Industrial Ethernet communication solution expert

Copyright © 2021 Indu-Sol GmbH. All rights reserved.

No company or individual is allowed to duplicate or transmit this manual in any forms without written permission issued by Indu-Sol GmbH.

Note

Purchased product, service or features should be constrained by Indu-Sol commercial contracts and clauses. The whole or part product, service or features described in this document may beyond purchasing or using range. Indu-Sol won't make any statement or warranty for this document content unless any other appointment exists. Due to product version upgrading or other reason, this document content will be upgraded periodically. Unless other appointment exists, this document only for usage guide, all statement, information and suggestion in this document won't constitute any warranty.
Preface

Managed Industrial Ethernet Switch User Manual has introduced this series of switches:

- Product features
- Product network management configuration
- Overview of related principles of network management

Audience

This manual applies to the following engineers:

- Network administrators
- Technical support engineers
- Network engineer

Text Format Convention

<table>
<thead>
<tr>
<th>Format</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot; &quot;</td>
<td>Words with &quot;&quot; represent the interface words. For example &quot;Port number&quot;.</td>
</tr>
<tr>
<td>&gt;</td>
<td>Multi-level path is separated by &quot;&gt;&quot;. Such as opening the local connection path description: Open &quot;Control Panel&gt; Network Connection&gt; Local Area Connection&quot;.</td>
</tr>
<tr>
<td>Light Blue Font</td>
<td>It represents the words clicked to achieve hyperlink. The font color is as follows: ‘Light Blue’.</td>
</tr>
</tbody>
</table>

Symbols

<table>
<thead>
<tr>
<th>Format</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Notice</td>
<td>Remind the announcements in the operation, improper operation may result in data loss or equipment damage.</td>
</tr>
<tr>
<td>Warning</td>
<td>Pay attention to the notes on the mark, improper operation may cause personal injury.</td>
</tr>
<tr>
<td>Note</td>
<td>Conduct a necessary supplements and explanations for the description of operation content.</td>
</tr>
<tr>
<td>Key</td>
<td>Configuration, operation, or tips for device usage.</td>
</tr>
<tr>
<td>Format</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
</tr>
<tr>
<td>Tips</td>
<td>Pay attention to the operation or information to ensure success device configuration or normal working.</td>
</tr>
</tbody>
</table>

**Revision Record**

<table>
<thead>
<tr>
<th>Version No.</th>
<th>Date</th>
<th>Revision note</th>
</tr>
</thead>
<tbody>
<tr>
<td>01</td>
<td>9/21/2020</td>
<td>Product release</td>
</tr>
<tr>
<td>02</td>
<td>6/01/2021</td>
<td>Function optimization</td>
</tr>
<tr>
<td>03</td>
<td>7/09/2021</td>
<td>Upgrade</td>
</tr>
<tr>
<td>04</td>
<td>09/17/2021</td>
<td>Document optimization</td>
</tr>
</tbody>
</table>
Contents

