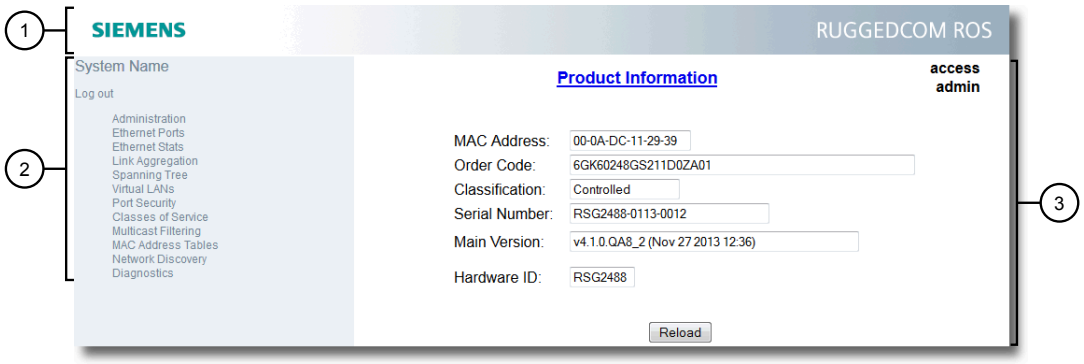
Figure 2.5 Web interface (example)

Note

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

2.4 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.



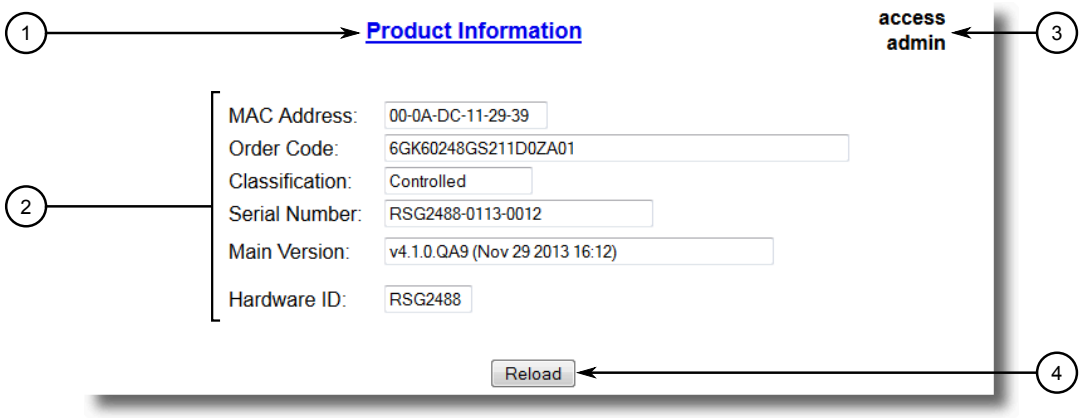
① Top Frame
② Side Frame
③ Main Frame

Figure 2.6 Web Interface Layout (Example)

Frame	Description
Top	The top frame displays the system name for the device.
Side	The side frame contains a logout option and a collapsible list of links that open various screens in the main frame. For information about logging out of RUGGEDCOM ROS, refer to "Logging out" (Page 20).
Main	The main frame displays the parameters and/or data related to the selected feature.

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

When an alarm is generated, an alarm notification replaces the current user's access level on each screen until the alarm is cleared. The notification indicates how many alarms are currently active. For more information about alarms, refer to "Managing alarms" (Page 110).



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

Figure 2.7 Elements of a Typical Screen (Example)

Note

If desired, the web interface can be disabled. For more information, refer to "Enabling/disabling the Web interface" (Page 110).

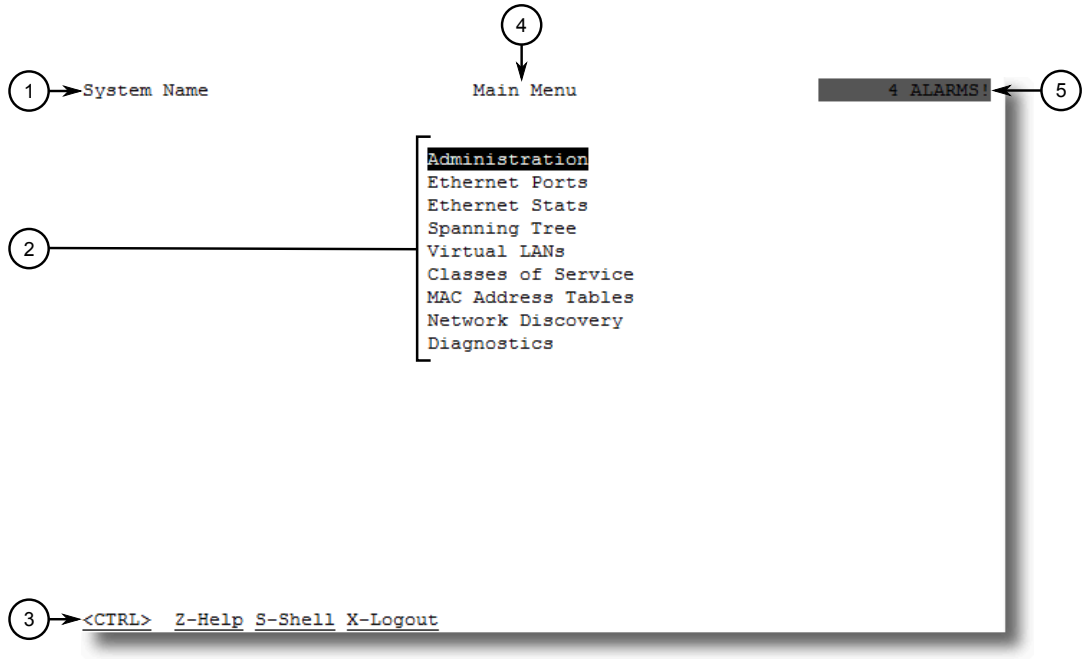
2.5 Using the console interface

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 "Configuring IP services" (Page 94).

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



① System identification
② Menus
③ Command bar
④ Menu name
⑤ Alarms indicator

Figure 2.8 Console interface (example)

Note

The system identifier is user configurable. For more information about setting the system name, refer to "Configuring the system information" (Page 109).

Navigating the interface

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

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

Configuring parameters

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

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

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

Commands

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

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

2.6 Using the command line interface

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

2.6.1 Available CLI commands

The following commands are available at the command line:

Command	Description	Authorized users
`alarms[ latched | active | all ]`	Displays a list of available alarms. Optional and/or required parameters include: • `latched` displays all latched alarms `active` displays all active alarms `all` displays all available alarms	Guest, Operator, Admin
`arp`	Displays the IP to MAC address resolution table.	Admin
`banner { -? } { -c } { -l } { -f }{ -s <enter>{ text } | -s { text } } -e { line_number } -d { line_number }`	Modifies the banner file **banner.txt**. Optional and/or required parameters include: • { -? } Displays the command options help. • { -c } Clears the content of the banner file. • { -l } Displays the banner file with line numbers indexed. • { -f } Restores the factory default banner.	Admin

Command	Description	Authorized users
	• `-s <enter> { text }` Inputs text into the banner file. The existing banner text is erased and replaced by the new text. Accepts up to 8190 characters and supports sets of control characters for editing text. • `-s { text }` Inputs text into the banner file. Can be used to modify the file via terminal. The existing banner text is erased and replaced by the new text. Accepts up to 500 characters, maximum 250 words. • `-e { line_number }` Edits the selected line of the banner file. • `-d { line_number }` Deletes the selected line of the banner file.	
`clearalarms`	Clears all alarms.	Operator, Admin
`clearethstats[ all | { port } ]`	Clears Ethernet statistics for one or more ports. Optional and/or required parameters include: • `all` clears statistics for all ports • { port } is a comma separated list of port numbers (e.g. 1,3-5,7)	Operator, Admin
`clearlogs`	Clears the system and crash logs.	Admin
`clrcblstats[ all | { port } ]`	Clears cable diagnostics statistics for one or more ports. 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)	Admin
`clrstpstats`	Clears all spanning tree statistics.	Operator, Admin
`cls`	Clears the screen.	Guest, Operator, Admin
`dir`	Prints the directory listing of the internal memory.	Guest, Operator, Admin
`exit`	Terminates the session.	Guest, Operator, Admin
`factory`	Enables factory mode, which includes several factory-level commands used for testing and troubleshooting. Only available to admin users. **⚠ NOTICE** **Configuration hazard – risk of firmware corruption** Misuse of the factory commands may corrupt the operational state of device and/or may permanently damage the ability to recover the device without manufacturer intervention.	Admin
`flashfiles{ info { filename } | defrag }`	A set of diagnostic commands to display information about the Flash filesystem and to defragment Flash memory. Optional and/or required parameters include: • `info { filename }` displays information about the specified file in the Flash file system • `defrag` defragments files in the Flash file system For more information about the `flashfiles` command, refer to "Managing the flash file system" (Page 37).	Admin

Command	Description	Authorized users
`flashleds { timeout }`	Flashes the LED indicators on the device for a specified number of seconds. Optional and/or required parameters include: • { timeout } is the number of seconds to flash the LED indicators. To stop the LEDs from flashing, set the timeout period to 0 (zero).	Admin
`fpgacmd`	Provides access to the FPGA management tool for troubleshooting time synchronization.	Admin
`help { command }`	Displays a brief description of the specified command. If no command is specified, it displays a list of all available commands, including a description for each. Optional and/or required parameters include: • { command } is the command name.	Guest, Operator, Admin
`ipconfig`	Displays the current IP address, subnet mask and default gateway. This command provides the only way of determining these values when DHCP is used.	Guest, Operator, Admin
`loaddflts`	Loads the factory default configuration.	Admin
`logout`	Logs out of the shell.	Guest, Operator, Admin
`logs`	Displays syslog entries in CLI shell.	Admin
`passwd { user_name } { new_password }`	Changes the selected user's password. Optional and/or required parameters include: • { user_name } is an existing user_name in RUGGEDCOM ROS. • { new_password } is the new password that will replace the existing password of the selected user. This command is only available in serial console and SSH sessions.	Admin
`ping { address }{ { count } | { timeout } }`	Sends an ICMP echo request to a remotely connected device. For each reply received, the round trip time is displayed. Use this command to verify connectivity to the next connected device. It is a useful tool for testing commissioned links. This command also includes the ability to send a specific number of pings with a specified time for which to wait for a response. Optional and/or required parameters include: • { address } is the target IP address. • { count } is the number of echo requests to send. The default is 4. • { timeout } is the time in milliseconds to wait for each reply. The range is 2 to 5000 seconds. The default is 300 milliseconds. **Note** The device to be pinged must support ICMP echo. Upon commencing the ping, an ARP request for the MAC address of the device is issued. If the device to be pinged is not on the same network as the device pinging the other device, the default gateway must be programmed.	Guest, Operator, Admin
`purgemac`	Purges the MAC Address table.	Operator, Admin

Command	Description	Authorized users
`random`	Display seeds or random numbers.	Admin
`reset`	Perform a hard reset of the switch.	Operator, Admin
`resetport{ all | { ports } }`	Resets one or more Ethernet ports, which may be useful for forcing re-negotiation of speed and duplex, or in situations where the link partner has latched into an inappropriate state. Optional and/or required parameters include: • `all` resets all ports • { ports } is a comma separated list of port numbers (e.g. 1,3-5,7)	Operator, Admin
`rmon`	Displays the names of all RMON alarm eligible objects.	Guest, Operator, Admin
`route`	Displays the gateway configuration.	Guest, Operator, Admin
`sfp { port }{ base | alarms | diag | calibr | thr | all | no 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	Admin
`sql{ default | delete | help | info | insert | save | select | update }`	Provides an SQL-like interface for manipulating all system configuration and status parameters. All commands, clauses, table, and column names are case insensitive. Optional and/or required parameters include: • `default` sets all records in a table(s) to factory defaults • `delete` allows for records to be deleted from a table • `help` provides a brief description for any SQL command or clause • `info` displays a variety of information about the tables in the database • `insert` enables new records to be inserted into a table • `save` saves the database to non-volatile memory storage • `select` queries the database and displays selected records • `update` enable existing records in a table to be updated For more information about the `sql` command, refer to "Using SQL commands" (Page 33).	Admin
`sshdigest`	Displays the host key fingerprints of the device.	Admin
`sshkeygen { keytype } { N }`	Generates new RSA, DSA or ED25519 keys in **ssh.keys**. Optional and/or required parameters include: • { keytype } is the type of key, either rsa, dsa or ED25519 (recommended).	Admin

Command	Description	Authorized users
	• { N } is the number of bits in length. For RSA and DSA keys, the allowable sizes are 1024, 2048 or 3072. For ED25519 keys, the allowable size is 256.	
`sshpubkey`	List, remove and update key entries in sshpub.keys file.	Admin
`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 (recommended). • { 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 256, 384, or 521.	Admin
`svcmod -s { snmpaccess }{ -i { GroupName } | -d { GroupName } } -sm { SecurityModel } -sl { SecurityLevel } -rv { ReadViewName } -wv { WriteViewName } -nv { NotifyViewName }`	Modifies SNMP access groups. Optional and/or required parameters include: • `-i { GroupName }` creates a new access group with a specified group name or modifies parameters associated with a specified access group, if it already exists • `-d { GroupName }` deletes a specified access group • `-sm { SecurityModel }` specifies the security model to be used • `-sl { SecurityLevel }` specifies the SNMP security level to be granted to the specified access group. Allowable values are 'authPriv' (i.e. communication with authentication and privacy), 'authNoPriv' (i.e. communication with authentication and without privacy), or 'noAuthnoPriv' (i.e. communication with neither authentication nor privacy). • `-rv { ReadViewName }` identifies the MIB tree(s) to which this entry authorizes read access. Allowable values are 'noView', 'V1Mib', or 'allOfMib'. • `-wv { WriteViewName }` identifies the MIB tree(s) to which this entry authorizes write access. Allowable values are 'noView', 'V1Mib', or 'allOfMib'. • `-nv { NotifyViewName }` identifies the MIB tree(s) to which this entry authorizes access for notifications. Allowable values are 'noView', 'V1Mib', or 'allOfMib'.	Admin
`svcmod -s { snmpgroup }{ -i { UserName } | -d { UserName } } -sm { SecurityModel } -g { group }`	Modifies SNMP security-to-group maps. Optional and/or required parameters include: • `-i { UserName } -sm { SecurityModel }` creates a new user name and security profile as specified or modifies parameters associated with a specified user name and security profile, if they already exist • `-d { UserName } -sm { SecurityModel }` deletes a specified user name and security profile • `-g { group }` specifies the group to which the user name and secuirty profile belong	Admin
`svcmod -s { snmpuser }{ -i { UserName } | -d { UserName } } -c { Community } -ip { IP } -ap { protocol } -`	Modifies SNMP users. Optional and/or required parameters include:	Admin

Command	Description	Authorized users
`ak { key } -pp { protocol } -pk { key }`	**Note** For the SNMPv3 USM private protocols AES-192 and AES-256, RUGGEDCOM ROS supports the Blumenthal AES algorithm. • `-i { UserName }` creates a new user name as specified or modifies parameters associated with a specified user name, if it already exists • `-d { UserName }` deletes a specified user name • `-c { Community }` specifies the SNMP community string (for SNMPv1 or SNMPv2c). • `-ip { IP }` configures a specified IP address to be used for SNMP authentication • `-ap { protocol }` configures SNMP authetication via a specified authentication protocol. Allowable values are 'noAuth', 'HMACMD5', 'HMACSHA', or 'HMACSHA256' (recommended). • `-ak { key }` sets a secret key (of 0 or 6+ characters) to be used for SNMP authentication • `-pp { protocol }` configures data encryption via a specified privacy protocol. Allowable values are 'noPriv', 'CBC-DES', 'AES-128', 'AES-192', or 'AES-256' (recommended). • `-pk { key }` sets a secret key (of 0 or 6+ characters) to be used for data encryption	
`svcmod -s radius{ -id[ 1 | 2 ] | -ip { IP } | -ak { AuthKey } } -pt { Port } -ux { UsernameExtension } -mr { MaxRetries } -to { timeout } -fma[ yes | no ]`	Modifies RADIUS security server. Optional and/or required parameters include: • `-id { 1 }` selects the specified server as the primary RADIUS server • `-id { 2 }` selects the specified server as the backup RADIUS server • `-id { 1 } -ip` deletes the primary RADIUS server • `-id { 2 } -ip` deletes the backup RADIUS server • `-ip { IP }` specifies the IP address of the RADIUS server • `-ak { AuthKey }` specifies an authentication key to be shared with the RADIUS server • `-pt { Port }` specifies the port number of the IP port on the RADIUS server • `-ux { UsernameExtension }` defines an affix to be added when a user name is sent to the RADIUS server for authentication. Values may include predefined keywords (wrapped in % delimiters) or user-defined strings. Predefined keywords are '%Username%' (i.e. the name associated with the user profile), '%IPaddr%' (i.e. the management IP address of the Network Access Server), '%SysName%' (i.e. the system name given to the device), and '%SysLocation%' (i.e. the phyiscal location of the device). • `-mr { MaxRetries }` specifies the maximum number of times the authenticator will attempt to authenticate a user in the case of any failure. After the specified value is exceeded, authentication fails.	Admin

Command	Description	Authorized users
	• `-to { timeout }` specifies the number of milliseconds (ms) the authenticator will wait for a response from the RADUS server before reattempting authentication. • `-fma [ yes | no ]` enables or disables the Force Message-Authenticator attribute. When set to `yes`, the RADIUS client requires that all Access-Accept, Access-Reject, and Access-Challenge packets contain a Message-Authenticator attribute. If any packet does not contain a Message-Authenticator attribute, then it will be discarded. When set to `no`, the RADIUS client does not require a Message-Authenticator attribute, but will accept and validate the Message-Authenticator attribute if it is present in replies to Access-Request packets.	
`svcmod -s tacacsplus{ -id[ 1 | 2 ] | -ip { IP } | -ak { AuthKey } } -ip { IP } -ak { AuthKey } -pt { Port } -ux { UsernameExtension } -mr { MaxRetries } -to { timeout } -apl { AdminPrivilege } -opl { OperPrivilege } -gpl { GuestPrivilege }`	Modifies TACACS+ security server. Optional and/or required parameters include: • `-id { 1 }` sets the specified server as the primary TACACS+ server • `-id { 2 }` sets the specified server as the backup TACACS+ server • `-id { 1 } -ip` deletes the primary TACACS+ server • `-id { 2 } -ip` deletes the backup TACACS+ server • `-ip { IP }` specifies the IP address of the TACACS+ server • `-ak { AuthKey }` specifies an authentication key to be shared with the TACACS+ server • `-pt { Port }` specifies the port number of the IP port on the TACACS+ server • `-ux { UsernameExtension }` defines an affix to be added when a user name is sent to the TACACS+ server for authentication. Values may include predefined keywords (wrapped in % delimiters) or user-defined strings. Predefined keywords are '%Username%' (i.e. the name associated with the user profile), '%IPaddr%' (i.e. the management IP address of the Network Access Server), '%SysName%' (i.e. the system name given to the device), and '%SysLocation%' (i.e. the phyiscal location of the device). • `-mr { MaxRetries }` specifies the maximum number of times the authenticator will attempt to authenticate a user in the case of any failure. After the specified value is exceeded, authentication fails. • `-to { timeout }` specifies the number of milliseconds (ms) the authenticator will wait for a response from the TACACS+ server before reattempting authentication. • `-apl { AdminPrivilege }` specifies the level to which administrator users are able to configure the TACACS+ server. Values must correspond with one or more option(s) defined numerically (between 0 and 15) in the TACACS+ configuration file. • `-opl { OperPrivilege }` specifies the level to which operator users are able to configure the TACACS+ server. Values must correspond with one or more option(s) defined numerically (between 0 and 15) in the TACACS+ configuration file.	Admin

Command	Description	Authorized users
	• `-gpl { GuestPrivilege }` specifies the level to which guest users are able to configure the TACACS + server. Values must correspond with one or more option(s) defined numerically (between 0 and 15) in the TACACS+ configuration file.	
`telnet { dest }`	Opens a telnet session. Press **Ctrl-C** to close the session. Optional and/or required parameters include: • { dest } is the server's IP address	Guest, Operator, Admin
`tftp { address }[ put | get ] { source } { target }`	Opens a TFTP session. Press **Ctrl-C** to close the session. Optional and/or required parameters include: • { address } is the IP address of the remote TFTP server • `put` indicates TFTP will be uploading the source file to replace the destination file • `get` indicates TFTP will be downloading the source file to replace the destination file • { source } is the name of the source file • { target } is the name of the file that will be replaced	Admin
`trace`	Starts event tracing. Run `trace ?` for more help.	Operator, Admin
`type { filename }`	Displays the contents of a text file. Optional and/or required parameters include: • { filename } is the name of the file to be read	Guest, Operator, Admin
`usermod{ -b | -r { username } | { old_user_name } { new_user_name } }`	A set of commands to display, remove and change existing usernames. Optional and/or required parameters include: • `-b` browses through the existing user names in RUGGEDCOM ROS. • `-r { username }` removes a specified user name to disable the account • { old_user_name } and { new_user_name } define the user name to be changed This command is only available in serial console and SSH sessions.	Admin
`version`	Prints the software version.	Guest, Operator, Admin
`xmodem{ send | receive } { filename }`	Opens an XModem session. Optional and/or required parameters include: • `send` sends the file to the client. • `receive` receives the file from the client. • { filename } is the name of the file to be read.	Operator, Admin

2.6.2 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 "Using the command line interface" (Page 24).
2. Determine the protocols and associated options available by typing:

   ```
   trace ?
   ```

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

   ```
   trace { protocol } ?
   ```

   Note

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

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

   ```
   trace { protocol } { option }
   ```

   Where:

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

   Example:

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

4. Start the trace by typing:

   ```
   trace
   ```

2.6.3 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.

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 "Available CLI commands" (Page 24).

Note

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

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
```

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
```

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
```

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

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:\
```

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.

2.8 Managing the flash file system

This section describes how to manage the file system.

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 "Using the command line interface" (Page 24).
2. Type `flashfiles`. A list of files currently in Flash memory is displayed, along with their locations and the amount of memory they consume. For example:

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

2.8.2 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 "Using the command line interface" (Page 24).
2. Display information about a file by typing:

   ```
   flashfiles info { filename }
   ```

   Where:

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

   Details, similar to the following, are displayed.

```
>flashfiles info main.bin

Flash file information for main.bin:
Header version   : 4
Platform         : ROS-MPC83
File name        : main.bin
Firmware version : v5.10.0
Build date       : Sep 27 2014 15:50
File length      : 2624659
Board IDs        :  3d
Header CRC       : 73b4
Header CRC Calc  : 73b4
Body CRC         : b441
Body CRC Calc    : b441
```

2.8.3 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.

⚠ NOTICE

Take precautions to avoid power interruption during the defragmentation process. If power is interrupted during the process, the device may be rendered inaccessible.

To defragment the flash memory, do the following:

1. Log in to the device as an admin user and access the CLI shell. For more information about accessing the CLI shell, refer to "Using the command line interface" (Page 24).
2. Defragment the flash memory by typing:

```
flashfiles defrag
```

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.

⚠ NOTICE

Mechanical hazard – risk of damage to the device

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

To access BIST mode, do the following:

⚠ NOTICE

Configuration hazard – risk of communication disruption

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

1. Disconnect the device from the network.
2. Connect to RUGGEDCOM ROS through the RS-232 console connection and a terminal application. For more information, refer to "Connecting directly" (Page 43).

3. Reset the device. For more information, refer to "Rebooting the device" (Page 105).
4. During the boot up sequence, press **Ctrl-C** when prompted. The command prompt for BIST appears.

```
>
```

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

Alternatively, BIST functions can be accessed via factory mode. For more information about factory mode, refer to "Available CLI commands" (Page 24).

2.10 Managing access to the boot loader interface

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

Note

Access to the boot loader interface is disabled at the factory by default on all devices running RUGGEDCOM ROS v5.10. All console inputs are ignored and users are directed automatically to the RUGGEDCOM ROS user interface.

Note

Siemens recommends disabling access to the boot loader interface following an upgrade from an earlier version of RUGGEDCOM ROS to RUGGEDCOM ROS v5.10. For more information about disabling the boot loader, refer to "Enabling/disabling access to the boot loader interface" (Page 40).

2.10.1 Enabling/disabling access to the boot loader interface

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

Create file bootoption.txt

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

If the file is not available, do the following:

1. Using a PC/laptop, create a file named **bootoption.txt**.

⚠ NOTICE

If the *Security* parameter is either commented out using the hash (#) character or does not exist in the file, it will be created by RUGGEDCOM ROS with its default value following reboot.

2. Include the following line in the file:

```
Security = [No | Yes]
```

   - *Security = No* enables access to the boot loader.
   - *Security = Yes* disables access to the boot loader. This is the default value.

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

Enabling the boot loader

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

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

```
Security = Yes
```

   to

```
Security = No
```

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

Disabling the boot loader

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

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

```
Security = No
```

   to

```
Security = Yes
```

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

2.10.2 Accessing the boot loader interface

To access the boot loader interface, do the following:

1. Connect to RUGGEDCOM ROS through the RS-232 console connection and a terminal application. For more information, refer to "Connecting directly" (Page 43).
2. Reset the device. For more information, refer to "Rebooting the device" (Page 105).

3. As soon as the device starts to boot up, press **Ctrl-Z**. The command prompt for Uboot appears.

```
=>
```

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

2.11 Enabling/disabling the console service

The local console service is enabled by default in RUGGEDCOM ROS. For added security, an admin user can disable and re-enable access to the console as desired.

Note

Enabling/disabling the console service is only available using SQL commands. For more information, refer to "Using SQL commands" (Page 33).

To enable/disable access to the console service, do the following:

1. Log in to the device as an admin user and access the CLI shell. For more information about accessing the CLI shell, refer to "Using the command line interface" (Page 24).
2. **⚠ NOTICE**

   To disable the console service, at least one SSH session must be enabled. For more information about enabling SSH access, refer to "Configuring IP services" (Page 94).

   Enable or disable the console service by typing either:

   Enabling

   ```
   sql update consoleServices SET Local Console Service =
   Enabled
   ```

   Disabling

   ```
   sql update consoleServices SET Local Console Service =
   Disabled
   ```

The changes will take effect immediately on the next local console login.

3 Getting started

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

⚠ NOTICE
Security hazard – risk of unauthorized access and/or exploitation
Siemens recommends the following actions before commissioning the device: • Replace the factory-provisioned, self-signed TLS certificate with one signed by a trusted Certificate Authority (CA) • Configure the SSH client to use *diffie-hellman-group14-sha1* or better

3.1 Connecting to ROS

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

3.1.1 Default IP address

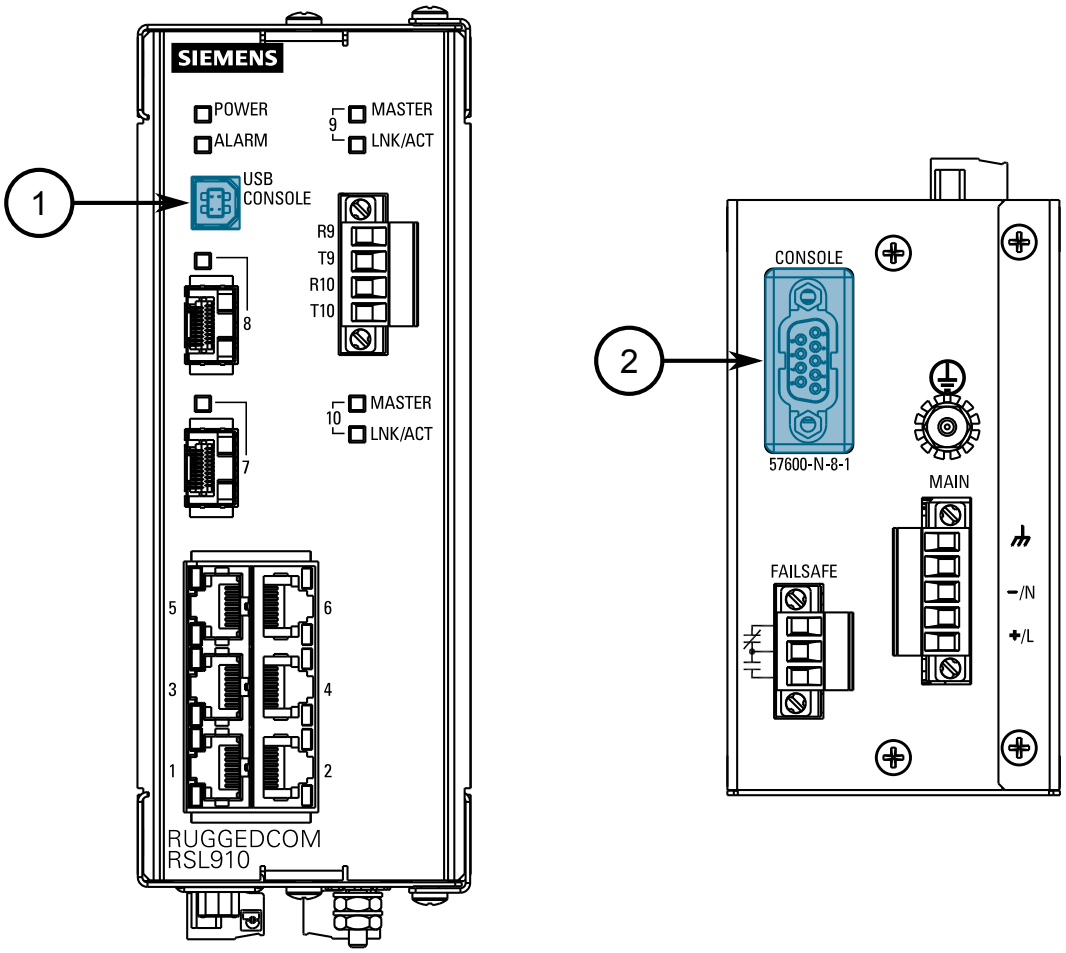
The default IP address for the device is 192.168.0.1/24.

3.1.2 Connecting directly

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

Using the console port

The RUGGEDCOM RSL910 features both a DB9 port and a USB Type-B port for establishing a console connection.



① USB Type-B Console Port
② Serial Console Port

Figure 3.1 Console Ports

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

Note

For Microsoft Windows users, the RUGGEDCOM USB Serial Console driver must be installed on the users workstation before connecting via the USB Type-B console port. For more information, refer to "Installing the RUGGEDCOM USB serial console driver (Windows only)" (Page 47).

Note

When the USB Type-B console port is in use, the serial console port will echo the console output but not accept any user input.

1. Connect a workstation (either a terminal or computer running terminal emulation software) to the DB9 or USB Type-B console port on the device.

For more information about the RS-232 serial console ports, refer to the "RUGGEDCOMRSL910 Equipment Manual".

Note

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

Note

The baud rate for the device is printed on the chassis exterior near the DB9 port.

2. Configure the workstation as follows:
   - Speed (baud): 57600
   - Data Bits: 8
   - Parity: None
   - Flow Control: Off
   - Terminal ID: VT100
   - Stop Bit: 1
3. Connect to the device. Once the connection is established, the login form appears. For more information about logging in to the device, refer to "Logging in" (Page 19).

3.1.3 Connecting remotely

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

Using a Web browser

Web browsers provide a secure connection to the Web interface for RUGGEDCOM ROS using the TLS (Transport Layer Security) communication method. TLS 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 TLS will only be granted to clients that provide a valid user name and password.

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

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

   For example, to configure the device to connect to one of the available Ethernet ports, assign an IP address to the Ethernet port on the workstation in the range of 192.168.0.3 to 192.168.0.254.

2. Open a Web browser. For a list of recommended Web browsers, refer to "System requirements" (Page xvi).

⚠ NOTICE
Upon connecting to the device, some Web browsers may report the Web server's certificate cannot be verified against any known certificates. For secure access, please generate and provision a custom TLS certificate. For more information, refer to "Managing SSH/TLS keys and certificates" (Page 150).

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

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

   For more information about logging in to the device, refer to "Logging in" (Page 19). For more information about the Web interface, refer to "Using the Web interface" (Page 20).

Using a terminal or terminal emulation software

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

Note

IP services can be restricted to control access to the device. For more information, refer to "Configuring IP services" (Page 94).

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

1. Select the service (i.e. Telnet, RSH or SSH).
2. Enter the IP address for the port that is connected to the network.
3. Connect to the device. Once the connection is established, the login form appears. For more information about logging in to the device, refer to "Logging in" (Page 19).

3.2 Installing the RUGGEDCOM USB serial console driver (Windows only)

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

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

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

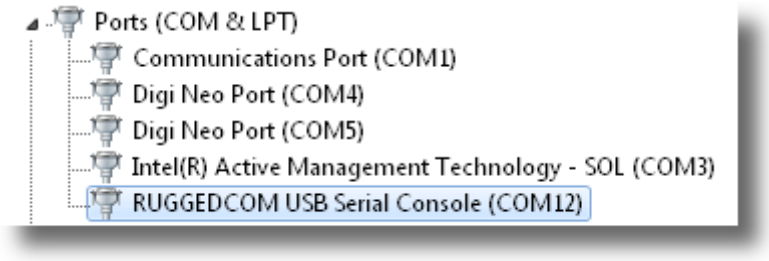


Figure 3.2 RUGGEDCOM USB Serial Console Port

3.3 Configuring a basic network

To configure a basic network, do the following:

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

4 Device management

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

4.1 Viewing product information

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

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

This screen displays the following information:

Parameter	Description
`MAC Address`	**Synopsis:** ##-##-##-##-##-## where ## ranges 0 to FF Shows the unique MAC address of the device.
`Order Code`	**Synopsis:** A string up to 57 characters long Shows the order code of the device.
`Classification`	**Synopsis:** A string up to 15 characters long Provides system classification. The value **Controlled** indicates the main firmware is a Controlled release. The value **Non-Controlled** indicates the main firmware is a Non-Controlled release. The **Controlled** main firmware can run on Controlled units, but it can not run on Non-Controlled units. The **Non-Controlled** main firmware can run on both Controlled and Non-Controlled units.
`Serial Number`	**Synopsis:** A string up to 31 characters long Shows the serial number of the device.
`Main Version`	**Synopsis:** A string up to 47 characters long Shows the version and build date of the main operating system software.
`Hardware ID`	Shows the type, part number, and revision level of the hardware. Example:RSL910,RSL910v2

Parameter	Description
`Descr`	**Synopsis:** A string up to 57 characters long The description of product based on Hardware ID, order code and classification.

4.2 Viewing CPU diagnostics

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

This screen displays the following information:

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

4.3 Restoring factory defaults

The device can be completely or partially restored to its original factory default settings. Excluding groups of parameters from the factory reset, such as those that

affect basic connectivity and SNMP management, is useful when communication with the device is still required during the reset.

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

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

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

- Time Zone
- DST Offset
- DST Rule

To restore factory defaults, do the following:

1. Navigate to ***Diagnostics » Load Factory Defaults***. The **Load Factory Defaults** form appears.
2. Configure the following parameter(s) as required:

   Note

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

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

3. Click **Apply**.

4.4 Uploading/downloading files

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

- Xmodem using the CLI shell over a Telnet, SSH 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

Note

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.

RUGGEDCOM ROS will generate an SNMP trap and log a message in the syslog to indicate the transfer details and status when files are transferred to or from a remote computer or external media.

Files that may need to be uploaded or downloaded include:

- **main.bin** – the main RUGGEDCOM ROS application firmware image (e.g. **ROS-MPC83_v5.10.0.zb**)
- **boot.bin** – the boot loader firmware 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
- **sshpub.key** – the public keys for user authentication

  Note

  Public keys can only be uploaded to the **sshaddpub.keys** file. For more information about uploading a public key, refer to "Adding a public key" (Page 155).

- **ssl.crt** – the TLS certificate (uploadable only). Contains both the TLS certificate and the corresponding RSA private key file.
- **ssh.keys** – the SSH keys for the device (uploadable only)

4.4.1 Uploading/downloading files using XMODEM

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

Note

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

1. Establish a connection between the device and the host computer. For more information, refer to "Connecting to ROS" (Page 43).
2. Log in to the device as an admin user and access the CLI shell. For more information about accessing the CLI shell, refer to "Using the command line interface" (Page 24).
3. At the CLI prompt, type:

   `xmodem[ send | receive ] { filename }`

   Where:

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

   Note

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

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

   Note

   When SSH is used to establish a connection between the RSL910 device and the host computer, XMODEM can take a long time to download an image.

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

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

5. Once the file has been uploaded, reset the device. For more information, refer to "Rebooting the device" (Page 105).

4.4.2 Uploading/downloading files using a TFTP client

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

⚠ NOTICE

Security hazard – risk of unauthorized access and/or exploitation

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

Note

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

1. Identify the IP address of the computer running the TFTP server.
2. Establish a connection between the device and the host computer. For more information, refer to "Connecting to ROS" (Page 43).
3. Log in to the device as an admin user and access the CLI shell. For more information about accessing the CLI shell, refer to "Using the command line interface" (Page 24).
4. At the CLI prompt, type:

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

   Where:

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

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

   ```
   >tftp 10.0.0.1 get ROS-MPC83_Main_v5.10.0.zb main.bin
    TFTP CMD: main.bin transfer ok. Please wait, closing file ...
    TFTP CMD: main.bin loading successful.
   ```

5. Once the file has been uploaded, reset the device. For more information, refer to "Rebooting the device" (Page 105).

4.4.3 Uploading/downloading files using a TFTP server

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

⚠ NOTICE

Security hazard – risk of unauthorized access and/or exploitation

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

1. Establish a connection between the device and the host computer. For more information, refer to "Connecting to ROS" (Page 43).
2. Initialize the TFTP server on the device and launch the TFTP transfer. The server will indicate when the transfer is complete.

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

```
C:\>tftp -i 10.1.0.1 put C:\files\ROS-MPC83_Main_v5.10.0.zb main.bin
     Transfer successful: 1428480 bytes in 4 seconds, 375617 bytes/s
```

3. Once the file has been uploaded, reset the device. For more information, refer to "Rebooting the device" (Page 105).

4.4.4 Uploading/downloading files using an SFTP server

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

Note

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

To upload 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-MPC83_Main_v5.10.0.zb main.bin
Uploading ROS-MPC83_Main_v5.10.zb to /main.bin
ROS-MPC83_Main_v5.10.0.zb 100% 2139KB 48.6KB/s 00:44
sftp>
```

3. the file has been uploaded, reset the device. For more information, refer to "Rebooting the device" (Page 105).

4.5 Managing logs

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

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

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

4.5.1 File storage capacity

The device has the following log storage capacities:

File	Description	Capacity
syslog.txt	Storage size	1.75 MB (1,835,008 bytes)
	Maximum entry size	400 bytes
	Minimum entries	~4,500 entries
crashlog.txt	Storage size	256 KB (262,144 bytes)
	Maximum entry size	~800 bytes
	Minimum entries	~320 entries

4.5.2 Viewing local and system logs

The local crash and system logs can both be downloaded from the device and viewed in a text editor. For more information about downloading log files, refer to "Uploading/downloading files" (Page 51).

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

4.5.3 Clearing local and system logs

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

```
clearlogs
```

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

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

4.5.4 Configuring the local system log

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

Note

For maximum reliability, use remote logging. For more information, refer to "Managing remote logging" (Page 57).

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

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

3. Click **Apply**.

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

4.5.5.1 Syslog format

RUGGEDCOM ROS supports both the RFC 3164 and RFC 5424 syslog formats, used to convey event notification messages.

As RFC 3164 has been obsoleted by RFC 5424, this section focuses on the RFC 5424 format.

Each RFC 5424 compliant remote syslog message is divided into three parts, as follows:

- Header
- Structured-Element
- Message

Header

The message header includes the following fields:



Figure 4.1 Message Header Fields

Field	Description
PRI	The Priority value (PRIVAL) represents both the Facility and Severity. PRIVAL = (Facility * 8) + Severity.
VERSION	The version of the RFC 5424 syslog protocol (e.g. "1").
SP	This field is used to represent an ASCII Space.
TS	The timestamp, in format YYYY-MM-DDTHH-MM-SSuZ. Example: "2020-10-06T20:14:47.476406-5:00" represents 6th October 2020 at 08:14:47pm, 476406 microseconds into the next second. The timestamp indicates that its local time is -5 hours from UTC.
HN	The host name. It is set to either the static or dynamic IP Address of the device (depending on the IP address type selected by the user during interface configuration). When no dynamic address is assigned to the device, a NILVALUE (i.e. "-") is used to denote the field.
AN	The APP-NAME. The device chassis type is used for this field. For example, "RSL910".
PID	The process ID.
MID	The message ID.

Structured-Element

A Structured-Element consists of name and parameter-value pairs in format "["SD-ID SP SD-PARAM) "]". The name is referred to as SD-ID. The parameter-value pairs are referred to as "SD-PARAM".

In RUGGEDCOM ROS, Time Quality information is being sent using "timeQuality" SD-ID and 2 parameter-value pairs:

- **tzKnown**: Indicates whether or not the originator knows its time zone. As RUGGEDCOM ROS is time zone aware, tzKnown is always set as "1".

- **isSynced**: Indicates whether or not the originator is synchronized to a reliable external time source. A value of "1" indicates that an external clock master has been selected as the time source and synchronization between the master and the slave has been achieved. A value of "0" indicates that the local clock is selected as the time source.

Message

The message contains a free-form message that provides information about the event.

Examples

The following message indicates the time source is configured to the local clock:

```
<190>1 2020-10-08T23:48:57.582209-5:00 192.168.2.102 RSG2488 - - [timeQuality
tzKnown="1" isSynced="0"] RemoteSyslog update collector 192.168.2.101
```

The following message indicates the time source is configured to an external clock:

```
<190>1 2020-10-08T23:40:31.534206-5:00 192.168.2.102 RSG2488R - - [timeQuality
tzKnown="1" isSynced="1"] RemoteSyslog update collector 192.168.2.101
```

For more information about configuring the syslog format, refer to "Adding a remote syslog server" (Page 60).

4.5.5.2 Configuring the remote syslog client

To configure the remote syslog client, do the following:

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

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

3. Click **Apply**.

4.5.5.3 Viewing a list of remote syslog servers

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

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

4.5.5.4 Adding a remote syslog server

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

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

1. Navigate to ***Administration » Configure Syslog » Configure Remote Syslog Server***. The **Remote Syslog Server** table appears.
2. Click **InsertRecord**. The **Remote Syslog Server** form appears.
3. Configure the following parameter(s) as required:

Parameter	Description
`IP Address`	**Synopsis:** Any valid IP address Syslog server IP Address.
`UDP Port`	**Synopsis:** An integer between 1025 and 65535 or [514] **Default:** 514 The UDP port number on which the remote server listens.
`Facility`	**Synopsis:** [USER | LOCAL0 | LOCAL1 | LOCAL2 | LOCAL3 | LOCAL4 | LOCAL5 | LOCAL6 | LOCAL7] **Default:** LOCAL7 The application or operating system component that generates a log message. RUGGEDCOM ROS maps all syslog logging information to a single facility, configurable by the user.
`Severity`	**Synopsis:** [EMERGENCY | ALERT | CRITICAL | ERROR | WARNING | NOTICE | INFORMATIONAL | DEBUGGING] **Default:** DEBUGGING The severity of the generated message. The selected severity level is considered the minimum severity level for the system. For example, if 'ERROR' is selected, then the system will send any syslog message having the severity level ERROR, CRITICAL, ALERT and EMERGENCY.

Parameter	Description
`Format`	**Synopsis:** [RFC3164 | RFC5424] **Default:** RFC3164 The format of syslog messages which are sent to the remote syslog server.
`Reachable`	**Synopsis:** [--- | Yes | No] The status of the server. Options include: • **---** – The server probe is disabled or the server status is unknown • **Yes** – The server is reachable • **No** – The server is unreachable
`Probe Period`	**Synopsis:** An integer between 1 and 1440 **Default:** 5 Determines how frequently in minutes the Remote Syslog server is polled for reachability when the Probe Method is ICMP.
`Probe Method`	**Synopsis:** [Disabled | ICMP] **Default:** Disabled Determines the protocol used to probe the Remote Syslog server reachability or disables the reachability check. Options include: • **Disabled** – Disables the reachability check • **ICMP** – The server probe uses ICMP ping. Three consecutive ICMP ping requests with a 500-millisecond timeout are sent to the server until a response is received. If no response received, a server unreachable alarm is generated.

4. Click **Apply**.

4.5.5.5 Deleting a remote syslog server

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

1. Navigate to ***Administration » Configure Syslog » Configure Remote Syslog Server***. The **Remote Syslog Server** table appears.
2. Select the server from the table. The **Remote Syslog Server** form appears.
3. Click **Delete**.

4.6 Managing Ethernet ports

This section describes how to manage Ethernet ports.

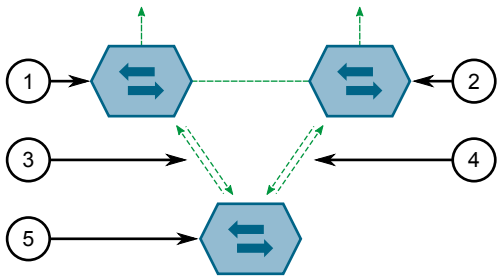
Note

For information about configuring remote monitoring for Ethernet ports, refer to "Managing remote monitoring" (Page 96).

4.6.1 Controller protection through Link Fault Indication (LFI)

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

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



① Switch A
② Switch B
③ Main transmit path
④ Backup transmit path
⑤ Controller

Figure 4.2 Example

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

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

100Base-TX, 1000Base-T, 1000Base-X	Includes a built-in auto-negotiation feature (i.e. a special flag called Remote Fault Indication is set in the transmitted auto-negotiation signal).
100Base-FX Links	Includes a standard Far-End-Fault-Indication (FEFI) feature defined by the IEEE 802.3 standard for this link type. This feature includes: • **Transmitting FEFI** Transmits a modified link integrity signal in case a link failure is detected (i.e. no link signal is received from the link partner)

	• **Detecting FEFI** Indicates link loss in case an FEFI signal is received from the link partner
10Base-FL LInks	No standard support.

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

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

⚠ NOTICE

Configuration hazard – risk of communication disruption

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

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

4.6.2 Viewing the status of Ethernet ports

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

This table displays the following information:

Parameter	Description
`Port`	**Synopsis:** 1 to maximum port number The port number.
`Name`	**Synopsis:** A string up to 15 characters long A descriptive name that may be used to identify the device connected on that port.
`Link`	**Synopsis:** [---- | Down | Up] The port's link status.
`Speed`	**Synopsis:** [--- | 10M | 100M | 1G | 10G] The port's current speed.

Parameter	Description
`Duplex`	**Synopsis:** [---- | Half | Full] The port's current duplex status.

4.6.3 Viewing statistics for all Ethernet ports

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

This table displays the following information:

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

4.6.4 Viewing statistics for specific Ethernet ports

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

This table displays the following information:

Parameter	Description
`Port`	**Synopsis:** 1 to maximum port number The port number.

Parameter	Description
InOctets	**Synopsis:** An integer between 0 and 18446744073709551615 The number of octets in received good packets (Unicast+Multicast +Broadcast) and dropped packets.
OutOctets	**Synopsis:** An integer between 0 and 18446744073709551615 The number of octets in transmitted good packets.
InPkts	**Synopsis:** An integer between 0 and 18446744073709551615 The number of received good packets (Unicast+Multicast +Broadcast) and dropped packets.
OutPkts	**Synopsis:** An integer between 0 and 18446744073709551615 The number of transmitted good packets.
TotalInOctets	**Synopsis:** An integer between 0 and 18446744073709551615 The total number of octets of all received packets. This includes data octets of rejected and local packets which are not forwarded to the switching core for transmission. It should reflect all the data octets received on the line.
TotalInPkts	**Synopsis:** An integer between 0 and 18446744073709551615 The number of received packets. This includes rejected, dropped local, and packets which are not forwarded to the switching core for transmission. It should reflect all packets received ont the line.
InBroadcasts	**Synopsis:** An integer between 0 and 18446744073709551615 The number of good Broadcast packets received.
InMulticasts	**Synopsis:** An integer between 0 and 18446744073709551615 The number of good Multicast packets received.
CRCAlignErrors	**Synopsis:** An integer between 0 and 4294967295 The number of packets received which meet all the following conditions: • Packet data length is between 64 and 1536 octets inclusive • Packet has invalid CRC • Collision Event has not been detected • Late Collision Event has not been detected
OversizePkts	**Synopsis:** An integer between 0 and 4294967295 The number of packets received with data length greater than 1536 octets and valid CRC.
Fragments	**Synopsis:** An integer between 0 and 4294967295 The number of packets received which meet all the following conditions: • Packet data length is less than 64 octets, or packet without SFD and is less than 64 octets in length

Parameter	Description
	• Collision Event has not been detected • Late Collision Event has not been detected • Packet has invalid CRC
`Jabbers`	**Synopsis:** An integer between 0 and 4294967295 The number of packets which meet all the following conditions: • Packet data length is greater that 1536 octets • Packet has invalid CRC
`Collisions`	**Synopsis:** An integer between 0 and 4294967295 The number of received packets for which Collision Event has been detected.
`LateCollisions`	**Synopsis:** An integer between 0 and 4294967295 The number of received packets for which Late Collision Event has been detected.
`Pkt64Octets`	**Synopsis:** An integer between 0 and 4294967295 The number of received and transmitted packets with size of 64 octets. This includes received and transmitted packets as well as dropped and local received packets. This does not include rejected received packets.
`Pkt65to127Octets`	**Synopsis:** An integer between 0 and 4294967295 The number of received and transmitted packets with size of 65 to 127 octets. This includes received and transmitted packets as well as dropped and local received packets. This does not include rejected received packets.
`Pkt128to255Octets`	**Synopsis:** An integer between 0 and 4294967295 The number of received and transmitted packets with size of 128 to 257 octets. This includes received and transmitted packets as well as dropped and local received packets. This does not include rejected received packets.
`Pkt256to511Octets`	**Synopsis:** An integer between 0 and 4294967295 The number of received and transmitted packets with size of 256 to 511 octets. This includes received and transmitted packets as well as dropped and local received packets. This does not include rejected received packets.
`Pkt512to1023Octets`	**Synopsis:** An integer between 0 and 4294967295 The number of received and transmitted packets with size of 512 to 1023 octets. This includes received and transmitted packets as well as dropped and local received packets. This does not include rejected received packets.
`Pkt1024to1536Octets`	**Synopsis:** An integer between 0 and 4294967295 The number of received and transmitted packets with size of 1024 to 1536 octets. This includes received and transmitted packets as

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

4.6.5 Clearing statistics for specific ethernet ports

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

1. Navigate to ***Ethernet Stats » Clear Ethernet Port Statistics***. The **Clear Ethernet Port Statistics** form appears.
2. Select one or more Ethernet ports.
3. Click **Apply**.

4.6.6 Configuring an Ethernet port

To configure an Ethernet port, do the following:

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

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

Parameter	Description
`Name`	**Synopsis:** A string up to 15 characters long **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`	**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`	**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.

Parameter	Description
`LFI`	**Synopsis:** [Off | On] **Default:** Off Enabling Link-Fault-Indication (LFI) inhibits transmitting link integrity signal when the receive link has failed. This allows the device at far end to detect link failure under all circumstances. **Note** This feature must not be enabled at both ends of a fiber link.
`Alarm`	**Synopsis:** [On | Off] **Default:** On Disabling link state alarms will prevent alarms and LinkUp and LinkDown SNMP traps from being sent for that port.
`Act on LinkDown`	**Synopsis:** [Do nothing | Admin Disable] **Default:** Do nothing The action to be taken upon a port LinkDown event. Options include: • **Do nothing** – No action is taken. • **Admin Disable** – The port state is disabled. The State parameter must be set to Enabled before the link can be restored.
`Downshift`	**Synopsis:** [Disabled | Enabled] **Default:** Enabled Enable or disable auto-negotiation on a gigabit (1000BASE-T) port with a two-pair twisted cable. If this option is enabled, the device is able to auto-negoatiate with another 1000BASE-T link partner using a two-pair cable and establish a link at 100Mbps or 10Mbps.
`UnidirectionalMode`	**Synopsis:** [Disabled | TX-Only] **Default:** Disabled Sets the Unidirectional Mode on a port. Options include: • **Disabled** – The port behaves normally with no unidirectional mode support. If the RX strand of the cable is removed, there is no link to the partner. • **TX-Only** – The port is forced into a Link-Up state and is able to transmit data, even if the RX strand is removed. **Note** This parameter only applies to fiber ports.

Note

If one end of the link is fixed to a specific speed and duplex type and the peer auto-negotiates, there is a strong possibility the link will either fail to raise, or

raise with the wrong settings on the auto-negotiating side. The auto-negotiating peer will fall back to half-duplex operation, even when the fixed side is full duplex. Full-duplex operation requires that both ends are configured as such or else severe frame loss will occur during heavy network traffic. At lower traffic volumes the link may display few, if any, errors. As the traffic volume rises, the fixed negotiation side will begin to experience dropped packets, while the auto-negotiating side will experience excessive collisions. Ultimately, as traffic load approaches 100%, the link will become entirely unusable. These problems can be avoided by always configuring ports to the appropriate fixed values.

4. Click **Apply**.

4.6.7 Configuring port rate limiting

To configure port rate limiting, do the following:

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

⚠ NOTICE

Configuration hazard – risk of data loss

When configuring EoVDSL ports, make sure **Egress Limit** is lower than the link rate configured for the EoVDSL port at the other end of the EoVDSL link. If the egress limit is higher than the link rate, packets will be dropped.

Parameter	Description
`Port`	The port number.
`Ingress Limit`	The rate after which received frames (of the type described by the ingress frames parameter) will be discarded by the switch.
`Ingress Frames`	**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 are limited
`Egress Limit`	**Default:** Disabled The maximum rate at which the switch will transmit (multicast, broadcast and unicast) frames on this port. The switch will discard frames in order to meet this rate if required.

4. Click **Apply**.

4.6.8 Configuring link detection

To configure link detection, do the following:

1. Navigate to ***Ethernet Ports » Configure Link Detection***. The **Link Detection** form appears.
2. Configure the following parameter(s) as required:

Note

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

Parameter	Description
`Fast Link Detection`	**Synopsis:** [Off | On | On_withPortGuard] **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: • **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. • **On** – In certain special cases where a prolonged excessive link state changes constitute a legitimate link operation, using this setting can prevent Port Guard from disabling FAST LINK DETECTION on the port in question. If excessive link state changes persist for more than 2 minutes, an alarm will be generated to warn user about the observed bouncing link. If the excessive link state changes condition is resolved later on, the alarm will be cleared automatically. Since this option does not disable FAST LINK DETECTION, a persistent bouncing link could continue affect the system in terms of response time. This setting should be used with caution. • **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,

Parameter	Description
	the port will need a longer time to detect a link failure. This may result in a longer network recovery time of up to 2s. Once Port Guard disables FAST LINK DETECTION of a particular port, user can re-enable FAST LINK DETECTION on the port by clearing the alarm.
`Link Detection Time`	**Synopsis:** An integer between 100 and 1000 **Default:** 100 The time that the link has to continuously stay up before the "link up" decision is made by the device. (The device performs de-bouncing of Ethernet link detection to avoid multiple responses to an occasional link bouncing event, e.g. when a cable is shaking while being plugged-in or unplugged).

3. Click **Apply**.

4.6.9 Traffic mirroring

Traffic mirroring is a Layer 2 feature that allows the duplication of one or more traffic streams for the purpose of traffic monitoring and analysis. Mirrored traffic is forwarded to an external packet analyzer/sniffer. Network administrators and engineers analyse the traffic to detect intrusions, troubleshoot/debug errors, and monitor the overall performance of the network.

4.6.9.1 Configuring traffic mirroring

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

⚠ NOTICE

Configuration hazard – risk of communication disruption

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

⚠ NOTICE

Configuration hazard – risk of communication disruption

Frames will be dropped if the full-duplex rate of frames on the source port exceeds the transmission speed of the target port. Since both transmitted and received frames on the source port are mirrored to the target port, frames will be discarded if the sum traffic exceeds the target port's transmission rate. This problem reaches its

extreme in the case where traffic on a 100 Mbps full-duplex port is mirrored onto a 10 Mbps half-duplex port.

⚠ NOTICE

Before configuring traffic mirroring, note the following:

- When local port mirroring is enabled, by default, RUGGEDCOM ROS blocks ingress frames on the target port from being switched. Management service traffic such as SNMP and SSH is blocked. However, other network management traffic such as RSTP, MRP, PTP, and LLDP is allowed.
- The target port of the local port mirroring feature cannot be used to authenticate connected devices through 802.1x or manage a RUGGEDCOM ROS device through SSH, Telnet, RSH or Web UI.
- Traffic will be mirrored onto the target port irrespective of its VLAN membership. It could be the same as or different from the source port's membership.
- Network management frames (such as RSTP, GVRP etc.) cannot be mirrored.
- Switch management frames generated by the switch (such as Telnet, HTTP, SNMP, etc.) cannot be mirrored.
- EoVDSL ports cannot be set as target ports for port mirroring.

Note

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

To configure traffic mirroring, do the following:

1. Navigate to ***Ethernet Ports » Configure Traffic Mirroring***. The **Traffic Mirroring** form appears.
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/or transmitted by the source port(s) to be transmitted out of the target port, or to be re-tagged to the target VID and then re-switched on the target VID (if supported by the device).
`Source Ports Egr`	**Synopsis:** Comma-separated list of ports **Default:** None Traffic egressing these ports will be monitored.

Parameter	Description
`Source Ports Ingr`	**Synopsis:** Comma-separated list of ports **Default:** None Traffic ingressing these ports will be monitored.
`Target Port`	**Synopsis:** 1 to maximum port number or { None } **Default:** None The port where a monitoring device should be connected.
`Mirror Guard`	**Synopsis:** [Disabled | Enabled] **Default:** Enabled This parameter controls the treatment of ingress traffic on the Target Port when Local Port Mirroring is enabled. Options include: • **Enabled** – Port level VLAN Ingress Filtering is automatically enabled on the Target Port regardless of other configuration settings. Ingress data plane traffic on the Target Port is blocked. • **Disabled** – Port level VLAN Ingress Filtering is not automatically enabled on the Target Port. Ingress Filtering can be enabled or disabled using other VLAN configuration parameters. Ingress data plane traffic on the Target Port may egress other switch ports, and may be directed to the CPU. **Note** Control Plane traffic (including, but not limited to RSTP and LLDP) will not be blocked on the Target Port.

3. Click **Apply**.

4.6.10 Managing SFP transceivers

RUGGEDCOM ROS supports Small Form-factor Pluggable (SFP) transceivers.

Digital Diagnostic Monitoring (DDM) is supported on devices equipped with SFP ports. DDM is disabled by default, and can be enabled by configuring the polling interval. When enabled, installed SFP transceivers are monitored for temperature, voltage, Tx bias current, Rx power and Tx power. An alarm is generated when a specific measured parameter exceeds its threshold.

For more information about alarms, refer to "Managing alarms" (Page 110).

Note

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

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

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

Note

SFP transceivers are hot swappable.

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

4.6.10.1 SFP transceiver requirements

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

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

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

For more information about configuring SFP transceiver ports and other Ethernet ports on the device, refer to "Configuring an Ethernet port" (Page 67).

4.6.10.2 Monitoring an SFP port

RUGGEDCOM ROS supports hot-swapping of SFP transceivers on SFP ports and will automatically detect when an SFP transceiver is removed or installed.

When RUGGEDCOM ROS detects that an SFP transceiver is plugged into an SFP port, it reads the transceiver information and determines the transceiver type. This

decision results in RUGGEDCOM ROS either *accepting*, *accepting and reconfiguring*, or *rejecting* the SFP port.

The following table shows in which cases an SFP transceiver is *accepted* or *accepted and reconfigured*.

Configured speed	Detected SFP type: 1000Base-X	Detected SFP type: 100Base-FX	Detected SFP type: 1000Base-T
Gbps	Accept	Accept and automatically set the speed to 100 Mbps and set auto-negotiation to *Off*	Accept
100 Mbps	Accept and automatically set the speed to 1 Gbps and set auto-negotiation to *On*	Accept	Compare the transceiver model against a list of supported models. Accept if it is in the list. Otherwise, automatically set the speed to 1 Gbps and set auto-negotiation to *On*.

If the transceiver is *accepted*, the **Media** parameter under ***Ethernet Ports » Configure Port Parameters*** shows detailed information about the SFP transceiver, including Gigabit Ethernet Compliance Code, transmission media, connector type, and link length. For example:

```
SFP 1000LX SM LC 10 km
SFP 1000T 100 m
```

If the transceiver is not recognized, it is *rejected*. An alarm is also generated and the port is blocked so that no link can be established until the transceiver is replaced. The **Media** parameter shows the rejected SFP transceiver is unidentified. For example:

```
SFP Unidentified
```

If no transceiver is installed on an SFP port, the **Media** parameter shows the SFP transceiver is unplugged:

```
SFP Unplugged
```

4.6.10.3 Displaying information for an SFP port

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

1. Log in to the device and access the CLI shell. For more information about accessing the CLI shell, refer to "Using the command line interface" (Page 24).
2. Type the following command:

   ```
   sfp { port }
   ```

Where:

- `{ port }` is the port number

Information about the SFP port is displayed. For example:

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

4.6.10.4 Setting the SFP polling interval

To set the SFP polling interval, navigate to ***Ethernet Ports » Configure SFP DDM Options***. The **SFP DDM Options** table appears.

Note

For information about viewing the status of active SFPs, refer to "Viewing SFP diagnostics" (Page 78).

This table displays the following information:

Parameter	Description
`Polling Interval`	**Synopsis:** An integer between 1 and 30 or [Disabled] **Default:** Disabled This parameter configures the time interval the system should wait between two consecutive readings from SFP/SFP+ transceivers.

4.6.10.5 Viewing SFP diagnostics

To view the status of an SFP, navigate to ***Ethernet Ports » View SFP Diagnostics***. The **SFP Diagnostics** table appears.

Note

For information about how to set the polling interval, refer to "Setting the SFP polling interval" (Page 77).

This table displays the following information:

Parameter	Description
`Port`	The port number.
`DDM Status`	**Synopsis:** [N/A | OK | Warning | Alarm] The DDM status of the SFP.
`Temperature`	**Synopsis:** An integer between -128.000 and 128.000 **Default:** 0.000 The current temperature of the SFP transceiver, in degrees Celsius.
`Temp Alarm Low`	**Synopsis:** An integer between -128.000 and 128.000 **Default:** 0.000 The temperature low alarm threshold of the SFP transceiver, in degrees Celsius.
`Temp Warn Low`	**Synopsis:** An integer between -128.000 and 128.000 **Default:** 0.000 The temperature low warning threshold of the SFP transceiver, in degrees Celsius.
`Temp Warn High`	**Synopsis:** An integer between -128.000 and 128.000 **Default:** 0.000 The temperature high warning threshold of the SFP transceiver, in degrees Celsius.
`Temp Alarm High`	**Synopsis:** An integer between -128.000 and 128.000 **Default:** 0.000 The temperature high alarm threshold of the SFP transceiver, in degrees Celsius.
`Voltage`	**Synopsis:** An integer between 0.000 and 65.535 **Default:** 0.000 The current supply voltage of the SFP transceiver, in volts.
`Volt Alarm Low`	**Synopsis:** An integer between 0.000 and 65.535 **Default:** 0.000 The voltage low alarm threshold of the SFP transceiver, in volts.

Parameter	Description
`Volt Warn Low`	**Synopsis:** An integer between 0.000 and 65.535 **Default:** 0.000 The voltage low warning threshold of the SFP transceiver, in volts.
`Volt Warn High`	**Synopsis:** An integer between 0.000 and 65.535 **Default:** 0.000 The voltage high warning threshold of the SFP transceiver, in volts.
`Volt Alarm High`	**Synopsis:** An integer between 0.000 and 65.535 **Default:** 0.000 The voltage high alarm threshold of the SFP transceiver, in volts.
`Tx Bias`	**Synopsis:** An integer between 0.000 and 131.070 **Default:** 0.000 The current Tx bias current of the SFP transceiver, in milliamperes.
`TxBias Alarm Low`	**Synopsis:** An integer between 0.000 and 131.070 **Default:** 0.000 The Tx bias current low alarm threshold of the SFP transceiver, in milliamperes.
`TxBias Warn Low`	**Synopsis:** An integer between 0.000 and 131.070 **Default:** 0.000 The Tx bias current low warning threshold of the SFP transceiver, in milliamperes.
`TxBias Warn High`	**Synopsis:** An integer between 0.000 and 131.070 **Default:** 0.000 The Tx bias current high warning threshold of the SFP transceiver, in milliamperes.
`TxBias Alarm High`	**Synopsis:** An integer between 0.000 and 131.070 **Default:** 0.000 The Tx bias current high alarm threshold of the SFP transceiver, in milliamperes.
`Rx Power`	**Synopsis:** An integer between 0.000 and 65.535 **Default:** 0.000 The Rx input power of the SFP transceiver, in microwatts.
`RxPower Alarm Low`	**Synopsis:** An integer between 0.000 and 65.535 **Default:** 0.000 The Rx power low alarm threshold of the SFP transceiver, in microwatts.

Parameter	Description
`RxPower Warn Low`	**Synopsis:** An integer between 0.000 and 65.535 **Default:** 0.000 The Rx power low warning threshold of the SFP transceiver, in microwatts.
`RxPower Warn High`	**Synopsis:** An integer between 0.000 and 65.535 **Default:** 0.000 The Rx power high warning threshold of the SFP transceiver, in microwatts.
`RxPower Alarm High`	**Synopsis:** An integer between 0.000 and 65.535 **Default:** 0.000 The Rx power high alarm threshold of the SFP transceiver, in microwatts.
`Tx Power`	**Synopsis:** An integer between 0.000 and 65.535 **Default:** 0.000 The current Tx output power of the SFP transceiver, in milliwatts.
`TxPower Alarm Low`	**Synopsis:** An integer between 0.000 and 65.535 **Default:** 0.000 The Tx power low alarm threshold of the SFP transceiver, in milliwatts.
`TxPower Warn Low`	**Synopsis:** An integer between 0.000 and 65.535 **Default:** 0.000 The Tx power low warning threshold of the SFP transceiver, in milliwatts.
`TxPower Warn High`	**Synopsis:** An integer between 0.000 and 65.535 **Default:** 0.000 The Tx power high warning threshold of the SFP transceiver, in milliwatts.
`TxPower Alarm High`	**Synopsis:** An integer between 0.000 and 65.535 **Default:** 0.000 The Tx power high alarm threshold of the SFP transceiver, in milliwatts.
`Alarm Flags`	**Synopsis:** An integer between 0 and 4294967295 **Default:** 00000000 The current alarm flag bits of the SFP transceiver.
`Warning Flags`	**Synopsis:** An integer between 0 and 4294967295 **Default:** 00000000 The current warning flag bits of the SFP transceiver.

4.6.11 Managing EoVDSL Ports

RUGGEDCOM ROS supports Ethernet over very-high-bit-rate digital subscriber line (EoVDSL).

4.6.11.1 Understanding EoVDSL

The following describes some of the concepts important to EoVDSL:

Functionality

From the switching functionality point of view, Ethernet-over-VDSL (EoVDSL) ports function the same way as 10/100Base-TX Ethernet ports. The VDSL interface is only used as a media to transfer regular Ethernet frames. However, the link throughput and the link establishment procedure are different.

According to the VDSL standard, one of the VDSL link partners is required to operate as a LT (Line Termination) or Master device, while the second link partner operates as an NT (Network Termination) or Slave device.

Universal VDSL port

The Universal VDSL port provides symmetric upstream and downstream throughput and is suitable for high throughput connections that span a short distance (< 2.5 km or 1.6 mi). Note that a Universal VDSL master port must be connected to a Universal VDSL slave port. Long-Reach VDSL is not supported.

Establishing an optimum profile

When the EoVDSL link is initially established, the RUGGEDCOM ROS EoVDSL Master device automatically scans several different VDSL profiles, while measuring the Signal-to-Noise Ratio (SNR). Eventually the profile with the highest throughput (where the SNR is still high enough to guarantee reliable communication – the required SNR values are specified by the VDSL standard) will be selected by RUGGEDCOM ROS.

Even after locking onto the optimum profile, RUGGEDCOM ROS will continuously monitor the signal quality and, if the link-quality should drop below an acceptable limit, RUGGEDCOM ROS will restart the scan process in an attempt to find a new optimal profile that is suitable for the degraded link-quality. Typically this means using a lower throughput profile, thus maintaining high channel reliability – although sacrificing link-throughput.

SNR margin

The SNR margin is a status parameter indicating how much increase in the noise level can be tolerated without breaking the VDSL link. For example, if the SNR margin is 20 db, the link will stay active for up to a 20 db increase in the noise level. However, if the increase in noise level exceeds 20 db then the VDSL link will be broken. As the

noise level increases, the SNR Margin decreases. The link will stay active as long as the current SNR Mrgn is above 3 dB.

Target SNR margin

The target SNR margin must be met in order to establish a link. A link will be established only when a data rate can be achieved (between the configured Max Data Rate and Min Data Rate) such that the SNR margin is equal to or greater than the configured target SNR margin.

RUGGEDCOM ROS dynamically adjusts the rate such that the SNR margin remains close to the target SNR margin. For example, if the current SNR margin is less than the specified target SNR margin value (by at least 0.5 dB), the link data rate will decrease until the SNR margin is equal to the specified target SNR margin or until the current data rate is equal to the configured Min Data Rate.

Similarly, if the current SNR margin is greater than the specified target SNR margin value (by at least 3 dB), the link data rate will increase until the SNR margin is equal to the specified target SNR margin or until the current data rate is equal to the configured Max Data Rate.

Note

For information about configuring EoVDSL ports, refer to "Configuring an EoVDSL port" (Page 84).

Note

For information about EoVDSL performance characteristics and requirements, refer to the "Equipment Manual" for the RUGGEDCOM RSL910.

4.6.11.2 Viewing the status of EoVDSL ports

To view the current status of the EoVDSL , navigate to ***Ethernet Ports » Configure/ View EoVDSL Parameters***. The **EoVDSL Parameters** table appears.

This table displays the following information:

Parameter	Description
`Port`	**Synopsis:** [9 | 10] The port number.
`Type`	**Synopsis:** [Univ] **Default:** Univ The type of VDSL port. Options include: • **Univ** – Universal EoVDSL

Parameter	Description
`Mode`	**Synopsis:** [Master | Slave] **Default:** Master Determines if the port should operate as a VDSL Master or Slave.
`Max Data Rate`	**Synopsis:** An integer between 0.2 and 160.0 **Default:** 100.0 Specify the maximum allowed down-stream (Master-to-Slave) and up-stream (Slave-to-Master) data rate.
`Min Data Rate`	**Synopsis:** An integer between 0.2 and 160.0 **Default:** 1.0 Specify the minimum required down-stream (Master-to-Slave) and up-stream (Slave-to-Master) data rate.
`Target SNR Margin`	**Synopsis:** An integer between 6 and 31 **Default:** 10 Specify the SNR margin value that a particular VDSL link should operate on. SNR margin is the difference between the actual SNR and minimal SNR required to sync at a specific data rate.
`SED Period`	**Synopsis:** [1 ms | 5 ms | 10 ms | 20 ms | 50 ms | 100 ms | 200 ms | 400 ms | 800 ms | Disabled] **Default:** 10 Specify the signal error detection period. Higher values provide more impulse noise tolerance while lower values provide faster link down detection. If disabled, the link has high impulse noise tolerance but slow link down detection.
`Link State`	**Synopsis:** [Down | Scan | Up] **Status parameter** – indicates if configured or automatically found optimal VDSL link is established. While establishing the optimal link, the device is scanning different VDSL profiles for signal quality to find the profile with the highest throughput.
`Data Rate (DS/US)`	**Synopsis:** #/# Mbps where # is a floating point number between 0.0 and 100.0 **Status parameter** – actual VDSL down-stream (Master-to-Slave) and up-stream (Slave-to-Master) data rate.
`SNR Mrgn`	**Synopsis:** A floating point number between 0.0 and 50.0 **Status parameter** – VDSL signal-to-noise ratio (SNR) margin. The SNR margin is the computed SNR minus the SNR required for 10^{e-7} Bit-Error Rate (BER). A positive SNR margin of 6 dB or more is required to ensure reliable service with unknown impairments and temperature variations.

4.6.11.3 Configuring an EoVDSL port

To configure an EoVDSL port, do the following:

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

Parameter	Description
`Port`	**Synopsis:** [9 | 10] The port number.
`Mode`	**Synopsis:** [Master | Slave] **Default:** Master Determines if the port should operate as a VDSL Master or Slave.
`Max Data Rate`	**Synopsis:** An integer between 0.2 and 160.0 **Default:** 100.0 Specify the maximum allowed down-stream (Master-to-Slave) and up-stream (Slave-to-Master) data rate.
`Min Data Rate`	**Synopsis:** An integer between 0.2 and 160.0 **Default:** 1.0 Specify the minimum required down-stream (Master-to-Slave) and up-stream (Slave-to-Master) data rate.
`Target SNR Margin`	**Synopsis:** An integer between 6 and 31 **Default:** 10 Specify the SNR margin value that a particular VDSL link should operate on. SNR margin is the difference between the actual SNR and minimal SNR required to sync at a specific data rate.
`SED Period`	**Synopsis:** [1 ms | 5 ms | 10 ms | 20 ms | 50 ms | 100 ms | 200 ms | 400 ms | 800 ms | Disabled] **Default:** 10 Specify the signal error detection period. Higher values provide more impulse noise tolerance while lower values provide faster link down detection. If disabled, the link has high impulse noise tolerance but slow link down detection.
`Link State`	**Synopsis:** [Down | Scan | Up] **Status parameter** – indicates if configured or automatically found optimal VDSL link is established. While establishing the optimal link, the device is scanning different VDSL profiles for signal quality to find the profile with the highest throughput.

Parameter	Description
`Data Rate (DS/US)`	**Synopsis:** #/# Mbps where # is a floating point number between 0.0 and 100.0 **Status parameter** – actual VDSL down-stream (Master-to-Slave) and up-stream (Slave-to-Master) data rate.
`SNR Mrgn`	**Synopsis:** A floating point number between 0.0 and 50.0 **Status parameter** – VDSL signal-to-noise ratio (SNR) margin. The SNR margin is the computed SNR minus the SNR required for 10^{e-7} Bit-Error Rate (BER). A positive SNR margin of 6 dB or more is required to ensure reliable service with unknown impairments and temperature variations.

4. Click **Apply**.

4.6.11.4 Adjusting EoVDSL settings

The default EoVDSL settings in RUGGEDCOM ROS are intended to achieve maximum performance in most environments. However, factors such as ambient noise can impact the link.

The following scenarios describe how to configure EoVDSL parameters in challenging environments to achieve desired performance.

For more information about configuring EoVDSL parameters, refer to "Configuring an EoVDSL port" (Page 84).

Note

The values shown in the following table are provided as examples only. Actual values can vary based on the user's configuration.

Requirement	Action	Result
Restrict the data rate of the VDSL link to a maximum limit (e.g. 50 Mbps)	Configure the **Max Data Rate** to 50 Mbps	A higher SNR margin will be achieved by selecting a lower data rate. An increase in the maximum data rate may result in a decrease in the SNR margin, as the VDSL chip would then try to achieve the maximum data rate while meeting the target SNR margin. It is strongly recommended to maintain a healthy SNR Margin (minimum 10 db) in the network to ensure error-free data and to maintain the link, even when the link conditions are not ideal in a marginally noisy environment.
Restrict the data rate of the VDSL link to a minimum limit (e.g. 1.0 Mbps)	Configure the **Min Data Rate** to 1.0Mbps	The link will go down whenever the minimum data rate is not achieved (for example due to ambient noise). This is useful in scenarios where redundant paths exist in the network, and when a data rate over a path is lower than the required minimum traffic can be switched to another path (for example using RSTP).

Requirement	Action	Result
Configure the minimum and maximum data rates of the VDSL link to a specific value (e.g. 20 Mbps)	Configure the **Min Data Rate** to 20 Mbps and the **Max Data Rate** to 20 Mbps	The link is forced to adhere to a specific speed (e.g. 20 Mbps).
Make sure the VDSL link comes up only when a required minimum SNR Margin value (e.g. 10dB) is achieved	Configure the **Target SNR Mrgn** to 10dB	The VDSL link will not be established until the link SNR margin meets the minimum target SNR margin. The higher the value of the Target SNR Mrgn parameter, the higher the noise tolerance of the link, therefore the link does not break down because of noise. Conversely, a higher target SNR margin value in a noisy environment would cause the link not to go up unless the specified target SNR margin is met. After a link is established at the target SNR margin, a minimum of 3 db SNR Margin is required to maintain the link.
Make sure the link stays up for a specified time (e.g. 10 ms) despite a significant Bit Error Rate (BER)	Configure the **SED Period** to 10 ms	The link will remain active for 10 ms, regardless of the BER. In some instances, when sudden impulse noise is introduced in the network the BER momentarily increases. This can cause the link to go down. If the duration of the high BER in the network is short, the link can withstand the impact for a few milliseconds and does not go down completely. The SED parameter specifies the duration of high BER that can be tolerated without breaking the link. If this parameter is set to disabled, then the link will will stay up for the longest possible duration of high BER.

4.6.12 Detecting cable faults

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

4.6.12.1 Viewing cable diagnostics results

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

Note

For information about how to start a diagnostic test, refer to "Performing cable diagnostics" (Page 88).

This table displays the following information:

Parameter	Description
`Port`	The port number.
`State`	Control the start/stop of the cable diagnostics on the selected port. If a port does not support cable diagnostics, State will be reported as N/A.
`Runs`	**Synopsis:** An integer between 0 and 65535 The total number of times cable diagnostics to be performed on the selected port. If this number is set to 0, cable diagnostics will be performed forever on the selected port.
`Calib.`	**Synopsis:** An integer between -100.0 and 100.0 This calibration value can be used to adjust or calibrate the estimated distance to fault. User can take following steps to calibrate the cable diagnostics estimated distance to fault: 1. Pick a particular port which calibration is needed. 2. Connect an Ethernet cable with a known length (e.g. 50m) to the port. 3. DO NOT connect the other end of the cable to any link partner. 4. Run cable diagnostics a few times on the port. OPEN fault should be detected. 5. Find the average distance to the OPEN fault recorded in the log and compare it to the known length of the cable. The difference can be used as the calibration value. 6. Enter the calibration value and run cable diagnostics a few more times. 7. The distance to OPEN fault should now be at similar distance as the cable length. 8. Distance to fault for the selected port is now calibrated.
`Good`	**Synopsis:** An integer between 0 and 65535 The number of times GOOD TERMINATION (no fault) is detected on the cable pairs of the selected port.
`Open`	**Synopsis:** An integer between 0 and 65535 The number of times OPEN is detected on the cable pairs of the selected port.
`Short`	**Synopsis:** An integer between 0 and 65535 The number of times SHORT is detected on the cable pairs of the selected port.
`Imped`	**Synopsis:** An integer between 0 and 65535 The number of times IMPEDANCE MISMATCH is detected on the cable pairs of the selected port.
`Pass /Fail /Total`	**Synopsis:** A string up to 19 characters long This field summarizes the results of the cable diagnostics performed so far.

Parameter	Description
	• **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 "Viewing local and system logs" (Page 56).

4.6.12.2 Performing cable diagnostics

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

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

   ⚠ NOTICE

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

2. Connect the other end of the cable to a similar network port. For example, connect a 100Base-T port to a 100Base-T port, or a 1000Base-T port to a 1000Base-T port.
3. In RUGGEDCOM ROS, navigate to ***Ethernet Ports » Configure/View Cable Diagnostics Parameters***. The **Cable Diagnostics Parameters** table appears.
4. Select an Ethernet port. The **Cable Diagnostics Parameters** form appears.
5. Under **Runs**, enter the number of consecutive diagnostic tests to perform. A value of 0 indicates the test will run continuously until stopped by the user.
6. Under **Calib.**, enter the estimated Distance To Fault (DTF) value. For information about how to determine the DTF value, refer to "Determining the Estimated Distance To Fault (DTF)" (Page 89).
7. Select **Started**.

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

8. Click **Apply**. The state of the Ethernet port will automatically change to **Stopped** when the test is complete. For information about how to monitor the test and view the results, refer to "Viewing cable diagnostics results" (Page 86).

4.6.12.3 Clearing cable diagnostics

To clear the cable diagnostic results, do the following:

1. Navigate to ***Ethernet Ports » Clear Cable Diagnostics Statistics***. The **Clear Cable Diagnostics Statistics** form appears.
2. Select one or more Ethernet ports.
3. Click **Apply**.

4.6.12.4 Determining the Estimated Distance To Fault (DTF)

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

1. Connect a CAT-5 (or better quality) Ethernet cable with a known length to the device. Do not connect the other end of the cable to another port.
2. Configure the cable diagnostic utility to run a few times on the selected Ethernet port and start the test. For more information, refer to "Performing cable diagnostics" (Page 88). Open faults should be detected and recorded in the system log.
3. Review the errors recorded in the system log and determine the average distance of the open faults. For more information about the system log, refer to "Viewing local and system logs" (Page 56).
4. Subtract the average distance from the cable length to determine the calibration value.
5. Configure the cable diagnostic utility to run a few times with the new calibration value. The distance to the open fault should now be the same as the actual length of the cable. The Distance To Fault (DTF) is now calibrated for the selected Ethernet port.

4.6.13 Resetting Ethernet ports

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

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

1. Navigate to ***Ethernet Ports » Reset Port(s)***. The **Reset Port(s)** form appears.
2. Select one or more Ethernet ports to reset.
3. Click **Apply**. The selected Ethernet ports are reset.

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

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

For more information, refer to "Configuring IP services" (Page 94).

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.

⚠ NOTICE

Configuration hazard – risk of communication disruption

Changing the ID for the management VLAN will break any active Raw Socket TCP connections. If this occurs, reset all serial ports.

4.7.1 Viewing a list of IP interfaces

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

If IP interfaces have not been configured, add IP interfaces as needed. For more information, refer to "Adding an IP interface" (Page 91).

4.7.2 Adding an IP interface

To add an IP interface, do the following:

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

⚠ NOTICE

Security hazard – risk of unauthorized access and/or exploitation

IP interfaces that belong to a management or auxiliary management VLAN must be connected to a trusted network.

⚠ NOTICE

Configuration hazard – risk of communication disruption.

Changing the ID for the management VLAN will break any active Raw Socket TCP connections. If this occurs, reset all serial ports.

Note

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

Note

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

Parameter	Description
`Type`	**Synopsis:** [VLAN] **Default:** VLAN Specifies the type of the interface for which this IP interface is created.

Parameter	Description
`ID`	**Synopsis:** An integer between 1 and 4094 **Default:** 1 Specifies the the ID of the interface for which this IP interface is created. If interface type is VLAN, represents VLAN ID.
`Mgmt`	**Synopsis:** [No | Yes | Aux] **Default:** No Specifies whether the IP interface can support management functions. • **Aux** – Supports management functions • **Yes** – Supports management functions and dynamic address assignment such as DHCP • **No** – Does not support management functions or dynamic address assignment
`IP Address Type`	**Synopsis:** [Static | Dynamic | DHCP | BOOTP] **Default:** Static Specifies whether the IP address is static or dynamically assigned via DHCP or BOOTP. Option DYNAMIC is a common case of dynamically assigned IP address. It switches between BOOTP and DHCP until it gets the response from the relevant server. Must be static for non management interfaces.
`IP Address`	**Synopsis:** Any valid IP address **Default:** 192.168.0.1 Specifies the Internet Protocol address of this interface. An IP address is a 128-bit number that is notated by using eight fields of four hexadecimal digits, for which leading zeros can be omitted, delimited by colons. Consult offline documentation for more information. A version 4 address can be encoded by four decimal numbers from 0 through 255, separated by periods. Only a unicast IP addresses is allowed, which does not begin with "FF", or ranges from 1.0.0.0 to 233.255.255.255 for version 4.
`Subnet`	**Synopsis:** An integer between 0 and 128 **Default:** 24 Specifies the number of contiguous highest order bits that comprise the subnet mask for the current interface. For example, 24 would be equivalent to a 255.255.255.0 IPv4 subnet mask, while 64 would specify the subnet mask to consist of the highest order 64 bits (valid for IPv6). **Note** Each IP interface must have a unique network address.

4. Click **Apply**.

4.7.3 Deleting an IP interface

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

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

4.8 Managing IP gateways

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

Note

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

4.8.1 Viewing a list of IP gateways

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

If IP gateways have not been configured, add IP gateways as needed. For more information, refer to "Adding an IP gateway" (Page 93).

4.8.2 Adding an IP gateway

Note

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

To add an IP gateway, do the following:

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

Parameter	Description
`Destination`	**Synopsis:** Any valid IP address Specifies the IP address of destination network or host. For default gateway, both the destination and subnet are 0.

Parameter	Description
`Subnet`	**Synopsis:** An integer between 0 and 128 **Default:** 0 Specifies the destination IP subnet mask. For default gateway, both the destination and subnet are 0.
`Gateway`	**Synopsis:** Any valid IP address Specifies the gateway to be used to reach the destination.

4. Click **Apply**.

4.8.3 Deleting an IP gateway

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

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

4.9 Configuring IP services

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

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

Parameter	Description
`Inactivity Timeout`	**Synopsis:** An integer between 1 and 60 or [Disabled] **Default:** 5 The time in minutes 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 the maximum timeout value is limited to 30 minutes.
`Telnet Sessions Allowed`	**Synopsis:** An integer between 1 and 4 or [Disabled] **Default:** Disabled Limits the number of Telnet sessions. A value of zero prevents any Telnet access.
`Web Server Users Allowed`	**Synopsis:** An integer between 1 and 4 or [Disabled] **Default:** 4 Limits the number of simultaneous web server users.

Parameter	Description
TFTP Server	**Synopsis:** [Disabled | Get Only | Enabled] **Default:** Disabled As this is an insecure protocol, this parameter allows user to limit or disable the service. **Disabled** – disables read and write access through this service **Get Only** – only allows to read files through this service **Enabled** – allows to read and write files through this service
ModBus Address	**Synopsis:** An integer between 1 and 255 or [Disabled] **Default:** Disabled Determines the Modbus address to be used for Management through Modbus.
SSH Sessions Allowed (Controlled Version Only)	**Synopsis:** An integer between 1 and 4 or [Disabled] **Default:** 4 Limits the number of SSH sessions. When set to **Disabled**, SSH access is prevented, however active SSH sessions will not be disconnected. **⚠ NOTICE** To disable SSH access, the console service must be enabled. For more information about enabling the console service, refer to "Enabling/disabling the console service" (Page 42).
MMS Sessions Allowed	**Synopsis:** An integer between 1 and 8 **Default:** Disabled Limits the number of MMS sessions. "Disabled" prevents any MMS access.
RSH Server	**Synopsis:** [Disabled | Enabled] **Default:** Disabled Disables/enables Remote Shell access.
Failed Attempts Window	**Synopsis:** An integer between 1 and 30 **Default:** 5 The time in minutes (min) in which the maximum number of failed login attempts must be exceeded before a service is blocked. The counter of failed attempts resets to 0 when the timer expires. This parameter resets to the default value when the factory default configuration is reloaded.
Lockout Time	**Synopsis:** An integer between 1 and 120 **Default:** 60 The time in minutes (min) the service remains locked out after the maximum number of failed access attempts has been reached. With the exception of the device management

Parameter	Description
	interface, this parameter resets to the default value when the factory default configuration is reloaded.

3. Click **Apply**.

4.10 Managing remote monitoring

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

4.10.1 Managing rmon history controls

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

4.10.1.1 Viewing a list of RMON history controls

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

If history controls have not been configured, add controls as needed. For more information, refer to "Adding an rmon history control" (Page 96).

4.10.1.2 Adding an rmon history control

To add an RMON history control, do the following:

1. Navigate to ***Ethernet Stats » Configure RMON History Controls***. The **RMON History Controls** table appears.
2. Click **InsertRecord**. The **RMON History Controls** form appears.
3. Configure the following parameter(s) as required:

Parameter	Description
`Index`	**Synopsis:** An integer between 1 and 65535 **Default:** 1 The index of this RMON History Contol record.
`Port`	The port number.

Parameter	Description
Requested Buckets	**Synopsis:** An integer between 1 and 5000 **Default:** 50 The maximum number of buckets requested for this RMON collection history group of statistics. The range is 1 to 4000. The default is 50.
Granted Buckets	**Synopsis:** An integer between 0 and 65535 The number of buckets granted for this RMON collection history. This field is not editable.
Interval	**Synopsis:** An integer between 1 and 3600 **Default:** 1800 The number of seconds in over which the data is sampled for each bucket. The range is 1 to 3600. The default is 1800.
Owner	**Synopsis:** A string up to 127 characters long **Default:** Monitor The owner of this record. It is suggested to start this string withword 'monitor'.

4. Click **Apply**.

4.10.1.3 Deleting an RMON history control

To delete an RMON history control, do the following:

1. Navigate to ***Ethernet Stats » Configure RMON History Controls***. The **RMON History Controls** table appears.
2. Select the history control from the table. The **RMON History Controls** form appears.
3. Click **Delete**.

4.10.2 Managing RMON alarms

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

Remote Monitoring (RMON) alarms define upper and lower thresholds for legal values of specific statistical variables in a given interval. This allows RUGGEDCOM ROS to detect events as they occur more quickly than a specified maximum rate or less 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 "Viewing and clearing latched alarms" (Page 111).

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

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

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

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

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

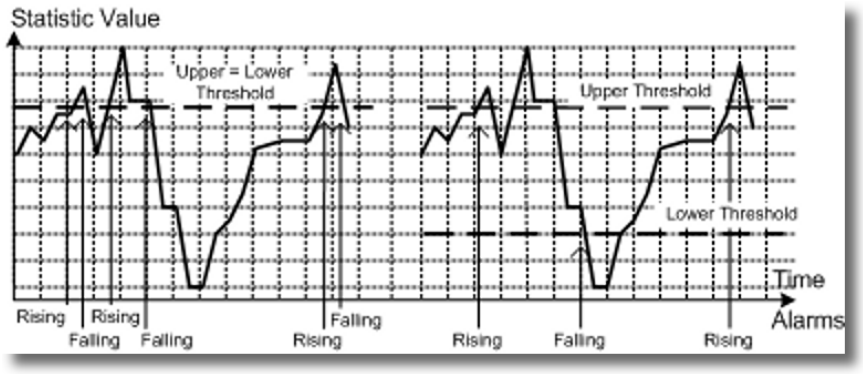


Figure 4.3 The alarm process

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

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

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

4.10.2.1 Viewing a list of RMON alarms

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

If alarms have not been configured, add alarms as needed. For more information, refer to "Adding an RMON alarm" (Page 99).

4.10.2.2 Adding an RMON alarm

To add an RMON alarm, do the following:

1. Navigate to ***Ethernet Stats » Configure RMON Alarms***. The **RMON Alarms** table appears.
2. Click **InsertRecord**. The **RMON Alarms** form appears.
3. Configure the following parameter(s) as required:

Parameter	Description
`Index`	**Synopsis:** An integer between 1 and 65535 **Default:** 1 The index of this RMON Alarm record.
`Variable`	**Synopsis:** An integer up to 39 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:** An integer between -2147483647 and 2147483647 **Default:** 0 A threshold for the sampled variable. When the current sampled variable value is greater than or equal to this threshold, and the value at the last sampling interval was less than this threshold, a single event will be generated. A single event will also be generated if the first sample after this record is created is greater than or equal to this threshold and the associated startup alarm ils equal to 'rising'.After rising alarm is generated, another such event will not be generated until the sampled value falls below this threshold and reaches the value of FallingThreshold.
`Falling Thr`	**Synopsis:** An integer between -2147483647 and 2147483647 **Default:** 0 A threshold for the sampled variable. When the current sampled variable value is less than or equal to this threshold, and the value at the last sampling interval was greater than this threshold, a single event will be generated. A single event will also be generated if the first sample after this record is created is less than or equal to this threshold and the associated startup alarm ils equal to 'falling'.After falling alarm is generated, another such event will not be generated until the sampled value rises above this threshold and reaches the value of RisingThreshold.

Parameter	Description
`Value`	**Synopsis:** An integer between -2147483647 and 2147483647 The value of monitoring object during the last sampling period. The presentation of value depends of sample type ('absolute' or 'delta').
`Type`	**Synopsis:** [absolute | delta] **Default:** delta The method of sampling the selected variable and calculating the value to be compared against the thresholds. The value of sample type can be 'absolute' or 'delta'.
`Interval`	**Synopsis:** An integer between 0 and 2147483647 **Default:** 60 The number of seconds in over which the data is sampled and compared with the rising and falling thresholds.
`Startup Alarm`	**Synopsis:** [rising | falling | risingOrFalling] **Default:** risingOrFalling The alarm that may be sent when this record is first created if condition for raising alarm is met. The value of startup alarm can be 'rising', 'falling' or 'risingOrFalling'.
`Rising Event`	**Synopsis:** An integer between 0 and 65535 **Default:** 0 The index of the event that is used when a falling threshold is crossed. If there is no corresponding entryl in the Event Table, then no association exists. In particular, if this value is zero, no associated event will be generated.
`Falling Event`	**Synopsis:** An integer between 0 and 65535 **Default:** 0 The index of the event that is used when a rising threshold is crossed. If there is no corresponding entryl in the Event Table, then no association exists. In particular, if this value is zero, no associated event will be generated.
`Owner`	**Synopsis:** A string up to 127 characters long **Default:** Monitor The owner of this record. It is suggested to start this string withword 'monitor'.

4. Click **Apply**.

4.10.2.3 Deleting an RMON alarm

To delete an RMON alarm, do the following:

1. Navigate to ***Ethernet Stats » Configure RMON Alarms***. The **RMON Alarms** table appears.
2. Select the alarm from the table. The **RMON Alarms** form appears.
3. Click **Delete**.

4.10.3 Managing RMON events

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

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

Two traps are defined: risingAlarm and fallingAlarm.

4.10.3.1 Viewing a list of RMON events

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

If events have not been configured, add events as needed. For more information, refer to "Adding an RMON event" (Page 101).

4.10.3.2 Adding an RMON event

To add an RMON alarm, do the following:

1. Navigate to ***Ethernet Stats » Configure RMON Events***. The **RMON Events** table appears.
2. Click **InsertRecord**. The **RMON Events** form appears.
3. Configure the following parameter(s) as required:

Parameter	Description
`Index`	**Synopsis:** An integer between 1 and 65535 **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

Parameter	Description
	table for each event. In the case of snmp_trap, an SNMP trap is sent to one or more management stations.
Community	**Synopsis:** A string up to 31 characters long **Default:** public If the SNMP trap is to be sent, it will be sent to the SNMP community specified by this string.
Last Time Sent	**Synopsis:** DDDD days, HH:MM:SS The time from last reboot at the time this event entry last generated an event. If this entry has not generated any events, this value will be 0.
Description	**Synopsis:** A string up to 127 characters long **Default:** EV2-Rise A comment describing this event.
Owner	**Synopsis:** A string up to 127 characters long **Default:** Monitor The owner of this event record. It is suggested to start this string withword 'monitor'.

4. Click **Apply**.

4.10.3.3 Deleting an RMON event

To delete an RMON event, do the following:

1. Navigate to ***Ethernet Stats » Configure RMON Events***. The **RMON Events** table appears.
2. Select the event from the table. The **RMON Events** form appears.
3. Click **Delete**.

4.11 Upgrading/downgrading firmware

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

4.11.1 Verifying the hash checksum

Before installing new firmware for RUGGEDCOM ROS, it is recommended to verify the hash checksum to ensure the firmware is authentic and error-free.

For instructions on how to verify the hash checksum, including a list of hash checksums for all RUGGEDCOM ROS devices and releases, refer to FAQ "RUGGEDCOM

ROS Hash Checksums" (https://support.industry.siemens.com/cs/ww/en/view/109779935).

4.11.2 Upgrading firmware

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

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

Note

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

Note

It is recommended to enable access to the bootloader interface during this procedure in case emergency recovery is needed (e.g. power interruption during the upgrade). For increased security, Siemens recommends disabling bootloader access following the upgrade. For more information about managing bootloader access, refer to "Enabling/disabling access to the boot loader interface" (Page 40).

To upgrade the RUGGEDCOM ROS firmware, do the following:

1. Enable access to the bootloader interface. For more information, refer to "Enabling/disabling access to the boot loader interface" (Page 40).
2. Upload a different version of the binary firmware image to the device. For more information, refer to "Uploading/downloading files" (Page 51).
3. Reset the device to complete the installation. For more information, refer to "Rebooting the device" (Page 105).
4. Access the CLI shell and verify the new software version has been installed by typing `version`. The currently installed versions of the main and boot firmware are displayed.