PREFACE ........................................................................................................................................... 3
CONTENTS ........................................................................................................................................ 1
1 LOG IN THE WEB INTERFACE ......................................................................................................... 1
  1.1 WEB BROWSING SYSTEM REQUIREMENT ................................................................. 1
  1.2 SETTING IP ADDRESS OF PC .................................................................................... 1
  1.3 LOG IN THE WEB CONFIGURATION INTERFACE ...................................................... 2
2 SYSTEM ......................................................................................................................................... 5
  2.1 SYSTEM INFORMATION ................................................................................................. 5
     2.1.1 System Information Configuration ........................................................................ 5
     2.1.2 System Information Monitor .............................................................................. 6
     2.1.3 Load..................................................................................................................... 7
  2.2 IP ......................................................................................................................................... 7
     2.2.1 IP Configuration .................................................................................................. 7
     2.2.2 IP Status Monitoring .......................................................................................... 11
  2.3 NTP CONFIGURATION ....................................................................................................... 12
     2.3.1 NTP Client Configuration ............................................................................... 12
     2.3.2 NTP Server Configuration .............................................................................. 13
  2.4 TIME ZONE ....................................................................................................................... 14
  2.5 LOG ..................................................................................................................................... 14
     2.5.1 Log Configuration ............................................................................................... 14
     2.5.2 Alert Log ............................................................................................................ 15
3 PORT ............................................................................................................................................ 17
  3.1 PORT ................................................................................................................................. 17
     3.1.1 Port Configuration ............................................................................................... 17
     3.1.2 Port State Monitoring ...................................................................................... 19
     3.1.3 Summary Statistical Monitoring ................................................................... 20
     3.1.4 Detailed Port Statistics .................................................................................... 21
  3.2 DDMI ................................................................................................................................... 23
     3.2.1 DDMI Configuration ....................................................................................... 23
     3.2.2 DDMI Overview Monitoring ............................................................................ 24
  3.3 RELAY ALARM .................................................................................................................. 25
     3.3.1 Relay Configuration ......................................................................................... 25
  3.4 IO ALARM ............................................................................................................................. 27
4 SAFETY DEVICE ............................................................... 28
  4.1 USER CONFIGURATION ............................................. 28
  4.2 PRIVILEGE LEVEL .................................................. 30
  4.3 AUTHENTICATION METHOD ....................................... 31
  4.4 SSH CONFIGURATION ............................................. 34
    4.4.1 HTTPS Setting ................................................ 34
  4.5 ACCESS MANAGEMENT ........................................... 36
    4.5.1 Access Management Configuration ......................... 36
    4.5.2 Access Management Statistics Monitoring ................. 38
  4.6 SNMP .............................................................. 38
    4.6.1 System Configuration ....................................... 38
    4.6.2 Trap Configuration ........................................... 40
    4.6.3 Community Configuration .................................. 45
    4.6.4 User Configuration .......................................... 45
    4.6.5 Group Configuration ......................................... 47
    4.6.6 View Configuration .......................................... 48
    4.6.7 Access Configuration ........................................ 49
  4.7 RMON ............................................................ 50
    4.7.1 Statistics Configuration .................................... 50
    4.7.2 History Configuration ....................................... 51
    4.7.3 Alarm Configuration .......................................... 52
    4.7.4 Link Event Configuration .................................... 54
    4.7.5 Statistics Monitoring ....................................... 54
    4.7.6 History Monitoring .......................................... 57
    4.7.7 Alarm Monitoring ............................................ 59
    4.7.8 Event Monitoring ............................................ 60
5 SECURE NETWORK .......................................................... 62
  5.1 PORT LIMIT CONTROL .............................................. 62
  5.2 PORT SECURITY ..................................................... 66
    5.2.1 Switch Monitoring ........................................... 66
    5.2.2 Port Monitoring ............................................... 68
  5.3 NAS .................................................................... 69
    5.3.1 NAS Configuration ............................................ 69
    5.3.2 Device Monitoring ............................................. 76
    5.3.3 Port Monitoring ............................................... 77
  5.4 ACL ................................................................. 78
    5.4.1 Port Configuration ............................................. 78
    5.4.2 Rate Limiter Configuration .................................. 80
    5.4.3 Access Control List Configuration ......................... 81
    5.4.4 ACL Status ..................................................... 83
  5.5 ETHERNET SERVICES ............................................... 84
    5.5.1 Port Configuration ............................................. 84
    5.5.2 L2CP Configuration ........................................... 85
5.5.3 Bandwidth Limitation Subset ................................................................. 86
5.5.4 EVCs Configuration ............................................................................. 88
5.5.5 ECEs Configuration ............................................................................. 93
5.5.6 EVC Statistics ..................................................................................... 101
5.6 RADIUS ............................................................................................... 102
5.6.1 RADIUS Server Configuration ............................................................ 102
5.6.2 RADIUS Server Status Overview Monitoring .................................... 105
5.6.3 RADIUS Authentication Statistics Link Monitoring .......................... 106
5.7 TACACS+ SERVER CONFIGURATION ................................................. 112

6 LAYER 2 PROTOCOL ............................................................................. 114

6.1 MAC ADDRESS TABLE ....................................................................... 114
6.1.1 MAC Address Table Configuration .................................................... 114
6.1.2 MAC Address Table Monitoring ....................................................... 116
6.2 VLAN ..................................................................................................... 117
6.2.1 VLAN ............................................................................................... 117
6.2.2 Access interface ................................................................................. 118
6.2.3 Trunk ................................................................................................. 120
6.2.4 Hybrid ............................................................................................... 121
6.3 DHCP SERVER ..................................................................................... 123
6.3.1 Mode Setting ..................................................................................... 123
6.3.2 Reserve IP Address Configuration ...................................................... 124
6.3.3 DHCP Pool Configuration ................................................................. 125
6.3.4 Statistics Monitoring ....................................................................... 131
6.3.5 Binding Monitoring .......................................................................... 132
6.3.6 Conflict Monitoring ......................................................................... 133
6.4 DHCP SNOOPING ............................................................................... 134
6.4.1 Snooping Configuration ................................................................. 134
6.4.2 Snooping Table Monitor .................................................................. 136
6.5 DHCP RELAY .................................................................................... 137
6.5.1 Relay Configuration ......................................................................... 137
6.5.2 Relay Statistics Monitoring ............................................................... 139
6.6 DHCP DETAILED STATISTICS ............................................................ 140
6.7 LLDP ..................................................................................................... 142
6.7.1 LLDP Configuration ......................................................................... 142
6.7.2 LLDP Neighbor Information .............................................................. 145
6.7.3 PoE Monitoring ............................................................................... 147
6.7.4 Port Statistics Monitoring ................................................................. 148
6.8 STORM SUPPRESSION .................................................................... 150
6.9 LOOP PROTECTION .......................................................................... 151
6.9.1 Loop Protection Configuration ......................................................... 151
6.9.2 Loop Protection Status ................................................................... 153
6.10 STATIC AGGREGATION .................................................................... 154
6.10.1 Static Link Aggregation Mode Configuration .................................. 154
9.6 EGRESS RELABELING ................................................................. 234
9.7 PORT DSCP ........................................................................ 235
9.8 DSCP-BASED QoS ................................................................. 237
9.9 DSCP CONVERSION ............................................................... 240
9.10 DSCP CLASSIFICATION ....................................................... 243
9.11 QoS CONTROL LIST .............................................................. 244
9.12 QoS STATISTICS ................................................................. 246
9.13 QCL STATUS .................................................................. 247

10 SYSTEM DIAGNOSIS ............................................................ 249
  10.1 MIRRORING ................................................................. 249
  10.2 PING ......................................................................... 251
  10.3 CABLE DETECTION ....................................................... 252

11 SYSTEM MAINTENANCE ......................................................... 254
  11.1 RESTART DEVICE .......................................................... 254
  11.2 RESTORE FACTORY SETTINGS ....................................... 254
  11.3 UPGRADE ................................................................ 255
  11.4 FIRMWARE SELECTION ................................................ 256

12 SYSTEM CONFIGURATION ........................................................ 257
  12.1 SAVE START-UP-CONFIG ................................................ 257
  12.2 DOWNLOAD ................................................................ 258
  12.3 UPLOAD .................................................................. 258
  12.4 ACTIVATE ................................................................. 259
  12.5 DELETE ............................................................... 260

13 FAQ ........................................................................... 261
  13.1 SIGN IN PROBLEMS ........................................................ 261
  13.2 CONFIGURATION PROBLEM .......................................... 261
  13.3 INDICATOR PROBLEM .................................................. 262

14 MAINTENANCE AND SERVICE .............................................. 264
  14.1 INTERNET SERVICE ....................................................... 264
  14.2 SERVICE HOTLINE ........................................................ 264
  14.3 PRODUCT REPAIR OR REPLACEMENT ....................... 265
1 Log in the Web Interface

1.1 WEB Browsing System Requirement

While using managed industrial Ethernet switches, the system should meet the following conditions.

<table>
<thead>
<tr>
<th>Hardware and software</th>
<th>System requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU</td>
<td>Above Pentium 586</td>
</tr>
<tr>
<td>Memory</td>
<td>Above 128MB</td>
</tr>
<tr>
<td>Resolution</td>
<td>Above 1024x768</td>
</tr>
<tr>
<td>Color</td>
<td>256 color or above</td>
</tr>
<tr>
<td>Browser</td>
<td>Internet Explorer 6.0 or above</td>
</tr>
<tr>
<td>Operating system</td>
<td>Windows XP/7/8/10</td>
</tr>
</tbody>
</table>

1.2 Setting IP Address of PC

The switch default management as follows:

<table>
<thead>
<tr>
<th>IP Settings</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>192.168.1.254</td>
</tr>
<tr>
<td>Subnet mask</td>
<td>255.255.255.0</td>
</tr>
</tbody>
</table>

When configuring a switch through the Web:
- Before making remote configuration, make sure that the route between the computer and the switch is reachable.
- Before local configuration, please make sure the IP address of the computer is on the same subnet to the one of switch.

Note:
When the switch is first configured. If it is configured locally, make sure the current computer network segment is 1.

Eg: Assume that the IP address of the current PC is 192.168.5.60, change the network segment "5" of the IP address to "1".

**Operation Steps**

Amendment steps as follow:

2. Change the selected "5" in red frame of the picture below to "1".

![Internet Protocol Version 4 (TCP/IPv4) Properties](image)

1. Click “OK”, IP address is modified successfully.
2. End.

### 1.3 Log in the Web Configuration Interface

**Operation Steps**

The initial password of the default user must be changed when logging in to the device for the first time. Login in the web configuration interface as follow:

1. Run the computer browser.
2. Enter the address of the switch "http://192.168.1.254" in the address bar of the browser.
3. Click the Enter key.
4. Pop-up dialog box as shown below, enter the user name and password in the login window.