```
>version
Current ROS-MPC83 Main Software v5.10.0 (Jan 01 5.10 00:01)
```

5. Disable access to the bootloader interface. For more information, refer to "Enabling/disabling access to the boot loader interface" (Page 40).

4.11.3 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:

Note

Before downgrading the firmware, make sure the hardware is supported by the older firmware version. Refer to the Release Notes for the older firmware version to confirm.

Note

Do not downgrade the RUGGEDCOM ROS boot version.

1. Disconnect the device from the network.
2. Log in to the device as an admin user. For more information, refer to "Logging in" (Page 19).
3. Make a local copy of the current configuration file. For more information, refer to "Uploading/downloading files" (Page 51).

   ⚠ NOTICE

   Configuration hazard – risk of communication disruption

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

4. Restore the device to its factory defaults. For more information, refer to "Restoring factory defaults" (Page 50).
5. Upload and apply the older firmware version using the same methods used to install newer firmware versions. For more information , refer to "Upgrading firmware" (Page 103).
6. Press **Ctrl-S** to access the CLI.
7. Clear all logs by typing:

   ```
   clearlogs
   ```

8. Clear all alarms by typing:

   ```
   clearalarms
   ```

   ⚠ NOTICE

   Security hazard – risk of unauthorized access and/or exploitation

   After downgrading the firmware, be aware that some settings from the previous configuration may be lost or reverted back to the factory defaults (including user passwords if downgrading from a security related version), as

those particular tables or fields may not exist in the older firmware version. Because of this, the unit must be configured after the downgrade.

9. Configure the device as required.

4.12 Rebooting the device

To reboot the device without impacting the existing configuration, do the following:

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

4.13 Decommissioning the device

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

To decommission the device, do the following:

1. Disconnect all network cables from the device.
2. Connect to the device via the RS-232 serial console port. For more information, refer to "Connecting directly" (Page 43).
3. Restore all factory default settings for the device. For more information, refer to "Restoring factory defaults" (Page 50).
4. Access the CLI. For more information, refer to "Using the command line interface" (Page 24).
5. Clear the existing banner file by typing:

   ```
   banner -c
   ```

6. Confirm the banner clearing was successful by typing:

   ```
   type banner.txt
   ```

7. Clear the system and crash logs by typing:

   ```
   clearlogs
   ```

8. Generate a new self-signed TLS certificate by typing:

   ```
   sslkeygen ecc 256
   ```

   The message *ssl.crt generation is now pending* will appear, indicating the TLS certificate generation process has started.

Note

The certificate generation process will take several minutes to complete.

For more information about TLS certificates, including requirements and examples, refer to "Managing SSH/TLS keys and certificates" (Page 150).

9. Verify the certificate has been generated by typing:

   ```
   type syslog.txt
   ```

   The syslog will display messages similar to the following:

   ```
   21/08/30 15:36:57.958 INFO 35C Generation pending for ssl.crt: SSL
    Certificate
   21/08/30 15:36:58.186 INFO 35C Started generating ssl.crt: SSL Certificate
   21/08/30 15:36:58.489 INFO 35C Successfully generated ssl.crt: SSL
    Certificate
   21/08/30 15:36:59.059 INFO 35C Flashing ssl.crt started
   21/08/30 15:36:59.066 INFO 35C Flashing ssl.crt done
   21/08/30 15:36:59.066 INFO 35C Successfully updated ssl.crt.
   21/08/30 15:36:59.067 INFO 35C Generated ssl.crt was saved
   21/08/30 15:36:59.068 INFO 35C Key generation task finished for ssl.crt
   ```

10. Generate random SSH keys by typing:

    ```
    sshkeygen rsa 1024
    ```

    The message *ssh.keys generation is now pending* will appear, indicating the SSH keys generation process has started.

    Note

    The SSH keys generation process will take several minutes to complete.

    For more information about SSH keys, including requirements and examples, refer to "Managing SSH/TLS keys and certificates" (Page 150).

11. Verify the SSH keys have been generated by typing:

    ```
    type syslog.txt
    ```

    The syslog will display messages similar to the following:

    ```
    21/08/30 15:33:37.179 INFO 35C Generation pending for ssh.keys: SSH Keys
    21/08/30 15:33:37.860 INFO 35C Started generating ssh.keys: SSH Keys21/08/30
     15:34:52.098 INFO 35C Successfully generated ssh.keys: SSH Keys
    21/08/30 15:34:53.266 INFO 35C SSH host key installed, MD5#
     BD:BD:07:E5:9F:83:E3:4A:48:DA:F8:93:6E:37:D6:A6
    21/08/30 15:34:53.268 INFO 35C Flashing ssh.keys started
    21/08/30 15:34:53.280 INFO 35C Flashing ssh.keys done
    21/08/30 15:34:53.280 INFO 35C Successfully updated ssh.keys.
    21/08/30 15:34:53.281 INFO 35C Generated ssh.keys was saved
    21/08/30 15:34:53.283 INFO 35C Key generation task finished for ssh.keys
    ```

    For more information about SSH keys, including requirements and examples, refer to "Managing SSH/TLS keys and certificates" (Page 150).

12. De-fragment and erase all free flash memory by typing:

    ```
    flashfile defrag
    ```

    Note

    This process will take several minutes to complete.

13. Clear the system and crash logs by typing:

    ```
    clearlogs
    ```

5 System administration

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

5.1 Configuring the system information

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

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

Parameter	Description
`System Name`	**Synopsis:** A string up to 24 characters long The system name is displayed in allRUGGEDCOM ROSmenu screens. This can make it easier to identify the switches within your network provided that all switches are given a unique name.
`Location`	**Synopsis:** A string up to 49 characters long The location can be used to indicate the physical location of the switch. It is displayed in the login screen as another means to ensure you are dealing with the desired switch.
`Contact`	**Synopsis:** A string up to 49 characters long The contact can be used to help identify the person responsible for managing the switch. You can enter name, phone number, email, etc. It is displayed in the login screen so that this person may be contacted should help be required.

3. Click **Apply**.

5.2 Customizing the login screen

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

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

To update the **banner.txt** file, download the file from the device, modify it and then load it back on to the device. For information about uploading and downloading files, refer to "Uploading/downloading files" (Page 51).

Alternatively, the **banner.txt** file can be updated using the `banner` CLI command. For more information, refer to "Available CLI commands" (Page 24).

5.3 Enabling/disabling the Web interface

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

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

Note

The Web interface can be disabled via the Web UI by configuring the Web Server Users Allowed parameter in the **IP Services form**. For more information, refer to "Configuring IP services" (Page 94).

1. Log in to the device as an admin user and access the CLI shell. For more information about accessing the CLI shell, refer to "Using the command line interface" (Page 24).
2. Navigate to ***Administration » Configure IP Services » Web Server Users Allowed***.
3. Select **Disabled** to disable the Web interface, or select the desired number of Web server users allowed to enable the interface.

5.4 Managing alarms

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

There are two types of alarms:

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

Note

For more information about RMON alarms, refer to "Managing RMON alarms" (Page 97).

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

Note

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

5.4.1 Viewing a list of pre-configured alarms

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

Note

This list of alarms (configurable and non-configurable) is accessible through the Command Line Interface (CLI) using the `alarms` command. For more information, refer to "Available CLI commands" (Page 24).

For information about modifying a pre-configured alarm, refer to "Configuring an alarm" (Page 111).

5.4.2 Viewing and clearing latched alarms

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

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

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

5.4.3 Configuring an alarm

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

To configuring an alarm, do the following:

⚠ NOTICE

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

1. Navigate to ***Diagnostic » Configure Alarms***. The **Alarms** table appears.
2. Select an alarm. The **Alarms** form appears.
3. Configure the following parameter(s) as required:

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

Parameter	Description
`Refresh Time`	**Synopsis:** An integer between 0 and 60 **Default:** 60 Refreshing time for this alarm.

4. Click **Apply**.

5.4.4 Authentication related security alarms

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

5.4.4.1 Security alarms for login authentication

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

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

- Weak Password Configured
- Login and Logout Information
- Excessive Failed Login Attempts
- RADIUS Server Unreachable
- TACACS Server Unreachable
- TACACS Response Invalid
- SNMP Authentication Failure

Note

All alarms and log messages related to login authentication are configurable. For more information about configuring alarms, refer to "Configuring an alarm" (Page 111).

Weak Password Configured

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

Message name	Alarm	SNMP trap	Syslog
Weak Password Configured	Yes	Yes	Yes

Default Keys In Use

RUGGEDCOM ROS generates this alarm and logs a message in the syslog when default keys are in use. For more information about default keys, refer to "Managing SSH/TLS keys and certificates" (Page 150).

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

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

For more information about configuring the maximum failed attempts and lockout time, refer to "Configuring IP services" (Page 94).

Message name	Alarm	SNMP trap	Syslog
Excessive Failed Login Attempts	Yes	Yes	Yes

RADIUS Server Unreachable

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

Message name	Alarm	SNMP trap	Syslog
Primary RADIUS Server Unreachable	Yes	Yes	Yes

TACACS+ Server Unreachable

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

Message name	Alarm	SNMP trap	Syslog
Primary TACACS Server Unreachable	Yes	Yes	Yes

TACACS+ Response Invalid

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

Message name	Alarm	SNMP trap	Syslog
TACACS Response Invalid	Yes	Yes	Yes

SNMP Authentication Failure

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

Message name	Alarm	SNMP trap	Syslog
SNMP Authentication Failure	Yes	Yes	Yes

5.4.4.2 Security messages for port authentication

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

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

MAC Address Authorization Failure

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

Message name	Alarm	SNMP trap	Syslog
MAC Address Authorization Failure	Yes	Yes	Yes

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

5.4.5 List of alarms

The following tables lists the possible user-configurable and non-configurable alarms in RUGGEDCOM ROS.

For more information about configuring alarms, refer to "Configuring an alarm" (Page 111).

User-configurable alarms

Name	Trigger condition	Level	Latch	Trap	Log	LED & relay
Admin Level Password Changed	The Admin user password is changed	Note	Off	On	On	Off
ARP security notification	ARP request dropped on any port for corresponding VLAN ID	Warn	On	On	On	On
BPDU Guard activated	The BPDU Guard is activated on a port	Error	On	On	On	On
Configuration changed	The device configuration is changed	Info	Off	On	On	Off
Data Storage passphrase changed	The data storage passphrase is changed	Note	Off	On	On	Off
DHCP security notification	DHCP request dropped on any port for corresponding VLAN ID	Warn	On	On	On	On
Excessive failed login attempts	The user failed to login 3 times in succession	Warn	On	On	On	On

Name	Trigger condition	Level	Latch	Trap	Log	LED & relay
GMRP cannot learn more addresses	GMRP groups are full and cannot learn more MAC addresses	Warn	On	On	On	On
Guest Level Password Changed	The Guest user password is changed	Note	Off	On	On	Off
GVRP cannot learn more VLANs	The VLAN database is full and cannot learn more VLAN IDs for GVRP	Warn	On	On	On	On
IGMP Group Membership table full	IGMP request is denied as the group membership table is full	Warn	On	On	On	On
IGMP Mcast Forwarding table full	IGMP request is denied as the group multicast table is full	Warn	On	On	On	On
Inconsistent speed/dpx in trunk	Trunk ports are working at different speed/duplex	Error	On	On	On	On
Link up/down	Link is updated to up or down	Warn	On	On	On	On
Login failed	User login attempt failed due to incorrect login credentials or access rights	Info	On	On	On	Off
Login information	If login fails, provides the user mode, user name, user type, IP address, and source of authentication	Info	On	On	On	Off
MAC address authorization failed	The MAC address cannot be saved as authorized on a secure port	Error	On	Off	On	On
MAC address not learned	The MAC address is not learned successfully	Warn	On	On	On	On
Mcast CPU filtering table full	No space for more filters in Mcast CPU filtering table	Warn	On	On	On	On
MRP Inst 1 ring multiple MRM error	MRP instance error having multiple managers in the ring	Warn	On	On	On	On
MRP Inst 1 ring One Side Rx error	MRP instance received on a single side	Warn	On	On	On	On
MRP Inst 1 ring open	MRP ring is open if any link is down	Warn	On	On	On	On
MRP Inst 1 ring port down	Any port in the MRP ring is down	Warn	On	On	On	On
MRP Inst 2 ring multiple MRM error	MRP instance error having multiple managers in the ring	Warn	On	On	On	On
MRP Inst 2 ring One Side Rx error	MRP instance received on a single side	Warn	On	On	On	On
MRP Inst 2 ring open	MRP ring is open if any link is down	Warn	On	On	On	On
MRP Inst 2 ring port down	Any port in MRP ring is down	Warn	On	On	On	On
MRP Inst 3 ring multiple MRM error	MRP instance error having multiple managers in the ring	Warn	On	On	On	On
MRP Inst 3 ring One Side Rx error	MRP instance received on a single side	Warn	On	On	On	On
MRP Inst 3 ring open	MRP ring is open if any link is down	Warn	On	On	On	On

Name	Trigger condition	Level	Latch	Trap	Log	LED & relay
MRP Inst 3 ring port down	Any port in the MRP ring is down	Warn	On	On	On	On
MRP Inst 4 ring multiple MRM error	MRP Instance error having multiple managers in the ring	Warn	On	On	On	On
MRP Inst 4 ring One Side Rx error	MRP instance received on a single side	Warn	On	On	On	On
MRP Inst 4 ring open	MRP ring is open if any link is down	Warn	On	On	On	On
MRP Inst 4 ring port down	Any port in MRP ring is down	Warn	On	On	On	On
New STP root	Bridge has become the new spanning tree root bridge	INFO	Off	Off	Off	Off
NTP service status changed	NTP service availability status changed	Info	On	On	On	Off
Operator Level Password Changed	Operator user password is changed	Note	Off	On	On	Off
Port placed in Quarantined VLAN	Port is placed in quarantined or Guest VLAN type	Note	On	Off	On	On
Port security violated	Access is restricted for the port	Warn	On	On	On	On
RADIUS authenticate key changed	The RADIUS server authentication key changed	Note	Off	On	On	Off
RADIUS server unreachable	A reachable RADIUS server went unreachable	Warn	On	On	On	Off
RADIUS service status changed	Radius service availability status is changed	Info	On	On	On	Off
Received looped back BPDU	STP port received loopback BPDU due to simulation or faulty hardware	Error	On	On	On	On
Remote Syslog server unreachable	A reachable Remote Syslog server went unreachable	Warn	On	Off	Off	Off
SFP DDM Alarm	Signals higher-priority, critical threshold breaches in temperature, supply voltage, TX bias current, TX optical power, or RX optical power	Warn	On	On	On	On
SFP DDM Warning	Indicates early, lower-priority deviations in monitored parameters such as temperature, supply voltage, TX bias current, TX optical power, and RX optical power	Warn	On	On	On	On
SNMP authenticate key changed	SNMP authentication key is changed	Note	Off	On	On	Off
SNMP authentication failed	SNMP authentication failed due to incorrect authentication key	Warn	On	On	On	Off
SNMP community changed	SNMP community string is changed	Note	Off	On	On	Off
SNMP private Key changed	SNMP privacy key is changed	Note	Off	On	On	Off
SSH user pub key add failed	SSH user public key add failed due to an invalid key	Warn	On	On	On	On

Name	Trigger condition	Level	Latch	Trap	Log	LED & relay
STP events	STP protocol operational event related to ports, messages, or topology	Info	Off	Off	On	Off
STP topology change	STP topology change as port transitioned from Learning to Forwarding, or Forwarding to Discarding	Info	Off	Off	Off	Off
Tacacs+ authenticate key changed	Tacacs+ server authentication key changed	Note	Off	On	On	Off
TACACS+ response invalid	TACACS+ server response is invalid or no response received	Warn	On	On	On	On
TACACS+ server unreachable	A reachable TACACS+ server went unreachable	Warn	On	On	On	Off
TACACS+ service status changed	TACACS+ service availability status is changed	Info	On	On	On	Off
Unknown privKey from SNMPv3 user	SNMP operation failed due to unknown privacy key for SNMPv3 user	Warn	On	On	On	Off
WeakPswdAdmin	Configured weak admin password	Warn	On	On	On	Off
WeakPswdGuest	Configured weak guest password	Warn	On	On	On	Off
WeakPswdOper	Configured weak operator password	Warn	On	On	On	Off
WeakRadiusBackupKey	Radius backup server authentication key is weak	Warn	On	On	On	Off
WeakRadiusPrimaryKey	Radius primary server authentication key is weak	Warn	On	On	On	Off
WeakSnmpAuthKey	SNMP authentication key is weak	Warn	On	On	On	Off
WeakSnmpPrivKey	SNMP privacy key is weak	Warn	On	On	On	Off
WeakSSHKey	SSH key is weak	Warn	On	On	On	Off
WeakSSLKey	SSL key is weak	Warn	On	On	On	Off
WeakTacacsBackupKey	Tacacs+ backup server authentication key is weak	Warn	On	On	On	Off
WeakTacacsPrimaryKey	Tacas+ primary server authentication key is weak	Warn	On	On	On	Off

Non-configurable alarms

Name	Level	Latch	Trap	Log	LED & Relay
Bootp - cfg transfer failed	Error	On	On	On	On
Bootup error	Critical	On	Off	On	On
Bouncing link	Critical	On	On	On	On
Bundle port inconsistent speed	Error	On	On	On	On
ClkMgr Out of Resources	Warn	On	No	On	On

Name	Level	Latch	Trap	Log	LED & Relay
ClkMgr PrimarySource Failed	Warn	On	Off	On	On
Crashlog created	Critical	On	Off	No	On
Daughter card reading failed	Critical	On	On	On	On
Device Error	Critical	On	On	Off	On
Fast link detection disabled	Critical	On	On	On	On
File Transfer Happened	Note	Off	On	On	Off
Heap error	Alert	On	Off	On	On
Intermittent link	Error	On	On	On	On
Invalid configuration	Critical	On	Off	Off	On
LLDP remote table changed	Info	Off	On	On	Off
Local Console Disabled	Note	Off	On	On	Off
Local Console Enabled	Note	Off	On	On	Off
New active STP topology	Info	Off	On	Off	Off
Real Time Clock failed	Error	On	Off	On	On
RMON alarm	Info	On	Off	On	On
ROS FPGA compatibility alarm	Warn	On	Off	On	Off
Rx Buffer Low	Note	On	Off	On	On
SFP Alarm	Error	On	On	On	On
Stack overflow	Alert	On	Off	On	On
Unable to obtain IP address	Critical	On	On	On	On
Unresolved speed	Error	On	On	On	On
Watchdog reset	Alert	On	Off	On	On

5.5 Managing the configuration file

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

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

5.5.1 Configuring data encryption

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

Note

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

Note

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

Note

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

Note

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

⚠ NOTICE

Configuration hazard – risk of communication disruption

Never downgrade the RUGGEDCOM ROS software version beyond RUGGEDCOM ROS v5.10 when encryption is enabled. Make sure the device has been restored to factory defaults before downgrading.

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

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

Parameter	Description
`Confirm Passphrase`	**Synopsis:** A string up to 31 characters long This passphrase is used as a secret key to encrypt the configuration data. Encrypted data can be decrypted by any device configured with the same passphrase.

3. Click **Apply**.

5.5.2 Updating the configuration file

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

Note

For information about uploading/downloading files, refer to "Uploading/downloading files" (Page 51).

- 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)

⚠ NOTICE

Configuration hazard – risk of data loss

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

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

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

5.6 Managing MMS

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

5.6.1 Understanding MMS

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

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

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

5.6.1.1 MMS reporting

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

The MMS Report is based on the *MMS Sessions Allowed* parameter, which controls how many clients can build MMS connections simultaneously to the RUGGEDCOM ROS bridge device. For more information about configuring MMS reporting, refer to "Configuring IP services" (Page 94).

5.6.1.2 Reports/data sets

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

- **ChannelLinkStatus**
  A time-based report belonging to the logical node LCCH, indicating the working status of the channel. It includes the data objects ChLiv (channel live) and RedChliv (redundant channel live, for RNA equipped devices only).
- **ChannelStatistics**
  A time-based report belonging to the logical node LCCH, indicating the static data of the channel. It includes the data objects FerCh (frame error rate channel), RxCnt (received counter), TxCnt (transmitted counter), RedFerCh (redundant frame error rate channel, for RNA equipped devices only) and RedRxCnt (redundant received counter, for RNA equipped devices only).
- **LLDPStatus**
  A time-based report belonging to the logical node LPLD, indicating the LLDP status of the device. It includes three data objects: LPLD.RemPortId (remote port identifier), LPLD.RemChsId (remote port chassis identifier) and LPLD.RemAddr (remote system management address).

- **PortLinkStatus**
  An event-driven report belonging to the logical node LPCP, indicating the device's physical port MAU status. It includes the data object LPCP.Mau (medium attachment unit link status).
- **PortStatistics**
  A time-based report belonging to the logical node LPCP, indicating the device's physical port working status. It includes four data objects: LPCP.AutoNgt (If true, the port is auto-negotiation), LPCP.RxCnt (Number of messages received since last reset), LPCP.TxCnt (number of messages sent since last reset) and LPCP.FerPort (frame error rate on the port).
- **RSTPStatus**
  An event-driven report belonging to the logical node LBRI, indicating the RSTP status of the device. It includes three data objects: LBRI.RstpRoot (device is RSTP root or not), LBRI.RstpTopoCnt (RSTP topology change count) and LBSP.RstpSt (RSTP port state).
- **SystemStatus**
  An event-driven report belonging to the logical node LPHD, indicating the device's working status. It includes two data objects: LPHD.PhyHealth (device health status) and LPHD.PwrSupAlm (device power supply alarm status).

Note

The files **ruggedcom.icd** (IEC61850 IED Capability Description of the device) and **ruggedcom.iid** (IEC61850 Instantiated IED Description of the device) list the logical nodes supported by RUGGEDCOM ROS. For information about downloading these files, refer to "Uploading/downloading files" (Page 51).

5.6.1.3 Supported logical nodes

RUGGEDCOM ROS supports the following logical nodes:

Logical node	Description
LLN0	A common logical node providing generic information about the device as a whole, such as the vendor name and software version.
LPHD (Physical Device)	A logical node bearing system level information about the physical device, such as the system name and system description.
LBRI (Bridge)	A logical node providing spanning tree related information when the device functions as a bridge, such as RSTP priority and RSTP hello time.
LPCP (Physical Communication Port)	A logical node providing port specific information for each physical interface on the device, such as port admin status and port auto negotiation status.
LPLD (Port Link Discovery)	A logical node providing port specific information related to LLDP (Link Layer Discovery Protocol) for each physical interface on the device, such as local port ID and remote port ID.
LBSP (Bridge Spanning tree Port)	A logical node providing port specific information related to spanning tree for each physical interface on the device, such as RSTP port state and RSTP edge port status.

Logical node	Description
LCMF (Communication channel MAC Filtering)	A logical node bearing filtering information related to Multicast MAC addresses, such as the white list of multicast MAC addresses and related VLAN IDs.
LCVF (Communication channel VLAN Filtering)	A logical node providing port specific information related to VLAN configuration, such as port VLAN ID and CoS priority.
LCCH (Physical Communications Channel Supervision)	A logical node providing information related to each physical channel or each pair of link level redundant physical channels.

5.6.2 Viewing a list of preconfigured MMS reports

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

This table displays the following information:

Parameter	Description
`Name`	**Synopsis:** A string up to 32 characters long or [SysStatus] **Default:** SysStatus The MMS report name (i.e.the name of the data set).
`Status`	**Synopsis:** [Disabled | Enabled] **Default:** Disabled The MMS reporting status initiated or changed by the client application. If any client application enables a data set's report functionality, the status of this data set is 'Enabled'. If no client application enables the data set's report functionality, the status of this data set is 'Disabled'.
`EventDriven`	**Synopsis:** [False | True] **Default:** True The reporting criteria: • **True** – Reporting is event-driven • **False** – Reporting is time-based
`Period`	**Synopsis:** An integer between 30 and 10800 or [Disabled] **Default:** 300 The reporting interval, in seconds, for time-based reports. This parameter is 'Disabled' for event-driven reports.

For information about modifying an MMS report, refer to "Configuring an MMS report" (Page 126).

5.6.3 Configuring an MMS report

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

To configuring an MMS report, do the following:

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

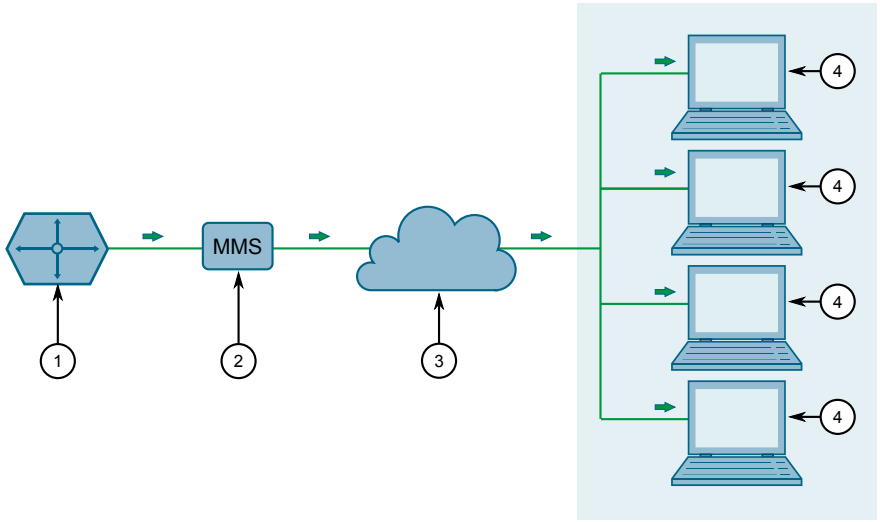
Parameter	Description
`Period`	**Synopsis:** An integer between 30 and 10800 or [Disabled] **Default:** 300 The reporting interval, in seconds, for time-based reports. This parameter is 'Disabled' for event-driven reports.

4. Click **Apply**.

5.6.4 Example: Configuring MMS reports

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

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



① RUGGEDCOM ROS
② MMS report
③ LAN

④ Client

Figure 5.1 Topology – MMS

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

1. On the client side, do the following:

   Note

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

   a. Enable or disable specific MMS reports, as desired. For a list of available reports in RUGGEDCOM ROS, refer to "Reports/data sets" (Page 123).

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

2. In RUGGEDCOM ROS, do the following:

   a. Configure the number of MMS sessions allowed, to specify how many clients will be receiving reports. Per the topology, 4 sessions are allowed. For more information about configuring MMS sessions, refer to "Configuring IP services" (Page 94).

   b. If time-based reports are selected on the client side, configure the reporing time interval as desired. For more information, refer to "Configuring an MMS report" (Page 126).

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

6 Security

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

6.1 Configuring passwords

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

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

   Note

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

   - Must not be less than 8 characters in length.
   - Must not include the username or any 4 continuous characters found in the username. For example, if the username is *Subnet25*, the password may not be *subnet25admin*, *subnetadmin* or *net25admin*. However, *net-25admin* or *Sub25admin* is permitted.
   - Must have at least one alphabetic character and one number. Special characters are permitted.
   - Must not have more than 3 continuously incrementing or decrementing numbers. For example, *Sub123* and *Sub19826* are permitted, but *Sub12345* is not.

   An alarm will generate if a weak password is configured. The weak password alarm can be disabled by the user. For more information about disabling alarms, refer to "Managing alarms" (Page 110).

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

Parameter	Description
`Auth Type`	**Synopsis:** [Local | RADIUS | TACACS+ | RADIUSorLocal | TACACS+orLocal | RADIUSandLocal | TACACS+andLocal] **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.

Parameter	Description
	Settings: • **Local** – Authentication from the local Password Table. • **RADIUS** – Authentication using a RADIUS server for network access only (HTTP/HTTPS, SSH, RSH, Telnet). For console access, authenticate from the local Password Table. If local authentication fails, then authenticate using RADIUS server. • **TACACS+** – Authentication using a TACACS+ server for network access only (HTTP/HTTPS, SSH, RSH, Telnet). For console access, authenticate from the local Password Table. If local authentication fails, then authenticate using TACACS + server. • **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. • **RADIUSandLocal** – Authentication using RADIUS. If failed, authenticate from the local Password Table. • **TACACS+andLocal** – Authentication using TACACS+. If failed, authenticate from the local Password Table.
`Guest Username`	**Synopsis:** A string up to 15 characters long **Default:** guest Related password is in field Guest Password; view only, cannot change settings or run any commands.
`Guest Password`	**Synopsis:** A string up to 19 characters long Related username is in field Guest Username; view only, cannot change settings or run any commands.
`Confirm Guest Password`	**Synopsis:** A string up to 19 characters long Related username is in field Guest Username; view only, cannot change settings or run any commands.
`Operator Username`	**Synopsis:** A string up to 15 characters long **Default:** operator Related password is in field Oper Password; cannot change settings; can reset alarms, statistics, logs, etc.
`Operator Password`	**Synopsis:** A string up to 19 characters long Related username is in field Oper Username; cannot change settings; can reset alarms, statistics, logs, etc
`Confirm Operator Password`	**Synopsis:** A string up to 19 characters long Related username is in field Oper Username; cannot change settings; can reset alarms, statistics, logs, etc.

Parameter	Description
Admin Username	**Synopsis:** A string up to 15 characters long **Default:** admin Related password is in field Admin Password; full read/write access to all settings and commands.
Admin Password	**Synopsis:** A string up to 19 characters long Related username is in field Admin Username; full read/write access to all settings and commands.
Confirm Admin Password	**Synopsis:** A string up to 19 characters long Related username is in field Admin Username; full read/write access to all settings and commands.
Password Minimum Length	**Synopsis:** An integer between 1 and 17 **Default:** 1 Configure the password string minimum length. The new password shorter than the minimum length will be rejected.

3. Click **Apply**.

6.2 Clearing private data

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

To clear private data, do the following:

Note

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

1. Connect to the device via the RS-232 serial console port. For more information, refer to "Connecting directly" (Page 43).
2. Cycle power to the device. As the device is booting up, the following prompt will appear:

```
Press any key to start
```

3. Within four seconds, press **CTRL** + **r**. The access banner will appear, followed by the command prompt:

```
>
```

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

   ```
   clear private data
   ```

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

6.3 Managing user authentication

This section describes the various methods for authenticating users.

6.3.1 Authentication methods

RUGGEDCOM ROS supports Local, RADIUS, TACACS+, RADIUS or Local, and TACAS+ or Local server authentication. The chosen method is configurable using the **Auth Type** parameter.

For more information about configuring the **Auth Type** parameter, refer to "Configuring passwords" (Page 129).

The following table shows user access capabilities in different scenarios using the supported authentication methods.

Auth Type	Authentication Method/Scenario	Login Access Credentials	Access Method	
			Local Console	Network (SSH/ Telnet/WebUI)
Local	Local authentication	Local	✓	✓
	RADIUS server	RADIUS	×	×
RADIUS	RADIUS server authentication	RADIUS	✓	✓
	Local authentication	Local	✓	×
	Server unreachable	Local	✓	×
		RADIUS	×	×
	Wrong Shared Key	Local	✓	×
		RADIUS	×	×
	Wrong Destination Port	Local	✓	×
		RADIUS	×	×
TACACS+	TACACS+ server authentication	TACACS+	✓	✓
	Local authentication	Local	✓	✓
	Server unreachable	Local	✓	×
		TACACS+	×	×

Auth Type	Authentication Method/Scenario	Login Access Credentials	Access Method	
			Local Console	Network (SSH/ Telnet/WebUI)
	Wrong Shared Key	Local	✓	×
		TACACS+	×	×
	Wrong Destination Port	Local	✓	×
		TACACS+	×	×
RADIUSorLocal	RADIUS server authentication	RADIUS	✓	✓
	Local authentication	Local	×	×
	Server unreachable	Local	✓	✓
		RADIUS	×	×
	Wrong Shared Key	Local	×	×
		RADIUS	×	×
	Wrong Destination Port	Local	✓	✓
		RADIUS	×	×
TACACS+orLocal	TACACS+ server authentication	TACACS+	✓	✓
	Local authentication	Local	✓	×
	Server unreachable	Local	✓	✓
		TACACS+	×	×
	Wrong Shared Key	Local	×	×
		TACACS+	×	×
	Wrong Destination Port	Local	✓	✓
		TACACS+	×	×
RADIUSandLocal	RADIUS server authentication	RADIUS	✓	✓
	Local authentication	Local	✓	✓
	Server unreachable	Local	✓	✓
		RADIUS	×	×
	Wrong Shared Key	Local	✓	✓
		RADIUS	×	×
	Wrong Destination Port	Local	✓	✓
		RADIUS	×	×
TACACS+andLocal	TACACS+ server authentication	TACACS+	✓	✓
	Local authentication	Local	✓	✓
	Server unreachable	Local	✓	✓
		TACACS+	×	×
	Wrong Shared Key	Local	✓	✓
		TACACS+	×	×

Auth Type	Authentication Method/Scenario	Login Access Credentials	Access Method	
			Local Console	Network (SSH/ Telnet/WebUI)
	Wrong Destination Port	Local	✓	✓
		TACACS+	×	×

6.3.2 Configuring user name extensions

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

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

Note

Extensions are ignored when IEEE 802.1x port-based authentication is enabled. RUGGEDCOM ROS will remain transparent and not make any changes to the username. For more information about IEEE 802.1x authentication, refer to "Port security concepts" (Page 141).

To configure a username extension, do the following:

1. Navigate to ***Administration » Configure Security Server » Configure Common Security Parameters***. The **Common Security Parameters** form appears.
2. Configure the following parameter(s) as required:

Parameter	Description
`Username Extension`	**Synopsis:** A string up to 127 characters long Defines the format of all user names sent to a RADIUS or TACACS+ server for authentication. A prefix or suffix can be added to the user name using predefined keywords (wrapped in % delimiters) or user-defined strings. Delimited values include: %Username%: The name associated with the user profile (e.g. admin, oper, etc.) %IPaddr%: The management IP address of the switch that acts as a Network Access Server (NAS). %SysName%: The system name given to the device. %SysLocation%: The system location given to the device. All pre-defined keywords are case-insensitive. Examples: %Username%@ABC.com %Username%_%SysLocation%

Parameter	Description
	If an extension is not defined, only the user name is sent to the authentication server.

3. Click **Apply**.

6.3.3 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

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

Note

For port security, RUGGEDCOM ROS supports Protected Extensible Authentication Protocol (PEAP), EAP Transport Layer Security (EAP-TLS) and EAP-MD5. EAP-MD5 is not considered a secure protocol and should not be used by the supplicant. Where possible, the supplicant should be configured to use the certificate-based EAP-TLS authentication protocol to communicate with the RADIUS server.

Note

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

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

6.3.3.1 Configuring the RADIUS server

Note

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

Note

The **Attribute** parameter value is case-sensitive.

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

Attribute	Value
Vendor-Specific	Vendor-ID: 15004 Format: String Number: 2 Attribute: { guest, operator, admin }

Note

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

6.3.3.2 Configuring the RADIUS client on the device

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

For CLI commands related to configuring the RADIUS client on the device, refer to "Available CLI commands" (Page 24).

⚠ NOTICE

Security hazard – risk of unauthorized access and/or exploitation

For increased security, Siemens recommends setting both the RADIUS server (if supported) and the RUGGEDCOM ROS Force Msg-Auth attribute to **Yes**.

The Force Message-Authenticator attribute is used to sign packets to ensure their integrity is protected.

When set to **Yes**, RUGGEDCOM ROS requires the Message-Authenticator attribute to be present in the message from the RADIUS server. If the attribute is not present, RUGGEDCOM ROS will return an invalid request, an alarm will be generated and authentication will fail. A message will be written to the syslog.txt file indicating the failed authentication.

When set to **No**, RUGGEDCOM ROS will ignore the Message-Authenticator attribute, and will authenticate whether the attribute is present or not.

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

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

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

Parameter	Description
`Server`	**Synopsis:** A string up to 8 characters long or [Primary] **Default:** Primary This field tells whether this configuration is for a Primary or a Backup Server.
`IP Address`	**Synopsis:** Any valid IP address The Server IP Address.
`Auth UDP Port`	**Synopsis:** An integer between 1 and 65535 **Default:** 1812 The IP Port on server.
`Max Retry`	**Synopsis:** An integer between 1 and 10 **Default:** 2 The maximum number of times the Authenticator will attempt to contact the authentication server to authenticate the user in case of any failure.
`Timeout`	**Synopsis:** An integer between 1000 and 120000 **Default:** 10000 The amount of time in milliseconds the Authenticator will wait for a response from the authentication server.
`Reachable`	**Synopsis:** [--- | Yes | No] The status of the server. Options include: • **---** – The server probe is disabled or the server status is unknown • **Yes** – The server is reachable • **No** – The server is unreachable
`Probe Period`	**Synopsis:** An integer between 1 and 1440 **Default:** 5 Determines how frequently in minutes the RADIUS server is polled for reachability when the Probe Method is ICMP.
`Probe Method`	**Synopsis:** [Disabled | ICMP] **Default:** Disabled Determines the protocol used to probe RADIUS server reachability or disables the reachability check. Options include: • **Disabled** – Disables the reachability check • **ICMP** – The server probe uses ICMP ping. Three consecutive ICMP ping requests with a 500-millisecond timeout are sent

Parameter	Description
	to the server until a response is received. If no response received, a server unreachable alarm is generated.
`Force Msg-Auth attr`	**Synopsis:** [No | Yes] **Default:** No The Force Message-Authenticator attribute. Options include: • **Yes** – The RADIUS client requires that all Access-Accept, Access-Reject, and Access-Challenge packets contain a Message-Authenticator attribute. If any packet does not contain a Message-Authenticator attribute, it will be discarded. • **No** – The RADIUS client does not require a Message-Authenticator attribute, but will accept and validate the Message-Authenticator attribute if it is present in replies to Access-Request packets.
`Auth Key`	**Synopsis:** A string up to 31 characters long The authentication key to be shared with server.
`Confirm Auth Key`	**Synopsis:** A string up to 31 characters long The authentication key to be shared with server.

4. Click **Apply**.

6.3.4 Managing TACACS+ authentication

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

6.3.4.1 Configuring TACACS+

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

For CLI commands related to configuring TACACS+, refer to "Available CLI commands" (Page 24).

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

1. Navigate to ***Administration » Configure Security Server » Configure TacPlus Server » Configure TACACS Plus Server***. The **TACACS Plus Server Table** appears.
2. Select either **Primary** or **Backup** from the table. The **TACACS Plus Server** form appears.

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

Parameter	Description
`Server`	**Synopsis:** A string up to 8 characters long or [Primary] **Default:** Primary This field tells whether this configuration is for a Primary or a Backup Server.
`IP Address`	**Synopsis:** Any valid IP address The Server IP Address.
`Auth TCP Port`	**Synopsis:** An integer between 1 and 65535 **Default:** 49 The IP Port on server.
`Max Retry`	**Synopsis:** An integer between 1 and 10 **Default:** 3 The maximum number of times the Authenticator will attempt to contact the authentication server to authenticate the user in case of any failure.
`Timeout`	**Synopsis:** An integer between 1000 and 120000 **Default:** 1000 The amount of time in milliseconds the Authenticator will wait for a response from the authentication server.
`Reachable`	**Synopsis:** [--- | Yes | No] The status of the server. Options include: • **---** – The server probe is disabled or the server status is unknown • **Yes** – The server is reachable • **No** – The server is unreachable
`Probe Period`	**Synopsis:** An integer between 1 and 1440 **Default:** 5 Determines how frequently in minutes the TACACS+ server is polled for reachability when the Probe Method is ICMP.
`Probe Method`	**Synopsis:** [Disabled | ICMP] **Default:** Disabled Determines the protocol used to probe TACACS+ server reachability or disables the reachability check. Options include: • **Disabled** – Disables the reachability check • **ICMP** – The server probe uses ICMP ping. Three consecutive ICMP ping requests with a 500-millisecond timeout are sent to the server until a response is received. If no response received, a server unreachable alarm is generated.

Parameter	Description
Auth Key	**Synopsis:** A string up to 31 characters long or [mySecret] **Default:** mySecret The authentication key to be shared with server.
Confirm Auth Key	**Synopsis:** A string up to 31 characters long The authentication key to be shared with server.

4. Set the privilege levels for each user type (i.e. admin, operator and guest). For more information, refer to "Configuring user privileges" (Page 140).
5. Click **Apply**.

6.3.4.2 Configuring user privileges

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

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

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

For more information about the **svcmod** CLI command, refer to "Available CLI commands" (Page 24).

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

1. Navigate to ***Administration » Configure Security Server » Configure TacPlus Server » Configure TACPLUS Serv Privilege Config***. The **TACPLUS Serv Privilege Config** form appears.
2. Configure the following parameter(s) as required:

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

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

3. Click **Apply**.

6.4 Managing port security

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

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

Frames to unknown destination addresses are flooded through secure ports.

6.4.1 Port security concepts

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

6.4.1.1 Static MAC address-based authentication

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

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

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

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

6.4.1.2 Static MAC address-based authentication in an MRP ring

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

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

For information about configuring MRP, refer to "Managing the Media Redundancy Protocol (MRP)" (Page 222).

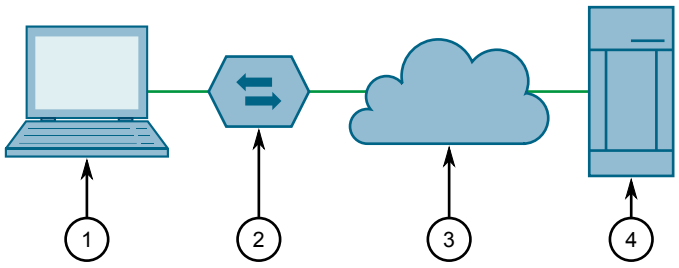
For information about configuring a static MAC address, refer to "Adding a static MAC address" (Page 176).

6.4.1.3 IEEE 802.1X authentication

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

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

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



① Supplicant
② Authenticator switch
③ LAN
④ Authentication server

Figure 6.1 IEEE 802.1X general topology

⚠ NOTICE

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

IEEE 802.1X makes use of the Extensible Authentication Protocol (EAP), which is a generic PPP authentication protocol that supports various authentication methods.

IEEE 802.1X defines a protocol for communication between the supplicant and the Authenticator, referred to as EAP over LAN (EAPOL).

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

Note

The switch supports authentication of one host per port.

Note

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

Standard IEEE 802.1X Port Security

Following successful 802.1X authentication, a supplicant is authorized by RUGGEDCOM ROS on the connected port . The supplicant's MAC address is then installed as a static MAC address entry on either the port's native VLAN (port VLAN ID) or the VLAN assigned from the RADIUS server on the RUGGEDCOM ROS device. Through the standard 802.1X authentication process, a single MAC address may only be authorized on a single VLAN.

802.1X Port Security on Multiple VLANs

Multiple VLAN port security is configurable using the **Security** and **Autolearn** parameters.

When multiple VLAN support is enabled, the standard IEEE 802.1X authentication process begins and authentication frames are exchanged between the supplicant, authenticator switch and authentication server. Once authentication succeeds, the port enters the "Authorized" state, and the MAC address of the connected device is added to the Authorized MAC Addresses table on the VLAN resolved through 802.1X.

Next, RUGGEDCOM ROS begins to learn the same MAC address on multiple VLANs by listening to frames ingressing on this port. The maximum number of VLANs on which the MAC address can be authorized on the port is configurable through the **Autolearn** parameter in the Port Security table. The MAC addresses learned on each of the new VLANs is also added to the Authorized MAC Addresses table.

Once the total number of VLANs reaches the configured **Autolearn** setting, if the same MAC address is found on a new VLAN on this port, then a port security violation alarm is raised to indicate the auto-learn failure on the port, and the MAC address is not learned on the port.

For more information about configuring port security on multiple VLANs, refer to "Configuring port security" (Page 148).

6.4.1.4 IEEE 802.1X authentication with MAC address-based authentication

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

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

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

6.4.1.5 Restricted VLANs

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

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

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

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

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

There are no re-authentication attempts for clients in Guest VLANs. When an EAPOL Start frame is received from the client, the port will revert to the unauthenticated

state, removing the client's access from the Guest VLAN to continue with the authentication process.

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

Port security mode	Client security	Placement following authentication failure
802.1x	802.1x Capable	Quarantine VLAN
	802.1x Not Capable	Guest VLAN
802.1x/MAC-Auth	802.1x Capable	Quarantine VLAN
	802.1x Not Capable	Quarantine VLAN

For more information about configuring a Guest/Quarantine VLAN, refer to "Configuring port security" (Page 148).

6.4.1.6 Assigning VLANS with tunnel attributes

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

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

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

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

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

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

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

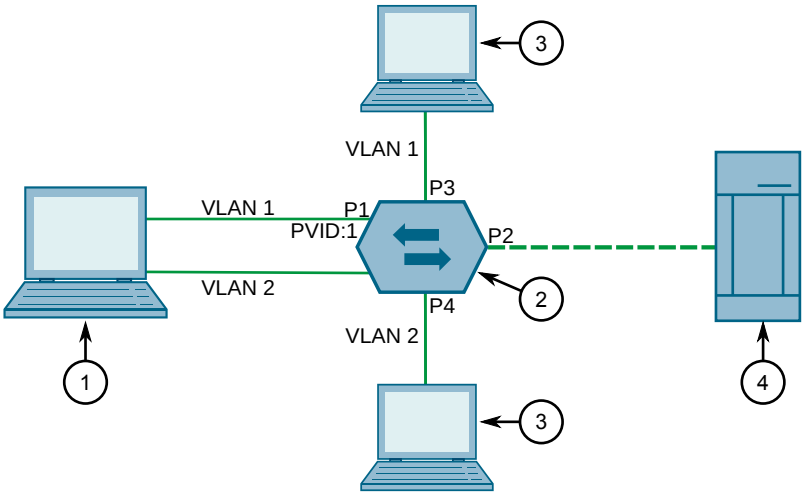
6.4.1.7 Example: 802.1X port security on multiple VLANs

This example demonstrates how to configure 802.1X port security on multiple VLANs.

In the following example, a device (D1) with a single MAC address is connected to RUGGEDCOM ROS via port P1, a VLAN trunk port, on VLANs 1 and 2. The device communicates with other devices on VLAN 1 following authentication from the RADIUS authenication server. Once authenticated on VLAN 1, the MAC address is auto learned on VLAN 2 by RUGGEDCOM ROS and can then also communicate with the other devices.

⚠ NOTICE

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



① Device D1
② RUGGEDCOM ROS device
③ Connected devices
④ Authentication server

Figure 6.2 Topology – Port security on multiple VLANs

To configure the device per the topology, do the following:

1. Connect device D1 to port P1 on the RUGGEDCOM ROS device.
2. Add VLAN 1 and VLAN 2.

   For more information about adding VLANs, refer to "Adding a static VLAN" (Page 171).
3. Configure PVID 1 on port P1.

   For more information, refer to "Configuring VLANs for specific Ethernet ports" (Page 169).

4. In the **Ports Security** form, configure the following parameters on port P1 of the RUGGEDCOM ROS device:

Parameter	Value
Security	802.1X
Autolearn	2[a]

[a] Set a value greater than 1 to enable VLAN aware mode.

5. In the **Port VLAN Parameters** form, configure the following parameter on port P1 of the RUGGEDCOM ROS device:

Parameter	Value
Type	Trunk

6. To verify the configuration, make sure device D1 can communicate with the connected devices on both VLAN 1 and VLAN 2. The MAC address of device D1 should appear in the Autorized MAC Address table.

6.4.2 Viewing a list of authorized MAC addresses

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

Note

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

This table displays the following information:

Parameter	Description
`Port`	Port on which MAC address has been learned.
`MAC Address`	**Synopsis:** ##-##-##-##-##-## where ## ranges 0 to FF Authorized MAC address learned by the switch.
`VID`	**Synopsis:** An integer between 0 and 65535 VLAN Identifier of the VLAN upon which the MAC address operates.
`Security`	**Synopsis:** [Static MAC | 802.1X | 802.1x/MAC-Auth] Security mode of the port on which the MAC address is authorized.

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

- Configure port security. For more information, refer to "Configuring port security" (Page 148).
- Configure IEEE 802.1X. For more information, refer to "Configuring IEEE 802.1X" (Page 149).

6.4.3 Configuring port security

To configure port security, do the following:

1. Navigate to ***Network Access Control » Port Security » Configure Ports Security***. The **Ports Security** table appears.
2. Select an Ethernet port. The **Ports Security** form appears.
3. Configure the following parameter(s) as required:

Parameter	Description
`Port`	The port number.
`Security`	**Synopsis:** [Off | Static MAC | 802.1X | 802.1x/MAC-Auth] **Default:** Off Enables or disables security feature for the port. Several 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 unknown behind which port they are going to reside), there is still an option to configure the switch to auto-learn certain number of MAC addresses. Once learned, they don't age out; they can only be removed from the static MAC table by user. • IEEE 802.1X standard authentication. In VLAN-aware mode, if the 'Autolearn' field is set to a number greater than '1', after the Supplicant's MAC address is authorized on the port's PVID, the same MAC address can be detected and authorized on other VLANs, until the total number of VLANs reaches the setting of 'Autolearn'. • 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.
`Quarantine VID`	**Synopsis:** An integer between 1 and 4096 or [None] **Default:** None The VLAN identifier for the Quarantine VLAN. Only applicable when the 'Security' field has been set to '802.1x' or '802.1x/MAC-Auth'. The port will be placed in the Quarantine VLAN if a client fails authentication.
`Guest VID`	**Synopsis:** An integer between 1 and 4096 or [None] **Default:** None The VLAN identifier for the Guest VLAN. Only applicable when the 'Security' field has been set to '802.1x'. The port will be placed in the Guest VLAN if a client does not support the 802.1x standard.
`Autolearn`	**Synopsis:** An integer between 1 and 16 or [None] **Default:** None Only applicable when the 'Security' field has been set to 'Static MAC', or '802.1X'. In 'Static MAC' mode, it specifies the

Parameter	Description
	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. In '802.1X' mode, it specifies the maximum number of VLANs on which the Supplicant's MAC address can be authorized on the port. If this parameter is set to 'None' or '1', the MAC address can be authorized on one VLAN over 802.1X standard authentication; if it is set to a number greater than '1', after the MAC address has been authorized over 802.1X standard authentication, the number of additional VLANs on which the MAC address can be detected and authorized on the port is the configured number minus 1.
`Shutdown Time`	**Synopsis:** An integer between 1 and 86400 or [Until reset | Don't shutdown] **Default:** Don't shutdown Specifies for how long to shut down the port, if a security violation occurs.
`Status`	**Synopsis:** A string up to 31 characters long Describes the security status of the port.

Note

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

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

Note

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

4. Click **Apply**.

6.4.4 Configuring IEEE 802.1X

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

1. Navigate to ***Network Access Control » Port Security » Configure 802.1X***. The **802.1X Parameters** table appears.
2. Select an Ethernet port. The **802.1X Parameters** form appears.
3. Configure the following parameter(s) as required:

Parameter	Description
`Port`	The port number.

Parameter	Description
txPeriod	**Synopsis:** An integer between 1 and 65535 **Default:** 30 The time to wait for the Supplicant's EAP Response/Identity packet before retransmitting an EAP Request/Identity packet.
quietPeriod	**Synopsis:** An integer between 0 and 65535 **Default:** 60 The period of time not to attempt to acquire a Supplicant after the authorization session failed.
reAuthEnabled	**Synopsis:** [No | Yes] **Default:** No Enables or disables periodic re-authentication.
reAuthPeriod	**Synopsis:** An integer between 60 and 86400 **Default:** 3600 The time between periodic re-authentication of the Supplicant.
reAuthMax	**Synopsis:** An integer between 1 and 10 **Default:** 2 The number of re-authentication attempts that are permitted before the port becomes unauthorized.
suppTimeout	**Synopsis:** An integer between 1 and 300 **Default:** 30 The time to wait for the Supplicant's response to the authentication server's EAP packet.
serverTimeout	**Synopsis:** An integer between 1 and 300 **Default:** 30 The time to wait for the authentication server's response to the Supplicant's EAP packet.
maxReq	**Synopsis:** An integer between 1 and 10 **Default:** 2 The maximum number of times to retransmit the authentication server's EAP Request packet to the Supplicant before the authentication session times out.

4. Click **Apply**.

6.5 Managing SSH/TLS keys and certificates

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

⚠ NOTICE

Security hazard – risk of unauthorized access and/or exploitation

Siemens recommends the following actions before commissioning the device:

- Replace the factory-provisioned, self-signed TLS certificate with one signed by a trusted Certificate Authority (CA). The keys and certificates must be unique for each device. Do not reuse certificates and keys on multiple devices or servers.
- Configure the SSH client to use *diffie-hellman-group14-sha1* or better.

Note

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

Each RUGGEDCOM ROS device is shipped with a unique ECC 256 self-signed TLS certificate and an RSA 2048 SSH host key pair that are generated at and provisioned by the factory. The administrator may upload a new certificate and keys to the system at any time, which will overwrite the existing ones. In addition, CLI commands are available to regenerate TLS certificate and key pair as well as the SSH host key pair.

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

- **Default**
  A default certificate and TLS/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 TLS certificate or TLS/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 TLS (HTTPS) sessions can be served until generated or provisioned keys are available.

  Note

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

  Note

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

- **Auto-Generated**
  If a default TLS certificate and TLS/SSH keys are in use, RUGGEDCOM ROS immediately begins to generate a unique certificate and TLS/SSH keys for the

device in the background. This process may take several minutes to complete depending on the requested key length and how busy the device is at the time. If a custom certificate and keys are loaded while auto-generated certificates and keys are being generated, the generator will abort and the custom certificate and keys and will be used.

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

Note

The RSA or EC private key corresponding to the TLS certificate must be appended to the certificate in the **ssl.crt** file.

6.5.1 TLS certificates

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

- X.509 v3 digital certificate format
- PEM format
- For RUGGEDCOM ROS Controlled versions: RSA key pair, 1024, 2048 or 3072 bits; or NIST P-256, P-384 or P-521

Note

Elliptic curve keys smaller than P-256 bits in length are not supported.

Note

RSA keys smaller than 2048 bits in length are not recommended.

Two standard PEM files are required: the TLS certificate and the corresponding RSA private key file. These are concatenated into the resulting **ssl.crt** file, which may then be uploaded to RUGGEDCOM ROS. For more information about transferring files between the device and a host computer, refer to "Uploading/downloading files" (Page 51).

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

6.5.2 SSH host key

Note

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

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

- PEM format
- DSA key pair, 1024, 2048 or 3072 bits in length
- RSA key pair, 1024, 2048 or 3072 bits in length
- SSH-Ed25519 key pair, 256 bits in length (recommended)

Note

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

Note

To avoid using weak MAC algorithms, set SSH client preferences to use GCM ciphers. For a list of supported algorithms, refer to "Cipher suites and algorithms" (Page 438).

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

```
# RSA key size:
BITS=2048

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

For an example of an SSH key generated by RUGGEDCOM ROS, refer to "Certificate and key examples" (Page 157).

6.5.3 Managing SSH public keys

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

6.5.3.1 Public key requirements

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

- Header
- Key

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

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

The key must be in RFC4716, RFC4253 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 RFC4716 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 RFC4253 format:

```
2,userkey,admin,active,bob
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDH0NivR8zzbTxlecvFPzR/
GR24NrRJa0Lc7scNsWRgi0XulHuGrRLRB5RoQ39+spdig88Y8CqhRI49XJx7uLJe0Su3RvyNYz1jkdSwHq2h
SZCpukJxJ6CK95Po/sVa5Gq2gMaHowiYDSkcx+AJywzK/eM6i/jc125lRxFPdfkj74u
+ob3PCvmIWz5z3WAJBrQU1IDPHDets511WMu8O9/mAPZRwjqrWhRsqmcXZuv5oo54wIopCAZ
So20SPzM2VmXFuUsEwDkvYMXLJK1koJPbDjH7yFFC7mwK2eMU/
oMFFn934cbO5N6etsJSvplYQ4pMCw6Ok8Q/bB5cPSOa/rAt bob@work
```

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

```
7,userkey,admin,active,Fiona
-----BEGIN RSA PUBLIC KEY-----
MIIBCgKCAQEAqa+vrdUi9NWYdccrRdm9Se/iRs/vwL5lB4TETTTowXeEgKQ1+PW9
R/rroiT11hRrJqz24uVIji2FjipzLsHcsAd6hHRj1dcg5b4Ftzl+tIjg2vwMaEOw
lI76MCkTvfoPSt70m3Wx+bChHFghqvdq/+1P0z0OhnWF8UuGmv1AVpDU+n/FOaFu
CUKx+bXOt/P9r5DYLRmEz07UUupo4P8F9xLgzJvWqGj+ikXYl9tMk+Ggo6cyD0vk
Bl9/4X8QwGva4xkncjlEGQZtHpr9mEhjrKfMpzAZJ9Mtx08MH7RdbTmflYxUmo1I
YNHS6cXruvRWoBeDZM8OSluabPiIDYx4eQIDAQAB
-----END RSA PUBLIC KEY-----
```

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

- Key type must be either SSH-Ed25519 key pair (256 bits), DSA 1024, 2048 or 3072 bits, or RSA 1024, 2048 or 3072 bits
- Key size must not exceed 4000 base64 encoded characters
- Entry Type in the header must not exceed 8 ASCII characters
- Access Level in the header must not exceed 8 ASCII characters (*operator* is maximum)
- Revocation status in the header must not exceed 8 ASCII characters (*inactive* is maximum)
- User Name must not exceed 12 ASCII characters

6.5.3.2 Adding a public key

Administrators can add one or more public keys to RUGGEDCOM ROS by uploading a locally-created file to the *sshaddpub.keys* file. The content of the file is appended to the existing entries in the *sshpub.keys* file.

⚠ NOTICE

Configuration hazard – risk of communication disruption

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

To add keys, do the following:

1. Create a public key file via a host computer.
2. Transfer the public key file to the device using SFTP or Xmodem. For more information about transferring files, refer to "Uploading/downloading files" (Page 51).
3. Log in to the device as an admin user and access the CLI shell. For more information about accessing the CLI shell, refer to "Using the command line interface" (Page 24).

4. Check the system log to make sure the files were properly transferred. For more information about viewing the system log, refer to "Viewing local and system logs" (Page 56).

6.5.3.3 Viewing a list of public keys

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

To view public keys, do the following:

1. Log in to the device as an admin user and access the CLI shell. For more information about accessing the CLI shell, refer to "Using the command line interface" (Page 24).
2. At the CLI prompt, type:

   ```
   sshpubkey list
   ```

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

6.5.3.4 Updating a public key

Admin users can update public keys.

To update public keys, do the following:

1. Log in to the device as an admin user and access the CLI shell. For more information about accessing the CLI shell, refer to "Using the command line interface" (Page 24).
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. • `{ 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 **Note** The user public key ID must be a number between 0 and 9999.
`sshpubkey update_al { AL }`	Updates the access level of a user public key. • `{ AL }` is the access level (admin, operator or guest) of the public key to be updated

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

6.5.3.5 Deleting a public key

Admin users can delete one or more public keys.

To delete a public key, do the following:

1. Log in to the device as an admin user and access the CLI shell. For more information about accessing the CLI shell, refer to "Using the command line interface" (Page 24).
2. At the CLI prompt, type:

   ```
   sshpubkey list
   ```

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

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

6.5.4 Certificate and key examples

For TLS, certificates must meet the requirements outlined in "TLS certificates" (Page 152).

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 TLS certificate and key:

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

```
A1UdEwQCMAAwHQYDVR0OBBYEFER0utgQOifnrflnDtsqNcnvRB0XMA0GCSqGSIb3
DQEBBQUAA4GBAHtBsNZuh8tB3kdqR7Pn+XidCsD70YnI7w0tiy9yiRRhARmVXH8h
5Q1rOeHceri3JFFIOxIxQt4KgCUYJLu+c9Esk/nXQQar3zR7IQCt0qOABPkviiY8
c3ibVbhJjLpR2vNW4xRAJ+HkNNtBOg1xUlp4vOmJ2syYZR+7XAy/OP/S
-----END CERTIFICATE-----
-----BEGIN RSA PRIVATE KEY-----
MIIEpQIBAAKCAQEAn3UT94ZjlmBjygLXaA21ULum7EDmgsvFvg2tKYyaMj1en5UW
x172GvlDLUm5EwGmcG9u6DyuO3wOyv/taD1OUFkZA1W7cPu9NjeTtZjIQCx33xSU
1d6INMi2oOzwJmWzqwqIkIgy0uMdw78be4n7359U0UOOEtCStOmUfdw34jv6c38J
8sb+lC/FktX8Eilka4mDr07tf/ivC2kdwpPlGZIKt/xjcwjOsNHIBSfqbEbg5mO3
9OAPqsPRWKhBQZ6rM8aqEQjGPlrSTTNHrxO/CYVxAh0gtz+6qUytL3zi7Z9P7EzD
H8V8qNdXRNN0w5hsh2A5ZJj6+cbQJm0JHQeOowIDAQABAoIBAH2zXqUfBLyTibbC
3KoDPG7DLwhI9S4gkuaKg3ogg6GdLU2hys4p9to2qxU1a7cm8tzpi0V6KGNuHX87
lxw4T9cZFZXCbLvZR0RJNaDPKvUj2O87m0SpYzgxDX74qSuruqHX8OX26BHExj78
FR8jHDIhuUwp9AKy9yO0isFY65jkLov6tdRpNy5A+QrGyRVBilCIT6YFYKSzEEI8
6+29FkLtX+ERjqxJs+aGHyEPDWE4Zy7dBsuTk1Fwz8F6/rOz4PS2pNQXc2sWmomn
muQXv0hwKY5gMcovCkC3y/op3kNuc/3qeBHjeCBYEMLR0o25hZHGrKOrQahFsy+R
V48sgIECgYEA0H66Ijfcc7NpgKOQwyvCt9/uhRZ3RkeABoSBLb/wYfQjw4pMadqr
RMMzVPzOLC459Giv4m8GeikNPl53rYdTCRmd/t1nZClU/UQKhgj+RRt4xY2cJNsg
j2CTZDr5SJO8H957K1IbvN5mxdsWZuDc5dtf0wBMIaCJoXR/iDMcf2MCgYEAw8oK
Dkpz9PdhGkbTE0ARLeUv7okelBkfDIGgucXBFHUElHAGe+XLF5dMppmzRDHXi2NG
gSNPJsDOlgSyLJjKX7HapYeAJWm91w5kJEX+oERr1EnEPWPvOHI+OW5DjM6eR1s9
xRJ87e3ymgLIF7G5rmf0p3OlnVvCaQvIVYTB98ECgYEAl+sPI2nCp0eeY05LZ/rV
6fcwLCdfh4UHwzf/jF9j/2vON2fpH+RmkTcOiymd7NFOB0nUhtBRTufkr4JT/8wv
89yHpDKdaH05YUWXyWx6Ic7PpFr34F8OjYpYO1tBUuHa3PnWk41Dis4e4qIt446L
Rq0fWHbKAmKghlWFq69aX3MCgYEArKU2JM/mXHbfe0pEyk7OV0gn8hGbk0Brrp2H
2wjUb3OYbEQ0k4BYjB7wimAyQcoppVIPU8SNAUE3afYOH2FD4wp0IU7Q4yzRKBga
mhnWpABxjSrXDsNWqNGkqQPgMQPpcka0u1jILQ6LxN77Dlm7wF0O0bIash292t92
8mI0oIECgYEAql8/uRHGtwSk64rXWXI+uq+x4ewwZkVc+mMmJ0yCMuQsOzbQTxhx
v9GEi3xsFbNazGCx4b56+/6Bi6gf7aH+NeK2+7C4ddlpHGEawoEcW1CW8hRQ2brp
vWgC+m5nmQ2SaYGzlilzZVK3JE6qOZ/AG8k+ZEG9tsvakMliG1SoJXk=
-----END RSA PRIVATE KEY-----
```

For SSH, DSA or RSA host key pairs must meet the requirements outlined in "SSH host key" (Page 153).