Note:
- This switch supports one default user. This user has administrator privilege and can configure devices via WEB, TELNET, SSH, CLI, etc.
- The default username and password are “admin”; please strictly distinguish capital and small letter while entering.
- If you log in to the device for the first time, you will be prompted to change the default user's initial password. If the password has been modified through the WEB or CLI, the subsequent steps can be ignored and the modified password can be used to log in to the device directly.
- If the number of incorrect login information input reaches 5 times, the system will automatically lock the user for 5 minutes.

5. Click "Login".

6. Pop up a window as the figure below, enter the user name and new password on the login window.

Note:
- The device could be logged in for the first time by default username and initial password; After logging in, the system will prompt you to modify the default user's initial password, and you can log in normally after modification.
The length of the new password string must be greater than or equal to 8 and be composed of two or more of uppercase letters, lowercase letters, numbers and special characters.

After changing the password, save the current configuration on the "System Configuration > Save startup-config" page to take effect.

7. Click "OK".

8. Pop up a window as the figure below, enter the user name and password on the login window.

9. Click the "login" button.

10. End.

After login in successfully, user can configure relative parameters and information according to demands.

Note:
After logging in to the device, you can modify the IP address of the switch for ease of use.
2.1 System Information

2.1.1 System Information Configuration

The switch system information is provided here.

<table>
<thead>
<tr>
<th>System Information</th>
<th>System Information Configuration</th>
<th>System Information Monitoring</th>
<th>Sys Load</th>
</tr>
</thead>
<tbody>
<tr>
<td>contacts</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>System Name</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>System Location</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Contact

The textual identification of the contact person for this managed node, together with information on how to contact this person. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 32 to 126.

System Name

An administratively assigned name for this managed node. By convention, this is the node's fully-qualified domain name. A domain name is a text string consisting of the alphabet (A-Z, a-z), digits (0-9) and minus sign (-). No space characters are permitted as part of a name. The first character must be an alpha character. And the first or last character must not be a minus sign. The allowed string length is 0 to 255.
System Location
The physical location of this node (e.g., telephone closet, 3rd floor). The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 32 to 126.

Buttons
Save: Click to save changes.
Reset: Click to undo any changes made locally and revert to previously saved values.

2.1.2 System Information Monitor
The switch system information is provided here.

<table>
<thead>
<tr>
<th>System Information</th>
<th>System Information Configuration</th>
<th>System Information Monitoring</th>
<th>Sys Load</th>
<th>Auto-refresh</th>
<th>Refresh</th>
</tr>
</thead>
<tbody>
<tr>
<td>System</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Contact</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Location</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hardware</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MAC Address</td>
<td>00-22-01-00-00-00</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Time</td>
<td>System Date: 1970-01-01T07:13:52+00:00</td>
<td>Synchronize PC time</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>System Uptime</td>
<td>0d 0h:13:52</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Software</td>
<td>Software Version: 5.2.2.8020101000801178020000</td>
<td>Software Date: Jun 10 2021 14:32:35 by Jaguar</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Contact
System contacts configured by the path "System > System Information > System Information Configuration > Contacts".

Name
System name configured by the path "System > System Information > System Information Configuration > System Name".

Location
System location configured by the path "System > System Information > System Information Configuration > System Location".

MAC Address
The MAC Address of this switch.

System Date
The current (GMT) system time and date. The system time is obtained through the Timing server running on the switch, if any.
**System Uptime**

The period of time the device has been operational.

**Software Version**

The software version of this switch.

**Software Date**

The date when the switch software was produced.

**Buttons**

Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
Refresh: Click to refresh the page.

### 2.1.3 Load

This page uses dashboard graphics to display CPU utilization and memory utilization.

![Dashboard Graphics](image)

**Buttons**

Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
Refresh: Click to refresh the page.

### 2.2 IP

#### 2.2.1 IP Configuration

Configure IP basic settings, control IP interfaces and IP routes.
The maximum number of interfaces supported is 8 and the maximum number of routes is 32.

### Mode

Configure whether the IP stack should act as a Host or a Router. In Host mode, IP traffic between interfaces will not be routed. In Router mode traffic is routed between all interfaces.

### IP Interface

#### Delete

Select this option to delete an existing IP interface.
VLAN
The VLAN associated with the IP interface. Only ports in this VLAN will be able to access the IP interface. This field is only available for input when creating a new interface.