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-----
```

7 Layer 2

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

7.1 Managing Virtual Local Area Networks (VLANs)

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

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

VLANs are created in three ways:

- **Explicitly**
  Static VLANs can be created in the switch. For more information about static VLANs, refer to "Managing static VLANs" (Page 170).
- **Implicitly**
  When a VLAN ID (VID) is set for a port-based VLAN, static MAC address or IP interface, an appropriate VLAN is automatically created if it does not yet exist.
- **Dynamically**
  VLANs can be learned through GVRP. For more information about GVRP, refer to "GARP VLAN Registration Protocol (GVRP)" (Page 163)

For more information about VLANs, refer to "VLAN concepts" (Page 159).

7.1.1 VLAN concepts

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

7.1.1.1 Tagged vs. untagged frames

VLAN tags identify frames as part of a VLAN network. When a switch receives a frame with a VLAN (or 802.1Q) tag, the VLAN identifier (VID) is extracted and the frame is forwarded to other ports on the same VLAN.

When a frame does not contain a VLAN tag, or contains an 802.1p (prioritization) tag that only has prioritization information and a VID of 0, it is considered an untagged frame.

7.1.1.2 Native VLAN

Each port is assigned a native VLAN number, the Port VLAN ID (PVID). When an untagged frame ingresses a port, it is associated with the port's native VLAN.

By default, when a switch transmits a frame on the native VLAN, it sends the frame untagged. The switch can be configured to transmit tagged frames on the native VLAN.

7.1.1.3 The management VLAN

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

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

⚠ NOTICE

Security hazard – risk of unauthorized access and/or exploitation

IP interfaces that belong to the management VLAN must be connected to a trusted network.

7.1.1.4 Auxiliary management VLANs

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

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

- Web Server

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

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

⚠ NOTICE

Security hazard – risk of unauthorized access and/or exploitation

IP interfaces that belong to an auxiliary management VLAN must be connected to a trusted network.

7.1.1.5 Edge and trunk port types

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

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

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

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

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

Note

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

For more information about the Forbidden Ports list, refer to "Forbidden ports list" (Page 162).

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

7.1.1.6 Ingress and egress rules

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

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

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

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

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

7.1.1.7 Forbidden ports list

Each VLAN can be configured to exclude ports from membership in the VLAN using the forbidden ports list. For more information, refer to "Adding a static VLAN" (Page 171).

7.1.1.8 VLAN-aware and VLAN-unaware modes

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

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

Note

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

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

In that mode:

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

7.1.1.9 GARP VLAN Registration Protocol (GVRP)

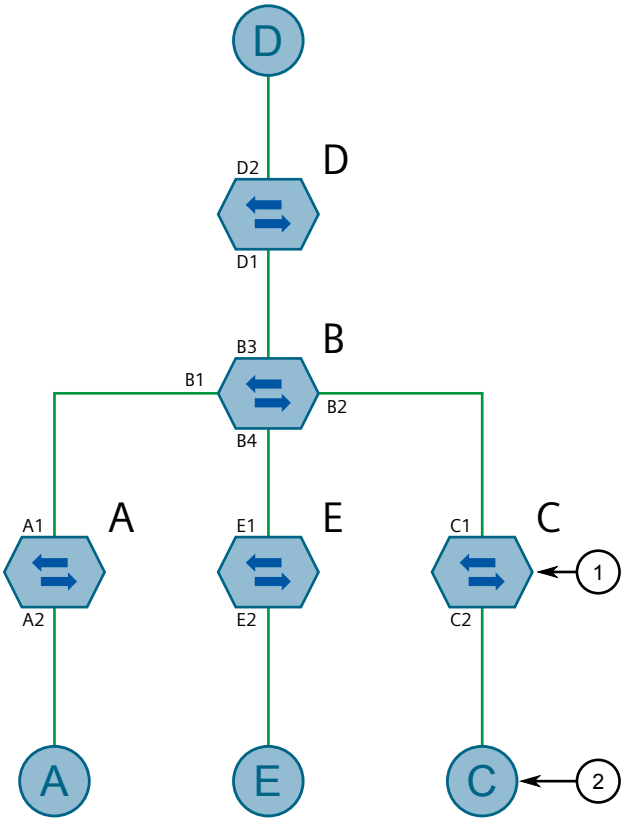
GARP VLAN Registration Protocol (GVRP) is a standard protocol built on GARP (Generic Attribute Registration Protocol) to automatically distribute VLAN configuration information in a network. Each switch in a network needs only to be configured with VLANs it requires locally. VLANs configured elsewhere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

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

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

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

The following is an example of how to use GVRP:



① Switch
② End node

Figure 7.1 Using GVRP

- Switch B is the core switch, all others are edge switches
- Ports A1, B1 to B4, C1, D1, D2 and E1 are GVRP aware
- Ports B1 to B4, D1 and D2 are set to advertise and learn
- Ports A1, C1 and E1 are set to advertise only
- Ports A2, C2 and E2 are edge ports
- End node D is GVRP aware
- End nodes A, E and C are GVRP unaware
- Ports A2 and C2 are configured with PVID 7
- Port E2 is configured with PVID 20
- End node D is interested in VLAN 20, hence VLAN 20 is advertised by it towards switch D
- D2 becomes a member of VLAN 20
- Ports A1 and C1 advertise VID 7

- Ports B1 and B2 become members of VLAN 7
- Ports B1, B2 and D1 advertise VID 20
- Ports B3, B4 and D1 become members of VLAN 20

For more information about how to configure GVRP, refer to "Configuring VLANs for specific Ethernet ports" (Page 169).

7.1.1.10 PVLAN edge

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

For more information about how to configure a port as *protected*, refer to "Configuring VLANs for specific Ethernet ports" (Page 169).

Note

This feature is strictly local to the switch. PVLAN Edge ports are not prevented from communicating with ports outside of the switch, whether protected (remotely) or not.

7.1.1.11 QinQ

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

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

Any tagged frames ingressing an edge port of the service provider's switch are tagged with VIDs of the customer’s private network. When those frames egress the switch's QinQ-enabled port into the service provider network, the switch always adds an extra tag (called an *outer tag*) on top of the frame's original VLAN tag (called an *inner tag*). The outer tag VID is the PVID of the frame's ingress edge port. This means that traffic from an individual customer is tagged with their unique VID and is thus segregated from other customers' traffic. For untagged ingress frames, the switch will only add the outer VLAN tag.

Within the service provider network, switching is based on the VID in the outer tag.

The service provider strips the outer VID from the frame on egress, leaving the frame with its original VLAN ID tag. Those frames are then forwarded on the appropriate VLANs.

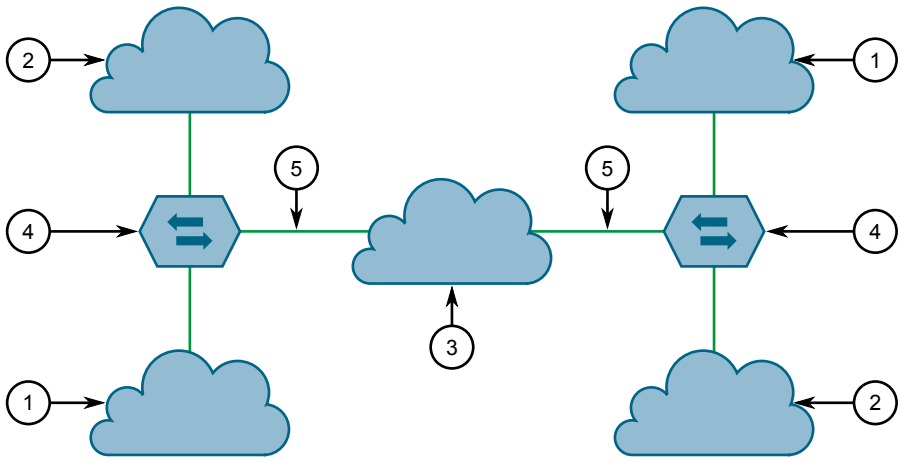
The following figure shows an example of traffic flow using QinQ.

For tagged frames:

- Frames received from customer 1 with VID 100 would carry an inner tag of 100 and an outer tag of VID X (i.e. VLAN 110) which is configured on the edge port connected to customer 1.
- Next, the frames from customer 1 are forwarded through the QinQ port carrying an inner and an outer tag.
- Finally, upon arrival of the frames in the peer switch, the outer VLAN tag is removed and the frames are forwarded with the inner VLAN tag towards customer 1.

For untagged frames:

- Frames received from customer 2 would carry an outer tag of VID Y(i.e VLAN 220) which is configured on the edge port connected to customer 2.
- Next, the frames from customer 2 are forwarded through the QinQ port carrying the outer tag.
- Finally, upon arrival of the frames in the peer switch, the outer VLAN tag is removed before the frames are forwarded to customer 2.



① Customer 1 (PVID is X)
② Customer 2 (PVID is Y)
③ Network service provider infrastructure
④ Switch
⑤ QinQ

Figure 7.2 Using QinQ

Note

Depending on the hardware installed, some switch models allow only one switch port be configured to QinQ mode at a time.

Note

When QinQ is enabled, all non-QinQ ports will be untagged and cannot be changed, and all QinQ ports will be tagged, and cannot be changed.

7.1.1.12 VLAN advantages

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

Traffic domain isolation

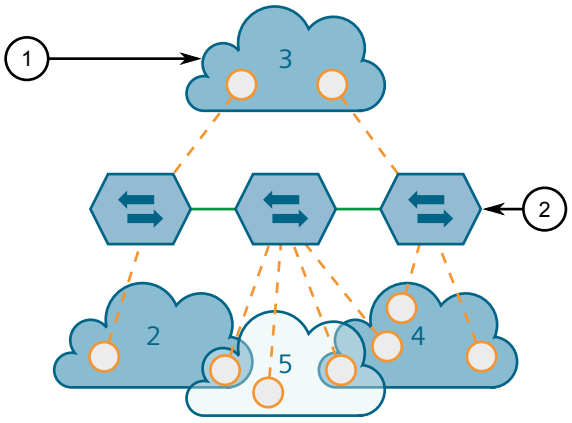
VLANs are most often used for their ability to restrict traffic flows between groups of devices.

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

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

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

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



① VLAN
② Switch

Figure 7.3 Multiple overlapping VLANs

Administrative convenience

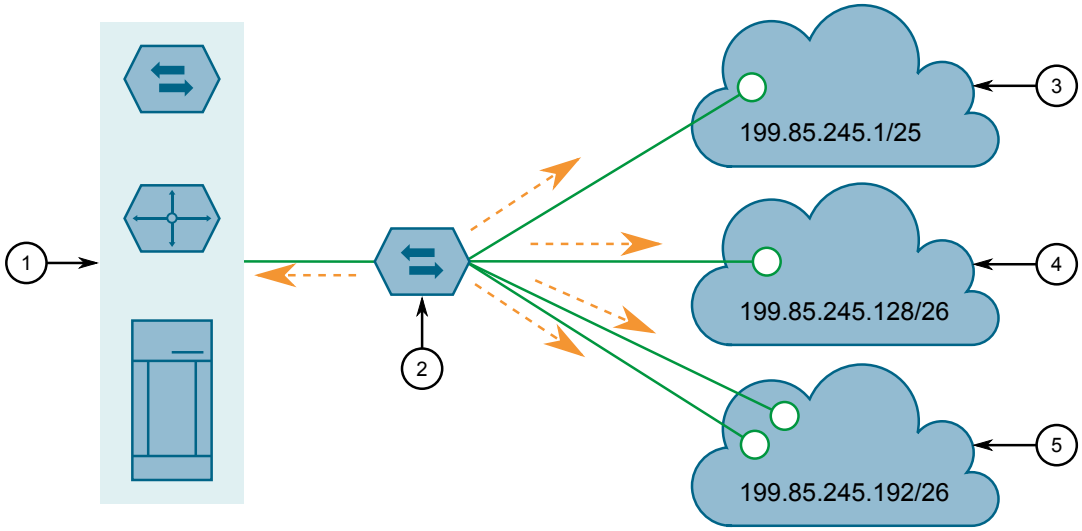
VLANs enable equipment moves to be handled by software reconfiguration instead of by physical cable management. When a host's physical location is changed, its connection point is often changed as well. With VLANs, the host's VLAN membership and priority are simply copied to the new port.

Reduced hardware

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

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

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



① Server, router or Layer 3 switch
② Switch
③ VLAN 2
④ VLAN 3
⑤ VLAN 4

Figure 7.4 Inter-VLAN communications

7.1.2 Viewing a list of VLANs

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

If a VLANs are not listed, add static VLANs as needed. For more information, refer to "Adding a static VLAN" (Page 171).

7.1.3 Configuring VLANs globally

To configure global settings for all VLANs, do the following:

1. Navigate to ***Virtual LANs » Configure Global VLAN Parameters***. The **Global VLAN Parameters** form appears.
2. Configure the following parameter(s) as required:

Parameter	Description
`VLAN-aware`	**Synopsis:** [No | Yes] **Default:** Yes Set either VLAN-aware or VLAN-unaware mode of operation.

3. Click **Apply**.

7.1.4 Configuring VLANs for specific Ethernet ports

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

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

1. Navigate to ***Virtual LANs » Configure Port VLAN Parameters***. The **Port VLAN Parameters** table appears.
2. Select a port. The **Port VLAN Parameters** form appears.
3. Configure the following parameter(s) as required:

Parameter	Description
`Port(s)`	**Synopsis:** Any combination of numbers valid for this parameter The port number of the device (or a list of ports, if aggregated in a port trunk).
`Type`	**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.

Parameter	Description
PVID	**Synopsis:** An integer between 1 and 4094 **Default:** 1 The Port VLAN Identifier specifies the VLAN ID associated with untagged (and 802.1p priority tagged) frames received on this port. Frames tagged with a non-zero VLAN ID will always be associated with the VLAN ID retrieved from the frame tag. Modify this parameter with care! By default, the switch is programmed to use VLAN 1 for management and every port on the switch is programmed to use VLAN 1. If you modify a switch port to use a VLAN other than the management VLAN, devices on that port will not be able to manage the switch.
PVID Format	**Synopsis:** [Untagged | Tagged] **Default:** Untagged Specifies whether frames transmitted out of the port on its native VLAN (specified by the**PVID**parameter) will be tagged or untagged. **Note** When QinQ is enabled, all non-QinQ ports will be untagged and cannot be changed, and all QinQ ports will be tagged, and cannot be changed.
GVRP	**Synopsis:** [Adv&Learn | Adv Only | Disabled] **Default:** Disabled Configures GVRP (Generic VLAN Registration Protocol) operation on the port. There are several GVRP operation modes: • **Adv&Learn** – the port will declare all VLANs existing in the switch (configured or learned) and can dynamically learn VLANs. • **Adv Only** – the port will declare all VLANs existing in the switch (configured or learned) but will not learn any VLANs. • **Disabled** – the port is not capable of any GVRP processing. Only Trunk ports are GVRP-capable.

4. Click **Apply**.

7.1.5 Managing static VLANs

This section describes how to configure and manage static VLANs.

7.1.5.1 Viewing a list of static VLANs

To view a list of static VLANs, navigate to ***Virtual LANs » Configure Static VLANs***. The **Static VLANs** table appears.

If a static VLAN is not listed, add the VLAN. For more information, refer to "Adding a static VLAN" (Page 171).

7.1.5.2 Adding a static VLAN

To add a static VLAN, do the following:

1. Navigate to ***Virtual LANs » Configure Static VLANs***. The **Static VLANs** table appears.
2. Click **InsertRecord**. The **Static VLANs** form appears.
3. Configure the following parameter(s) as required:

Note

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

Parameter	Description
`VID`	**Default:** 1 The VLAN Identifier is used to identify the VLAN in tagged Ethernet frames according to IEEE 802.1Q.
`VLAN Name`	**Synopsis:** A string up to 19 characters long The VLAN name provides a description of the VLAN purpose (for example, Engineering VLAN).
`Forbidden Ports`	**Synopsis:** Any combination of numbers valid for this parameter or [None] 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.

Parameter	Description
MSTI	**Synopsis:** An integer between 0 and 16 **Default:** 0 This parameter is only valid for Multiple Spanning Tree Protocol (MSTP) and has no effect if MSTP is not used. The parameter specifies the Multiple Spanning Tree Instance (MSTI) to which the VLAN should be mapped.

4. Click **Apply**.

7.1.5.3 Deleting a static VLAN

To delete a static VLAN, do the following:

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

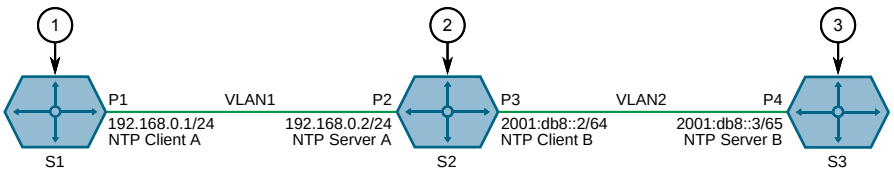
7.1.6 Example: Configuring management support on multiple VLANs

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

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

⚠ NOTICE

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



① Switch S1
② Switch S2
③ Switch S3

Figure 7.5 Topology – Management support on multiple VLANs

To replicate the topology, do the following:

1. Configure switch S1 as follows:
   a. Connect port P1 to port P2 on switch S2.
   b. Assign IP address *192.168.0.1/24* to port P1.
   c. Configure port P1 as the management interface. For more information, refer to "Adding an IP interface" (Page 91).
   d. Assign port P1 to VLAN 1. For more information, refer to Section "Configuring VLANs for specific Ethernet ports" (Page 169).
   e. Configure the NTP server on switch S1 as follows:

Server	Primary
IP Address	192.168.0.2
Update Period	1 min

   For more information, refer to "Configuring NTP servers" (Page 249).
2. Configure switch S2 as follows:
   a. Connect port P3 to port P4 on switch S3.
   b. Assign IP address *192.168.0.2/24* to port P2.
   c. Assign IP address *2001:db8::2/64* to port P3.
   d. Configure port P2 as an auxiliary management interface. For more information, refer to "Adding an IP interface" (Page 91).
   e. Configure port P3 as a non-management interface. For more information, refer to "Adding an IP interface" (Page 91).
   f. Assign port P2 to VLAN 1. For more information, refer to Section "Configuring VLANs for specific Ethernet ports" (Page 169).
   g. Assign port P3 to VLAN 2. For more information, refer to Section "Configuring VLANs for specific Ethernet ports" (Page 169).
   h. Configure the NTP server on switch S2 as follows:

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

   For more information, refer to "Configuring NTP servers" (Page 249).
3. Configure switch S3 as follows:
   a. Assign IP address *2001:db8::3/64* to port P4.
   b. Configure port P4 as a non-management interface. For more information, refer to "Adding an IP interface" (Page 91).
   c. Assign port P4 to VLAN 2. For more information, refer to Section "Configuring VLANs for specific Ethernet ports" (Page 169).
   d. Enable SNTP on switch S3. For more information, refer to Section "Enabling/disabling NTP service" (Page 248).

4. Verify the following:
   a. The local clock of switch S1 is synchronized with the local clock of switch S2. For more information, refer to "Managing NTP" (Page 248).
   b. The local clock of switch S2 is *not* synchronized with the local clock of switch S3. For more information, refer to "Managing NTP" (Page 248).
   c. The SNTP server on switch S2 is unreachable from the primary NTP server (because VLAN 2 is a non-management VLAN). For more information, refer to "Managing NTP" (Page 248).

7.2 Managing MAC addresses

This section describes how to manage MAC addresses.

7.2.1 Viewing a list of MAC addresses

To view a list of all static and dynamically learned MAC addresses, navigate to ***MAC Address Tables » View MAC Addresses***. The **MAC Addresses** table appears.

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

1. Configure the MAC address learning options to control the aging time of dynamically learned MAC addresses of other devices on the network. For more information, refer to "Configuring MAC address learning options" (Page 174).
2. Configure the address on the device as a static MAC address. For more information, refer to "Adding a static MAC address" (Page 176).

7.2.2 Configuring MAC address learning options

The MAC address learning options control how and when MAC addresses are removed automatically from the MAC address table. Individual addresses are removed when the aging timer is exceeded. Addresses can also be removed when a link failure or topology change occurs.

To configure the MAC address learning options, do the following:

1. Navigate to ***MAC Address Tables » Configure MAC Address Learning Options***. The **MAC Address Learning Options** form appears.
2. Configure the following parameter(s) as required:

Parameter	Description
`Aging Time`	**Synopsis:** An integer between 15 and 800 **Default:** 300 This parameter configures the time that a learned MAC address is held before being aged out.

Parameter	Description
`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, is enabled on the switch, that redundancy protocol may, upon a link failure, flush MAC addresses learned on the failed port regardless of the setting of this parameter.

3. Click **Apply**.

7.2.3 Configuring MAC address flooding options

To configure the MAC address flooding options, do the following:

1. Navigate to ***MAC Address Tables » Configure MAC Address Flooding Options***. The **Flooding Options** table appears.
2. Select a port. The **Flooding Options** form appears.
3. Configure the following parameter(s) as required:

Parameter	Description
`Port(s)`	**Synopsis:** Comma-separated list of ports The port number of the device (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**.

7.2.4 Managing static MAC addresses

Static MAC addresses must be configured when the device is only able to receive frames, not transmit them. They may also need to be configured if port security (if supported) must be enforced.

Prioritized MAC addresses are configured when traffic to or from a specific device on a LAN segment is to be assigned a higher CoS priority than other devices on that LAN segment.

Note

A MAC address cannot be learned on a VLAN that has not been configured in the Static VLAN table. If a frame with an unknown VLAN tag arrives on a secured port, it is considered a security violation and RUGGEDCOM ROS will generate a port security alarm.

7.2.4.1 Viewing a list of static MAC addresses

To view a list of static MAC addresses configured on the device, navigate to ***MAC Address Tables » Configure Static MAC Addresses***. The **Static MAC Addresses** table appears.

If static MAC addresses have not been configured, add addresses as needed. For more information, refer to "Adding a static MAC address" (Page 176).

7.2.4.2 Adding a static MAC address

To add a static MAC address to the Static MAC Address Table, do the following:

1. Navigate to ***MAC Address Tables » Configure Static MAC Addresses***. The **Static MAC Addresses** table appears.
2. Click **InsertRecord**. The **Static MAC Addresses** form appears.
3. Configure the following parameter(s) as required:

Parameter	Description
`MAC Address`	**Synopsis:** ##-##-##-##-##-## where ## ranges 0 to FF 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`	**Default:** 1 VLAN Identifier of the VLAN upon which the MAC address operates.

Parameter	Description
Port	**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.

4. Click **Apply**.

7.2.4.3 Deleting a static MAC address

To delete a static MAC address from the Static MAC Address Table, do the following:

1. Navigate to ***MAC Address Tables » Configure Static MAC Addresses***. The **Static MAC Addresses** table appears.
2. Select the MAC address from the table. The **Static MAC Addresses** form appears.
3. Click **Delete**.

7.2.5 Purging all dynamic MAC addresses

To purge the dynamic MAC address list of all entries, do the following:

1. Navigate to ***MAC Address Tables » Purge MAC Address Table***. The **Purge MAC Address Table** form appears.
2. Click **Confirm**.

7.3 Managing multicast filtering

Multicast traffic can be filtered using IGMP (Internet Group Management Protocol) snooping or GMRP (GARP Multicast Registration Protocol).

7.3.1 Managing IGMP

IGMP is used by IP hosts to report their host group memberships with multicast routers. As hosts join and leave specific multicast groups, streams of traffic are directed to or withheld from that host.

The IGMP protocol operates between multicast routers and IP hosts. When an unmanaged switch is placed between multicast routers and their hosts, the multicast streams will be distributed to all ports.This may introduce significant traffic onto ports that do not require it and receive no benefit from it.

IGMP Snooping, when enabled, will act on IGMP messages sent from the router and the host, restricting traffic streams to the appropriate LAN segments.

⚠ NOTICE

RUGGEDCOM ROS restricts IGMP hosts from subscribing to the following special multicast addresses:

- 224.0.0.0 to 224.0.0.255
- 224.0.1.129

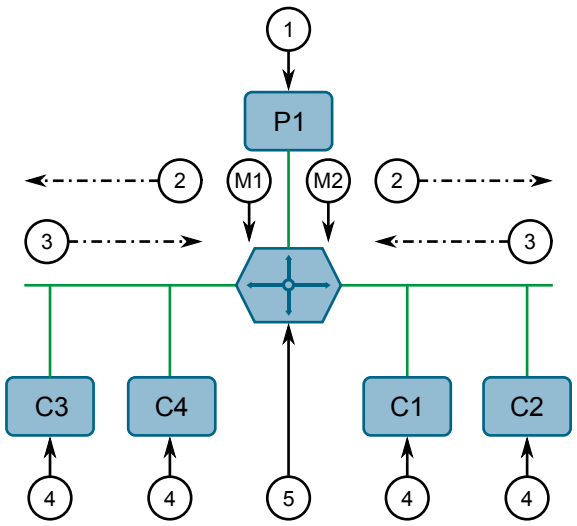
These addresses are reserved for routing protocols and IEEE 1588. If an IGMP membership report contains one of these addresses, the report is forwarded by the switch without learning about the host.

7.3.1.1 IGMP concepts

The following describes some of the concepts important to the implementation of multicast filtering using IGMP:

IGMP in operation

The following network diagram provides a simple example of the use of IGMP.



① Producer
② Membership queries
③ Membership reports
④ Consumer
⑤ Multicast router

Figure 7.6 Example – IGMP In Operation

One *producer* IP host (P1) is generating two IP multicast streams, M1 and M2. There are four potential *consumers* of these streams, C1 through C4. The multicast

router discovers which host wishes to subscribe to which stream by sending general membership queries to each segment.

In this example, the general membership query sent to the C1-C2 segment is answered by a membership report (or *join*) indicating the desire to subscribe to stream M2. The router will forward the M2 stream to the C1-C2 segment. In a similar fashion, the router discovers that it must forward stream M1 to segment C3-C4.

A *consumer* may join any number of multicast groups, issuing a membership report for each group. When a host issues a membership report, other hosts on the same network segment that also require membership to the same group suppress their own requests, since they would be redundant. In this way, the IGMP protocol guarantees the segment will issue only one membership report for each group.

The router periodically queries each of its segments in order to determine whether at least one consumer still subscribes to a given stream. If it receives no responses within a given time period (usually two query intervals), the router will prune the multicast stream from the given segment.

A more common method of pruning occurs when consumers wishing to unsubscribe issue an IGMP *leave group* message. The router will immediately issue a group-specific membership query to determine whether there are any remaining subscribers of that group on the segment. After the last consumer of a group has unsubscribed, the router will prune the multicast stream from the given segment.

Switch IGMP operation

The IGMP Snooping feature provides a means for switches to snoop (i.e. watch) the operation of routers, respond with joins/leaves on the behalf of consumer ports, and prune multicast streams accordingly. There are two modes of IGMP the switch can be configured to assume: active and passive.

- **Active Mode**
  IGMP supports a *routerless* mode of operation.

  When such a switch is used without a multicast router, it is able to function as if it is a multicast router sending IGMP general queries.
- **Passive Mode**
  When such a switch is used in a network with a multicast router, it can be configured to run Passive IGMP. This mode prevents the switch from sending the queries that can confuse the router causing it to stop issuing IGMP queries.

Note

A switch running in passive mode requires the presence of a multicast router or it will be unable to forward multicast streams at all if no multicast routers are present.

Note

At least one IGMP Snooping switch must be in active mode to make IGMP functional.

IGMP snooping rules

IGMP Snooping adheres to the following rules:

- When a multicast source starts multicasting, the traffic stream will be immediately blocked on segments from which joins have not been received.
- Unless configured otherwise, the switch will forward all multicast traffic to the ports where multicast routers are attached.
- Packets with a destination IP multicast address in the 224.0.0.X range that are not IGMP are always forwarded to all ports. This behavior is based on the fact that many systems do not send membership reports for IP multicast addresses in this range while still listening to such packets.
- The switch implements IGMPv2 *proxy-reporting* (i.e. membership reports received from downstream are summarized and used by the switch to issue its own reports).
- The switch will only send IGMP membership reports out of those ports where multicast routers are attached, as sending membership reports to hosts could result in unintentionally preventing a host from joining a specific group.
- Multicast routers use IGMP to elect a master router known as the *querier*. The *querier* is the router with the lowest IP address. All other routers become non-queriers, participating only in forwarding multicast traffic. Switches running in active mode participate in the querier election the same as multicast routers.
- When the querier election process is complete, the switch simply relays IGMP queries received from the querier.
- When sending IGMP packets, the switch uses its own IP address, if it has one, for the VLAN on which packets are sent, or an address of 0.0.0.0, if it does not have an assigned IP address.

Note

IGMP Snooping switches perform multicast pruning using a multicast frames' destination MAC multicast address, which depends on the group IP multicast address. IP address W.X.Y.Z corresponds to MAC address 01-00-5E-XX-YY-ZZ where XX is the lower 7 bits of X, and YY and ZZ are simply Y and Z coded in hexadecimal.

One can note that IP multicast addresses, such as 224.1.1.1 and 225.1.1.1, will both map onto the same MAC address 01-00-5E-01-01-01. This is a problem for which the IETF Network Working Group currently has offered no solution. Users are advised to be aware of and avoid this problem.

IGMP and RSTP

An RSTP change of topology can render the routes selected to carry multicast traffic as incorrect. This results in lost multicast traffic.

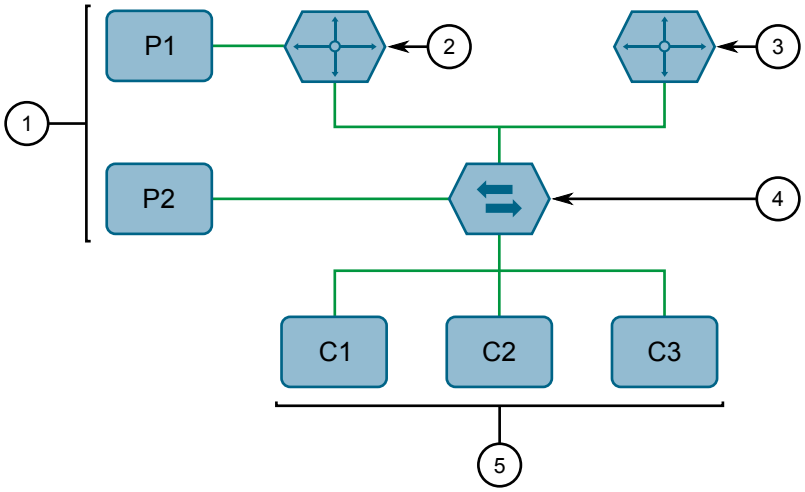
If RSTP detects a change in the network topology, IGMP will take some actions to avoid the loss of multicast connectivity and reduce network convergence time:

- The switch will immediately issue IGMP queries (if in IGMP Active mode) to obtain potential new group membership information.
- The switch can be configured to flood multicast streams temporarily out of all ports that are not configured as RSTP Edge Ports.

Combined router and switch IGMP operation

The following example illustrates the challenges faced with multiple routers, VLAN support and switching.

Producer P1 resides on VLAN 2 while P2 resides on VLAN 3. Consumer C1 resides on both VLANs whereas C2 and C3 reside on VLANs 3 and 2, respectively. Router 2 resides on VLAN 2, presumably to forward multicast traffic to a remote network or act as a source of multicast traffic itself.



① Producer
② Multicast router 1
③ Multicast router 2
④ Switch
⑤ Host

Figure 7.7 Example – Combined router and switch IGMP in operation

In this example:

- P1, Router 1, Router 2 and C3 are on VLAN 2
- P2 and C2 are on VLAN 3
- C1 is on both VLAN 2 and 3

Assuming that router 1 is the querier for VLAN 2 and router 2 is simply a non-querier, the switch will periodically receive queries from router 1 and maintain the information concerning which port links to the multicast router. However, the switch port that links to router 2 must be manually configured as a *router port*. Otherwise, the switch will send neither multicast streams nor joins/leaves to router 2.

Note that VLAN 3 does not have an external multicast router. The switch should be configured to operate in its *routerless* mode and issue general membership queries as if it is the router.

- **Processing joins**
  If host C1 wants to subscribe to the multicast streams for both P1 and P2, it will generate two membership reports. The membership report from C1 on VLAN 2 will cause the switch to immediately initiate its own membership report to multicast router 1 (and to issue its own membership report as a response to queries).

  The membership report from host C1 for VLAN 3 will cause the switch to immediately begin forwarding multicast traffic from producer P2 to host C2.
- **Processing leaves**
  When host C1 decides to leave a multicast group, it will issue a leave request to the switch. The switch will poll the port to determine if host C1 is the last member of the group on that port. If host C1 is the last (or only) member, the group will immediately be pruned from the port.

  Should host C1 leave the multicast group without issuing a leave group message and then fail to respond to a general membership query, the switch will stop forwarding traffic after two queries.

  When the last port in a multicast group leaves the group (or is aged-out), the switch will issue an IGMP leave report to the router.

7.3.1.2 Viewing a list of multicast group memberships

Using IGMP snooping, RUGGEDCOM ROS records group membership information on a per-port basis based on membership reports it observes between the router and host.

To view a list of multicast group memberships, navigate to ***Multicast Filtering » View IGMP Group Membership***. The **IGMP Group Membership** table appears.

This table provides the following information:

Parameter	Description
`Port`	The port number.
`VID`	**Synopsis:** An integer between 0 and 65535 VLAN Identifier of the VLAN upon which the multicast group operates.
`Group`	**Synopsis:** ###.###.###.### where ### ranges from 0 to 255 Multicast Group Address.
`Ver`	**Synopsis:** [v3 | v2 | v1] Specifies the IGMP version of the learnt multicast group.

Parameter	Description
Reporter	**Synopsis:** ###.###.###.### where ### ranges from 0 to 255 Specifies the source IP address that is reporting subscription to the multicast group.
Age	**Synopsis:** An integer between 0 and 7210 Specifies the current age of the IP multicast group learned on the port in seconds.

If the table is empty, do the following:

- Make sure traffic is being sent to the device.
- Make sure IGMP is properly configured on the device. For more information, refer to "Configuring IGMP" (Page 184).

7.3.1.3 Viewing forwarding information for multicast groups

Multicast forwarding information for every source, group and VLAN combination learned by RUGGEDCOM ROS is recorded in the IGMP Multicast Forwarding table.

To view the IGMP Multicast Forwarding table, navigate to ***Multicast Filtering » View IGMP Multicast Forwarding***. The **IGMP Multicast Forwarding** table appears.

This table provides the following information:

Parameter	Description
VID	**Synopsis:** An integer between 0 and 65535 VLAN Identifier of the VLAN upon which the multicast group operates.
Group	**Synopsis:** ###.###.###.### where ### ranges from 0 to 255 Multicast Group Address.
Source	**Synopsis:** ###.###.###.### where ### ranges from 0 to 255 or [*] Source Address. * means all possible source addresses.
Joined Ports	**Synopsis:** Comma-separated list of ports All ports that currently receive multicast traffic for the specified multicast group.
Router Ports	**Synopsis:** Comma-separated list of ports All ports that have been manually configured or dynamically discovered (by observing router specific traffic) as ports that link to multicast routers.

If the table is empty, do the following:

- Make sure traffic is being sent to the device.

- Make sure IGMP is properly configured on the device. For more information, refer to "Configuring IGMP" (Page 184).

7.3.1.4 Configuring IGMP

To configure the IGMP, do the following:

1. Make sure one or more static VLANs exist with IGMP enabled. For more information, refer to "Managing static VLANs" (Page 170).
2. Navigate to ***Multicast Filtering » Configure IGMP Parameters***. The **IGMP Parameters** form appears.
3. Configure the following parameter(s) as required:

Parameter	Description
`Mode`	**Synopsis:** [Passive | Active] **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:** An integer between 10 and 3600 **Default:** 60 The time interval between IGMP queries generated by the switch. **Note** This parameter also affects the Group Membership Interval (i.e. the group subscriber aging time), therefore, it takes effect even in PASSIVE mode.

Parameter	Description
`Router Ports`	**Synopsis:** Comma-separated list of ports **Default:** None This parameter specifies ports that connect to multicast routers. If you do not configure known router ports, the switch may be able to detect them, however it is advisable to pre-configure them.
`Router Forwarding`	**Synopsis:** [Off | On] **Default:** On This parameter specifies whether multicast streams will be always forwarded to multicast routers.
`RSTP Flooding`	**Synopsis:** [Off | On] **Default:** Off This parameter specifies whether multicast streams will be flooded out of all RSTP non-edge ports upon topology change detection. Such flooding is desirable, if guaranteed multicast stream delivery after topology change is most important.

4. Click **Apply**.

7.3.2 Managing GMRP

The GMRP is an application of the Generic Attribute Registration Protocol (GARP) that provides a Layer 2 mechanism for managing multicast group memberships in a bridged Layer 2 network. It allows Ethernet switches and end stations to register and unregister membership in multicast groups with other switches on a LAN, and for that information to be disseminated to all switches in the LAN that support Extended Filtering Services.

GMRP is an industry-standard protocol first defined in IEEE 802.1D-1998 and extended in IEEE 802.1Q-2005. GARP was defined in IEEE 802.1D-1998 and updated in 802.1D-2004.

Note

GMRP provides similar functionality at Layer 2 to what IGMP provides at Layer 3.

7.3.2.1 GMRP concepts

The following describes some of the concepts important to the implementation of multicast filtering using GMRP:

Joining a multicast group

To join a multicast group, an end station transmits a GMRP *join* message. The switch that receives the *join* message adds the port through which the message was received to the multicast group specified in the message. It then propagates the *join* message to all other hosts in the VLAN, one of which is expected to be the multicast source.

When a switch transmits GMRP updates (from GMRP-enabled ports), all of the multicast groups known to the switch, whether configured manually or learned dynamically through GMRP, are advertised to the rest of network.

As long as one host on the Layer 2 network has registered for a given multicast group, traffic from the corresponding multicast source will be carried on the network. Traffic multicast by the source is only forwarded by each switch in the network to those ports from which it has received join messages for the multicast group.

Leaving a multicast group

Periodically, the switch sends GMRP queries in the form of a *leave all* message. If a host (either a switch or an end station) wishes to remain in a multicast group, it reasserts its group membership by responding with an appropriate *join* request. Otherwise, it can either respond with a *leave* message or simply not respond at all. If the switch receives a *leave* message or receives no response from the host for a timeout period, the switch removes the host from the multicast group.

Notes about GMRP

Since GMRP is an application of GARP, transactions take place using the GARP protocol. GMRP defines the following two Attribute Types:

- The Group Attribute Type, used to identify the values of group MAC addresses
- The Service Requirement Attribute Type, used to identify service requirements for the group

Service Requirement Attributes are used to change the receiving port's multicast filtering behavior to one of the following:

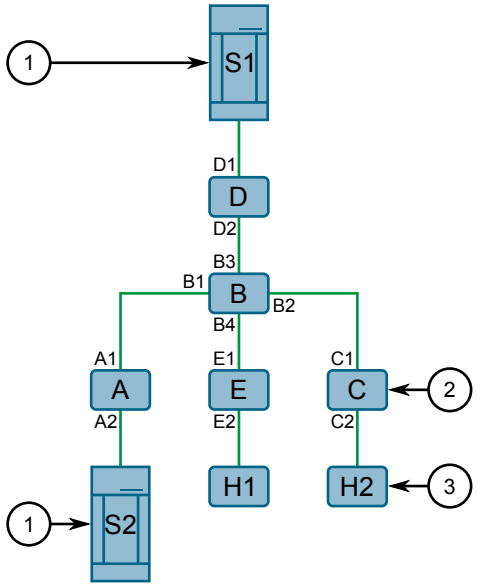
- Forward All Multicast group traffic in the VLAN, or
- Forward All Unknown Traffic (Multicast Groups) for which there are no members registered in the device in a VLAN

If GMRP is disabled, GMRP packets received will be forwarded like any other traffic. Otherwise, GMRP packets will be processed and not forwarded.

Establishing membership with GMRP

The following example illustrates how a network of hosts and switches can dynamically join two multicast groups using GMRP.

In this scenario, there are two multicast sources, S1 and S2, multicasting to Multicast Groups 1 and 2, respectively. A network of five switches, including one core switch (B), connects the sources to two hosts, H1 and H2, which receive the multicast streams from S1 and S2, respectively.



① Multicast source
② Switch
③ Multicast host

Figure 7.8 Example – Establishing membership with GMRP

The hosts and switches establish membership with the Multicast Group 1 and 2 as follows:

1. Host H1 is GMRP unaware, but needs to see traffic for Multicast Group 1. Therefore, Port E2 on Switch E is statically configured to forward traffic for Multicast Group 1.
2. Switch E advertises membership in Multicast Group 1 to the network through Port E1, making Port B4 on Switch B a member of Multicast Group 1.
3. Switch B propagates the *join* message, causing Ports A1, C1 and D1 to become members of Multicast Group 1.
4. Host H2 is GMRP-aware and sends a *join* request for Multicast Group 2 to Port C2, which thereby becomes a member of Multicast Group 2.
5. Switch C propagates the *join* message, causing Ports A1, B2, D1 and E1 to become members of Multicast Group 2.

Once GMRP-based registration has propagated through the network, multicast traffic from S1 and S2 can reach its destination as follows:

- Source S1 transmits multicast traffic to Port D2 which is forwarded via Port D1, which has previously become a member of Multicast Group 1.

- Switch B forwards the Group 1 multicast via Port B4 towards Switch E.
- Switch E forwards the Group 1 multicast via Port E2, which has been statically configured for membership in Multicast Group 1.
- Host H1, connected to Port E2, thus receives the Group 1 multicast.
- Source S2 transmits multicast traffic to Port A2, which is then forwarded via port A1, which has previously become a member of Multicast Group 2.
- Switch B forwards the Group 2 multicast via Port B2 towards Switch C.
- Switch C forwards the Group 2 multicast via Port C2, which has previously become a member of Group 2.
- Ultimately, Host H2, connected to Port C2, receives the Group 2 multicast.

7.3.2.2 Viewing a summary of multicast groups

To view a summary of all multicast groups, navigate to ***Multicast Filtering » View Multicast Group Summary***. The **Multicast Group Summary** table appears.

This table provides the following information:

Parameter	Description
`VID`	**Synopsis:** An integer between 0 and 65535 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.

7.3.2.3 Configuring GMRP globally

To configure global settings for GMRP, do the following:

1. Navigate to ***Multicast Filtering » Configure Global GMRP Parameters***. The **Global GMRP Parameters** form appears.
2. Configure the following parameter(s) as required:

Parameter	Description
GMRP Enable	**Synopsis:** [No | Yes] **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:** An integer between 600 and 300000 **Default:** 4000 Time (milliseconds) to wait after issuing Leave or LeaveAll before removing registered multicast groups. If Join messages for specific addresses are received before this timer expires, the addresses will be kept registered.

3. Click **Apply**.

7.3.2.4 Configuring GMRP for specific Ethernet ports

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

1. Make sure the global settings for GMRP have been configured. For more information, refer to "Configuring GMRP globally" (Page 188).
2. Navigate to ***Multicast Filtering » Configure Port GMRP Parameters***. The **Port GMRP Parameters** table appears.
3. Select an Ethernet port. The **Port GMRP Parameters** form appears.
4. Configure the following parameter(s) as required:

Parameter	Description
Port(s)	**Synopsis:** Any combination of numbers valid for this parameter The port number of the device (or a list of ports, if aggregated in a port trunk).
GMRP	**Synopsis:** [Disabled | Adv Only | Adv&Learn] **Default:** Disabled Configures GMRP (GARP Multicast Registration Protocol) operation on the port. There are several GMRP operation modes: • **Disabled** – the port is not capable of any GMRP processing.

Parameter	Description
	• **Adv Only** – the port will declare all MCAST addresses existing in the switch (configured or learned) but will not learn any MCAST addresses. • **Adv&Learn** – the port will declare all MCAST Addresses existing in the switch (configured or learned) and can dynamically learn MCAST addresses.

5. Click **Apply**.

7.3.2.5 Viewing a list of static multicast groups

To view a list of static multicast groups, navigate to ***Multicast Filtering » Configure Static Multicast Groups***. The **Static Multicast Groups** table appears.

If a static multicast group is not listed, add the group. For more information, refer to "Adding a static multicast group" (Page 190).

7.3.2.6 Adding a static multicast group

To add a static multicast group from another device, do the following:

1. Navigate to ***Multicast Filtering » Configure Static Multicast Groups***. The **Static Multicast Groups** table appears.
2. Click **InsertRecord**. The **Static Multicast Groups** form appears.
3. Configure the following parameter(s) as required:

Parameter	Description
`MAC Address`	**Synopsis:** ##-##-##-##-##-## where ## ranges 0 to FF **Default:** 00-00-00-00-00-00 Multicast group MAC address.
`VID`	**Default:** 1 VLAN Identifier of the VLAN upon which the multicast group operates.
`Ports`	**Synopsis:** Any combination of numbers valid for this parameter **Default:** None A comma-separated list of ports to which the multicast group traffic is forwarded. If a port is part of a Link Aggregation Group (LAG), or port trunk, specify all ports in the LAG.

4. Click **Apply**.

7.3.2.7 Deleting a static multicast group

To delete a static multicast group, do the following:

1. Navigate to ***Multicast Filtering » Configure Static Multicast Groups***. The **Static Multicast Groups** table appears.
2. Select the group from the table. The **Static Multicast Groups** form appears.
3. Click **Delete**.

8 Network redundancy

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

8.1 Managing Spanning Tree Protocol (STP)

This section describes how to manage the spanning tree protocol.

8.1.1 RSTP operation

The 802.1D Spanning Tree Protocol (STP) was developed to enable the construction of robust networks that incorporate redundancy while pruning the active topology of the network to prevent loops. While STP is effective, it requires that frame transfer halt after a link outage until all bridges in the network are guaranteed to be aware of the new topology. Using the values recommended by 802.1D, this period lasts 30 seconds.

The Rapid Spanning Tree Protocol (RSTP, IEEE 802.1w) was a further evolution of the 802.1D Spanning Tree Protocol. It replaced the settling period with an active handshake between bridges that guarantees the rapid propagation of topology information throughout the network. RSTP also offers a number of other significant innovations, including:

- Topology changes in RSTP can originate from and be acted upon by any designated bridges, leading to more rapid propagation of address information, unlike topology changes in STP, which must be passed to the root bridge before they can be propagated to the network.
- RSTP explicitly recognizes two blocking roles - Alternate and Backup Port - which are included in computations of when to learn and forward. STP, however, recognizes only one state - Blocking - for ports that should not forward.
- RSTP bridges generate their own configuration messages, even if they fail to receive any from the root bridge. This leads to quicker failure detection. STP, by contrast, must relay configuration messages received on the root port out its designated ports. If an STP bridge fails to receive a message from its neighbor, it cannot be sure where along the path to the root a failure occurred.
- RSTP offers edge port recognition, allowing ports at the edge of the network to forward frames immediately after activation, while at the same time protecting them against loops.

While providing much better performance than STP, IEEE 802.1w RSTP still required up to several seconds to restore network connectivity when a topology change occurred.

A revised and highly optimized RSTP version was defined in the IEEE standard 802.1D-2004 edition. IEEE 802.1D-2004 RSTP reduces network recovery times to just milliseconds and optimizes RSTP operation for various scenarios.

RUGGEDCOM ROS supports IEEE 802.1D-2004 RSTP.

8.1.1.1 RSTP states and roles

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

State

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

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

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

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

⚠ NOTICE

RUGGEDCOM ROS introduces two additional states: Disabled and Link Down. These states are useful for network monitoring and troubleshooting.

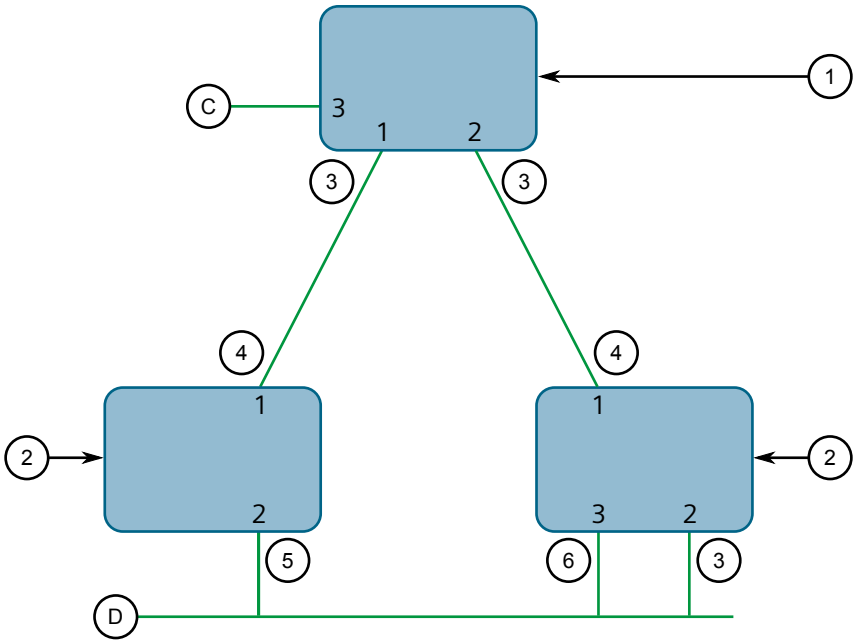
The Disabled state refers to links for which RSTP has been disabled. In the Disabled state, the port is always “Forwarding”.

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 to which it is connected. All bridges on the same LAN segment listen to each others' messages and agree on which bridge is the Root Bridge. The ports of other bridges on the segment must become either Root, Alternate or Backup ports.



① Root bridge
② Designated bridge
③ Designated port
④ Root port
⑤ Alternate port
⑥ Backup port

Figure 8.1 Bridge and port roles

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

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

8.1.1.2 Edge ports

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

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

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

8.1.1.3 Point-to-point and multipoint links

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

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

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

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

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

8.1.1.4 Path and port costs

The STP path cost is the main metric by which root and designated ports are chosen. The path cost for a designated bridge is the sum of the individual port costs of the links between the root bridge and that designated bridge. The port with the lowest path cost is the best route to the root bridge and is chosen as the root port.

Note

In actuality the primary determinant for root port selection is the root bridge ID. Bridge ID is important mainly at network startup when the bridge with the lowest ID is elected as the root bridge. After startup (when all bridges agree on the root bridge's ID) the path cost is used to select root ports. If the path costs of candidates for the root port are the same, the ID of the peer bridge is used to select the port. Finally, if candidate root ports have the same path cost and peer bridge ID, the port

ID of the peer bridge is used to select the root port. In all cases the lower ID, path cost or port ID is selected as the best.

How port costs are generated

Port costs can be generated either as a result of link auto-negotiation or manual configuration. When the link auto-negotiation method is used, the port cost is derived from the speed of the link. This method is useful when a well-connected network has been established. It can be used when the designer is not too concerned with the resultant topology as long as connectivity is assured.

Manual configuration is useful when the exact topology of the network must be predictable under all circumstances. The path cost can be used to establish the topology of the network exactly as the designer intends.

STP vs. RSTP costs

The IEEE 802.1D-1998 specification limits port costs to values of 1 to 65536. Designed at a time when 9600 bps links were state of the art, this method breaks down in modern use, as the method cannot represent a link speed higher than 10 gigabits per second.

To remedy this problem in future applications, the IEEE 802.1w specification limits port costs to values of 1 to 20000000, and a link speed up to 10 Tb per second can be represented with a value of 2.

RUGGEDCOM bridges support interoperability with legacy STP bridges by selecting the style to use. In practice, it makes no difference which style is used as long as it is applied consistently across the network, or if costs are manually assigned.

8.1.1.5 Bridge diameter

The bridge diameter is the maximum number of bridges between any two possible points of attachment of end stations to the network.

The bridge diameter reflects the realization that topology information requires time to propagate hop by hop through a network. If configuration messages take too long to propagate end to end through the network, the result will be an unstable network.

There is a relationship between the bridge diameter and the maximum age parameter. To achieve extended ring sizes, Siemens eRSTP™ uses an age increment of ¼ of a second. The value of the maximum bridge diameter is thus four times the configured maximum age parameter.

Note

The RSTP algorithm is as follows:

- STP configuration messages contain *age* information.

- Messages transmitted by the root bridge have an age of 0. As each subsequent designated bridge transmits the configuration message it must increase the age by at least 1 second.
- When the age exceeds the value of the maximum age parameter the next bridge to receive the message immediately discards it.

⚠ NOTICE

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

8.1.1.6 eRSTP

Siemens's enhanced Rapid Spanning Tree Protocol (eRSTP) improves the performance of RSTP in two ways:

- Improves the fault recovery time performance (< 5 ms per hop)
- Improves performance for large ring network topologies (up to 160 switches)

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

8.1.1.7 Fast Root Failover

Siemens's *Fast Root Failover* feature is an enhancement to RSTP that may be enabled or disabled. Fast Root Failover improves upon RSTP's handling of root bridge failures in mesh-connected networks.

⚠ NOTICE

Configuration hazard – risk of communication disruption

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

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

Two Fast Root Failover algorithms are available:

- **Robust** – Guarantees a deterministic root failover time, but requires support from all switches in the network, including the root switch

- **Relaxed** – Ensures a deterministic root failover time in most network configurations, but allows the use of a standard bridge in the root role

Note

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

Fast Root Failover and RSTP performance

- Running RSTP with Fast Root Failover disabled has no impact on RSTP performance in ring-connected networks.
- Fast Root Failover has no effect on RSTP performance in the case of failures that do not involve the root bridge or one of its links.
- The extra processing introduced by Fast Root Failover significantly decreases the worst-case failover time due to root bridge failure in mesh networks.

Recommendations on the use of Fast Root Failover

- It is not recommended to enable Fast Root Failover in single ring network topologies.
- It is strongly recommended to always connect the root bridge to each of its neighbor bridges using more than one link when enabled in ring-connected networks.

8.1.2 RSTP applications

This section describes various applications of RSTP.

8.1.2.1 RSTP in structured wiring configurations

RSTP may be used to construct structured wiring systems where connectivity is maintained in the event of link failures. For example, a single link failure of any link between A and N in figure 8.2, "Example - Structured wiring configuration" (Page 200) would leave all the ports of bridges 555 through 888 connected to the network.

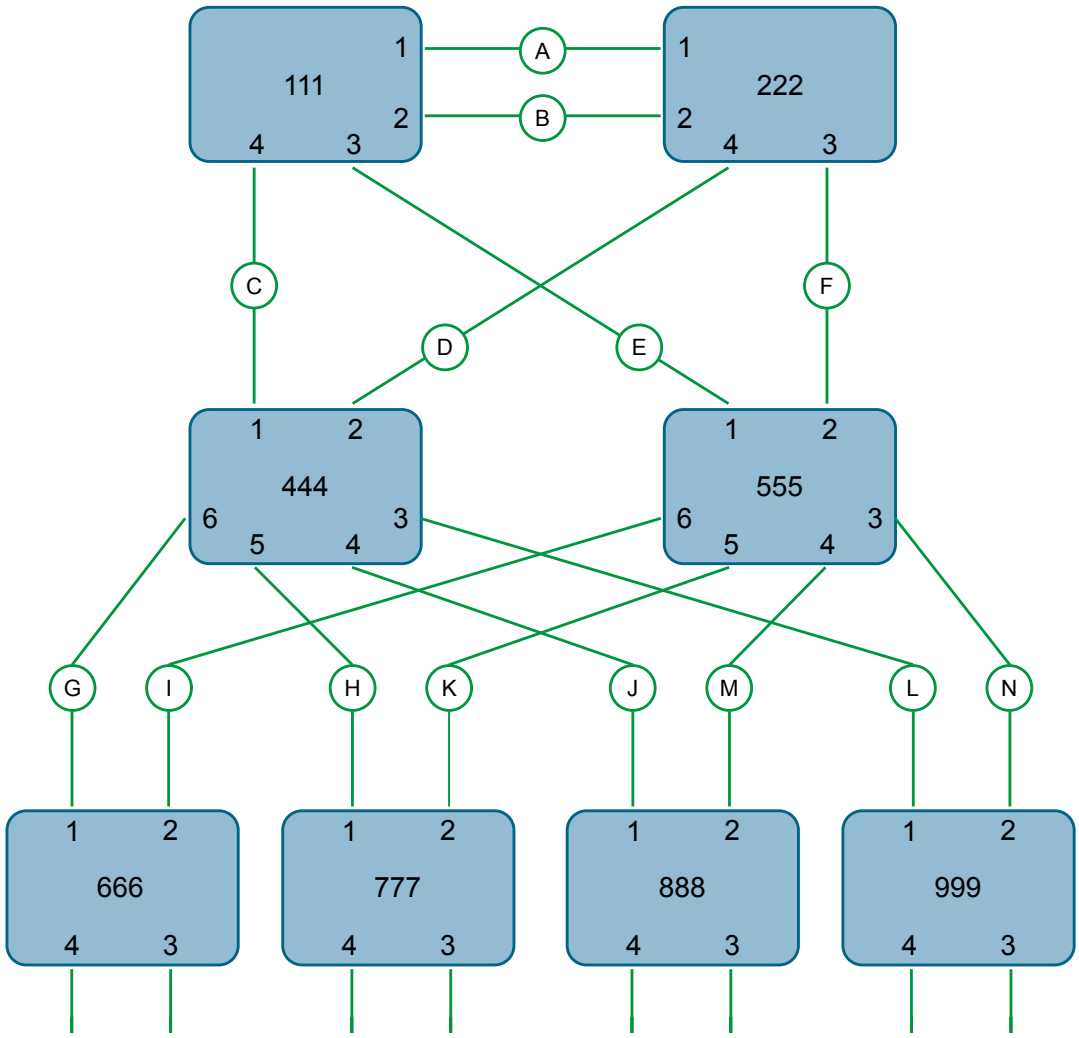


Figure 8.2 Example - Structured wiring configuration

To design a structured wiring configuration, do the following:

1. Select the design parameters for the network.
   - What are the requirements for robustness and network failover/recovery times?
   - Are there any special requirements for diverse routing to a central host computer?
   - Are there any special port redundancy requirements?
2. Identify required legacy support.
   - Are STP bridges used in the network?
   - These bridges do not support rapid transitioning to forwarding. If these bridges are present, can they be re-deployed closer to the network edge?
3. Identify edge ports and ports with half-duplex/shared media restrictions.

- Ports that connect to host computers, Intelligent Electronic Devices (IEDs) and controllers may be set to edge ports to guarantee rapid transitioning to forwarding as well as to reduce the number of topology change notifications in the network.
- Ports with half-duplex/shared media restrictions require special attention to guarantee that they do not cause extended fail-over/recovery times.

4. Choose the root bridge and backup root bridge carefully.
   - The root bridge should be selected to be at the concentration point of network traffic.
   - Locate the backup root bridge adjacent to the root bridge.
   - One strategy that may be used is to tune the bridge priority to establish the root bridge and then tune each bridge's priority to correspond to its distance from the root bridge.
5. Identify desired steady state topology.
   - Identify the desired steady state topology, taking into account link speeds, offered traffic, and QOS.
   - Examine of the effects of breaking selected links, taking into account network loading and the quality of alternate links.
6. Decide upon a port cost calculation strategy.
   - Select whether fixed or auto-negotiated costs should be used?

     It is recommended to use the auto-negotiated cost style, unless it is necessary for the network design to change the auto-negotiated cost style.
   - Select whether the STP or RSTP cost style should be used. Make sure to configure the same cost style on all devices on the network.
7. Enable Fast Root Failover option.
   - It is recommended to enable the Fast Root Failover option in mesh network topologies to minimize the network downtime in the event of a root bridge failure.
   - Fast Root Failover is a Siemens' proprietary eRSTP feature.
   - Fast Root Failover must be supported by all switches in the network, including the root, to guarantee optimal performance.
8. Calculate and configure priorities and costs.
9. Implement the network and test under load.

8.1.2.2 RSTP in ring backbone configurations

RSTP may be used in ring backbone configurations where rapid recovery from link failure is required. In normal operation, RSTP will block traffic on one of the links, for example, as indicated by the double bars through link H in figure 8.3, "Example - Ring

backbone configuration" (Page 202). In the event of a failure on link D, bridge 444 will unblock link H. Bridge 333 will communicate with the network through link F.

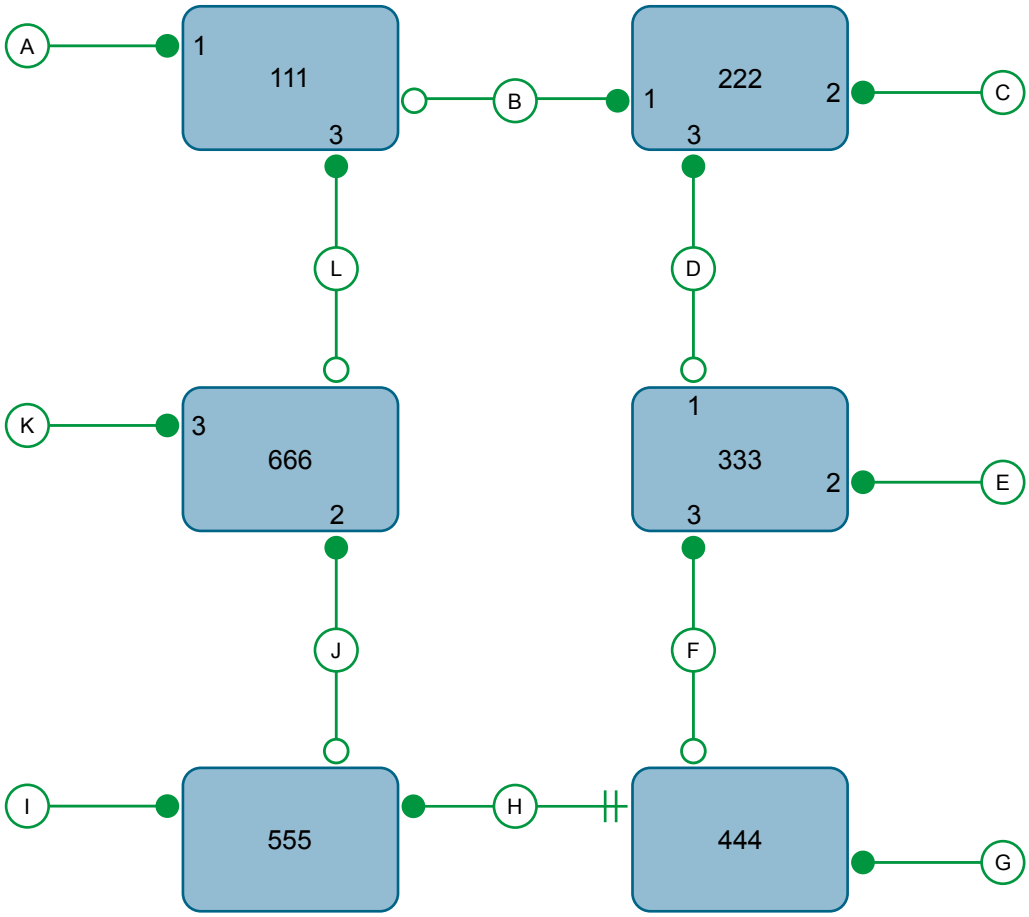


Figure 8.3 Example - Ring backbone configuration

To design a ring backbone configuration with RSTP, do the following:

1. Select the design parameters for the network.
   - What are the requirements for robustness and network fail-over/recovery times?
   - Typically, ring backbones are chosen to provide cost effective but robust network designs.
2. Identify required legacy support and ports with half-duplex/shared media restrictions.
   - These bridges should not be used if network fail-over/recovery times are to be minimized.
3. Identify edge ports.
   - Ports that connect to host computers, Intelligent Electronic Devices (IEDs) and controllers may be set to edge ports to guarantee rapid transitioning to

forwarding as well as to reduce the number of topology change notifications in the network.

4. Choose the root bridge.
   - The root bridge can be selected to equalize either the number of bridges, number of stations or amount of traffic on either of its legs. It is important to realize that the ring will always be broken in one spot and that traffic always flows through the root.
5. Assign bridge priorities to the ring.
   - For more information, refer to the RUGGEDCOM White Paper "Performance of the Rapid Spanning Tree Protocol in Ring Network Topology" available at https://assets.new.siemens.com/siemens/assets/api/uuid:d4af5d17-728c-493f-b00a-9c4db67b23ed/RSTP-whitepaper-EN-09-2020.pdf.
6. Decide upon a port cost calculation strategy.
   - It is recommended to use the auto-negotiated cost style, unless it is necessary for the network design to change the auto-negotiated cost style.
   - Select whether the STP or RSTP cost style should be used.
   - Make sure to configure the same cost style on all devices on the network.
7. Disable RSTP Fast Root Failover option.
   - This is a proprietary feature of Siemens. In RUGGEDCOM ROS, the RSTP Fast Root Failover option is enabled by default. It is recommended to disable this feature when operating in a Ring network.
8. Implement the network and test under load.

8.1.2.3 RSTP port redundancy

In cases where port redundancy is essential, RSTP allows more than one bridge port to service a LAN. In the following example, if port 3 is designated to carry the network traffic of LAN A, port 4 will block traffic. Should an interface failure occur on port 3, port 4 will assume control of the LAN.

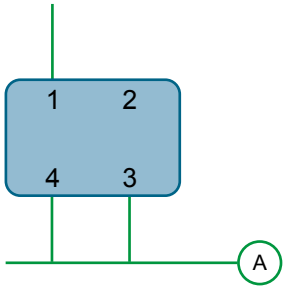


Figure 8.4 Example - Port redundancy

8.1.3 MSTP operation

The Multiple Spanning Tree (MST) algorithm and protocol provide greater control and flexibility than RSTP and legacy STP. MSTP (Multiple Spanning Tree Protocol) is an extension of RSTP, whereby multiple spanning trees may be maintained on the same bridged network. Data traffic is allocated to one or another of several spanning trees by mapping one or more VLANs onto the network.

The sophistication and utility of the Multiple Spanning Tree implementation on a given bridged network is proportional to the amount of planning and design invested in configuring MSTP.

If MSTP is activated on some or all of the bridges in a network with no additional configuration, the result will be a fully and simply connected network, but at best, the result will be the same as a network using only RSTP. Taking full advantage of the features offered by MSTP requires a potentially large number of configuration variables to be derived from an analysis of data traffic on the bridged network, and from requirements for load sharing, redundancy, and path optimization. Once these parameters have all been derived, it is also critical that they are consistently applied and managed across all bridges in an MST region.

By design, MSTP processing time is proportional to the number of active STP instances. This means that MSTP will likely be significantly slower than RSTP. Therefore, for mission critical applications, RSTP should be considered a better network redundancy solution than MSTP.

8.1.3.1 MSTP regions and interoperability

In addition to supporting multiple spanning trees in a network of MSTP-capable bridges, MSTP is capable of inter-operating with bridges that support only RSTP or legacy STP, without requiring any special configuration.

An MST region may be defined as the set of interconnected bridges whose MST Region Identification is identical. The interface between MSTP bridges and non-MSTP bridges, or between MSTP bridges with different MST Region Identification information, becomes part of an MST Region boundary.

Bridges outside an MST region will see the entire region as though it were a single (R)STP bridge; the internal detail of the MST region is hidden from the rest of the bridged network. In support of this, MSTP maintains separate *hop counters* for spanning tree information exchanged at the MST region boundary versus that propagated inside the region. For information received at the MST region boundary, the (R)STP Message Age is incremented only once. Inside the region, a separate Remaining Hop Count is maintained, one for each spanning tree instance. The external Message Age parameter is referred to the (R)STP Maximum Age Time, whereas the internal Remaining Hop Counts are compared to an MST region-wide Maximum Hops parameter.

MSTI

An MSTI (Multiple Spanning Tree Instance) is one of sixteen independent spanning tree instances that may be defined in an MST region (not including the IST – see below). An MSTI is created by mapping a set of VLANs (in RUGGEDCOM ROS, via the VLAN configuration) to a given MSTI ID. The same mapping must be configured on all bridges that are intended to be part of the MSTI. Moreover, all VLAN to MSTI mappings must be identical for all bridges in an MST region.

RUGGEDCOM ROS supports 16 MSTIs in addition to the IST.

Each MSTI has a topology that is independent of every other. Data traffic originating from the same source and bound to the same destination but on different VLANs on different MSTIs may therefore travel a different path across the network.

IST

An MST region always defines an IST (Internal Spanning Tree). The IST spans the entire MST region, and carries all data traffic that is not specifically allocated (by VLAN) to a specific MSTI. The IST is always computed and is defined to be MSTI zero.

The IST is also the extension inside the MST region of the CIST (see below), which spans the entire bridged network, inside and outside of the MST region and all other RSTP and STP bridges, as well as any other MST regions.

CST

The CST (Common Spanning Tree) spans the entire bridged network, including MST regions and any connected STP or RSTP bridges. An MST region is seen by the CST as an individual bridge, with a single cost associated with its traversal.

CIST

The CIST (Common and Internal Spanning Tree) is the union of the CST and the ISTs in all MST regions. The CIST therefore spans the entire bridged network, reaching into each MST region via the latter's IST to reach every bridge on the network.

8.1.3.2 MSTP bridge and port roles

MSTP supports the following bridge and port roles:

Bridge roles

Role	Description
CIST Root	The CIST Root is the elected root bridge of the CIST (Common and Internal Spanning Tree), which spans all connected STP and RSTP bridges and MSTP regions.
CIST Regional Root	The root bridge of the IST within an MSTP region. The CIST Regional Root is the bridge within an

Role	Description
	MSTP region with the lowest cost path to the CIST Root. Note that the CIST Regional Root will be at the boundary of an MSTP region. Note also that it is possible for the CIST Regional Root to be the CIST Root.
MSTI Regional Root	The root bridge for an MSTI within an MSTP region. A root bridge is independently elected for each MSTI in an MSTP region.

Port roles

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

Role	Description
CIST Port Roles	• The Root Port provides the minimum cost path from the bridge to the CIST Root via the CIST Regional Root. If the bridge itself happens to be the CIST Regional Root, the Root Port is also the Master Port for all MSTIs, and provides the minimum cost path to a CIST Root located outside the region. • A Designated Port provides the minimum cost path from an attached LAN, via the bridge to the CIST Regional Root. • Alternate and Backup Ports function the same as they do in RSTP, but relative to the CIST Regional Root.
MSTI Port Roles	For each MSTI on a bridge: • The Root Port provides the minimum cost path from the bridge to the MSTI Regional Root, if the bridge itself is not the MSTI Regional Root. • A Designated Port provides the minimum cost path from an attached LAN, via the bridge to the MSTI Regional Root. • Alternate and Backup Ports function the same as they do in RSTP, but relative to the MSTI Regional Root. The Master Port, which is unique in an MSTP region, is the CIST Root Port of the CIST Regional Root, and provides the minimum cost path to the CIST Root for all MSTIs.
Boundary Ports	A Boundary Port is a port on a bridge in an MSTP region that connects to either: a bridge belonging to a different MSTP region, or a bridge supporting only RSTP or legacy STP. A Boundary Port blocks or forwards all VLANs from all MSTIs and the CIST alike. A Boundary Port may be: • The CIST Root Port of the CIST Regional Root (and therefore also the MSTI Master Port). • A CIST Designated Port, CIST Alternate/ Backup Port, or Disabled. At the MSTP region

Role	Description
	boundary, the MSTI Port Role is the same as the CIST Port Role. A Boundary Port connected to an STP bridge will send only STP BPDUs. One connected to an RSTP bridge need not refrain from sending MSTP BPDUs. This is made possible by the fact that the MSTP carries the CIST Regional Root Identifier in the field that RSTP parses as the Designated Bridge Identifier.

8.1.3.3 Benefits of MSTP

Despite the fact that MSTP is configured by default to arrive automatically at a spanning tree solution for each configured MSTI, advantages may be gained from influencing the topology of MSTIs in an MST region. The fact that the Bridge Priority and each port cost are configurable per MST makes it possible to control the topology of each MSTI within a region.

Load balancing

MSTP can be used to balance data traffic load among sets of VLANs, enabling more complete utilization of a multiply interconnected bridged network.

A bridged network controlled by a single spanning tree will block redundant links by design, to avoid harmful loops. Using MSTP, however, any given link may have a different blocking state for MSTI, as maintained by MSTP. Any given link, therefore, might be in blocking state for some VLANs, and in forwarding state for other VLANs, depending on the mapping of VLANs to MSTIs.

It is possible to control the spanning tree solution for each MSTI, especially the set of active links for each tree, by manipulating, per MSTI, the bridge priority and the port costs of links in the network. If traffic is allocated judiciously to multiple VLANs, redundant interconnections in a bridged network which, using a single spanning tree, would have gone unused, can now be made to carry traffic.

Isolation of Spanning Tree reconfiguration.

A link failure in an MSTP region that does not affect the roles of Boundary ports will not cause the CST to be reconfigured, nor will the change affect other MSTP regions. This is due to the fact that MSTP information does not propagate past a region boundary.

MSTP vs. PVST

An advantage of MSTP over the Cisco Systems Inc. proprietary Per-VLAN Spanning Tree (PVST) protocol is the ability to map multiple VLANs onto a single MSTI. Since each spanning tree requires processing and memory, the expense of keeping track of an increasing number of VLANs increases much more rapidly for PVST than for MSTP.

Compatibility with STP and RSTP

No special configuration is required for the bridges of an MST region to connect fully and simply to non-MST bridges on the same bridged network. Careful planning and configuration is, however, recommended to arrive at an optimal network.

8.1.3.4 Implementing MSTP on a bridged network

It is recommended the configuration of MSTP on a network proceed in the sequence outlined below.

Naturally, it is also recommended that network analysis and planning inform the steps of configuring the VLAN and MSTP parameters in particular.

Begin with a set of MSTP-capable Ethernet bridges and MSTP disabled. For each bridge in the network:

Note

MSTP does not need to be enabled to map a VLAN to an MSTI. However, the mapping must be identical for each bridge that belongs to the MSTP region.

1. Configure and enable STP globally and/or for specific Ethernet ports. For more information, refer to "Configuring STP globally" (Page 209) or "Configuring STP for specific Ethernet ports" (Page 210).

   Note

   Static VLANs must be used in an MSTP configuration. GVRP is not supported.

2. Add static VLANs and map them to MSTIs. For more information, refer to "Adding a static VLAN" (Page 171).

   Note

   The Region Identifier and Revision Level must be the same for each bridge in the MST region.

3. Configure the revision level for the MST Region Identifier. For more information, refer to "Configuring the MST region identifier" (Page 220).
4. Make sure the read-only digest for the MST Region Identifier is identical for each bridge in the MST region. If the digest is different, the set of mappings from VLANs to MSTIs differs.
5. Configure the Bridge Priority for the global MSTI. For more information, refer to "Configuring a global MSTI" (Page 220).
6. Configure the Port Cost and Priority per Port for each MSTI. For more information, refer to "Configuring an MSTI for an Ethernet port" (Page 221).
7. Set the STP Protocol Version to MSTP and enable STP. For more information, refer to "Configuring STP globally" (Page 209).

8.1.4 Configuring STP globally

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

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

Parameter	Description
`State`	**Synopsis:** [Disabled | Enabled] **Default:** Enabled Enable STP/RSTPfor the bridge globally. Note that STP/RSTPis enabled on a port when it is enabled globally and along with enabling per port setting.
`Version Support`	**Default:** RSTP Selects the version of Spanning Tree Protocol to support, either only STP or Rapid STP.
`Bridge Priority`	**Synopsis:** [0 | 4096 | 8192 | 12288 | 16384 | 20480 | 24576 | 28672 | 32768 | 36864 | 40960 | 45056 | 49152 | 53248 | 57344 | 61440] **Default:** 32768 Bridge Priority provides a way to control the topology of the STP connected network. The desired Root and Designated bridges can be configured for a particular topology. The bridge with the lowest priority will become root. In the event of a failure of the root bridge, the bridge with the next lowest priority will then become root. Designated bridges that (for redundancy purposes) service a common LAN also use priority to determine which bridge is active. In this way careful selection of Bridge Priorities can establish the path of traffic flows in normal and abnormal conditions.
`Hello Time`	**Synopsis:** An integer between 1 and 10 **Default:** 2 Time between configuration messages issued by the root bridge. Shorter hello times result in faster detection of topology changes at the expense of moderate increases in STP traffic.
`Max Age Time`	**Synopsis:** An integer between 6 and 40 **Default:** 20 The time for which a configuration message remains valid after being issued by the root bridge. Configure this parameter with care when many tiers of bridges exist, or slow speed links (such as those used in WANs) are part of the network
`Transmit Count`	**Synopsis:** An integer between 3 and 100 or [Unlimited] **Default:** Unlimited Maximum number of BPDUs on each port that may be sent in one second. Larger values allow the network to recover from failed links/bridges more quickly.

Parameter	Description
`Forward Delay`	**Synopsis:** An integer between 4 and 30 **Default:** 15 The amount of time a bridge spends learning MAC addresses on a rising port before beginning to forward traffic. Lower values allow the port to reach the forwarding state more quickly, but at the expense of flooding unlearned addresses to all ports.
`Max Hops`	**Synopsis:** An integer between 6 and 40 **Default:** 20 Only applicable to MSTP. The maximum possible bridge diameter inside an MST region. MSTP BPDUs propagating inside an MST region specify a time-to-live that is decremented by every switch that propagates the BPDU. If the maximum number of hops inside the region exceeds the configured maximum, BPDUs may be discarded due to their time-to-live setting.

3. Click **Apply**.

8.1.5 Configuring STP for specific Ethernet ports

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

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

Parameter	Description
`Port(s)`	**Synopsis:** Comma-separated list of ports The port number of the device (or a list of ports, if aggregated in a port trunk).
`Enabled`	**Synopsis:** [Disabled | Enabled] **Default:** Enabled Enabling STP activates the STP or RSTP protocol for this port per the configuration in the STP Configuration menu. STP may be disabled for the port ONLY if the port does not attach to an STP enabled bridge in any way. Failure to meet this requirement WILL result in an undetectable traffic loop in the network. A better alternative to disabling the port is to leave STP enabled but to configure the port as an edge port. A good candidate for disabling STP would be a port that services only a single host computer.

Parameter	Description
`Priority`	**Synopsis:** [0 | 16 | 32 | 48 | 64 | 80 | 96 | 112 | 128 | 144 | 160 | 176 | 194 | 208 | 224 | 240] **Default:** 128 Selects the STP port priority. Ports of the same cost that attach to a common LAN will select the port to be used based upon the port priority.
`STP Cost`	**Synopsis:** An integer between 0 and 65535 or [Auto] **Default:** Auto Selects the cost to use in cost calculations, when the Cost Style parameter is set to STP in the Bridge RSTP Parameters configuration. Setting the cost manually provides the ability to preferentially select specific ports to carry traffic over others. Leave this field set to "auto" to use the standard STP port costs as negotiated (4 for 1Gbps, 19 for 100 Mbps links and 100 for 10 Mbps links). For MSTP, this parameter applies to both external and internal path cost.
`RSTP Cost`	**Synopsis:** An integer between 0 and 2147483647 or [Auto] **Default:** Auto Selects the cost to use in cost calculations, when the Cost Style parameter is set to RSTP in the Bridge RSTP Parameters configuration. Setting the cost manually provides the ability to preferentially select specific ports to carry traffic over others. Leave this field set to "auto" to use the standard RSTP port costs as negotiated (20,000 for 1Gbps, 200,000 for 100 Mbps links and 2,000,000 for 10 Mbps links).
`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

Parameter	Description
	true when the port operates a point-to-point link but cannot run the link in full-duplex mode. Force the parameter false when the port operates the link in full-duplex mode, but is still not point-to-point (e.g. a full-duplex link to an unmanaged bridge that concentrates two other STP bridges).
`Restricted Role`	**Synopsis:** [True | False] **Default:** False A boolean value set by management. If TRUE, causes the Port not to be selected as the Root Port for the CIST or any MSTI, even if it has the best spanning tree priority vector. Such a Port will be selected as an Alternate Port after the Root Port has been selected. This parameter should be FALSE by default. If set, it can cause a lack of spanning tree connectivity. It is set by a network administrator to prevent bridges that are external to a core region of the network from influencing the spanning tree active topology. This may be necessary, for example, if those bridges are not under the full control of the administrator.
`Restricted TCN`	**Synopsis:** [True | False] **Default:** False A boolean value set by management. If TRUE, it causes the Port not to propagate received topology change notifications and topology changes to other Ports. If set, it can cause temporary loss of connectivity after changes in a spanning tree's active topology as a result of persistent, incorrectly learned, station location information. It is set by a network administrator to prevent bridges that are external to a core region of the network from causing address flushing in that region. This may be necessary, for example, if those bridges are not under the full control of the administrator or if the MAC_Operational status parameter for the attached LANs transitions frequently.

4. Click **Apply**.

8.1.6 Configuring eRSTP

To configure eRSTP, do the following:

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

Parameter	Description
`Max Network Diameter`	**Synopsis:** [MaxAgeTime | 4*MaxAgeTime] **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

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

Parameter	Description
	• **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**.

8.1.7 Viewing global statistics for STP

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

This table displays the following information:

Parameter	Description
`Bridge Status`	**Synopsis:** [Designated Bridge | Not Designated For Any LAN | Root Bridge] 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`	If the bridge is designated, this is the port that provides connectivity towards the root bridge of the network.
`Root Path Cost`	**Synopsis:** An integer between 0 and 4294967295 Total cost of the path to the root bridge composed of the sum of the costs of each link in the path. If custom costs have not been configured. 1Gbps ports will contribute 4, 100 Mbps ports will contribute 19 and 10 Mbps ports will contribute a cost of 100 to this figure.
`Configured Hello Time`	**Synopsis:** An integer between 0 and 65535 The configured Hello time from the Bridge RSTP Parameters menu.
`Learned Hello Time`	**Synopsis:** An integer between 0 and 65535 The actual Hello time provided by the root bridge as learned in configuration messages. This time is used in designated bridges.
`Configured Forward Delay`	**Synopsis:** An integer between 0 and 65535 The configured Forward Delay time from the Bridge RSTP Parameters menu.
`Learned Forward Delay`	**Synopsis:** An integer between 0 and 65535 The actual Forward Delay time provided by the root bridge as learned in configuration messages. This time is used in designated bridges.
`Configured Max Age`	**Synopsis:** An integer between 0 and 65535 The configured Maximum Age time from the Bridge RSTP Parameters menu.
`Learned Max Age`	**Synopsis:** An integer between 0 and 65535 The actual Maximum Age time provided by the root bridge as learned in configuration messages. This time is used in designated bridges.

Parameter	Description
`Total Topology Changes`	**Synopsis:** An integer between 0 and 65535 A count of topology changes in the network, as detected on this bridge through link failures or as signaled from other bridges. Excessively high or rapidly increasing counts signal network problems.
`Time since Last TC`	**Synopsis:** DDDD days, HH:MM:SS The time since the last time a topology change was detected by the bridge.

8.1.8 Viewing STP statistics for Ethernet ports

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

This table displays the following information:

Parameter	Description
`Port(s)`	**Synopsis:** Comma-separated list of ports The port number of the device (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. • **Listening** – This state is not used by . • **Learning** – The port is learning MAC addresses to prevent flooding when it begins forwarding traffic. • **Forwarding** – The port is forwarding traffic. • **Blocking** – The port is blocking traffic. • **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.
`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.

Parameter	Description
	• **Alternate** – The port is attached to a bridge that provides connectivity to the root bridge. It is not used but is standing by. • **Master** – Only exists in MSTP. The port is an MST region boundary port and the single port on the bridge, which provides connectivity for the Multiple Spanning Tree Instance towards the Common Spanning Tree root bridge (i.e. this port is the root port for the Common Spanning Tree Instance).
`Cost`	**Synopsis:** An integer between 0 and 4294967295 Cost offered by this port. If the Bridge RSTP Parameters Cost Style is set to STP, 1Gbps ports will contribute 4, 100 Mbps ports will contribute 19 and 10 Mbps ports contribute a cost of 100. If the Cost Style is set to RSTP, 1Gbps will contribute 20,000, 100 Mbps ports will contribute a cost of 200,000 and 10 Mbps ports contribute a cost of 2,000,000. Note that even if the Cost style is set to RSTP, a port that migrates to STP will have its cost limited to a maximum of 65535.
`RX RSTs`	**Synopsis:** An integer between 0 and 4294967295 The count of RSTP configuration messages received on this port.
`TX RSTs`	**Synopsis:** An integer between 0 and 4294967295 The count of RSTP configuration messages transmitted on this port.
`RX Configs`	**Synopsis:** An integer between 0 and 4294967295 The count of STP configuration messages received on this port.
`TX Configs`	**Synopsis:** An integer between 0 and 4294967295 The count of STP configuration messages transmitted on this port.
`RX Tcns`	**Synopsis:** An integer between 0 and 4294967295 The count of STP topology change notification messages received on this port. Excessively high or rapidly increasing counts signal network problems.
`TX Tcns`	**Synopsis:** An integer between 0 and 4294967295 The count of STP topology change notification messages transmitted on this port.
`Desig Bridge ID`	**Synopsis:** $$ / ##-##-##-##-##-## where $$ is 0 to 65535, ## is 0 to FF Provided on the root ports of designated bridges, the Bridge Identifier of the bridge this port is connected to.
`operEdge`	**Synopsis:** [True | False] The port is operating as an edge port or not.

8.1.9 Managing multiple spanning tree instances

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

8.1.9.1 Viewing statistics for global MSTIs

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

This table displays the following information:

Parameter	Description
`Bridge Status`	**Synopsis:** [Designated Bridge | Not Designated For Any LAN | Root Bridge] 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`	If the bridge is designated, this is the port that provides connectivity towards the root bridge of the network.
`Root Path Cost`	**Synopsis:** An integer between 0 and 4294967295 Total cost of the path to the root bridge composed of the sum of the costs of each link in the path. If custom costs have not been configured. 1Gbps ports will contribute 4, 100 Mbps ports will contribute 19 and 10 Mbps ports will contribute a cost of 100 to this figure.
`Total Topology Changes`	**Synopsis:** An integer between 0 and 65535 A count of topology changes in the network, as detected on this bridge through link failures or as signaled from other bridges. Excessively high or rapidly increasing counts signal network problems.

8.1.9.2 Viewing statistics for port MSTIs

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

This table displays the following information:

Parameter	Description
`Port(s)`	**Synopsis:** Comma-separated list of ports The port number of the device (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. • **Listening** – This state is not used by . • **Learning** – The port is learning MAC addresses in order to prevent flooding when it begins forwarding traffic. • **Forwarding** – The port is forwarding traffic. • **Blocking** – The port is blocking traffic. • **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.
`Role`	**Synopsis:** [Root | Designated | Alternate | Backup | Master] Role of this port in Spanning Tree. This may be one of the following: • **Designated** – The port is designated for (i.e. carries traffic towards the root for) the LAN it is connected to. • **Root** – The single port on the bridge, which provides connectivity towards the root bridge. • **Backup** – The port is attached to a LAN that is serviced by another port on the bridge. It is not used but is standing by. • **Alternate** – The port is attached to a bridge that provides connectivity to the root bridge. It is not used but is standing by. • **Master** – Only exists in MSTP. The port is an MST region boundary port and the single port on the bridge, which provides connectivity for the Multiple Spanning Tree Instance towards the Common Spanning Tree root bridge (i.e. this port is the root port for the Common Spanning Tree Instance).
`Cost`	**Synopsis:** An integer between 0 and 4294967295 Cost offered by this port. If the Bridge RSTP Parameters Cost Style is set to STP, 1Gbps ports will contribute 4, 100 Mbps ports will contribute 19 and 10 Mbps ports contribute a cost of 100. If the Cost Style is set to RSTP, 1Gbps will contribute 20,000, 100 Mbps ports will contribute a cost of 200,000 and 10 Mbps ports contribute a cost of 2,000,000. Note that even if the Cost style is set to RSTP, a port that migrates to STP will have its cost limited to a maximum of 65535.
`Desig Bridge ID`	**Synopsis:** $$ / ##-##-##-##-##-## where $$ is 0 to 65535, ## is 0 to FF Provided on the root ports of designated bridges, the Bridge Identifier of the bridge this port is connected to.

8.1.9.3 Configuring the MST region identifier

Configuring the region identifier and revision level puts the MSTP bridge in a defined group. Other bridges that have the same identifier and revision level are interconnected within this region. For more information, refer to "MSTP regions and interoperability" (Page 204).

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

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

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

3. Click **Apply**.

8.1.9.4 Configuring a global MSTI

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

1. Navigate to ***Network Redundancy » Spanning Tree » Configure Bridge MSTI Parameters***. The **Bridge MSTI Parameters** form appears.
2. Under **Instance ID**, type an ID number for a Multiple Spanning Tree Instance (MSTI) and click **GET**. The settings for the MSTI are displayed. Any changes made to the configuration will be applied specifically to this instance ID.

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

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

4. Click **Apply**.

8.1.9.5 Configuring an MSTI for an Ethernet port

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

1. Navigate to ***Network Redundancy » Spanning Tree » Configure Port MSTI Parameters***. The **Port MSTI Parameters** table appears.
2. Select an Ethernet port. The **Port MSTI Parameters** form appears.
3. Under **Instance ID**, type an ID number for a Multiple Spanning Tree Instance (MSTI) and click **GET**. The settings for the MSTI are displayed. Any changes made to the configuration will be applied specifically to this instance ID.
4. Configure the following parameter(s) as required:

Parameter	Description
`Port(s)`	**Synopsis:** Comma-separated list of ports The port number of the device (or a list of ports, if aggregated in a port trunk).
`Priority`	**Synopsis:** [0 | 16 | 32 | 48 | 64 | 80 | 96 | 112 | 128 | 144 | 160 | 176 | 192 | 208 | 224 | 240] **Default:** 128 Selects the STP port priority. Ports of the same cost that attach to a common LAN will select the port to be used based upon the port priority.
`STP Cost`	**Synopsis:** An integer between 0 and 65535 or [Auto] **Default:** Auto Selects the cost to use in cost calculations, when the Cost Style parameter is set to STP in the Bridge RSTP Parameters

Parameter	Description
	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).
`RSTP Cost`	**Synopsis:** An integer between 0 and 2147483647 or [Auto] **Default:** Auto Selects the cost to use in cost calculations, when the Cost Style parameter is set to RSTP in the Bridge RSTP Parameters configuration. Setting the cost manually provides the ability to preferentially select specific ports to carry traffic over others. Leave this field set to "auto" to use the standard RSTP port costs as negotiated (20,000 for 1Gbps, 200,000 for 100 Mbps links and 2,000,000 for 10 Mbps links).

5. Click **Apply**.

8.1.10 Clearing spanning tree protocol statistics

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

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

8.2 Managing the Media Redundancy Protocol (MRP)

RUGGEDCOM ROS supports the Media Redundancy Protocol (MRP).

8.2.1 Understanding MRP

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

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

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

⚠ NOTICE
MRP does not function on Ethernet-over-VDSL (EoVDSL) ports. For more information about EoVDSL, refer to "Managing EoVDSL Ports" (Page 81).

8.2.1.1 MRM vs MRC devices

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

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

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

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

8.2.1.2 MRA devices

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

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

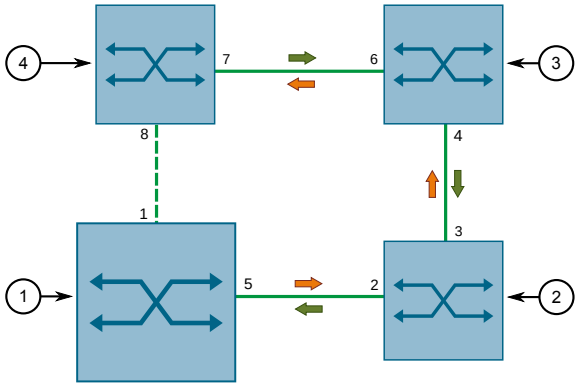
8.2.1.3 Ring port states

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

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

8.2.1.4 Ring-closed vs ring-open

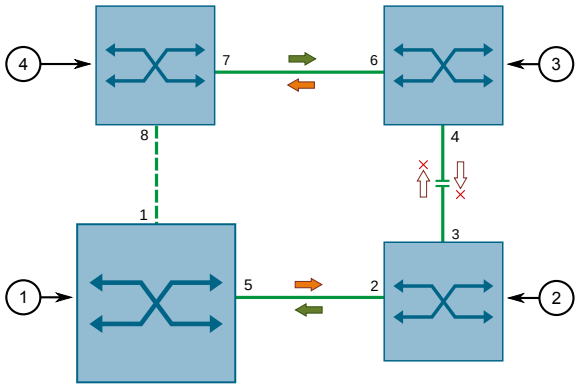
During normal operation, the network works in the ring-closed state. In this state, one of the MRM ring ports is blocked, while the other is forwarding. Both ring ports of all MRCs are forwarding.



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

Figure 8.5 MRP Ring-Closed State

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



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

④ MRP Client 3

Figure 8.6 MRP Ring-Open State

8.2.2 Configuring MRP globally

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

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

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

3. Click **Apply**.

8.2.3 Viewing the status of MRP instances

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

This table displays the following information:

Parameter	Description
`Index`	The MRP instance number.
`Name`	**Synopsis:** A string up to 24 characters long or [default-mrpdomain] **Default:** default-mrpdomain The name of the MRP domain/ring. All MRP instances belonging to the same ring must have the same domain name.
`Role`	The role assigned to the MRP instance: • **Disabled** – No role is assigned. The MRP instance is disabled. • **Client** – MRP Client. • **Manager** – MRP Manager.

Parameter	Description
	• **ManagerAuto** – MRP instance automatically determines the role.
Ring Status	The status of the MRP ring. Possible values include: • **N/A** – The status of the ring is unknown. This is displayed when the device is an MRC. • **Open** – The MRP ring is open. Both ring ports are forwarding packets. • **Closed** – The MRP ring is closed. One ring port is forwarding packets, while the other is blocking packets.
PRM Port	The port number and state of the MRP ring port. Possible values include: • **{ port }-OFF** – MRP not running. • **{ port }-DWN** – The ring port is down. • **{ port }-BLK** – The ring port is blocking packets. • **{ port }-FWD** – The ring port is forwarding packets.
SEC Port	The port number and state of the MRP ring port. Possible values include: • **{ port }-OFF** – MRP not running. • **{ port }-DWN** – The ring port is down. • **{ port }-BLK** – The ring port is blocking packets. • **{ port }-FWD** – The ring port is forwarding packets.
Multi-MRM Err	Error indicated by an MRM when more than one MRM are active in the MRP ring. Possible values include: • **false** – No Multi-MRM error. • **true** – More than one MRM present in the ring.
One Side Rx Err	Error indicated by an MRM when the test frames of an MRM have been seen, but only on one ring port. Possible values include: • **false** – No One Side Rx error. • **true** – Test frame received only on one ring port.

8.2.4 Adding an MRP instance

To configure an MRP instance, do the following:

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

⚠ NOTICE

Configuration hazard – risk of communication disruption

RUGGEDCOM ROS only allows multiple MRP instances if the device is the ring manager in each instance. A device can have up to four ring manager instances.

⚠ NOTICE

Configuration hazard – risk of communication disruption

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

For more information about configuring port parameters, refer to "Configuring an Ethernet port" (Page 67).

For more information about open and closed MRP rings, refer to "Managing the Media Redundancy Protocol (MRP)" (Page 222).

Note

To avoid potential misconfiguration issues which can result in loss of network access, Siemens recommends disabling the ring port of an MRC before configuring it. For more information about configuring port parameters, refer to "Configuring an Ethernet port" (Page 67).

Note

When using port security in an MRP ring, the MAC addresses of devices in the ring must be configured to allow communication between them. Also, the MRM's ring port must be configured in the **Static MAC Addresses** table for the ring to remain in a closed state. For more information, refer to "Static MAC address-based authentication in an MRP ring" (Page 142).

3. Configure the following parameters:

Parameter	Description
`Index`	**Synopsis:** An integer between 1 and 4 **Default:** 1 The MRP instance number.
`Name`	**Synopsis:** A string up to 24 characters long **Default:** default-mrpdomain The name of the MRP domain/ring. All MRP instances belonging to the same ring must have the same domain name. **⚠ NOTICE** Names cannot contain spaces between words (e.g. "LAN Ring"). Spaces must be replaced with underscores (e.g. LAN_Ring).
`Role`	**Synopsis:** [Disabled | Client | Manager | ManagerAuto] **Default:** Client The role assigned to the MRP instance:

Parameter	Description
	• **Disabled** – No role is assigned. The MRP instance is disabled. • **Client** – MRP Client. • **Manager** – MRP Manager. • **ManagerAuto** – MRP instance automatically determines the role.
PRM Port	**Synopsis:** 1 to maximum port number **Default:** 1 MRP ring port number. The port number as seen on the device.
SEC Port	**Synopsis:** 1 to maximum port number **Default:** 1 MRP ring port number. The port number as seen on the device.
Priority	**Synopsis:** A string up to 4 characters long **Default:** 8000 The priority assigned to the MRP instance. This is used when negotiating with other MRP devices to determine which is the MRP Manager. Possible values include: • **0000** – Highest priority (Manager) • **1000-7000** – High priority (Manager) • **8000** – Default priority (Manager) • **9000-E000** – Low priority (ManagerAuto) • **F000** – Lowest priority (ManagerAuto) The priority only applies when Role is set to Manager or ManagerAuto.
ID	**Synopsis:** A string up to 32 characters long **Default:** FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF 128-bit domain UUID unique to a domain/ring. All MRP instances belonging to the same ring must have the same domain ID. If the Auto Generate UUID parameter is enabled, ROS automatically generates the domain ID as an MD5 hash of the domain name. In this case, any attempt to modify the domain ID will be rejected. If the Auto Generate UUID parameter is disabled, the domain ID can be modified by the user.

4. Click **Apply**.

8.2.5 Deleting an MRP instance

To delete an MRP instance, do the following:

1. Navigate to ***Network Redundancy » Ring Redundancy » Configure MRP Instances***. The **MRP Instances** table appears.

2. Click the desired record. The **MRP Instances** form appears.

⚠ NOTICE

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

For more information about configuring port parameters, refer to "Configuring an Ethernet port" (Page 67).

For more information about open and closed MRP rings, refer to "Managing the Media Redundancy Protocol (MRP)" (Page 222).

Note

To avoid potential misconfiguration issues which can result in loss of network access, Siemens recommends disabling the ring port of an MRC before configuring it. For more information about configuring port parameters, refer to "Configuring an Ethernet port" (Page 67).

3. Click **Delete**.

8.2.6 Example: Configuring an MRP ring

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

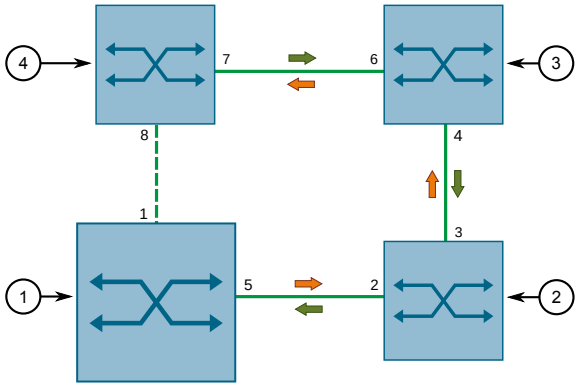
In the following topology, the MRP ring is operating in the ring-closed state. The MRP Manager (MRM) device serves as the ring manager, while the MRP Client (MRC) devices act as member nodes of the ring. Each MRM or MRC node has two ports participating in the ring.

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

For more information about ring-closed and ring-open states, refer to "Managing the Media Redundancy Protocol (MRP)" (Page 222).

⚠ NOTICE

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



① MRP Manager
② MRP client 1
③ MRP client 2
④ MRP client 3

Figure 8.7 Topology – MRP ring

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

1. Make sure RSTP is disabled on ports acting as PRM and SEC ports in the ring. For more information, refer to "Configuring an Ethernet port" (Page 67).
2. Enable MRP on the MRP Manager and all MRP Client devices. For more information, refer to "Configuring MRP globally" (Page 225).
3. Configure an MRP instance for the MRP Manager device as follows:

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

For more information about configuring MRP instances, refer to "Adding an MRP instance" (Page 226).

4. Configure an MRP instance for each MRP Client device as follows:

Note

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

Device	Parameter	Value
MRP Client 1	Name	{ name }
	Role	Client
	PRM Port	2

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

For more information about configuring MRP instances, refer to "Adding an MRP instance" (Page 226).

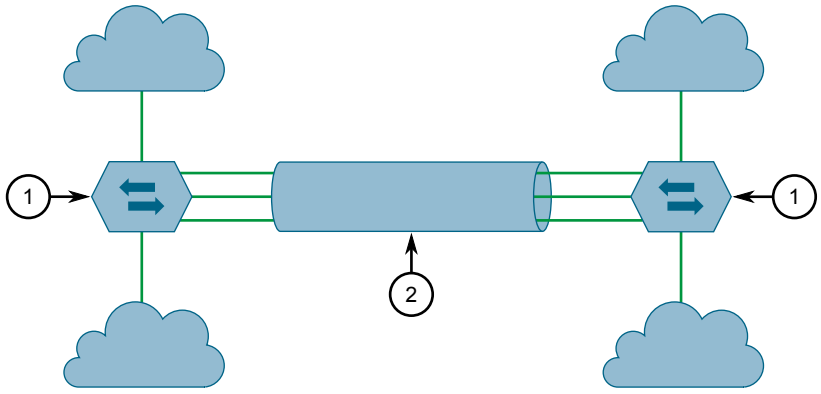
5. To verify the configuration, make sure the MRP Instance ID is generated automatically on the MRP Manager device and each MRP client device. For more information about the MRP Instance ID, refer to "Adding an MRP instance" (Page 226).

8.3 Managing link aggregation

Link aggregation, also referred to as *port trunking* or *port bundling*, provides the ability to aggregate or combine several Ethernet ports into one logical link (Link Aggregation Group) with higher bandwidth. This allows for highly randomized load balancing between the aggregated links based on both the source and destination MAC addresses of the forwarded frames.

Link aggregation can be used for two purposes:

- To obtain increased, linearly incremental link bandwidth.
- To improve network reliability by creating link redundancy. If one of the aggregated links fails, the switch will balance the traffic between the remaining links.



① Device
② Link Aggregation Group (LAG)

Figure 8.8 Basic link aggregation topography

8.3.1 Link aggregation concepts

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

8.3.1.1 Static vs. dynamic link aggregation

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

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

- **Failover**
  In static link aggregation, devices are unable to communicate the status of their LAGs. Should all ports in a LAG go down and there is a media converter between both devices, the device at the other end will not know and continue to send traffic to its partner. Dynamic link aggregation, however, will detect the failed link and stop sending traffic to the other device.
- **Renegotiation**
  Should all ports on the partner device go down and/or the Signal-to-Noise Ratio (SNR) be too high, LACP will automatically seek another LACP-enabled device on the network with which to form a new port channel.

- **Standby**
  If more ports are added to a LAG than the device supports, LACP will automatically put the excess ports on standby. It determines which ports to put on standby based on criteria defined by the user. These standby ports will wait until an active port fails and then take its place.
- **Link verification**
  In dynamic link aggregation, both partners can mutually verify the port channel between them, making it easy for users to confirm the configuration. Static link aggregation offers no such verification.

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

8.3.1.2 Rules and limitations

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

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

  The switch will raise an appropriate alarm, if such a speed/duplex mismatch is detected.
- The Spanning Tree Protocol (STP) dynamically calculates the path cost of the LAG based on its aggregated bandwidth. However, if the aggregated ports are running at different speeds, the path cost may not be calculated correctly.
- Enabling STP is the best way for handling link redundancy in switch-to-switch connections composed of more than one physical link. If STP is enabled and increased bandwidth is not required, link aggregation should not be used, as it may lead to a longer fail-over time.

8.3.1.3 Link aggregation and Layer 2 features

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

- If the Spanning Tree Protocol (STP) sets the status of an aggregated port to **Blocking** or **Forwarding**, it does it for the whole LAG.
- If one of the aggregated ports joins or leaves a multicast group (e.g. via IGMP or GMRP), all other ports in the LAG will join or leave too.
- Any port configuration parameter (e.g. VLAN, CoS) change will be automatically applied to all ports in the LAG.
- Configuration/status parameters of the secondary ports will not be shown and their port numbers will be simply listed next to the primary port number in the appropriate configuration/status user interface sessions.
- When a secondary port is added to a LAG, it inherits all the configuration settings of the primary port. When this secondary port is removed from the LAG, the settings it had previous to the aggregation are restored.

8.3.1.4 Link aggregation and physical layer features

Physical layer features (e.g. physical link configuration, link status, rate limiting, Ethernet statistics) will still treat each aggregated port separately.

- Physical configuration/status parameters will NOT be automatically applied to other ports in the Link Aggregation Group (LAG) and will be displayed for each port as usual.
- Make sure only ports with the same speed and duplex settings are aggregated. If auto-negotiation is used, make sure it is resolved to the same speed for all ports in the LAG.
- To get a value of an Ethernet statistics counter for the LAG, add the values of the counters for all ports in the LAG.

8.3.2 Configuring link aggregation

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

1. Disconnect or disable each port to be aggregated. For information about disabling a port, refer to "Configuring an Ethernet port" (Page 67).
2. Create one or more Link Aggregation Groups (LAGs) consisting of two or more ports. For more information, refer to "Adding a link aggregation group" (Page 235).
3. Connect or enable each port in the LAG. For information about enabling a port, refer to "Configuring an Ethernet port" (Page 67).

4. If dynamic link aggregation is required, configure the global and per port LACP settings. For more information, refer to "Configuring global LACP settings" (Page 238) and "Configuring LACP per port" (Page 239).
5. Repeat step 1 (Page 234) to step 4 (Page 235) for a neighboring device that has the same capabilities (i.e. port speed, media type, etc.), making sure to refer to the device's user documentation for details.

8.3.3 Managing link aggregation groups

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

Note

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

Note

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

8.3.3.1 Viewing a list of link aggregation groups

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

If LAGs have not been configured, add LAGs as needed. For more information, refer to "Adding a link aggregation group" (Page 235).

8.3.3.2 Adding a link aggregation group

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

⚠ NOTICE

Configuration hazard – risk of communication disruption

The LAG must be properly configured on both sides of the port channel. In switch-to-switch connections, if the configuration of both sides does not match (i.e. some ports are mistakenly not included in the port trunk), it will result in a loop. Therefore, the following procedure is strongly recommended to configure a LAG:

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

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

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

Note

Make sure only ports with the same speed and duplex settings are aggregated. If auto-negotiation is used, make sure it is resolved to the same speed for all ports in the LAG.

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

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

4. Click **Apply**.

8.3.3.3 Deleting a link aggregation group

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

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

3. Click **Delete**.

8.3.3.4 Viewing the status of link aggregation groups

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

This table displays the following information about each LAG:

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

8.3.4 Managing the link aggregation control protocol

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

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

⚠ NOTICE

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

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

8.3.4.1 Viewing information about the LACP partner

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

This table displays the following information:

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

8.3.4.2 Configuring global LACP settings

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

1. Navigate to ***Link Aggregation » Configure Global LACP Parameters***. The **Global LACP Parameters** form appears.
2. Configure the following parameter(s) as required:

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

3. Click **Apply**.

8.3.4.3 Configuring LACP per port

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

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

Parameter	Description
`Port`	The port number.
`Mode`	**Synopsis:** [Active | Passive] **Default:** Passive Defines the LACP mode for the port. Options include:: • **Active** – The port actively sends LACP packets, regardless of the mode of the partner port. • **Passive** – The port does not send LACP packets unless the partner port is in Active mode.

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

4. Click **Apply**.

8.3.4.4 Viewing LACP statistics

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

This table displays the following information:

Parameter	Description
`Port`	The port number.
`Link`	The link status of the port.

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

8.3.5 Clearing link aggregation statistics

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

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

9 Traffic control and classification

Use the traffic control and classification subsystems to control the flow of data packets to connected network interfaces.

9.1 Managing Classes of Service (CoS)

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

⚠ NOTICE

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

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

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

1. **Inspection phase**
   In the inspection phase, the CoS priority of a received frame is determined from either:
   - A specific CoS based upon the source and destination MAC address (as set in the Static MAC Address Table)
   - The priority field in the IEEE 802.1Q tags
   - The Differentiated Services Code Point (DSCP) component of the Type Of Service (TOS) field in the IP header, if the frame is IP
   - The default CoS for the port

   Each frame's CoS will be determined once the first examined parameter is found in the frame.

   Note

   For information on how to configure the **Inspect TOS** parameter, refer to "Configuring classes of service for specific ethernet ports" (Page 244).

   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.

9.1.1 Configuring classes of service globally

To configure global settings for Classes of Service (CoS), do the following:

1. Navigate to ***Classes of Service » Configure Global CoS Parameters***. The **Global CoS Parameters** form appears.
2. Configure the following parameter(s) as required:

Parameter	Description
`CoS Weighting`	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:

3. Click **Apply**.
4. If necessary, configure CoS mapping based on either the IEEE 802.1p priority or Differentiated Services (DS) field set in the IP header for each packet. For more information, refer to "Configuring priority to CoS mapping" (Page 245) or "Configuring DSCP to CoS mapping" (Page 245).

9.1.2 Configuring classes of service for specific ethernet ports

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

1. Navigate to ***Classes of Service » Configure Port CoS Parameters***. The **Port CoS Parameters** table appears.
2. Select an Ethernet port. The **Port CoS Parameters** form appears.

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

Parameter	Description
`Port(s)`	**Synopsis:** Any combination of numbers valid for this parameter The port number of the device (or a list of ports, if aggregated in a port trunk).
`Inspect TOS`	**Synopsis:** [No | Yes] **Default:** No This parameters enables or disables parsing of the Type-Of-Service (TOS) field in the IP header of the received frames to determine what Class of Service they should be assigned. When TOS parsing is enabled the switch will use the Differentiated Services bits in the TOS field.

4. Click **Apply**.

9.1.3 Configuring priority to CoS mapping

Frames received untagged can be automatically assigned a CoS based on their priority level.

To map a priority level to a CoS, do the following:

1. Navigate to ***Classes of Service » Configure Priority to CoS Mapping***. The **Priority to CoS Mapping** table appears.
2. Select a priority level. The **Priority to CoS Mapping** form appears.
3. Configure the following parameter(s) as required:

Parameter	Description
`Priority`	**Synopsis:** An integer between 0 and 7 **Default:** 0 Value of the IEEE 802.1p priority.
`CoS`	**Default:** Normal CoS assigned to received tagged frames with the specified IEEE 802.1p priority value.

4. Click **Apply**.

9.1.4 Configuring DSCP to CoS mapping

Mapping CoS to the Differentiated Services (DS) field set in the IP header for each packet is done by defining Differentiated Services Code Points (DSCPs) in the CoS configuration.

To map a DSCP to a Class of Service, do the following:

1. Navigate to ***Classes of Service » Configure DSCP to CoS Mapping***. The **DSCP to CoS Mapping** table appears.
2. Select a DSCP level. The **DSCP to CoS Mapping** form appears.
3. Configure the following parameter(s) as required:

Parameter	Description
DSCP	**Synopsis:** An integer between 0 and 63 **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.

4. Click **Apply**.
5. Configure the CoS parameters on select switched Ethernet ports as needed. For more information, refer to "Configuring classes of service for specific ethernet ports" (Page 244).

10 Time services

This chapter describes the time-keeping and time synchronization features in RUGGEDCOM ROS.

10.1 Configuring the time and date

To set the time, date and other time-keeping related parameters, do the following:

1. Navigate to ***Administration » System Time Manager » Configure Time and Date***. The **Time and Date** form appears.
2. Configure the following parameter(s) as required:

Parameter	Description
`Time`	**Synopsis:** HH:MM:SS 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) 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.

Parameter	Description
`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.

10.2 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.

10.2.1 Enabling/disabling NTP service

To enable or disable NTP Service, do the following:

Note

If the device is running as an NTP server, NTP service must be enabled.

1. Navigate to ***Administration » System Time Manager » Configure NTP » Configure NTP Service***. The **SNTP Parameters** form appears.
2. Select **Enabled** to enable SNTP, or select **Disabled** to disable SNTP.
3. Click **Apply**.

10.2.2 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.
2. Select either **Primary** or **Backup**. The **NTP Servers** form appears.
3. Configure the following parameter(s) as required:

Parameter	Description
`Server`	**Synopsis:** A string up to 8 characters long **Default:** Primary This field tells whether this configuration is for a Primary or a Backup Server.
`IP Address`	**Synopsis:** Any valid IP address The Server IP Address.
`Reachable`	**Synopsis:** [--- | Yes | No] The status of the server. Options include: • **---** – The server status is unknown • **Yes** – The server is reachable • **No** – The server is unreachable
`Probe Period`	**Synopsis:** An integer between 1 and 1440 **Default:** 5 Determines how frequently in minutes the (S)NTP server is polled for reachability when the Probe Method is ICMP.
`Probe Method`	**Synopsis:** [ICMP | SNTP Message] **Default:** SNTP Message Determines the protocol used to probe (S)NTP server reachability. Options include: • **ICMP** – Server probe uses ICMP ping. Three consecutive ICMP ping requests with a 500-millisecond timeout are sent to the server until a response is received. If no response received, a server unreachable alarm is generated. • **SNTP Message** – Server reachability status relies on the server's response to SNTP messages sent during periodic time synchronization per the 'Update Period' interval. If no response received, a server unreachable alarm is generated.
`Update Period`	**Synopsis:** An integer between 1 and 1440 **Default:** 60 Determines how frequently the (S)NTP server is polled for a time update.If the server cannot be reached in three attempts that are made at one minute intervals an alarm is generated.

4. Click **Apply**.

11 Network discovery and management

RUGGEDCOM ROS supports the following protocols for automatic network discovery, monitoring and device management:

- **RUGGEDCOM Discovery Protocol (RCDP)**
  Use RCDP to discover RUGGEDCOM ROS-based devices over a Layer 2 network.
- **Link Layer Device Protocol (LLDP)**
  Use LLDP to broadcast the device's network capabilities and configuration to other devices on the network, as well as receive broadcasts from other devices.
- **Simple Network Management Protocol (SNMP)**
  Use SNMP to notify select users or groups of certain events that happen during the operation of the device, such as changes to network topology, link state, spanning tree root, etc.

11.1 Enabling/disabling RCDP

RUGGEDCOM ROS supports the RUGGEDCOM Discovery Protocol (RCDP). RCDP supports the deployment of RUGGEDCOM ROS-based devices that have not been configured since leaving the factory. RUGGEDCOM ROS devices that have not been configured all have the default IP (Layer 3) address. Connecting more than one of them on a Layer 2 network means that one cannot use standard IP-based configuration tools to configure them. The behavior of IP-based mechanisms such as the web interface, SSH, telnet, or SNMP will all be undefined.

Since RCDP operates at Layer 2, it can be used to reliably and unambiguously address multiple devices even though they may share the same IP configuration.

Siemens' RUGGEDCOM SINEC PNI ia a lightweight, standalone Windows application that support 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.
- Firmware updates.

Note

For more information about using SINEC PNI, refer to the "SINEC PNI Operating Instructions".

RUGGEDCOM ROS will set all devices to *Get Only* mode in the following conditions:

- 60 minutes after the last RCDP frame has been received.
- The IP address, subnet, gateway or any passwords are changed for the device via SSH, RSH, Telnet, serial console or SNMP.

⚠ NOTICE

For increased security, Siemens recommends disabling RCDP if it is not intended for use.

Note

RUGGEDCOM ROS responds to RCDP requests only. It does not under any circumstances initiate any RCDP-based communication.

To enable or disable RCDP, do the following:

1. Navigate to ***Network Discovery » RuggedCom Discovery Protocol » Configure RCDP Parameters***. The **RCDP Parameters** form appears.
2. Under **RCDP Discovery**, select one of the following options:

   ⚠ NOTICE

   The **Enabled** option is only available for devices loaded with factory default settings. This option will not be selectable once a device has been configured.

   - **Disabled** – Disables read and write access
   - **Get Only** – Enables only read access
   - **Enabled** – Enables read and write access
3. Click **Apply**.

11.2 Managing LLDP

The Link Layer Discovery Protocol (LLDP) defined by IEEE 802.11AB allows a networked device to advertise its own basic networking capabilities and configuration.

LLDP allows a networked device to discover its neighbors across connected network links using a standard mechanism. Devices that support LLDP are able to advertise information about themselves, including their capabilities, configuration, interconnections, and identifying information.

LLDP agent operation is typically implemented as two modules: the LLDP transmit module and LLDP receive module. The LLDP transmit module, when enabled, sends

the local device's information at regular intervals, in IEEE 802.1AB standard format. Whenever the transmit module is disabled, it transmits an LLDPDU (LLDP data unit) with a time-to-live (TTL) type-length-value (TLV) containing 0 in the information field. This enables remote devices to remove the information associated with the local device in their databases. The LLDP receive module, when enabled, receives remote devices' information and updates its LLDP database of remote systems. When new or updated information is received, the receive module initiates a timer for the valid duration indicated by the TTL TLV in the received LLDPDU. A remote system's information is removed from the database when an LLDPDU is received from it with TTL TLV containing 0 in its information field.

Note

LLDP is implemented to keep a record of only one device per Ethernet port. Therefore, if there are multiple devices sending LLDP information to a switch port on which LLDP is enabled, information about the neighbor on that port will change constantly.

11.2.1 Configuring LLDP globally

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

1. Navigate to ***Network Discovery » Link Layer Discovery Protocol » Configure Global LLDP Parameters***. The **Global LLDP Parameters** form appears.
2. Configure the following parameter(s) as required:

Parameter	Description
`State`	**Synopsis:** [Disabled | Enabled] **Default:** Enabled Enables LLDP protocol. Note that LLDP is enabled on a port when LLDP is enabled globally and along with enabling per port setting in Port LLDP Parameters menu.
`Tx Interval`	**Synopsis:** An integer between 5 and 32768 **Default:** 30 The interval at which LLDP frames are transmitted on behalf of this LLDP agent.
`Tx Hold`	**Synopsis:** An integer between 2 and 10 **Default:** 4 The multiplier of the Tx Interval parameter that determines the actual time-to-live (TTL) value used in a LLDPDU. The actual TTL value can be expressed by the following formula: `TTL = MIN(65535, (Tx Interval * Tx Hold)`

Parameter	Description
`Reinit Delay`	**Synopsis:** An integer between 1 and 10 **Default:** 2 The delay in seconds from when the value of Admin Status parameter of a particular port becomes 'Disbled' until re-initialization will be attempted.
`Tx Delay`	**Synopsis:** An integer between 1 and 8192 **Default:** 2 The delay in seconds between successive LLDP frame transmissions initiated by value or status changed. The recommended value is set by the following formula: `1 <= txDelay <= (0.25 * Tx Interval)`

3. Click **Apply**.

11.2.2 Configuring LLDP for an Ethernet port

To configure LLDP for a specific Ethernet Port, do the following:

1. Navigate to ***Network Discovery » Link Layer Discovery Protocol » Configure Port LLDP Parameters***. The **Port LLDP Parameters** table appears.
2. Select a port. The **Port LLDP Parameters** form appears.
3. Configure the following parameter(s) as required:

Parameter	Description
`Port`	The port number.
`Admin Status`	**Synopsis:** [rxTx | txOnly | rxOnly | Disabled] **Default:** rxTx rxTx: the local LLDP agent can both transmit and receive LLDP frames through the port. txOnly: the local LLDP agent can only transmit LLDP frames. rxOnly: the local LLDP agent can only receive LLDP frames. disabled: the local LLDP agent can neither transmit or receive LLDP frames.
`Notifications`	**Synopsis:** [Disabled | Enabled] **Default:** Disabled Disabling notifications will prevent sending notifications and generating alarms for particular port from the LLDP agent.

4. Click **Apply**.

11.2.3 Viewing global statistics and advertised system information

To view global statistics for LLDP and the system information that is advertised to neighbors, navigate to ***Network Discovery » Link Layer Discovery Protocol » View LLDP Global Remote Statistics***. The **LLDP Global Remote Statistics** form appears.

This form displays the following information:

Parameter	Description
`Inserts`	**Synopsis:** An integer between 0 and 4294967295 A number of times the entry in LLDP Neighbor Information Table was inserted.
`Deletes`	**Synopsis:** An integer between 0 and 4294967295 A number of times the entry in LLDP Neighbor Information Table was deleted.
`Drops`	**Synopsis:** An integer between 0 and 4294967295 A number of times an entry was deleted from LLDP Neighbor Information Table because the information timeliness interval has expired.
`Ageouts`	**Synopsis:** An integer between 0 and 4294967295 A counter of all TLVs discarded.

11.2.4 Viewing statistics for LLDP neighbors

To view statistics for LLDP neighbors, navigate to ***Network Discovery » Link Layer Discovery Protocol » View LLDP Neighbor Information***. The **LLDP Neighbor Information** table appears.

This form displays the following information:

Parameter	Description
`Port`	The local port associated with this entry.
`ChassisId`	**Synopsis:** A string up to 45 characters long Chassis Id information received from remote LLDP agent.
`PortId`	**Synopsis:** A string up to 45 characters long Port Id information received from remote LLDP agent.
`SysName`	**Synopsis:** A string up to 45 characters long System Name information received from remote LLDP agent.
`SysDesc`	**Synopsis:** A string up to 45 characters long System Descriptor information received from remote LLDP agent.

11.2.5 Viewing statistics for LLDP ports

To view statistics for LLDP ports, navigate to ***Network Discovery » Link Layer Discovery Protocol » View LLDP Statistics***. The **LLDP Statistics** table appears.

This table displays the following information:

Parameter	Description
`Port`	The port number.
`FrmDrop`	**Synopsis:** An integer between 0 and 4294967295 A counter of all LLDP frames discarded.
`ErrFrm`	**Synopsis:** An integer between 0 and 4294967295 A counter of all LLDPDUs received with detectable errors.
`FrmIn`	**Synopsis:** An integer between 0 and 4294967295 A counter of all LLDPDUs received.
`FrmOut`	**Synopsis:** An integer between 0 and 4294967295 A counter of all LLDPDUs transmitted.
`Ageouts`	**Synopsis:** An integer between 0 and 4294967295 A counter of the times that a neighbor's information has been deleted from the LLDP remote system MIB because the txinfoTTL timer has expired.
`TLVsDrop`	**Synopsis:** An integer between 0 and 4294967295 A counter of all TLVs discarded.
`TLVsUnknown`	**Synopsis:** An integer between 0 and 4294967295 A counter of all TLVs received on the port that are not recognized by the LLDP local agent.

11.3 Managing SNMP

RUGGEDCOM ROS supports versions 1, 2 and 3 of the Simple Network Management Protocol (SNMP), otherwise referred to as SNMPv1, SNMPv2c and SNMPv3 respectively. SNMPv3 provides secure access to the devices through a combination of authentication and packet encryption over the network. Security features for this protocol include:

Feature	Description
Message Integrity	Makes sure that a packet has not been tampered with in-transit.
Authentication	Determines if the message is from a valid source.
Encryption	Encrypts the contents of a packet to prevent it from being seen by an unauthorized source.

SNMPv3 provides security models and security levels. A security model is an authentication strategy setup for a user and the group in which the user resides. A

security level is a permitted level of security within a security model. A combination of a security model and level will determine which security mechanism is employed when handling an SNMP packet.

Before configuring SNMPv3, note the following:

- Each user belongs to a group
- A group defines the access policy for a set of users
- An access policy defines what SNMP objects can be accessed for (i.e. reading, writing and creating notifications)
- A group determines the list of notifications its users can receive
- A group also defines the security model and security level for its users

For SNMPv1 and SNMPv2c, a community string can be configured. The string is mapped to the group and access level with a security name, which is configured as **User Name**.

SNMP Management Interface Base (MIB) support

RUGGEDCOM ROS supports a variety of standard MIBs, proprietary RUGGEDCOM MIBs, Agent Capabilities MIBs and traps, all for SNMP (Simple Network Management Protocol).

For more information about supported MIBs, agent capabilities and traps, refer to "Reference" (Page 291).

11.3.1 Improving SNMP performance

Follow the recommendations below to improve the SNMP response time and manage the CPU load:

- **Limit the number of SNMP managers**
  A network device that is being queried by multiple SNMP managers or SNMP monitoring tools simultaneously can lead to high CPU utilization and delayed SNMP responses. To mitigate the risk of sustained high CPU load, avoid having more than one NMS server actively polling the device.
- **Limit the SNMP queries**
  Limit the scope of SNMP queries to only the MIB tables and the OIDs required to be monitored, as per the requirements of a network. Only polling the essential OIDs and MIB tables frees the CPU to perform more critical tasks, rather than responding to SNMP queries.
- **Stagger the SNMP queries**
  Instead of sending all queries at once, which can lead to high CPU load, stagger the SNMP queries to poll different MIB tables and the OIDs at different intervals.
- **Optimize the polling interval, retry, and timeout values**
  Adjust the SNMP polling intervals according to the needs of your network. Short polling intervals (e.g. 3 to 5 minutes) can be used for the OID set that are critical

for the operation of a network device. Whereas, longer polling intervals (e.g. 30 to 60 minutes) can be used for the OID set that are considered non-critical.

Using longer timeout values (e.g. 4 to 5 seconds) and setting the retry count to two or more also allows a network node to reply to a query even under sustained CPU load.

- **Adjust the maximum repetition for the SNMP GetBulk request**
  Setting the maximum repetition for the SNMP GetBulk request too low or too high in a SNMP manager (i.e. NMS) can lead to high CPU utilization. The maximum repetition value can be adjusted to allow for a more effective SNMP response from the device.
- **Use SNMP traps**
  Configure SNMP traps to get spontaneous notifications about the status of a network node. This can help network administrators respond quickly to events.

11.3.2 Managing SNMP users

This section describes how to manage SNMP users.

11.3.2.1 Viewing a list of SNMP users

To view a list of SNMP users configured on the device, navigate to ***Administration » Configure SNMP » Configure SNMP Users***. The **SNMP Users** table appears.

If users have not been configured, add users as needed. For more information, refer to "Adding an SNMP user" (Page 258).

11.3.2.2 Adding an SNMP user

Multiple users (up to a maximum of 32) can be configured for the local SNMPv3 engine, as well as SNMPv1 and SNMPv2c communities.

Note

When employing the SNMPv1 or SNMPv2c security level, the **User Name** parameter maps the community name with the security group and access level.

For CLI commands related to adding an SNMP user, refer to "Available CLI commands" (Page 24).

To add a new SNMP user, do the following:

1. Navigate to ***Administration » Configure SNMP » Configure SNMP Users***. The **SNMP Users Table** appears.
2. Click **InsertRecord**. The **SNMP Users** form appears.

Note

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

- Must not be less than 6 characters in length.
- Must not include the username or any 4 continuous alphanumeric characters found in the username. For example, if the username is *Subnet25*, the password may not be *subnet25admin* or *subnetadmin*. However, *net25admin* or *Sub25admin* is permitted.
- Must have at least one alphabetic character and one number. Special characters are permitted.
- Must not have more than 3 continuously incrementing or decrementing numbers. For example, *Sub123* and *Sub19826* are permitted, but *Sub12345* is not.

An alarm will generate if a weak password is configured. The weak password alarm can be disabled by the user. For more information about disabling alarms, refer to "Managing alarms" (Page 110).

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

Parameter	Description
`Name`	**Synopsis:** A string up to 32 characters long **Default:** initial The name of the user. This user name also represents the security name that maps this user to the security group.
`IP Address`	**Synopsis:** Any valid IP address The IP address of the user's SNMP management station. If IP address is configured, SNMP requests from that user will be verified by IP address as well. SNMP Authentication trap will be generated to trap receivers if request was received from this user, but from any other IP address.If IP address is empty, traps can not be generated to this user, but SNMP requests will be served for this user from any IP address.
`v1/v2c Community`	**Synopsis:** A string up to 32 characters long The community string which is mapped by this user/security name to the security group if security model is SNMPv1 or SNMPv2c. If this string is left empty, it will be assumed to be equal to the same as user name.

Parameter	Description
`Auth Protocol`	**Synopsis:** [noAuth | HMACMD5 | HMACSHA | HMACSHA256] **Default:** HMACSHA256 **⚠ NOTICE** For increased security, Siemens recommends using HMACSHA256. 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 | AES-128 | AES-192 | AES-256] **Default:** AES-256 **Note** For the SNMPv3 USM private protocols AES-192 and AES-256, RUGGEDCOM ROS supports the Blumenthal AES algorithm. **⚠ NOTICE** For increased security, Siemens recommends using AES-256. An Indication of whether messages sent on behalf of this user to/from SNMP engine can be protected from disclosure, and if so, the type of privacy protocol which is used.
`Auth Key`	**Synopsis:** A string up to 31 characters long The secret authentication key (password) that must be shared with SNMP client. If the key is not an emtpy string, it must be at least 6 characters long.
`Confirm Auth Key`	**Synopsis:** A string up to 31 characters long The secret authentication key (password) that must be shared with SNMP client. If the key is not an emtpy string, it must be at least 6 characters long.
`Priv Key`	**Synopsis:** A string up to 31 characters long The secret encription key (password) that must be shared with SNMP client. If the key is not an emtpy string, it must be at least 6 characters long.
`Confirm Priv Key`	**Synopsis:** A string up to 31 characters long The secret encription key (password) that must be shared with SNMP client. If the key is not an emtpy string, it must be at least 6 characters long.

4. Click **Apply**.

11.3.2.3 Deleting an SNMP user

For CLI commands related to deleting an SNMP user, refer to "Available CLI commands" (Page 24).

To delete an SNMP user, do the following:

1. Navigate to ***Administration » Configure SNMP » Configure SNMP Users***. The **SNMP Users Table** appears.
2. Select the user from the table. The **SNMP Users** form appears.
3. Click **Delete**.

11.3.3 Managing security-to-group mapping

This section describes how to configure and manage security-to-group maps.

11.3.3.1 VIewing a list of security-to-group maps

To view a list of security-to-group maps configured on the device, navigate to ***Administration » Configure SNMP » Configure SNMP Security to Group Maps***. The **SNMP Security to Group Maps** table appears.

If security-to-group maps have not been configured, add maps as needed. For more information, refer to "Adding a security-to-group map" (Page 261).

11.3.3.2 Adding a security-to-group map

Multiple combinations of security models and groups can be mapped (up to a maximum of 32) for SNMP.

For CLI commands related to adding an SNMP security-to-group map, refer to "Available CLI commands" (Page 24).

To add a security-to-group map, do the following:

1. Navigate to ***Administration » Configure SNMP » Configure SNMP Security to Group Maps***. The **SNMP Security to Group Maps Table** appears.
2. Click **InsertRecord**. The **SNMP Security to Group Maps** form appears.
3. Configure the following parameter(s) as required:

Parameter	Description
`SecurityModel`	**Synopsis:** [snmpV1 | snmpV2c | snmpV3] **Default:** snmpV3 The Security Model that provides the name referenced in this table.

Parameter	Description
`Name`	**Synopsis:** A string up to 32 characters long The user name which is mapped by this entry to the specified group name.
`Group`	**Synopsis:** A string up to 32 characters long The group name to which the security model and name belong. This name is used as an index to the SNMPv3 VACM Access Table.

4. Click **Apply**.

11.3.3.3 Deleting a security-to-group map

For CLI commands related to deleting an SNMP security-to-group map, refer to "Available CLI commands" (Page 24).

To delete a security-to-group map, do the following:

1. Navigate to ***Administration » Configure SNMP » Configure SNMP Security to Group Maps***. The **SNMP Security to Group Maps Table** appears.
2. Select the map from the table. The **SNMP Security to Group Maps** form appears.
3. Click **Delete**.

11.3.4 Managing SNMP groups

Multiple SNMP groups (up to a maximum of 32) can be configured to have access to SNMP.

11.3.4.1 Viewing a list of SNMP groups

To view a list of SNMP groups configured on the device, navigate to ***Administration » Configure SNMP » Configure SNMP Access***. The **SNMP Access** table appears.

If SNMP groups have not been configured, add groups as needed. For more information, refer to "Adding an SNMP group" (Page 262).

11.3.4.2 Adding an SNMP group

For CLI commands related to adding an SNMP group, refer to "Available CLI commands" (Page 24).

To add an SNMP group, do the following:

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

Parameter	Description
`Group`	**Synopsis:** A string up to 32 characters long The group name to which the security model and name belong. This name is used as an index to the SNMPv3 VACM Access Table.
`SecurityModel`	**Synopsis:** [snmpV1 | snmpV2c | snmpV3] **Default:** snmpV3 In order to gain the access rights allowed by this entry, configured security model must be in use.
`SecurityLevel`	**Synopsis:** [noAuthNoPriv | authNoPriv | authPriv] **Default:** authPriv The SNMP security level. Options include: • **authPriv** – Communication with authentication and privacy • **authNoPriv** – Communication with authentication and without privacy • **noAuthnoPriv** – Communication without authentication and privacy
`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**.

11.3.4.3 Deleting an SNMP group

For CLI commands related to deleting an SNMP group, refer to "Available CLI commands" (Page 24).

To delete an SNMP group, do the following:

1. Navigate to ***Administration » Configure SNMP » Configure SNMP Access***. The **SNMP Access Table** appears.
2. Select the group from the table. The **SNMP Access** form appears.
3. Click **Delete**.

11.4 ModBus management support

Modbus management support in RUGGEDCOM devices provides a simple interface for retrieving basic status information. ModBus support simplifies the job of SCADA (Supervisory Control and Data Acquisition) system integrators by providing familiar protocols for retrieving RUGGEDCOM device information. ModBus provides mostly read-only status information, but there are some writeable registers for operator commands.

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

Function Code	Data

11.4.1 ModBus function codes

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

Note

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

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

Read input registers or read holding registers – 0x04 or 0x03

Example PDU request

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

Example PDU Response

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

[a] The number of input registers

Write multiple registers – 0x10

Example PDU request

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

[a] The number of input registers

Example PDU Response

Function Code	1 Byte	0x10
Starting Address	2 Bytes	0x0000 to 0xFFFF
Number of Registers	2 Bytes	1 to 121 (0x79)

11.4.2 ModBus memory map

The following details how ModBus process variable data is mapped.

Note

Address values are in hexadecimal format.

Product info

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

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

Product write register

The following data is mapped to various tables:

Address	#Registers	Description (reference table in UI)	R/W	Format
0080	1	Clear Alarms	W	Cmd
0081	2	Reset Ethernet Ports	W	PortCmd
0083	2	Clear Ethernet Statistics	W	PortCmd
0085	2	Reset Serial Ports	W	PortCmd
0087	2	Clear Serial Port Statistics	W	PortCmd

Alarms

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

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

Ethernet port status

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

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

Ethernet Statistics

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

Address	#Registers	Description (reference table in UI)	R/W	Format
0400	2	Port 1 Statistics - Ethernet In Packets	R	Uint32
0402	2	Port 2 Statistics - Ethernet In Packets	R	Uint32
0404	2	Port 3 Statistics - Ethernet In Packets	R	Uint32
0406	2	Port 4 Statistics - Ethernet In Packets	R	Uint32
0408	2	Port 5 Statistics - Ethernet In Packets	R	Uint32
040A	2	Port 6 Statistics - Ethernet In Packets	R	Uint32
040C	2	Port 7 Statistics - Ethernet In Packets	R	Uint32
040E	2	Port 8 Statistics - Ethernet In Packets	R	Uint32
0410	2	Port 9 Statistics - Ethernet In Packets	R	Uint32

Address	#Registers	Description (reference table in UI)	R/W	Format
0412	2	Port 10 Statistics - Ethernet In Packets	R	Uint32
0414	2	Port 11 Statistics - Ethernet In Packets	R	Uint32
0416	2	Port 12 Statistics - Ethernet In Packets	R	Uint32
0418	2	Port 13 Statistics - Ethernet In Packets	R	Uint32
041A	2	Port 14 Statistics - Ethernet In Packets	R	Uint32
041C	2	Port 15 Statistics - Ethernet In Packets	R	Uint32
041E	2	Port 16 Statistics - Ethernet In Packets	R	Uint32
0420	2	Port 17 Statistics - Ethernet In Packets	R	Uint32
0422	2	Port 18 Statistics - Ethernet In Packets	R	Uint32
0424	2	Port 19 Statistics - Ethernet In Packets	R	Uint32
0426	2	Port 20 Statistics - Ethernet In Packets	R	Uint32
0440	2	Port 1 Statistics - Ethernet Out Packets	R	Uint32
0442	2	Port 2 Statistics - Ethernet Out Packets	R	Uint32
0444	2	Port 3 Statistics - Ethernet Out Packets	R	Uint32
0446	2	Port 4 Statistics - Ethernet Out Packets	R	Uint32
0448	2	Port 5 Statistics - Ethernet Out Packets	R	Uint32
044A	2	Port 6 Statistics - Ethernet Out Packets	R	Uint32
044C	2	Port 7 Statistics - Ethernet Out Packets	R	Uint32
044E	2	Port 8 Statistics - Ethernet Out Packets	R	Uint32
0450	2	Port 9 Statistics - Ethernet Out Packets	R	Uint32
0452	2	Port 10 Statistics - Ethernet Out Packets	R	Uint32
0454	2	Port 11 Statistics - Ethernet Out Packets	R	Uint32
0456	2	Port 12 Statistics - Ethernet Out Packets	R	Uint32
0458	2	Port 13 Statistics - Ethernet Out Packets	R	Uint32

Address	#Registers	Description (reference table in UI)	R/W	Format
045A	2	Port 14 Statistics - Ethernet Out Packets	R	Uint32
045C	2	Port 15 Statistics - Ethernet Out Packets	R	Uint32
045E	2	Port 16 Statistics - Ethernet Out Packets	R	Uint32
0460	2	Port 17 Statistics - Ethernet Out Packets	R	Uint32
0462	2	Port 18 Statistics - Ethernet Out Packets	R	Uint32
0464	2	Port 19 Statistics - Ethernet Out Packets	R	Uint32
0466	2	Port 20 Statistics - Ethernet Out Packets	R	Uint32
0480	2	Port 1 Statistics - Ethernet In Octets	R	Uint32
0482	2	Port 2 Statistics - Ethernet In Octets	R	Uint32
0484	2	Port 3 Statistics - Ethernet In Octets	R	Uint32
0486	2	Port 4 Statistics - Ethernet In Octets	R	Uint32
0488	2	Port 5 Statistics - Ethernet In Octets	R	Uint32
048A	2	Port 6 Statistics - Ethernet In Octets	R	Uint32
048C	2	Port 7 Statistics - Ethernet In Octets	R	Uint32
048E	2	Port 8 Statistics - Ethernet In Octets	R	Uint32
0490	2	Port 9 Statistics - Ethernet In Octets	R	Uint32
0492	2	Port 10 Statistics - Ethernet In Octets	R	Uint32
0494	2	Port 11 Statistics - Ethernet In Octets	R	Uint32
0496	2	Port 12 Statistics - Ethernet In Octets	R	Uint32
0498	2	Port 13 Statistics - Ethernet In Octets	R	Uint32
049A	2	Port 14 Statistics - Ethernet In Octets	R	Uint32
049C	2	Port 15 Statistics - Ethernet In Octets	R	Uint32
049E	2	Port 16 Statistics - Ethernet In Octets	R	Uint32
04A0	2	Port 17 Statistics - Ethernet In Octets	R	Uint32
04A2	2	Port 18 Statistics - Ethernet In Octets	R	Uint32
04A4	2	Port 19 Statistics - Ethernet In Octets	R	Uint32
04A6	2	Port 20 Statistics - Ethernet In Octets	R	Uint32
04C0	2	Port 1 Statistics - Ethernet Out Octets	R	Uint32
04C2	2	Port 2 Statistics - Ethernet Out Octets	R	Uint32
04C4	2	Port 3 Statistics - Ethernet Out Octets	R	Uint32
04C6	2	Port 4 Statistics - Ethernet Out Octets	R	Uint32
04C8	2	Port 5 Statistics - Ethernet Out Octets	R	Uint32

Address	#Registers	Description (reference table in UI)	R/W	Format
04CA	2	Port 6 Statistics - Ethernet Out Octets	R	Uint32
04CC	2	Port 7 Statistics - Ethernet Out Octets	R	Uint32
04CE	2	Port 8 Statistics - Ethernet Out Octets	R	Uint32
04D0	2	Port 9 Statistics - Ethernet Out Octets	R	Uint32
04D2	2	Port 10 Statistics - Ethernet Out Octets	R	Uint32
04D4	2	Port 11 Statistics - Ethernet Out Octets	R	Uint32
04D6	2	Port 12 Statistics - Ethernet Out Octets	R	Uint32
04D8	2	Port 13 Statistics - Ethernet Out Octets	R	Uint32
04DA	2	Port 14 Statistics - Ethernet Out Octets	R	Uint32
04DC	2	Port 15 Statistics - Ethernet Out Octets	R	Uint32
04DE	2	Port 16 Statistics - Ethernet Out Octets	R	Uint32
04E0	2	Port 17 Statistics - Ethernet Out Octets	R	Uint32
04E2	2	Port 18 Statistics - Ethernet Out Octets	R	Uint32
04E4	2	Port 19 Statistics - Ethernet Out Octets	R	Uint32
04E6	2	Port 20 Statistics - Ethernet Out Octets	R	Uint32

Serial Statistics

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

Address	#Registers	Description (reference table in UI)	R/W	Format
0600	2	Port 1 Statistics – Serial In characters	R	Uint32
0602	2	Port 2 Statistics – Serial In characters	R	Uint32
0604	2	Port 3 Statistics – Serial In characters	R	Uint32
0606	2	Port 4 Statistics – Serial In characters	R	Uint32
0640	2	Port 1 Statistics – Serial Out characters	R	Uint32
0642	2	Port 2 Statistics – Serial Out characters	R	Uint32
0644	2	Port 3 Statistics – Serial Out characters	R	Uint32
0646	2	Port 4 Statistics – Serial Out characters	R	Uint32
0680	2	Port 1 Statistics – Serial In Packets	R	Uint32
0682	2	Port 2 Statistics – Serial In Packets	R	Uint32
0684	2	Port 3 Statistics – Serial In Packets	R	Uint32

Address	#Registers	Description (reference table in UI)	R/W	Format
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

11.4.3 Modbus memory formats

This section defines the Modbus memory formats supported by RUGGEDCOM ROS.

11.4.3.1 Text

The Text format provides a simple ASCII representation of the information related to the product. The most significant register byte of an ASCII characters comes first.

For example, consider a *Read Multiple Registers* request to read Product Identification from location 0x0000.

10x04	10x00	10x00	10x00	10x08

The response may look like:

10x04	10x10	10x53	10x59	10x53	10x54	10x45	10x4D	10x20	10x4e	10x41	10x4D	10x45
10x00	10x00	10x00	10x00	10x00								

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).

11.4.3.2 Cmd

The Cmd format instructs the device to set the output to either *true* or *false*. The most significant byte comes first.

- FF 00 hex requests output to be True
- 00 00 hex requests output to be False
- Any value other than the suggested values does not affect the requested operation

For example, consider a *Write Multiple Registers* request to clear alarms in the device.

10x10	10x00	10x80	10x00	10x01	2	10xFF	10x00

- FF 00 for register 00 80 clears the system alarms
- 00 00 does not clear any alarms

The response may look like:

10x10	10x00	10x80	10x00	10x01

11.4.3.3 Uint16

The Uint16 format describes a Standard ModBus 16 bit register.

11.4.3.4 Uint32

The Uint32 format describes Standard 2 ModBus 16 bit registers. The first register holds the most significant 16 bits of a 32 bit value. The second register holds the least significant 16 bits of a 32 bit value.

11.4.3.5 PortCmd

The PortCmd format describes a bit layout per port, where 1 indicates the requested action is true, and 0 indicates the requested action is false.

PortCmd provides a bit layout of a maximum of 32 ports. Therefore, it uses two ModBus regsiters:

- The first ModBus register corresponds to ports 1 – 16
- The second ModBus register corresponds to ports 17 – 32 for a particular action

Bits that do not apply to a particular product are always set to zero (0).

A bit value of 1 indicates that the requested action is true. For example, the port is *up*.

A bit value of 0 indicates that the requested action is false. For example, the port is *down*.

Reading data using PortCmd

To understand how to read data using PortCmd, consider a ModBus Request to read multiple registers from location 0x03FE.

0x04	0x03	0xFE	0x00	0x02

The response depends on how many ports are available on the device. For example, if the maximum number of ports on a connected RUGGEDCOM device is 20, the response would be similar to the following:

0x04	0x04	0xF2	0x76	0x00	0x05

In this example, bytes 3 and 4 refer to register 1 at location 0x03FE, and represent the status of ports 1 – 16. Bytes 5 and 6 refer to register 2 at location 0x03FF, and represent the status of ports 17 – 32. The device only has 20 ports, so byte 6

contains the status for ports 17 – 20 starting from right to left. The rest of the bites in register 2 corresponding to the non-existing ports 21 – 31 are zero (0).

Performing write actions using PortCmd

To understand how data is written using PortCmd, consider a Write Multiple Register request to clear Ethernet port statistics:

0x10	0x00	0x83	0x00	0x01	2	0x55	0x76	0x00	0x50

A bit value of 1 clears Ethernet statistics on the corresponding port. A bit value of 0 does not clear the Ethernet statistics.

0x10	0x00	0x81	0x00	0x02

11.4.3.6 Alarm

The Alarm format is another form of text description. Alarm text corresponds to the alarm description from the table holding all of the alarms. Similar to the Text format, this format returns an ASCII representation of alarms.

Note

Alarms are stacked in the device in the sequence of their occurrence (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.

11.4.3.7 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, consider a ModBus request to read multiple 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.

12 IP address assignment

This chapter describes features related to the assignment of IP addresses.

12.1 Managing DHCP

Dynamic Host Configuration Protocol (DHCP) is a communications protocol that allows network administrators to centrally manage and automate the network configuration of devices attached to an Internet Protocol (IP) network.

12.1.1 DHCP concepts

The following section describes concepts important to the configuration and application of DHCP.

12.1.1.1 DHCP snooping

DHCP snooping is a network security feature that protects the network from untrusted DHCP servers and untrusted clients by keeping track of ports where DHCP clients and servers reside. This information is tracked by building a DHCP binding table that contains all MAC-IP associations the switch has learned by snooping client and server DHCP communications. The binding table contains MAC-IP information which can be further utilized by DHCP snooping applications. RUGGEDCOM ROS will log messages in the syslog and/or raise an alarm when DHCP violations are detected.

Note

DHCP Snooping is enabled on the device on a per-VLAN basis. For more information about enabling DHCP snooping on individual VLANs, refer to "Managing static VLANs" (Page 170).

12.1.1.2 Trusted and untrusted ports

DHCP Snooping classifies ports as trusted and untrusted. This port classification determines how a DHCP message is handled by the switch. DHCP messages received on trusted ports are forwarded without any further checking, while messages received from untrusted ports are verified to determine if the message is legitimate. The user is expected to configure the ports as trusted or untrusted.

From a deployment perspective, it is also expected the user configures network ports as trusted. Network ports typically connect to another switch or a router. This is necessary because a DHCP server may not be directly connected to a switch port.

For more information about configuring ports as trusted or untrusted, refer to "Configuring trusted/untrusted ports" (Page 280).

12.1.1.3 DHCP relay agent (Option 82)

A DHCP Relay Agent is a device that forwards DHCP packets between clients and servers when they are not on the same physical LAN segment or IP subnet. The feature is enabled if the DHCP server IP address and a set of ethernet ports are configured.

DHCP Option 82 provides a mechanism for assigning an IP Address based on the location of the client device in the network. Information about the client's location can be sent along with the DHCP request to the server. Based on this information, the DHCP server makes a decision about an IP Address to be assigned.

The DHCP Relay Agent takes the broadcast DHCP requests from clients received on the configured port and inserts the relay agent information option (Option 82) into the packet. Option 82 contains the VLAN ID (2 bytes) and the port number of the client port (2 bytes: the circuit ID sub-option) and the relay agent's MAC address (the remote ID sub-option). This information uniquely defines the client's position in the network.

For example, the Circuit ID for a client which is connected to VLAN 1 on port 1 is `00:01:00:01`.

The DHCP Server supporting DHCP Option 82 sends a unicast reply and echoes Option 82. The DHCP Relay Agent removes the Option 82 field and forwards the packet to the port from which the original request was received.

These parameters provide the ability to configure the information based DHCP relay agent (Option 82).

For more information about configuring the DHCP Relay Agent, refer to "Configuring the DHCP relay agent" (Page 279).

12.1.1.4 DHCP binding table

DHCP snooping dynamically builds and maintains a binding table using information extracted from intercepted DHCP messages. The table contains an entry for each untrusted host with a leased IP address from the DHCP server. The table does not contain entries for hosts connected through trusted interfaces. The DHCP snooping feature updates the table when the switch receives specific DHCP messages.

When the device is reset, all the MAC-IP binding information learned by the switch will be lost, unless the learned bindings are saved in the switch configuration file.

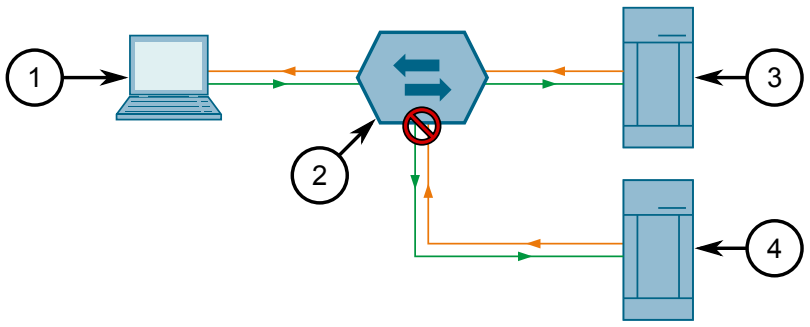
If a switch port link goes down, all the dynamically-learned binding table entries on that particular port are removed from the table.

Manually-entered records can also be configured using a static binding table. For more information about configuring the static DHCP binding table, refer to "Adding entries to the DHCP binding table" (Page 281).

12.1.1.5 Preventable network attacks

The following network attacks can be prevented by enabling DHCP snooping on the switch. For more information, refer to "Configuring DHCP snooping" (Page 280).

- **Host Misconfiguration by a rogue DHCP server**
  A rogue DHCP server can assign an incorrect IP address, default gateway and/or DNS server parameters to the client. A misconfigured client is susceptible to a potential network attack. Switches that support DHCP snooping can identify DHCP messages from a rogue DHCP server and block these messages in the switch itself.

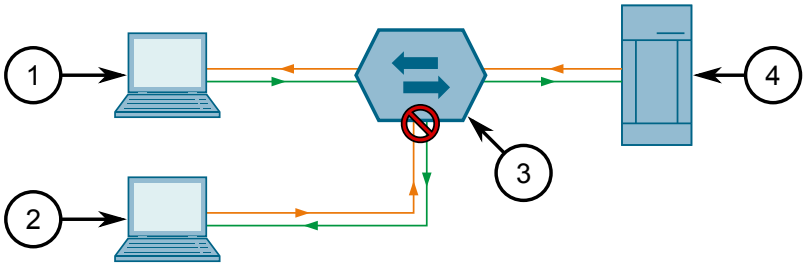


① DHCP client
② Switch
③ DHCP server
④ Rogue DHCP server

Figure 12.1 Misconfiguration by a rogue DHCP server

- **DHCP client attack**
  A roque DHCP client, or attacker host, can cancel the lease for an IP address assigned to another client by sending a DHCPRELEASE message to the DHCP server. It can also decline the IP address for another client by sending a DHCPDECLINE message.

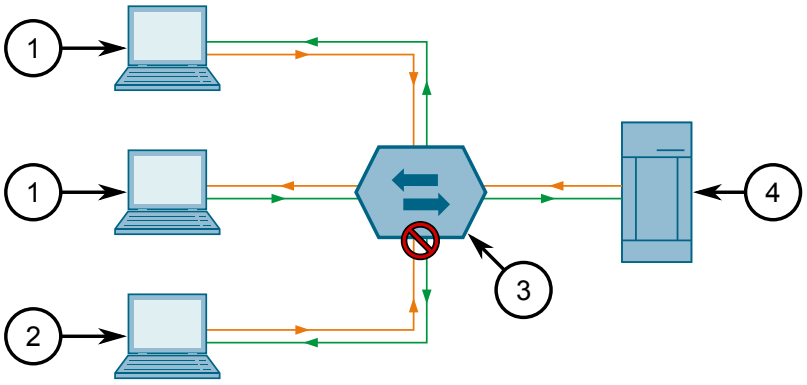
  DHCP snooping builds a DHCP binding table to validate the legitimacy of DHCPRELEASE and DHCPDECLINE messages. If validation of these messages fail, they are dropped by the device.



① DHCP client
② Attacker host
③ Switch
④ DHCP server

Figure 12.2 DHCP client attack

- **DHCP starvation attack**
  DHCP starvation occurs when a DHCP server is flooded with DHCP requests from a single rogue DHCP client that has spoofed the client hardware addresses of other clients. This exhausts the DHCP server's IP address pool, after which the server is unable to respond and provide new leases to legitimate DHCP clients. DHCP snooping provides users an option to verify the client hardware address in the DHCP-REQUEST message, thus preventing a starvation attack.



① DHCP client
② Attacker
③ Switch
④ DHCP server

Figure 12.3 DHCP starvation/consumption attack

12.1.2 Configuring the DHCP relay agent

To configure the device as a DHCP Relay Agent (Option 82), do the following:

1. Navigate to ***Network Access Control » DHCP Snooping » Configure DHCP Parameters***. The **DHCP Parameters** form appears.
2. Configure the following parameter(s) as required:

Parameter	Description
`DHCP Server Address`	**Synopsis:** Any valid IP address IP address of the DHCP server to which DHCP requests will be forwarded. DHCP server IP must be configured for Relay Agent to work.

3. Click **Apply**.

12.1.3 Enabling DHCP relay agent information (Option 82) for specific ports

DHCP Relay Agent (Option 82) can be enabled for any Ethernet port connected to a DHCP client.

To enable DHCP Relay Agent (Option 82) for a specific port, do the following:

1. Navigate to ***Network Access Control » DHCP Snooping » Configure DHCP Port Parameters***. The **DHCP Port Parameters** table appears.
2. Select a port. The **DHCP Port Parameters** form appears.

Note

The **Trusted** parameter is configured as part of the DHCP snooping feature. For more information, refer to "Configuring trusted/untrusted ports" (Page 280).

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

Parameter	Description
`Port`	**Synopsis:** 1 to maximum port number The port number.
`Option-82`	**Synopsis:** [Disabled | Enabled] **Default:** Disabled Insert DHCP Option 82.

4. Click **Apply**.

12.1.4 Configuring DHCP snooping

To configure DHCP snooping, do the following:

Note

DHCP Snooping is enabled on the device on a per-VLAN basis. For more information about enabling DHCP snooping on individual VLANs, refer to "Managing static VLANs" (Page 170).

1. Navigate to ***Network Access Control » DHCP Snooping » Configure DHCP Parameters***. The **DHCP Parameters** form appears.
2. Configure the following parameter(s) as required:

Parameter	Description
`DHCP Server Address`	**Synopsis:** Any valid IP address IP address of the DHCP server to which DHCP requests will be forwarded. DHCP server IP must be configured for Relay Agent to work.
`Verify Hardware Address`	**Synopsis:** [No | Yes] **Default:** Yes Verify if the Client hardware address present in the DHCP message received on untrusted port matches with the Source MAC address.

3. Click **Apply**.
4. Configure individual ports as *trusted* or *untrusted*. For more information, refer to "Configuring trusted/untrusted ports" (Page 280).

12.1.5 Configuring trusted/untrusted ports

Once DHCP Snooping has been enabled, individual ports need to be marked as *trusted* or *untrusted*. Ports connected to the DHCP server should be *trusted*, whereas ports connected to the client or an untrusted DHCP server should be considered *untrusted*.

To configure a port as *trusted* or *untrusted*, do the following:

1. Navigate to ***Network Access Control » DHCP Snooping » Configure DHCP Port Parameters***. The **DHCP Port Parameters** table appears.
2. Select an Ethernet port. The **DHCP Port Parameters** form appears.

   Note

   The **Option-82** parameter is configured as part of the DHCP Relay Agent feature. For more information, refer to "Enabling DHCP relay agent information (Option 82) for specific ports" (Page 279).

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

Parameter	Description
Trusted	**Synopsis:** [No | Yes] **Default:** No DHCP trust setting for the port.

4. Click **Apply**.

12.1.6 Managing the DHCP binding table

This section describes how to configure and manage the DHCP binding table.

12.1.6.1 Adding entries to the DHCP binding table

The DHCP binding table is populated automatically with information RUGGEDCOM ROS learns about untrusted hosts. Specific hosts can also be added to the table. Static entries do not expire and will not be removed when DHCP snooping is disabled or the device is reset.

To add a static entry to the DHCP binding table, do the following:

1. Navigate to ***Network Access Control » DHCP Snooping » Configure Static DHCP Binding Table***. The **Configure Static DHCP Binding Table** appears.
2. Click **InsertRecord**. The **Static DHCP Binding Table** form appears.
3. Configure the following parameter(s) as required:

Parameter	Description
MAC Address	**Synopsis:** ##-##-##-##-##-## where ## ranges 0 to FF **Default:** 00-00-00-00-00-00 MAC Address of the DHCP Host.
IP Address	**Synopsis:** ##-##-##-##-##-## where ## ranges 0 to 255 IP Address assigned to the DHCP Host.
VID	**Synopsis:** An integer between 0 and 65535 **Default:** 1 VLAN where in the IP-MAC binding entry was registered.
Port	**Synopsis:** 1 to maximum port number **Default:** 1 Port on which IP-MAC binding entry was regsitered.

4. Click **Apply**.

12.1.6.2 Viewing the DHCP binding table

To view the DHCP binding table, do the following:

1. Navigate to ***Network Access Control » DHCP Snooping » View DHCP Binding Table***. The **View DHCP Binding Table** appears.
2. Select an Ethernet port. The **DHCP Binding Table** form appears.

The DHCP binding table displays the following information:

Parameter	Description
`MAC Address`	**Synopsis:** ##-##-##-##-##-## where ## ranges 0 to FF MAC Address of the DHCP Host.
`IP Address`	**Synopsis:** ##-##-##-##-##-## where ## ranges 0 to 255 IP Address assigned to the DHCP Host.
`VID`	**Synopsis:** An integer between 0 and 65535 VLAN where in the IP-MAC binding entry was registered.
`Port`	**Synopsis:** 1 to maximum port number **Default:** 1 Port on which IP-MAC binding entry was regsitered.
`Type`	**Synopsis:** [Static | Dynamic] Dynamic DHCP IP-MAC Binding Entries.
`Lease (secs)`	**Synopsis:** An integer between 0 and 4294967295 or [–] Lease time assigned to a Dynamic binding entry in seconds.If the entry is Static then the lease time is infinite denoted as "– ".

To refresh the table, click **Reload**.

12.1.6.3 Saving the DHCP binding table

Information learned dynamically and added to the DHCP binding table is removed automatically when the following occurs:

- The lease expires
- DHCP snooping is disabled
- The device is reset

However, this information can be saved to the configuration file for future reference/ use.

To save the DHCP binding table, do the following:

1. Navigate to ***Network Access Control » DHCP Snooping » Save DHCP Binding Table***. The **Save DHCP Binding Table** table appears.
2. Click **Confirm**.

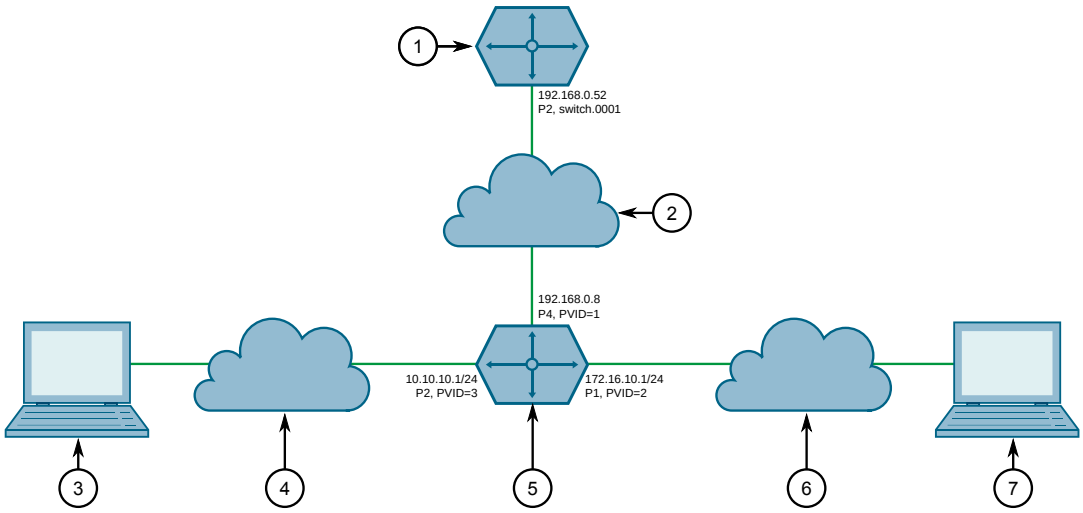
12.1.6.4 Example: Configuring the device as a relay agent

This example demonstrates how to configure the device as a DHCP relay agent.

The following topology depicts a scenario where two clients on separate LANs require IP addresses on different subnets from a DHCP server. Each client connects to the DHCP relay agent using different VLANs. The DHCP relay agent manages the requests and responses between the clients and the DHCP server.

⚠ NOTICE

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



① DHCP server
② LAN A
③ Client 2
④ LAN B
⑤ DHCP relay agent (RUGGEDCOM ROS device)
⑥ LAN C
⑦ Client 1

Figure 12.4 Topology – Device as a relay agent

To configure the device as a DHCP relay agent per the topology, do the following:

1. Configure a separate device as the DHCP Server. If the DHCP server being used is a RUGGEDCOM ROX II device, refer to the device-specific Configuration Manual for more information.
2. Configure the RUGGEDCOM ROS device as a DHCP relay agent:
   a. Add VLAN 2 and VLAN 3. For more information, refer to "Adding a static VLAN" (Page 171).
   b. Assign IP address *192.168.0.8* to VLAN 1. For more information, refer to "Adding an IP interface" (Page 91).

c. Change the PVID of port 1 to PVID 2, and change the PVID of port 2 to PVID 3. Refer to "Configuring VLANs for specific Ethernet ports" (Page 169) for more information.

d. Configure *192.168.0.52* as the DHCP server address. Refer to "Configuring the DHCP relay agent" (Page 279) for more information.

e. Configure DHCP client and server ports as follows:

Port	Option 82
1	Enabled
2	Enabled
4	Disabled

For more information about configuring the DHCP relay agent (Option 82) for a specific port, refer to "Enabling DHCP relay agent information (Option 82) for specific ports" (Page 279).

f. To verify the configuration, make sure Client 1 has IP address 172.16.10.1/24 and Client 2 has IP address 10.10.10.1/24.

3. [Optional] Configure DHCP snooping:

a. Enable DHCP snooping on the DHCP server. If the DHCP server being used is a RUGGEDCOM ROX II device, refer to the device-specific Configuration Manual for more information.

b. Make sure DHCP option is enabled on VLANs 1, 2, and 3. For more information about enabling DHCP for a specific VLAN, refer to "Adding a static VLAN" (Page 171).

c. Configure DHCP client and server ports:

For more information about configuring DHCP port parameters, refer to "Configuring trusted/untrusted ports" (Page 280).

Port	Trusted
1	No
2	No
4	Yes

To verify the configuration, make sure Client 1 has the IP address 172.16.10.1/24 and Client 2 has the IP address 10.10.10.1/24.

In the relay agent binding table, make sure records have been added for Port 1 and Port 2, and make sure no record exists for Port 4. For more information, refer to "Viewing the DHCP binding table" (Page 282).

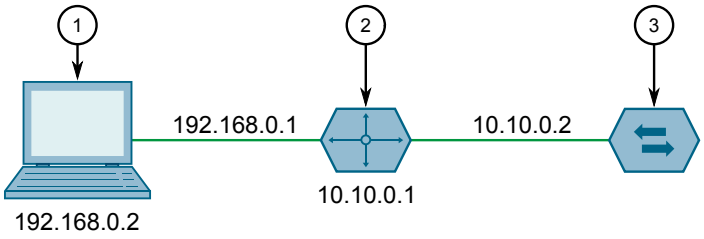
13 Troubleshooting

This chapter describes troubleshooting steps for common issues that may be encountered when using RUGGEDCOM ROS or designing a network.

⚠ NOTICE
For further assistance, contact a Customer Service representative.

13.1 General

The following describes common problems.

Problem	Solution
The switch is not responding to ping attempts, even though the IP address and gateway have been configured. The switch is receiving the ping because the LEDs are flashing and the device statistics are logging the pings. What is going on?	Is the switch being pinged through a router? If so, the switch gateway address must be configured as well. The following figure illustrates the problem.  ① Work station ② Router ③ Switch Figure 13.1 Using a router as a gateway The router is configured with the appropriate IP subnets and will forward the ping from the workstation to the switch. When the switch responds, however, it will not know which of its interfaces to use to reach the workstation and will drop the response. Programming a gateway of 10.0.0.1 will cause the switch to forward unresolvable frames to the router. This problem will also occur if the gateway address is not configured and the switch tries to raise an SNMP trap to a host that is not on the local subnet.

13.2 Ethernet ports

The following describes common problems related to Ethernet ports.

Problem	Solution
A link seems fine when traffic levels are low, but fails as traffic rates increase OR a link can be pinged but has problems with FTP/SQL/HTTP/etc.	A possible cause of intermittent operation with auto-negotiation off is that of a 'duplex mismatch'. If one end of the link is fixed to full-duplex and the peer auto-negotiates, the auto-negotiating end falls back to half-duplex operation. At lower traffic volumes, the link may display few if any errors. As the traffic volume rises, the fixed negotiation side will begin to experience dropped packets while the auto-negotiating side will experience collisions. Ultimately, as traffic loads approach 100%, the link will become entirely unusable. The ping command with flood options is a useful tool for testing commissioned links. The command `ping {destination} {count} {timeout}` can be used to ping the next switch by a specified number of echo requests, separated by the defined number of milliseconds. For example, `ping 192.168.0.1 500 2` issues 500 pings each separated by two milliseconds to the next switch. If the link used is of high quality, then no pings should be lost and the average round trip time should be small.
Links are inaccessible, even when using the Link Fault Indication (LFI) protection feature.	Make sure LFI is not enabled on the peer as well. If both sides of the link have LFI enabled, then both sides will withhold link signal generation from each other.
Previously stable port links experience up/down events when new media is introduced.	This is normal behavior when fiber optic devices are introduced. When a newly inserted fiber optic device is booting up, the fiber ports are in a transitional state and therefore adjacent systems that are live (i.e. functional and stable) will observe port up/down events until the device has completed the boot up sequence. This is due to the fact that fiber transceiver power levels are changing during the boot up transition, thereby toggling the connected link up or down. Installing fiber optic cables in a live network will also cause these effects, especially for connectors that are designed to be keyed and locked, such as ST connectors.
The remote syslog appears to skip events or log them out of sequence.	This is normal behavior when a new Ethernet switch is introduced into a network. In RUGGEDCOM ROS, system and network stability is the highest priority. When a new Ethernet switch is introduced into a network, network reconfiguration occurs so as to prevent loops from occurring and causing broadcast storms. When such reconfiguration takes place, a higher priority is given to RSTP messages and reconfiguration activities than to event logging activities.

13.3 Spanning tree

The following describes common problems related to the Spanning Tree Protocol (STP).

Problem	Solution
The network locks up when a new port is connected and the	Is it possible that one of the switches in the network or one of the ports on a switch in the network has STP disabled and accidentally

Problem	Solution
port status LEDs are flashing rapidly.	connects to another switch? If this has occurred, then a traffic loop has been formed.
Occasionally, the ports seem to experience significant flooding for a brief period of time.	If the problem appears to be transient in nature, it is possible that ports that are part of the spanning tree have been configured as edge ports. After the link layers have come up on edge ports, STP will directly transition them (perhaps improperly) to the forwarding state. If an RSTP configuration message is then received, the port will be returned to blocking. A traffic loop may be formed for the length of time the port was in forwarding. If one of the switches appears to flip the root from one port to another, the problem may be one of traffic prioritization. For more information refer to The network becomes unstable when a specific application is started (Page 288). Another possible cause of intermittent operation is that of an auto-negotiation mismatch. If one end of the link is fixed to full-duplex mode and the peer auto-negotiates, the auto-negotiating end will fall back to half-duplex operation. At lower traffic, the volumes the link may display few if any errors. As the traffic volume rises, the fixed negotiation side will begin to experience dropped packets while the auto-negotiating side will experience collisions. Ultimately, as traffic loads approach 100%, the link will become entirely unusable. At this point, RSTP will not be able to transmit configuration messages over the link and the spanning tree topology will break down. If an alternate trunk exists, RSTP will activate it in the place of the congested port. Since activation of the alternate port often relieves the congested port of its traffic, the congested port will once again become reliable. RSTP will promptly enter it back into service, beginning the cycle once again. The root port will flip back and forth between two ports on the switch.