DHCPv4 Enable
Enable the DHCPv4 client by checking this box. If this option is enabled, the system will configure the IPv4 address and mask of the interface using the DHCPv4 protocol. The DHCPv4 client will announce the configured System Name as hostname to provide DNS lookup.

DHCPv4 Fallback
The number of seconds for trying to obtain a DHCP lease. After this period expires, a configured IPv4 address will be used as IPv4 interface address. A value of zero disables the fallback mechanism, such that DHCP will keep retrying until a valid lease is obtained. Legal values are 0 to 4294967295 seconds.

DHCPv4 Current Lease
For DHCP interfaces with an active lease, this column shows the current interface address, as provided by the DHCP server.

IPv4 Address
The IPv4 address of the interface in dotted decimal notation.
If DHCP is enabled, this field configures the fallback address. The field may be left blank if IPv4 operation on the interface is not desired - or no DHCP fallback address is desired.

IPv4 Mask Length
The IPv4 network mask, in number of bits (prefix length). Valid values are between 0 and 30 bits for a IPv4 address.
If DHCP is enabled, this field configures the fallback address network mask. The field may be left blank if IPv4 operation on the interface is not desired - or no DHCP fallback address is desired.

IP Routes
Delete
Select this option to delete an existing IP route.
Internet
The destination IP network or host address of this route. Valid format is dotted decimal notation or a valid IPv6 notation. A default route can use the value 0.0.0.0 or IPv6:: notation.

Mask Length
The destination IP network or host mask, in number of bits (prefix length). It defines how much of a network address that must match, in order to qualify for this route. Valid values are between 0 and 32 bits respectively 128 for IPv6 routes. Only a default route will have a mask length of 0 (as it will match anything).

Gateway
The IP address of the IP gateway. Valid format is dotted decimal notation or a valid IPv6 notation. Gateway and Network must be of the same type.

Next Hop VLAN (Only for IPv6)
The VLAN ID (VID) of the specific IPv6 interface associated with the gateway. The given VID ranges from 1 to 4095 and will be effective only when the corresponding IPv6 interface is valid. If the IPv6 gateway address is link-local, it must specify the next hop VLAN for the gateway. If the IPv6 gateway address is not link-local, system ignores the next hop VLAN for the gateway.

Static ARP Configuration
Delete
Select this option to delete an existing entry. It will be deleted during the next Save operation.

IP Address
Allowed Source IP address in ARP request packets.

MAC Address
Allowed Source MAC address in ARP request packets.

Buttons
Add new IP interface: click here to add new IP interface. A maximum of 8 interfaces is supported.
Add new IP route: click to add new IP route. A maximum of 32 routes is supported.
Add Arp: click to add a new entry to the static ARP checklist.
Save: Click to save changes.
Reset: Click to undo any changes made locally and revert to previously saved values.

2.2.2 IP Status Monitoring

This page displays the status of the IP protocol layer. The status is defined by the IP interfaces, the IP routes and the neighbour cache (ARP cache) status.

<table>
<thead>
<tr>
<th>Interface</th>
<th>Type</th>
<th>Address</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>OS:lo</td>
<td>LINK</td>
<td>00:00:00:00:00:00:00-00:00-&lt;UP LOOPBACK RUNNING MULTICAST&gt;</td>
<td></td>
</tr>
<tr>
<td>OS:lo</td>
<td>IPv4</td>
<td>127.0.0.1/8</td>
<td></td>
</tr>
<tr>
<td>VLAN1</td>
<td>LINK</td>
<td>00-00-00-00-00-00-00-00-00-&lt;UP BROADCAST RUNNING MULTICAST&gt;</td>
<td></td>
</tr>
<tr>
<td>VLAN1</td>
<td>IPv4</td>
<td>192.168.1.254/24</td>
<td></td>
</tr>
</tbody>
</table>

**IP Routes**

<table>
<thead>
<tr>
<th>Network</th>
<th>Gateway</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>127.0.0.1/32</td>
<td>127.0.0.1</td>
<td>&lt;UP HOST&gt;</td>
</tr>
<tr>
<td>224.0.0.0/4</td>
<td>127.0.0.1</td>
<td>&lt;UP&gt;</td>
</tr>
<tr>
<td>::1/128</td>
<td>::1</td>
<td>&lt;UP HOST&gt;</td>
</tr>
</tbody>
</table>

**Neighbor cache**

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Link Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.1.161</td>
<td>VLAN1:00-40-4d-2f-2f-52</td>
</tr>
<tr>
<td>fe80::222:6ff:fe00:0</td>
<td>VLAN1:00-22-6f-00-00-00</td>
</tr>
</tbody>
</table>

**IP Interface**

**Interface**

- Interface Name.