A switch displays a strange behavior where the root port hops back and forth between two switch ports and never settles down.	
A computer or device is connected to a switch. After the switch is reset, it takes a long time for it to come up.	Is it possible that the RSTP edge setting for this port is set to false? If Edge is set to false, the bridge will make the port go through two forward delay times before the port can send or receive frames. If Edge is set to true, the bridge will transition the port directly to forwarding upon link up. Another possible explanation is that some links in the network run in half-duplex mode. RSTP uses a peer-to-peer protocol called Proposal-Agreement to ensure transitioning in the event of a link failure. This protocol requires full-duplex operation. When RSTP detects a non-full duplex port, it cannot rely on Proposal-Agreement protocol and must make the port transition the slow (i.e. STP) way. If possible, configure the port for full-duplex operation. Otherwise, configure the port's point-to-point setting to true. Either one will allow the Proposal-Agreement protocol to be used.
When the switch is tested by deliberately breaking a link, it takes a long time before devices beyond the switch can be polled.	Is it possible that some ports participating in the topology have been configured to STP mode or that the port's point-to-point parameter is set to false? STP and multipoint ports converge slowly after failures occur. Is it possible that the port has migrated to STP? If the port is connected to the LAN segment by shared media and STP bridges are connected to that media, then convergence after link failure will be slow. Delays on the order of tens or hundreds of milliseconds can result in circumstances where the link broken is the sole link to the root bridge and the secondary root bridge is poorly chosen. The worst of all possible designs occurs when the secondary root bridge is

Problem	Solution
	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 to reestablish the topology.
The network is composed of a ring of bridges, of which two (connected to each other) are managed and the rest are unmanaged. Why does the RSTP protocol work quickly when a link is broken between the managed bridges, but not in the unmanaged bridge part of the ring?	A properly operating unmanaged bridge is transparent to STP configuration messages. The managed bridges will exchange configuration messages through the unmanaged bridge part of the ring as if it is non-existent. When a link in the unmanaged part of the ring fails however, the managed bridges will only be able to detect the failure through timing out of hello messages. Full connectivity will require three hello times plus two forwarding times to be restored.
The network becomes unstable when a specific application is started. The network returns to normal when the application is stopped.	RSTP sends its configuration messages using the highest possible priority level. If CoS is configured to allow traffic flows at the highest priority level and these traffic flows burst continuously to 100% of the line bandwidth, STP may be disrupted. It is therefore advised not to use the highest CoS.
When a new port is brought up, the root moves on to that port instead of the port it should move to or stay on.	Is it possible that the port cost is incorrectly programmed or that auto-negotiation derives an undesired value? Inspect the port and path costs with each port active as root.
An Intelligent Electronic Device (IED) or controller does not work with the device.	Certain low CPU bandwidth controllers have been found to behave less than perfectly when they receive unexpected traffic. Try disabling STP for the port. If the controller fails around the time of a link outage, there is the remote possibility that frame disordering or duplication may be the cause of the problem. Try setting the root port of the failing controller's bridge to STP.
Polls to other devices are occasionally lost.	Review the network statistics to determine whether the root bridge is receiving Topology Change Notifications (TCNs) around the time of observed frame loss. It may be possible there are problems with intermittent links in the network.
The root is receiving a number of TCNs. Where are they coming from?	Examine the RSTP port statistics to determine the port from which the TCNs are arriving. Sign-on to the switch at the other end of the link attached to that port. Repeat this step until the switch generating the TCNs is found (i.e. the switch that is itself not receiving a large number of TCNs). Determine the problem at that switch.

13.4 VLANs

The following describes common problems related to the VLANs.

Problem	Solution
VLANs are not needed on the network. Can they be turned off?	Yes. Simply leave all ports set to type *edge* and leave the native VLAN set to 1. This is the default configuration for the switch.
Two VLANs were created and a number of ports were made members of them. Now some of the devices in one VLAN need to	If the devices need to communicate at the physical address layer, they must be members of the same VLAN. If they can communicate in a Layer 3 fashion (i.e. using a protocol such as IP or IPX), use a router. The router will treat each VLAN as a separate interface, which will have its own associated IP address space.

Problem	Solution
send messages to devices in the other VLAN.	
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.

14 Reference

This chapter provides additional information that may be required to understand and/or configure related features in RUGGEDCOM ROS.

14.1 SNMP

The following sections describe the available SNMP MIBs, agent capabilities and traps available in RUGGEDCOM ROS v5.10:

14.1.1 Supported standard MIBs

RUGGEDCOM ROS supports the following standard MIBs:

⚠ NOTICE
This section lists all MIBs supported by RUGGEDCOM ROS, and is intended for reference purposes only. Individual device support may vary.

- **BRIDGE-MIB**
  For more information, refer to "BRIDGE-MIB" (Page 292).
- **IEC-62439-3-MIB**
  For more information, refer to "IEC-62439-3-MIB" (Page 299).
- **IEEEC37-238-MIB**
  For more information, refer to "IEEEC37-238-MIB" (Page 307).
- **IF-MIB**
  For more information, refer to "IF-MIB" (Page 317).
- **IP-MIB**
  For more information, refer to "IP-MIB" (Page 325).
- **LLDP-MIB**
  For more information, refer to "LLDP-MIB" (Page 331).
- **Q-BRIDGE-MIB**
  For more information, refer to "Q-BRIDGE-MIB" (Page 339).
- **RMON-MIB**
  For more information, refer to "RMON-MIB" (Page 345).
- **RS-232-MIB**
  For more information, refer to "RS-232-MIB" (Page 357).

- **RSTP-MIB**
  For more information, refer to "RSTP-MIB" (Page 361).
- **SNMP-FRAMEWORK-MIB**
  For more information, refer to "SNMP-FRAMEWORK-MIB" (Page 362).
- **SNMP-USER-BASED-SM-MIB**
  For more information, refer to "SNMP-USER-BASED-SM-MIB" (Page 363).
- **SNMPv2-MIB**
  For more information, refer to "SNMPv2-MIB" (Page 367).
- **SNMP-VIEW-BASED-ACM-MIB**
  For more information, refer to "SNMP-VIEW-BASED-ACM-MIB" (Page 371).
- **TCP-MIB**
  For more information, refer to "TCP-MIB" (Page 373).
- **UDP-MIB**
  For more information, refer to "UDP-MIB" (Page 376).

BRIDGE-MIB

Group/Object	Description
Group: dot1dBaseBridgeGroup **Object:** dot1dBaseBridgeAddress	**Access:** Read-Only **Syntax:** Hex-String **OID:** .1.3.6.1.2.1.17.1.1.0 **Definition:** The MAC address used by this bridge when it must be referred to in a unique fashion. It is recommended that this be the numerically smallest MAC address of all ports that belong to this bridge. However, it is only required to be unique. When concatenated with dot1dStpPriority, a unique BridgeIdentifier is formed, which is used in the Spanning Tree Protocol.
Group: dot1dBaseBridgeGroup **Object:** dot1dBaseNumPorts	**Access:** Read-Only **Syntax:** Integer **OID:** .1.3.6.1.2.1.17.1.2.0 **Definition:** The number of ports controlled by this bridging entity.
Group: dot1dBasePortGroup **Object:** dot1dBasePort	**Access:** Read-Only **Syntax:** Integer **OID:** .1.3.6.1.2.1.17.1.4.1.1.1 **Definition:** The port number of the port for which this entry contains bridge management information.
Group: dot1dBasePortGroup **Object:** dot1dBasePortCircuit	**Access:** Read-Only **Syntax:** OID **OID:** .1.3.6.1.2.1.17.1.3.1 **Definition:** For a port that (potentially) has the same value of dot1dBasePortIfIndex as another port on the same bridge. This object contains the name of an object instance unique to this port. For example, in the case where multiple ports correspond one-to-one with multiple X.25 virtual circuits, this value might identify an (e.g., the first) object instance associated with the X.25 virtual circuit corresponding to this port. For a port that has a unique value of dot1dBasePortIfIndex, this object can have the value { 0 0 }.

Group/Object	Description
Group: dot1dBasePortGroup **Object:** dot1dBasePortDelayExceededDiscards	**Agent Capability:** RC-BRIDGE-MIB-AC **Access:** Read-Only **Syntax:** Counter32 **OID:** .1.3.6.1.2.1.17.1.4.1.4.1 **Definition:** The number of frames discarded by this port due to excessive transit delay through the bridge. It is incremented by both transparent and source route bridges. **Note** The switch does not have a knowledge of the value of this object. In a response to a get request a zero value will be returned.
Group: dot1dBasePortGroup **Object:** dot1dBasePortIfIndex	**Access:** Read-Only **Syntax:** Integer **OID:** .1.3.6.1.2.1.17.1.4.1.2.1 **Definition:** The value of the instance of the ifIndex object, defined in IF-MIB, for the interface corresponding to this port.
Group: dot1dBasePortGroup **Object:** dot1dBasePortMtuExceededDiscards	**Access:** Read-Only **Syntax:** Counter32 **OID:** .1.3.6.1.2.1.17.1.4.1.5.1 **Definition:** The number of frames discarded by this port due to an excessive size. It is incremented by both transparent and source route bridges.
Group: dot1dBaseBridgeGroup **Object:** dot1dBaseType	**Access:** Read-Only **Syntax:** Integer **OID:** .1.3.6.1.2.1.17.1.3.0 **Definition:** Indicates what type of bridging this bridge can perform. If a bridge is actually performing a certain type of bridging, this will be indicated by entries in the port table for the given type.
Group: dot1dStpBridgeGroup **Object:** dot1dStpBridgeForwardDelay	**Agent Capability:** RC-BRIDGE-MIB-AC **Access:** Read-Write **Syntax:** Integer **OID:** .1.3.6.1.2.1.17.2.14.0 **Definition:** The value that all bridges use for ForwardDelay when this bridge is acting as the root. Note that 802.1D-1998 specifies that the range for this parameter is related to the value of dot1dStpBridgeMaxAge. The granularity of this timer is specified by 802.1D-1998 to be 1 second. An agent may return a badValue error if a set is attempted to a value that is not a whole number of seconds. **Note** The value of this object will be rounded to the closest number of tenths of a second.
Group: dot1dStpBridgeGroup **Object:** dot1dStpBridgeHelloTime	**Agent Capability:** RC-BRIDGE-MIB-AC **Access:** Read-Write **Syntax:** Integer **OID:** .1.3.6.1.2.1.17.2.13.0

Group/Object	Description
	Definition: The value that all bridges use for HelloTime when this bridge is acting as the root. The granularity of this timer is specified by 802.1D-1998 to be 1 second. An agent may return a badValue error if a set is attempted to a value that is not a whole number of seconds. **Note** The value of this object will be rounded to the closest number of tenths of a second.
Group: dot1dStpBridgeGroup **Object:** dot1dStpBridgeMaxAge	**Agent Capability:** RC-BRIDGE-MIB-AC **Access:** Read-Write **Syntax:** Integer **OID:** .1.3.6.1.2.1.17.2.12.0 **Definition:** The value that all bridges use for MaxAge when this bridge is acting as the root. Note that 802.1D-1998 specifies that the range for this parameter is related to the value of dot1dStpBridgeHelloTime. The granularity of this timer is specified by 802.1D-1998 to be 1 second. An agent may return a badValue error if a set is attempted to a value that is not a whole number of seconds. **Note** The value of this object will be rounded to the closest number of tenths of a second.
Group: dot1dStpBridgeGroup **Object:** dot1dStpDesignatedRoot	**Access:** Read-Only **Syntax:** Hex-String **OID:** .1.3.6.1.2.1.17.2.5.0 **Definition:** The bridge identifier of the root of the spanning tree, as determined by the Spanning Tree Protocol, as executed by this node. This value is used as the Root Identifier parameter in all Configuration Bridge PDUs originated by this node.
Group: dot1dStpBridgeGroup **Object:** dot1dStpForwardDelay	**Access:** Read-Only **Syntax:** Integer **OID:** .1.3.6.1.2.1.17.2.11.0 **Definition:** This time value, measured in units of hundredths of a second, controls how fast a port changes its spanning state when moving towards the Forwarding state. The value determines how long the port stays in each of the Listening and Learning states, which precede the Forwarding state. This value is also used when a topology change has been detected and is underway, to age all dynamic entries in the Forwarding Database. [Note that this value is the one that this bridge is currently using, in contrast to dot1dStpBridgeForwardDelay, which is the value that this bridge and all others would start using if/when this bridge were to become the root.]
Group: dot1dStpBridgeGroup **Object:** dot1dStpHelloTime	**Access:** Read-Only **Syntax:** Integer **OID:** .1.3.6.1.2.1.17.2.9.0 **Definition:** The amount of time between the transmission of Configuration bridge PDUs by this node on any port when it is the root of the spanning tree, or trying to become so, in units of hundredths of a second. This is the actual value that this bridge is currently using.

Group/Object	Description
Group: dot1dStpBridgeGroup **Object:** dot1dStpHoldTime	**Access:** Read-Only **Syntax:** Integer **OID:** .1.3.6.1.2.1.17.2.10.0 **Definition:** This time value determines the interval length during which no more than two Configuration bridge PDUs shall be transmitted by this node, in units of hundredths of a second.
Group: dot1dStpBridgeGroup **Object:** dot1dStpMaxAge	**Access:** Read-Only **Syntax:** Integer **OID:** .1.3.6.1.2.1.17.2.8.0 **Definition:** The maximum age of Spanning Tree Protocol information learned from the network on any port before it is discarded, in units of hundredths of a second. This is the actual value that this bridge is currently using.
Group: dot1dStpPortGroup **Object:** dot1dStpPort	**Access:** Read-Only **Syntax:** Integer **OID:** .1.3.6.1.2.1.17.2.15.1.1.1 **Definition:** The port number of the port for which this entry contains Spanning Tree Protocol management information.
Group: dot1dStpPortGroup **Object:** dot1dStpPortDesignatedBridge	**Access:** Read-Only **Syntax:** Hex-String **OID:** .1.3.6.1.2.1.17.2.15.1.8.1 **Definition:** The Bridge Identifier of the bridge that this port considers to be the Designated Bridge for this port's segment.
Group: dot1dStpPortGroup **Object:** dot1dStpPortDesignatedCost	**Access:** Read-Only **Syntax:** Integer **OID:** .1.3.6.1.2.1.17.2.15.1.7.1 **Definition:** The path cost of the Designated Port of the segment connected to this port. This value is compared to the Root Path Cost field in received bridge PDUs.
Group: dot1dStpPortGroup **Object:** dot1dStpPortDesignatedPort	**Access:** Read-Only **Syntax:** Hex-String **OID:** .1.3.6.1.2.1.17.2.15.1.9.1 **Definition:** The Port Identifier of the port on the Designated Bridge for this port's segment.
Group: dot1dStpPortGroup **Object:** dot1dStpPortDesignatedRoot	**Access:** Read-Only **Syntax:** Hex-String **OID:** .1.3.6.1.2.1.17.2.15.1.6.1 **Definition:** The unique Bridge Identifier of the Bridge recorded as the Root in the Configuration BPDUs transmitted by the Designated Bridge for the segment to which the port is attached.
Group: dot1dStpPortGroup **Object:** dot1dStpPortEnable	**Access:** Read-Write **Syntax:** Integer **OID:** .1.3.6.1.2.1.17.2.15.1.4.1 **Definition:** The enabled/disabled status of the port.
Group: dot1dStpPortGroup **Object:** dot1dStpPortForwardTransitions	**Access:** Read-Only **Syntax:** Counter32

Group/Object	Description
	OID: .1.3.6.1.2.1.17.2.15.1.10.1 **Definition:** The number of times this port has transitioned from the Learning state to the Forwarding state.
Group: dot1dStpPortGroup **Object:** dot1dStpPortPathCost	**Access:** Read-Write **Syntax:** Integer **OID:** .1.3.6.1.2.1.17.2.15.1.5.1 **Definition:** The contribution of this port to the path cost of paths towards the spanning tree root which include this port. 802.1D-1998 recommends that the default value of this parameter be in inverse proportion to the speed of the attached LAN. New implementations should support dot1dStpPortPathCost32. If the port path costs exceeds the maximum value of this object then this object should report the maximum value, namely 65535. Applications should try to read the dot1dStpPortPathCost32 object if this object reports the maximum value.
Group: dot1dStpPortGroup **Object:** dot1dStpPortPriority	**Agent Capability:** RC-BRIDGE-MIB-AC **Access:** Read-Write **Syntax:** Integer **OID:** .1.3.6.1.2.1.17.2.15.1.2.1 **Definition:** The value of the priority field that is contained in the first (in network byte order) octet of the (2 octet long) Port ID. The other octet of the Port ID is given by the value of dot1dStpPort. On bridges supporting IEEE 802.1t or IEEE 802.1w, permissible values are 0-240, in steps of 16. **Note** Permissible values for this object are 0 to 240 in steps of 16 as per RFC 4188.
Group: rstpPortGroup **Object:** dot1dStpPortProtocolMigration	**Access:** Read-Write **TruthValue** **OID:** .1.3.6.1.2.1.17.2.19.1.1 **Definition:** When operating in RSTP (version 2) mode, writing true(1) to this object forces this port to transmit RSTP BPDUs. Any other operation on this object has no effect and it always returns false(2) when read.
Group: dot1dStpPortGroup **Object:** dot1dStpPortState	**Access:** Read-Only **Syntax:** Integer **OID:** .1.3.6.1.2.1.17.2.15.1.3.1 **Definition:** The port's current state, as defined by application of the Spanning Tree Protocol. This state controls what action a port takes on reception of a frame. If the bridge has detected a port that is malfunctioning, it will place that port into the broken(6) state. For ports that are disabled (see dot1dStpPortEnable), this object will have a value of disabled(1).
Group: dot1dStpBridgeGroup **Object:** dot1dStpPriority	**Agent Capability:** RC-BRIDGE-MIB-AC **Access:** Read-Write **Syntax:** Integer **OID:** .1.3.6.1.2.1.17.2.2.0 **Definition:** The value of the write-able portion of the Bridge ID (i.e., the first two octets of the (8 octet long) Bridge ID). The other (last) 6 octets of the Bridge ID are given by the value of dot1dBaseBridgeAddress. On bridges supporting IEEE 802.1t or IEEE 802.1w, permissible values are 0-61440, in steps of 4096.

Group/Object	Description
	Note Permissible values for this object are 0 to 61440 in steps of 4096 as per RFC 4188.
Group: dot1dStpBridgeGroup **Object:** dot1dStpProtocolSpecification	**Access:** Read-Only **Syntax:** Integer **OID:** .1.3.6.1.2.1.17.2.1.0 **Definition:** An indication of what version of the Spanning Tree Protocol is being run. The value **decLb100(2)** indicates the DEC LANbridge 100 Spanning Tree protocol. IEEE 802.1D implementations will return **ieee8021d(3)**. If future versions of the IEEE Spanning Tree Protocol that are incompatible with the current version are released a new value will be defined.
Group: dot1dStpBridgeGroup **Object:** dot1dStpRootCost	**Access:** Read-Only **Syntax:** Integer **OID:** .1.3.6.1.2.1.17.2.6.0 **Definition:** The cost of the path to the root as seen from this bridge.
Group: dot1dStpBridgeGroup **Object:** dot1dStpRootPort	**Access:** Read-Only **Syntax:** Integer **OID:** .1.3.6.1.2.1.17.2.7.0 **Definition:** The port number of the port that offers the lowest cost path from this bridge to the root bridge.
Group: dot1dStpBridgeGroup **Object:** dot1dStpTimeSinceTopologyChange	**Agent Capability:** RC-BRIDGE-MIB-AC **Access:** Read-Only **Syntax:** Timeticks **OID:** .1.3.6.1.2.1.17.2.3.0 **Definition:** The time (in hundredths of a second) since the last time a topology change was detected by the bridge entity. For RSTP, this reports the time since the tcWhile timer for any port on this Bridge was nonzero. **Note** The time since the tcWhile timer for any port on this Bridge was non-zero as per RFV 4188.
Group: dot1dStpBridgeGroup **Object:** dot1dStpTopChanges	**Access:** Read-Only **Syntax:** Counter32 **OID:** .1.3.6.1.2.1.17.2.4.0 **Definition:** The total number of topology changes detected by this bridge since the management entity was last reset or initialized.
Group: dot1dTpBridgeGroup **Object:** dot1dTpAgingTime	**Access:** Read-Write **Syntax:** Integer **OID:** .1.3.6.1.2.1.17.4.2.0 **Definition:** The timeout period in seconds for aging out dynamically-learned forwarding information. 802.1D-1998 recommends a default of 300 seconds.

Group/Object	Description
	Note The range of valid values is restricted to 15 to 800 seconds. Lower limit of 15 seconds is a hardware limitation.
Group: dot1dTpFdbGroup **Object:** dot1dTpFdbAddress	**Access:** Read-Only **Syntax:** Hex-String **OID:** .1.3.6.1.2.1.17.4.3.1.1.148.184.197.5.176.0 **Definition:** A unicast MAC address for which the bridge has forwarding and/or filtering information.
Group: dot1dTpFdbGroup **Object:** dot1dTpFdbPort	**Access:** Read-Only **Syntax:** Integer **OID:** .1.3.6.1.2.1.17.4.3.1.2.148.184.197.5.176.0 **Definition:** Either the value **0**, or the port number of the port on which a frame having a source address equal to the value of the corresponding instance of dot1dTpFdbAddress has been seen. A value of **0** indicates that the port number has not been learned, but that the bridge does have some forwarding/filtering information about this address (e.g., in the dot1dStaticTable). Implementors are encouraged to assign the port value to this object whenever it is learned, even for addresses for which the corresponding value of dot1dTpFdbStatus is not learned(3).
Group: dot1dTpFdbGroup **Object:** dot1dTpFdbStatus	**Access:** Read-Only **Syntax:** Integer **OID:** .1.3.6.1.2.1.17.4.3.1.3.148.184.197.5.176.0 **Definition:** The status of this entry. The meanings of the values are: • other(1) - none of the following. This would include the case where some other MIB object (not the corresponding instance of dot1dTpFdbPort, nor an entry in the dot1dStaticTable) is being used to determine if and how frames addressed to the value of the corresponding instance of dot1dTpFdbAddress are being forwarded. • invalid(2) - this entry is no longer valid (e.g., it was learned but has since aged out), but has not yet been flushed from the table. • learned(3) - the value of the corresponding instance of dot1dTpFdbPort was learned, and is being used. • self(4) - the value of the corresponding instance of dot1dTpFdbAddress represents one of the bridge's addresses. The corresponding instance of dot1dTpFdbPort indicates which of the bridge's ports has this address. • mgmt(5) - the value of the corresponding instance of dot1dTpFdbAddress is also the value of an existing instance of dot1dStaticAddress.
Group: dot1dTpBridgeGroup **Object:** dot1dTpLearnedEntryDiscards	**Agent Capability:** RC-BRIDGE-MIB-AC **Access:** Read-Only **Syntax:** Counter32 **OID:** .1.3.6.1.2.1.17.4.1.0 **Definition:** The total number of Forwarding Database entries that have been or would have been learned, but have been discarded due to a lack of storage space in the Forwarding Database. If this counter is increasing, it indicates that the Forwarding Database is regularly becoming full (a condition that has unpleasant performance effects on the subnetwork). If

Group/Object	Description
	this counter has a significant value but is not presently increasing, it indicates that the problem has been occurring but is not persistent. **Note** The switch does not have a knowledge of the value of this object. In a response to a get request a zero value will be returned.
Group: dot1dTpGroup **Object:** dot1dTpPort	**Access:** Read-Only **Syntax:** Integer **OID:** .1.3.6.1.2.1.17.4.4.1.1.1 **Definition:** The port number of the port for which this entry contains Transparent bridging management information.
Group: dot1dTpGroup **Object:** dot1dTpPortInDiscards	**Access:** Read-Only **Syntax:** Counter32 **OID:** .1.3.6.1.2.1.17.4.4.1.5.1 **Definition:** Count of received valid frames that were discarded (i.e., filtered) by the Forwarding Process.
Group: dot1dTpGroup **Object:** dot1dTpPortInFrames	**Access:** Read-Only **Syntax:** Counter32 **OID:** .1.3.6.1.2.1.17.4.4.1.3.1 **Definition:** The number of frames that have been received by this port from its segment. Note that a frame received on the interface corresponding to this port is only counted by this object if and only if it is for a protocol being processed by the local bridging function, including bridge management frames.
Group: dot1dTpGroup **Object:** dot1dTpPortMaxInfo	**Access:** Read-Only **Syntax:** Integer **OID:** .1.3.6.1.2.1.17.4.4.1.2.1 **Definition:** The maximum size of the INFO (non-MAC) field that this port will receive or transmit.
Group: dot1dTpGroup **Object:** dot1dTpPortOutFrames	**Access:** Read-Only **Syntax:** Counter32 **OID:** .1.3.6.1.2.1.17.4.4.1.4.1 **Definition:** The number of frames that have been transmitted by this port to its segment. Note that a frame transmitted on the interface corresponding to this port is only counted by this object if and only if it is for a protocol being processed by the local bridging function, including bridge management frames.

IEC-62439-3-MIB

Group/Object	Description
Group: lreStatisticsInterfaceGroup **Object:** lreCntDuplicateA	**Access:** Read-Only **Syntax:** Counter32 **OID:** 1.0.62439.2.21.1.1.0.1.1.19.1 **Definition:** Number of entries in the duplicate detection mechanism on port A for which one single duplicate was received.

Group/Object	Description
Group: lreStatisticsInterfaceGroup **Object:** lreCntDuplicateB	**Access:** Read-Only **Syntax:** Counter32 **OID:** 1.0.62439.2.21.1.1.0.1.1.20.1 **Definition:** Number of entries in the duplicate detection mechanism on port B for which one single duplicate was received.
Group: lreStatisticsInterfaceGroup **Object:** lreCntDuplicateC	**Access:** Read-Only **Syntax:** Counter32 **OID:** 1.0.62439.2.21.1.1.0.1.1.21.1 **Definition:** Number of entries in the duplicate detection mechanism on port C for which one single duplicate was received.
Group: lreStatisticsInterfaceGroup **Object:** lreCntErrorsA	**Access:** Read-Only **Syntax:** Counter32 **OID:** 1.0.62439.2.21.1.1.0.1.1.11.1 **Definition:** Number of frames with errors received on this LRE port A. Initial value = 0.
Group: lreStatisticsInterfaceGroup **Object:** lreCntErrorsB	**Access:** Read-Only **Syntax:** Counter32 **OID:** 1.0.62439.2.21.1.1.0.1.1.12.1 **Definition:** Number of frames with errors received on this LRE port B. Initial value = 0.
Group: lreStatisticsInterfaceGroup **Object:** lreCntErrorsC	**Access:** Read-Only **Syntax:** Counter32 **OID:** 1.0.62439.2.21.1.1.0.1.1.13.1 **Definition:** Number of frames with errors received on the application interface of a DANP or DANH or on the interlink of a RedBox. Initial value = 0.
Group: lreStatisticsInterfaceGroup **Object:** lreCntErrWrongLanA	**Access:** Read-Only **Syntax:** Counter32 **OID:** 1.0.62439.2.21.1.1.0.1.1.5.1 **Definition:** Number of frames with the wrong LAN identifier received on LRE port A. Initial value = 0. Only applicable to PRP ports.
Group: lreStatisticsInterfaceGroup **Object:** lreCntErrWrongLanB	**Access:** Read-Only **Syntax:** Counter32 **OID:** 1.0.62439.2.21.1.1.0.1.1.6.1 **Definition:** Number of frames with the wrong LAN identifier received on LRE port B. Initial value = 0. Only applicable to PRP ports.
Group: lreStatisticsInterfaceGroup **Object:** lreCntErrWrongLanC	**Agent Capability:** RC-IEC-62439-3-MIB-AC **Access:** not-implemented **Syntax:** Counter32 **OID:** 1.0.62439.2.21.1.1.0.1.1.7.1 **Definition:** Number of frames with the wrong LAN identifier received on the interlink of a RedBox. Only applicable to HSR RedBoxes in HSR-PRP configuration.
Group: lreStatisticsInterfaceGroup **Object:** lreCntMultiA	**Agent Capability:** RC-IEC-62439-3-MIB-AC **Access:** not-implemented

Group/Object	Description
	Syntax: Counter32 **OID:** 1.0.62439.2.21.1.1.0.1.1.22.1 **Definition:** Number of entries in the duplicate detection mechanism on port A for which more than one duplicate was received.
Group: lreStatisticsInterfaceGroup **Object:** lreCntMultiB	**Agent Capability:** RC-IEC-62439-3-MIB-AC **Access:** not-implemented **Syntax:** Counter32 **OID:** 1.0.62439.2.21.1.1.0.1.1.23.1 **Definition:** Number of entries in the duplicate detection mechanism on port B for which more than one duplicate was received.
Group: lreStatisticsInterfaceGroup **Object:** lreCntMultiC	**Agent Capability:** RC-IEC-62439-3-MIB-AC **Access:** not-implemented **Syntax:** Counter32 **OID:** 1.0.62439.2.21.1.1.0.1.1.24.1 **Definition:** Number of entries in the duplicate detection mechanism on the application interface of the DAN or the interlink of the RedBox for which more than one duplicate was received.
Group: lreStatisticsInterfaceGroup **Object:** lreCntNodes	**Access:** Read-Only **Syntax:** Integer **OID:** 1.0.62439.2.21.1.1.0.1.1.14.1 **Definition:** Number of nodes in the Nodes Table.
Group: lreStatisticsInterfaceGroup **Object:** lreCntOwnRxA	**Access:** Read-Only **Syntax:** Counter32 **OID:** 1.0.62439.2.21.1.1.0.1.1.25.1 **Definition:** Number of HSR tagged frames received on Port A that originated from this device. Frames originate from this device if the source MAC matches the MAC of the LRE, or if the source MAC appears in the proxy node table (if implemented). Applicable only to HSR. Initial value = 0.
Group: lreStatisticsInterfaceGroup **Object:** lreCntOwnRxB	**Access:** Read-Only **Syntax:** Counter32 **OID:** 1.0.62439.2.21.1.1.0.1.1.26.1 **Definition:** Number of HSR tagged frames received on Port B that originated from this device. Frames originate from this device if the source MAC matches the MAC of the LRE, or if the source MAC appears in the proxy node table (if implemented). Applicable only to HSR. Initial value = 0.
Group: lreStatisticsInterfaceGroup **Object:** lreCntProxyNodes	**Access:** Read-Only **Syntax:** Integer **OID:** 1.0.62439.2.21.1.1.0.1.1.15.1 **Definition:** Number of nodes in the Proxy Node Table. Only applicable to RedBox. Initial value = 0.
Group: lreStatisticsInterfaceGroup **Object:** lreCntRxA	**Access:** Read-Only **Syntax:** Counter32 **OID:** 1.0.62439.2.21.1.1.0.1.1.8.1 **Definition:** Number of frames received on a LRE port A. Only frames that are HSR tagged or fitted with a PRP Redundancy Control Trailer are counted.

Group/Object	Description
	Frames that are not forwarded anywhere (e.g. because the sender of the frame is in the proxy node table) are counted, too. Only frames received completely and without error are counted. Initial value = 0.
Group: lreStatisticsInterfaceGroup **Object:** lreCntRxB	**Access:** Read-Only **Syntax:** Counter32 **OID:** 1.0.62439.2.21.1.1.0.1.1.9.1 **Definition:** Number of frames received on a LRE port B. Only frames that are HSR tagged or fitted with a PRP Redundancy Control Trailer are counted. Frames that are not forwarded anywhere (e.g. because the sender of the frame is in the proxy node table) are counted, too. Only frames received completely and without error are counted. Initial value = 0.
Group: lreStatisticsInterfaceGroup **Object:** lreCntRxC	**Agent Capability:** RC-IEC-62439-3-MIB-AC **Access:** Read-Only **Syntax:** Counter32 **OID:** 1.0.62439.2.21.1.1.0.1.1.10.1 **Definition:** Number of frames received from the application interface of a DANP or DANH or the number of number of frames received on the interlink of a RedBox. Frames with and without PRP RCT or HSR tag are counted, but not linklocal frames. Only frames received completely and without error are counted. Initial value = 0. **Note** Only frames received on the local port are counted.
Group: lreStatisticsInterfaceGroup **Object:** lreCntTxA	**Access:** Read-Only **Syntax:** Counter32 **OID:** 1.0.62439.2.21.1.1.0.1.1.2.1 **Definition:** Number of frames sent over port A that are HSR tagged or fitted with a PRP Redundancy Control Trailer. Only frames that are HSR tagged or do have a PRP RCT are counted. A frame aborted during the transmission is not counted. Initial value = 0.
Group: lreStatisticsInterfaceGroup **Object:** lreCntTxB	**Access:** Read-Only **Syntax:** Counter32 **OID:** 1.0.62439.2.21.1.1.0.1.1.3.1 **Definition:** Number of frames sent over port B that are HSR tagged or fitted with a PRP Redundancy Control Trailer. Only frames that are HSR tagged or do have a PRP RCT are counted. A frame aborted during the transmission is not counted. Initial value = 0.
Group: lreStatisticsInterfaceGroup **Object:** lreCntTxC	**Agent Capability:** RC-IEC-62439-3-MIB-AC **Access:** Read-Only **Syntax:** Counter32 **OID:** 1.0.62439.2.21.1.1.0.1.1.4.1 **Definition:** Number of frames sent towards the application interface of the DANP or DANH or over the interlink of the RedBox. Frames with and without PRP RCT or HSR tag are counted, but not link-local frames. A frame aborted during the transmission is not counted. Initial value = 0.

Group/Object	Description
	Note Only frames sent out the local port are counted.
Group: lreStatisticsInterfaceGroup **Object:** lreCntUniqueA	**Agent Capability:** RC-IEC-62439-3-MIB-AC **Access:** not-implemented **Syntax:** Counter32 **OID:** 1.0.62439.2.21.1.1.0.1.1.16.1 **Definition:** Number of entries in the duplicate detection mechanism on port A for which no duplicate was received.
Group: lreStatisticsInterfaceGroup **Object:** lreCntUniqueB	**Agent Capability:** RC-IEC-62439-3-MIB-AC **Access:** not-implemented **Syntax:** Counter32 **OID:** 1.0.62439.2.21.1.1.0.1.1.17.1 **Definition:** Number of entries in the duplicate detection mechanism on port B for which no duplicate was received.
Group: lreStatisticsInterfaceGroup **Object:** lreCntUniqueC	**Agent Capability:** RC-IEC-62439-3-MIB-AC **Access:** not-implemented **Syntax:** Counter32 **OID:** 1.0.62439.2.21.1.1.0.1.1.18.1 **Definition:** Number of entries in the duplicate detection mechanism on port C for which no duplicate was received.
Group: lreConfigurationInterfaceGroup **Object:** lreDuplicateDiscard	**Agent Capability:** RC-IEC-62439-3-MIB-AC **Access:** Read-Only **Syntax:** Integer **OID:** 1.0.62439.2.21.0.1.0.1.1.11.1 **Definition:** Specifies whether a duplicate discard algorithm is used at reception. Default: discard.
Group: lreConfigurationInterfaceGroup **Object:** lreEvaluateSupervision	**Agent Capability:** RC-IEC-62439-3-MIB-AC **Access:** Read-Only **Syntax:** Integer **OID:** 1.0.62439.2.21.0.1.0.1.1.16.1 **Definition:** True if the LRE evaluates received supervision frames. False if it drops the supervision frames without evaluating. Note: LREs are required to send supervision frames, but reception is optional. Default value is dependent on implementation.
Group: lreConfigurationInterfaceGroup **Object:** lreHsrLREMode	**Agent Capability:** RC-IEC-62439-3-MIB-AC **Access:** Read-Only **Syntax:** Integer **OID:** 1.0.62439.2.21.0.1.0.1.1.13.1 **Definition:** This enumeration is only applicable if the LRE is an HSR bridging node or RedBox. It shows the mode of the HSR LRE: • (1): Default mode: The HSR LRE is in mode h and bridges tagged HSR traffic.

Group/Object	Description
	• (2): Optional mode: The HSR LRE is in mode n and bridging between its HSR ports Is disabled. Traffic is HSR tagged. • (3): Optional mode: The HSR LRE is in mode t and bridges nontagged HSR traffic between its HSR ports. • (4): Optional mode: The HSR LRE is in mode u and behaves like in mode h, except it does not remove unicast messages. • (5): Optional mode: The HSR LRE is configured in mixed mode. HSR frames are handled according to mode h. Non-HSR frames are handled according to 802.1D ridging rules. When the switch is in HSR mode, this configuration setting is accessible but is Read-Only. Value: modeh(1). When the switch is in PRP mode, this setting is not accessible because it does not apply.
Group: lreConfigurationInterfaceGroup **Object:** lreInterfaceConfigEntry	**Access:** not-implemented **Syntax:** Integer **OID:** 1.0.62439.2.21.0.1.0.1.1 **Definition:** Each entry contains management information applicable to a particular LRE.
Group: lreConfigurationInterfaceGroup **Object:** lreInterfaceConfigIndex	**Access:** not-implemented **Syntax:** Integer **OID:** 1.0.62439.2.21.0.1.0.1.1.1 **Definition:** A unique value for each LRE.
Group: lreConfigurationInterfaceGroup **Object:** lreInterfaceConfigTable	**Access:** not-implemented **Syntax:** Integer **OID:** 1.0.62439.2.21.0.1.0.1 **Definition:** List of PRP/HSR LREs. Each entry corresponds to one PRP/HSR Link Redundancy Entity (LRE), each representing a pair of LAN ports A and B. Basic devices supporting PRP/HSR may have only one LRE and thus one entry in the table, while more complex devices may have several entries for multiple LREs.
Group: lreConfigurationGeneralGroup **Object:** lreInterfaceCount	**Access:** Read-Only **Syntax:** Integer **OID:** 1.0.62439.2.21.0.0.2.0 **Definition:** Total number of LREs present in this system.
Group: lreStatisticsInterfaceGroup **Object:** lreInterfaceStatsEntry	**Access:** not-implemented **Syntax:** Integer **OID:** 1.0.62439.2.21.1.1.0.1.1 **Definition:** An entry containing management information applicable to a particular LRE.
Group: lreStatisticsInterfaceGroup **Object:** lreInterfaceStatsIndex	**Access:** not-implemented **Syntax:** Integer **OID:** 1.0.62439.2.21.1.1.0.1.1.1 **Definition:** A unique value for each LRE.
Group: lreStatisticsInterfaceGroup **Object:** lreInterfaceStatsTable	**Access:** not-implemented **Syntax:** Integer **OID:** 1.0.62439.2.21.1.1.0.1

Group/Object	Description
	Definition: List of PRP/HSR LREs. Each entry corresponds to one PRP/HSR Link Redundancy Entity (LRE), each representing a pair of LAN ports A and B and a port C towards the application/interlink. Basic devices supporting PRP/HSR may have only one LRE and thus one entry in the table, while more complex devices may have several entries for multiple LREs.
Group: lreConfigurationInterfaceGroup **Object:** lreLinkStatusA	**Access:** Read-Only **Syntax:** Integer **OID:** 1.0.62439.2.21.0.1.0.1.1.9.1 **Definition:** Shows the actual link status of the LRE's port A.
Group: lreConfigurationInterfaceGroup **Object:** lreLinkStatusB	**Access:** Read-Only **Syntax:** Integer **OID:** 1.0.62439.2.21.0.1.0.1.1.10.1 **Definition:** Shows the actual link status of the LRE's port B.
Group: lreConfigurationInterfaceGroup **Object:** lreMacAddress	**Agent Capability:** RC-IEC-62439-3-MIB-AC **Access:** Read-Only **Syntax:**MacAddress **OID:** 1.0.62439.2.21.0.1.0.1.1.6.1 **Definition:** Specifies the MAC address to be used by this LRE. MAC addresses are identical for all ports of a single LRE.
Group: lreConfigurationGeneralGroup **Object:** lreManufacturerName	**Access:** Read-Only **Syntax:**DisplayString **OID:** 1.0.62439.2.21.0.0.1.0 **Definition:** Specifies the name of the LRE device manufacturer.
Group: lreConfigurationInterfaceGroup **Object:** lreNodeName	**Access:** Read-Write **Syntax:**DisplayString **OID:** 1.0.62439.2.21.0.1.0.1.1.4.1 **Definition:** Specifies this LRE's node name.
Group: lreConfigurationInterfaceGroup **Object:** lreNodesTableClear	**Access:** Read-Write **Syntax:** Integer **OID:** 1.0.62439.2.21.0.1.0.1.1.17.1 **Definition:** Specifies that the Node Table is to be cleared.
Group: lreConfigurationInterfaceGroup **Object:** lreNodeType	**Access:** Read-Write **Syntax:** Integer **OID:** 1.0.62439.2.21.0.1.0.1.1.3.1 **Definition:** Specifies the operation mode of the LRE: • PRP mode 1 (1) • HSR mode (2) **Note** PRP mode 0 is considered deprecated and is not supported by this revision of the MIB.
Group: lreConfigurationInterfaceGroup **Object:** lrePortAdminStateA	**Access:** Read-Write **Syntax:** Integer

Group/Object	Description
	OID: 1.0.62439.2.21.0.1.0.1.1.7.1 **Definition:** Specifies whether the port A shall be active or not Active through administrative action. Default: active
Group: lreConfigurationInterfaceGroup **Object:** lrePortAdminStateB	**Access:** Read-Write **Syntax:** Integer **OID:** 1.0.62439.2.21.0.1.0.1.1.8.1 **Definition:** Specifies whether the port B shall be active or not Active through administrative action. Default: active
Group: lreConfigurationInterfaceGroup **Object:** lreProxyNodeTableClear	**Agent Capability:** RC-IEC-62439-3-MIB-AC **Access:** not-implemented **Syntax:** Integer **OID:** 1.0.62439.2.21.0.1.0.1.1.18 **Definition:** Specifies that the Proxy Node Table is to be cleared.
Group: lreConfigurationInterfaceGroup **Object:** lreRedBoxIdentity	**Agent Capability:** RC-IEC-62439-3-MIB-AC **Access:** not-implemented **Syntax:** Integer **OID:** 1.0.62439.2.21.0.1.0.1.1.15 **Definition:** Applicable to RedBox HSR-PRP A and RedBox HSR-PRP B. One ID is used by one pair of RedBoxes (one configured to A and one configured to B) coupling an HSR ring to a PRP network. The integer value states the value of the path field a RedBox inserts into each frame it receives from its interlink and injects into the HSR ring. When interpreted as binary values, the LSB denotes the configuration of the RedBox (A or B), and the following 3 bits denote the identifier of a RedBox pair.
Group: lreConfigurationInterfaceGroup **Object:** lreRowStatus	**Agent Capability:** RC-IEC-62439-3-MIB-AC **Access:** Read-Only **Syntax:** RowStatus **OID:** 1.0.62439.2.21.0.1.0.1.1.2 **Definition:** Indicates the status of the LRE table entry.
Group: lreConfigurationInterfaceGroup **Object:** lreSwitchingEndNode	**Agent Capability:** RC-IEC-62439-3-MIB-AC **Access:** Read-Only **Syntax:** Integer **OID:** 1.0.62439.2.21.0.1.0.1.1.14.1 **Definition:** This enumeration shows which feature is enabled in this particular LRE: • (1): an unspecified non-bridging node, e.g. SRP. • (2): an unspecified bridging node, e.g. RSTP. • (3): a PRP node/RedBox. • (4): an HSR RedBox with regular Ethernet traffic on its interlink. • (5): an HSR switching node. • (6): an HSR RedBox with HSR tagged traffic on its interlink. • (7): an HSR RedBox with PRP traffic for LAN A on its interlink. • (8): an HSR RedBox with PRP traffic for LAN B on its interlink.
Group: lreConfigurationInterfaceGroup **Object:** lreTransparentReception	**Access:** Read-Only **Syntax:** Integer

Group/Object	Description
	OID: 1.0.62439.2.21.0.1.0.1.1.12.1 **Definition:** If removeRCT is configured, the RCT is removed when forwarding to the upper layers, only applicable for PRP LRE (Default: removeRCT).
Group: lreConfigurationInterfaceGroup **Object:** lreVersionName	**Access:** Read-Only **Syntax:** String **OID:** 1.0.62439.2.21.0.1.0.1.1.5.1 **Definition:** Specifies the version of this LRE's software.

IEEEC37-238-MIB

Group/Object	Description
Group: ieeeC37238SystemCurrentGroup **Object:** ieeeC37238CurrentDSLocTimeInacc	**Access:** Read-Only **Syntax:** Gauge32 **OID:** 1.3.111.3.37.238.9999.1.2.3 **Definition:** TimeInaccuracy contribution of the device in nanoseconds.
Group: ieeeC37238SystemCurrentGroup **Object:** ieeeC37238CurrentDSOfstFrMaster	**Access:** Read-Only **Syntax:** IEEEC37238TimeInterval **OID:** 1.3.111.3.37.238.9999.1.2.2 **Definition:** Implementation-specific representation of the current value of the time difference between a master and a slave as computed by the slave; i.e., <offsetFromMaster> = <Time on the slave clock> ? <Time on the master clock>. The most significant 4 bytes. The data type should be TimeInterval.
Group: ieeeC37238SystemCurrentGroup **Object:** ieeeC37238CurrentDSStepsRemoved	**Access:** Read-Only **Syntax:** Integer **OID:** 1.3.111.3.37.238.9999.1.2.1 **Definition:** The number of communication paths traversed between the local clock and the grandmaster clock. The initialization value shall be 0.
Group: ieeeC37238SystemDefaultReqdGroup **Object:** ieeeC37238DefaultDSClkClass	**Access:** Read-Only **Syntax:** IEEEC37238ClockAccuracyValue **OID:** 1.3.111.3.37.238.9999.1.1.4 **Definition:** ClockClass of the local clock.
Group: ieeeC37238SystemDefaultReqdGroup **Object:** ieeeC37238DefaultDSClkIdentity	**Access:** Read-Only **Syntax:** ClockIdentity **OID:** 1.3.111.3.37.238.9999.1.1.2 **Definition:** ClockIdentity of the local clock.
Group: ieeeC37238SystemDefaultReqdGroup **Object:** ieeeC37238DefaultDSDomainNumber	**Agent Capability:** AC-IEEEC37-238-MIB-AC **Access:** not-implemented **Syntax:** Integer **OID:** 1.3.111.3.37.238.9999.1.1.9 **Definition:** Default domain of the local clock.
Group: ieeeC37238SystemDefaultReqdGroup **Object:** ieeeC37238DefaultDSEngTimeInacc	**Agent Capability:** AC-IEEEC37-238-MIB-AC **Access:** not-implemented **Syntax:** Integer

Group/Object	Description
	OID: 1.3.111.3.37.238.9999.1.1.13 **Definition:** Engineered networkTimeInaccuracy in ns. This value represents the worst networkTimeInaccuracy from this device to all.
Group: ieeeC37238SystemDefaultReqdGroup **Object:** ieeeC37238DefaultDSGMIdentity	**Access:** Read-Write **Syntax:** Integer **OID:** 1.3.111.3.37.238.9999.1.1.11 **Definition:** Grandmaster Identity to be transmitted in IEEE_C37_238 TLV (2 bytes). Most significant byte is reserved and shall be 0. Configurable for grandmaster-capable devices only.
Group: ieeeC37238SystemDefaultReqdGroup **Object:** ieeeC37238DefaultDSLocTimeInacc	**Access:** Read-Only **Syntax:** Gauge32 **OID:** 1.3.111.3.37.238.9999.1.1.14 **Definition:** Maximum TimeInaccuracy that the device contributes to the total networkTimeInaccuracy.
Group: ieeeC37238SystemDefaultReqdGroup **Object:** ieeeC37238DefaultDSNetTimeInacc	**Access:** Read-Write **Syntax:** Gauge32 **OID:** 1.3.111.3.37.238.9999.1.1.12 **Definition:** networkTimeInaccuracy to be transmitted in IEEE_C37_238 TLV.
Group: ieeeC37238SystemDefaultReqdGroup **Object:** ieeeC37238DefaultDSNumberPorts	**Access:** Read-Only **Syntax:** Gauge32 **OID:** 1.3.111.3.37.238.9999.1.1.3 **Definition:** The number of PTP ports on the device. For an ordinary clock, this value shall be 1.
Group: ieeeC37238SystemDefaultReqdGroup **Object:** ieeeC37238DefaultDSOfsScdLogVar	**Access:** Read-Only **Syntax:** Integer **OID:** 1.3.111.3.37.238.9999.1.1.6 **Definition:** The value is scaled, offset representation of an estimate of the PTP variance. The PTP variance characterizes the precision and frequency stability of the grandmaster clock.
Group: ieeeC37238SystemDefaultReqdGroup **Object:** ieeeC37238DefaultDSOfstFrMLimit	**Agent Capability:** RC-IEEEC37-238-MIB-AC **Access:** Read-Only **Syntax:** IEEEC37238TimeInterval **OID:** 1.3.111.3.37.238.9999.1.1.15 **Definition:** Offset from Master Limit to generate OfstExceedsLimit event.
Group: ieeeC37238SystemDefaultReqdGroup **Object:** ieeeC37238DefaultDSPriority1	**Access:** Read-Write **Syntax:** Gauge32 **OID:** 1.3.111.3.37.238.9999.1.1.7 **Definition:** Priority1 attribute of the local clock.
Group: ieeeC37238SystemDefaultReqdGroup **Object:** ieeeC37238DefaultDSPriority2	**Access:** Read-Write **Syntax:** Gauge32 **OID:** 1.3.111.3.37.238.9999.1.1.8 **Definition:** Priority2 attribute of the local clock.
Group: ieeeC37238SystemDefaultReqdGroup **Object:** ieeeC37238DefaultDSSlaveOnly	**Access:** Read-Write **Syntax:** Integer

Group/Object	Description
	OID: 1.3.111.3.37.238.9999.1.1.10 **Definition:** True if the local clock is a slave-only clock, False otherwise.
Group: ieeeC37238SystemDefaultReqdGroup **Object:** ieeeC37238DefaultDSTwoStepFlag	**Access:** Read-Write **Syntax:** Integer **OID:** 1.3.111.3.37.238.9999.1.1.1 **Definition:** True if the clock is a two-step clock, False otherwise.
Group: ieeeC37238EventsPropertiesGroup **Object:** ieeeC37238EventFaultyState	**Agent Capability:** RC-IEEEC37-238-MIB-AC **OID:** 1.3.111.3.37.238.9999.0.0.3.0 **Definition:** Indicates that a clock has entered faulty state. **Note** This notification is not supported.
Group: ieeeC37238EventsPropertiesGroup **Object:** ieeeC37238EventLeapSecAnnounced	**Agent Capability:** RC-IEEEC37-238-MIB-AC **OID:** 1.3.111.3.37.238.9999.0.0.7.0 **Definition:** Indicates that a leap second has been announced. **Note** This notification is not supported.
Group: ieeeC37238EventsPropertiesGroup **Object:** ieeeC37238EventOtherProfileDetect	**Agent Capability:** RC-IEEEC37-238-MIB-AC **OID:** 1.3.111.3.37.238.9999.0.0.6.0 **Definition:** Indicates that other then C37.238 PTP profile has been detected. **Note** This notification is not supported.
Group: ieeeC37238EventsPropertiesGroup **Object:** ieeeC37238EventPortStateChange	**Agent Capability:** RC-IEEEC37-238-MIB-AC **OID:** 1.3.111.3.37.238.9999.0.0.4.0 **Definition:** Indicates that port state has changed. **Note** This notification is not supported.
Group: ieeeC37238SystemClockParentGroup **Object:** ieeeC37238ParentDSClkIdentity	**Access:** Read-Only **Syntax:** ClockIdentity **OID:** 1.3.111.3.37.238.9999.1.3.1.0 **Definition:** Clock Identity of the master that synchronizes this clock.
Group: ieeeC37238SystemClockParentGroup **Object:** ieeeC37238ParentDSGMClkAccuracy	**Access:** Read-Only **Syntax:** IEEEC37238ClockAccuracyValue **OID:** 1.3.111.3.37.238.9999.1.3.8.0 **Definition:** ClockAccuracy of the grandmaster clock.
Group: ieeeC37238SystemClockParentGroup **Object:** ieeeC37238ParentDSGMClkClass	**Access:** Read-Only **Syntax:** IEEEC37238ClockClassValue **OID:** 1.3.111.3.37.238.9999.1.3.7.0

Group/Object	Description
	Definition: ClockClass of the grandmaster clock.
Group: ieeeC37238SystemClockParentGroup **Object:** ieeeC37238ParentDSGMClkIdentity	**Access:** Read-Only **Syntax:** ClockIdentity **OID:** 1.3.111.3.37.238.9999.1.3.6.0 **Definition:** ClockIdentity of the grandmaster clock.
Group: ieeeC37238SystemClockParentGroup **Object:** ieeeC37238ParentDSGMIdentity	**Access:** Read-Only **Syntax:** Integer **OID:** 1.3.111.3.37.238.9999.1.3.12.0 **Definition:** Grandmaster Identity received in IEEE_C37_238 TLV.
Group: ieeeC37238SystemClockParentGroup **Object:** ieeeC37238ParentDSGMOfstScdLVar	**Agent Capability:** RC-IEEEC37-238-MIB-AC **Access:** Read-Only **Syntax:** Integer **OID:** 1.3.111.3.37.238.9999.1.3.4.0 **Definition:** OffsetScaledLog Variance of the grandmaster clock.
Group: ieeeC37238SystemClockParentGroup **Object:** ieeeC37238ParentDSGMPriority1	**Access:** Read-Only **Syntax:** Gauge32 **OID:** 1.3.111.3.37.238.9999.1.3.10.0 **Definition:** Priority1 attribute of the grandmaster clock.
Group: ieeeC37238SystemClockParentGroup **Object:** ieeeC37238ParentDSGMPriority2	**Access:** Read-Only **Syntax:** Gauge32 **OID:** 1.3.111.3.37.238.9999.1.3.11.0 **Definition:** Priority2 attribute of the grandmaster clock.
Group: ieeeC37238SystemClockParentGroup **Object:** ieeeC37238ParentDSGMTimeInacc	**Agent Capability:** RC-IEEEC37-238-MIB-AC **Access:** Read-Only **Syntax:** Gauge32 **OID:** 1.3.111.3.37.238.9999.1.3.13.0 **Definition:** NetworkTimeInaccuracy received in IEEE_C37_238 TLV in nanoseconds.
Group: ieeeC37238SystemClockParentGroup **Object:** ieeeC37238ParentDSNetTimeInacc	**Agent Capability:** RC-IEEEC37-238-MIB-AC **Access:** Read-Only **Syntax:** Gauge32 **OID:** 1.3.111.3.37.238.9999.1.3.14.0 **Definition:** NetworkTimeInaccuracy received in IEEE_C37_238 TLV in nanoseconds.
Group: ieeeC37238SystemClockParentGroup **Object:** ieeeC37238ParentDSObsOfstScdLVar	**Agent Capability:** RC-IEEEC37-238-MIB-AC **Access:** Read-Only **Syntax:** Gauge32 **OID:** 1.3.111.3.37.238.9999.1.3.4.0 **Definition:** An estimate of the parent clock PTP variance as observed by the slave clock, computed and represented as described in IEEE Std 1588-2008 7.6.3.5. The initialization value shall be FFFF.
Group: ieeeC37238SystemClockParentGroup **Object:** ieeeC37238ParentDSObsPhChgRate	**Agent Capability:** RC-IEEEC37-238-MIB-AC **Access:** Read-Only

Group/Object	Description
	Syntax: Gauge32 **OID:** 1.3.111.3.37.238.9999.1.3.5.0 **Definition:** An estimate of the parent clock phase change rate as observed by the slave clock as defined in IEEE Std 1588-2008 7.6.4.4. If the estimate exceeds the capacity of its data type, this value shall be set to 7FFF FFFF or 8000 0000, as appropriate. A positive sign indicates that the parent clock phase change rate is greater than the rate of the slave clock. The initialization value shall be 7FFF FFFF.
Group: ieeeC37238SystemClockParentGroup **Object:** ieeeC37238ParentDSPortNumber	**Access:** Read-Only **Syntax:** Gauge32 **OID:** 1.3.111.3.37.238.9999.1.3.2.0 **Definition:** Port Number of the port on the master that issues the Sync messages used in synchronizing this clock.
Group: ieeeC37238SystemClockParentGroup **Object:** ieeeC37238ParentDSStats	**Agent Capability:** RC-IEEEC37-238-MIB-AC **Access:** Read-Only **Syntax:** Integer **OID:** 1.3.111.3.37.238.9999.1.3.3.0 **Definition:** True if all of the following 2 conditions are satisfied: • The clock has a port in the SLAVE state. • The clock has computed statistically valid estimates of the parentDS.observedParentOffsetScaledLog Variance and the parentDS.observedParentClockPhaseChangeRate members. False otherwise. The initialization value shall be FALSE.
Group: ieeeC37238TCPropertiesGroup **Object:** ieeeC37238TCDefaultDSClkIdentity	**Access:** Read-Only **Syntax:** ClockIdentity **OID:** 1.3.111.3.37.238.9999.1.6.1 **Definition:** The Clock Identity of the local clock.
Group: ieeeC37238TCPropertiesGroup **Object:** ieeeC37238TCDefaultDSCurGMaster	**Access:** Read-Only **Syntax:** ClockIdentity **OID:** 1.3.111.3.37.238.9999.1.6.6 **Definition:** Comprises current grandmaster identity.
Group: ieeeC37238TCPropertiesGroup **Object:** ieeeC37238TCDefaultDSDelayMech	**Agent Capability:** RC-IEEEC37-238-MIB-AC **Access:** Read-Only **Syntax:** Integer **OID:** 1.3.111.3.37.238.9999.1.6.3 **Definition:** The Delay Mechanism used by the device.For IEEE C37.238 compliant implementations this value shall be 2 (p2p).
Group: ieeeC37238TCPropertiesGroup **Object:** ieeeC37238TCDefaultDSGMIdentity	**Agent Capability:** RC-IEEEC37-238-MIB-AC **Access:** not-implemented **Syntax:** Integer **OID:** 1.3.111.3.37.238.9999.1.6.8 **Definition:** Grandmaster Identity received in GRANDMASTER_ID TLV.
Group: ieeeC37238TCPropertiesGroup **Object:** ieeeC37238TCDefaultDSGMTimeInacc	**Agent Capability:** RC-IEEEC37-238-MIB-AC **Access:** Read-Only **Syntax:** Gauge32

Group/Object	Description
	OID: 1.3.111.3.37.238.9999.1.6.12 **Definition:** GrandmasterTimeInaccuracy received in IEEE_C37_238 TLV.
Group: ieeeC37238TCPropertiesGroup **Object:** ieeeC37238TCDefaultDSLocTimeInacc	**Access:** Read-Only **Syntax:** Gauge32 **OID:** 1.3.111.3.37.238.9999.1.6.14 **Definition:** TimeInaccuracy contribution of the local clock in nanoseconds.
Group: ieeeC37238TCPropertiesGroup **Object:** ieeeC37238TCDefaultDSNetProtocol	**Access:** Read-Write **Syntax:** Integer **OID:** 1.3.111.3.37.238.9999.1.6.9 **Definition:** Indicates Network Protocol in use. For IEEE C37.238 compliant implementations this value shall be 1 (ieee8023).
Group: ieeeC37238TCPropertiesGroup **Object:** ieeeC37238TCDefaultDSNetTimeInacc	**Agent Capability:** RC-IEEEC37-238-MIB-AC **Access:** Read-Only **Syntax:** Gauge32 **OID:** 1.3.111.3.37.238.9999.1.6.13 **Definition:** NetworkTimeInaccuracy received in IEEE_C37_238 TLV.
Group: ieeeC37238TCPropertiesGroup **Object:** ieeeC37238TCDefaultDSNumberPorts	**Access:** Read-Only **Syntax:** Gauge32 **OID:** 1.3.111.3.37.238.9999.1.6.2 **Definition:** The number of PTP ports of the device.
Group: ieeeC37238TCPropertiesGroup **Object:** ieeeC37238TCDefaultDSPriDomain	**Agent Capability:** RC-IEEEC37-238-MIB-AC **Access:** Read-Only **Syntax:** Integer **OID:** 1.3.111.3.37.238.9999.1.6.4 **Definition:** Domain number of the primary syntonization domain. The initialization value shall be 0.
Group: ieeeC37238TCPropertiesGroup **Object:** ieeeC37238TCDefaultDSPriority	**Agent Capability:** RC-IEEEC37-238-MIB-AC **Access:** Read-Only **Syntax:** Gauge32 **OID:** 1.3.111.3.37.238.9999.1.6.11 **Definition:** Indicates VLAN tag Priority in use.
Group: ieeeC37238TCPropertiesGroup **Object:** ieeeC37238TCDefaultDSSyntonize	**Agent Capability:** RC-IEEEC37-238-MIB-AC **Access:** Read-Only **Syntax:** Integer **OID:** 1.3.111.3.37.238.9999.1.6.5 **Definition:** True if syntonization enabled.
Group: ieeeC37238TCPropertiesGroup **Object:** ieeeC37238TCDefaultDSTwoStepFlag	**Access:** Read-Write **Syntax:** Integer **OID:** 1.3.111.3.37.238.9999.1.6.7 **Definition:** True if the clock is a two-step clock.
Group: ieeeC37238TCPropertiesGroup **Object:** ieeeC37238TCDefaultDSVlanId	**Agent Capability:** AC-IEEEC37-238-MIB-AC **Access:** not-implemented

Group/Object	Description
	Syntax: Gauge32 **OID:** 1.3.111.3.37.238.9999.1.6.10 **Definition:** Indicates VLAN ID in use.
Group: ieeeC37238SystemTimePropGroup **Object:** ieeeC37238TimePropDSCurUTCOfst	**Access:** Read-Only **Syntax:** Integer **OID:** 1.3.111.3.37.238.9999.1.4.1 **Definition:** The current offset between TAI and UTC in units of seconds.
Group: ieeeC37238SystemTimePropGroup **Object:** ieeeC37238TimePropDSCurUTCOfstVd	**Access:** Read-Only **Syntax:** Integer **OID:** 1.3.111.3.37.238.9999.1.4.2 **Definition:** True if the the currentUtcOffset is known to be correct.
Group: ieeeC37238SystemTimePropGroup **Object:** ieeeC37238TimePropDSFrqTraceable	**Access:** Read-Only **Syntax:** Integer **OID:** 1.3.111.3.37.238.9999.1.4.6 **Definition:** True if the frequency determining the timescale is traceable to a primary reference, False otherwise.
Group: ieeeC37238SystemTimePropGroup **Object:** ieeeC37238TimePropDSLeap59	**Agent Capability:** RC-IEEEC37-238-MIB-AC **Access:** Read-Only **Syntax:** Integer **OID:** 1.3.111.3.37.238.9999.1.4.3 **Definition:** True value indicates that the last minute of the current UTC day contains 59 seconds.
Group: ieeeC37238SystemTimePropGroup **Object:** ieeeC37238TimePropDSLeap61	**Access:** Read-Only **Syntax:** Integer **OID:** 1.3.111.3.37.238.9999.1.4.4 **Definition:** True value indicates that the last minute of the current UTC day contains 61 seconds.
Group: ieeeC37238SystemTimePropGroup **Object:** ieeeC37238TimePropDSLeapEvExpiry	**Agent Capability:** RC-IEEEC37-238-MIB-AC **Access:** not-implemented **Syntax:** Integer **OID:** 1.3.111.3.37.238.9999.1.4.15 **Definition:** The seconds portion of PTP time for the expiry of the latest IERS-announced leap-second event. If PTP time > LeapEvExpiry, devices shall set CurUTCOfstVd to False.
Group: ieeeC37238SystemTimePropGroup **Object:** ieeeC37238TimePropDSLeapEvLatest	**Agent Capability:** RC-IEEEC37-238-MIB-AC **Access:** not-implemented **Syntax:** Integer **OID:** 1.3.111.3.37.238.9999.1.4.13 **Definition:** The seconds portion of PTP time for the second prior to the latest IERS-announced leap-second event (may be past or future).
Group: ieeeC37238SystemTimePropGroup **Object:** ieeeC37238TimePropDSLocalTCurOfs	**Agent Capability:** RC-IEEEC37-238-MIB-AC **Access:** not-implemented **Syntax:** Integer

Group/Object	Description
	OID: 1.3.111.3.37.238.9999.1.4.9 **Definition:** The offset of the alternate time, in seconds, from the node time. The alternate time is the sum of this value and the node time.
Group: ieeeC37238SystemTimePropGroup **Object:** ieeeC37238TimePropDSLocalTJumpS	**Agent Capability:** RC-IEEEC37-238-MIB-AC **Access:** not-implemented **Syntax:** Integer **OID:** 1.3.111.3.37.238.9999.1.4.10 **Definition:** The size of the next discontinuity, in seconds, of the alternate time. A value of zero indicates that no discontinuity is expected. A positive value indicates that the discontinuity will cause the currentOffset of the alternate time to increase.
Group: ieeeC37238SystemTimePropGroup **Object:** ieeeC37238TimePropDSLocalTName	**Agent Capability:** RC-IEEEC37-238-MIB-AC **Access:** not-implemented **Syntax:** String **OID:** 1.3.111.3.37.238.9999.1.4.12 **Definition:** The value of displayName shall be the text name of the alternate timescale.
Group: ieeeC37238SystemTimePropGroup **Object:** ieeeC37238TimePropDSLocalTNtJump	**Agent Capability:** RC-IEEEC37-238-MIB-AC **Access:** not-implemented **Syntax:** Integer **OID:** 1.3.111.3.37.238.9999.1.4.11 **Definition:** The value of the seconds portion of the transmitting node time at the time that the next discontinuity will occur. The discontinuity occurs at the start of the second indicated by this value.
Group: ieeeC37238SystemTimePropGroup **Object:** ieeeC37238TimePropDSPTPTimescale	**Access:** Read-Only **Syntax:** Integer **OID:** 1.3.111.3.37.238.9999.1.4.7 **Definition:** True if the clock timescale of the grandmaster clock is PTP. This value shall always be True for IEEE C37.238 compliant implementations.
Group: ieeeC37238SystemTimePropGroup **Object:** ieeeC37238TimePropDSTmeTraceable	**Access:** Read-Only **Syntax:** Integer **OID:** 1.3.111.3.37.238.9999.1.4.5 **Definition:** True if the timescale and the value of currentUtcOffset are traceable to a primary reference; False otherwise.
Group: ieeeC37238SystemTimePropGroup **Object:** ieeeC37238TimePropDSUTCOfstNext	**Agent Capability:** RC-IEEEC37-238-MIB-AC **Access:** not-implemented **Syntax:** Integer **OID:** 1.3.111.3.37.238.9999.1.4.14 **Definition:** Seconds offset between TAI and UTC timescales after LeapEvLatest(same as CurUTCOfst after LeapEvLatest time).
Group: ieeeC37238PortDataSetGlobalGroup **Object:** ifIeeeC37238PortDSAnnounceRcTout	**Agent Capability:** RC-IEEEC37-238-MIB-AC **Access:** Read-Only **Syntax:** Integer **OID:** 1.3.111.3.37.238.9999.1.5.1.7

Group/Object	Description
	Definition: Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime.
Group: ieeeC37238PortDataSetGlobalGroup **Object:** ifIeeeC37238PortDSClkIdentity	**Access:** Read-Only **Syntax:** ClockIdentity **OID:** 1.3.111.3.37.238.9999.1.5.1.2 **Definition:** Clock Identity of the local clock.
Group: ieeeC37238PortDataSetGlobalGroup **Object:** ifIeeeC37238PortDSDelayMech	**Agent Capability:** RC-IEEEC37-238-MIB-AC **Access:** Read-Only **Syntax:** Integer **OID:** 1.3.111.3.37.238.9999.1.5.1.9 **Definition:** The propagation delay measuring option used by the port. For IEEE C37.238 compliant implementations this value shall be 2 (p2p).
Group: ieeeC37238PortDataSetGlobalGroup **Object:** ifIeeeC37238PortDSDlyAsymmetry	**Agent Capability:** RC-IEEEC37-238-MIB-AC **Access:** not-implemented **Syntax:** Integer **OID:** 1.3.111.3.37.238.9999.1.5.1.13 **Definition:** Path delay asymmetry.
Group: ieeeC37238PortDataSetGlobalGroup **Object:** ifIeeeC37238PortDSLogAnnounceInt	**Agent Capability:** RC-IEEEC37-238-MIB-AC **Access:** Read-Only **Syntax:** Integer **OID:** 1.3.111.3.37.238.9999.1.5.1.6 **Definition:** The logarithm to the base 2 of the mean announceInterval.
Group: ieeeC37238PortDataSetGlobalGroup **Object:** ifIeeeC37238PortDSLogMinPdlyRInt	**Agent Capability:** RC-IEEEC37-238-MIB-AC **Access:** Read-Only **Syntax:** Integer **OID:** 1.3.111.3.37.238.9999.1.5.1.10 **Definition:** The logarithm to the base 2 of the minPdelayReqInterval.
Group: ieeeC37238PortDataSetGlobalGroup **Object:** ifIeeeC37238PortDSLogSyncInt	**Agent Capability:** RC-IEEEC37-238-MIB-AC **Access:** Read-Only **Syntax:** Integer **OID:** 1.3.111.3.37.238.9999.1.5.1.8 **Definition:** The logarithm to the base 2 of the mean SyncInterval for multicast messages.
Group: ieeeC37238PortDataSetGlobalGroup **Object:** ifIeeeC37238PortDSMPathPDly	**Access:** Read-Only **Syntax:** IEEEC37238TimeInterval **OID:** 1.3.111.3.37.238.9999.1.5.1.5 **Definition:** An estimate of the current one-way propagation delay on the link, attached to this port computed using the peer delay mechanism. The initialization value shall be zero.
Group: ieeeC37238PortDataSetGlobalGroup **Object:** ifIeeeC37238PortDSNetProtocol	**Agent Capability:** RC-IEEEC37-238-MIB-AC **Access:** Read-Only **Syntax:** Integer

Group/Object	Description
	OID: 1.3.111.3.37.238.9999.1.5.1.15 **Definition:** Indicates Network Protocol in use. For IEEE C37.238 compliant implementations this value shall be 1 (ieee8023).
Group: ieeeC37238PortDataSetGlobalGroup **Object:** ifIeeeC37238PortDSPortNumber	**Access:** Read-Only **Syntax:** Gauge32 **OID:** 1.3.111.3.37.238.9999.1.5.1.3 **Definition:** Port Number of the local port.
Group: ieeeC37238PortDataSetGlobalGroup **Object:** ifIeeeC37238PortDSPortState	**Access:** Read-Only **Syntax:** Integer **OID:** 1.3.111.3.37.238.9999.1.5.1.4 **Definition:** The current state of the PTP protocol engine associated with this port.
Group: ieeeC37238PortDataSetGlobalGroup **Object:** ifIeeeC37238PortDSPriority	**Agent Capability:** RC-IEEEC37-238-MIB-AC **Access:** Read-Only **Syntax:** Gauge32 **OID:** 1.3.111.3.37.238.9999.1.5.1.17 **Definition:** Indicates VLAN tag Priority in use.
Group: ieeeC37238PortDataSetGlobalGroup **Object:** ifIeeeC37238PortDSProfileId	**Agent Capability:** RC-IEEEC37-238-MIB-AC **Access:** Read-Only **Syntax:** Integer **OID:** 1.3.111.3.37.238.9999.1.5.1.14 **Definition:** Indicates the PTP Profile in use.
Group: ieeeC37238PortDataSetGlobalGroup **Object:** ifIeeeC37238PortDSPtpPortEnabled	**Agent Capability:** RC-IEEEC37-238-MIB-AC **Access:** Read-Only **Syntax:** Integer **OID:** 1.3.111.3.37.238.9999.1.5.1.12 **Definition:** True if port is enabled.
Group: ieeeC37238PortDataSetGlobalGroup **Object:** ifIeeeC37238PortDSVersionNumber	**Access:** Read-Only **Syntax:** Gauge32 **OID:** 1.3.111.3.37.238.9999.1.5.1.11 **Definition:** The PTP version in use on the port. For IEEE C37.238 compliant implementations this value shall be 2.
Group: ieeeC37238PortDataSetGlobalGroup **Object:** ifIeeeC37238PortDSVlanId	**Agent Capability:** RC-IEEEC37-238-MIB-AC **Access:** Read-Only **Syntax:** Gauge32 **OID:** 1.3.111.3.37.238.9999.1.5.1.16 **Definition:** Indicates VLAN ID in use.
Group: ieeeC37238TCPortDataSetGroup **Object:** ifIeeeC37238TCPortDSDlyAsymm	**Agent Capability:** RC-IEEEC37-238-MIB-AC **Access:** not-implemented **Syntax:** Integer **OID:** 1.3.111.3.37.238.9999.1.7.16 Path delay asymmetry.

Group/Object	Description
Group: ieeeC37238TCPortDataSetGroup **Object:** ifIeeeC37238TCPortDSFaulty	**Agent Capability:** RC-IEEEC37-238-MIB-AC **Access:** Read-Only **Syntax:** Integer **OID:** 1.3.111.3.37.238.9999.1.7.1.4 **Definition:** True if the port is faulty and False if the port is operating normally. The initialization value shall be False.
Group: ieeeC37238TCPortDataSetGroup **Object:** ifIeeeC37238TCPortDSLMinPdlyRInt	**Agent Capability:** RC-IEEEC37-238-MIB-AC **Access:** Read-Only **Syntax:** Integer **OID:** 1.3.111.3.37.238.9999.1.7.1.3 **Definition:** The logarithm to the base 2 of the minPdelayReqInterval.
Group: ieeeC37238TCPortDataSetGroup **Object:** ifIeeeC37238TCPortDSMPathPDly	**Access:** Read-Only **Syntax:** IEEEC37238TimeInterval **OID:** 1.3.111.3.37.238.9999.1.7.1.5 **Definition:** The estimate of the current one-way propagation delay.
Group: ieeeC37238TCPortDataSetGroup **Object:** ifIeeeC37238TCPortDSPortNumber	**Access:** Read-Only **Syntax:** Gauge32 **OID:** 1.3.111.3.37.238.9999.1.7.1.2 **Definition:** Port number of the local port.

IF-MIB

Group/Object	Description
Group: IfGeneralInformationGroup **Object:** IfAdminStatus	**Agent Capability:** RC-IEEEC37-238-MIB-AC **Access:** Read-Write **Syntax:** Integer **OID:** .1.3.6.1.2.1.2.2.1.7.1 **Definition:** The desired state of the interface. The testing(3) state indicates that no operational packets can be passed. When a managed system initializes, all interfaces start with ifAdminStatus in the down(2) state. As a result of either explicit management action or per configuration information retained by the managed system, ifAdminStatus is then changed to either the up(1) or testing(3) states (or remains in the down(2) state). **Note** Support for the value **testing(3)** is not implemented per RFC 2863 compliance statement.
Group: IfGeneralInformationGroup **Object:** IfAlias	**Agent Capability:** RC-IF-MIB-AC **Syntax:** String **OID:** .1.3.6.1.2.1.31.1.1.1.18.1 **Definition:** This object is an **alias** name for the interface as specified by a network manager, and provides a non-volatile **handle** for the interface. On the first instantiation of an interface, the value of ifAlias associated with that interface is the zero-length string. As and when a value is written into an instance of ifAlias through a network management set operation, then

Group/Object	Description
	the agent must retain the supplied value in the ifAlias instance associated with the same interface for as long as that interface remains instantiated, including across all re- initializations/reboots of the network management system, including those which result in a change of the interface's ifIndex value. An example of the value which a network manager might store in this object for a WAN interface is the (Telco's) circuit number/identifier of the interface. Some agents may support write-access only for interfaces having particular values of ifType. An agent which supports write access to this object is required to keep the value in non-volatile storage, but it may limit the length of new values depending on how much storage is already occupied by the current values for other interfaces. **Note** String length is limited to 15 characters.
Group: IfGeneralInformationGroup **Object:** IfConnectorPresent	**Agent Capability:** RC-IF-MIB-AC **Access:** Read-Only **Syntax:** Integer **OID:** .1.3.6.1.2.1.31.1.1.1.17.1 **Definition:** This object has the value **true(1)** if the interface sublayer has a physical connector and the value **false(2)** otherwise.
Group: IfCounterDiscontinuityGroup **Object:** IfCounterDiscontinuityTime	**Access:** Read-Only **Syntax:** Timeticks **OID:** .1.3.6.1.2.1.31.1.1.1.19.1 **Definition:** The value of sysUpTime on the most recent occasion at which any one or more of this interface's counters suffered a discontinuity. The relevant counters are the specific instances associated with this interface of any Counter32 or
Group: IfGeneralInformationGroup **Object:** IfDescr	**Access:** Read-Only **Syntax:** String **OID:** .1.3.6.1.2.1.2.2.1.2.1 **Definition:** A textual string containing information about the interface This string should include the name of the manufacturer, the product name and the version of the interface hardware/software.
Group: IfVHCPacketGroup **Object:** IfHCInBroadcastPkts	**Access:** Read-Only **Definition:** Counter64 **OID:** .1.3.6.1.2.1.31.1.1.1.9.1 **Definition:** Counter64 object contained in the ifTable or ifXTable. If no such discontinuities have occurred since the last re- initialization of the local management subsystem, then this object contains a zero value.
Group: IfVHCPacketGroup **Object:** IfHCInMulticastPkts	**Access:** Read-Only **Definition:** Counter64 **OID:** .1.3.6.1.2.1.31.1.1.1.8.1 **Definition:** The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were addressed to a multicast address at this sub-layer. For a MAC layer protocol, this includes both Group and Functional addresses. This object is a 64-bit version of ifInMulticastPkts. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime.

Group/Object	Description
Group: IfVHCPacketGroup **Object:** IfHCInOctets	**Access:** Read-Only **Definition:** Counter64 **OID:** .1.3.6.1.2.1.31.1.1.1.6.1 **Definition:** The total number of octets received on the interface, including framing characters. This object is a 64-bit version of ifInOctets. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime.
Group: IfVHCPacketGroup **Object:** IfHCInUcastPkts	**Access:** Read-Only **Definition:** Counter64 **OID:** .1.3.6.1.2.1.31.1.1.1.7.1 **Definition:** The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were not addressed to a multicast or broadcast address at this sub-layer. This object is a 64-bit version of ifInUcastPkts. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime.
Group: IfVHCPacketGroup **Object:** IfHCOutBroadcastPkts	**Access:** Read-Only **Definition:** Counter64 **OID:** .1.3.6.1.2.1.31.1.1.1.13.1 **Definition:** The total number of packets that higher-level protocols requested be transmitted, and which were addressed to a broadcast address at this sub-layer, including those that were discarded or not sent. This object is a 64-bit version of ifOutBroadcastPkts. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime.
Group: IfVHCPacketGroup **Object:** IfHCOutMulticastPkts	**Access:** Read-Only **Definition:** Counter64 **OID:** .1.3.6.1.2.1.31.1.1.1.12.1 **Definition:** The total number of packets that higher-level protocols requested be transmitted, and which were addressed to a multicast address at this sub-layer, including those that were discarded or not sent. For a MAC layer protocol, this includes both Group and Functional addresses. This object is a 64-bit version of ifOutMulticastPkts. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime.
Group: IfVHCPacketGroup **Object:** IfHCOutOctets	**Access:** Read-Only **Definition:** Counter64 **OID:** .1.3.6.1.2.1.31.1.1.1.10.1 **Definition:** The total number of octets transmitted out of the interface, including framing characters. This object is a 64-bit version of ifOutOctets.
Group: IfVHCPacketGroup **Object:** IfHCOutUcastPkts	**Access:** Read-Only **Definition:** Counter64 **OID:** .1.3.6.1.2.1.31.1.1.1.11.1 **Definition:** The total number of packets that higher-level protocols requested be transmitted, and which were not addressed to a multicast or broadcast address at this sub-layer, including those that were discarded or not sent. This object is a 64-bit version of ifOutUcastPkts.

Group/Object	Description
Group: IfGeneralInformationGroup **Object:** IfHighSpeed	**Access:** Read-Only **Syntax:** Gauge32 **OID:** .1.3.6.1.2.1.31.1.1.1.15.1 **Definition:** An estimate of the interface's current bandwidth in units of 1,000,000 bits per second. If this object reports a value of **n** then the speed of the interface is somewhere in the range of **n-500,000** to **n+499,999**. For interfaces which do not vary in bandwidth or for those where no accurate estimation can be made, this object should contain the nominal bandwidth. For a sub-layer which has no concept of bandwidth, this object should be zero.
Group: IfVHCPacketGroup **Object:** IfInBroadcastPkts	**Access:** Read-Only **Syntax:** Counter32 **OID:** .1.3.6.1.2.1.31.1.1.1.3.1 **Definition:** The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were addressed to a broadcast address at this sub-layer. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime.
Group: IfGeneralInformationGroup **Object:** IfIndex	**Agent Capability:** RC-IEEEC37-238-MIB-AC **Access:** Read-Only **Syntax:** Integer **OID:** .1.3.6.1.2.1.2.2.1.1.1 **Definition:** A unique value, greater than zero, for each interface. It is recommended that values are assigned contiguously starting from 1. The value for each interface sub-layer must remain constant at least from one re-initialization of the entity's network management system to the next re-initialization. **Note** Creation and deletion of an entry in ifTable is not supported.
Group: IfVHCPacketGroup **Object:** IfInDiscards	**Access:** Read-Only **Syntax:** Counter32 **OID:** .1.3.6.1.2.1.2.2.1.13.1 **Definition:** The number of inbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. One possible reason for discarding such a packet could be to free up buffer space. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime.
Group: IfVHCPacketGroup **Object:** IfInErrors	**Access:** Read-Only **Syntax:** Counter32 **OID:** .1.3.6.1.2.1.2.2.1.14.1 **Definition:** For packet-oriented interfaces, the number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol. For character- oriented or fixed-length interfaces, the number of inbound transmission units that contained errors preventing them from being deliverable to a higher-layer protocol. Discontinuities in the value of

Group/Object	Description
	this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime.
Group: IfVHCPacketGroup **Object:** IfInMulticastPkts	**Access:** Read-Only **Syntax:** Counter32 **OID:** .1.3.6.1.2.1.31.1.1.1.2.1 **Definition:** The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were addressed to a multicast address at this sub-layer. For a MAC layer protocol, this includes both Group and Functional addresses. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime.
Group: IfVHCPacketGroup **Object:** IfInOctets	**Access:** Read-Only **Syntax:** Counter32 **OID:** .1.3.6.1.2.1.2.2.1.10.1 **Definition:** The total number of octets received on the interface, including framing characters. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime.
Group: IfVHCPacketGroup **Object:** IfInUcastPkts	**Access:** Read-Only **Syntax:** Counter32 **OID:** .1.3.6.1.2.1.2.2.1.11.1 **Definition:** The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were not addressed to a multicast or broadcast address at this sub-layer. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime.
Group: IfVHCPacketGroup **Object:** IfInUnknownProtos	**Access:** Read-Only **Syntax:** Counter32 **OID:** .1.3.6.1.2.1.2.2.1.15.1 **Definition:** For packet-oriented interfaces, the number of packets received via the interface which were discarded because of an unknown or unsupported protocol. For character-oriented or fixed-length interfaces that support protocol multiplexing the number of transmission units received via the interface which were discarded because of an unknown or unsupported protocol. For any interface that does not support protocol multiplexing, this counter will always be 0. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime.
Group: IfGeneralInformationGroup **Object:** IfLastChange	**Access:** Read-Only **Syntax:** Timeticks **OID:** .1.3.6.1.2.1.2.2.1.9.1 **Definition:** The value of sysUpTime at the time the interface entered its current operational state. If the current state was entered prior to the last re-initialization of the local network management subsystem, then this object contains a zero value.
Group: IfGeneralInformationGroup **Object:** IfLinkUpDownTrapEnable	**Access:** Read-Write **Syntax:** Integer **OID:** .1.3.6.1.2.1.31.1.1.1.14.1

Group/Object	Description
	Definition: Indicates whether linkUp/linkDown traps should be generated for this interface. By default, this object should have the value enabled(1) for interfaces which do not operate on **top** of any other interface (as defined in the ifStackTable), and disabled(2) otherwise.
Group: IfVHCPacketGroup **Object:** IfMtu	**Access:** Read-Only **Syntax:** Integer **OID:** .1.3.6.1.2.1.2.2.1.4.1 **Definition:** The size of the largest packet which can be sent/received on the interface, specified in octets. For interfaces that are used for transmitting network datagrams, this is the size of the largest network datagram that can be sent on the interface.
Group: IfGeneralInformationGroup **Object:** IfName	**Access:** Read-Only **Syntax:** String **OID:** .1.3.6.1.2.1.31.1.1.1.1.1 **Definition:** The textual name of the interface. The value of this object should be the name of the interface as assigned by the local device and should be suitable for use in commands entered at the device's **console**. This might be a text name, such as **le0** or a simple port number, such as **1**, depending on the interface naming syntax of the device. If several entries in the ifTable together represent a single interface as named by the device, then each will have the same value of ifName. Note that for an agent which responds to SNMP queries concerning an interface on some other (proxied) device, then the value of ifName for such an interface is the proxied device's local name for it. If there is no local name, or this object is otherwise not applicable, then this object contains a zero-length string.
Group: IfGeneralInformationGroup **Object:** IfNumber	**Access:** Read-Only **Syntax:** Integer **OID:** .1.3.6.1.2.1.2.1.0 **Definition:** The number of network interfaces (regardless of their current state) present on this system.
Group: IfGeneralInformationGroup **Object:** IfOperStatus	**Agent Capability:** RC-IF-MIB-AC **Access:** Read-Only **Syntax:** Integer **OID:** .1.3.6.1.2.1.2.2.1.8.1 **Definition:** The current operational state of the interface. The testing(3) state indicates that no operational packets can be passed. If ifAdminStatus is down(2) then ifOperStatus should be down(2). If ifAdminStatus is changed to up(1) then ifOperStatus should change to up(1) if the interface is ready to transmit and receive network traffic; it should change to dormant(5) if the interface is waiting for external actions (such as a serial line waiting for an incoming connection); it should remain in the down(2) state if and only if there is a fault that prevents it from going to the up(1) state; it should remain in the notPresent(6) state if the interface has missing (typically, hardware) components. **Note** Information limited by Rugged Switch Agent for Read-Only object.
Group: IfVHCPacketGroup **Object:** IfOutBroadcastPkts	**Access:** Read-Only **Syntax:** Counter32

Group/Object	Description
	OID: .1.3.6.1.2.1.31.1.1.1.5.1 **Definition:** The total number of packets that higher-level protocols requested be transmitted, and which were addressed to a broadcast address at this sub-layer, including those that were discarded or not sent. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime.
Group: IfVHCPacketGroup **Object:** IfOutDiscards	**Access:** Read-Only **Syntax:** Counter32 **OID:** .1.3.6.1.2.1.2.2.1.19.1 **Definition:** The number of outbound packets which were chosen to be discarded even though no errors had been detected to prevent their being transmitted. One possible reason for discarding such a packet could be to free up buffer space. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime.
Group: IfVHCPacketGroup **Object:** IfOutErrors	**Access:** Read-Only **Syntax:** Counter32 **OID:** .1.3.6.1.2.1.2.2.1.20.1 **Definition:** For packet-oriented interfaces, the number of outbound packets that could not be transmitted because of errors. For character-oriented or fixed-length interfaces, the number of outbound transmission units that could not be transmitted because of errors. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime.
Group: IfVHCPacketGroup **Object:** IfOutMulticastPkts	**Access:** Read-Only **Syntax:** Counter32 **OID:** .1.3.6.1.2.1.31.1.1.1.4.1 **Definition:** The total number of packets that higher-level protocols requested be transmitted, and which were addressed to a multicast address at this sub-layer, including those that were discarded or not sent. For a MAC layer protocol, this includes both Group and Functional addresses. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime.
Group: IfVHCPacketGroup **Object:** IfOutOctets	**Access:** Read-Only **Syntax:** Counter32 **OID:** .1.3.6.1.2.1.2.2.1.16.1 **Definition:** The total number of octets transmitted out of the interface, including framing characters. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime.
Group: IfVHCPacketGroup **Object:** IfOutUcastPkts	**Access:** Read-Only **Syntax:** Counter32 **OID:** .1.3.6.1.2.1.2.2.1.17.1 **Definition:** The total number of packets that higher-level protocols requested be transmitted, and which were not addressed to a multicast or broadcast address at this sub-layer, including those that were discarded or not sent. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime.

Group/Object	Description
Group: IfGeneralInformationGroup **Object:** IfPhysAddress	**Access:** Read-Only **Syntax:** PhysAddress **OID:** .1.3.6.1.2.1.2.2.1.6.1 **Definition:** The interface's address at its protocol sub-layer. For example, for an 802.x interface, this object normally contains a MAC address. The interface's media-specific MIB must define the bit and byte ordering and the format of the value of this object. For interfaces which do not have such an address (e.g., a serial line), this object should contain an octet string of zero length.
Group: IfVHCPacketGroup **Object:** IfPromiscuousMode	**Agent Capability:** RC-IF-MIB-AC **Access:** Read-Only **Syntax:** Integer **OID:** .1.3.6.1.2.1.31.1.1.1.16.1 **Definition:** This object has a value of false(2) if this interface only accepts packets/frames that are addressed to this station. This object has a value of true(1) when the station accepts all packets/frames transmitted on the media. The value true(1) is only legal on certain types of media. If legal, setting this object to a value of true(1) may require the interface to be reset before becoming effective. The value of ifPromiscuousMode does not affect the reception of broadcast and multicast packets/frames by the interface. **Note** Write access is not implemented per RFC 2863 compliance statement. This mode is always **false(1)**.
Group: IfGeneralInformationGroup **Object:** IfSpeed	**Agent Capability:** RC-IF-MIB-AC **Access:** Read-Only **Syntax:** Integer **OID:** .1.3.6.1.2.1.2.2.1.5.1 **Definition:** An estimate of the interface's current bandwidth in bits per second. For interfaces which do not vary in bandwidth or for those where no accurate estimation can be made, this object should contain the nominal bandwidth. If the bandwidth of the interface is greater than the maximum value reportable by this object then this object should report its maximum value (4,294,967,295) and ifHighSpeed must be used to report the interace's speed. For a sub-layer which has no concept of bandwidth, this object should be zero.