**Type**

- The address type of the entry. This may be LINK or IPv4.

**Address**

- The current address of the interface (of the given type).
Status
The status flags of the interface (and/or address).

IP Routes

Network
The destination IP network or host address of this route.

Gateway
The gateway address of this route.

Status
The status flags of the route.

Neighbour Cache

IP Address
The IP address of the entry.

Link Address
The Link (MAC) address for which a binding to the IP address given exist.

Buttons
Refresh: Click to refresh the page immediately.
Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

2.3 NTP Configuration

2.3.1 NTP Client Configuration
Configure NTP client on this page.
**Mode**

Indicates the NTP mode operation. Possible modes are:

- Enabled: Enable NTP client mode operation.
- Disabled: Disable NTP client mode operation.

**Server #**

Provide the IPv4 or IPv6 address of a NTP server. A IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example, fe80::215:c5ff:fe03:4dc7. The symbol is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can appear only once. It can also represent a legally valid IPv4 address. For example, "::192.1.2.34". In addition, it can also accept a domain name address.

### 2.3.2 NTP Server Configuration

Configure NTP server on this page.
Mode

Configure the NTP server mode, options are as follows:

- Enable: Enable NTP Server.
- Disable: Disable NTP Server.

2.4 Time Zone

Time Zone

Lists the various Time Zones worldwide. Select appropriate Time Zone from the drop down and click Save to set.

Acronym

User can set the acronym of the time zone. This is a User configurable acronym to identify the time zone. (Range: Up to 16 characters).

2.5 Log

2.5.1 Log Configuration
Server Mode

Indicates the server mode operation. When the mode operation is enabled, the syslog message will send out to the syslog server. The syslog protocol is based on UDP communication and received on UDP port 514 and the syslog server will not send acknowledgments back since UDP is a connectionless protocol and it does not provide acknowledgments. The syslog packet will always send out even if the syslog server does not exist. Possible modes are:

- Enabled: Enable server mode operation.
- Disabled: Disable server mode operation.

Server Address

Indicates the IPv4 host address of syslog server. If the switch provides DNS feature, it also can be a domain name.

2.5.2 Alert Log

The alarm log interface of switch system is as follows.

![Alert Log Interface]

**Level**

The level of the alarm log entry.

- Notification: the alarm log entry belongs to the notification level.
- Important: the alarm log entry belongs to the important level.
- Warning: the alarm log entry belongs to the warning level.
- Error: the alarm log entry belongs to the error level.
- All: All alarm logs.
ID
ID of the log entry (>= 1).

Level
Severity level of the log entry.

Type
Log category.

Time
Log occurrence time.

Message
Details of the log entry.

Buttons
Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
Refresh: Update the log entry to the current entry ID.
| < <: update the log entry to the first available entry ID.
< <: update the log entry to the previously available entry ID.
> >: update the log entry to the next available entry ID.
> > |: update the log entry to the last available entry ID.
3.1 Port

3.1.1 Port Configuration

This feature displays current port configurations. Ports can also be configured using this feature.

<table>
<thead>
<tr>
<th>Port</th>
<th>Description</th>
<th>Speed</th>
<th>Configured</th>
<th>Auto Neg</th>
<th>Adorn M</th>
<th>Jumbo</th>
<th>Ig</th>
<th>FcoE</th>
<th>Ctep Rx</th>
<th>Ctep Tx</th>
<th>Frame</th>
<th>Maximum</th>
<th>Error Control Mode</th>
<th>Frame Length Check</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Port

This is the logical port number for this row.

Description

The description of the port. It is an ASCII string no longer than 256 characters.

Link

The current link state is displayed graphically. Green indicates the link is up and red that it is down.
**Current Link Speed**

Current speed duplexes the current link speed of this port.

**Configured Link Speed**

Selects any available link speed for the given switch port. Only speeds supported by the specific port is shown. Possible speeds are:

- **Disabled**: disables the switch port.
- **Auto**: the port automatically negotiates the transmission speed and duplex with the connected device, and keeps the highest compatible speed with the connected device.
- **10Mbps HDX**: Forces the port in 10 Mbps half duplex mode.
- **10Mbps FDX**: Forces the port in 10 Mbps full duplex mode.
- **100Mbps HDX**: Forces the port in 100 Mbps half duplex mode.
- **100Mbps FDX**: Forces the port in 100 Mbps full duplex mode.
- **1Gbps FDX**: Forces the port in 1 Gbps full duplex.
- **2.5Gbps FDX**: Forces the port in 2.5Gbps full duplex mode.

**Advertise Duplex**

When duplex is set as auto that is, Autonegotiation, the port will only advertise the specified duplex as either Fdx or Hdx to the link partner. By default port will advertise all the supported duplexes if the Duplex is Auto.

**Advertise Speed**

When Speed is set as auto that is, Autonegotiation, the port will only advertise the specified speeds (10M 100M 1G) to the link partner. By default port will advertise all the supported speeds if speed is set as Auto.

**Flow Control**

When Auto Speed is selected on a port, this section indicates the flow control capability that is advertised to the link partner. When a fixed-speed setting is selected, that is what is used. The Current Rx column indicates whether pause frames on the port are obeyed, and the Current Tx column indicates whether pause frames on the port are transmitted. The Rx and Tx settings are determined by the result of the last Auto-Negotiation.

**Maximum Frame Size**

Enter the maximum frame size allowed for the switch port, including FCS. The range is 1518-10240 bytes.

**Excessive Collision Mode**

Configure port transmit collision behavior.
- Discard: Discard frame after 16 collisions (default).
- Restart: Restart backoff algorithm after 16 collisions.

**Frame Length Check**

Configures if frames with incorrect frame length in the EtherType/Length field shall be dropped. An Ethernet frame contains a field EtherType which can be used to indicate the frame payload size (in bytes) for values of 1535 and below. If the EtherType/Length field is above 1535, it indicates that the field is used as an EtherType (indicating which protocol is encapsulated in the payload of the frame). If "frame length check" is enabled, frames with payload size less than 1536 bytes are dropped, if the EtherType/Length field doesn't match the actually payload length. If "frame length check" is disabled, frames are not dropped due to frame length mismatch. Note: Frames with mismatched frame lengths calculated by the calculator are not deleted.

**Buttons**

Save: Click to save changes.
Reset: Click to undo any changes made locally and revert to previously saved values.
Refresh: Click to refresh the page; any changes made locally will be undone.

### 3.1.2 Port State Monitoring

This page provides port state monitoring of the current switch.

The port states are illustrated as follows:

- **RJ45 port**
- **SFP ports**
- **Status**
  - Disable
  - Disconnect
  - Link

**Buttons**

Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
3.1.3 Summary Statistical Monitoring

This page provides an overview of general traffic statistics for all switch ports. The displayed counters are:

<table>
<thead>
<tr>
<th>Port</th>
<th>Description</th>
<th>Packets</th>
<th>Bytes</th>
<th>Errors</th>
<th>Drops</th>
<th>Filtered</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Received</td>
<td>Transmitted</td>
<td>Received</td>
<td>Transmitted</td>
<td>Received</td>
</tr>
<tr>
<td>1</td>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>...</td>
<td></td>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td>12</td>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Port
The switch port number.

Description
The description of the port.

Packets
The number of received and transmitted packets per port.

Bytes
The number of received and transmitted bytes per port.

Errors
The number of frames received in error and the number of incomplete transmissions per port.

Drops
The number of frames discarded due to ingress or egress congestion.

Filtered
The number of received frames filtered by the forwarding process.

Buttons
Refresh: Click to refresh the page immediately.
Clear: Clears the counters for all ports.
Auto-refresh: Check this box to enable an automatic refresh. Automatic refresh occurs every 3 seconds.

### 3.1.4 Detailed Port Statistics

This page provides detailed traffic statistics for a specific switch port. Use the port select box to select which switch port details to display.

The displayed counters are the totals for receive and transmit, the size counters for receive and transmit, and the error counters for receive and transmit.

<table>
<thead>
<tr>
<th>Port</th>
<th>Ports Configuration</th>
<th>State Monitor</th>
<th>Traffic Overview Monitor</th>
<th>Detailed Statistics Monitor</th>
<th>Port 1</th>
<th>Auto-refresh</th>
<th>Refresh</th>
<th>Clear</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rx 64 bytes</td>
<td>0</td>
<td>Tx 64 bytes</td>
<td>0</td>
<td>Rx 64-127 bytes</td>
<td>0</td>
<td>Tx 64-127 bytes</td>
<td>0</td>
<td>Rx 128-255 bytes</td>
</tr>
<tr>
<td>Rx Q0</td>
<td>0</td>
<td>Tx Q0</td>
<td>0</td>
<td>Rx Q1</td>
<td>0</td>
<td>Tx Q1</td>
<td>0</td>
<td>Rx Q2</td>
</tr>
<tr>
<td>Rx Drops</td>
<td>0</td>
<td>Tx Drops</td>
<td>0</td>
<td>Rx CRC/Alignment</td>
<td>0</td>
<td>Tx Late/Frac. Cell</td>
<td>0</td>
<td>Rx Undersize</td>
</tr>
</tbody>
</table>

**Receive and Transmit Total**

**Rx and Tx Packets**

The number of received and transmitted (good and bad) packets.