Group: IfGeneralInformationGroup **Object:** IfTableLastChange	**Agent Capability:** RC-IF-MIB-AC **Access:** Read-Only **Syntax:** Timeticks **OID:** .1.3.6.1.2.1.31.1.5.0 **Definition:** The value of sysUpTime at the time of the last creation or deletion of an entry in the ifTable. If the number of entries has been unchanged since the last re-initialization of the local network management subsystem, then this object contains a zero value.
Group: IfGeneralInformationGroup **Object:** IfType	**Agent Capability:** RC-IP-MIB-AC **Access:** Read-Only **Syntax:** Integer **OID:** .1.3.6.1.2.1.2.2.1.3.1

Group/Object	Description
	Definition: The type of interface. Additional values for ifType are assigned by the Internet Assigned Numbers Authority (IANA), through updating the syntax of the IANAifType textual convention.

IP-MIB

Group/Object	Description
Group: icmpGroup **Object:** icmpInAddrMaskReps	**Access:** Read-Only **Syntax:** Counter32 **OID:** .1.3.6.1.2.1.5.13 **Definition:** The number of ICMP Address Mask Reply messages received.
Group: icmpGroup **Object:** icmpInAddrMasks	**Access:** Read-Only **Syntax:** Counter32 **OID:** .1.3.6.1.2.1.5.12 **Definition:** The number of ICMP Address Mask Request messages received.
Group: icmpGroup **Object:** icmpInDestUnreachs	**Access:** Read-Only **Syntax:** Counter32 **OID:** .1.3.6.1.2.1.5.3 **Definition:** The number of ICMP Destination Unreachable messages received.
Group: icmpGroup **Object:** icmpInEchoReps	**Access:** Read-Only **Syntax:** Counter32 **OID:** .1.3.6.1.2.1.5.9 **Definition:** The number of ICMP Echo Reply messages received.
Group: icmpGroup **Object:** icmpInEchos	**Access:** Read-Only **Syntax:** Counter32 **OID:** .1.3.6.1.2.1.5.8 **Definition:** The number of ICMP Echo (request) messages received.
Group: icmpGroup **Object:** icmpInErrors	**Access:** Read-Only **Syntax:** Counter32 **OID:** .1.3.6.1.2.1.5.2 **Definition:** The number of ICMP messages which the entity received but determined as having ICMP-specific errors (bad ICMP checksums, bad length, etc.).
Group: icmpGroup **Object:** icmpInMsgs	**Access:** Read-Only **Syntax:** Counter32 **OID:** .1.3.6.1.2.1.5.1 **Definition:** The total number of ICMP messages which the entity received. Note that this counter includes all those counted by icmpInErrors.
Group: icmpGroup **Object:** icmpInParmProbs	**Access:** Read-Only **Syntax:** Counter32 **OID:** .1.3.6.1.2.1.5.5 **Definition:** The number of ICMP Parameter Problem messages received.
Group: icmpGroup	**Access:** Read-Only

Group/Object	Description
Object: icmpInRedirects	**Syntax:** Counter32 **OID:** .1.3.6.1.2.1.5.7 **Definition:** The number of ICMP Redirect messages received.
Group: icmpGroup **Object:** icmpInSrcQuenchs	**Access:** Read-Only **Syntax:** Counter32 **OID:** .1.3.6.1.2.1.5.6 **Definition:** The number of ICMP Time Exceeded messages received.
Group: icmpGroup **Object:** icmpInTimeExcds	**Access:** Read-Only **Syntax:** Counter32 **OID:** .1.3.6.1.2.1.5.4 **Definition:** The number of ICMP Timestamp Reply messages received.
Group: icmpGroup **Object:** icmpInTimestampReps	**Access:** Read-Only **Syntax:** Counter32 **OID:** .1.3.6.1.2.1.5.11 **Definition:** The number of ICMP Timestamp Reply messages received.
Group: icmpGroup **Object:** icmpInTimestamps	**Access:** Read-Only **Syntax:** Counter32 **OID:** .1.3.6.1.2.1.5.10 **Definition:** The number of ICMP Timestamp (request) messages received.
Group: icmpGroup **Object:** icmpOutAddrMaskReps	**Access:** Read-Only **Syntax:** Counter32 **OID:** .1.3.6.1.2.1.5.26 **Definition:** The number of ICMP Address Mask Reply messages sent.
Group: icmpGroup **Object:** icmpOutDestUnreachs	**Access:** Read-Only **Syntax:** Counter32 **OID:** .1.3.6.1.2.1.5.16 **Definition:** The number of ICMP Destination Unreachable messages sent.
Group: icmpGroup **Object:** icmpOutEchoReps	**Access:** Read-Only **Syntax:** Counter32 **OID:** .1.3.6.1.2.1.5.22 **Definition:** The number of ICMP Echo Reply messages sent.
Group: icmpGroup **Object:** icmpOutErrors	**Access:** Read-Only **Syntax:** Counter32 **OID:** .1.3.6.1.2.1.5.15 **Definition:** The number of ICMP messages which this entity did not send due to problems discovered within ICMP such as a lack of buffers. This value should not include errors discovered outside the ICMP layer such as the inability of IP to route the resultant datagram. In some implementations there may be no types of error which contribute to this counter's value.
Group: icmpGroup **Object:** icmpOutMsgs	**Access:** Read-Only **Syntax:** Counter32 **OID:** .1.3.6.1.2.1.5.14

Group/Object	Description
	Definition: The total number of ICMP messages which this entity attempted to send. Note that this counter includes all those counted by icmpOutErrors.
Group: icmpGroup **Object:** icmpOutParmProbs	**Access:** Read-Only **Syntax:** Counter32 **OID:** .1.3.6.1.2.1.5.18 **Definition:** The number of ICMP Parameter Problem messages sent.
Group: icmpGroup **Object:** icmpOutRedirects	**Access:** Read-Only **Syntax:** Counter32 **OID:** .1.3.6.1.2.1.5.20 **Definition:** The number of ICMP Redirect messages sent. For a host, this object will always be zero, since hosts do not send redirects.
Group: icmpGroup **Object:** icmpOutSrcQuenchs	**Access:** Read-Only **Syntax:** Counter32 **OID:** .1.3.6.1.2.1.5.19 **Definition:** The number of ICMP Source Quench messages sent.
Group: icmpGroup **Object:** icmpOutTimeExcds	**Access:** Read-Only **Syntax:** Counter32 **OID:** .1.3.6.1.2.1.5.17 **Definition:** The number of ICMP Time Exceeded messages sent.
Group: icmpGroup **Object:** icmpOutTimestampReps	**Access:** Read-Only **Syntax:** Counter32 **OID:** .1.3.6.1.2.1.5.24 **Definition:** The number of ICMP Timestamp Reply messages sent.
Group: icmpGroup **Object:** icmpOutTimestamps	**Access:** Read-Only **Syntax:** Counter32 **OID:** .1.3.6.1.2.1.5.23 **Definition:** The number of ICMP Timestamp (request) messages sent.
Group: ipGroup **Object:** ipAdEntAddr	**Access:** Read-Only **Syntax:** IpAddress **OID:** .1.3.6.1.2.1.4.20.1.1.192.168.0.180 **Definition:** The IP address to which this entry's addressing information pertains.
Group: ipGroup **Object:** ipAdEntBcastAddr	**Access:** Read-Only **Syntax:** Integer **OID:** .1.3.6.1.2.1.4.20.1.4.192.168.0.180 **Definition:** The value of the least-significant bit in the IP broadcast address used for sending datagrams on the (logical) interface associated with the IP address of this entry. For example, when the Internet standard all-ones broadcast address is used, the value will be 1. This value applies to both the subnet and network broadcasts addresses used by the entity on this (logical) interface.
Group: ipGroup **Object:** ipAdEntIfIndex	**Access:** Read-Only **Syntax:** Integer **OID:** .1.3.6.1.2.1.4.20.1.2.192.168.0.180

Group/Object	Description
	Definition: The index value which uniquely identifies the interface to which this entry is applicable. The interface identified by a particular value of this index is the same interface as identified by the same value of RFC 1573's ifIndex.
Group: ipGroup **Object:** ipAdEntNetMask	**Access:** Read-Only **Syntax:** IpAddress **OID:** .1.3.6.1.2.1.4.20.1.3.192.168.0.180 **Definition:** The subnet mask associated with the IP address of this entry. The value of the mask is an IP address with all the network bits set to 1 and all the hosts bits set to 0.
Group: ipGroup **Object:** ipAdEntReasmMaxSize	**Access:** Read-Only **Syntax:** Integer **OID:** .1.3.6.1.2.1.4.20.1.5.192.168.0.180 **Definition:** The size of the largest IP datagram which this entity can re-assemble from incoming IP fragmented datagrams received on this interface.
Group: ipGroup **Object:** ipDefaultTTL	**Agent Capability:** RC-IP-MIB-AC **Access:** Read-Only **Syntax:** Integer **OID:** .1.3.6.1.2.1.4.2.0 **Definition:** The default value inserted into the Time-To-Live field of the IP header of datagrams originated at this entity, whenever a TTL value is not supplied by the transport layer protocol. **Note** Write access is not supported.
Group: ipGroup **Object:** ipForwarding	**Agent Capability:** RC-IP-MIB-AC **Access:** Read-Write **Syntax:** Integer **OID:** .1.3.6.1.2.1.4.1.0 **Definition:** The indication of whether this entity is acting as an IP router in respect to the forwarding of datagrams received by, but not addressed to, this entity. IP routers forward datagrams. IP hosts do not (except those source-routed via the host). **Note** Support for the value **forwarding(1)** is not implemented per RFC 2011.
Group: ipGroup **Object:** ipForwDatagrams	**Access:** Read-Only **Syntax:** Counter32 **OID:** .1.3.6.1.2.1.4.6.0 **Definition:** The number of input datagrams for which this entity was not their final IP destination, as a result of which an attempt was made to find a route to forward them to that final destination. In entities which do not act as IP routers, this counter will include only those packets which were Source-Routed via this entity, and the Source-Route option processing was successful.
Group: ipGroup	**Access:** Read-Only

Group/Object	Description
Object: ipFragCreates	**Syntax:** Counter32 **OID:** .1.3.6.1.2.1.4.19.0 **Definition:** The number of IP datagram fragments that have been generated as a result of fragmentation at this entity.
Group: ipGroup **Object:** ipFragFails	**Access:** Read-Only **Syntax:** Counter32 **OID:** .1.3.6.1.2.1.4.18.0 **Definition:** The number of IP datagrams that have been discarded because they needed to be fragmented at this entity but could not be, e.g., because their Don't Fragment flag was set.
Group: ipGroup **Object:** ipFragOKs	**Access:** Read-Only **Syntax:** Counter32 **OID:** .1.3.6.1.2.1.4.17.0 **Definition:** The number of IP datagrams that have been successfully fragmented at this entity.
Group: ipGroup **Object:** ipInAddrErrors	**Agent Capability:** RC-LLDP-MIB-AC **Access:** Read-Only **Syntax:** Counter32 **OID:** .1.3.6.1.2.1.4.5.0 **Definition:** The number of input datagrams discarded because the IP address in their IP header's destination field was not a valid address to be received at this entity. This count includes invalid addresses (e.g., 0.0.0.0) and addresses of unsupported Classes (e.g., Class E). For entities which are not IP routers and therefore do not forward datagrams, this counter includes datagrams discarded because the destination address was not a local address.
Group: ipGroup **Object:** ipInDelivers	**Access:** Read-Only **Syntax:** Counter32 **OID:** .1.3.6.1.2.1.4.9.0 **Definition:** The total number of input datagrams successfully delivered to IP user-protocols (including ICMP).
Group: ipGroup **Object:** ipInDiscards	**Access:** Read-Only **Syntax:** Counter32 **OID:** .1.3.6.1.2.1.4.8.0 **Definition:** The number of input IP datagrams for which no problems were encountered to prevent their continued processing, but which were discarded (e.g., for lack of buffer space). Note that this counter does not include any datagrams discarded while awaiting re-assembly.
Group: ipGroup **Object:** ipInHdrErrors	**Access:** Read-Only **Syntax:** Counter32 **OID:** .1.3.6.1.2.1.4.4.0 **Definition:** The number of input datagrams discarded due to errors in their IP headers, including bad checksums, version number mismatch, other format errors, time-to-live exceeded, errors discovered in processing their IP options, etc.
Group: ipGroup **Object:** ipInReceives	**Access:** Read-Only **Syntax:** Counter32

Group/Object	Description
	OID: .1.3.6.1.2.1.4.3.0 **Definition:** The total number of input datagrams received from interfaces, including those received in error.
Group: ipGroup **Object:** ipInUnknownProtos	**Access:** Read-Only **Syntax:** Counter32 **OID:** .1.3.6.1.2.1.4.7.0 **Definition:** The number of locally-addressed datagrams received successfully but discarded because of an unknown or unsupported protocol.
Group: ipGroup **Object:** ipNetToMediaIfIndex	**Access:** Read-Create **Syntax:** Integer **OID:** .1.3.6.1.2.1.4.22.1.1.1002.192.168.0.254 **Definition:** The interface on which this entry's equivalence is effective. The interface identified by a particular value of this index is the same interface as identified by the same value of RFC 1573's ifIndex.
Group: ipGroup **Object:** ipNetToMediaNetAddress	**Access:** Read-Create **Syntax:** IpAddress **OID:** .1.3.6.1.2.1.4.22.1.3.1002.192.168.0.254 **Definition:** The IpAddress corresponding to the media-dependent **physical** address.
Group: ipGroup **Object:** ipNetToMediaPhysAddress	**Access:** Read-Create **Syntax:** String **OID:** .1.3.6.1.2.1.4.22.1.2.1002.192.168.0.254 **Definition:** The media-dependent **physical** address.
Group: ipGroup **Object:** ipNetToMediaType	**Access:** Read-Create **Syntax:** Integer **OID:** .1.3.6.1.2.1.4.22.1.4.1002.192.168.0.254 **Definition:** The type of mapping. Setting this object to the value invalid(2) has the effect of invalidating the corresponding entry in the ipNetToMediaTable. That is, it effectively disassociates the interface identified with said entry from the mapping identified with said entry. It is an implementation- specific matter as to whether the agent removes an invalidated entry from the table. Accordingly, management stations must be prepared to receive tabular information from agents that corresponds to entries not currently in use. Proper interpretation of such entries requires examination of the relevant ipNetToMediaType object.
Group: ipGroup **Object:** ipOutDiscards	**Access:** Read-Only **Syntax:** Counter32 **OID:** .1.3.6.1.2.1.4.11.0 **Definition:** The number of output IP datagrams for which no problem was encountered to prevent their transmission to their destination, but which were discarded (e.g., for lack of buffer space). Note that this counter would include datagrams counted in ipForwDatagrams if any such packets met this (discretionary) discard criterion.
Group: ipGroup **Object:** ipOutNoRoutes	**Access:** Read-Only **Syntax:** Counter32 **OID:** .1.3.6.1.2.1.4.12.0

Group/Object	Description
	Definition: The number of IP datagrams discarded because no route could be found to transmit them to their destination. Note that this counter includes any packets counted in ipForwDatagrams which meet this **no-route** criterion. Note that this includes any datagrams which a host cannot route because all of its default routers are down.
Group: ipGroup **Object:** ipOutRequests	**Access:** Read-Only **Syntax:** Counter32 **OID:** .1.3.6.1.2.1.4.10.0 **Definition:** The total number of IP datagrams which local IP user-protocols (including ICMP) supplied to IP in requests for transmission. Note that this counter does not include any datagrams counted in ipForwDatagrams.
Group: ipGroup **Object:** ipReasmFails	**Access:** Read-Only **Syntax:** Counter32 **OID:** .1.3.6.1.2.1.4.16.0 **Definition:** The number of failures detected by the IP re-assembly algorithm (for whatever reason: timed out, errors, etc). Note that this is not necessarily a count of discarded IP fragments since some algorithms (notably the algorithm in RFC 815) can lose track of the number of fragments by combining them as they are received.
Group: ipGroup **Object:** ipReasmOKs	**Access:** Read-Only **Syntax:** Counter32 **OID:** .1.3.6.1.2.1.4.15.0 **Definition:** The number of IP datagrams successfully re-assembled.
Group: ipGroup **Object:** ipReasmReqds	**Access:** Read-Only **Syntax:** Counter32 **OID:** .1.3.6.1.2.1.4.14.0 **Definition:** The number of IP fragments received which needed to be reassembled at this entity.
Group: ipGroup **Object:** ipReasmTimeout	**Access:** Read-Only **Syntax:** Integer **OID:** .1.3.6.1.2.1.4.13.0 **Definition:** The maximum number of seconds which received fragments are held while they are awaiting reassembly at this entity.
Group: ipGroup **Object:** ipRoutingDiscards	**Access:** Read-Only **Syntax:** Counter32 **OID:** .1.3.6.1.2.1.4.23 **Definition:** The number of routing entries which were chosen to be discarded even though they are valid. One possible reason for discarding such an entry could be to free-up buffer space for other routing entries.

LLDP-MIB

Group/Object	Description
Group: lldpConfigTxGroup **Object:** lldpConfigManAddrPortsTxEnable	**Agent Capability:** RC-LLDP-MIB-AC **Access:** Read-Write **Syntax:** Hex-String

Group/Object	Description
	OID: .1.0.8802.1.1.2.1.1.7.1.1.4 **Definition:** A set of ports that are identified by a PortList, in which each port is represented as a bit. The corresponding local system management address instance will be transmitted on the member ports of the lldpManAddrPortsTxEnable. The default value for lldpConfigManAddrPortsTxEnable object is empty binary string, which means no ports are specified for advertising indicated management address instance. Write access is not implemented.
Group: lldpLocSysGroup **Object:** lldpLocChassisId	**Access:** Read-Only **Syntax:** Hex-String **OID:** .1.0.8802.1.1.2.1.3.2.0 **Definition:** The type of encoding used to identify the chassis associated with the local system.
Group: lldpLocSysGroup **Object:** lldpLocChassisIdSubtype	**Access:** Read-Only **Syntax:** Integer **OID:** .1.0.8802.1.1.2.1.3.1.0 **Definition:** The type of encoding used to identify the chassis associated with the local system.
Group: lldpLocSysGroup **Object:** lldpLocManAddrIfId	**Access:** Read-Only **Syntax:** Integer **OID:** .1.0.8802.1.1.2.1.3.8.1.5.192.168.0.180 **Definition:** The integer value used to identify the interface number regarding the management address component associated with the local system.
Group: lldpLocSysGroup **Object:** lldpLocManAddrIfSubtype	**Access:** Read-Only **Syntax:** Integer **OID:** .1.0.8802.1.1.2.1.3.8.1.4.192.168.0.180 **Definition:** The enumeration value that identifies the interface numbering method used for defining the interface number, associated with the local system.
Group: lldpLocSysGroup **Object:** lldpLocManAddrLen	**Access:** Read-Only **Syntax:** Integer **OID:** .1.0.8802.1.1.2.1.3.8.1.3 **Definition:** The total length of the management address subtype and the management address fields in LLDPDUs transmitted by the local LLDP agent. The management address length field is needed so that the receiving systems that do not implement SNMP will not be required to implement an iana family numbers/address length equivalency table in order to decode the management adress.
Group: lldpLocSysGroup **Object:** lldpLocManAddrOID	**Access:** Read-Only **Syntax:** OID **OID:** .1.0.8802.1.1.2.1.3.8.1.6.192.168.0.180 **Definition:** The OID value used to identify the type of hardware component or protocol entity associated with the management address advertised by the local system agent.
Group: lldpLocSysGroup **Object:** lldpLocPortDesc	**Access:** Read-Only **Syntax:** String

Group/Object	Description
	OID: .1.0.8802.1.1.2.1.3.7.1.4.1 **Definition:** The string value used to identify the 802 LAN station's port description associated with the local system. If the local agent supports IETF RFC 2863, lldpLocPortDesc object should have the same value of ifDescr object.
Group: lldpLocSysGroup **Object:** lldpLocPortId	**Access:** Read-Only **Syntax:** String **OID:** .1.0.8802.1.1.2.1.3.7.1.3.1 **Definition:** The string value used to identify the port component associated with a given port in the local system.
Group: lldpLocSysGroup **Object:** lldpLocPortIdSubtype	**Access:** Read-Only **Syntax:** Integer **OID:** .1.0.8802.1.1.2.1.3.7.1.2.1 **Definition:** The type of port identifier encoding used in the associated **lldpLocPortId** object.
Group: lldpLocSysGroup **Object:** lldpLocSysCapEnabled	**Access:** Read-Only **Syntax:** Hex-String **OID:** .1.0.8802.1.1.2.1.3.6.0 **Definition:** The bitmap value used to identify which system capabilities are enabled on the local system.
Group: lldpLocSysGroup **Object:** lldpLocSysCapSupported	**Access:** Read-Only **Syntax:** Hex-String **OID:** .1.0.8802.1.1.2.1.3.5.0 **Definition:** The bitmap value used to identify which system capabilities are supported on the local system.
Group: lldpLocSysGroup **Object:** lldpLocSysDesc	**Access:** Read-Only **Syntax:** String **OID:** .1.0.8802.1.1.2.1.3.4.0 **Definition:** The string value used to identify the system description of the local system. If the local agent supports IETF RFC 3418, lldpLocSysDesc object should have the same value of sysDesc object.
Group: lldpLocSysGroup **Object:** lldpLocSysName	**Access:** Read-Only **Syntax:** String **OID:** .1.0.8802.1.1.2.1.3.3.0 **Definition:** The string value used to identify the system name of the local system. If the local agent supports IETF RFC 3418, lldpLocSysName object should have the same value of sysName object.
Group: lldpConfigTxGroup **Object:** lldpMessageTxHoldMultiplier	**Access:** Read-Write **Syntax:** Integer **OID:** .1.0.8802.1.1.2.1.1.2.0 **Definition:** The time-to-live value expressed as a multiple of the lldpMessageTxInterval object. The actual time-to-live value used in LLDP frames, transmitted on behalf of this LLDP agent, can be expressed by the following formula: TTL = min(65535, (lldpMessageTxInterval * lldpMessageTxHoldMultiplier)) For example, if the value of lldpMessageTxInterval is **30**, and the value of lldpMessageTxHoldMultiplier is **4**, then the value **120** is encoded in the TTL field in the LLDP header. The

Group/Object	Description
	default value for lldpMessageTxHoldMultiplier object is 4. The value of this object must be restored from non-volatile storage after a re-initialization of the management system.
Group: lldpConfigTxGroup **Object:** lldpMessageTxInterval	**Access:** Read-Write **Syntax:** Integer **OID:** .1.0.8802.1.1.2.1.1.1.0 **Definition:** The interval at which LLDP frames are transmitted on behalf of this LLDP agent. The default value for lldpMessageTxInterval object is 30 seconds. The value of this object must be restored from non-volatile storage after a re-initialization of the management system.
Group: lldpConfigRxGroup **Object:** lldpNotificationInterval	**Agent Capability:** RC-LLDP-MIB-AC **Access:** Read-Write **Syntax:** Integer **OID:** .1.0.8802.1.1.2.1.1.5.0 **Definition:** This object controls the transmission of LLDP notifications. The agent must not generate more than one lldpRemTablesChange notification-event in the indicated period, where a **notification-event** is the transmission of a single notification PDU type to a list of notification destinations. If additional changes in lldpRemoteSystemsData object groups occur within the indicated throttling period, then these trap-events must be suppressed by the agent. An NMS should periodically check the value of lldpStatsRemTableLastChangeTime to detect any missed lldpRemTablesChange notification-events, e.g. due to throttling or transmission loss. If notification transmission is enabled for particular ports, the suggested default throttling period is 5 seconds. The value of this object must be restored from non-volatile storage after a re-initialization of the management system. **Note** Write access is not implemented.
Group: lldpConfigGroup **Object:** lldpPortConfigAdminStatus	**Access:** Read-Write **Syntax:** Integer **OID:** .1.0.8802.1.1.2.1.1.6.1.2.1 **Definition:** The administratively desired status of the local LLDP agent. If the associated lldpPortConfigAdminStatus object has a value of **txOnly(1)**, then LLDP agent will transmit LLDP frames on this port and it will not store any information about the remote systems connected. If the associated lldpPortConfigAdminStatus object has a value of **rxOnly(2)**, then the LLDP agent will receive, but it will not transmit LLDP frames on this port. If the associated lldpPortConfigAdminStatus object has a value of **txAndRx(3)**, then the LLDP agent will transmit and receive LLDP frames on this port. If the associated lldpPortConfigAdminStatus object has a value of **disabled(4)**, then LLDP agent will not transmit or receive LLDP frames on this port. If there is remote systems information which is received on this port and stored in other tables, before the port's lldpPortConfigAdminStatus becomes disabled, then the information will naturally age out.
Group: lldpConfigRxGroup **Object:** lldpPortConfigNotificationEnable	**Access:** Read-Write **Syntax:** Integer **OID:** .1.0.8802.1.1.2.1.1.6.1.3.1

Group/Object	Description
	Definition: The lldpPortConfigNotificationEnable controls, on a per port basis, whether or not notifications from the agent are enabled. The value true(1) means that notifications are enabled; the value false(2) means that they are not.
Group: lldpConfigTxGroup **Object:** lldpPortConfigTLVsTxEnable	**Agent Capability:** RC-LLDP-MIB-AC **Access:** Read-Write **Syntax:** Hex-String **OID:** .1.0.8802.1.1.2.1.1.6.1.4.1 **Definition:** The lldpPortConfigTLVsTxEnable, defined as a bitmap, includes the basic set of LLDP TLVs whose transmission is allowed on the local LLDP agent by the network management. Each bit in the bitmap corresponds to a TLV type associated with a specific optional TLV. It should be noted that the organizationally-specific TLVs are excluded from the lldpTLVsTxEnable bitmap. LLDP Organization Specific Information Extension MIBs should have similar configuration object to control transmission of their organizationally defined TLVs. The bit **portDesc(0)** indicates that LLDP agent should transmit **Port Description TLV**. The bit **sysName(1)** indicates that LLDP agent should transmit **System Name TLV**. The bit **sysDesc(2)** indicates that LLDP agent should transmit **System Description TLV**. The bit **sysCap(3)** indicates that LLDP agent should transmit **System Capabilities TLV**. There is no bit reserved for the management address TLV type since transmission of management address TLVs are controlled by another object, lldpConfigManAddrTable. The default value for lldpPortConfigTLVsTxEnable object is empty set, which means no enumerated values are set. The value of this object must be restored from non-volatile storage after a re-initialization of the management system. Write access is not implemented.
Group: lldpConfigTxGroup **Object:** lldpReinitDelay	**Access:** Read-Write **Syntax:** Integer **OID:** .1.0.8802.1.1.2.1.1.3.0 **Definition:** The lldpReinitDelay indicates the delay (in units of seconds) from when lldpPortConfigAdminStatus object of a particular port becomes **disabled** until re-initialization will be attempted. The default value for lldpReintDelay object is two seconds. The value of this object must be restored from non-volatile storage after a re-initialization of the management system.
Group: lldpRemSysGroup **Object:** lldpRemChassisId	**Access:** Read-Only **Syntax:** Hex-String **OID:** .1.0.8802.1.1.2.1.4.1.1.5.3496.7.1 **Definition:** The string value used to identify the chassis component associated with the remote system.
Group: lldpRemSysGroup **Object:** lldpRemChassisIdSubtype	**Access:** Read-Only **Syntax:** Integer **OID:** .1.0.8802.1.1.2.1.4.1.1.4.3496.7.1 **Definition:** The type of encoding used to identify the chassis associated with the remote system.
Group: lldpRemSysGroup **Object:** lldpRemManAddrIfId	**Access:** Read-Only **Syntax:** Integer **OID:** .1.0.8802.1.1.2.1.4.2.1.4.3496.7.1.1.4.192.168.0.20

Group/Object	Description
	Definition: The integer value used to identify the interface number regarding the management address component associated with the remote system.
Group: lldpRemSysGroup **Object:** lldpRemManAddrIfSubtype	**Access:** Read-Only **Syntax:** Integer **OID:** .1.0.8802.1.1.2.1.4.2.1.3.3496.7.1.1.4.192.168.0.20 **Definition:** The enumeration value that identifies the interface numbering method used for defining the interface number, associated with the remote system.
Group: lldpRemSysGroup **Object:** lldpRemManAddrOID	**Access:** Read-Only **Syntax:** OID **OID:** .1.0.8802.1.1.2.1.4.2.1.5.6036.6.1.1.4.192.168.0.33 **Definition:** The OID value used to identify the type of hardware component or protocol entity associated with the management address advertised by the remote system agent.
Group: lldpRemSysGroup **Object:** lldpRemOrgDefInfo	**Access:** Read-Only **Syntax:** String **OID:** .1.0.8802.1.1.2.1.4.4.1.4 **Definition:** This table contains one or more rows per physical network connection which advertises the organizationally defined information. Note that this table contains one or more rows of organizationally defined information that is not recognized by the local agent. If the local system is capable of recognizing any organizationally defined information, appropriate extension MIBs from the organization should be used for information retrieval.
Group: lldpRemSysGroup **Object:** lldpRemPortDesc	**Access:** Read-Only **Syntax:** String **OID:** .1.0.8802.1.1.2.1.4.1.1.8 **Definition:** The string value used to identify the description of the given port associated with the remote system.
Group: lldpRemSysGroup **Object:** lldpRemPortId	**Access:** Read-Only **Syntax:** String **OID:** .1.0.8802.1.1.2.1.4.1.1.7.3496.7.1 **Definition:** The string value used to identify the port component associated with the remote system.
Group: lldpRemSysGroup **Object:** lldpRemPortIdSubtype	**Access:** Read-Only **Syntax:** Integer **OID:** .1.0.8802.1.1.2.1.4.1.1.6.3496.7.1 **Definition:** The type of port identifier encoding used in the associated **lldpRemPortId** object.
Group: lldpRemSysGroup **Object:** lldpRemSysCapEnabled	**Access:** Read-Only **Syntax:** Hex-String **OID:** .1.0.8802.1.1.2.1.4.1.1.12.3496.7.1 **Definition:** The bitmap value used to identify which system capabilities are enabled on the remote system.
Group: lldpRemSysGroup **Object:** lldpRemSysCapSupported	**Access:** Read-Only **Syntax:** Hex-String

Group/Object	Description
	OID: .1.0.8802.1.1.2.1.4.1.1.11.3496.7.1 **Definition:** The bitmap value used to identify which system capabilities are supported on the remote system.
Group: lldpRemSysGroup **Object:** lldpRemSysDesc	**Access:** Read-Only **Syntax:** String **OID:** .1.0.8802.1.1.2.1.4.1.1.10.3496.7.1 **Definition:** The string value used to identify the system description of the remote system.
Group: lldpRemSysGroup **Object:** lldpRemSysName	**Access:** Read-Only **Syntax:** String **OID:** .1.0.8802.1.1.2.1.4.1.1.9.3496.7.1 **Definition:** The string value used to identify the system name of the remote system.
Group: lldpNotificationsGroup **Object:** lldpRemTablesChange	**Syntax:** String **OID:** 1.0.8802.1.1.2.0.0.1.0 **Definition:** A lldpRemTablesChange notification is sent when the value of lldpStatsRemTableLastChangeTime changes. It can be utilized by an NMS to trigger LLDP remote systems table maintenance polls. Note that transmission of lldpRemTablesChange notifications are throttled by the agent, as specified by the **lldpNotificationInterval** object.
Group: lldpRemSysGroup **Object:** lldpRemUnknownTLVInfo	**Access:** Read-Only **Syntax:** String **OID:** 1.0.8802.1.1.2.1.4.3.1.2 **Definition:** This object represents the value extracted from the value field of the TLV.
Group: lldpStatsRxGroup **Object:** lldpStatsRemTablesLastChangeTime	**Access:** Read-Only **Syntax:** Timeticks **OID:** .1.0.8802.1.1.2.1.2.1.0 **Definition:** The value of sysUpTime object (defined in IETF RFC 3418) at the time an entry is created, modified, or deleted in the in tables associated with the lldpRemoteSystemsData objects and all LLDP extension objects associated with remote systems. An NMS can use this object to reduce polling of the lldpRemoteSystemsData objects.
Group: lldpStatsRxGroup **Object:** lldpStatsRxPortAgeoutsTotal	**Access:** Read-Only **Syntax:** Counter32 **OID:** .1.0.8802.1.1.2.1.2.7.1.7.1 **Definition:** The counter that represents the number of age-outs that occurred on a given port. An age-out is the number of times the complete set of information advertised by a particular MSAP has been deleted from tables contained in lldpRemoteSystemsData and lldpExtensions objects because the information timeliness interval has expired. This counter is similar to lldpStatsRemTablesAgeouts, except that the counter is on a per port basis. This enables NMS to poll tables associated with the lldpRemoteSystemsData objects and all LLDP extension objects associated with remote systems on the indicated port only. This counter should be set to zero during agent initialization and its value should not be saved in non-volatile storage. When a port's admin status changes from **disabled** to **rxOnly**, **txOnly** or **txAndRx**, the counter associated with the same port should reset to 0. The agent should also flush all remote system information associated with the same

Group/Object	Description
	port. This counter should be incremented only once when the complete set of information is invalidated (aged out) from all related tables on a particular port. Partial aging is not allowed, and thus, should not change the value of this counter.
Group: lldpStatsRxGroup **Object:** lldpStatsRxPortFramesDiscardedTotal	**Access:** Read-Only **Syntax:** Counter32 **OID:** .1.0.8802.1.1.2.1.2.7.1.2.1 **Definition:** The number of LLDP frames received by this LLDP agent on the indicated port, and then discarded for any reason. This counter can provide an indication that LLDP header formating problems may exist with the local LLDP agent in the sending system or that LLDPDU validation problems may exist with the local LLDP agent in the receiving system.
Group: lldpStatsRxGroup **Object:** lldpStatsRxPortFramesErrors	**Access:** Read-Only **Syntax:** Counter32 **OID:** .1.0.8802.1.1.2.1.2.7.1.3.1 **Definition:** The number of invalid LLDP frames received by this LLDP agent on the indicated port, while this LLDP agent is enabled.
Group: lldpStatsRxGroup **Object:** lldpStatsRxPortFramesTotal	**Access:** Read-Only **Syntax:** Counter32 **OID:** .1.0.8802.1.1.2.1.2.7.1.4.1 **Definition:** The number of valid LLDP frames received by this LLDP agent on the indicated port, while this LLDP agent is enabled.
Group: lldpStatsRxGroup **Object:** lldpStatsRxPortTLVsDiscardedTotal	**Access:** Read-Only **Syntax:** Counter32 **OID:** .1.0.8802.1.1.2.1.2.7.1.5.1 **Definition:** The number of LLDP TLVs discarded for any reason by this LLDP agent on the indicated port.
Group: lldpStatsRxGroup **Object:** lldpStatsRxPortTLVsUnrecognizedTotal	**Access:** Read-Only **Syntax:** Counter32 **OID:** .1.0.8802.1.1.2.1.2.7.1.6.1 **Definition:** The number of LLDP TLVs received on the given port that are not recognized by this LLDP agent on the indicated port. An unrecognized TLV is referred to as the TLV whose type value is in the range of reserved TLV types (000 1001 - 111 1110) in Table 9.1 of IEEE Std 802.1AB-2005. An unrecognized TLV may be a basic management TLV from a later LLDP version.
Group: lldpStatsTxGroup **Object:** lldpStatsTxPortFramesTotal	**Access:** Read-Only **Syntax:** Counter32 **OID:** .1.0.8802.1.1.2.1.2.6.1.2.1 **Definition:** The number of LLDP frames transmitted by this LLDP agent on the indicated port.
Group: lldpConfigTxGroup **Object:** lldpTxDelay	**Access:** Read-Write **Syntax:** Integer **OID:** .1.0.8802.1.1.2.1.1.4.0 **Definition:** The lldpTxDelay indicates the delay (in units of seconds) between successive LLDP frame transmissions initiated by value/status changes in the LLDP local systems MIB. The recommended value for the lldpTxDelay is set by the following formula:

Group/Object	Description
	1 <= lldpTxDelay <= (0.25 * lldpMessageTxInterval) The default value for lldpTxDelay object is two seconds. The value of this object must be restored from non-volatile storage after a re-initialization of the management system.

Q-BRIDGE-MIB

Group/Object	Description
Group: qBridgeFdbUnicastGroup **Object:** dot1qFdbDynamicCount	**Access:** Read-Only **Syntax:** Counter32 **OID:** .1.3.6.1.2.1.17.7.1.2.1.1.2.255.148.184.197.5.176.0 **Definition:** The current number of dynamic entries in this Filtering Database.
Group: qBridgeServiceRequirementsGroup **Object:** dot1qForwardAllForbiddenPorts	**Agent Capability:** RC-Q-BRIDGE-MIB-AC **Access:** Read-Only **Syntax:** Hex-String **OID:** .1.3.6.1.2.1.17.7.1.2.4.1.3.22 **Definition:** The set of ports configured by management in this VLAN for which the Service Requirement attribute Forward All Multicast Groups may not be dynamically registered by GMRP. This value will be restored after the device is reset. A port may not be added in this set if it is already a member of the set of ports in dot1qForwardAllStaticPorts. The default value is a string of zeros of appropriate length. The value of this object MUST be retained across reinitializations of the management system.
Group: qBridgeServiceRequirementsGroup **Object:** dot1qForwardAllPorts	**Access:** Read-Only **Syntax:** Hex-String **OID:** .1.3.6.1.2.1.17.7.1.2.4.1.1.22 **Definition:** The complete set of ports in this VLAN to which all multicast group-addressed frames are to be forwarded. This includes ports for which this need has been determined dynamically by GMRP, or configured statically by management.
Group: qBridgeServiceRequirementsGroup **Object:** dot1qForwardAllStaticPorts	**Agent Capability:** RC-Q-BRIDGE-MIB-AC **Access:** Read-Only **Syntax:** Hex-String **OID:** .1.3.6.1.2.1.17.7.1.2.4.1.2.22 **Definition:** The set of ports configured by management in this VLAN to which all multicast group-addressed frames are to be forwarded. Ports entered in this list will also appear in the complete set shown by dot1qForwardAllPorts. This value will be restored after the device is reset. This only applies to ports that are members of the VLAN, defined by dot1qVlanCurrentEgressPorts. A port may not be added in this set if it is already a member of the set of ports in dot1qForwardAllForbiddenPorts. The default value is a string of ones of appropriate length, to indicate the standard behaviour of using basic filtering services, i.e., forward all multicasts to all ports. The value of this object MUST be retained across reinitializations of the management system.
Group: qBridgeServiceRequirementsGroup **Object:** dot1qForwardUnregisteredForbiddenPorts	**Access:** Read-Write **Syntax:** Hex-String **OID:** .1.3.6.1.2.1.17.7.1.2.5.1.3.22

Group/Object	Description
	Definition: The set of ports configured by management in this VLAN for which the Service Requirement attribute Forward Unregistered Multicast Groups may not be dynamically registered by GMRP. This value will be restored after the device is reset. A port may not be added in this set if it is already a member of the set of ports in dot1qForwardUnregisteredStaticPorts. The default value is a string of zeros of appropriate length. The value of this object MUST be retained across reinitializations of the management system.
Group: qBridgeServiceRequirementsGroup **Object:** dot1qForwardUnregisteredPorts	**Access:** Read-Only **Syntax:** Hex-String **OID:** .1.3.6.1.2.1.17.7.1.2.5.1.1.22 **Definition:** The complete set of ports in this VLAN to which multicast group-addressed frames for which there is no more specific forwarding information will be forwarded. This includes ports for which this need has been determined dynamically by GMRP, or configured statically by management.
Group: qBridgeServiceRequirementsGroup **Object:** dot1qForwardUnregisteredStaticPorts	**Access:** Read-Write **Syntax:** Hex-String **OID:** .1.3.6.1.2.1.17.7.1.2.5.1.2.22 **Definition:** The set of ports configured by management, in this VLAN, to which multicast group-addressed frames for which there is no more specific forwarding information are to be forwarded. Ports entered in this list will also appear in the complete set shown by dot1qForwardUnregisteredPorts. This value will be restored after the device is reset. A port may not be added in this set if it is already a member of the set of ports in dot1qForwardUnregisteredForbiddenPorts. The default value is a string of zeros of appropriate length, although this has no effect with the default value of dot1qForwardAllStaticPorts. The value of this object MUST be retained across reinitializations of the management system.
Group: qBridgeBaseGroup **Object:** dot1qGvrpStatus	**Access:** Read-Write **Syntax:** Integer **OID:** .1.3.6.1.2.1.17.7.1.1.5.0 **Definition:** The administrative status requested by management for GVRP. The value enabled(1) indicates that GVRP should be enabled on this device, on all ports for which it has not been specifically disabled. When disabled(2), GVRP is disabled on all ports, and all GVRP packets will be forwarded transparently. This object affects all GVRP Applicant and Registrar state machines. A transition from disabled(2) to enabled(1) will cause a reset of all GVRP state machines on all ports. The value of this object MUST be retained across reinitializations of the management system.
Group: qBridgeBaseGroup **Object:** dot1qMaxSupportedVlans	**Access:** Read-Only **Syntax:** Gauge32 **OID:** .1.3.6.1.2.1.17.7.1.1.3.0 **Definition:** The maximum number of IEEE 802.1Q VLANs that this device supports.
Group: qBridgeBaseGroup **Object:** dot1qMaxVlanId	**Access:** Read-Only **Syntax:** Integer **OID:** .1.3.6.1.2.1.17.7.1.1.2.0 **Definition:** The maximum IEEE 802.1Q VLAN-ID that this device supports.
Group: qBridgeVlanStaticGroup	**Access:** Read-Only

Group/Object	Description
Object: dot1qNextFreeLocalVlanIndex	**Syntax:** Integer **OID:** .1.3.6.1.2.1.17.7.1.4.4.0 **Definition:** The next available value for dot1qVlanIndex of a local VLAN entry in dot1qVlanStaticTable. This will report values >=4096 if a new Local VLAN may be created or else the value 0 if this is not possible. A row creation operation in this table for an entry with a local VlanIndex value may fail if the current value of this object is not used as the index. Even if the value read is used, there is no guarantee that it will still be the valid index when the create operation is attempted; another manager may have already got in during the intervening time interval. In this case, dot1qNextFreeLocalVlanIndex should be re-read and the creation re-tried with the new value. This value will automatically change when the current value is used to create a new row.
Group: qBridgeBaseGroup **Object:** dot1qNumVlans	**Access:** Read-Only **Syntax:** Gauge32 **OID:** .1.3.6.1.2.1.17.7.1.1.4.0 **Definition:** The current number of IEEE 802.1Q VLANs that are configured in this device.
Group: qBridgePortGroup2 **Object:** dot1qPortAcceptableFrameTypes	**Agent Capability:** RC-Q-BRIDGE-MIB-AC **Access:** Read-Write **Syntax:** Integer **OID:** .1.3.6.1.2.1.17.7.1.4.5.1.2.1 **Definition:** When this is admitOnlyVlanTagged(2), the device will discard untagged frames or Priority-Tagged frames received on this port. When admitAll(1), untagged frames or Priority-Tagged frames received on this port will be accepted and assigned to a VID based on the PVID and VID Set for this port. This control does not affect VLAN-independent Bridge Protocol Data Unit (BPDU) frames, such as GVRP and Spanning Tree Protocol (STP). It does affect VLAN- dependent BPDU frames, such as GMRP. The value of this object MUST be retained across reinitializations of the management system. **Note** The value of **admitOnlyVlanTagged(2)** is not supported.
Group: qBridgePortGroup2 **Object:** dot1qPortGvrpStatus	**Agent Capability:** RC-Q-BRIDGE-MIB-AC **Access:** Read-Write **Syntax:** Integer **OID:** .1.3.6.1.2.1.17.7.1.4.5.1.4.1 **Definition:** The state of GVRP operation on this port. The value enabled(1) indicates that GVRP is enabled on this port, as long as dot1qGvrpStatus is also enabled for this device. When disabled(2) but dot1qGvrpStatus is still enabled for the device, GVRP is disabled on this port: any GVRP packets received will be silently discarded, and no GVRP registrations will be propagated from other ports. This object affects all GVRP Applicant and Registrar state machines on this port. A transition from disabled(2) to enabled(1) will cause a reset of all GVRP state machines on this port. The value of this object MUST be retained across reinitializations of the management system. **Note** The default value is **disabled(2)**.

Group/Object	Description
Group: qBridgePortGroup2 **Object:** dot1qPortIngressFiltering	**Agent Capability:** RC-Q-BRIDGE-MIB-AC **Access:** Read-Write **Syntax:** Integer **OID:** .1.3.6.1.2.1.17.7.1.4.5.1.3.1 **Definition:** When this is true(1), the device will discard incoming frames for VLANs that do not include this Port in its Member set. When false(2), the port will accept all incoming frames. This control does not affect VLAN-independent BPDU frames, such as GVRP and STP. It does affect VLAN-dependent BPDU frames, such as GMRP. The value of this object MUST be retained across reinitializations of the management system. **Note** The value **true(1)** is not supported.
Group: qBridgePortGroup2 **Object:** dot1qPvid	**Access:** Read-Write **Syntax:** Gauge32 **OID:** .1.3.6.1.2.1.17.7.1.4.5.1.1.1 **Definition:** The PVID, the VLAN-ID assigned to untagged frames or Priority-Tagged frames received on this port. The value of this object MUST be retained across reinitializations of the management system.
Group: qBridgeFdbUnicastGroup **Object:** dot1qTpFdbPort	**Access:** Read-Only **Syntax:** Integer **OID:** .1.3.6.1.2.1.17.7.1.2.2.1.2.255.148.184.197.5.176.0 **Definition:** Either the value **0**, or the port number of the port on which a frame having a source address equal to the value of the corresponding instance of dot1qTpFdbAddress has been seen. A value of **0** indicates that the port number has not been learned but that the device does have some forwarding/filtering information about this address (e.g., in the dot1qStaticUnicastTable). Implementors are encouraged to assign the port value to this object whenever it is learned, even for addresses for which the corresponding value of dot1qTpFdbStatus is not learned(3).
Group: qBridgeFdbUnicastGroup **Object:** dot1qTpFdbStatus	**Access:** Read-Only **Syntax:** Integer **OID:** .1.3.6.1.2.1.17.7.1.2.2.1.3.255.148.184.197.5.176.0 **Definition:** The status of this entry. The meanings of the values are: • other(1) - none of the following. This may include the case where some other MIB object (not the corresponding instance of dot1qTpFdbPort, nor an entry in the dot1qStaticUnicastTable) is being used to determine if and how frames addressed to the value of the corresponding instance of dot1qTpFdbAddress are being forwarded. • invalid(2) - this entry is no longer valid (e.g., it was learned but has since aged out), but has not yet been flushed from the table. • learned(3) - the value of the corresponding instance of dot1qTpFdbPort was learned and is being used. • self(4) - the value of the corresponding instance of dot1qTpFdbAddress represents one of the device's addresses. The corresponding instance of dot1qTpFdbPort indicates which of the device's ports has this address. • mgmt(5) - the value of the corresponding instance of dot1qTpFdbAddress is also the value of an existing instance of dot1qStaticAddress.

Group/Object	Description
Group: qBridgeFdbMulticastGroup **Object:** dot1qTpGroupEgressPorts	**Access:** Read-Only **Syntax:** Integer **OID:** .1.3.6.1.2.1.17.7.1.2.3.1.2 **Definition:** The complete set of ports, in this VLAN, to which frames destined for this Group MAC address are currently being explicitly forwarded. This does not include ports for which this address is only implicitly forwarded, in the dot1qForwardAllPorts list.
Group: qBridgeFdbMulticastGroup **Object:** dot1qTpGroupLearnt	**Access:** Read-Only **Syntax:** Integer **OID:** .1.3.6.1.2.1.17.7.1.2.3.1.3 **Definition:** The subset of ports in dot1qTpGroupEgressPorts that were learned by GMRP or some other dynamic mechanism, in this Filtering database.
Group: qBridgeVlanGroup **Object:** dot1qVlanCreationTime	**Access:** Read-Only **Syntax:** Timeticks **OID:** .1.3.6.1.2.1.17.7.1.4.2.1.7 **Definition:** The value of sysUpTime when this VLAN was created.
Group: qBridgeVlanGroup **Object:** dot1qVlanCurrentEgressPorts	**Access:** Read-Only **Syntax:** Hex-String **OID:** .1.3.6.1.2.1.17.7.1.4.2.1.4 **Definition:** The set of ports that are transmitting traffic for this VLAN as either tagged or untagged frames.
Group: qBridgeVlanGroup **Object:** dot1qVlanCurrentUntaggedPorts	**Access:** Read-Only **Syntax:** Hex-String **OID:** .1.3.6.1.2.1.17.7.1.4.2.1.5 **Definition:** The set of ports that are transmitting traffic for this VLAN as untagged frames.
Group: qBridgeVlanGroup **Object:** dot1qVlanFdbId	**Access:** Read-Only **Syntax:** Gauge32 **OID:** .1.3.6.1.2.1.17.7.1.4.2.1.3 **Definition:** The Filtering Database used by this VLAN. This is one of the dot1qFdbId values in the dot1qFdbTable. This value is allocated automatically by the device whenever the VLAN is created: either dynamically by GVRP, or by management, in dot1qVlanStaticTable. Allocation of this value follows the learning constraints defined for this VLAN in dot1qLearningConstraintsTable.
Group: qBridgeVlanStaticGroup **Object:** dot1qVlanForbiddenEgressPorts	**Access:** Read-Create **Syntax:** String **OID:** .1.3.6.1.2.1.17.7.1.4.3.1.3.22 **Definition:** The set of ports that are prohibited by management from being included in the egress list for this VLAN. Changes to this object that cause a port to be included or excluded affect the per-port, per-VLAN Registrar control for Registration Forbidden for the relevant GVRP state machine on each port. A port may not be added in this set if it is already a member of the set of ports in dot1qVlanStaticEgressPorts. The default value of this object is a string of zeros of appropriate length, excluding all ports from the forbidden set.
Group: qBridgeVlanGroup	**Access:** Read-Only

Group/Object	Description
Object: dot1qVlanNumDeletes	**Syntax:** Counter32 **OID:** .1.3.6.1.2.1.17.7.1.4.1 **Definition:** The number of times a VLAN entry has been deleted from the dot1qVlanCurrentTable (for any reason). If an entry is deleted, then inserted, and then deleted, this counter will be incremented by 2.
Group: qBridgeVlanStaticGroup **Object:** dot1qVlanStaticEgressPorts	**Access:** Read-Create **Syntax:** String **OID:** .1.3.6.1.2.1.17.7.1.4.3.1.2.22 **Definition:** The set of ports that are permanently assigned to the egress list for this VLAN by management. Changes to a bit in this object affect the per-port, per-VLAN Registrar control for Registration Fixed for the relevant GVRP state machine on each port. A port may not be added in this set if it is already a member of the set of ports in dot1qVlanForbiddenEgressPorts. The default value of this object is a string of zeros of appropriate length, indicating not fixed.
Group: qBridgeVlanStaticGroup **Object:** dot1qVlanStaticName	**Access:** Read-Create **Syntax:** String **OID:** .1.3.6.1.2.1.17.7.1.4.3.1.1.22 **Definition:** An administratively assigned string, which may be used to identify the VLAN.
Group: qBridgeVlanStaticGroup **Object:** dot1qVlanStaticRowStatus	**Access:** Read-Create **Syntax:** Integer **OID:** .1.3.6.1.2.1.17.7.1.4.3.1.5.22 **Definition:** This object indicates the status of this entry.
Group: qBridgeVlanStaticGroup **Object:** dot1qVlanStaticUntaggedPorts	**Access:** Read-Create **Syntax:** String **OID:** .1.3.6.1.2.1.17.7.1.4.3.1.4.22 **Definition:** The set of ports that should transmit egress packets for this VLAN as untagged. The default value of this object for the default VLAN (dot1qVlanIndex = 1) is a string of appropriate length including all ports. There is no specified default for other VLANs. If a device agent cannot support the set of ports being set, then it will reject the set operation with an error. For example, a manager might attempt to set more than one VLAN to be untagged on egress where the device does not support this IEEE 802.1Q option.
Group: qBridgeVlanGroup **Object:** dot1qVlanStatus	**Access:** Read-Only **Syntax:** Integer **OID:** .1.3.6.1.2.1.17.7.1.4.2.1.6 **Definition:** This object indicates the status of this entry. • other(1) - this entry is currently in use, but the conditions under which it will remain so differ from the following values. • permanent(2) - this entry, corresponding to an entry in dot1qVlanStaticTable, is currently in use and will remain so after the next reset of the device. The port lists for this entry include ports from the equivalent dot1qVlanStaticTable entry and ports learned dynamically. • dynamicGvrp(3) - this entry is currently in use and will remain so until removed by GVRP. There is no static entry for this VLAN, and it will be removed when the last port leaves the VLAN.

Group/Object	Description
Group: qBridgeBaseGroup **Object:** dot1qVlanVersionNumber	**Access:** Read-Only **Syntax:** Integer **OID:** .1.3.6.1.2.1.17.7.1.1.1.0 **Definition:** The version number of IEEE 802.1Q that this device supports.

RMON-MIB

Group/Object	Description
Group: rmonAlarmGroup **Object:** AlarmFallingEventIndex	**Access:** Read-Create **Syntax:** Integer **OID:** 1.3.6.1.2.1.16.3.1.1.10.1 **Definition:** The index of the eventEntry that is used when a falling threshold is crossed. The eventEntry identified by a particular value of this index is the same as identified by the same value of the eventIndex object. If there is no corresponding entry in the eventTable, then no association exists. In particular, if this value is zero, no associated event will be generated, as zero is not a valid event index. This object may not be modified if the associated alarmStatus object is equal to valid(1).
Group: rmonAlarmGroup **Object:** AlarmFallingThreshold	**Access:** Read-Create **Syntax:** Integer **OID:** 1.3.6.1.2.1.16.3.1.1.8.1 **Definition:** A threshold for the sampled statistic. When the current sampled 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 entry becomes valid is less than or equal to this threshold and the associated alarmStartupAlarm is equal to fallingAlarm(2) or risingOrFallingAlarm(3). After a falling event is generated, another such event will not be generated until the sampled value rises above this threshold and reaches the alarmRisingThreshold. This object may not be modified if the associated alarmStatus object is equal to valid(1).
Group: rmonAlarmGroup **Object:** AlarmIndex	**Agent Capability:** RC-RMON-MIB-AC **Access:** Read-Only **Syntax:** Integer **OID:** 1.3.6.1.2.1.16.3.1.1.1.1 **Definition:** An index that uniquely identifies an entry in the alarm table. Each such entry defines a diagnostic sample at a particular interval for an object on the device. An average of four entries per port can be created in alarmTable.
Group: rmonAlarmGroup **Object:** AlarmInterval	**Agent Capability:** RC-RMON-MIB-AC **Access:** Read-Create **Syntax:** Integer **OID:** 1.3.6.1.2.1.16.3.1.1.2.1 **Definition:** The interval in seconds over which the data is sampled and compared with the rising and falling thresholds. When setting this variable, care should be taken in the case of deltaValue sampling - the interval should be set short enough that the sampled variable is very unlikely to increase or decrease by more than 2^31 - 1 during a single sampling interval. This object

Group/Object	Description
	may not be modified if the associated alarmStatus object is equal to valid(1). A default value of an alarmInterval is 60 seconds.
Group: rmonAlarmGroup **Object:** AlarmOwner	**Agent Capability:** RC-RMON-MIB-AC **Access:** Read-Create **Syntax:** String **OID:** 1.3.6.1.2.1.16.3.1.1.11.1 **Definition:** The entity that configured this entry and is therefore using the resources assigned to it. A default value of an alarmOwner is a **Monitor** string.
Group: rmonAlarmGroup **Object:** AlarmRisingEventIndex	**Access:** Read-Create **Syntax:** Integer **OID:** 1.3.6.1.2.1.16.3.1.1.9.1 **Definition:** The index of the eventEntry that is used when a rising threshold is crossed. The eventEntry identified by a particular value of this index is the same as identified by the same value of the eventIndex object. If there is no corresponding entry in the eventTable, then no association exists. In particular, if this value is zero, no associated event will be generated, as zero is not a valid event index. This object may not be modified if the associated alarmStatus object is equal to valid(1).
Group: rmonAlarmGroup **Object:** AlarmRisingThreshold	**Access:** Read-Create **Syntax:** Integer **OID:** 1.3.6.1.2.1.16.3.1.1.7.1 **Definition:** A threshold for the sampled statistic. When the current sampled 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 entry becomes valid is greater than or equal to this threshold and the associated alarmStartupAlarm is equal to risingAlarm(1) or risingOrFallingAlarm(3). After a rising event is generated, another such event will not be generated until the sampled value falls below this threshold and reaches the alarmFallingThreshold. This object may not be modified if the associated alarmStatus object is equal to valid(1).
Group: rmonAlarmGroup **Object:** AlarmSampleType	**Agent Capability:** RC-RMON-MIB-AC **Access:** Read-Create **Syntax:** Integer **OID:** 1.3.6.1.2.1.16.3.1.1.4.1 **Definition:** The method of sampling the selected variable and calculating the value to be compared against the thresholds. If the value of this object is absoluteValue(1), the value of the selected variable will be compared directly with the thresholds at the end of the sampling interval. If the value of this object is deltaValue(2), the value of the selected variable at the last sample will be subtracted from the current value, and the difference compared with the thresholds. This object may not be modified if the associated alarmStatus object is equal to valid(1). A default value of an alarmSampleType is **deltaValue(2)**.
Group: rmonAlarmGroup **Object:** AlarmStartupAlarm	**Agent Capability:** RC-RMON-MIB-AC **Access:** Read-Create **Syntax:** Integer **OID:** 1.3.6.1.2.1.16.3.1.1.6.1

Group/Object	Description
	Definition: The alarm that may be sent when this entry is first set to valid. If the first sample after this entry becomes valid is greater than or equal to the risingThreshold and alarmStartupAlarm is equal to risingAlarm(1) or risingOrFallingAlarm(3), then a single rising alarm will be generated. If the first sample after this entry becomes valid is less than or equal to the fallingThreshold and alarmStartupAlarm is equal to fallingAlarm(2) or risingOrFallingAlarm(3), then a single falling alarm will be generated. This object may not be modified if the associated alarmStatus object is equal to valid(1). A default value of alarmStartupAlarm is **risingOrFallingAlarm(3)**.
Group: rmonAlarmGroup **Object:** AlarmStatus	**Access:** Read-Create **Syntax:** Integer **OID:** 1.3.6.1.2.1.16.3.1.1.12.1 **Definition:** The status of this alarm entry.
Group: rmonAlarmGroup **Object:** AlarmValue	**Access:** Read-Only **Syntax:** Integer **OID:** 1.3.6.1.2.1.16.3.1.1.5.1 **Definition:** The value of the statistic during the last sampling period. For example, if the sample type is deltaValue, this value will be the difference between the samples at the beginning and end of the period. If the sample type is absoluteValue, this value will be the sampled value at the end of the period. This is the value that is compared with the rising and falling thresholds. The value during the current sampling period is not made available until the period is completed and will remain available until the next period completes.
Group: rmonAlarmGroup **Object:** AlarmVariable	**Access:** Read-Create **Syntax:** OID **OID:** 1.3.6.1.2.1.16.3.1.1.3.1 **Definition:** The object identifier of the particular variable to be sampled. Only variables that resolve to an ASN.1 primitive type of Integer (Integer, Integer32, Counter32, Counter64, Gauge, or TimeTicks) may be sampled. Because SNMP access control is articulated entirely in terms of the contents of MIB views, no access control mechanism exists that can restrict the value of this object to identify only those objects that exist in a particular MIB view. Because there is thus no acceptable means of restricting the read access that could be obtained through the alarm mechanism, the probe must only grant write access to this object in those views that have read access to all objects on the probe. During a set operation, if the supplied variable name is not available in the selected MIB view, a badValue error must be returned. If at any time the variable name of an established alarmEntry is no longer available in the selected MIB view, the probe must change the status of this alarmEntry to invalid(4). This object may not be modified if the associated alarmStatus object is equal to valid(1).
Group: rmonEthernetHistoryGroup **Object:** etherHistoryBroadcastPkts	**Access:** Read-Only **Syntax:** Counter32 **OID:** 1.3.6.1.2.1.16.2.2.1.7.1 **Definition:** The number of good packets received during this sampling interval that were directed to the broadcast address.
Group: rmonEthernetHistoryGroup **Object:** etherHistoryCollisions	**Access:** Read-Only **Syntax:** Counter32 **OID:** 1.3.6.1.2.1.16.2.2.1.14.1

Group/Object	Description
	Definition: The best estimate of the total number of collisions on this Ethernet segment during this sampling interval. The value returned will depend on the location of the RMON probe. Section 8.2.1.3 (10BASE-5) and section 10.3.1.3 (10BASE-2) of IEEE standard 802.3 states that a station must detect a collision, in the receive mode, if three or more stations are transmitting simultaneously. A repeater port must detect a collision when two or more stations are transmitting simultaneously. Thus a probe placed on a repeater port could record more collisions than a probe connected to a station on the same segment would. Probe location plays a much smaller role when considering 10BASE-T. 14.2.1.4 (10BASE-T) of IEEE standard 802.3 defines a collision as the simultaneous presence of signals on the DO and RD circuits (transmitting and receiving at the same time). A 10BASE-T station can only detect collisions when it is transmitting. Thus probes placed on a station and a repeater, should report the same number of collisions. Note also that an RMON probe inside a repeater should ideally report collisions between the repeater and one or more other hosts (transmit collisions as defined by IEEE 802.3k) plus receiver collisions observed on any coax segments to which the repeater is connected.
Group: rmonEthernetHistoryGroup **Object:** etherHistoryCRCAlignErrors	**Access:** Read-Only **Syntax:** Counter32 **OID:** 1.3.6.1.2.1.16.2.2.1.9.1 **Definition:** The number of packets received during this sampling interval that had a length (excluding framing bits but including FCS octets) between 64 and 1518 octets, inclusive, but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
Group: rmonEthernetHistoryGroup **Object:** etherHistoryDropEvents	**Access:** Read-Only **Syntax:** Counter32 **OID:** 1.3.6.1.2.1.16.2.2.1.4.1 **Definition:** The total number of events in which packets were dropped by the probe due to lack of resources during this sampling interval. Note that this number is not necessarily the number of packets dropped, it is just the number of times this condition has been detected.
Group: rmonEthernetHistoryGroup **Object:** etherHistoryFragments	**Access:** Read-Only **Syntax:** Counter32 **OID:** 1.3.6.1.2.1.16.2.2.1.12.1 **Definition:** The total number of packets received during this sampling interval that were less than 64 octets in length (excluding framing bits but including FCS octets) had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error). Note that it is entirely normal for etherHistoryFragments to increment. This is because it counts both runts (which are normal occurrences due to collisions) and noise hits.
Group: rmonEthernetHistoryGroup **Object:** etherHistoryIndex	**Access:** Read-Only **Syntax:** Integer **OID:** 1.3.6.1.2.1.16.2.2.1.1.1 **Definition:** The history of which this entry is a part. The history identified by a particular value of this index is the same history as identified by the same value of historyControlIndex.
Group: rmonEthernetHistoryGroup **Object:** etherHistoryIntervalStart	**Access:** Read-Only **Syntax:** Timeticks

Group/Object	Description
	OID: 1.3.6.1.2.1.16.2.2.1.3.1 **Definition:** The value of sysUpTime at the start of the interval over which this sample was measured. If the probe keeps track of the time of day, it should start the first sample of the history at a time such that when the next hour of the day begins, a sample is started at that instant. Note that following this rule may require the probe to delay collecting the first sample of the history, as each sample must be of the same interval. Also note that the sample which is currently being collected is not accessible in this table until the end of its interval.
Group: rmonEthernetHistoryGroup **Object:** etherHistoryJabbers	**Access:** Read-Only **Syntax:** Counter32 **OID:** 1.3.6.1.2.1.16.2.2.1.13.1 **Definition:** The number of packets received during this sampling interval that were longer than 1518 octets (excluding framing bits but including FCS octets), and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error). Note that this definition of jabber is different than the definition in IEEE-802.3 section 8.2.1.5 (10BASE5) and section 10.3.1.4 (10BASE2). These documents define jabber as the condition where any packet exceeds 20 ms. The allowed range to detect jabber is between 20 ms and 150 ms.
Group: rmonEthernetHistoryGroup **Object:** etherHistoryMulticastPkts	**Access:** Read-Only **Syntax:** Counter32 **OID:** 1.3.6.1.2.1.16.2.2.1.8.1 **Definition:** The number of good packets received during this sampling interval that were directed to a multicast address. Note that this number does not include packets addressed to the broadcast address.
Group: rmonEthernetHistoryGroup **Object:** etherHistoryOctets	**Access:** Read-Only **Syntax:** Counter32 **OID:** 1.3.6.1.2.1.16.2.2.1.5.1 **Definition:** The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octets).
Group: rmonEthernetHistoryGroup **Object:** etherHistoryOversizePkts	**Access:** Read-Only **Syntax:** Counter32 **OID:** 1.3.6.1.2.1.16.2.2.1.11.1 **Definition:** The number of packets received during this sampling interval that were longer than 1518 octets (excluding framing bits but including FCS octets) but were otherwise well formed.
Group: rmonEthernetHistoryGroup **Object:** etherHistoryPkts	**Access:** Read-Only **Syntax:** Counter32 **OID:** 1.3.6.1.2.1.16.2.2.1.6.1 **Definition:** The number of packets (including bad packets) received during this sampling interval.
Group: rmonEthernetHistoryGroup **Object:** etherHistorySampleIndex	**Access:** Read-Only **Syntax:** Integer **OID:** 1.3.6.1.2.1.16.2.2.1.2.1

Group/Object	Description
	Definition: An index that uniquely identifies the particular sample this entry represents among all samples associated with the same historyControlEntry. This index starts at 1 and increases by one as each new sample is taken.
Group: rmonEthernetHistoryGroup **Object:** etherHistoryUndersizePkts	**Access:** Read-Only **Syntax:** Counter32 **OID:** 1.3.6.1.2.1.16.2.2.1.10.1 **Definition:** The number of packets received during this sampling interval that were less than 64 octets long (excluding framing bits but including FCS octets) and were otherwise well formed.
Group: rmonEthernetHistoryGroup **Object:** etherHistoryUtilization	**Access:** Read-Only **Syntax:** Integer **OID:** 1.3.6.1.2.1.16.2.2.1.15.1 **Definition:** The best estimate of the mean physical layer network utilization on this interface during this sampling interval, in hundredths of a percent.
Group: rmonEtherStatsGroup **Object:** etherStatsBroadcastPkts	**Access:** Read-Only **Syntax:** Counter32 **OID:** 1.3.6.1.2.1.16.1.1.1.6.1 **Definition:** The total number of good packets received that were directed to the broadcast address. Note that this does not include multicast packets.
Group: rmonEtherStatsGroup **Object:** etherStatsCollisions	**Access:** Read-Only **Syntax:** Counter32 **OID:** 1.3.6.1.2.1.16.1.1.1.13.1 **Definition:** The best estimate of the total number of collisions on this Ethernet segment. The value returned will depend on the location of the RMON probe. Section 8.2.1.3 (10BASE-5) and section 10.3.1.3 (10BASE-2) of IEEE standard 802.3 states that a station must detect a collision, in the receive mode, if three or more stations are transmitting simultaneously. A repeater port must detect a collision when two or more stations are transmitting simultaneously. Thus a probe placed on a repeater port could record more collisions than a probe connected to a station on the same segment would. Probe location plays a much smaller role when considering 10BASE-T. 14.2.1.4 (10BASE-T) of IEEE standard 802.3 defines a collision as the simultaneous presence of signals on the DO and RD circuits (transmitting and receiving at the same time). A 10BASE-T station can only detect collisions when it is transmitting. Thus probes placed on a station and a repeater, should report the same number of collisions. Note also that an RMON probe inside a repeater should ideally report collisions between the repeater and one or more other hosts (transmit collisions as defined by IEEE 802.3k) plus receiver collisions observed on any coax segments to which the repeater is connected.
Group: rmonEtherStatsGroup **Object:** etherStatsCRCAlignErrors	**Access:** Read-Only **Syntax:** Counter32 **OID:** 1.3.6.1.2.1.16.1.1.1.8.1 **Definition:** The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
Group: rmonEtherStatsGroup **Object:** etherStatsDataSource	**Access:** Read-Create **OID:** 1.3.6.1.2.1.16.1.1.1.2.1

Group/Object	Description
	Definition: This object identifies the source of the data that this etherStats entry is configured to analyze. This source can be any ethernet interface on this device. In order to identify a particular interface, this object shall identify the instance of the ifIndex object, defined in RFC 2233 [17], for the desired interface. For example, if an entry were to receive data from interface #1, this object would be set to ifIndex.1. The statistics in this group reflect all packets on the local network segment attached to the identified interface. An agent may or may not be able to tell if fundamental changes to the media of the interface have occurred and necessitate an invalidation of this entry. For example, a hot-pluggable ethernet card could be pulled out and replaced by a token-ring card. In such a case, if the agent has such knowledge of the change, it is recommended that it invalidate this entry. This object may not be modified if the associated etherStatsStatus object is equal to valid(1).
Group: rmonEtherStatsGroup **Object:** etherStatsDropEvents	**Access:** Read-Only **Syntax:** Counter32 **OID:** 1.3.6.1.2.1.16.1.1.1.3.1 **Definition:** The total number of events in which packets were dropped by the probe due to lack of resources. Note that this number is not necessarily the number of packets dropped; it is just the number of times this condition has been detected.
Group: rmonEtherStatsGroup **Object:** etherStatsFragments	**Access:** Read-Only **Syntax:** Counter32 **OID:** 1.3.6.1.2.1.16.1.1.1.11.1 **Definition:** The total number of packets received that were less than 64 octets in length (excluding framing bits but including FCS octets) and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error). Note that it is entirely normal for etherStatsFragments to increment. This is because it counts both runts (which are normal occurrences due to collisions) and noise hits.
Group: rmonEtherStatsGroup **Object:** etherStatsIndex	**Agent Capability:** RC-RMON-MIB-AC **Access:** Read-Only **Syntax:** Integer **OID:** 1.3.6.1.2.1.16.1.1.1.1.1 **Definition:** The value of this object uniquely identifies this etherStats entry. **Note** Two entries per port are created in etherStatsTable.
Group: rmonEtherStatsGroup **Object:** etherStatsJabbers	**Access:** Read-Only **Syntax:** Counter32 **OID:** 1.3.6.1.2.1.16.1.1.1.12.1 **Definition:** The total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error). Note that this definition of jabber is different than the definition in IEEE-802.3 section 8.2.1.5 (10BASE5) and section 10.3.1.4 (10BASE2). These documents define jabber as the condition where any packet exceeds 20 ms. The allowed range to detect jabber is between 20 ms and 150 ms.
Group: rmonEtherStatsGroup	**Access:** Read-Only

Group/Object	Description
Object: etherStatsMulticastPkts	**Syntax:** Counter32 **OID:** 1.3.6.1.2.1.16.1.1.1.7.1 **Definition:** The total number of good packets received that were directed to a multicast address. Note that this number does not include packets directed to the broadcast address.

Group: rmonEtherStatsGroup
Object: etherStatsOctets
	Access: Read-Only
	Syntax: Counter32
	OID: 1.3.6.1.2.1.16.1.1.1.4.1
	Definition: The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octets). This object can be used as a reasonable estimate of 10-Megabit ethernet utilization. If greater precision is desired, the etherStatsPkts and etherStatsOctets objects should be sampled before and after a common interval. The differences in the sampled values are Pkts and Octets, respectively, and the number of seconds in the interval is Interval. These values are used to calculate the Utilization as follows:
	`Pkts * (9.6 + 6.4) + (Octets * .8)`
	`Utilization = ----------------------------------`
	`Interval * 10,000`
	The result of this equation is the value Utilization which is the percent utilization of the ethernet segment on a scale of 0 to 100 percent.

Group: rmonEtherStatsGroup **Object:** etherStatsOversizePkts	**Access:** Read-Only **Syntax:** Counter32 **OID:** 1.3.6.1.2.1.16.1.1.1.10.1 **Definition:** The total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets) and were otherwise well formed.
Group: rmonEtherStatsGroup **Object:** etherStatsOwner	**Agent Capability:** RC-RMON-MIB-AC **Access:** Read-Create **Syntax:** String **OID:** 1.3.6.1.2.1.16.1.1.1.20.1 **Definition:** The entity that configured this entry and is therefore using the resources assigned to it. The value of this entry is always set to **Monitor** and may not be modified.
Group: rmonEtherStatsGroup **Object:** etherStatsPkts	**Access:** Read-Only **Syntax:** Counter32 **OID:** 1.3.6.1.2.1.16.1.1.1.5.1 **Definition:** The total number of packets (including bad packets, broadcast packets, and multicast packets) received.
Group: rmonEtherStatsGroup **Object:** etherStatsPkts1024to1518Octets	**Access:** Read-Only **Syntax:** Counter32 **OID:** 1.3.6.1.2.1.16.1.1.1.19.1 **Definition:** The total number of packets (including bad packets) received that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets).
Group: rmonEtherStatsGroup	**Access:** Read-Only

Group/Object	Description
Object: etherStatsPkts128to255Octets	**Syntax:** Counter32 **OID:** 1.3.6.1.2.1.16.1.1.1.16.1 **Definition:** The total number of packets (including bad packets) received that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets).
Group: rmonEtherStatsGroup **Object:** etherStatsPkts256to511Octets	**Access:** Read-Only **Syntax:** Counter32 **OID:** 1.3.6.1.2.1.16.1.1.1.17.1 **Definition:** The total number of packets (including bad packets) received that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets).
Group: rmonEtherStatsGroup **Object:** etherStatsPkts512to1023Octets	**Access:** Read-Only **Syntax:** Counter32 **OID:** 1.3.6.1.2.1.16.1.1.1.18.1 **Definition:** The total number of packets (including bad packets) received that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets).
Group: rmonEtherStatsGroup **Object:** etherStatsPkts64Octets	**Access:** Read-Only **Syntax:** Counter32 **OID:** 1.3.6.1.2.1.16.1.1.1.14.1 **Definition:** The total number of packets (including bad packets) received that were 64 octets in length (excluding framing bits but including FCS octets).
Group: rmonEtherStatsGroup **Object:** etherStatsPkts65to127Octets	**Access:** Read-Only **Syntax:** Counter32 **OID:** 1.3.6.1.2.1.16.1.1.1.15.1 **Definition:** The total number of packets (including bad packets) received that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets).
Group: rmonEtherStatsGroup **Object:** etherStatsStatus	**Agent Capability:** RC-RMON-MIB-AC **Access:** Read-Create **Syntax:** Integer **OID:** 1.3.6.1.2.1.16.1.1.1.21.1 **Definition:** The status of this etherStats entry. **Note** One entry per port is created in etherStatsTable upon initialization up. These entries may not be modified or deleted. No new entries can be created. Therefore, historyControlStatus is always set to **valid(1)**.
Group: rmonEtherStatsGroup **Object:** etherStatsUndersizePkts	**Access:** Read-Only **Syntax:** Counter32 **OID:** 1.3.6.1.2.1.16.1.1.1.9.1 **Definition:** The total number of packets received that were less than 64 octets long (excluding framing bits, but including FCS octets) and were otherwise well formed.
Group: rmonEventGroup	**Agent Capability:** RC-RMON-MIB-AC

Group/Object	Description
Object: eventCommunity	**Access:** Read-Create **Syntax:** String **OID:** 1.3.6.1.2.1.16.9.1.1.4.1 **Definition:** If an SNMP trap is to be sent, it will be sent to the SNMP community specified by this octet string. The string of up to 30 characters is supported for this object.
Group: rmonEventGroup **Object:** eventDescription	**Agent Capability:** RC-RMON-MIB-AC **Access:** Read-Create **Syntax:** String **OID:** 1.3.6.1.2.1.16.9.1.1.2.1 **Definition:** A comment describing this event entry.
Group: rmonEventGroup **Object:** eventIndex	**Agent Capability:** RC-RMON-MIB-AC **Access:** Read-Only **Syntax:** Integer **OID:** 1.3.6.1.2.1.16.9.1.1.1.1 **Definition:** An index that uniquely identifies an entry in the event table. Each such entry defines one event that is to be generated when the appropriate conditions occur. An average of one entry per alarmEntry may be created in eventTable.
Group: rmonEventGroup **Object:** eventLastTimeSent	**Agent Capability:** RC-RMON-MIB-AC **Access:** Read-Only **Syntax:** Timeticks **OID:** 1.3.6.1.2.1.16.9.1.1.5.1 **Definition:** The value of sysUpTime at the time this event entry last generated an event. If this entry has not generated any events, this value will be zero.
Group: rmonEventGroup **Object:** eventOwner	**Agent Capability:** RC-RMON-MIB-AC **Access:** Read-Create **Syntax:** String **OID:** 1.3.6.1.2.1.16.9.1.1.6.1 **Definition:** The entity that configured this entry and is therefore using the resources assigned to it. If this object contains a string starting with **monitor** and has associated entries in the log table, all connected management stations should retrieve those log entries, as they may have significance to all management stations connected to this device. A default value of an eventOwner is a **Monitor** string.
Group: rmonEventGroup **Object:** eventStatus	**Access:** Read-Create **Syntax:** Integer **OID:** 1.3.6.1.2.1.16.9.1.1.7.1 **Definition:** The status of this event entry. If this object is not equal to valid(1), all associated log entries shall be deleted by the agent.
Group: rmonEventGroup **Object:** eventType	**Agent Capability:** RC-RMON-MIB-AC **Access:** Read-Create **Syntax:** Integer **OID:** 1.3.6.1.2.1.16.9.1.1.3.1

Group/Object	Description
	Definition: The type of notification that the probe will make about this event. In the case of log, an entry is made in the log table for each event. In the case of snmp-trap, an SNMP trap is sent to one or more management stations. A default value of an eventType is **logandtrap(4)**.
Group: rmonHistoryControlGroup **Object:** historyControlBucketsGranted	**Access:** Read-Only **Syntax:** Integer **OID:** 1.3.6.1.2.1.16.2.1.1.4.1 **Definition:** The number of discrete sampling intervals over which data shall be saved in the part of the media-specific table associated with this historyControlEntry. When the associated historyControlBucketsRequested object is created or modified, the probe should set this object as closely to the requested value as is possible for the particular probe implementation and available resources. The probe must not lower this value except as a result of a modification to the associated historyControlBucketsRequested object. There will be times when the actual number of buckets associated with this entry is less than the value of this object. In this case, at the end of each sampling interval, a new bucket will be added to the media-specific table. When the number of buckets reaches the value of this object and a new bucket is to be added to the media-specific table, the oldest bucket associated with this historyControlEntry shall be deleted by the agent so that the new bucket can be added. When the value of this object changes to a value less than the current value, entries are deleted from the media-specific table associated with this historyControlEntry. Enough of the oldest of these entries shall be deleted by the agent so that their number remains less than or equal to the new value of this object. When the value of this object changes to a value greater than the current value, the number of associated media- specific entries may be allowed to grow.
Group: rmonHistoryControlGroup **Object:** historyControlBucketsRequested	**Agent Capability:** RC-RMON-MIB-AC **Access:** Read-Create **Syntax:** Integer **OID:** 1.3.6.1.2.1.16.2.1.1.3.1 **Definition:** The requested number of discrete time intervals over which data is to be saved in the part of the media-specific table associated with this historyControlEntry. When this object is created or modified, the probe should set historyControlBucketsGranted as closely to this object as is possible for the particular probe implementation and available resources. **Definition:** The value of historyControBucketRequested is restricted to 4000.
Group: rmonHistoryControlGroup **Object:** historyControlDataSource	**Access:** Read-Create **Syntax:** OID **OID:** 1.3.6.1.2.1.16.2.1.1.2.1 **Definition:** This object identifies the source of the data for which historical data was collected and placed in a media-specific table on behalf of this historyControlEntry. This source can be any interface on this device. In order to identify a particular interface, this object shall identify the instance of the ifIndex object, defined in RFC 2233 [17], for the desired interface. For example, if an entry were to receive data from interface #1, this object would be set to ifIndex.1. The statistics in this group reflect all packets on the local network segment attached to the identified interface. An agent may or may not be able to tell if fundamental changes to the media of the interface have occurred and necessitate an invalidation of this entry. For example, a hot-pluggable ethernet card could be pulled out and replaced by a token-ring card. In such a case, if the agent has such knowledge of the change, it is

Group/Object	Description
	recommended that it invalidate this entry. This object may not be modified if the associated historyControlStatus object is equal to valid(1).
Group: rmonHistoryControlGroup **Object:** historyControlIndex	**Agent Capability:** RC-RMON-MIB-AC **Access:** Read-Only **Syntax:** Integer **OID:** 1.3.6.1.2.1.16.2.1.1.1.1 **Definition:** An index that uniquely identifies an entry in the historyControl table. Each such entry defines a set of samples at a particular interval for an interface on the device. An average of four entries per ethernet port can be created in historyControlTable.
Group: rmonHistoryControlGroup **Object:** historyControlInterval	**Access:** Read-Create **Syntax:** Integer **OID:** 1.3.6.1.2.1.16.2.1.1.5.1 **Definition:** The interval in seconds over which the data is sampled for each bucket in the part of the media-specific table associated with this historyControlEntry. This interval can be set to any number of seconds between 1 and 3600 (1 hour). Because the counters in a bucket may overflow at their maximum value with no indication, a prudent manager will take into account the possibility of overflow in any of the associated counters. It is important to consider the minimum time in which any counter could overflow on a particular media type and set the historyControlInterval object to a value less than this interval. This is typically most important for the **octets** counter in any media-specific table. For example, on an Ethernet network, the etherHistoryOctets counter could overflow in about one hour at the Ethernet's maximum utilization. This object may not be modified if the associated historyControlStatus object is equal to valid(1).
Group: rmonHistoryControlGroup **Object:** historyControlOwner	**Agent Capability:** RC-RMON-MIB-AC **Access:** Read-Create **Syntax:** String **OID:** 1.3.6.1.2.1.16.2.1.1.6.1 **Definition:** The entity that configured this entry and is therefore using the resources assigned to it. A default value of a historyControlOwner is a **Monitor** string.
Group: rmonHistoryControlGroup **Object:** historyControlStatus	**Access:** Read-Create **Syntax:** Integer **OID:** 1.3.6.1.2.1.16.2.1.1.7.1 **Definition:** The status of this historyControl entry. Each instance of the media-specific table associated with this historyControlEntry will be deleted by the agent if this historyControlEntry is not equal to valid(1).
Group: rmonEventGroup **Object:** logDescription	**Access:** Read-Only **Syntax:** String **OID:** 1.3.6.1.2.1.16.9.2.1.4.1 **Definition:** An implementation dependent description of the event that activated this log entry.
Group: rmonEventGroup **Object:** logEventIndex	**Access:** Read-Only **Syntax:** Integer **OID:** 1.3.6.1.2.1.16.9.2.1.1.1

Group/Object	Description
	Definition: The event entry that generated this log entry. The log identified by a particular value of this index is associated with the same eventEntry as identified by the same value of eventIndex.
Group: rmonEventGroup **Object:** logIndex	**Agent Capability:** RC-RMON-MIB-AC **Access:** Read-Only **Syntax:** Integer **OID:** 1.3.6.1.2.1.16.9.2.1.2.1 **Definition:** An index that uniquely identifies an entry in the log table amongst those generated by the same eventEntries. These indexes are assigned beginning with 1 and increase by one with each new log entry. The association between values of logIndex and logEntries is fixed for the lifetime of each logEntry. The agent may choose to delete the oldest instances of logEntry as required because of lack of memory. It is an implementation-specific matter as to when this deletion may occur. **Note** For each eventEntry a hundred of entries in logTable may be created. The value of this object will increase for each new log generated for corresponding event. When value of this object becomes greater than 100, oldest entries will be deleted.
Group: rmonEventGroup **Object:** logTime	**Access:** Read-Only **Syntax:** Timeticks **OID:** 1.3.6.1.2.1.16.9.2.1.3.1 **Definition:** The value of sysUpTime when this log entry was created.

RS-232-MIB

Group/Object	Description
Group: rs232AsyncGroup **Object:** rs232AsyncPortAutobaud	**Access:** Read-Write **Syntax:** Integer **OID:** 1.3.6.1.2.1.10.33.3.1.3.101 **Definition:** A control for the port's ability to automatically sense input speed. When rs232PortAutoBaud is **enabled**, a port may autobaud to values different from the set values for speed, parity, and character size. As a result a network management system may temporarily observe values different from what was previously set.
Group: rs232AsyncGroup **Object:** rs232AsyncPortBits	**Access:** Read-Write **Syntax:** Integer **OID:** 1.3.6.1.2.1.10.33.2.1.5.1.4 **Definition:** The port's number of bits in a character.
Group: rs232AsyncGroup **Object:** rs232AsyncPortFramingErrs	**Access:** Read-Only **Syntax:** Counter32 **OID:** 1.3.6.1.2.1.10.33.2.1.5.1.2 **Definition:** Total number of characters with a framing error, input from the port since system re-initialization and while the port state was **up** or **test**.
Group: rs232AsyncGroup	**Access:** Read-Only

Group/Object	Description
Object: rs232AsyncPortIndex	**Syntax:** Integer **OID:** 1.3.6.1.2.1.10.33.2.1.5.1.1 **Definition:** A unique value for each port. Its value is the same as rs232PortIndex for the port.
Group: rs232AsyncGroup **Object:** rs232AsyncPortOverrunErrs	**Access:** Read-Only **Syntax:** Counter32 **OID:** 1.3.6.1.2.1.10.33.2.1.5.1.3 **Definition:** Total number of characters with an overrun error, input from the port since system re-initialization and while the port state was **up** or **test**.
Group: rs232AsyncGroup **Object:** rs232AsyncPortParity	**Access:** Read-Write **Syntax:** Integer **OID:** 1.3.6.1.2.1.10.33.1.0 **Definition:** The port's sense of a character parity bit.
Group: rs232AsyncGroup **Object:** rs232AsyncPortParityErrs	**Access:** Read-Only **Syntax:** Counter32 **OID:** 1.3.6.1.2.1.10.33.2.1.6.1.4 **Definition:** Total number of characters with a parity error, input from the port since system re-initialization and while the port state was **up** or **test**.
Group: rs232AsyncGroup **Object:** rs232AsyncPortStopBits	**Access:** Read-Write **Syntax:** Integer **OID:** 1.3.6.1.2.1.10.33.2.1.6.1.2 **Definition:** The port's number of stop bits.
Group: rs232Group **Object:** rs232InSigChanges	**Access:** Read-Only **Syntax:** Counter32 **OID:** 1.3.6.1.2.1.10.33.2.1.6.1.1 **Definition:** The number of times the signal has changed from **on** to **off** or from **off** to **on**.
Group: rs232Group **Object:** rs232InSigName	**Access:** Read-Only **Syntax:** Integer **OID:** 1.3.6.1.2.1.10.33.2.1.6.1.3 **Definition:** Identification of a hardware signal, as follows: • rts: Request to Send • cts: Clear to Send • dsr: Data Set Ready • dtr: Data Terminal Ready • ri: Ring Indicator • dcd: Received Line Signal Detector • sq: Signal Quality Detector • srs: Data Signaling Rate Selector • srts: Secondary Request to Send • scts: Secondary Clear to Send • sdcd: Secondary Received Line Signal Detector
Group: rs232Group **Object:** rs232InSigPortIndex	**Access:** Read-Only **Syntax:** Integer

Group/Object	Description
	OID: 1.3.6.1.2.1.10.33.2.1.1.101 **Definition:** The value of rs232PortIndex for the port to which this entry belongs.
Group: rs232Group **Object:** rs232InSigState	**Access:** Read-Only **Syntax:** Integer **OID:** 1.3.6.1.2.1.10.33.2.1.7.101 **Definition:** The current signal state.
Group: rs232Group **Object:** rs232Number	**Access:** Read-Only **Syntax:** Integer **OID:** 1.3.6.1.2.1.10.33.2.1.3.101 **Definition:** The number of ports (regardless of their current state) in the RS-232-like general port table.
Group: rs232Group **Object:** rs232OutSigChanges	**Access:** Read-Only **Syntax:** Integer **OID:** 1.3.6.1.2.1.10.33.2.1.5.101 **Definition:** The number of times the signal has changed from **on** to **off** or from **off** to **on**.
Group: rs232Group **Object:** rs232OutSigName	**Access:** Read-Only **Syntax:** Integer **OID:** 1.3.6.1.2.1.10.33.2.1.7.101 **Definition:** Identification of a hardware signal, as follows: • rts: Request to Send • cts: Clear to Send • dsr: Data Set Ready • dtr: Data Terminal Ready • ri: Ring Indicator • dcd: Received Line Signal Detector • sq: Signal Quality Detector • srs: Data Signaling Rate Selector • srts: Secondary Request to Send • scts: Secondary Clear to Send • sdcd: Secondary Received Line Signal Detector
Group: rs232Group **Object:** rs232OutSigPortIndex	**Access:** Read-Only **Syntax:** Integer **OID:** 1.3.6.1.2.1.10.33.2.1.4.101 **Definition:** The value of rs232PortIndex for the port to which this entry belongs.
Group: rs232Group **Object:** rs232OutSigState	**Access:** Read-Only **Syntax:** Integer **OID:** 1.3.6.1.2.1.10.33.2.1.5.101 **Definition:** The current signal state.
Group: rs232Group **Object:** rs232PortIndex	**Access:** Read-Only **Syntax:** Integer **OID:** 1.3.6.1.2.1.10.33.2.1.2.101

Group/Object	Description
	Definition: The value of ifIndex for the port. By convention and if possible, hardware port numbers map directly to external connectors. The value for each port must remain constant at least from one re-initialization of the network management agent to the next.
Group: rs232Group **Object:** rs232PortInFlowType	**Access:** Read-Write **Syntax:** Integer **OID:** 1.3.6.1.6.3.10.2.1.2.0 **Definition:** The port's type of input flow control. **none** indicates no flow control at this level. **ctsRts** and **dsrDtr** indicate use of the indicated hardware signals.
Group: rs232Group **Object:** rs232PortInSigNumber	**Access:** Read-Only **Syntax:** Integer **OID:** 1.3.6.1.6.3.10.2.1.1.0 **Definition:** The number of input signals for the port in the input signal table (rs232PortInSigTable). The table contains entries only for those signals the software can detect and that are useful to observe.
Group: rs232Group **Object:** rs232PortInSpeed	**Access:** Read-Write **Syntax:** Integer **OID:** 1.3.6.1.6.3.10.2.1.4.0 **Definition:** The port's input speed in bits per second. Note that non-standard values, such as 9612, are probably not allowed on most implementations.
Group: rs232Group **Object:** rs232PortOutFlowType	**Access:** Read-Write **Syntax:** Integer **OID:** 1.3.6.1.6.3.10.2.1.3.0 **Definition:** The port's type of output flow control. **none** indicates no flow control at this level. **ctsRts** and **dsrDtr** indicate use of the indicated hardware signals.
Group: rs232Group **Object:** rs232PortOutSigNumber	**Access:** Read-Only **Syntax:** Integer **OID:** 1.3.6.1.2.1.11.6.0 **Definition:** The number of output signals for the port in the output signal table (rs232PortOutSigTable). The table contains entries only for those signals the software can assert and that are useful to observe.
Group: rs232Group **Object:** rs232PortOutSpeed	**Access:** Read-Write **Syntax:** Integer **OID:** 1.3.6.1.2.1.11.4.0 **Definition:** The port's output speed in bits per second. Note that non-standard values, such as 9612, are probably not allowed on most implementations.
Group: rs232Group **Object:** rs232PortType	**Access:** Read-Only **Syntax:** Integer **OID:** 1.3.6.1.2.1.11.5.0 **Definition:** The port's hardware type.

RSTP-MIB

Group/Object	Description
Group: rstpPortGroup **Object:** dot1dStpPortAdminEdgePort	**Access:** Read-Write **TruthValue** **OID:** .1.3.6.1.2.1.17.2.19.1.2 **Definition:** The administrative value of the Edge Port parameter. A value of true(1) indicates that this port should be assumed as an edge-port, and a value of false(2) indicates that this port should be assumed as a non-edge-port. Setting this object will also cause the corresponding instance of dot1dStpPortOperEdgePort to change to the same value. Note that even when this object's value is true, the value of the corresponding instance of dot1dStpPortOperEdgePort can be false if a BPDU has been received. The value of this object MUST be retained across reinitializations of the management system.
Group: rstpPortGroup **Object:** dot1dStpPortAdminPathCost	**Access:** Read-Write **Syntax:** Integer **OID:** .1.3.6.1.2.1.17.2.19.1.6 **Definition:** The administratively assigned value for the contribution of this port to the path cost of paths toward the spanning tree root. Writing a value of **0** assigns the automatically calculated default Path Cost value to the port. If the default Path Cost is being used, this object returns **0** when read. This complements the object dot1dStpPortPathCost or dot1dStpPortPathCost32, which returns the operational value of the path cost. The value of this object MUST be retained across reinitializations of the management system.
Group: rstpPortGroup **Object:** dot1dStpPortAdminPointToPoint	**Access:** Read-Write **Syntax:** Integer **OID:** .1.3.6.1.2.1.17.2.19.1.4 **Definition:** The administrative point-to-point status of the LAN segment attached to this port, using the enumeration values of the IEEE 802.1w clause. A value of forceTrue(0) indicates that this port should always be treated as if it is connected to a point-to-point link. A value of forceFalse(1) indicates that this port should be treated as having a shared media connection. A value of auto(2) indicates that this port is considered to have a point-to-point link if it is an Aggregator and all of its members are aggregatable, or if the MAC entity is configured for full duplex operation, either through auto-negotiation or by management means. Manipulating this object changes the underlying adminPortToPortMAC. The value of this object MUST be retained across reinitializations of the management system.
Group: rstpPortGroup **Object:** dot1dStpPortOperEdgePort	**Access:** Read-Only **TruthValue** **OID:** .1.3.6.1.2.1.17.2.19.1.3 **Definition:** The operational value of the Edge Port parameter. The object is initialized to the value of the corresponding instance of dot1dStpPortAdminEdgePort. When the corresponding instance of dot1dStpPortAdminEdgePort is set, this object will be changed as well. This object will also be changed to false on reception of a BPDU.
Group: rstpPortGroup **Object:** dot1dStpPortOperPointToPoint	**Access:** Read-Only **TruthValue** **OID:** .1.3.6.1.2.1.17.2.19.1.5 **Definition:** The operational point-to-point status of the LAN segment attached to this port. It indicates whether a port is considered to have a

Group/Object	Description
	point-to-point connection. If adminPointToPointMAC is set to auto(2), then the value of operPointToPointMAC is determined in accordance with the specific procedures defined for the MAC entity concerned, as defined in IEEE 802.1w, clause 6.5. The value is determined dynamically; that is, it is re-evaluated whenever the value of adminPointToPointMAC changes, and whenever the specific procedures defined for the MAC entity evaluate a change in its point-to-point status.
Group: rstpBridgeGroup **Object:** dot1dStpTxHoldCount	**Agent Capability:** RC-RSTP-MIB-AC **Access:** Read-Write **Syntax:** Integer **OID:** .1.3.6.1.2.1.17.2.17.0 **Definition:** The value used by the Port Transmit state machine to limit the maximum transmission rate. The value of this object MUST be retained across reinitializations of the management system. **Note** RFC specified range is 1..10. Implementation uses 0...100. The value 0 is used for Unlimited and ROS range is actually 3..100.
Group: rstpBridgeGroup **Object:** dot1dStpVersion	**Access:** Read-Write **Syntax:** Integer **OID:** .1.3.6.1.2.1.17.2.16.0 **Definition:** The version of Spanning Tree Protocol the bridge is currently running. The value **stpCompatible(0)** indicates the Spanning Tree Protocol specified in IEEE 802.1D-1998 and **rstp(2)** indicates the Rapid Spanning Tree Protocol specified in IEEE 802.1w and clause 17 of 802.1D-2004. The values are directly from the IEEE standard. New values may be defined as future versions of the protocol become available. The value of this object MUST be retained across reinitializations of the management system.

SNMP-FRAMEWORK-MIB

Group/Object	Description
Group: snmpEngineGroup **Object:** snmpEngineBoots	**Access:** Read-Only **Syntax:** Integer **OID:** 1.3.6.1.2.1.11.31.0 **Definition:** The number of times that the SNMP engine has (re-)initialized itself since snmpEngineID was last configured.
Group: snmpEngineGroup **Object:** snmpEngineID	**Access:** Read-Only **Syntax:** Hex-String **OID:** 1.3.6.1.2.1.1.4.0 **Definition:** An SNMP engine's administratively-unique identifier. This information SHOULD be stored in non-volatile storage so that it remains constant across re-initializations of the SNMP engine.
Group: snmpEngineGroup **Object:** snmpEngineMaxMessageSize	**Access:** Read-Only **Syntax:** Integer **OID:** 1.3.6.1.2.1.1.1.0

Group/Object	Description
	Definition: The maximum length in octets of an SNMP message which this SNMP engine can send or receive and process, determined as the minimum of the maximum message size values supported among all of the transports available to and supported by the engine.
Group: snmpEngineGroup **Object:** snmpEngineTime	**Access:** Read-Only **Syntax:** Integer **OID:** 1.3.6.1.2.1.1.6.0 **Definition:** The number of seconds since the value of the snmpEngineBoots object last changed. When incrementing this object's value would cause it to exceed its maximum, snmpEngineBoots is incremented as if a re-initialization had occurred, and this object's value consequently reverts to zero.

SNMP-USER-BASED-SM-MIB

Group/Object	Description
Group: usmMIBBasicGroup **Object:** usmStatsDecryptionErrors	**Access:** Read-Only **Syntax:** Counter32 **OID:** 1.3.6.1.6.3.15.1.2.2.1.9 **Definition:** The total number of packets received by the SNMP engine which were dropped because they could not be decrypted.
Group: usmMIBBasicGroup **Object:** usmStatsNotInTimeWindows	**Access:** Read-Only **Syntax:** Counter32 **OID:** 1.3.6.1.6.3.15.1.2.2.1.8.11.128.0.58.156.3.0.10.220.0.128.72.4.97.112.118.51 **Definition:** The total number of packets received by the SNMP engine which were dropped because they appeared outside of the authoritative SNMP engine's window.
Group: usmMIBBasicGroup **Object:** usmStatsUnknownEngineIDs	**Access:** Read-Only **Syntax:** Counter32 **OID:** 1.3.6.1.6.3.15.1.2.2.1.11 **Definition:** The total number of packets received by the SNMP engine which were dropped because they referenced an snmpEngineID that was not known to the SNMP engine.
Group: usmMIBBasicGroup **Object:** usmStatsUnknownUserNames	**Access:** Read-Only **Syntax:** Counter32 **OID:** 1.3.6.1.6.3.15.1.2.2.1.3 **Definition:** The total number of packets received by the SNMP engine which were dropped because they referenced a user that was not known to the SNMP engine.
Group: usmMIBBasicGroup **Object:** usmStatsUnsupportedSecLevels	**Access:** Read-Only **Syntax:** Counter32 **OID:** 1.3.6.1.6.3.15.1.2.1.0 **Definition:** The total number of packets received by the SNMP engine which were dropped because they requested a securityLevel that was unknown to the SNMP engine or otherwise unavailable.
Group: usmMIBBasicGroup	**Access:** Read-Only

Group/Object	Description
Object: usmStatsWrongDigests	**Syntax:** Counter32 **OID:** 1.3.6.1.6.3.15.1.2.2.1.13 **Definition:** The total number of packets received by the SNMP engine which were dropped because they didn't contain the expected digest value.
Group: usmMIBBasicGroup **Object:** usmUserAuthKeyChange	**Access:** Read-Create **Syntax:** String **OID:** 1.3.6.1.6.3.15.1.2.2.1.12 **Definition:** An object, which when modified, causes the secret authentication key used for messages sent on behalf of this user to/from the SNMP engine identified by usmUserEngineID, to be modified via a one-way function. The associated protocol is the usmUserAuthProtocol. The associated secret key is the user's secret authentication key (authKey). The associated hash algorithm is the algorithm used by the user's usmUserAuthProtocol. When creating a new user, it is an **inconsistentName** error for a set operation to refer to this object unless it is previously or concurrently initialized through a set operation on the corresponding instance of usmUserCloneFrom. When the value of the corresponding usmUserAuthProtocol is usmNoAuthProtocol, then a set is successful, but effectively is a no-op. When this object is read, the zero-length (empty) string is returned. The recommended way to do a key change is as follows: • 1) GET(usmUserSpinLock.0) and save in sValue. • 2) generate the keyChange value based on the old (existing) secret key and the new secret key, let us call this kcValue. If you do the key change on behalf of another user: • 3) SET(usmUserSpinLock.0=sValue, usmUserAuthKeyChange=kcValue usmUserPublic=randomValue) If you do the key change for yourself: • 4) SET(usmUserSpinLock.0=sValue, usmUserOwnAuthKeyChange=kcValue usmUserPublic=randomValue) If you get a response with error-status of noError, then the SET succeeded and the new key is active. If you do not get a response, then you can issue a GET(usmUserPublic) and check if the value is equal to the randomValue you did send in the SET. If so, then the key change succeeded and the new key is active (probably the response got lost). If not, then the SET request probably never reached the target and so you can start over with the procedure above.
Group: usmMIBBasicGroup **Object:** usmUserAuthProtocol	**Access:** Read-Create **Syntax:** OID **OID:** 1.3.6.1.6.3.16.1.4.1.4.8.71.112.114.105.118.97.116.101.0.2.1 **Definition:** An indication of whether messages sent on behalf of this user to/from the SNMP engine identified by usmUserEngineID, can be authenticated, and if so, the type of authentication protocol which is used. An instance of this object is created concurrently with the creation of any other object instance for the same user (i.e., as part of the processing of the set operation which creates the first object instance in the same conceptual row). If an initial set operation (i.e. at row creation time) tries to set a value for an unknown or unsupported protocol, then a **wrongValue** error must be returned. The value will be overwritten/set when a set operation is performed on the corresponding instance of usmUserCloneFrom. Once instantiated, the value of such an instance of this object can only be changed via a set operation to the value of the usmNoAuthProtocol. If a set operation tries to change the value of an existing instance of this object to any value other than usmNoAuthProtocol, then an **inconsistentValue** error must be

Group/Object	Description
	returned. If a set operation tries to set the value to the usmNoAuthProtocol while the usmUserPrivProtocol value in the same row is not equal to usmNoPrivProtocol, then an **inconsistentValue** error must be returned. That means that an SNMP command generator application must first ensure that the usmUserPrivProtocol is set to the usmNoPrivProtocol value before it can set the usmUserAuthProtocol value to usmNoAuthProtocol.
Group: usmMIBBasicGroup **Object:** usmUserCloneFrom	**Access:** Read-Create **Syntax:** OID **OID:** 1.3.6.1.6.3.16.1.4.1.7.8.71.112.114.105.118.97.116.101.0.2.1 **Definition:** A pointer to another conceptual row in this usmUserTable. The user in this other conceptual row is called the clone-from user. When a new user is created (i.e., a new conceptual row is instantiated in this table), the privacy and authentication parameters of the new user must be cloned from its clone-from user. These parameters are: • - authentication protocol (usmUserAuthProtocol) • - privacy protocol (usmUserPrivProtocol) They will be copied regardless of what the current value is. Cloning also causes the initial values of the secret authentication key (authKey) and the secret encryption key (privKey) of the new user to be set to the same values as the corresponding secrets of the clone-from user to allow the KeyChange process to occur as required during user creation. The first time an instance of this object is set by a management operation (either at or after its instantiation), the cloning process is invoked. Subsequent writes are successful but invoke no action to be taken by the receiver. The cloning process fails with an **inconsistentName** error if the conceptual row representing the clone-from user does not exist or is not in an active state when the cloning process is invoked. When this object is read, the ZeroDotZero OID is returned.
Group: usmMIBBasicGroup **Object:** usmUserOwnAuthKeyChange	**Access:** Read-Create **Syntax:** String **OID:** 1.3.6.1.6.3.16.1.4.1.5.8.71.112.114.105.118.97.116.101.0.2.1 **Definition:** Behaves exactly as usmUserAuthKeyChange, with one notable difference: in order for the set operation to succeed, the usmUserName of the operation requester must match the usmUserName that indexes the row which is targeted by this operation. In addition, the USM security model must be used for this operation. The idea here is that access to this column can be public, since it will only allow a user to change his own secret authentication key (authKey). Note that this can only be done once the row is active. When a set is received and the usmUserName of the requester is not the same as the umsUserName that indexes the row which is targeted by this operation, then a **noAccess** error must be returned. When a set is received and the security model in use is not USM, then a **noAccess** error must be returned.
Group: usmMIBBasicGroup **Object:** usmUserOwnPrivKeyChange	**Access:** Read-Create **Syntax:** String **OID:** 1.3.6.1.6.3.16.1.4.1.9.8.71.112.114.105.118.97.116.101.0.2.1 **Definition:** Behaves exactly as usmUserPrivKeyChange, with one notable difference: in order for the Set operation to succeed, the usmUserName of the operation requester must match the usmUserName that indexes the row which is targeted by this operation. In addition, the USM security model must be used for this operation. The idea here is that access to this column can be public, since it will only allow a user to change his own secret privacy key (privKey). Note that this can only be done once the row is active. When a set is received and the usmUserName of the requester is not the same as the

Group/Object	Description
	umsUserName that indexes the row which is targeted by this operation, then a **noAccess** error must be returned. When a set is received and the security model in use is not USM, then a **noAccess** error must be returned.
Group: usmMIBBasicGroup **Object:** usmUserPrivKeyChange	**Access:** Read-Create **Syntax:** String **OID:** 1.3.6.1.6.3.16.1.4.1.8.8.71.112.114.105.118.97.116.101.0.2.1 **Definition:** An object, which when modified, causes the secret encryption key used for messages sent on behalf of this user to/from the SNMP engine identified by usmUserEngineID, to be modified via a one-way function. The associated protocol is the usmUserPrivProtocol. The associated secret key is the user's secret privacy key (privKey). The associated hash algorithm is the algorithm used by the user's usmUserAuthProtocol. When creating a new user, it is an **inconsistentName** error for a set operation to refer to this object unless it is previously or concurrently initialized through a set operation on the corresponding instance of usmUserCloneFrom. When the value of the corresponding usmUserPrivProtocol is usmNoPrivProtocol, then a set is successful, but effectively is a no-op. When this object is read, the zero-length (empty) string is returned. See the description clause of usmUserAuthKeyChange for a recommended procedure to do a key change.
Group: usmMIBBasicGroup **Object:** usmUserPrivProtocol	**Access:** Read-Create **Syntax:** OID **OID:** 1.3.6.1.6.3.16.1.4.1.6.8.71.112.114.105.118.97.116.101.0.2.1 **Definition:** An indication of whether messages sent on behalf of this user to/from the SNMP engine identified by usmUserEngineID, can be protected from disclosure, and if so, the type of privacy protocol which is used. An instance of this object is created concurrently with the creation of any other object instance for the same user (i.e., as part of the processing of the set operation which creates the first object instance in the same conceptual row). If an initial set operation (i.e. at row creation time) tries to set a value for an unknown or unsupported protocol, then a **wrongValue** error must be returned. The value will be overwritten/set when a set operation is performed on the corresponding instance of usmUserCloneFrom. Once instantiated, the value of such an instance of this object can only be changed via a set operation to the value of the usmNoPrivProtocol. If a set operation tries to change the value of an existing instance of this object to any value other than usmNoPrivProtocol, then an **inconsistentValue** error must be returned. Note that if any privacy protocol is used, then you must also use an authentication protocol. In other words, if usmUserPrivProtocol is set to anything else than usmNoPrivProtocol, then the corresponding instance of usmUserAuthProtocol cannot have a value of usmNoAuthProtocol. If it does, then an **inconsistentValue** error must be returned.
Group: usmMIBBasicGroup **Object:** usmUserPublic	**Access:** Read-Create **Syntax:** String **OID:** 1.3.6.1.6.3.16.1.1.1.1 **Definition:** A publicly-readable value which can be written as part of the procedure for changing a user's secret authentication and/or privacy key, and later read to determine whether the change of the secret was effected.
Group: usmMIBBasicGroup **Object:** usmUserSecurityName	**Access:** Read-Only **Syntax:** String **OID:** 1.3.6.1.6.3.16.1.2.1.3.2.7.112.114.105.118.97.116.101 **Definition:** A human readable string representing the user in Security Model independent format. The default transformation of the User-based Security

Group/Object	Description
	Model dependent security ID to the securityName and vice versa is the identity function so that the securityName is the same as the userName.
Group: usmMIBBasicGroup **Object:** usmUserSpinLock	**Access:** Read-Write **Syntax:** Integer **OID:** 1.3.6.1.6.3.16.1.2.1.5.2.7.112.114.105.118.97.116.101 **Definition:** An advisory lock used to allow several cooperating Command Generator Applications to coordinate their use of facilities to alter secrets in the usmUserTable.
Group: usmMIBBasicGroup **Object:** usmUserStatus	**Access:** Read-Create **Syntax:** Integer **OID:** 1.3.6.1.6.3.16.1.2.1.4.2.7.112.114.105.118.97.116.101 **Definition:** The status of this conceptual row. Until instances of all corresponding columns are appropriately configured, the value of the corresponding instance of the usmUserStatus column is **notReady**. In particular, a newly created row for a user who employs authentication, cannot be made active until the corresponding usmUserCloneFrom and usmUserAuthKeyChange have been set. Further, a newly created row for a user who also employs privacy, cannot be made active until the usmUserPrivKeyChange has been set. The RowStatus TC [RFC2579 <rfc2579.html>] requires that this DESCRIPTION clause states under which circumstances other objects in this row can be modified: The value of this object has no effect on whether other objects in this conceptual row can be modified, except for usmUserOwnAuthKeyChange and usmUserOwnPrivKeyChange. For these 2 objects, the value of usmUserStatus MUST be active.
Group: usmMIBBasicGroup **Object:** usmUserStorageType	**Access:** Read-Create **Syntax:** Integer **OID:** 1.3.6.1.6.3.16.1.5.1.0 **Definition:** The storage type for this conceptual row. Conceptual rows having the value **permanent** must allow write-access at a minimum to: • - usmUserAuthKeyChange, usmUserOwnAuthKeyChange and usmUserPublic for a user who employs authentication, and • - usmUserPrivKeyChange, usmUserOwnPrivKeyChange and usmUserPublic for a user who employs privacy. Note that any user who employs authentication or privacy must allow its secret(s) to be updated and thus cannot be **readOnly**. If an initial set operation tries to set the value to **readOnly** for a user who employs authentication or privacy, then an **inconsistentValue** error must be returned. Note that if the value has been previously set (implicit or explicit) to any value, then the rules as defined in the StorageType Textual Convention apply. It is an implementation issue to decide if a SET for a readOnly or permanent row is accepted at all. In some contexts this may make sense, in others it may not. If a SET for a readOnly or permanent row is not accepted at all, then a **wrongValue** error must be returned.

SNMPv2-MIB

Group/Object	Description
Group: snmpBasicNotificationsGroup **Object:** AuthenticationFailure	**Access:** 0 **Syntax:** —

Group/Object	Description
	OID: 1.3.6.1.6.3.1.1.5.5 **Definition:** An authenticationFailure trap signifies that the SNMPv2 entity, acting in an agent role, has received a protocol message that is not properly authenticated. While all implementations of the SNMPv2 must be capable of generating this trap, the snmpEnableAuthenTraps object indicates whether this trap will be generated.
Group: snmpGroup **Object:** snmpInASNParseErrs	**Access:** Read-Only **Syntax:** Counter32 **OID:** 1.3.6.1.2.1.1.5.0 **Definition:** The total number of ASN.1 or BER errors encountered by the SNMP entity when decoding received SNMP messages.
Group: snmpCommunityGroup **Object:** snmpInBadCommunityNames	**Access:** Read-Only **Syntax:** Counter32 **OID:** 1.3.6.1.2.1.1.2.0 **Definition:** The total number of SNMP messages delivered to the SNMP entity which used a SNMP community name not known to said entity.
Group: snmpCommunityGroup **Object:** snmpInBadCommunityUses	**Access:** Read-Only **Syntax:** Counter32 **OID:** 1.3.6.1.2.1.1.9.1.3.0 **Definition:** The total number of SNMP messages delivered to the SNMP entity which represented an SNMP operation which was not allowed by the SNMP community named in the message.
Group: snmpGroup **Object:** snmpInBadVersions	**Access:** Read-Only **Syntax:** Counter32 **OID:** 1.3.6.1.2.1.1.9.1.2.0 **Definition:** The total number of SNMP messages which were delivered to the SNMP entity and were for an unsupported SNMP version.
Group: snmpGroup **Object:** snmpInPkts	**Access:** Read-Only **Syntax:** Counter32 **OID:** 1.3.6.1.2.1.1.8.0 **Definition:** The total number of messages delivered to the SNMP entity from the transport service.
Group: snmpGroup **Object:** snmpProxyDrops	**Access:** Read-Only **Syntax:** Counter32 **OID:** 1.3.6.1.2.1.1.9.1.4.0 **Definition:** The total number of GetRequest-PDUs, GetNextRequest-PDUs, GetBulkRequest-PDUs, SetRequest-PDUs, and InformRequest-PDUs delivered to the SNMP entity which were silently dropped because the transmission of the (possibly translated) message to a proxy target failed in a manner (other than a time-out) such that no Response-PDU could be returned.
Group: snmpSetGroup **Object:** snmpSetSerialNo	**Access:** Read-Write **Syntax:** Integer **OID:** 1.3.6.1.2.1.1.7.0 **Definition:** An advisory lock used to allow several cooperating SNMPv2 entities, all acting in a manager role, to coordinate their use of the SNMPv2 set operation. This object is used for coarse-grain coordination. To achieve

Group/Object	Description
	fine-grain coordination, one or more similar objects might be defined within each MIB group, as appropriate.
Group: snmpGroup **Object:** snmpSilentDrops	**Access:** Read-Only **Syntax:** Counter32 **OID:** 1.3.6.1.2.1.1.3.0 **Definition:** The total number of GetRequest-PDUs, GetNextRequest-PDUs, GetBulkRequest-PDUs, SetRequest-PDUs, and InformRequest-PDUs delivered to the SNMP entity which were silently dropped because the size of a reply containing an alternate Response-PDU with an empty variable-bindings field was greater than either a local constraint or the maximum message size associated with the originator of the request.
Group: systemGroup **Object:** sysContact	**Agent Capability:** RC-SNMPv2-MIB-AC **Access:** Read-Write **Syntax:** String **OID:** .1.3.6.1.2.1.6.5.0 **Definition:** The textual identification of the contact person for this managed node, together with information on how to contact this person. If no contact information is known, the value is the zero-length string. The string of up to 49 characters is supported for this object.
Group: systemGroup **Object:** sysDescr	**Access:** Read-Only **Syntax:** String **OID:** .1.3.6.1.2.1.6.7.0 **Definition:** A textual description of the entity. This value should include the full name and version identification of the system's hardware type, software operating-system, and networking software.
Group: systemGroup **Object:** sysLocation	**Agent Capability:** RC-SNMPv2-MIB-AC **Access:** Read-Write **Syntax:** String **OID:** .1.3.6.1.2.1.6.13.1.2.0.0.0.0.22.0.0.0.0.0 **Definition:** The physical location of this node (e.g., **telephone closet, 3rd floor**). If the location is unknown, the value is the zero-length string. The string of up to 49 characters is supported for this object.
Group: systemGroup **Object:** sysName	**Agent Capability:** RC-SNMPv2-MIB-AC **Access:** Read-Write **Syntax:** String **OID:** .1.3.6.1.2.1.6.13.1.3.0.0.0.0.22.0.0.0.0.0 **Definition:** An administratively-assigned name for this managed node. By convention, this is the node's fully-qualified domain name. If the name is unknown, the value is the zero-length string. The string of up to 24 characters is supported for this object.
Group: systemGroup **Object:** sysObjectID	**Access:** Read-Only **Syntax:** String **OID:** .1.3.6.1.2.1.6.13.1.4.0.0.0.0.22.0.0.0.0.0 **Definition:** The vendor's authoritative identification of the network management subsystem contained in the entity. This value is allocated within the SMI enterprises subtree (1.3.6.1.4.1) and provides an easy and unambiguous means for determining **what kind of box** is being

Group/Object	Description
	managed. For example, if vendor **Flintstones, Inc.** was assigned the subtree 1.3.6.1.4.1.4242, it could assign the identifier 1.3.6.1.4.1.4242.1.1 to its **Fred Router**.
Group: systemGroup **Object:** sysORDescr	**Access:** Read-Only **Syntax:** String **OID:** .1.3.6.1.2.1.6.13.1.5.0.0.0.0.22.0.0.0.0.0 **Definition:** A textual description of the capabilities identified by the corresponding instance of sysORID.
Group: systemGroup **Object:** sysORID	**Access:** Read-Only **Syntax:** Integer **OID:** .1.3.6.1.2.1.6.13.1.1.0.0.0.0.22.0.0.0.0.0 **Definition:** An authoritative identification of a capabilities statement with respect to various MIB modules supported by the local SNMPv2 entity acting in an agent role.
Group: systemGroup **Object:** sysORLastChange	**Access:** Read-Only **Syntax:** Timeticks **OID:** .1.3.6.1.2.1.6.9.0 **Definition:** The value of sysUpTime at the time of the most recent change in state or value of any instance of sysORID.
Group: systemGroup **Object:** sysORUpTime	**Access:** Read-Only **Syntax:** TimeStamp **OID:** .1.3.6.1.2.1.6.8.0 **Definition:** The value of sysUpTime at the time this conceptual row was last instanciated.
Group: systemGroup **Object:** sysServices	**Access:** Read-Only **Syntax:** Integer **OID:** .1.3.6.1.2.1.6.14.0 **Definition:** A value which indicates the set of services that this entity may potentially offers. The value is a sum. This sum initially takes the value zero, Then, for each layer, L, in the range 1 through 7, that this node performs transactions for, 2 raised to (L - 1) is added to the sum. For example, a node which performs only routing functions would have a value of 4 (2^(3-1)). In contrast, a node which is a host offering application services would have a value of 72 (2^(4-1) + 2^(7-1)). Note that in the context of the Internet suite of protocols, values should be calculated accordingly: • Layer 1: physical (e.g., repeaters) • Layer 2: datalink/subnetwork (e.g., bridges) • Layer 3: internet (e.g., supports the IP) • Layer 4: end-to-end (e.g., supports the TCP) • Layer 7: applications (e.g., supports the SMTP) For systems including OSI protocols, layers 5 and 6 may also be counted.
Group: systemGroup **Object:** sysUpTime	**Access:** Read-Only **Syntax:** Timeticks **OID:** .1.3.6.1.2.1.6.17.0 **Definition:** The time (in hundredths of a second) since the network management portion of the system was last re-initialized.

SNMP-VIEW-BASED-ACM-MIB

Group/Object	Description
Group: vacmBasicGroup **Object:** vacmAccessContextMatch	**Agent Capability:** RC-SNMP-VIEW-BASED-ACM-MIB-AC **Access:** Read-Only **Syntax:** Integer **OID:** 1.3.6.1.6.3.16.1.5.2.1.3.5.86.49.77.105.98.1.1 **Definition:** If the value of this object is exact(1), then all rows where the contextName exactly matches vacmAccessContextPrefix are selected. If the value of this object is prefix(2), then all rows where the contextName whose starting octets exactly match vacmAccessContextPrefix are selected. This allows for a simple form of wildcarding.
Group: vacmBasicGroup **Object:** vacmAccessNotifyViewName	**Access:** Read-Create **Syntax:** String **OID:** 1.3.6.1.6.3.16.1.5.2.1.6.5.86.49.77.105.98.1.1 **Definition:** The value of an instance of this object identifies the MIB view of the SNMP context to which this conceptual row authorizes access for notifications. The identified MIB view is that one for which the vacmViewTreeFamilyViewName has the same value as the instance of this object; if the value is the empty string or if there is no active MIB view having this value of vacmViewTreeFamilyViewName, then no access is granted.
Group: vacmBasicGroup **Object:** vacmAccessReadViewName	**Access:** Read-Create **Syntax:** String **OID:** 1.3.6.1.6.3.16.1.5.2.1.5.5.86.49.77.105.98.1.1 **Definition:** The value of an instance of this object identifies the MIB view of the SNMP context to which this conceptual row authorizes read access. The identified MIB view is that one for which the vacmViewTreeFamilyViewName has the same value as the instance of this object; if the value is the empty string or if there is no active MIB view having this value of vacmViewTreeFamilyViewName, then no access is granted.
Group: vacmBasicGroup **Object:** vacmAccessStatus	**Access:** Read-Only **Syntax:** Integer **OID:** 1.3.6.1.6.3.16.1.5.2.1.4.5.86.49.77.105.98.1.1 **Definition:** The status of this conceptual row. The RowStatus TC [RFC2579 <rfc2579.html>] requires that this DESCRIPTION clause states under which circumstances other objects in this row can be modified: The value of this object has no effect on whether other objects in this conceptual row can be modified.
Group: vacmBasicGroup **Object:** vacmAccessStorageType	**Access:** Read-Only **Syntax:** Integer **Definition:** The storage type for this conceptual row. Conceptual rows having the value **permanent** need not allow write-access to any columnar objects in the row.
Group: vacmBasicGroup **Object:** vacmAccessWriteViewName	**Access:** Read-Create **Syntax:** String **Definition:** The value of an instance of this object identifies the MIB view of the SNMP context to which this conceptual row authorizes write access. The identified MIB view is that one for which the vacmViewTreeFamilyViewName has the same value as the instance of this object; if the value is the

Group/Object	Description
	empty string or if there is no active MIB view having this value of vacmViewTreeFamilyViewName, then no access is granted.
Group: vacmBasicGroup **Object:** vacmContextName	**Access:** Read-Only **Syntax:** String **Definition:** A human readable name identifying a particular context at a particular SNMP entity. The empty contextName (zero length) represents the default context.
Group: vacmBasicGroup **Object:** vacmGroupName	**Access:** Read-Create **Syntax:** String **Definition:** The name of the group to which this entry (e.g., the combination of securityModel and securityName) belongs. This groupName is used as index into the vacmAccessTable to select an access control policy. However, a value in this table does not imply that an instance with the value exists in table vacmAccesTable.
Group: vacmBasicGroup **Object:** vacmSecurityToGroupStatus	**Access:** Read-Create **Syntax:** Integer **Definition:** The status of this conceptual row. Until instances of all corresponding columns are appropriately configured, the value of the corresponding instance of the vacmSecurityToGroupStatus column is **notReady**. In particular, a newly created row cannot be made active until a value has been set for vacmGroupName. The RowStatus TC [RFC2579 <rfc2579.html>] requires that this DESCRIPTION clause states under which circumstances other objects in this row can be modified: The value of this object has no effect on whether other objects in this conceptual row can be modified.
Group: vacmBasicGroup **Object:** vacmSecurityToGroupStorageType	**Access:** Read-Create **Syntax:** Integer **Definition:** The storage type for this conceptual row. Conceptual rows having the value **permanent** need not allow write-access to any columnar objects in the row.
Group: vacmBasicGroup **Object:** vacmViewSpinLock	**Access:** Read-Write **Syntax:** Integer **Definition:** An advisory lock used to allow cooperating SNMP Command Generator applications to coordinate their use of the Set operation in creating or modifying views. When creating a new view or altering an existing view, it is important to understand the potential interactions with other uses of the view. The vacmViewSpinLock should be retrieved. The name of the view to be created should be determined to be unique by the SNMP Command Generator application by consulting the vacmViewTreeFamilyTable. Finally, the named view may be created (Set), including the advisory lock. If another SNMP Command Generator application has altered the views in the meantime, then the spin lock's value will have changed, and so this creation will fail because it will specify the wrong value for the spin lock. Since this is an advisory lock, the use of this lock is not enforced.
Group: vacmBasicGroup **Object:** vacmViewTreeFamilyMask	**Access:** Read-Only **Syntax:** String **Definition:** The bit mask which, in combination with the corresponding instance of vacmViewTreeFamilySubtree, defines a family of view subtrees. Each bit of this bit mask corresponds to a sub-identifier of vacmViewTreeFamilySubtree, with the most significant bit of the i-th octet

Group/Object	Description
	of this octet string value (extended if necessary, see below) corresponding to the (8*i - 7)-th sub-identifier, and the least significant bit of the i-th octet of this octet string corresponding to the (8*i)-th sub-identifier, where i is in the range 1 through 16. Each bit of this bit mask specifies whether or not the corresponding sub-identifiers must match when determining if an OBJECT IDENTIFIER is in this family of view subtrees: a **1** indicates that an exact match must occur: a **0** indicates **wild card**, i.e., any sub-identifier value matches.Thus, the OBJECT IDENTIFIER X of an object instance is contained in a family of view subtrees if, for each sub-identifier of the value of vacmViewTreeFamilySubtree, either: • the i-th bit of vacmViewTreeFamilyMask is 0, or • the i-th sub-identifier of X is equal to the i-th sub-identifier of the value of vacmViewTreeFamilySubtree If the value of this bit mask is M bits long and there are more than M sub-identifiers in the corresponding instance of vacmViewTreeFamilySubtree, then the bit mask is extended with 1's to be the required length. Note that when the value of this object is the zero-length string, this extension rule results in a mask of all-1's being used (i.e., no **wild card**), and the family of view subtrees is the one view subtree uniquely identified by the corresponding instance of vacmViewTreeFamilySubtree. Note that masks of length greater than zero length do not need to be supported. In this case this object is made Read-Only.
Group: vacmBasicGroup **Object:** vacmViewTreeFamilyStatus	**Access:** Read-Only **Syntax:** Integer **Definition:** The status of this conceptual row. The RowStatus TC [RFC2579 <rfc2579.html>] requires that this DESCRIPTION clause states under which circumstances other objects in this row can be modified: The value of this object has no effect on whether other objects in this conceptual row can be modified.
Group: vacmBasicGroup **Object:** vacmViewTreeFamilyStorageType	**Access:** Read-Only **Syntax:** Integer **Definition:** The storage type for this conceptual row. Conceptual rows having the value **permanent** need not allow write-access to any columnar objects in the row.
Group: vacmBasicGroup **Object:** vacmViewTreeFamilyType	**Access:** Read-Only **Syntax:** Integer **Definition:** Indicates whether the corresponding instances of vacmViewTreeFamilySubtree and vacmViewTreeFamilyMask define a family of view subtrees which is included in or excluded from the MIB view.

TCP-MIB

Group/Object	Description
Group: tcpGroup **Object:** tcpActiveOpens	**Access:** Read-Only **Syntax:** Counter32 **OID:** .1.3.6.1.2.1.6.4.0 **Definition:** The number of times TCP connections have made a direct transition to the SYN-SENT state from the CLOSED state.
Group: tcpGroup **Object:** tcpAttemptFails	**Access:** Read-Only **Syntax:** Counter32

Group/Object	Description
	OID: .1.3.6.1.2.1.6.15.0 **Definition:** The number of times TCP connections have made a direct transition to the CLOSED state from either the SYN-SENT state or the SYN-RCVD state, plus the number of times TCP connections have made a direct transition to the LISTEN state from the SYN-RCVD state.
Group: tcpGroup **Object:** tcpConnLocalAddress	**Access:** Read-Only **Syntax:** IpAddress **OID:** .1.3.6.1.2.1.6.11.0 **Definition:** The local IP address for this TCP connection. In the case of a connection in the listen state which is willing to accept connections for any IP interface associated with the node, the value 0.0.0.0 is used.
Group: tcpGroup **Object:** tcpConnLocalPort	**Access:** Read-Only **Syntax:** Integer **OID:** .1.3.6.1.2.1.6.6.0 **Definition:** The local port number for this TCP connection.
Group: tcpGroup **Object:** tcpConnRemAddress	**Access:** Read-Only **Syntax:** IpAddress **OID:** .1.3.6.1.2.1.6.12.0 **Definition:** The remote IP address for this TCP connection.
Group: tcpGroup **Object:** tcpConnRemPort	**Access:** Read-Only **Syntax:** Integer **OID:** .1.3.6.1.2.1.6.1.0 **Definition:** The remote port number for this TCP connection.
Group: tcpGroup **Object:** tcpConnState	**Access:** Read-Write **Syntax:** Integer **OID:** .1.3.6.1.2.1.6.3.0 **Definition:** The state of this TCP connection. The only value which may be set by a management station is deleteTCB(12). Accordingly, it is appropriate for an agent to return a **badValue** response if a management station attempts to set this object to any other value. If a management station sets this object to the value deleteTCB(12), then this has the effect of deleting the TCB (as defined in RFC 793) of the corresponding connection on the managed node, resulting in immediate termination of the connection. As an implementation-specific option, a RST segment may be sent from the managed node to the other TCP endpoint (note however that RST segments are not sent reliably).
Group: tcpGroup **Object:** tcpCurrEstab	**Access:** Read-Only **Syntax:** Gauge32 **OID:** .1.3.6.1.2.1.6.2.0 **Definition:** The number of TCP connections for which the current state is either ESTABLISHED or CLOSE- WAIT.
Group: tcpGroup **Object:** tcpEstabResets	**Access:** Read-Only **Syntax:** Counter32 **OID:** .1.3.6.1.2.1.7.1.0

Group/Object	Description
	Definition: The number of times TCP connections have made a direct transition to the CLOSED state from either the ESTABLISHED state or the CLOSE-WAIT state.
Group: tcpGroup **Object:** tcpInErrs	**Access:** Read-Only **Syntax:** Counter32 **OID:** .1.3.6.1.2.1.7.3.0 **Definition:** The total number of segments received in error (e.g., bad TCP checksums).
Group: tcpGroup **Object:** tcpInSegs	**Access:** Read-Only **Syntax:** Counter32 **OID:** .1.3.6.1.2.1.7.5.1.1.0.0.0.0.69 **Definition:** The total number of segments received, including those received in error. This count includes segments received on currently established connections.
Group: tcpGroup **Object:** tcpMaxConn	**Access:** Read-Only **Syntax:** Integer **OID:** .1.3.6.1.2.1.7.5.1.2.0.0.0.0.69 **Definition:** The limit on the total number of TCP connections the entity can support. In entities where the maximum number of connections is dynamic, this object should contain the value -1.
Group: tcpGroup **Object:** tcpOutRsts	**Access:** Read-Only **Syntax:** Counter32 **OID:** .1.3.6.1.2.1.7.2.0 **Definition:** The number of TCP segments sent containing the RST flag.
Group: tcpGroup **Object:** tcpOutSegs	**Access:** Read-Only **Syntax:** Counter32 **OID:** .1.3.6.1.2.1.7.4.0 **Definition:** The total number of segments sent, including those on current connections but excluding those containing only retransmitted octets.
Group: tcpGroup **Object:** tcpPassiveOpens	**Access:** Read-Only **Syntax:** Counter32 **OID:** 1.3.6.1.6.3.15.1.1.6.0 **Definition:** The number of times TCP connections have made a direct transition to the SYN-RCVD state from the LISTEN state.
Group: tcpGroup **Object:** tcpRetransSegs	**Access:** Read-Only **Syntax:** Counter32 **OID:** 1.3.6.1.6.3.15.1.1.2.0 **Definition:** The number of times TCP connections have made a direct transition to the SYN-RCVD state from the LISTEN state.
Group: tcpGroup **Object:** tcpRtoAlgorithm	**Access:** Read-Only **Syntax:** Integer **OID:** 1.3.6.1.6.3.15.1.1.4.0 **Definition:** The algorithm used to determine the timeout value used for retransmitting unacknowledged octets.
Group: tcpGroup	**Access:** Read-Only

Group/Object	Description
Object: tcpRtoMax	**Syntax:** Integer **OID:** 1.3.6.1.6.3.15.1.1.3.0 **Definition:** The maximum value permitted by a TCP implementation for the retransmission timeout, measured in milliseconds. More refined semantics for objects of this type depend upon the algorithm used to determine the retransmission timeout. In particular, when the timeout algorithm is rsre(3), an object of this type has the semantics of the UBOUND quantity described in RFC 793.
Group: tcpGroup **Object:** tcpRtoMin	**Access:** Read-Only **Syntax:** Integer **OID:** 1.3.6.1.6.3.15.1.1.1.0 **Definition:** The minimum value permitted by a TCP implementation for the retransmission timeout, measured in milliseconds. More refined semantics for objects of this type depend upon the algorithm used to determine the retransmission timeout. In particular, when the timeout algorithm is rsre(3), an object of this type has the semantics of the LBOUND quantity described in RFC 793.

UDP-MIB

Group/Object	Description
Group: udpGroup **Object:** udpInDatagrams	**Access:** Read-Only **Syntax:** Counter32 **OID:** 1.3.6.1.6.3.15.1.1.5.0 **Definition:** The total number of UDP datagrams delivered to UDP users.
Group: udpGroup **Object:** udpInErrors	**Access:** Read-Only **Syntax:** Counter32 **OID:** 1.3.6.1.6.3.15.1.2.2.1.6 **Definition:** The number of received UDP datagrams that could not be delivered for reasons other than the lack of an application at the destination port.
Group: udpGroup **Object:** udpLocalAddress	**Access:** Read-Only **Syntax:** IpAddress **OID:** 1.3.6.1.6.3.15.1.2.2.1.5.11.128.0.58.156.3.0.10.220.0.128.72.4.97.112.118.51 **Definition:** The local IP address for this UDP listener. In the case of a UDP listener which is willing to accept datagrams for any IP interface associated with the node, the value 0.0.0.0 is used.
Group: udpGroup **Object:** udpLocalPort	**Access:** Read-Only **Syntax:** Integer **OID:** 1.3.6.1.6.3.15.1.2.2.1.4.11.128.0.58.156.3.0.10.220.0.128.72.4.97.112.118.51 **Definition:** The local port number for this UDP listener.
Group: udpGroup **Object:** udpNoPorts	**Access:** Read-Only **Syntax:** Counter32 **OID:** 1.3.6.1.6.3.15.1.2.2.1.7 **Definition:** The total number of received UDP datagrams for which there was no application at the destination port.
Group: udpGroup	**Access:** Read-Only

Group/Object	Description
Object: udpOutDatagrams	**Syntax:** Counter32 **OID:** 1.3.6.1.6.3.15.1.2.2.1.10 **Definition:** The total number of UDP datagrams sent from this entity.

14.1.2 Supported proprietary RUGGEDCOM MIBs

RUGGEDCOM ROS supports the following proprietary RUGGEDCOM MIBs:

⚠ NOTICE

This section lists all MIBs supported by RUGGEDCOM ROS, and is intended for reference purposes only. Individual device support may vary.

- **RUGGEDCOM-AAA-SERVER-MIB**
  For more information, refer to "RUGGEDCOM-AAA-SERVER-MIB" (Page 378).
- **RUGGEDCOM-DIGITAL-INPUTS-MIB**
  For more information, refer to "RUGGEDCOM-DIGITAL-INPUTS-MIB" (Page 379).
- **RUGGEDCOM-GPS-MIB**
  For more information, refer to "RUGGEDCOM-GPS-MIB" (Page 380).
- **RUGGEDCOM-IP-MIB**
  For more information, refer to "RUGGEDCOM-IP-MIB" (Page 382).
- **RUGGEDCOM-IRIGB-MIB**
  For more information, refer to "RUGGEDCOM-IRIGB-MIB" (Page 382).
- **RUGGEDCOM-MC30-MIB**
  For more information, refer to "RUGGEDCOM-MC30-MIB" (Page 385).
- **RUGGEDCOM-NTP-MIB**
  For more information, refer to "RUGGEDCOM-NTP-MIB" (Page 385).
- **RUGGEDCOM-POE-MIB**
  For more information, refer to "RUGGEDCOM-POE-MIB" (Page 386).
- **RUGGEDCOM-PTP1588-MIB**
  For more information, refer to "RUGGEDCOM-PTP1588-MIB" (Page 389).
- **RUGGEDCOM-SERIAL-MIB**
  For more information, refer to "RUGGEDCOM-SERIAL-MIB" (Page 394).
- **RUGGEDCOM-SFP-DDM-MIB**
  For more information, refer to "RUGGEDCOM-SFP-DDM-MIB" (Page 406).
- **RUGGEDCOM-STP-MIB**
  For more information, refer to "RUGGEDCOM-STP-MIB" (Page 411).
- **RUGGEDCOM-SYS-INFO-MIB**
  For more information, refer to "RUGGEDCOM-SYS-INFO-MIB" (Page 412).
- **RUGGEDCOM-TIMECONFIG-MIB**
  For more information, refer to "RUGGEDCOM-TIMECONFIG-MIB" (Page 417).

RUGGEDCOM-AAA-SERVER-MIB

Group(s)	Object	Description
rcRadiusNotifyGroup	radiusServiceAvailableChange	**OID:** 1.3.6.1.4.1.15004.4.14.1.2.1.3 **Definition:** Notification generated when the status of RADIUS Service changes.
rcRadiusBaseGroup	rcRadiusServerAutUdpPort	**Access:** Read-Write **Syntax:** Integer32 **OID:** 1.3.6.1.4.1.15004.4.14.1.1.1.1.3 **Definition:** The RADIUS server UDP port.
rcRadiusBaseGroup	rcRadiusServerId	**Access:** Read-Only **Syntax:** Integer32 **OID:** 1.3.6.1.4.1.15004.4.14.1.1.1.1.1 **Definition:** The index value used to identify the RADIUS server. 1. Primary Server 2. Backup Server
rcRadiusBaseGroup	rcRadiusServerIP	**Access:** Read-Write **Syntax:** IpAddress **OID:** 1.3.6.1.4.1.15004.4.14.1.1.1.1.2 **Definition:** The RADIUS server IP address.
rcRadiusBaseGroup	rcRadiusServerMaxRetry	**Access:** Read-Write **Syntax:** Integer32 **OID:** 1.3.6.1.4.1.15004.4.14.1.1.1.1.4 **Definition:** The maximum number of times the authenticator will attempt to contact the RADIUS server to authenticate the user in case of any failure.
rcRadiusBaseGroup rcRadiusServiceStatusGroup	rcRadiusServerReachable	**Access:** Read-Only **Syntax:** TruthValue **OID:** 1.3.6.1.4.1.15004.4.14.1.1.1.1.6 **Definition:** The status of the primary RADIUS server.
rcRadiusBaseGroup	rcRadiusServerTimeOut	**Access:** Read-Write **Syntax:** Integer32 **OID:** 1.3.6.1.4.1.15004.4.14.1.1.1.1.5 **Definition:** The amount of time in milliseconds the authenticator will wait for a response from the RADIUS server.
rcRadiusBaseGroup	rcTacacsServerAutTcpPort	**Access:** Read-Write **Syntax:** Integer32 **OID:** 1.3.6.1.4.1.15004.4.14.2.1.1.1.3 **Definition:** The TACACS server TCP port.
rcRadiusBaseGroup	rcTacacsServerId	**Access:** Read-Only **Syntax:** Integer32 **OID:** 1.3.6.1.4.1.15004.4.14.2.1.1.1.1

Group(s)	Object	Description
		Definition: The index value used to identify the TACACS Server. 1. Primary Server 2. Backup Server
rcRadiusBaseGroup	rcTacacsServerIP	**Access:** Read-Write **Syntax:** IpAddress **OID:** 1.3.6.1.4.1.15004.4.14.2.1.1.1.2 **Definition:** The TACACS server IP address.
rcRadiusBaseGroup	rcTacacsServerMaxRetry	**Access:** Read-Write **Syntax:** Integer32 **OID:** 1.3.6.1.4.1.15004.4.14.2.1.1.1.4 **Definition:** The maximum number of times the authenticator will attempt to contact the TACACS server to authenticate the user in case of any failure.
rcTacacsBaseGroup rcTacacsServiceStatusGroup	rcTacacsServerReachable	**Access:** Read-Only **Syntax:** TruthValue **OID:** 1.3.6.1.4.1.15004.4.14.2.1.1.1.6 **Definition:** The status of the TACACS server.
rcTacacsBaseGroup	rcTacacsServerTimeOut	**Access:** Read-Write **Syntax:** Integer32 **OID:** 1.3.6.1.4.1.15004.4.14.2.1.1.1.5 **Definition:** The amount of time in milliseconds the authenticator will wait for a response from the TACACS server.
rcTacacsNotifyGroup	tacacsServiceAvailableChange	**OID:** 1.3.6.1.4.1.15004.5.23 **Definition:** Notification generated when the status of TACACS Service changes.

RUGGEDCOM-DIGITAL-INPUTS-MIB

Group(s)	Object	Description
rcDigitalInputsTableGroup	rcDiActiveState	**Access:** Read-Write **Syntax:** RcLowOrHigh **OID:** 1.3.6.1.4.1.15004.4.8.1.1.1.3.1 **Definition:** A state that would activate an alarm for this digital input.
rcDigitalInputsTableGroup	rcDiAlarm	**Access:** Read-Write **Syntax:** EnabledStatus **OID:** 1.3.6.1.4.1.15004.4.8.1.1.1.2.1 **Definition:** The current alarm status for this digital input. A change of the value of this object will result in sending notification (trap) digitalInputTrap.
rcDigitalInputsTableGroup	rcDiAlarmStatus	**Access:** Read-Only **Syntax:** RcActiveOrInactive **OID:** 1.3.6.1.4.1.15004.4.8.1.1.1.8.1

Group(s)	Object	Description
		Definition: The current alarm status for this digital input. A change of the value of this object will result in sending notification (trap) digitalInputTrap.
rcDigitalInputsTableGroup	rcDiDelayOff	**Access:** Read-Write **Syntax:** Integer32 **OID:** 1.3.6.1.4.1.15004.4.8.1.1.1.5.1 **Definition:** A time for which the input must be inactive before the alarm is deactivated.
rcDigitalInputsTableGroup	rcDiDelayOn	**Access:** Read-Write **Syntax:** Integer32 **OID:** 1.3.6.1.4.1.15004.4.8.1.1.1.4.1 **Definition:** A time for which the input must be active before the alarm is activated.
rcDigitalInputsTableGroup	rcDiDescription	**Access:** Read-Write **Syntax:** DisplayString **OID:** 1.3.6.1.4.1.15004.4.8.1.1.1.6.1 **Definition:** The current digital input state read from hardware.
rcDigitalInputsTableGroup	rcDiID	**Access:** Not-Accessible **Syntax:** Integer32 **OID:** 1.3.6.1.4.1.15004.4.8.1.1.1.1 **Definition:** The physical digital input ID of the device for which this Entry contains configuration settings.
rcDigitalInputsTableGroup	rcDiInputState	**Access:** Read-Only **Syntax:** RcLowOrHigh **OID:** 1.3.6.1.4.1.15004.4.8.1.1.1.7.1 **Definition:** Current digital input state read from hardware.

RUGGEDCOM-GPS-MIB

Group(s)	Object	Description
rcGpsBaseGroup01	rcFreqAdj	**Access:** Read-Only **Syntax:** Integer32 **OID:** 1.3.6.1.4.1.15004.4.9.1.9.0 **Definition:** The current amount of discipline applied to the local frequency reference (TCXO).
rcGpsBaseGroup01	rcGpsAntPower	**Access:** Read-Write **Syntax:** TruthValue **OID:** 1.3.6.1.4.1.15004.4.9.1.4.0 **Definition:** The GPS receiver requires an active antenna. An active antenna includes a preamplifier that filters and amplifies the GPS signals before delivery to the receiver. This option allows the user to activate or deactivate the power of the GPS antenna. If the GPS antenna is shared among

Group(s)	Object	Description
		multiple devices then all but one device should power the GPS antenna.
rcGpsBaseGroup01	rcGpsCableCompensate	**Access:** Read-Write **Syntax:** Integer32 **OID:** 1.3.6.1.4.1.15004.4.9.1.3.0 **Definition:** Cable compensation in nanoseconds may be desired to compensate for a long cable run to minimize the timing inaccuracy.
rcGpsBaseGroup01	rcGpsLatitude	**Access:** Read-Only **Syntax:** DisplayString **OID:** 1.3.6.1.4.1.15004.4.9.1.6.0 **Definition:** The GPS Latitude.
rcGpsBaseGroup01	rcGpsLocInt	**Access:** Read-Write **Syntax:** Integer32 **OID:** 1.3.6.1.4.1.15004.4.9.1.2.0 **Definition:** The time interval in minutes within which the GPS receiver should acquire a lock to the time source. Normally the GPS receiver needs a couple of minutes to lock the signal. The user should set reasonable time interval. If the time interval expires without acquiring the lock then system will distribute time using the local clock.
rcGpsBaseGroup01	rcGpsLongtitude	**Access:** Read-Only **Syntax:** DisplayString **OID:** 1.3.6.1.4.1.15004.4.9.1.7.0 **Definition:** The GPS Longtitude.
rcGpsNotifyGroup rcGpsBaseGroup rcGpsBaseGroup01	rcGpsStatus	**Access:** Read-Only **Syntax:** RcTimeSyncStatus **OID:** 1.3.6.1.4.1.15004.4.9.1.1.0 **Definition:** The system synchronization status when GPS is a primary time source. If the value of this object is changed, an rcGpsStatusChange notification will be generated.
rcGpsNotifyGroup	rcGpsStatusChange	**OID:** 1.3.6.1.4.1.15004.5.19 **Definition:** A notification generated if the status of the GPS module is changed.
rcGpsBaseGroup01	rcOFM	**Access:** Read-Only **Syntax:** Integer32 **OID:** 1.3.6.1.4.1.15004.4.9.1.8.0 **Definition:** The current time offset between system and reference clocks.
rcGpsBaseGroup01	rcSatelliteInView	**Access:** Read-Only **Syntax:** Integer32 **OID:** 1.3.6.1.4.1.15004.4.9.1.5.0 **Definition:** The number of satellites currently being tracked by the GPS module.

RUGGEDCOM-IP-MIB

Group(s)	Object	Description
rcIpObjectsGroup	rcIpConfigDefaultGateway	**Access:** Read-Write **Syntax:** IpAddress **OID:** 1.3.6.1.4.1.15004.4.3.1.3.0 **Definition:** The default IP Gateway for the device.
rcIpObjectsGroupDflt	rcIpConfigDfltMgmtIpAddress	**Access:** Read-Write **Syntax:** IpAddress **OID:** 1.3.6.1.4.1.15004.4.3.1.4.0 **Definition:** The management IP address of the device.
rcIpObjectsGroupDflt	rcIpConfigDfltMgmtIpSubnet	**Access:** Read-Write **Syntax:** IpAddress **OID:** 1.3.6.1.4.1.15004.4.3.1.5.0 **Definition:** The subnet mask associated with the management IP address entry. The value of the mask is an IP address with all the network bits set to 1 and all the hosts bits set to 0.
rcIpObjectsGroup	rcIpConfigMgmtIpAddress	**Access:** Read-Write **Syntax:** IpAddress **OID:** 1.3.6.1.4.1.15004.4.3.1.1.0 **Definition:** The management IP address of the device.
rcIpObjectsGroup	rcIpConfigMgmtIpSubnet	**Access:** Read-Write **Syntax:** IpAddress **OID:** 1.3.6.1.4.1.15004.4.3.1.2.0 **Definition:** The subnet mask associated with the management IP address entry. The value of the mask is an IP address with all the network bits set to 1 and all the hosts bits set to 0.

RUGGEDCOM-IRIGB-MIB

Group(s)	Object	Description
rcIrigbAMOutGroup	rcIrigbAMOutput	**Access:** Read-Write **Syntax:** Integer **OID:** 1.3.6.1.4.1.15004.4.10.1.2.0 **Definition:** Selects the AM (Amplitude Modulation) mode of an IRIGB port.
rcIrigbCommonGroup	rcIrigbCableComp	**Access:** Read-Write **Syntax:** Integer32 **OID:** 1.3.6.1.4.1.15004.4.10.1.7.0 **Definition:** Cable compensation in nanoseconds may be desired to compensate for a long cable run in order to minimize the timing inaccuracy.
rcIrigbCommonGroup	rcIrigbExt	**Access:** Read-Write **Syntax:** Integer

Group(s)	Object	Description
		OID: 1.3.6.1.4.1.15004.4.10.1.4.0 **Definition:** IRIGB extensions use extra bits of the Control Functions (CF) portion of the IRIGB time code. Within this portion of the time code, bits are designated for additional features, including: calendar year, leap seconds, leap seconds pending, Daylight Saving Time (DST), DST pending, local time offset and time quality. Note that only Bxx0, Bxx1, Bxx4 and Bxx5 time codes support IRIGB extensions.
rcIrigbCommonGroup	rcIrigbFreqAdj	**Access:** Read-Write **Syntax:** Integer32 **OID:** 1.3.6.1.4.1.15004.4.10.1.9.0 **Definition:** The current amount of discipline applied to the local frequency reference (TCXO).
rcIrigbInputGroup	rcIrigbInput	**Access:** Read-Write **Syntax:** Integer **OID:** 1.3.6.1.4.1.15004.4.10.1.5.0 **Definition:** This parameter covers both AM and PWM inputs.
rcIrigbCommonGroup	rcIrigbLockInt	**Access:** Read-Write **Syntax:** Integer32 **OID:** 1.3.6.1.4.1.15004.4.10.1.6.0 **Definition:** The time interval in minutes within which the IRIGB receiver should acquire a lock to the time source. Normally the IRIGB receiver needs a couple of minutes to lock the signal. The user should set reasonable time interval. If the time interval expires without acquiring the lock then system will distribute time using the local clock.
rcIrigbCommonGroup	rcIrigbOFM	**Access:** Read-Only **Syntax:** Integer32 **OID:** 1.3.6.1.4.1.15004.4.10.1.8.0 **Definition:** The current time offset between system and reference clocks.
rcIrigbTTLOutput01Group	rcIrigbOutputPWM1	**Access:** Read-Write **Syntax:** Integer **OID:** 1.3.6.1.4.1.15004.4.10.1.10.0 **Definition:** Selects the operational mode of TTL output port. PWM mode complies with IRIG Standard 200-04. PPx provides generic pulse per x second interface to synchronize external devices.
rcIrigbTTLOutput02Group	rcIrigbOutputPWM2	**Access:** Read-Write **Syntax:** Integer **OID:** 1.3.6.1.4.1.15004.4.10.1.14.0 **Definition:** Selects the operational mode of TTL output port2. PWM mode complies with IRIG Standard 200-04. PPx provides generic pulse per x second interface to synchronize external devices.
rcIrigbTTLOutput01Group	rcIrigbPulseInterval1	**Access:** Read-Write **Syntax:** Integer32

Group(s)	Object	Description
		OID: 1.3.6.1.4.1.15004.4.10.1.11.0 **Definition:** Selects the pulse interval in seconds for TTL output port. This parameter is used in conjunction with PPx in order to provide generic pulse per x second interface to synchronize external devices.
rcIrigbTTLOutput02Group	rcIrigbPulseInterval2	**Access:** Read-Write **Syntax:** Integer32 **OID:** 1.3.6.1.4.1.15004.4.10.1.15.0 **Definition:** Selects the pulse interval in seconds for TTL output port2. This parameter is used in conjunction with PPx in order to provide generic pulse per x second interface to synchronize external devices.
rcIrigbTTLOutput01Group	rcIrigbPulseWidth1	**Access:** Read-Write **Syntax:** Integer32 **OID:** 1.3.6.1.4.1.15004.4.10.1.12.0 **Definition:** Selects the pulse width in ms for TTL output port. This parameter is used in conjunction with PPx to control the width of the pulse.
rcIrigbTTLOutput02Group	rcIrigbPulseWidth2	**Access:** Read-Write **Syntax:** Integer32 **OID:** 1.3.6.1.4.1.15004.4.10.1.16.0 **Definition:** Selects the pulse width in ms for TTL output port2. This parameter is used in conjunction with PPx to control the width of the pulse.
rcIrigbTTLOutput01Group	rcIrigbStartTime1	**Access:** Read-Write **Syntax:** RcTimeStamp **OID:** 1.3.6.1.4.1.15004.4.10.1.13.0 **Definition:** This parameter is used in conjunction with PPx to set the starting time of first PPx event. This parameter must be set at least 15 seconds before the start of desired PPx otherwise the first PPx event might be lost.
rcIrigbTTLOutput02Group	rcIrigbStartTime2	**Access:** Read-Write **Syntax:** RcTimeStamp **OID:** 1.3.6.1.4.1.15004.4.10.1.17.0 **Definition:** This parameter is used in conjunction with PPx to set the starting time of first PPx event. This parameter must be set at least 15 seconds before the start of desired PPx otherwise the first PPx event might be lost.
rcIrigbCommonGroup rcIrigbBaseGroup	rcIrigbStatus	**Access:** Read-Only **Syntax:** RcTimeSyncStatus **OID:** 1.3.6.1.4.1.15004.4.10.1.1.0 **Definition:** The system synchronization status when IRIGB is a primary time source. If the value of this object is changed, an rcIrigbStatusChange notification will be sent.
rcIrigbNotifyGroup	rcIrigbStatusChange	**OID:** 1.3.6.1.4.1.15004.5.20 **Definition:** Notification generated if the status of the IRIGB module is changed.

Group(s)	Object	Description
rcIrigbCommonGroup	rcIrigbTimeCode	**Access:** Read-Write **Syntax:** Integer **OID:** 1.3.6.1.4.1.15004.4.10.1.3.0 **Definition:** This device uses the following convention to decode the IRIGB time code: letter [B] represents IRIG-B format, [xx] represents [00] for PWM/TTL mode of operation and [12] for AM operation. For example, Bxx7 represents B007 for PWM/TTL operation and B127 for AM operation. Only Bxx0, Bxx1, Bxx4 and Bxx5 time codes support IRIGB extensions.

RUGGEDCOM-MC30-MIB

Group(s)	Object	Description
rcPoeNotifyGroup	rcPoeOverheat	**Access:** Read-Only **Syntax:** Integer **OID:** 1.3.6.1.4.1.15004.5.12.1 **Definition:** The value of this object will be set to 'true(1)' if PoE is overheated. Whenever the value of this object changes from false(2) to true(1), the device will generate an rcPoeOverheat notification.

RUGGEDCOM-NTP-MIB

Group(s)	Object	Description
rcNTPNotifyGroup	ntpServiceAvailableChange	**OID:** 1.3.6.1.4.1.15004.5.21 **Definition:** A notification generated when the status of NTP service changes.
rcNTPBaseGroup	rcNTPBackUpServerIP	**Access:** Read-Write **Syntax:** IpAddress **OID:** 1.3.6.1.4.1.15004.4.13.1.4.0 **Definition:** The backup server IP address.
rcNTPServiceStatusGroup	rcNTPBackUpServerReachable	**Access:** Read-Only **Syntax:** TruthValue **OID:** 1.3.6.1.4.1.15004.4.13.1.9.0 **Definition:** The status of the backup NTP server.
rcNTPBaseGroup	rcNTPBackUpServerUpdatePeriod	**Access:** Read-Write **Syntax:** Integer32 **OID:** 1.3.6.1.4.1.15004.4.13.1.5.0 **Definition:** The frequency in minutes the (S)NTP server is polled for a time update.
rcNTPBaseGroup	rcNTPFRQADJ	**Access:** Read-Only **Syntax:** Integer32 **OID:** 1.3.6.1.4.1.15004.4.13.1.7.0

Group(s)	Object	Description
		Definition: The current amount of discipline applied to the local frequency reference (TCXO); i.e. the amount of correction on this system required to syntonize to the current reference.
rcNTPBaseGroup	rcNTPOFM	**Access:** Read-Only **Syntax:** Integer32 **OID:** 1.3.6.1.4.1.15004.4.13.1.6.0 **Definition:** The current time offset between (S)NTP server and client clocks and is calculated as <time on the client clock> - <time on the server clock>.
rcNTPBaseGroup	rcNTPPriServerIP	**Access:** Read-Write **Syntax:** IpAddress **OID:** 1.3.6.1.4.1.15004.4.13.1.2.0 **Definition:** The primary server IP Address.
rcNTPServiceStatusGroup	rcNTPPriServerReachable	**Access:** Read-Only **Syntax:** TruthValue **OID:** 1.3.6.1.4.1.15004.4.13.1.8.0 **Definition:** The status of the primary NTP server.
rcNTPBaseGroup	rcNTPPriServerUpdatePeriod	**Access:** Read-Write **Syntax:** Integer32 **OID:** 1.3.6.1.4.1.15004.4.13.1.3.0 **Definition:** The frequency in minutes the (S)NTP server is polled for a time update.
rcNTPBaseGroup	rcSNTPEnabled	**Access:** Read-Write **Syntax:** TruthValue **OID:** 1.3.6.1.4.1.15004.4.13.1.1.0 **Definition:** Enable/disable SNTP server functionality.

RUGGEDCOM-POE-MIB

Group(s)	Object	Description
rcBasePoeGroup	rcPoeCapacity	**Access:** Read-Write **Syntax:** Integer32 **OID:** 1.3.6.1.4.1.15004.4.7.1.1.0 **Definition:** The maximum total output power that can be provided by PoE ports. If the value of this object is set to '0', the capacity is unlimited. When total power consumption reaches this limit, low priority PoE ports will be shut down.
rcBasePoeGroup	rcPoeConsumption	**Access:** Read-Only **Syntax:** Integer32 **OID:** 1.3.6.1.4.1.15004.4.7.1.4.0 **Definition:** The current total power consumption by all PoE devices.

Group(s)	Object	Description
rcBasePoeGroup	rcPoeMinimumVoltage	**Access:** Read-Write **Syntax:** Integer32 **OID:** 1.3.6.1.4.1.15004.4.7.1.2.0 **Definition:** The minimum required voltage to be provided by PoE ports. The minimum required voltage for PoE ports. When PoE voltage drops below this threshold, low priority PoE ports will be shut down.
rcBasePoeStatusGroup	rcPoeOverheatStatus	**Access:** Read-Only **Syntax:** TruthValue **OID:** 1.3.6.1.4.1.15004.4.7.1.5.0 **Definition:** The value of this object will be set to true(1) if PoE is overheated. Whenever the value of this object changes from false(2) to true(1), the device will generate an *rcPoeOverheat* notification.
rcPoeNotifyGroup	rcPoeOverload	**Access:** Read-Only **Syntax:** Integer **OID:** 1.3.6.1.4.1.15004.5.12.2 **Definition:** The value of this object will be set to true(1) if PoE is overloaded. Whenever the value of this object changes from false(2) to true(1), the device will generate an *rcPoeOverload* notification.
rcBasePoeStatusGroup	rcPoeOverloadStatus	**Access:** Read-Only **Syntax:** TruthValue **OID:** 1.3.6.1.4.1.15004.4.7.1.6.0 **Definition:** The value of this object will be set to true(1) if PoE is overloaded. Whenever the value of this object changes from false(2) to true(1), the device will generate an *rcPoeOverload* notification.
rcPoeTableGroup	rcPoePort	**Access:** Not-Accessible **Syntax:** Integer32 **OID:** 1.3.6.1.4.1.15004.4.7.2.1.1.1 **Definition:** The PoE port for which this entry contains information. The value is limited by number of ports in the device.
rcPoeTableGroup	rcPoePortAdmin	**Access:** Read-Write **Syntax:** TruthValue **OID:** 1.3.6.1.4.1.15004.4.7.2.1.1.2.13 **Definition:** The PoE port for which this entry contains information. The value is limited by number of ports in the device.
rcPoeTableGroup	rcPoePortClass	**Access:** Read-Only **Syntax:** Integer32 **OID:** 1.3.6.1.4.1.15004.4.7.2.1.1.5.13 **Definition:** The PoE class value that defines the power level.
rcPoeTableGroup	rcPoePortCurrent	**Access:** Read-Only **Syntax:** Integer32

Group(s)	Object	Description
		OID: 1.3.6.1.4.1.15004.4.7.2.1.1.7.13 **Definition:** The PoE class value that defines the power level.
rcPoeTableGroup	rcPoePortPowered	**Access:** Read-Only **Syntax:** TruthValue **OID:** 1.3.6.1.4.1.15004.4.7.2.1.1.4.13 **Definition:** Whether or not power is currently supplied by the port.
rcPoeTablePriorityGroup	rcPoePortPriority	**Access:** Read-Write **Syntax:** Integer **OID:** 1.3.6.1.4.1.15004.4.7.2.1.1.3.13 **Definition:** The priority of the port. Low priority ports will be shut down first if the power supply is overloaded.
rcPoeTableGroup	rcPoePortVoltage	**Access:** Read-Only **Syntax:** Integer32 **OID:** 1.3.6.1.4.1.15004.4.7.2.1.1.6.13 **Definition:** The PoE Class value that defines the power level.
rcBasePoeGroup	rcPoeReenableTime	**Access:** Read-Write **Syntax:** Unsigned32 **OID:** 1.3.6.1.4.1.15004.4.7.1.3.0 **Definition:** The time to wait to turn on low priority PoE ports again after they were shut down due to overload condition.
rcPoeNotifyGroup	rcPoeUndervoltage	**OID:** 1.3.6.1.4.1.15004.5.12.3 **Definition:** PoE voltage low.
rcBasePoeStatusGroup	rcPoeUndervoltageStatus	**Access:** Read-Only **Syntax:** TruthValue **OID:** 1.3.6.1.4.1.15004.4.7.1.7.0 **Definition:** The character that can be used to force forwarding of accumulated data to the network for connection to the dynamic master. If a packetization character is not configured, accumulated data will be forwarded based upon the packetization timeout parameter *rcPreemptRSDynPackTimer*.
rcBasePoeGroup	rcPoeMaxReenableAttempts	**Access:** Read-Write **Syntax:** Unsigned32 **OID:** 1.3.6.1.4.1.15004.4.7.1.8.0 **Definition:** The maximum number of attempts to re-enable the shutdown PoE ports. If the value of this object is '0', the rcPoeMaxReenableAttempts is 'unlimited'.
rcBasePoeGroup	rcPoePowerManagement	**Access:** Read-Write **Syntax:** Integer **OID:** 1.3.6.1.4.1.15004.4.7.1.9.0 **Definition:** Power management that decides a port would be disconnected or connected. Measured: Use the instantaneous measured power. Negotiated: Use the power determined dynamically by an agreement between two devices (PSE and PD). Auto: For PDs that support power negotiation, the port

Group(s)	Object	Description
		power will be based on the Negotiated power class. All other PDs will use the Measured power.
	rcPoeModuleCapacity	**Access:** Read-Write **Syntax:** Integer32 **OID:** 1.3.6.1.4.1.15004.4.7.1.10.0 **Definition:** The capacity allowed per PoE module. That is, the maximum output power that can be provided by the four PoE ports of each module. When power consumption of a module reached this limit, some module ports will be shutdown.

RUGGEDCOM-PTP1588-MIB

Group(s)	Object	Description
rcPTP1588BaseGroup	rcPTP1588ClkType	**Access:** Read-Write **Syntax:** Integer **OID:** 1.3.6.1.4.1.15004.4.12.1.1.0 **Definition:** The PTP1588 clock type.
rcPTP1588BaseGroup	rcPTP1588E2EDelay	**Access:** Read-Only **Syntax:** Integer32 **OID:** 1.3.6.1.4.1.15004.4.12.1.12.0 **Definition:** The measured E2E (i.e. request-response) delay between master and slave clocks.
rcPTP1588BaseGroup	rcPTP1588GlobalEnable	**Access:** Read-Write **Syntax:** TruthValue **OID:** 1.3.6.1.4.1.15004.4.12.1.13.0 **Definition:** True if PTP is enabled globally.
rcPTP1588BaseGroup	rcPTP1588GlobalP2PRequestInterval	**Access:** Read-Write **Syntax:** TruthValue **OID:** 1.3.6.1.4.1.15004.4.12.1.14.0 **Definition:** The PTP (Precision Time Protocol) Announce interval (mean time interval between successive Announce messages) in seconds.
rcPTP1588BaseGroup	rcPTP1588GlobalE2ERequestInterval	**Access:** Read-Write **Syntax:** Integer32 **OID:** 1.3.6.1.4.1.15004.4.12.1.15.0 **Definition:** The PTP (Precision Time Protocol) Announce interval (mean time interval between successive Announce messages) in seconds.
rcPTP1588BaseGroup	rcPTP1588Global1Step	**Access:** Read-Write **Syntax:** TruthValue **OID:** 1.3.6.1.4.1.15004.4.12.1.16.0 **Definition:** True if PTP is enabled globally.
rcPTP1588BaseGroup	rcPTP1588ClkAnnounceInt	**Access:** Read-Write **Syntax:** Integer32

Group(s)	Object	Description
		OID: 1.3.6.1.4.1.15004.4.12.1.17.0 **Definition:** The PTP (Precision Time Protocol) Announce interval (mean time interval between successive Announce messages) in seconds.
rcPTP1588BaseGroup	rcPTP1588ClkAnnounceRcTout	**Access:** Read-Write **Syntax:** Unsigned32 **OID:** 1.3.6.1.4.1.15004.4.12.1.18.0 **Definition:** The AnnounceReceiptTimeout, an integral multiple of announceInterval.
rcPTP1588BaseGroup	rcPTP1588ClkSyncInt	**Access:** Read-Write **Syntax:** Integer32 **OID:** 1.3.6.1.4.1.15004.4.12.1.19.0 **Definition:** The PTP (Precision Time Protocol) Sync interval (mean time interval between successive Sync messages).
rcPTP1588BaseGroup	rcPTP1588ClkDelayMech	**Access:** Read-Write **Syntax:** Integer32 **OID:** 1.3.6.1.4.1.15004.4.12.1.20.0 **Definition:** The propagation delay measuring option used by the port. For IEEE C37.238 compliant implementations this value shall be 2 (p2p).
rcPTP1588BaseGroup	cPTP1588ClkProfileId	**Access:** Read-Write **Syntax:** Integer32 **OID:** 1.3.6.1.4.1.15004.4.12.1.21.0 **Definition:** Indicates the PTP Profile in use.
rcPTP1588BaseGroup	rcPTP1588ClkDomainNumber	**Access:** Read-Write **Syntax:** Unsigned32 **OID:** 1.3.6.1.4.1.15004.4.12.1.22 **Definition:** Selects the PTP (Precision Time Protocol) domain number. A PTP domain is a logical grouping of PTP clocks that synchronize to each other using the PTP protocol.
rcPTP1588BaseGroup	rcPTP1588ClkNetProtocol	**Access:** Read-Write **Syntax:** Integer32 **OID:** 1.3.6.1.4.1.15004.4.12.1.22.0 **Definition:** Indicates the Network Protocol in use. For IEEE C37.238 compliant implementations this value shall be 1 (ieee8023).
rcPTP1588BaseGroup	rcPTP1588ClkVlanId	**Access:** Read-Write **Syntax:** Integer32 **OID:** 1.3.6.1.4.1.15004.4.12.1.23.0 **Definition:** Indicates the VLAN ID in use: • -2: PVID • -1: Priority tagged • 0: Untagged

Group(s)	Object	Description
		• 1 to 4094: VID set
rcPTP1588BaseGroup	rcPTP1588ClkPriority	**Access:** Read-Write **Syntax:** Unsigned32 **OID:** 1.3.6.1.4.1.15004.4.12.1.24.0 **Definition:** Indicates VLAN tag Priority in use.
rcPTP1588BaseGroup	rcPTP1588ClkAccuracy	**Access:** Read-Write **Syntax:** Integer **OID:** 1.3.6.1.4.1.15004.4.12.1.26 **Definition:** This parameter allows the user to configure the desired clock accuracy. This represents the instantaneous value of the time offset between master and slave clocks. The system will generate an alarm if the time offset from the master exceeds the desired accuracy. • (0): timeAccurateTo50ns • (1): timeAccurateTo100ns • (2): timeAccurateTo250ns • (3): timeAccurateTo1us • (4): timeAccurateTo2to5us • (5): timeAccurateTo10us • (6): timeAccurateTo25us • (7): timeAccurateTo100us • (8): timeAccurateTo250us • (9): timeAccurateTo1ms • (10): timeAccurateTo2to5ms • (11): timeAccurateTo10ms • (12): timeAccurateTo25ms • (13): timeAccurateTo100ms • (14): timeAccurateTo250ms
rcPTP1588BaseGroup	rcPTP1588EthPorts	**Access:** Read-Write **Syntax:** PortList **OID:** 1.3.6.1.4.1.15004.4.12.1.2.0 **Definition:** Selects which Ethernet ports will take part in PTP (Precision Time Protocol) message exchanges.
rcPTP1588BaseGroup	rcPTP1588NetClass	**Access:** Read-Write **Syntax:** Integer **OID:** 1.3.6.1.4.1.15004.4.12.1.4.0 **Definition:** Indicates if all devices in the timing plane are IEEE1588 aware (IEEE1588 network) or if non-IEEE1588 devices are included as well (non-IEEE1588 network).
rcPTP1588BaseGroup	rcPTP1588ServoStatus	**Access:** Read-Only **Syntax:** DisplayString **OID:** 1.3.6.1.4.1.15004.4.12.1.10.0 **Definition:** Shows the status of the clock servo. The clock servo mechanism is used to regulate the system

Group(s)	Object	Description
		clock. The clock status represents clock accuracy is with in the desired limits.
rcPTP1588BaseGroup	rcPTP1588SlaveFeqAdj	**Access:** Read-Only **Syntax:** Integer32 **OID:** 1.3.6.1.4.1.15004.4.12.1.11.0 **Definition:** This parameter shows the current amount of discipline applied to the local frequency reference (TCXO), i.e. the amount of correction on this system required to syntonize to the current reference.
rcPTP1588BaseGroup	rcPTP1588StartUpWait	**Access:** Read-Write **Syntax:** Integer32 **OID:** 1.3.6.1.4.1.15004.4.12.1.3.0 **Definition:** The time in seconds to bootstrap the PTP network in an orderly fashion.
rcPTP1588BCTablesGroup	rcPTP1588BClkPorts	**Access:** Read-Write **Syntax:** PortList **OID:** 1.3.6.1.4.1.15004.4.12.4.1.1.1 **Definition:** The set of ports.
rcPTP1588BCTablesGroup	rcPTP1588BClkGroupName	**Access:** Read-Write **Syntax:** DisplayString **OID:** 1.3.6.1.4.1.15004.4.12.4.1.1.2 **Definition:** The Name assigned to the port group.
rcPTP1588BCTablesGroup	rcPTP1588BClkProfileID	**Access:** Read-Write **Syntax:** Integer **OID:** 1.3.6.1.4.1.15004.4.12.4.1.1.3 **Definition:** Indicates the PTP Profile in use: • (0): defaultP2PProfile • (1): powerProfile • (2): ieee8021as • (3): lxi • (4): telecom • (5): utilityProfile • (6): defaultE2EProfile • (7): customProfile • (8): powerProfileV2
rcPTP1588BCTablesGroup	rcPTP1588BClkDomainNumber	**Access:** Read-Write **Syntax:** Unsigned32 **OID:** 1.3.6.1.4.1.15004.4.12.4.1.1.4 **Definition:** Selects the PTP (Precision Time Protocol) domain number. A PTP domain is a logical grouping of PTP clocks that synchronize to each other using the PTP protocol.
rcPTP1588BCTablesGroup	rcPTP1588BClkTransportProtocol	**Access:** Read-Write **Syntax:** Integer **OID:** 1.3.6.1.4.1.15004.4.12.4.1.1.5

Group(s)	Object	Description
		Definition: Indicates Transport Protocol in use: • (1): layer2multicast • (2): layer3multicast • (3): layer3unicast
rcPTP1588BCTablesGroup	rcPTP1588BClkPathDelayMech	**Access:** Read-Write **Syntax:** Integer **OID:** 1.3.6.1.4.1.15004.4.12.4.1.1.6 **Definition:** The propagation delay measuring option used by the port: • (1): end2end • (2): peer2peer • (3): disabled
rcPTP1588BCTablesGroup	rcPTP1588BClkPTPPortType	**Access:** Read-Write **Syntax:** Integer **OID:** 1.3.6.1.4.1.15004.4.12.4.1.1.7 **Definition:** Selects the PTP (Precision Time Protocol) Port Type: • (1): auto • (2): slaveonly • (3): masteronly
rcPTP1588BCTablesGroup	rcPTP1588BClkSyncInt	**Access:** Read-Write **Syntax:** Integer **OID:** 1.3.6.1.4.1.15004.4.12.4.1.1.8 **Definition:** The PTP (Precision Time Protocol) Sync interval (mean time interval between successive Sync messages). Interpretation placed on the value: • (1): Sync interval value is 125 Milliseconds • (2): Sync interval value is 250 Milliseconds • (3): Sync interval value is 500 Milliseconds • (4): Sync interval value is 1 second • (5): Sync interval value is 2 seconds
rcPTP1588BCTablesGroup	rcPTP1588BClkAnnounceInt	**Access:** Read-Write **Syntax:** Integer **OID:** 1.3.6.1.4.1.15004.4.12.4.1.1.9 **Definition:** The PTP (Precision Time Protocol) Announce interval (mean time interval between successive Announce messages) in seconds. Interpretation placed on the value: • (1): Announce value is 1 second • (2): Announce value is 2 seconds • (3): Announce value is 4 seconds • (4): Announce value is 8 seconds • (5): Announce value is 16 seconds • (6): Announce value is 32 seconds
rcPTP1588BCTablesGroup	rcPTP1588BClkAnnounceRcTout	**Access:** Read-Write

Group(s)	Object	Description
		Syntax: Unsigned32 **OID:** 1.3.6.1.4.1.15004.4.12.4.1.1.10 **Definition:** The AnnounceReceiptTimeout, an integral multiple of announceInterval.
rcPTP1588BCTablesGroup	rcPTP1588BClkAutoReg	**Access:** Read-Write **Syntax:** TruthValue **OID:** 1.3.6.1.4.1.15004.4.12.4.1.1.11 **Definition:** This parameter is specific to unicast transport. This parameter allows users to auto register the slave clock to unicast master as specified by the 'Master IP Address' attribute.
rcPTP1588BCTablesGroup	rcPTP1588BClkMasterIP	**Access:** Read-Write **Syntax:** IpAddress **OID:** 1.3.6.1.4.1.15004.4.12.4.1.1.12 **Definition:** This parameter is specific to unicast transport and represents the IP address of the unicast PTP (Precision Time Protocol) master clock.
rcPTP1588BCTablesGroup	rcPTP1588BClkBackUpIP	**Access:** Read-Write **Syntax:** IpAddress **OID:** 1.3.6.1.4.1.15004.4.12.4.1.1.13 **Definition:** This parameter is specific to unicast transport and represents the IP address of the unicast backup PTP (Precision Time Protocol) master clock.
rcPTP1588BCTablesGroup	rcPTP1588BClkGMIdentity	**Access:** Read-Write **Syntax:** Integer32 **OID:** 1.3.6.1.4.1.15004.4.12.4.1.1.14 **Definition:** The Grandmaster Identity received in GRANDMASTER_ID TLV.
rcPTP1588BCTablesGroup	rcPTP1588BClkVlanId	**Access:** Read-Write **Syntax:** Integer32 **OID:** 1.3.6.1.4.1.15004.4.12.4.1.1.15 **Definition:** Indicates the VLAN ID in use: • -2: PVID • -1: Priority tagged • 0: Untagged • 1 to 4094: VID set
rcPTP1588BCTablesGroup	rcPTP1588BClkPriority	**Access:** Read-Write **Syntax:** Unsigned32 **OID:** 1.3.6.1.4.1.15004.4.12.4.1.1.16 **Definition:** Indicates VLAN tag Priority in use.

RUGGEDCOM-SERIAL-MIB

Group(s)	Object	Description
rcSerialConnStatsGroup	rcConnStatsRxPkts	**Access:** Read-Only

Group(s)	Object	Description
		Syntax: Integer32 **OID:** 1.3.6.1.4.1.15004.4.6.15.1.1.4 **Definition:** The number of received packets.
rcSerialConnStatsGroup	rcConnStatsTxPkts	**Access:** Read-Only **Syntax:** Integer32 **OID:** 1.3.6.1.4.1.15004.4.6.15.1.1.5 **Definition:** The number of transmitted packets
rcSerialDnpGroup	rcDnpAgingTimer	**Access:** Read-Write **Syntax:** Integer32 **OID:** 1.3.6.1.4.1.15004.4.6.8.4.0 **Definition:** The time of communication inactivity after which a learned DNP address is removed from the device address table. Entries in the Link Statistics table with the aged address will be kept until statistics are cleared.
rcSerialDnpGroup	rcDnpDscp	**Access:** Read-Write **Syntax:** Integer32 **OID:** 1.3.6.1.4.1.15004.4.6.8.6.0 **Definition:** The value of DS byte to be set in the IP header. The DS byte setting is supported in the egress direction only.
rcSerialDnpGroup	rcDnpIpPort	**Access:** Read-Write **Syntax:** Integer32 **OID:** 1.3.6.1.4.1.15004.4.6.8.2.0 **Definition:** A local port number on which DNP protocol listens to connections or UDP datagrams.
rcSerialDnpGroup	rcDnpLearning	**Access:** Read-Write **Syntax:** IpAddress **OID:** 1.3.6.1.4.1.15004.4.6.8.3.0 **Definition:** Enable or disable address learning. Learning can be disabled or enabled on the management IP interface, or enabled on an interface with a specific IP address. If learning is enabled and a remote address is not known, a UDP broadcast message will be sent and source addresses will be learned on devices that run the DNP protocol. If a local address is not known, a message will be sent to all serial ports running the DNP protocol. Local addresses will be learned from local responses. If TCP transport is configured, a connection will be established to the devices with the corresponding IP address.
rcSerialDnpGroup	rcDnpLinkStats	**Access:** Read-Write **Syntax:** Integer32 **OID:** 1.3.6.1.4.1.15004.4.6.8.5.0 **Definition:** Enables links statistics collection.
rcSerialDnpRsGroup	rcDnpRsCalllDir	**Access:** Read-Write **Syntax:** RcCallDir **OID:** 1.3.6.1.4.1.15004.4.6.9.1.1.2.1 **Definition:** Defines the following:

Group(s)	Object	Description
		• in(0): Accept an incoming connection • out(1): Place an outgoing connection • both(2): Place an outgoing connection and wait for an incoming connection **Note** This parameter is applicable only for TCP transport.
rcSerialDnpRsGroup	rcDnpRsIpAdd	**Access:** Read-Write **Syntax:** IpAddress **OID:** 1.3.6.1.4.1.15004.4.6.9.1.1.7.1 **Definition:** Defines the IpAddress based on the following: • For outgoing TCP connection (client), 'rcRawSockCallDir' is 'out(2)'. This is the remote IP address to communicate with. • For incoming TCP connection (server), 'rcRawSockCallDir' is 'out(2)' or 'both(3)'. This is the local interface IP address to listen to the local port for a connection request. • For both, outgoing and incoming connections enabled (client or server), 'rcRawSockCallDir' is 'both(3)'. This is the remote IP address where to place an outgoing TCP connection request or from which to accept calls. • For UDP transport, the address of the interface to listen to UDP datagrams.
rcSerialDnpRsGroup	rcDnpRsLinkStats	**Access:** Read-Write **Syntax:** EnabledStatus **OID:** 1.3.6.1.4.1.15004.4.6.9.1.1.8.1 **Definition:** Enables links statistics collection.
rcSerialDnpRsGroup	rcDnpRsLocPort	**Access:** Read-Write **Syntax:** Integer32 **OID:** 1.3.6.1.4.1.15004.4.6.9.1.1.5.1 **Definition:** The local IP port to listen to an incoming TCP connection or UDP datagrams.
rcSerialDnpRsGroup	rcDnpRsMaxConns	**Access:** Read-Write **Syntax:** Integer32 **OID:** 1.3.6.1.4.1.15004.4.6.9.1.1.4.1 **Definition:** The maximum number of allowed incoming TCP connections.
rcSerialDnpRsGroup	rcDnpRsRemPort	**Access:** Read-Write **Syntax:** Integer32 **OID:** 1.3.6.1.4.1.15004.4.6.9.1.1.6.1 **Definition:** The remote TCP port to use when placing an outgoing connection.
rcSerialDnpRsGroup	rcDnpRsTransport	**Access:** Read-Write **Syntax:** RcTransport **OID:** 1.3.6.1.4.1.15004.4.6.9.1.1.3.1

Group(s)	Object	Description
		Definition: A transport protocol used for IP traffic for DNPRS on this port.
rcSerialDnpGroup	rcDnpTransport	**Access:** Read-Write **Syntax:** RcTransport **OID:** 1.3.6.1.4.1.15004.4.6.8.1.0 **Definition:** A transport protocol used for IP traffic for DNP protocol.
	rcMbClient	**OID:** 1.3.6.1.4.1.15004.4.6.3 **Definition:** The main subtree for managing the Modbus protocol client settings on RUGGEDCOM serial devices.
	rcMbClientDscp	**Access:** Read-Write **Syntax:** Integer32 **OID:** 1.3.6.1.4.1.15004.4.6.3.4.0 **Definition:** The value of DS byte to be set in the IP header. DS byte setting is supported in the egress direction only.
	rcMbClientFwdExcp	**Access:** Read-Write **Syntax:** Integer32 **OID:** 1.3.6.1.4.1.15004.4.6.3.2.0 **Definition:** Enables forwarding exception messages to the Master as exception codes 10 (no path) or 11 (no response). When the Master polls for an unconfigured RTU or the remote Modbus server receives a poll for an RTU which is not configured or is timing out, it returns an exception message. This object should be set to 'disabled(2)' if the Master does not support exceptions but recognizes failure by time-out when waiting for response.
	rcMbClientIPPort	**Access:** Read-Write **Syntax:** Integer32 **OID:** 1.3.6.1.4.1.15004.4.6.3.1.0 **Definition:** A remote port number to which the protocol connection manager sends TCP connection requests.
	rcMbClientLinkStats	**Access:** Read-Write **Syntax:** Integer32 **OID:** 1.3.6.1.4.1.15004.4.6.3.3.0 **Definition:** Enables link statistics collection.
rcSerialMbServerGroup	rcMbServerAuxTcpPort	**Access:** Read-Write **Syntax:** Integer32 **OID:** 1.3.6.1.4.1.15004.4.6.2.1.1.3.1 **Definition:** The alternative TCP port number where an 'rcMbServerPort' may listen to incoming TCP connections. As the TCP Modbus server always listens on TCP port 502, this parameter allows the RUGGEDCOM serial device to accept TCP Modbus Protocol connections request on both TCP ports.
rcSerialMbServerGroup	rcMbServerLinkStats	**Access:** Read-Write **Syntax:** EnabledStatus **OID:** 1.3.6.1.4.1.15004.4.6.2.1.1.5.1

Group(s)	Object	Description
		Definition: Enables links statistics collection.
	rcMbServerPort	**Access:** Not-Accessible **Syntax:** Integer **OID:** 1.3.6.1.4.1.15004.4.6.2.1.1.1 **Definition:** The physical serial port number for which this entry contains the Modbus server protocol configuration settings.
rcSerialMbServerGroup	rcMbServerRespTimer	**Access:** Read-Write **Syntax:** Integer32 **OID:** 1.3.6.1.4.1.15004.4.6.2.1.1.2.1 **Definition:** The allowable time to wait for the RTU to start to respond.
rcSerialMbServerGroup	rcMbServerSendExcep	**Access:** Read-Write **Syntax:** EnabledStatus **OID:** 1.3.6.1.4.1.15004.4.6.2.1.1.4.1 **Definition:** Allows the RUGGEDCOM serial devices to enable or disable sending TCP Modbus exception back to the master if no response has been received from the RTU within the expected time.
rcSerialMicrolokGroup	rcMicrolokDscp	**Access:** Read-Write **Syntax:** Integer32 **OID:** 1.3.6.1.4.1.15004.4.6.7.4.0 **Definition:** The value of DS byte to be set in the IP header. The DS byte setting is supported in the egress direction only.
rcSerialMicrolokGroup	rcMicrolokIpPort	**Access:** Read-Write **Syntax:** Integer32 **OID:** 1.3.6.1.4.1.15004.4.6.7.2.0 **Definition:** A local port number on which the Microlok protocol listens to connections or UDP datagrams.
rcSerialMicrolokGroup	rcMicrolokLinkStats	**Access:** Read-Write **Syntax:** EnabledStatus **OID:** 1.3.6.1.4.1.15004.4.6.7.3.0 **Definition:** Enables links statistics collection.
rcSerialMicrolokGroup	rcMicrolokTransport	**Access:** Read-Write **Syntax:** RcTransport **OID:** 1.3.6.1.4.1.15004.4.6.7.1.0 **Definition:** A transport protocol used for IP traffic for the Microlok protocol.
rcSerialMirrBitsGroup	rcMirrBitsIpAdd	**Access:** Read-Write **Syntax:** IpAddress **OID:** 1.3.6.1.4.1.15004.4.6.10.1.1.5.1 **Definition:** The IP Address of the interface to listen to UDP datagrams.
rcSerialMirrBitsGroup	rcMirrBitsLinkStats	**Access:** Read-Write **Syntax:** EnabledStatus

Group(s)	Object	Description
		OID: 1.3.6.1.4.1.15004.4.6.10.1.1.6.1 **Definition:** Enables links statistics collection.
rcSerialMirrBitsGroup	rcMirrBitsLocPort	**Access:** Read-Write **Syntax:** Integer32 **OID:** 1.3.6.1.4.1.15004.4.6.10.1.1.3.1 **Definition:** The local IP port to listen to UDP datagrams.
rcSerialMirrBitsGroup	rcMirrBitsRemPort	**Access:** Read-Write **Syntax:** Integer32 **OID:** 1.3.6.1.4.1.15004.4.6.10.1.1.4.1 **Definition:** The remote port to which protocols on this port can exchange UDP datagrams.
rcSerialMirrBitsGroup	rcMirrBitsTransport	**Access:** Read-Write **Syntax:** RcTransport **OID:** 1.3.6.1.4.1.15004.4.6.10.1.1.2.1 **Definition:** A transport protocol used for IP traffic for mirrored bits on this port. This object is always set to value 'udp(2)'.
rcSerialPreEmpRawSockGroup	rcPreemptRSDynPackChar	**Access:** Read-Write **Syntax:** Integer32 **OID:** 1.3.6.1.4.1.15004.4.6.5.1.1.10.1 **Definition:** The character that can be used to force forwarding of accumulated data to the network for connection to the dynamic master. If a packetization character is not configured, accumulated data will be forwarded based upon the packetization timeout parameter *rcPreemptRSDynPackTimer*.
rcSerialPreEmpRawSockGroup	rcPreemptRSDynPackTimer	**Access:** Read-Write **Syntax:** Integer32 **OID:** 1.3.6.1.4.1.15004.4.6.5.1.1.11.1 **Definition:** The delay in milliseconds from the last received character until when data is forwarded to the dynamic master.
rcSerialPreEmpRawSockGroup	rcPreemptRSDynTimeout	**Access:** Read-Write **Syntax:** Integer32 **OID:** 1.3.6.1.4.1.15004.4.6.5.1.1.12.1 **Definition:** The time in seconds allowed for the dynamic master to be idle before its connection is closed. The protocol listens to the socket open to the dynamic master, and if no data is received within this time, the connection will be closed.
rcSerialPreEmpRawSockGroup	rcPreemptRSFlowControl	**Access:** Read-Write **Syntax:** RcFlowControl **OID:** 1.3.6.1.4.1.15004.4.6.5.1.1.5.1 **Definition:** The type of FlowControl to be used on the port.
rcSerialPreEmpRawSockGroup	rcPreemptRSIpAdd	**Access:** Read-Write **Syntax:** IpAddress

Group(s)	Object	Description
		OID: 1.3.6.1.4.1.15004.4.6.5.1.1.8.1 **Definition:** Defines the IpAddress based on the following: • For outgoing TCP connections (client), 'rcRawSockCallDir' is 'out(2)' is the remote IP address to communicate with. • For incoming TCP connections (server), 'rcRawSockCallDir' is 'out(2)' or 'both(3)' is the local interface IP address to listen to the local port for a connection request. • For both outgoing and incoming connections enabled (client or server), 'rcRawSockCallDir' is 'both(3)' is the remote IP address to place an outgoing TCP connection request or from which to accept calls.
rcSerialPreEmpRawSockGroup	rcPreemptRSLinkStats	**Access:** Read-Write **Syntax:** EnabledStatus **OID:** 1.3.6.1.4.1.15004.4.6.5.1.1.9.1 **Definition:** Enables links statistics collection.
rcSerialPreEmpRawSockGroup	rcPreemptRSLocPort	**Access:** Read-Write **Syntax:** Integer32 **OID:** 1.3.6.1.4.1.15004.4.6.5.1.1.6.1 **Definition:** The local IP port to listen to an incoming TCP connection or UDP datagram.
rcSerialPreEmpRawSockGroup	rcPreemptRSPackChar	**Access:** Read-Write **Syntax:** Integer32 **OID:** 1.3.6.1.4.1.15004.4.6.5.1.1.2.1 **Definition:** The character that can be used to force forwarding of accumulated data to the network. If a packetization character is not configured, the object is set to the value of '256' and accumulated data will be forwarded based on the packetization timeout parameter which is the value set for object *rcPreemptRSPackTimer*.
rcSerialPreEmpRawSockGroup	rcPreemptRSPackSize	**Access:** Read-Write **Syntax:** Integer32 **OID:** 1.3.6.1.4.1.15004.4.6.5.1.1.4.1 **Definition:** The Maximum number of bytes received from the serial port to be packed in one IP packet.
rcSerialPreEmpRawSockGroup	rcPreemptRSPackTimer	**Access:** Read-Write **Syntax:** Integer32 **OID:** 1.3.6.1.4.1.15004.4.6.5.1.1.3.1 **Definition:** The delay in milliseconds from the last received character until when data is forwarded.
rcSerialPreEmpRawSockGroup	rcPreemptRSRemPort	**Access:** Read-Write **Syntax:** Integer32 **OID:** 1.3.6.1.4.1.15004.4.6.5.1.1.7.1 **Definition:** The remote TCP port to use when placing an outgoing connection.
rcSerialRawSocketGroup	rcRawSockCallDir	**Access:** Read-Write **Syntax:** RcCallDir

Group(s)	Object	Description
		OID: 1.3.6.1.4.1.15004.4.6.4.1.1.7.1 **Definition:** Defines following: • in(0): Accept an incoming connection • out(1): Place an outgoing connection • both(2): Place an outgoing connection and wait for an incoming connection **Note** This parameter is applicable only for TCP transport.
rcSerialRawSocketGroup	rcRawSockFlowControl	**Access:** Read-Write **Syntax:** RcFlowControl **OID:** 1.3.6.1.4.1.15004.4.6.4.1.1.5.1 **Definition:** The type of FlowControl to be used on the port.
rcSerialRawSocketGroup	rcRawSockIpAdd	**Access:** Read-Write **Syntax:** IpAddress **OID:** 1.3.6.1.4.1.15004.4.6.4.1.1.11.1 **Definition:** >Defines the IpAddress based on the following: • For outgoing TCP connections (client), 'rcRawSockCallDir' is 'out(2)' is the remote IP address to communicate with. • For incoming TCP connections (server), 'rcRawSockCallDir' is 'out(2)' or 'both(3)' is the local interface IP address to listen to the local port for a connection request. • For both outgoing and incoming connections enabled (client or server), 'rcRawSockCallDir' is 'both(3)' is the remote IP address to place an outgoing TCP connection request or from which to accept calls. • For UDP transport, the address of the interface to listen to UDP datagrams.
rcSerialRawSocketGroup	rcRawSockLinkStats	**Access:** Read-Write **Syntax:** EnabledStatus **OID:** 1.3.6.1.4.1.15004.4.6.4.1.1.12.1 **Definition:** Enables links statistics collection for RawSocket on this port.
rcSerialRawSocketGroup	rcRawSockLocPort	**Access:** Read-Write **Syntax:** Integer32 **OID:** 1.3.6.1.4.1.15004.4.6.4.1.1.9.1 **Definition:** The local IP port to listen to an incoming TCP connection or UDP datagrams.
rcSerialRawSocketGroup	rcRawSockMaxConn	**Access:** Read-Write **Syntax:** Integer32 **OID:** 1.3.6.1.4.1.15004.4.6.4.1.1.8.1 **Definition:** The maximum number of allowed incoming TCP connections.
rcSerialMbClientGroup	rcRawSockPackChar	**Access:** Read-Write **Syntax:** Integer32

Group(s)	Object	Description
		OID: 1.3.6.1.4.1.15004.4.6.4.1.1.2.1 **Definition:** The character that can be used to force forwarding of accumulated data to the network. If a packetization character is not configured, the object is set to the value of '256', and accumulated data will be forwarded based upon the packetization timeout parameter which is the value set for object *rcRawSockPackTimer*.
rcSerialRawSocketGroup	rcRawSockPackSize	**Access:** Read-Write **Syntax:** Integer32 **OID:** 1.3.6.1.4.1.15004.4.6.4.1.1.4.1 **Definition:** The maximum number of bytes received from serial port to be forwarded.
rcSerialRawSocketGroup	rcRawSockPackTimer	**Access:** Read-Write **Syntax:** Integer32 **OID:** 1.3.6.1.4.1.15004.4.6.4.1.1.3.1 **Definition:** The delay in ms from the last received character until when data is forwarded.
rcSerialRawSocketGroup	rcRawSockRemPort	**Access:** Read-Write **Syntax:** Integer32 **OID:** 1.3.6.1.4.1.15004.4.6.4.1.1.10.1 **Definition:** The remote IP port to use when placing an outgoing connection.
rcSerialRawSocketGroup	rcRawSockTransport	**Access:** Read-Write **Syntax:** RcTransport **OID:** 1.3.6.1.4.1.15004.4.6.4.1.1.6.1 **Definition:** A transport protocol used for IP traffic for protocols on this port.
rcSerialCommandsGroup	rcSerDeviceCmndClearStats	**Access:** Read-Write **Syntax:** PortList **OID:** 1.3.6.1.4.1.15004.4.6.16.2.0 **Definition:** The list of ports for which the Clearing Statistics command should be performed on RUGGEDCOM serial devices. A read attempt for this object always returns an empty list of ports.
rcSerialCommandsGroup	rcSerDeviceCmndResetPort	**Access:** Read-Write **Syntax:** PortList **OID:** 1.3.6.1.4.1.15004.4.6.16.1.0 **Definition:** The list of ports for which Reset should be performed on RUGGEDCOM serial devices. A read attempt for this object always returns an empty list of ports.
rcSerialPortParamsGroup	rcSerialDscp	**Access:** Read-Write **Syntax:** Integer32 **OID:** 1.3.6.1.4.1.15004.4.6.1.1.1.9.1 **Definition:** The value of DS byte to be set in the IP header. The DS byte setting is supported in the egress direction only.
rcSerialPortParamsGroup	rcSerialForceHD	**Access:** Read-Write

Group(s)	Object	Description
		Syntax: Integer **OID:** 1.3.6.1.4.1.15004.4.6.1.1.1.5.1 **Definition:** Enables forcing half duplex mode of operation on the serial port. When sending data out from the serial port, all received data is ignored. This mode of operation is available only on ports that operate in full duplex mode.
rcSerialPortParamsGroup	rcSerialHoldTime	**Access:** Read-Write **Syntax:** Integer32 **OID:** 1.3.6.1.4.1.15004.4.6.1.1.1.8.1 **Definition:** The maximum amount of time in milliseconds that a serial packet can be held in the queue before being sent to the serial line. Time is measured from the moment the packet is received from the IP layer.
rcSerialPortParamsGroup	rcSerialPortIfIndex	**Access:** Read-Write **Syntax:** InerfaceIndex **OID:** 1.3.6.1.4.1.15004.4.6.1.1.1.2.1 **Definition:** The value of ifIndex for the port. This value is same as 'rs232PortIndex' which is the index used for 'rs232PortTable' in RS-232-MIB.
rcSerialPortParamsGroup	rcSerialPortType	**Access:** Read-Write **Syntax:** RcSerPortType **OID:** 1.3.6.1.4.1.15004.4.6.1.1.1.4.1 **Definition:** A serial port type supported on the serial port represented by this entry.
rcSerialPortParamsGroup	rcSerialPostTxDelay	**Access:** Read-Write **Syntax:** Integer32 **OID:** 1.3.6.1.4.1.15004.4.6.1.1.1.7.1 **Definition:** The number of bits needed to generate the required delay with the configured baud rate('rs232PortOutSpeed') after the last bit of the packet was sent out before serial UART starts listening to the RX line. This value is relevant for RS485 interface only with 'rs232PortType' equals other(1).
rcSerialPortParamsGroup	rcSerialProtocol	**Access:** Read-Write **Syntax:** RcSerProtocol **OID:** 1.3.6.1.4.1.15004.4.6.1.1.1.3.1 **Definition:** A serial protocol supported on the serial port represented by this entry.
rcSerialPortParamsGroup	rcSerialRxtoTxDelay	**Access:** Read-Write **Syntax:** Integer32 **OID:** 1.3.6.1.4.1.15004.4.6.1.1.1.10.1 **Definition:** The minimum amount of time in milliseconds the transmission of a new message should delay after the last message is received through the AI port. This parameter is useful, especially for the half duplex transmission mode, such as two-wire RS485 serial protocol. It ensures the connected device has enough time to turn off its transmitter and to turn

Group(s)	Object	Description
		on its receiver, so it can receive the next message without a single bit loss.
rcSerialPortParamsGroup	rcSerialTurnAround	**Access:** Read-Write **Syntax:** Integer32 **OID:** 1.3.6.1.4.1.15004.4.6.1.1.1.6.1 **Definition:** The amount of delay between the transmission of individual messages from the serial port. For 'rcSerialProtocol' object value modbusServer(3), this value must be non-zero. It represents the delay between sending a broadcast message and the next pollout of the serial port. As RTUs do not reply to a broadcast, sufficient time must be ensured to process them.
rcSerialTelnetComportGroup	rcTelnetComportCallDir	**Access:** Read-Write **Syntax:** RcCallDir **OID:** 1.3.6.1.4.1.15004.4.6.11.1.1.6.1 **Definition:** Defines the following: • in(0): Accept an incoming connection • out(1): Place an outgoing connection • both(2): Place an outgoing connection and wait for an incoming connection **Note** This parameter is applicable only for TCP transport.
rcSerialTelnetComportGroup	rcTelnetComportFlowControl	**Access:** Read-Write **Syntax:** RcFlowControl **OID:** 1.3.6.1.4.1.15004.4.6.11.1.1.5.1 **Definition:** The type of FlowControl to be used on the port.
rcSerialTelnetComportGroup	rcTelnetComportIpAdd	**Access:** Read-Write **Syntax:** IpAddress **OID:** 1.3.6.1.4.1.15004.4.6.11.1.1.9.1 **Definition:** Defines the IpAddress based on the following: • For outgoing TCP connections (client), 'rcRawSockCallDir' is 'out(2)' is the remote IP address to communicate with. • For incoming TCP connections (server), 'rcRawSockCallDir' is 'out(2)' or 'both(3)' is the local interface IP address to listen to the local port for a connection request. • For both outgoing and incoming connections enabled (client or server), 'rcRawSockCallDir' is 'both(3)' is the remote IP address to place an outgoing TCP connection request or from which to accept calls.
rcSerialTelnetComportGroup	rcTelnetComportLinkStats	**Access:** Read-Write **Syntax:** EnabledStatus **OID:** 1.3.6.1.4.1.15004.4.6.11.1.1.10.1 **Definition:** Defines the IpAddress based on the following: • For outgoing TCP connections (client), 'rcRawSockCallDir' is 'out(2)' is the remote IP address to communicate with.

Group(s)	Object	Description
		• For incoming TCP connections (server), 'rcRawSockCallDir' is 'out(2)' or 'both(3)' is the local interface IP address to listen to the local port for a connection request. • For both outgoing and incoming connections enabled (client or server), 'rcRawSockCallDir' is 'both(3)' is the remote IP address to place an outgoing TCP connection request or from which to accept calls.
rcSerialTelnetComportGroup	rcTelnetComportLocPort	**Access:** Read-Write **Syntax:** Integer32 **OID:** 1.3.6.1.4.1.15004.4.6.11.1.1.7.1 **Definition:** The local IP port to listen to an incoming TCP connection.
rcSerialTelnetComportGroup	rcTelnetComportPackChar	**Access:** Read-Write **Syntax:** Integer32 **OID:** 1.3.6.1.4.1.15004.4.6.11.1.1.2.1 **Definition:** The character that can be used to force forwarding of accumulated data to the network. If a packetization character is not configured, the object is set to the value '256', and accumulated data will be forwarded based upon the packetization timeout parameter which is the value set for object *rcTelnetComportPackTimer*.
rcSerialTelnetComportGroup	rcTelnetComportPackSize	**Access:** Read-Write **Syntax:** Integer32 **OID:** 1.3.6.1.4.1.15004.4.6.11.1.1.4.1 **Definition:** The maximum number of bytes received from the serial port to be packed in one IP packet.
rcSerialTelnetComportGroup	rcTelnetComportPackTimer	**Access:** Read-Write **Syntax:** Integer32 **OID:** 1.3.6.1.4.1.15004.4.6.11.1.1.3.1 **Definition:** The delay from the last received character until when data is forwarded.
rcSerialTelnetComportGroup	rcTelnetComportRemPort	**Access:** Read-Write **Syntax:** Integer32 **OID:** 1.3.6.1.4.1.15004.4.6.11.1.1.8.1 **Definition:** The remote TCP port to use when placing an outgoing connection.
rcTimeConfigBaseGroup	rcTimeAndDate	**Access:** Read-Write **Syntax:** DateandTime **OID:** 1.3.6.1.4.1.15004.4.11.1.2.0 **Definition:** This parameter allows for both the viewing and setting of the local time and date in *DateAndTime* format. DateAndTime is a standard textual convention defined in the SNMPv2-TC.

RUGGEDCOM-SFP-DDM-MIB

Group(s)	Object	Description
rcSfpDdmCfgGroup	rcSfpDdmPollingInterval	**Access:** Read-Write **Syntax:** Integer32 **OID:** 1.3.6.1.4.1.15004.4.17.1.1 **Definition:** The time interval in minutes to wait between two consecutive readings from SFP/SFP + transceivers installed. When this interval is set to 0, the SFP DDM feature will be disabled on the system.
rcSfpDdmTableGroup	rcSfpDdmPortTable	**Access:** Not-Accessible **Syntax:** SEQUENCE OF RcSfpDdmPortEntry **OID:** 1.3.6.1.4.1.15004.4.17.2.1 **Definition:** A list of SFP DDM port entries.
rcSfpDdmTableGroup	rcSfpDdmPortEntry	**Access:** Not-Accessible **Syntax:** RcSfpDdmPortEntry **OID:** 1.3.6.1.4.1.15004.4.17.2.1.1 **Definition:** SFP DDM parameters for an SFP port.
rcSfpDdmTableGroup	rcSfpPortId	**Access:** Not-Accessible **Syntax:** Integer32 **OID:** 1.3.6.1.4.1.15004.4.17.2.1.1.1 **Definition:** The SFP port identifier for which this entry contains information. The value is limited by number of SFP ports on the device.
rcSfpDdmTableGroup	rcSfpPlugged	**Access:** Read-Only **Syntax:** TruthValue **OID:** 1.3.6.1.4.1.15004.4.17.2.1.1.2 **Definition:** SFP transceiver is plugged or not. true(1) is plugged and false(2) is unplugged.
rcSfpDdmTableGroup	rcSfpDdmVendorName	**Access:** Read-Only **Syntax:** DisplayString **OID:** 1.3.6.1.4.1.15004.4.17.2.1.1.3 **Definition:** The vendor's name of the SFP transceiver.
rcSfpDdmTableGroup	rcSfpDdmVendorPartNumber	**Access:** Read-Only **Syntax:** DisplayString **OID:** 1.3.6.1.4.1.15004.4.17.2.1.1.4 **Definition:** The vendor's part number of the SFP transceiver.
rcSfpDdmTableGroup	rcSfpDdmVendorRevision	**Access:** Read-Only **Syntax:** DisplayString **OID:** 1.3.6.1.4.1.15004.4.17.2.1.1.5 **Definition:** The vendor's revision of the SFP transceiver.
rcSfpDdmTableGroup	rcSfpDdmVendorSerialNumber	**Access:** Read-Only

Group(s)	Object	Description
		Syntax: DisplayString **OID:** 1.3.6.1.4.1.15004.4.17.2.1.1.6 **Definition:** The vendor's serial number of the SFP transceiver.
rcSfpDdmTableGroup	rcSfpDdmEncoding	**Access:** Read-Only **Syntax:** DisplayString **OID:** 1.3.6.1.4.1.15004.4.17.2.1.1.7 **Definition:** The encoding mechanism of the SFP transceiver.
rcSfpDdmTableGroup	rcSfpDdmNominalBitrate	**Access:** Read-Only **Syntax:** DisplayString **OID:** 1.3.6.1.4.1.15004.4.17.2.1.1.8 **Definition:** The nominal bit rate of the SFP transceiver.
rcSfpDdmTableGroup	rcSfpDdmConnectorType	**Access:** Read-Only **Syntax:** DisplayString **OID:** 1.3.6.1.4.1.15004.4.17.2.1.1.9 **Definition:** The connector type of the SFP transceiver.
rcSfpDdmTableGroup	rcSfpDdmWavelength	**Access:** Read-Only **Syntax:** DisplayString **OID:** 1.3.6.1.4.1.15004.4.17.2.1.1.10 **Definition:** The laser wavelength of the SFP transceiver.
rcSfpDdmTableGroup	rcSfpDdmLinkLength	**Access:** Read-Only **Syntax:** DisplayString **OID:** 1.3.6.1.4.1.15004.4.17.2.1.1.11 **Definition:** The link length of the SFP transceiver.
rcSfpDdmTableGroup	rcSfpDdmImplemented	**Access:** Read-Only **Syntax:** TruthValue **OID:** 1.3.6.1.4.1.15004.4.17.2.1.1.12 **Definition:** SFP DDM is implemented on the SFP transceiver or not. true(1) is implemented and false(2) is not implemented.
rcSfpDdmTableGroup	rcSfpDdmCurrentStatus	**Access:** Read-Only **Syntax:** RcSfpDdmAlarmWarnStatus **OID:** 1.3.6.1.4.1.15004.4.17.2.1.1.12 **Definition:** The current alarm and warning status of the SFP transceiver.
rcSfpDdmTableGroup	rcSfpDdmCurrentTemperature	**Access:** Read-Only **Syntax:** Integer32 **OID:** 1.3.6.1.4.1.15004.4.17.2.1.1.14

Group(s)	Object	Description
		Definition: The current temperature (in units of 0.001 degrees Celsius) of the SFP transceiver.
rcSfpDdmTableGroup	rcSfpDdmThreshTempAlarmLow	**Access:** Read-Only **Syntax:** Integer32 **OID:** 1.3.6.1.4.1.15004.4.17.2.1.1.15 **Definition:** The threshold of low temperature alarm (in units of 0.001 degrees Celsius) of the SFP transceiver.
rcSfpDdmTableGroup	rcSfpDdmThreshTempWarnLow	**Access:** Read-Only **Syntax:** Integer32 **OID:** 1.3.6.1.4.1.15004.4.17.2.1.1.16 **Definition:** The threshold of low temperature warning (in units of 0.001 degrees Celsius) of the SFP transceiver.
rcSfpDdmTableGroup	rcSfpDdmThreshTempWarnHigh	**Access:** Read-Only **Syntax:** Integer32 **OID:** 1.3.6.1.4.1.15004.4.17.2.1.1.17 **Definition:** The threshold of high temperature warning (in units of 0.001 degrees Celsius) of the SFP transceiver.
rcSfpDdmTableGroup	rcSfpDdmThreshTempAlarmHigh	**Access:** Read-Only **Syntax:** Integer32 **OID:** 1.3.6.1.4.1.15004.4.17.2.1.1.18 **Definition:** The threshold of high temperature alarm (in units of 0.001 degrees Celsius) of the SFP transceiver.
rcSfpDdmTableGroup	rcSfpDdmCurrentVoltage	**Access:** Read-Only **Syntax:** Integer32 **OID:** 1.3.6.1.4.1.15004.4.17.2.1.1.19 **Definition:** The current voltage (in millivolts) of the SFP transceiver.
rcSfpDdmTableGroup	rcSfpDdmThreshVoltageAlarmLow	**Access:** Read-Only **Syntax:** Integer32 **OID:** 1.3.6.1.4.1.15004.4.17.2.1.1.20 **Definition:** The threshold of low voltage alarm (in millivolts) of the SFP transceiver.
rcSfpDdmTableGroup	rcSfpDdmThreshVoltageWarnLow	**Access:** Read-Only **Syntax:** Integer32 **OID:** 1.3.6.1.4.1.15004.4.17.2.1.1.21 **Definition:** The threshold of low voltage warning (in millivolts) of the SFP transceiver.
rcSfpDdmTableGroup	rcSfpDdmThreshVoltageWarnHigh	**Access:** Read-Only **Syntax:** Integer32 **OID:** 1.3.6.1.4.1.15004.4.17.2.1.1.22

Group(s)	Object	Description
		Definition: The threshold of high voltage warning (in millivolts) of the SFP transceiver.
rcSfpDdmTableGroup	rcSfpDdmThreshVoltageAlarmHigh	**Access:** Read-Only **Syntax:** Integer32 **OID:** 1.3.6.1.4.1.15004.4.17.2.1.1.23 **Definition:** The threshold of high voltage alarm (in millivolts) of the SFP transceiver.
rcSfpDdmTableGroup	rcSfpDdmCurrentTxBiasCurrent	**Access:** Read-Only **Syntax:** Integer32 **OID:** 1.3.6.1.4.1.15004.4.17.2.1.1.24 **Definition:** The current Tx bias current (in microamperes) of the SFP transceiver.
rcSfpDdmTableGroup	rcSfpDdmThreshTxBiasAlarmLow	**Access:** Read-Only **Syntax:** Integer32 **OID:** 1.3.6.1.4.1.15004.4.17.2.1.1.25 **Definition:** The threshold of low Tx bias current alarm (in microamperes) of the SFP transceiver.
rcSfpDdmTableGroup	rcSfpDdmThreshTxBiasWarnLow	**Access:** Read-Only **Syntax:** Integer32 **OID:** 1.3.6.1.4.1.15004.4.17.2.1.1.26 **Definition:** The threshold of low Tx bias current warning (in microamperes) of the SFP transceiver.
rcSfpDdmTableGroup	rcSfpDdmThreshTxBiasWarnHigh	**Access:** Read-Only **Syntax:** Integer32 **OID:** 1.3.6.1.4.1.15004.4.17.2.1.1.27 **Definition:** The threshold of high Tx bias current warning (in microamperes) of the SFP transceiver.
rcSfpDdmTableGroup	rcSfpDdmThreshTxBiasAlarmHigh	**Access:** Read-Only **Syntax:** Integer32 **OID:** 1.3.6.1.4.1.15004.4.17.2.1.1.28 **Definition:** The threshold of high Tx bias current alarm (in microamperes) of the SFP transceiver.
rcSfpDdmTableGroup	rcSfpDdmCurrentRxPower	**Access:** Read-Only **Syntax:** Integer32 **OID:** 1.3.6.1.4.1.15004.4.17.2.1.1.29 **Definition:** The current Rx power (in nanowatts) of the SFP transceiver.
rcSfpDdmTableGroup	rcSfpDdmThreshRxPowerAlarmLow	**Access:** Read-Only **Syntax:** Integer32 **OID:** 1.3.6.1.4.1.15004.4.17.2.1.1.30 **Definition:** The threshold of low Rx power alarm (in nanowatts) of the SFP transceiver.
rcSfpDdmTableGroup	rcSfpDdmThreshRxPowerWarnLow	**Access:** Read-Only

Group(s)	Object	Description
		Syntax: Integer32 **OID:** 1.3.6.1.4.1.15004.4.17.2.1.1.31 **Definition:** The threshold of low Rx power warning (in nanowatts) of the SFP transceiver.
rcSfpDdmTableGroup	rcSfpDdmThreshRxPowerWarnHigh	**Access:** Read-Only **Syntax:** Integer32 **OID:** 1.3.6.1.4.1.15004.4.17.2.1.1.32 **Definition:** The threshold of high Rx power warning (in nanowatts) of the SFP transceiver.
rcSfpDdmTableGroup	rcSfpDdmThreshRxPowerAlarmHigh	**Access:** Read-Only **Syntax:** Integer32 **OID:** 1.3.6.1.4.1.15004.4.17.2.1.1.33 **Definition:** The threshold of high Rx power alarm (in nanowatts) of the SFP transceiver.
rcSfpDdmTableGroup	rcSfpDdmCurrentTxPower	**Access:** Read-Only **Syntax:** Integer32 **OID:** 1.3.6.1.4.1.15004.4.17.2.1.1.34 **Definition:** The current Tx power (in microwatts) of the SFP transceiver.
rcSfpDdmTableGroup	rcSfpDdmThreshTxPowerAlarmLow	**Access:** Read-Only **Syntax:** Integer32 **OID:** 1.3.6.1.4.1.15004.4.17.2.1.1.35 **Definition:** The threshold of low Tx power alarm (in microwatts) of the SFP transceiver.
rcSfpDdmTableGroup	rcSfpDdmThreshTxPowerWarnLow	**Access:** Read-Only **Syntax:** Integer32 **OID:** 1.3.6.1.4.1.15004.4.17.2.1.1.36 **Definition:** The threshold of low Tx power warning (in microwatts) of the SFP transceiver.
rcSfpDdmTableGroup	rcSfpDdmThreshTxPowerWarnHigh	**Access:** Read-Only **Syntax:** Integer32 **OID:** 1.3.6.1.4.1.15004.4.17.2.1.1.37 **Definition:** The threshold of high Tx power warning (in microwatts) of the SFP transceiver.
rcSfpDdmTableGroup	rcSfpDdmThreshTxPowerAlarmHigh	**Access:** Read-Only **Syntax:** Integer32 **OID:** 1.3.6.1.4.1.15004.4.17.2.1.1.38 **Definition:** The threshold of high Tx power alarm (in microwatts) of the SFP transceiver.
rcSfpDdmTableGroup	rcSfpDdmWarningFlags	**Access:** Read-Only **Syntax:** Bits • tempHighWarning(0) • tempLowWarning(1) • vccHighWarning(2)

Group(s)	Object	Description
		• vccLowWarning(3) • txbiasHighWarning(4) • txbiasLowWarning(5) • rxpowerHighWarning(6) • rxpowerLowWarning(7) • txpowerHighWarning(8) • txpowerLowWarning(9) **OID:** 1.3.6.1.4.1.15004.4.17.2.1.1.39 **Definition:** Warning flags indicate if any of the monitored parameters exceeds its warning threshold or not. The change in the value of any of these bits will generate a warning trap.
rcSfpDdmTableGroup	rcSfpDdmAlarmFlags	**Access:** Read-Only **Syntax:** Bits • tempHighAlarm(0) • tempLowAlarm(1) • vccHighAlarm(2) • vccLowAlarm(3) • txbiasHighAlarm(4) • txbiasLowAlarm(5) • rxpowerHighAlarm(6) • rxpowerLowAlarm(7) • txpowerHighAlarm(8) • txpowerLowAlarm(9) **OID:** 1.3.6.1.4.1.15004.4.17.2.1.1.40 **Definition:** Alarm flags indicate if any of the monitored parameters exceeds its alarm threshold or not. The change in the value of any of these bits will generate an alarm trap.

RUGGEDCOM-STP-MIB

Group(s)	Object	Description
rcRstpBaseGroup	rcRstpDot1dRstpAlternatePorts	**Access:** Read-Only **Syntax:** PortList **OID:** 1.3.6.1.4.1.15004.4.5.1.5.0 **Definition:** The subset of ports with an Alternate role.
rcRstpBaseGroup	rcRstpDot1dRstpBackupPorts	**Access:** Read-Only **Syntax:** PortList **OID:** 1.3.6.1.4.1.15004.4.5.1.6.0 **Definition:** The subset of ports with a Backup role.
rcRstpBaseGroup	rcRstpDot1dStpBlockedPorts	**Access:** Read-Only **Syntax:** PortList **OID:** 1.3.6.1.4.1.15004.4.5.1.3.0

Group(s)	Object	Description
		Definition: The subset of ports with a Blocked role.
rcRstpBaseGroup	rcRstpDot1dStpBrokenPorts	**Access:** Read-Only **Syntax:** PortList **OID:** 1.3.6.1.4.1.15004.4.5.1.4.0 **Definition:** The subset of ports in *dot1dStpPortTable* that are in a 'broken' state (the value of the object *dot1dStpPortState* is 'broken').
rcRstpBaseGroup	rcRstpDot1dStpForwardingPorts	**Access:** Read-Only **Syntax:** PortList **OID:** 1.3.6.1.4.1.15004.4.5.1.2.0 **Definition:** The subset of ports in *dot1dStpPortTable* that are in a 'forwarding' state (the value of the object *dot1dStpPortState* is 'forwarding').
rcRstpBaseStpTxHoldCountGroup	rcRstpDot1dStpTxHoldCount	**Access:** Read-Write **Syntax:** Integer32 **OID:** 1.3.6.1.4.1.15004.4.5.1.1.0 **Definition:** The value used by the Port Transmit state machine to limit the maximum transmission rate. Larger values allow the network to recover from failed links/ bridges more quickly. A value of '0' means unlimited transmission rate. If the value of *dot1dStpTxHoldCount* object is 3..10, this object must match the value of the object *dot1dStpTxHoldCount* (RSTP-MIB). If the value the object *dot1dStpTxHoldCount* is 10, the value of this object represents real configured transmission rate limit.

RUGGEDCOM-SYS-INFO-MIB

Group(s)	Object	Description
rcSysDeviceCommGroup	rcDeviceCommClearAlarms	**Access:** Read-Write **Syntax:** TruthValue **OID:** 1.3.6.1.4.1.15004.4.2.4.3.0 **Definition:** Setting the value of this object to 'true(1)' will cause the device to clear all alarms. Following a read request the agent will return value 'false(2)'.
rcSysDeviceCommGroup	rcDeviceCommClearLogs	**Access:** Read-Write **Syntax:** TruthValue **OID:** 1.3.6.1.4.1.15004.4.2.4.5.0 **Definition:** Setting the value of this object to 'true(1)' will cause the device to clear syslog.txt and crashlog.txt files. Following a read request the agent will return value 'false(2)'.

Group(s)	Object	Description
rcSysDeviceCommGroup	rcDeviceCommClearSyslog	**Access:** Read-Write **Syntax:** TruthValue **OID:** 1.3.6.1.4.1.15004.4.2.4.4.0 **Definition:** Setting the value of this object to 'true(1)' will cause the device to clear the syslog.txt file. Following a read request the agent will return value 'false(2)'.
rcSysDeviceCommGroup	rcDeviceCommLoadDefaultCfg	**Access:** Read-Write **Syntax:** TruthValue **OID:** 1.3.6.1.4.1.15004.4.2.4.2.0 **Definition:** Setting the value of this object to 'true(1)' will force the device to load the default configuration to all tables. Following a read request the agent will return value 'false(2)'.
rcSysDeviceCommGroup	rcDeviceCommReset	**Access:** Read-Write **Syntax:** TruthValue **OID:** 1.3.6.1.4.1.15004.4.2.4.1.0 **Definition:** Setting the value of this object to 'true(1)' will cause the device to reboot. Following a read request the agent will return value 'false(2)'.
rcSysErrObjectsGroup	rcDeviceErrBootPTftpTrFailed	**Access:** Read-Only **Syntax:** TruthValue **OID:** 1.3.6.1.4.1.15004.4.2.1.9.0 **Definition:** Indicates whether the file was transferred properly after obtaining an IP address from the BootP server. Whenever the value of this object changes from false(2) to true(1), the device will generate a genericTrap notification.
rcSysErrObjectsGroup	rcDeviceErrBootupError	**Access:** Read-Only **Syntax:** DisplayString **OID:** 1.3.6.1.4.1.15004.4.2.1.1.0 **Definition:** The error discovered during the bootup process. If there was no error during device bootup, zero length DisplayString will be retrieved.
rcSysErrObjectsGroup	rcDeviceErrConfigurationFailure	**Access:** Read-Only **Syntax:** TruthValue **OID:** 1.3.6.1.4.1.15004.4.2.1.3.0 **Definition:** Indicates whether errors were detected while applying configuration settings from the configuration file. The configuration is updated from the configuration file at bootup time when a file is loaded from non-volatile memory, or when a new file is downloaded to the device. Whenever the value of this object changes from false(2) to true(1), the device will generate a genericTrap notification.

Group(s)	Object	Description
rcSysErrObjectsGroup	rcDeviceErrCrashLogCreated	**Access:** Read-Only **Syntax:** TruthValue **OID:** 1.3.6.1.4.1.15004.4.2.1.4.0 **Definition:** Indicates whether the device error that caused creation of an entry in crashlog.txt file was detected. Whenever the value of this object changes from false(2) to true(1), the device will generate a genericTrap notification.
rcSysErrObjectsGroup	rcDeviceErrDateAndTimeSetFailed	**Access:** Read-Only **Syntax:** TruthValue **OID:** 1.3.6.1.4.1.15004.4.2.1.7.0 **Definition:** Indicates whether the date and time setting in the device failed. Whenever the value of this object changes from false(2) to true(1), the device will generate a genericTrap notification.
rcSysErrObjectsGroup	rcDeviceErrHeapError	**Access:** Read-Only **Syntax:** TruthValue **OID:** 1.3.6.1.4.1.15004.4.2.1.6.0 **Definition:** Indicates whether the system memory corruption was detected. Whenever the value of this object changes from false(2) to true(1), the device will generate a genericTrap notification.
rcSysErrObjectsGroup	rcDeviceErrNtpServerUnreachable	**Access:** Read-Only **Syntax:** TruthValue **OID:** 1.3.6.1.4.1.15004.4.2.1.8.0 **Definition:** Indicates whether any of the NTP servers (if required) can be reached. The value of this object is 'false' if both servers become unreachable. Whenever the value of this object changes, the device will generate the *ntpServiceAvailableChange* notification.
rcSysErrObjectsGroup	rcDeviceErrRadiusServerUnreachable	**Access:** Read-Only **Syntax:** TruthValue **OID:** 1.3.6.1.4.1.15004.4.2.1.10.0 **Definition:** Indicates whether the RADIUS server (if required) can be reached. Whenever the value of this object changes, the device will generate the *radiusServiceAvailableChange* notification.
rcSysErrObjectsGroup	rcDeviceErrStackOverflow	**Access:** Read-Only **Syntax:** TruthValue **OID:** 1.3.6.1.4.1.15004.4.2.1.5.0 **Definition:** Indicates whether the stack of any of the system tasks is used over the system threshold. Whenever the value of this object changes from false(2) to true(1), the device will generate a *genericTrap* notification.

Group(s)	Object	Description
rcSysErrObjectsGroup	rcDeviceErrTacacsServerUnreachable	**Access:** Read-Only **Syntax:** TruthValue **OID:** 1.3.6.1.4.1.15004.4.2.1.11.0 **Definition:** Indicates whether the TACACS+ server (if required) can be reached. Whenever the value of this object changes, the device will generate the *tacacsServiceAvailableChange* notification.
rcSysErrObjectsGroup	rcDeviceErrWatchdogReset	**Access:** Read-Only **Syntax:** TruthValue **OID:** 1.3.6.1.4.1.15004.4.2.1.2.0 **Definition:** Indicates whether the last device reboot was caused by watchdog.
rcSysInfoDeviceInfoGroup	rcDeviceInfoBootSwVersion	**Access:** Read-Only **Syntax:** DisplayString **OID:** 1.3.6.1.4.1.15004.4.2.3.2.0 **Definition:** The version and the build date of the boot loader software.
rcSysInfoDeviceInfoGroup	rcDeviceInfoCfgRevision	**Access:** Read-Only **Syntax:** Integer32 **OID:** 1.3.6.1.4.1.15004.4.2.3.8.0 **Definition:** The configuration file revision. The revision number will be updated whenever a file is saved to the flash memory. This number is recorded in config.csv at the time file is uploaded from the device. Whenever the value of this object changes the device will generate a *cfgChangeTrap* notification.
rcSysInfoDeviceInfoGroup	rcDeviceInfoMainBoardType	**Access:** Read-Only **Syntax:** RcMainBoard **OID:** 1.3.6.1.4.1.15004.4.2.3.4.0 **Definition:** The identification code of the device main board.
rcSysInfoDeviceInfoGroup	rcDeviceInfoMainSwVersion	**Access:** Read-Only **Syntax:** DisplayString **OID:** 1.3.6.1.4.1.15004.4.2.3.3.0 **Definition:** The version and build date of the main operating system software.
rcSysInfoDeviceInfoGroup	rcDeviceInfoPendingBootSwVersion	**Access:** Read-Only **Syntax:** DisplayString **OID:** 1.3.6.1.4.1.15004.4.2.3.6.0 **Definition:** The version and build date of the boot loader software that has been loaded to the device and is pending reboot. Whenever the value of this object changes from zero-length DisplayString to any DisplayString of non-zero

Group(s)	Object	Description
		length, the device will generate *swUpgradeTrap* notification.
rcSysInfoDeviceInfoGroup	rcDeviceInfoPendingMainSwVersion	**Access:** Read-Only **Syntax:** DisplayString **OID:** 1.3.6.1.4.1.15004.4.2.3.7.0 **Definition:** The version and the build date of the main operating system software that has been loaded to the device and is pending reboot. Whenever the value of this object changes from zero-length DisplayString to any DisplayString of non-zero length, the device will generate *swUpgradeTrap* notification.
rcSysInfoDeviceInfoGroup	rcDeviceInfoSerialNumber	**Access:** Read-Only **Syntax:** DisplayString **OID:** 1.3.6.1.4.1.15004.4.2.3.1.0 **Definition:** The manufacturing serial number of the device.
rcSysInfoDeviceInfoGroup	rcDeviceInfoTotalRam	**Access:** Read-Only **Syntax:** Integer32 **OID:** 1.3.6.1.4.1.15004.4.2.3.5.0 **Definition:** The total number of bytes of RAM in the system control CPU.
rcSysStsObjectsGroup1	rcDeviceStsCpuUsage	**Access:** Read-Only **Syntax:** Integer32 **OID:** 1.3.6.1.4.1.15004.4.2.2.1 **Definition:** The percentage in tenths of percent of available CPU cycles used for device operation as measured over the last second when object was retrieved.
rcSysStsObjectsGroup1	rcDeviceStsAvailableRam	**Access:** Read-Only **Syntax:** Integer32 **OID:** 1.3.6.1.4.1.15004.4.2.2.2 **Definition:** The total number of bytes of RAM still available in the system control CPU.
rcSysStsPowerSupplyGroup	rcDeviceStsPowerSupply1	**Access:** Read-Only **Syntax:** RcHardwareStatus **OID:** 1.3.6.1.4.1.15004.4.2.2.4.0 **Definition:** Indicates the status of Power Supply Module 1. Whenever the value of this object changes from functional(2) to notFunctional(3), or from notFunctionl(3) to functional(2), the device will generate a *powerSupplyTrap* notification.
rcSysStsPowerSupplyGroup	rcDeviceStsPowerSupply2	**Access:** Read-Only **Syntax:** RcHardwareStatus **OID:** 1.3.6.1.4.1.15004.4.2.2.5.0

Group(s)	Object	Description
		Definition: Indicates the status of Power Supply Module 2. Whenever the value of this object changes from functional(2) to notFunctional(3), or from notFunctionl(3) to functional(2), the device will generate a *powerSupplyTrap* notification.
rcSysStsObjectsTemperatureGroup	rcDeviceStsTemperature	**Access:** Read-Only **Syntax:** Integer32 **OID:** 1.3.6.1.4.1.15004.4.2.2.3.0 **Definition:** The temperature measured in the device.

RUGGEDCOM-TIMECONFIG-MIB

Group(s)	Object	Description
rcTimeConfigBaseGroup	rcCurrentUTCOfst	**Access:** Read-Write **Syntax:** Unsigned32 **OID:** 1.3.6.1.4.1.15004.4.11.1.4.0 **Definition:** Allows the user to adjust the difference between UTC and TAI.
rcTimeConfigBaseGroup	rcDSTOfst	**Access:** Read-Write **Syntax:** Unsigned32 **OID:** 1.3.6.1.4.1.15004.4.11.1.3.0 **Definition:** This parameter specifies the amount of time to be shifted forward/backward when DST begins and ends. For example, for most of the USA and Canada, DST time shift is 1 hour (01:00:00) forward when DST begins and 1 hour backward when DST ends.
rcTimeConfigBaseGroup	rcDSTRule	**Access:** Read-Write **Syntax:** DisplayString **OID:** 1.3.6.1.4.1.15004.4.11.1.6.0 **Definition:** This parameter specifies a rule for time and date when the transition between Standard and Daylight Saving Time occurs. Format: mm.n.d/HH:MM:SS mm.n.d/HH:MM:SS • 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 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.

Group(s)	Object	Description
rcTimeConfigBaseGroup	rcLeapSecPending	**Access:** Read-Write **Syntax:** TruthValue **OID:** 1.3.6.1.4.1.15004.4.11.1.5.0 **Definition:** This parameter allows users to manage the leap second event. A leap second is a second added to Coordinated.
rcTimeConfigBaseGroup	rcTimeSource	**Access:** Read-Write **Syntax:** Integer **OID:** 1.3.6.1.4.1.15004.4.11.1.1.0 **Definition:** A time source that is driving the local clock.
rcSerialTinAndWinGroup	rcTinAndWinAddrAgingTime	**Access:** Read-Write **Syntax:** Integer32 **OID:** 1.3.6.1.4.1.15004.4.6.6.7.0 **Definition:** The time of communication inactivity in milliseconds after which a learned TIN address is removed from the dynamic device address table. Entries in Link Statistics table with the aged address will be kept until statistics are cleared.
rcSerialTinAndWinGroup	rcTinAndWinBroadCastAddr	**Access:** Read-Write **Syntax:** Integer **OID:** 1.3.6.1.4.1.15004.4.6.6.8.0 **Definition:** The device address table in which addresses will be found for broadcast messages.
rcSerialTinAndWinGroup	rcTinAndWinLinkStats	**Access:** Read-Write **Syntax:** EnabledStatus **OID:** 1.3.6.1.4.1.15004.4.6.6.10.0 **Definition:** Enables links statistics collection for TIN and WIN protocols.
rcSerialTinAndWinGroup	rcTinAndWinMsgAgingTime	**Access:** Read-Write **Syntax:** Integer32 **OID:** 1.3.6.1.4.1.15004.4.6.6.6.0 **Definition:** Aging time for TIN mode2 messages. The feature is disabled if the value of this object is '0'. When the feature is enabled, any TIN mode2 message received will be stored in an internal table. If the same message is received within the time window specified by this parameter, the new message is considered duplicate, and thus discarded.
rcSerialTinAndWinGroup	rcTinAndWinTinDscp	**Access:** Read-Write **Syntax:** Integer32 **OID:** 1.3.6.1.4.1.15004.4.6.6.12.0 **Definition:** The value of DS byte to be set in the IP header. The DS byte setting is supported in the egress direction only.
rcSerialTinAndWinGroup	rcTinAndWinTinIpPort	**Access:** Read-Write **Syntax:** Integer32 **OID:** 1.3.6.1.4.1.15004.4.6.6.4.0

Group(s)	Object	Description
		Definition: A local port number on which the TIN protocol listens to connections or UDP datagrams.
rcSerialTinAndWinGroup	rcTinAndWinTinMode	**Access:** Read-Write **Syntax:** Integer **OID:** 1.3.6.1.4.1.15004.4.6.6.1.0 **Definition:** The TIN protocol running mode.
rcSerialTinAndWinGroup	rcTinAndWinTinTrans	**Access:** Read-Write **Syntax:** RcTransport **OID:** 1.3.6.1.4.1.15004.4.6.6.2.0 **Definition:** A transport protocol used for IP traffic for TIN protocol.
rcSerialTinAndWinGroup	rcTinAndWinUniAddr	**Access:** Read-Write **Syntax:** Integer **OID:** 1.3.6.1.4.1.15004.4.6.6.9.0 **Definition:** The device address table in which addresses will be found for unicast messages.
rcSerialTinAndWinGroup	rcTinAndWinWinDscp	**Access:** Read-Write **Syntax:** Integer32 **OID:** 1.3.6.1.4.1.15004.4.6.6.11.0 **Definition:** The value of DS byte to be set in the IP header. The DS byte setting is supported in the egress direction only.
rcSerialTinAndWinGroup	rcTinAndWinWinIpPort	**Access:** Read-Write **Syntax:** Integer32 **OID:** 1.3.6.1.4.1.15004.4.6.6.5.0 **Definition:** A local port number on which the WIN protocol listens to connections or UDP datagrams.
rcSerialTinAndWinGroup	rcTinAndWinWinTrans	**Access:** Read-Write **Syntax:** RcTransport **OID:** 1.3.6.1.4.1.15004.4.6.6.3.0 **Definition:** A transport protocol used for IP traffic for the WIN protocol.

14.1.3 Supported agent capabilities

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

⚠ NOTICE

This section lists all MIBs supported by RUGGEDCOM ROS, and is intended for reference purposes only. Individual device support may vary.

Note

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

File Name	Agent capability	Supported MIB
RC-SNMPv2-MIB-AC.mib	RC-SNMPv2-MIB-AC	SNMPv2-MIB
RC-UDP-MIB-AC.mib	RC-UDP-MIB-AC	UDP-MIB
RC-TCP-MIB-AC.mib	RC-TCP-MIB-AC	TCP-MIB
RC-SNMP-USER-BASED-SM-MIB-AC.mib	RC-SNMP-USER-BASED-SM-MIB-AC	SNMP-USER-BASED-SM-MIB-AC
RC-SNMP-VIEW-BASED-ACM-MIB-AC.mib	RC-SNMP-VIEW-BASED-ACM-MIB-AC	SNMP-VIEW-BASED-ACM-MIB-AC
RC-IF-MIB-AC.mib	RC-IF-MIB-AC	IF-MIB
RC-BRIDGE-MIB-AC.mib	RC-BRIDGE-MIB-AC	BRIDGE-MIB
RC-RMON-MIB-AC.mib	RC-RMON-MIB-AC	RMON-MIB
RC-Q-BRIDGE-MIB-AC.mib	RC-Q-BRIDGE-MIB-AC	Q-BRIDGE-MIB
RC-IP-MIB-AC.mib	RC-IP-MIB-AC	IP-MIB
RC-LLDP-MIB-AC.mib	RC-LLDP-MIB-AC	LLDP-MIB
RC-LAG-MIB-AC.mib	RC-LAG-MIB-AC	IEEE8023-LAG-MIB
RC_RSTP-MIB-AC.mib	RC_RSTP-MIB-AC	RSTP-MIB
RC-RUGGEDCOM-DOT11-MIB-AC.mib	RC-RUGGEDCOM-DOT11-MIB-AC	RUGGEDCOM-DOT11- MIB
RC-RUGGEDCOM-POE-MIB-AC.mib	RC-RUGGEDCOM-POE-MIB-AC	RUGGEDCOM-POE-MIB
RC-RUGGEDCOM-STP-AC-MIB.mib	RC-RUGGEDCOM-STP-AC-MIB	RUGGEDCOM-STP-MIB
RC-RUGGEDCOM-SYS-INFO-MIB-AC.mib	RC-RUGGEDCOM-SYS-INFO-MIB-AC	RUGGEDCOM-SYS-INFO-MIB
RC-RUGGEDCOM-TRAPS-MIB-AC.mib	RC-RUGGEDCOM-TRAPS-MIB-AC	RUGGEDCOM-TRAPS-MIB
RUGGEDCOM_RS-232-MIB-AC.mib	RUGGEDCOM_RS-232-MIB-AC	RS-232-MIB
RC-RUGGEDCOM-SERIAL-MIB-AC.mib	RC-RUGGEDCOM-SERIAL-MIB-AC	RUGGEDCOM-SERIAL-MIB
RC-GPS-MIB-AC.mib	RC-GPS-MIB-AC	GPS-MIB
RC-IRIGB-MIB-AC.mib	RC-IRIGB-MIB-AC	IRIGB-MIB
RC-NTP-MIB-AC.mib	RC-NTP-MIB-AC	NTP-MIB
RC-PTP1588-MIB-AC.mib	RC-PTP1588-MIB-AC	PTP1588-MIB
RC-TIMECONFIG-MIB-AC.mib	RC-TIMECONFIG-MIB-AC	TIMECONFIG-MIB
RC-SNMP-FRAMEWORK-MIB-AC.MIB	RC-SNMP-FRAMEWORK-MIB-AC	SNMP-FRAMEWORK-MIB.MIB
RC-RUGGEDCOM-AAA-SERVER-MIB-AC.MIB	RC-RUGGEDCOM-AAA-SERVER-MIB-AC	RUGGEDCOM-AAA-SERVER-MIB.MIB
RC-RUGGEDCOM-SFP-DDM-MIB-AC.mib	RC-RUGGEDCOM-SFP-DDM-MIB-AC	RUGGEDCOM-SFP-DDM-MIB

14.1.4 SNMP trap bindings

SNMP trap bindings are key-value pairs within an SNMP trap that contain specific, contextual information about the event that triggered the trap. They help network administrators understand the details of an alert, providing information beyond the basic trap type.

⚠ NOTICE

This section lists all trap bindings supported by RUGGEDCOM ROS, and is intended for reference purposes only. Individual device support may vary.

The device supports the following trap bindings:

Binding	Description
alarmFallingThreshold	A threshold for the sampled statistic. A trap will be triggered when the current sampled value is less than or equal to this threshold, and the value at the last sampling interval was greater than this threshold.
alarmRisingThreshold	A threshold for the sampled statistic. A trap will be triggered when the current sampled value is greater than or equal to this threshold, and the value at the last sampling interval was less than this threshold.
alarmIndex	The unique index of the alarm entry that triggered the trap
alarmSampleType	Indicates whether the alarm is based on an absolute or delta value
alarmValue	The actual value of the monitored variable at the time the trap was triggered
alarmVariable	The OID of the variable being monitored (e.g. ifInOctets, ifInErrors, etc.)
C37238CurrentDSOfstFrMaster	The current master clock offset
C37238DefaultDSOfstFrMlimit	The default offset limit for the master clock
C37238ParentDSCLkIdentity	The new time source Clock ID based on the clock type
dot1dStpDesignatedRoot	The ID of the STP root bridge
dot1dStpRootPort	The port number of the STP bridge's root port
genericTrapDescription	The trap description
genericTrapSeverity	The severity level of the trap
ifAdminStatus	The current administrative state of an interface (up or down)
ifIndex	The interface number
ifName	The human-readable name of a network interface
ifOperStatus	The current administrative state of an interface (up, down, or testing)
lldpStatsRemTablesAgeouts	The number of times the complete set of information has been deleted from tables because the information timeliness interval has expired
lldpStatsRemTablesDeletes	The number of times the complete set of information has been deleted from tables
lldpStatsRemTablesDrops	The number of times the complete set of information could not be entered into tables due to insufficient resources
lldpStatsRemTablesInserts	The number of times the complete set of information has been inserted into tables
loginAccessLevel	The type of access the user has (admin, guest etc.)
loginMgmtApp	The management interface used for login/authentication on the device
loginUser	The user name used for authentication (e.g. admin, operator, guest)

Binding	Description
loginRemoteIP	The IP address from where the login attempt was made
powerSupplyDescription	The state of the power supply (failed or restored)
rcDeviceErrNtpServerUnreachable	NTP server unreachable error detected on device
rcDeviceErrRadiusServerUnreachable	RADIUS server unreachable error detected on device
rcDeviceErrSystem	The status or description of system errors detected by the device
rcDeviceErrTacacsServerUnreachable	TACACS+ server unreachable error detected on device
rcDeviceInfoBootSwVersion	The current boot SW version
rcDeviceInfoCfgRevision	The configuration revision number, i.e. the number of times the device configuration changed on the device
rcDeviceInfoMainSwVersion	The current main SW version
rcDeviceInfoPendingBootSwVersion	The new downloaded boot SW version
rcDeviceInfoPendingMainSwVersion	The new downloaded main SW version
rcDeviceStsKeysDflt	Default keys are in use for SSL or SSH
rcDeviceStsPwdsWeak	Username(s) with weak password configured
rcDiAlarmStatus	The current Digital Input alarm status
rcDiDescription	Description of a Digital Input alarm
rcFileTransferDirection	The file transfer direction (send/receive)
rcFileTransferStatusMsg	File transfer success or failure message
rcFileTransferTimeDate	The time and date the file transfer event occurred
rcGpsStatus	The status of GPS
rcNTPBackupServerReachable	The NTP backup server reachability status
rcNTPPriServerReachable,	The NTP primary server reachability status
rcRadiusServerReachable	The RADIUS server reachability status (primary and backup)
rcSfpDdmAlarmFlags	The bit mask of flag bits of all five parameters in such order from bit 31 - highest bit to bit 22: TempHigh, TempLow, VoltageHigh, VoltageLow, TxBiasCurrentHigh, TxBiasCurrenLow, RxPowerHigh, RxPowerLow, TxPowerHigh, TxPowerLow
rcSfpDdmWarningFlags	The bit mask of flag bits of all five parameters in such order from bit 31 - highest bit to bit 22: TempHigh, TempLow, VoltageHigh, VoltageLow, TxBiasCurrentHigh, TxBiasCurrenLow, RxPowerHigh, RxPowerLow, TxPowerHigh, TxPowerLow
rcSfpDdmTemp	The current SFP transceiver temperature in degrees Celsius
rcSfpDdmRxPower	The current SFP transceiver Rx input power in microwatts
rcSfpDdmTxBias	The current SFP transceiver Tx Bias in uA
rcSfpDdmTxPower	The current SFP transceiver Tx output power in milliwatts
rcSfpDdmVolt	The current SFP transceiver supply voltage in volts
rcSfpPortId	The port number of the connected SFP
rcTacacsServerReachable	The TACACS+ server reachability status (primary and backup)
rcTransferLoginLevel	The login level (admin, guest or operator)
rcTransferLoginName	The login username
rcTransferMgmtApp	The management application type that performed the file transfer operation

Binding	Description
rcTransferredBytes	The number of bytes sent or received for file transfer
rcTransferredFileName	The transferred file name
rcRstpDot1dRstpAlternatePorts	List of ports in RSTP Alternate port role
rcRstpDot1dRstpBackupPorts	List of ports in RSTP Backup role
rcRstpDot1dStpBlockedPorts	List of ports in STP Blocked state
rcRstpDot1dStpBrokenPorts	List of ports in STP Broken state
rcRstpDot1dStpForwardingPorts	List of ports currently in STP Forwarding state

14.1.5 SNMP traps

⚠ NOTICE

This section lists all traps supported by RUGGEDCOM ROS, and is intended for reference purposes only. Individual device support may vary.

The device generates the following traps:

Standard traps

Variable	Description
coldStart	**Object Group:** snmpBasicNotificationsGroup **MIB:** SNMPv2-MIB **Access:** read-only **OID:** 1.3.6.1.6.3.1.1.5.1.0 **Standard:** RFC-1907 **Definition:** A coldStart trap signifies that the SNMPv2 entity, acting in an agent role, is reinitializing itself and that its configuration may have been altered **Binding(s):** None
fallingAlarm	**Object Group:** rmonNotificationGroup **MIB:** RMON-MIB **Access:** read-only **Syntax:** String **OID:** 1.3.6.1.2.1.16.0.2.0 **Definition:** The current sampled value of the monitored variable is less than or equal to the falling threshold and the value at the last sampling interval was greater than the falling threshold **Binding(s):** • alarmIndex • alarmVariable • alarmSampleType • alarmValue • alarmRisingThreshold

Variable	Description
IeeeC37238EventChangeOfMaster	**Object Group:** ieeeC37238EventsPropertiesGroup **MIB:** IEEEC37-238-MIB **Access:** read-only **OID:** 1.3.111.3.37.238.9999.0.0.1.0 **Standard:** PC37.238/D5.5 **Definition:** Indicates that new grandmaster has been selected **Binding(s):** C37238ParentDSCLkIdentity
IeeeC37238EventMasterStepChange	**Object Group:** ieeeC37238EventsPropertiesGroup **MIB:** IEEEC37-238-MIB **Access:** read-only **OID:** 1.3.111.3.37.238.9999.0.0.2.0 **Standard:** Indicates that a step change occurred in current grandmaster time **Definition:** PC37.238/D5.5 **Binding(s):** C37238ParentDSCLkIdentity
IeeeC37238EventOfstExceedsLimit	**Object Group:** ieeeC37238EventsPropertiesGroup **MIB:** IEEEC37-238-MIB **Access:** read-only **OID:** 1.3.111.3.37.238.9999.0.0.5.0 **Standard:** PC37.238/D5.5 **Definition:** Indicates that for a clock in a slave state Offset from Master exceeds configurable limit **Binding(s):** • C37238CurrentDSOfstFrMaster • C37238DefaultDSOfstFrMlimit
IeeeC37238EventPTPServiceStarted	**Object Group:** ieeeC37238EventsPropertiesGroup **MIB:** IEEEC37-238-MIB **Access:** read-only **OID:** 1.3.111.3.37.238.9999.0.0.8.0 **Standard:** PC37.238/D5.5 **Definition:** Indicates that PTP service has started **Binding(s):** None
IeeeC37238EventPTPServiceStopped	**Object Group:** ieeeC37238EventsPropertiesGroup **MIB:** IEEEC37-238-MIB **Access:** read-only **OID:** 1.3.111.3.37.238.9999.0.0.9.0 **Standard:** PC37.238/D5.5 **Definition:** Indicates that PTP service has stopped **Binding(s):** None
LinkDown	**Object Group:** linkUpDownNotificationsGroup **MIB:** IF-MIB **Access:** read-only

Variable	Description
	Syntax: Counter32 **OID:** .1.3.6.1.6.3.1.1.5.3 **Standard:** RFC-2863 **Definition:** A linkDown trap signifies that the SNMP entity, acting in an agent role, has detected that the ifOperStatus object for one of its communication links is about to enter the down state from some other state (but not from the notPresent state). This other state is indicated by the included value of ifOperStatus. **Binding(s):** • ifIndex • ifAdminStatus • ifOperStatus • ifName
LinkUp	**Object Group:** linkUpDownNotificationsGroup **MIB:** IF-MIB **Agent Capability:** RC-IF-MIB-AC **Access:** read-only **OID:** .1.3.6.1.6.3.1.1.5.4 **Definition:** A linkUp trap signifies that the SNMP entity, acting in an agent role, has detected that the ifOperStatus object for one of its communication links left the down state and transitioned into some other state (but not into the notPresent state). This other state is indicated by the included value of ifOperStatus. **Binding(s):** • ifIndex • ifAdminStatus • ifOperStatus • ifName
LldpRemTablesChange	**Object Group:** lldpNotificationsGroup **MIB:** LLDP-MIB **Agent Capability:** RC-LLDP-MIB-AC **Access:** read-only **Syntax:** STRING **OID:** 1.0.8802.1.1.2.0.0.1.0 **Standard:** ISO8802-LLDP-MIB **Definition:** A lldpRemTablesChange notification is sent when the value of lldpStatsRemTableLastChangeTime changes. It can be utilized by an NMS to trigger LLDP remote systems table maintenance polls. Note that transmission of lldpRemTablesChange notifications are throttled by the agent, as specified by the lldpNotificationInterval object. **Binding(s):** • lldpStatsRemTablesInsert • lldpStatsRemTablesDeletes • lldpStatsRemTablesDrops

Variable	Description
	• lldpStatsRemTablesAgeouts
risingAlarm	**Object Group:** rmonNotificationGroup **MIB:** RMON-MIB **Access:** read-only **Syntax:** String **OID:** 1.3.6.1.2.1.16.0.1.0 **Definition:** The current sampled value of the monitored variable is greater than or equal to the rising threshold and the value at the last sampling interval was less than the rising threshold **Binding(s):** • alarmIndex • alarmVariable • alarmSampleType • alarmValue • alarmRisingThreshold
RstpNewRoot	**Object Group:** dot1dNotificationGroup **MIB:** BRIDGE-MIB **Access:** read-only **Syntax:** NOTIFICATION-TYPE **OID:** 1.3.6.1.2.1.17.0.1.0 **Definition:** Indicates that the sending agent has become the new root of the Spanning Tree. The trap is sent by a bridge soon after its election as the new root, i.e. upon expiration of the Topology Change Timer immediately subsequent to its election. **Binding(s):** None
SnmpAuthenticationFailure	**Object Group:** ruggedcomSnmpTrapGroup **MIB:** SNMPv2-MIB **Access:** read-only **Syntax:** String **OID:** 1.3.6.1.6.3.1.1.5.5.0 **Definition:** SNMP authentication failed due to incorrect authentication key **Binding(s):** None
SnmpEnableAuthenTraps	**Object Group:** snmpGroup **MIB:** SNMPv2-MIB **Access:** read-write **Syntax:** INTEGER **OID:** 1.3.6.1.2.1.11.30.0 **Definition:** Indicates whether the SNMP entity is permitted to generate authenticationFailure traps. The value of this object overrides any configuration information; as such, it provides a means whereby all authenticationFailure traps may be disabled. Note that it is strongly recommended that this object be stored

Variable	Description
	in non-volatile memory so that it remains constant across re-initializations of the network management system. **Binding(s):**
WarmStart	**Object Group:** ROS-Standard-Trap **MIB:** SNMPv2-MIB **Access:** read-only **Syntax:** 1.3.6.1.6.3.1.1.5.2.0 **OID:** 1.3.6.1.6.3.1.1.5.2.0 **Definition:** A warmStart trap signifies that the SNMPv2 entity, acting in an agent role, is reinitializing itself such that its configuration is unaltered **Binding(s):** None

Specific proprietary traps

Variable	Description
BootVersionMismatchTrap	**Object Group:** ruggedcomSecurityGroup01 **MIB:** RUGGEDCOM-TRAPS-MIB **OID:** 1.3.6.1.4.1.15004.5.14 **Definition:** The current boot software version and ROS firmware version installed on device are not compatible **Binding(s):** • rcDeviceInfoBootSwVersion • rcDeviceInfoMainSwVersion
Bouncing link (genericTrap)	**Object Group:** ruggedcomNotificationsGroup **MIB:** RUGGEDCOM-TRAPS-MIB **OID:** 1.3.6.1.4.1.15004.5.1 **Definition:** A generic trap generated when a bouncing link is detected on a port **Binding(s):** • genericTrapSeverity • genericTrapDescription
cfgChangeNoRevTrap	**Object Group:** ruggedcomNoRevCfgNotifGroup **MIB:** RUGGEDCOM-TRAPS-MIB **OID:** 1.3.6.1.4.1.15004.5.5 **Definition:** A generic trap generated upon configuration change by a device that does not support revision numbers **Binding(s):** None
CfgChangeTrap	**Object Group:** ruggedcomNotificationsGroup **MIB:** RUGGEDCOM-TRAPS-MIB **OID:** 1.3.6.1.4.1.15004.5.4 **Definition:** A generic trap generated upon configuration change **Binding(s):** rcDeviceInfoCfgRevision

Variable	Description
DefaultKeysTrap	**Object Group:** ruggedcomSecurityGroup01 **MIB:** RUGGEDCOM-TRAPS-MIB **OID:** 1.3.6.1.4.1.15004.5.13 **Definition:** A use of default keys for secure services (SSH and SSL/TLS) indication trap generated by RUGGEDCOM devices **Binding(s):** rcDeviceStsKeysDflt
deviceErrorTrap	**Object Group:** rcDeviceErrorNotificationGroup **MIB:** RUGGEDCOM-TRAPS-MIB **OID:** 1.3.6.1.4.1.15004.5.24 **Definition:** Triggered when device errors occur: Crashlog error, Watchdog reset error, Bootup error, Config failure error, Stack overflow error, Heap error, Real time clock error, Rx Buffer Low error, Clock manager out of resource error, Clock manager primary source failed error, FPGA cmpatibility error **Binding(s):** rcDeviceErrSystem
digitalInputTrap	**Object Group:** ruggedcomDigitalInputTrapGroup **MIB:** RUGGEDCOM-TRAPS-MIB **OID:** 1.3.6.1.4.1.15004.5.18 **Definition:** Digital Input is in active state **Binding(s):** • rcDiDescription • rcDiAlarmStatus
excessLoginFailureTrap	**Object Group:** ruggedcomDeviceLoginTrapGroup **MIB:** RUGGEDCOM-TRAPS-MIB **OID:** 1.3.6.1.4.1.15004.5.28 **Definition:** A trap indicating excessive failed login attempts to the device **Binding(s):** • loginUser • loginMgmtApp
Fast link detection disabled (genericTrap)	**Object Group:** ruggedcomNotificationsGroup **MIB:** RUGGEDCOM-TRAPS-MIB **OID:** 1.3.6.1.4.1.15004.5.1 **Definition:** Fast link detection is disabled due to excessive link bouncing observed on a network port **Binding(s):** • genericTrapSeverity • genericTrapDescription
fileTransferEventTrap	**Object Group:** ruggedcomNotificationsGroup **MIB:** RUGGEDCOM-TRAPS-MIB **OID:** 1.3.6.1.4.1.15004.5.49 **Definition:** Occurs when a file transfer event takes place in the device **Binding(s):**

Variable	Description
	• rcFileTransferTimeDate • rcFileTransferDirection • rcFileTransferStatusMsg • rcTransferredFileName • rcTransferredBytes • rcTransferLoginLevel • rcTransferLoginName • rcTransferMgmtApp
GenericTrap	**Object Group:** ruggedcomNotificationsGroup **MIB:** RUGGEDCOM-TRAPS-MIB **OID:** 1.3.6.1.4.1.15004.5.1 **Definition:** A generic trap generated by RUGGEDCOM devices **Binding(s):** • genericTrapSeverity • genericTrapDescription
Inconsistent speed is detected on port <port_number> (genericTrap)	**Object Group:** ruggedcomNotificationsGroup **MIB:** RUGGEDCOM-TRAPS-MIB **OID:** 1.3.6.1.4.1.15004.5.1 **Definition:** Inconsistent speed detected on bundle ports, such as RNA ports **Binding(s):** genericTrapDescription
LocalSerialConsoleDisabled	**Object Group:** ruggedcomLocalConsoleTrapGroup **MIB:** RUGGEDCOM-TRAPS-MIB **OID:** 1.3.6.1.4.1.15004.5.40 **Definition:** The Local console is disabled **Binding(s):** None
LocalSerialConsoleEnabled	**Object Group:** ruggedcomLocalConsoleTrapGroup **MIB:** RUGGEDCOM-TRAPS-MIB **OID:** 1.3.6.1.4.1.15004.5.41 **Definition:** The Local console is enabled **Binding(s):** None
loginFailureTrap	**Object Group:** ruggedcomDeviceLoginTrapGroup **MIB:** RUGGEDCOM-TRAPS-MIB **OID:** 1.3.6.1.4.1.15004.5.27 **Definition:** Failed login attempt to the device **Binding(s):** • loginUser • loginMgmtApp • loginRemoteIP • loginAccessLevel
loginInformationTrap	**Object Group:** ruggedcomDeviceLoginTrapGroup **MIB:** RUGGEDCOM-TRAPS-MIB **OID:** 1.3.6.1.4.1.15004.5.26

Variable	Description
	Definition: Indicates a successful login to the device **Binding(s):** • loginUser • loginMgmtApp • loginRemoteIP • loginAccessLevel
Link is intermittent on port<port number> (genericTrap)	**Object Group:** ruggedcomNotificationsGroup **MIB:** RUGGEDCOM-TRAPS-MIB **OID:** 1.3.6.1.4.1.15004.5.1 **Definition:** Intermittent link detected on a port **Binding(s):** • genericTrapSeverity • genericTrapDescription
MacAddressNotLearnedTrap	**Object Group:** ruggedcomNotificationsGroup **MIB:** RUGGEDCOM-TRAPS-MIB **OID:** 1.3.6.1.4.1.15004.5.34 **Definition:** The MAC address learn failed **Binding(s):** None
No valid SSH keys (genericTrap)	**Object Group:** ruggedcomNotificationsGroup **MIB:** RUGGEDCOM-TRAPS-MIB **OID:** 1.3.6.1.4.1.15004.5.1 **Definition:** The SSH key in the flash file becomes invalid or is not present **Binding(s):** genericTrapDescription
No valid SSL host (generic trap)	**Object Group:** ruggedcomNotificationsGroup **MIB:** RUGGEDCOM-TRAPS-MIB **OID:** 1.3.6.1.4.1.15004.5.1 **Definition:** The SSL host certificate is not valid **Binding(s):** genericTrapDescription
ntpServiceAvailableChange	**Object Group:** rcNTPNotifyGroup **MIB:** RUGGEDCOM-NTP-MIB **OID:** 1.3.6.1.4.1.15004.5.21 **Definition:** The NTP service availability status is updated **Binding(s):** • rcNTPPriServerReachable • rcNTPBackupServerReachable • rcDeviceErrNtpServerUnreachable
PowerSupplyTrap	**Object Group:** ruggedcomNotificationsGroup **MIB:** RUGGEDCOM-TRAPS-MIB **OID:** 1.3.6.1.4.1.15004.5.2 **Definition:** A trap generated when a power supply fails or comes up. The first trap would be generated on first power supply failure. The state of power supply (failed or restored)

Variable	Description
	is retrieved via object powerSupplyDescription at the time when trap is generated. The status of power supply units in device can be retrieved via objects rcDeviceStsPowerSupply1 and rcDeviceStsPowerSupply2. powerSupplyIdentifier object is recommended to be added as an optional parameter to the list of objects. **Binding(s):** powerSupplyDescription
privKeySnmpV3UserUnknwnTrap	**Object Group:** ruggedcomDeviceLoginTrapGroup **MIB:** RUGGEDCOM-TRAPS-MIB **OID:** 1.3.6.1.4.1.15004.5.25 **Definition:** A trap indicating an unknown private key from an SNMP V3 user **Binding(s):** None
radiusServiceAvailableChange	**Object Group:** rcRadiusNotifyGroup **MIB:** RUGGEDCOM-AAA-SERVER-MIB **OID:** 1.3.6.1.4.1.15004.5.22 **Definition:** The RADIUS service availability status is updated **Binding(s):** • rcRadiusServerReachable • rcDeviceErrRadiusServerUnreachable
rcBpduGuardActivated	**Object Group:** ruggedcomBpduTrapGroup **MIB:** RUGGEDCOM-TRAPS-MIB **OID:** 1.3.6.1.4.1.15004.5.41 **Definition:** BPDU Guard activated on a port **Binding(s):** ifIndex
rcChgPswdAdminTrap	**Object Group:** rcPswdChgTrapNotifyGroup **MIB:** RUGGEDCOM-TRAPS-MIB **OID:** 1.3.6.1.4.1.15004.5.20.1 **Definition:** The Admin user password is changed **Binding(s):** None
rcChgPswdDataStoreTrap	**Object Group:** rcPswdChgTrapNotifyGroup **MIB:** RUGGEDCOM-TRAPS-MIB **OID:** 1.3.6.1.4.1.15004.5.20.6 **Definition:** The password for data store encryption directive is changed **Binding(s):** None
rcChgPswdGuestTrap	**Object Group:** rcPswdChgTrapNotifyGroup **MIB:** RUGGEDCOM-TRAPS-MIB **OID:** 1.3.6.1.4.1.15004.5.20.3 **Definition:** The Guest user password is changed **Binding(s):** None
rcChgPswdOperTrap	**Object Group:** rcPswdChgTrapNotifyGroup **MIB:** RUGGEDCOM-TRAPS-MIB **OID:** 1.3.6.1.4.1.15004.5.20.2

Variable	Description
	Definition: The Operator user password is changed **Binding(s):** None
rcChgPswdRadiusTrap	**Object Group:** rcPswdChgTrapNotifyGroup **MIB:** RUGGEDCOM-TRAPS-MIB **OID:** 1.3.6.1.4.1.15004.5.20.4 **Definition:** The RADIUS server authentication key changed **Binding(s):** None
rcChgPswdSnmpAuthKeyTrap	**Object Group:** rcPswdChgTrapNotifyGroup **MIB:** RUGGEDCOM-TRAPS-MIB **OID:** 1.3.6.1.4.1.15004.5.20.8 **Definition:** The SNMP authentication key is changed **Binding(s):** None
rcChgPswdSnmpCommunityTrap	**Object Group:** rcPswdChgTrapNotifyGroup **MIB:** RUGGEDCOM-TRAPS-MIB **OID:** 1.3.6.1.4.1.15004.5.20.7 **Definition:** The SNMP community string is changed **Binding(s):** None
rcChgPswdSnmpPrivKeyTrap	**Object Group:** rcPswdChgTrapNotifyGroup **MIB:** RUGGEDCOM-TRAPS-MIB **OID:** 1.3.6.1.4.1.15004.5.20.9 **Definition:** The SNMP privacy key is changed **Binding(s):** None
rcChgPswdTacplusTrap	**Object Group:** rcPswdChgTrapNotifyGroup **MIB:** RUGGEDCOM-TRAPS-MIB **OID:** 1.3.6.1.4.1.15004.5.20.5 **Definition:** The TACACS+ server authentication key changed **Binding(s):** None
rcGMRPCantLrnMoreAddrs	**Object Group:** ruggedcomGMRPTrapGroup **MIB:** RUGGEDCOM-TRAPS-MIB **OID:** 1.3.6.1.4.1.15004.5.29 **Definition:** GMRP groups are full cannot learn more MAC addresses **Binding(s):** None
rcGpsStatusChange	**Object Group:** rtcGpsNotifyGroup **MIB:** RUGGEDCOM-GPS-MIB **OID:** 1.3.6.1.4.1.15004.5.19 **Definition:** Notification trap generated if the status of the GPS module is changed when GPS is the time source **Binding(s):** rcGpsStatus
rcGVRPCantLrnMoreVLANs	**Object Group:** ruggedcomGMRPTrapGroup **MIB:** RUGGEDCOM-TRAPS-MIB **OID:** 1.3.6.1.4.1.15004.5.30

Variable	Description
	Definition: The VLAN database is full, and cannot learn more VLAN IDs for GVRP **Binding(s):** None
rcIeee1588BMCErrorTrap	**Object Group:** ruggedcomPTP1588TrapGroup **MIB:** RUGGEDCOM-TRAPS-MIB **OID:** 1.3.6.1.4.1.15004.5.37 **Definition:** The PTP BMC(Best Master Clock) could not set a new time source **Binding(s):** None
rcIeee1588HoldoverStateTrap	**Object Group:** ruggedcomPTP1588TrapGroup **MIB:** RUGGEDCOM-TRAPS-MIB **OID:** 1.3.6.1.4.1.15004.5.36 **Definition:** The 1EEE1588 PTP clock is in a holdover state **Binding(s):** None
rcIgmpGrpMembershipTblFull	**Object Group:** ruggedcomIgmpTrapGroup **MIB:** RUGGEDCOM-TRAPS-MIB **OID:** 1.3.6.1.4.1.15004.5.32 **Definition:** IGMP request is denied as group membership table is full **Binding(s):** None
rcLoopedBpduRcvd	**Object Group:** ruggedcomBpduTrapGroup **MIB:** RUGGEDCOM-TRAPS-MIB **OID:** 1.3.6.1.4.1.15004.5.40 **Definition:** STP port received loopback BPDU due to simulation or faulty hardware **Binding(s):** ifIndex
rcMacAddressNotLearned	**Object Group:** ruggedcomNotificationsGroup **MIB:** RUGGEDCOM-TRAPS-MIB **OID:** 1.3.6.1.4.1.15004.5.34 **Definition:** If any VLAN is not learned for respective Vlan ID hence MAC address is not learned **Binding(s):** None
rcMcastCpuFiltTblFull	**Object Group:** ruggedcomMcastCpuFiltTblTrapGroup **MIB:** RUGGEDCOM-TRAPS-MIB **OID:** 1.3.6.1.4.1.15004.5.31 **Definition:** No space for more filters in the Mcast CPU filtering table **Binding(s):** None
rcIgmpMcastForwardTblFull	**Object Group:** ruggedcomIgmpTrapGroup **MIB:** RUGGEDCOM-TRAPS-MIB **OID:** 1.3.6.1.4.1.15004.5.33 **Definition:** IGMP request is denied as group membership table is full

Variable	Description
	Binding(s): None
rcPoeOverheat	**Object Group:** rcPoeNotifyGroup **MIB:** RUGGEDCOM-POE-MIB **OID:** 1.3.6.1.4.1.15004.5.12.1 **Definition:** When power consumption exceeds the limit the PoE module is overheated **Binding(s):** None
rcPoeOverload	**Object Group:** rcPoeNotifyGroup **MIB:** RUGGEDCOM-POE-MIB **OID:** 1.3.6.1.4.1.15004.5.12.2 **Definition:** When power consumption exceeds the limit the PoE module is overloaded **Binding(s):** None
rcPoeUndervoltage	**Object Group:** rcPoeNotifyGroup **MIB:** RUGGEDCOM-POE-MIB **OID:** 1.3.6.1.4.1.15004.5.12.3 **Definition:** The POE voltage is low **Binding(s):** None
rcPortSecurityViolated	**Object Group:** ruggedcomNotificationsGroup **MIB:** RUGGEDCOM-TRAPS-MIB **OID:** 1.3.6.1.4.1.15004.5.38 **Definition:** Access is restricted for the port **Binding(s):** ifIndex
RcSfpDdmAlarmTrap	**Object Group:** rcSfpDdmNotifyGroup **MIB:** RUGGEDCOM-SFP-DDM-MIB **OID:** 1.3.6.1.4.1.15004.5.52.2 **Definition:** An SFP DDM alarm trap indicates that at least one of the alarm flags is set or cleared on the SFP transceiver **Binding(s):** • rcSfpPortId • rcSfpDdmWarningFlags • rcSfpDdmTemp • rcSfpDdmVolt • rcSfpDdmTxBias • rcSfpDdmRxPower • rcSfpDdmTxPower
RcRstpNewTopology	**Object Groups:** rcRstpNotifyGroup, rcDigitalInputsNotifyGroup **MIB:** RUGGEDCOM-STP-MIB **OID:** 1.3.6.1.4.1.15004.5.11.1 **Definition:** A rcRstpNewTopology trap is sent by a bridge after topoogy change trap occures on one or more ports (topologyChange traps are sent), and topology becomes stable. Topology is stable when the tcWhile timer for all ports on this Bridge is zero. This trap is disabled if topologyChange trap is disabled by device configuration.

Variable	Description
	Binding(s): • rcRstpDot1dStpForwardingPorts • rcRstpDot1dStpBlockedPorts • rcRstpDot1dStpBrokenPorts • rcRstpDot1dRstpBackupPorts • rcRstpDot1dRstpAlternatePorts • dot1dStpRootPort • dot1dStpDesignatedRoot
RcSfpDdmWarningTrap	**Object Group:** rcSfpDdmNotifyGroup **MIB:** RUGGEDCOM-SFP-DDM-MIB **OID:** 1.3.6.1.4.1.15004.5.52.1 **Definition:** An SFP DDM warning trap indicates that at least one of the warning flags is set or cleared on the SFP transceiver **Binding(s):** • rcSfpPortId • rcSfpDdmWarningFlags • rcSfpDdmTemp • rcSfpDdmVolt • rcSfpDdmTxBias • rcSfpDdmRxPower • rcSfpDdmTxPower
Remote Syslog server(s) unreachable: ipaddress	**Object Group:** ruggedcomNotificationsGroup **MIB:** RUGGEDCOM-TRAPS-MIB **OID:** 1.3.6.1.4.1.15004.5.1 **Definition:** Remote syslog server status update **Binding(s):** • genericTrapSeverity • genericTrapDescription
serialCommBlocked	**Object Group:** ruggedcomSerialCommGroup **MIB:** RUGGEDCOM-TRAPS-MIB **OID:** 1.3.6.1.4.1.15004.5.42 **Definition:** Traffic congestion on TCP port; serial communication blocked **Binding(s):** None
SwUpgradeTrap	**Object Group:** ruggedcomNotificationsGroup **MIB:** RUGGEDCOM-TRAPS-MIB **OID:** 1.3.6.1.4.1.15004.5.3 **Definition:** A generic trap generated upon software upgrade. The rate at which this notification can be provided is 60 seconds. **Binding(s):** • rcDeviceInfoBootSwVersion • rcDeviceInfoMainSwVersion • rcDeviceInfoPendingBootSwVersion • rcDeviceInfoPendingMainSwVersion

Variable	Description
	• powerSupplyDescription
tacacsServiceAvailableChange	**Object Group:** rcTacacsNotifyGroup **MIB:** RUGGEDCOM-AAA-SERVER-MIB **OID:** 1.3.6.1.4.1.15004.5.23 **Definition:** The TACACS+ service availability status is updated **Binding(s):** • rcTacacsServerReachable • rcDeviceErrTacacsServerUnreachable
topologyChange	**Object Group:** rcRstpNotifyGroup **MIB:** RUGGEDCOM-STP-MIB **OID:** 1.3.6.1.2.1.17.0.2 **Definition:** STP topology change, as port transitioned from Learning to Forwarding or Forwarding to Discarding **Binding(s):** None
unknownRouteSerialProto	**Object Group:** ruggedcomSerialCommGroup **MIB:** RUGGEDCOM-TRAPS-MIB **OID:** 1.3.6.1.4.1.15004.5.43 **Definition:** A serial protocol is unable to route the address **Binding(s):** None
WeakPasswordTrap	**Object Group:** ruggedcomSecurityGroup01 **MIB:** RUGGEDCOM-SYS-INFO-MIB **OID:** 1.3.6.1.4.1.15004.5.8 **Definition:** A weak password indication trap generated by RUGGEDCOM devices **Binding(s):** rcDeviceStsPwdsWeak
WeakRadiusBackupKeyTrap	**Object Group:** ruggedcomNotificationsGroup **MIB:** RUGGEDCOM-TRAPS-MIB **OID:** 1.3.6.1.4.1.15004.5.56 **Definition:** The RADIUS backup server authentication key is weak **Binding(s):** None
WeakRadiusPrimaryKeyTrap	**Object Group:** ruggedcomWeakKeyTrapGroup **MIB:** RUGGEDCOM-TRAPS-MIB **OID:** 1.3.6.1.4.1.15004.5.55 **Definition:** The RADIUS primary server authentication key is weak **Binding(s):** None
WeakSnmpAuthKeyTrap	**Object Group:** ruggedcomNotificationsGroup **MIB:** RUGGEDCOM-TRAPS-MIB **OID:** 1.3.6.1.4.1.15004.5.57 **Definition:** The SNMP Authentication key is weak **Binding(s):** None
WeakSnmpPrivKeyTrap	**Object Group:** ruggedcomNotificationsGroup

Variable	Description
	MIB: RUGGEDCOM-TRAPS-MIB **OID:** 1.3.6.1.4.1.15004.5.58 **Definition:** The SNMP privacy key is weak **Binding(s):** None
WeakSSHKeyTrap	**Object Group:** ruggedcomNotificationsGroup **MIB:** RUGGEDCOM-TRAPS-MIB **OID:** 1.3.6.1.4.1.15004.5.53 **Definition:** The SSH key is weak **Binding(s):** None
WeakSSLKeyTrap	**Object Group:** ruggedcomNotificationsGroup **MIB:** RUGGEDCOM-TRAPS-MIB **OID:** 1.3.6.1.4.1.15004.5.54 **Definition:** The SSL key is weak **Binding(s):** None
WeakTacacsBackupKeyTrap	**Object Group:** ruggedcomWeakKeyTrapGroup **MIB:** RUGGEDCOM-TRAPS-MIB **OID:** 1.3.6.1.4.1.15004.5.60 **Definition:** The TACACS+ backup server key is weak **Binding(s):** None
WeakTacacsPrimaryKeyTrap	**Object Group:** ruggedcomWeakKeyTrapGroup **MIB:** RUGGEDCOM-TRAPS-MIB **OID:** 1.3.6.1.4.1.15004.5.59 **Definition:** The TACACS+ primary server key is weak **Binding(s):** None
Unable to obtain speed information from port <port_number> (genericTrap)	**Object Group:** ruggedcomNotificationsGroup **MIB:** RUGGEDCOM-TRAPS-MIB **OID:** 1.3.6.1.4.1.15004.5.1 **Definition:** Unknown speed of Ethernet port/Link speed is not in between 10MB to 10GB **Binding(s):** genericTrapDescription
Unresolved speed (genericTrap)	**Object Group:** ruggedcomNotificationsGroup **MIB:** RUGGEDCOM-TRAPS-MIB **OID:** 1.3.6.1.4.1.15004.5.1 **Definition:** Unable to read the port link speed from the HW **Binding(s):** • genericTrapSeverity • genericTrapDescription

14.2 Cipher suites and algorithms

The following cipher suites and algorithms are supported by RUGGEDCOM ROS v5.10.

HTTPS server (TCP/443)

Category/IANA name	Hexadecimal	Enabled by default
Named groups		
secp256r1 (prime256v1)	10017	✓
secp384r1	10018	✓
secp521r1	10019	✓
Cipher suite		
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	C02B	✓
TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384	C02E	✓
TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256	C02D	✓
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	C030	✓
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	C02F	✓
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	1009F	✓
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	1009E	✓
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	C02C	✓
Key type and length		
ECC 256 bits	—	✓
ECC 384 bits	—	—
ECC 521 bits	—	—
RSA 1024 bits[a]	—	—
RSA 2048 bits[a]	—	—
RSA 3072 bits	—	—
Signature		
sha256+ecdsa	0403	✓
sha256+rsa	0401	—
sha384+rsa	0501	—
sha512+rsa	0601	—
sha384+ecdsa	0503	—
sha512+ecdsa	0603	—

[a] Legacy

SSH server (TCP/22)

Category/IANA name	Hexadecimal	Enabled by default
Encryption algorithm		
aes128-ctr	—	✓

Category/IANA name	Hexadecimal	Enabled by default
aes192-ctr	—	✓
aes256-ctr	—	✓
aes128-gcm@openssh.com	—	✓
AEAD_AES_128_GCM	—	✓
aes256-gcm@openssh.com	—	✓
AEAD_AES_256_GCM	—	✓
Key algorithm		
ssh-ed25519	—	✓
ssh-rsa[a]	—	—
ssh-dss[a]	—	—
Key exchange algorithm		
curve25519-sha256	—	✓
curve25519-sha256@libssh.org	—	✓
ecdh-sha2-nistp256	—	✓
ecdh-sha2-nistp384	—	✓
ecdh-sha2-nistp521	—	✓
diffie-hellman-group16-sha512	—	✓
diffie-hellman-group18-sha512	—	✓
diffie-hellman-group15-sha512	—	✓
diffie-hellman-group17-sha512	—	✓
Key length		
ED22519, 256 bits	—	✓
RSA = 1024, 2048, 3072 bits[a]	—	—
DSA = 1024, 2048, 3072 bits[a]	—	—
MAC algorithm		
AEAD_AES_128_GCM	—	✓
aes128-gcm@openssh.com	—	✓
AEAD_AES_256_GCM	—	✓
aes256-gcm@openssh.com	—	✓
hmac-sha2-256[a]	—	✓
Compression algorithm	—	—

[a] Legacy

SNMP server (UDP/161)

Category/IANA name	Hexadecimal	Enabled by default
Authentication protocol		
HMAC-MD5-96[a]	—	—
HMAC-SHA-96[a]	—	—
HMACSHA256	—	✓

Category/IANA name	Hexadecimal	Enabled by default
Privacy protocol		
CBC-DES[a]	—	—
CFB128-AES128	—	—
CFB128-AES192 (Blumenthal)	—	—
CFB128-AES256 (Blumenthal)	—	✓

[a] Legacy

RADIUS client (UDP/1812)

Category/IANA name	Hexadecimal	Enabled by default
Integrity algorithm		
MD5[a]	—	—

[a] Legacy

TACACS+ client (TCP/49)

Category/IANA name	Hexadecimal	Enabled by default
Integrity algorithm		
MD5[a]	—	—
HMAC-MD5[a]	—	—
Encryption algorithm		
MD5[a]	—	—

[a] Legacy

For more information

Siemens RUGGEDCOM
https://www.siemens.com/ruggedcom

Industry Online Support (service and support)
https://support.industry.siemens.com

Industry Mall
https://mall.industry.siemens.com

Siemens Canada Ltd.
Digital Industries
Process Automation
300 Applewood Crescent
Concord, Ontario, L4K 4E5
Canada

© 2025 Siemens Canada Ltd.
Subject to change