**Rx and Tx Octets**

Number of bytes received and sent (good and bad). Includes FCS, but excludes framing bits.

**Rx and Tx Unicast**

The number of unicast packets received and sent (good and bad).
**Rx and Tx Multicast**

The number of multicast packets received and sent (good and bad).

**Rx and Tx Broadcast**

Number of broadcast packets received and sent (good and bad).

**Rx and Tx Pause**

A count of MAC control frames received or sent on this port, which have an opcode indicating pause operation.

**Receive and Transmit Size Counters**

Number of packets of different lengths received and sent. They are categorized according to their respective frame sizes.

**Receive and Transmit Queue Counters**

The number of received and transmitted packets per input and output queue.

**Receive Error Counters**

**Rx Drops**

The number of frames dropped due to lack of receive buffers or egress congestion.

**Rx CRC/Alignment**

The number of frames received with CRC or alignment errors.

**Rx Undersize**

The number of short 1 frames received with valid CRC.

**Rx Oversize**

The number of long 2 frames received with valid CRC.

**Rx Fragments**

The number of short 1 frames received with invalid CRC.

**Rx Jabber**

The number of long 2 frames received with invalid CRC.

**Rx Filtered**

The number of received frames filtered by the forwarding process.

1 Short frames are frames that are smaller than 64 bytes.

2 Long frames are frames that are longer than the configured maximum frame length for this port.
Transmit Error Counters

Tx Drops
The number of frames dropped due to output buffer congestion.

Tx Late/Exc.Coll
The number of frames dropped due to excessive or late collisions.

Buttons
The port select box determines which port is affected by clicking the buttons.
Refresh: Click to refresh the page immediately.
Clear: Clears the counters for all ports.
Auto-refresh: Check this box to enable an automatic refresh. Automatic refresh occurs every 3 seconds.

3.2 DDMI

3.2.1 DDMI Configuration
This page allows you to configure DDMI.

<table>
<thead>
<tr>
<th>DDMI</th>
<th>DDMI Configuration</th>
<th>DDMI Overview Monitor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mode</td>
<td>Enabled</td>
<td></td>
</tr>
</tbody>
</table>

Mode
Display DDMI mode operation. Possible modes are:
- Enable: enable DDMI mode operation.
- Disable: disable DDMI mode operation.

Buttons
Save: Click to save changes.
Reset: Click here to undo any changes made locally and revert to the previously saved values.
3.2.2 DDMI Overview Monitoring

This page displays an overview of DDMI information.

<table>
<thead>
<tr>
<th>Port</th>
<th>Vendor</th>
<th>Part Number</th>
<th>Serial Number</th>
<th>Revision</th>
<th>Data Code</th>
<th>Transceiver</th>
</tr>
</thead>
<tbody>
<tr>
<td>9</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>NONE</td>
</tr>
<tr>
<td>10</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>NONE</td>
</tr>
<tr>
<td>11</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>NONE</td>
</tr>
<tr>
<td>12</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>NONE</td>
</tr>
</tbody>
</table>

**Port**

DDMI port.

**Vendor**

Display the supplier name.

**Part Number**

Display the supplier PN component number provided by the SFP supplier.

**Serial Number**

Display the supplier serial number provided by the supplier.

**Revision**

Indicate the revision level of the supplier according to the part number provided by the supplier.

**Data Code**

Display the manufacturing date code of the supplier.

**Transceiver**

Indicate transceiver compatibility.

**Buttons**

Refresh: Click to refresh the page immediately.

Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
### 3.3 Relay Alarm

#### 3.3.1 Relay Configuration

On the page of “Relay Configuration”, user can enable power supply, port alarm, and configure relevant alarm information.

<table>
<thead>
<tr>
<th>Relay Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Global Configurations</strong></td>
</tr>
<tr>
<td><strong>Alarm Mode</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Power Mode Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power</td>
</tr>
<tr>
<td>1</td>
</tr>
<tr>
<td>2</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Port Mode Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
</tr>
<tr>
<td>1</td>
</tr>
<tr>
<td>2</td>
</tr>
<tr>
<td>3</td>
</tr>
<tr>
<td>4</td>
</tr>
<tr>
<td>5</td>
</tr>
<tr>
<td>6</td>
</tr>
<tr>
<td>7</td>
</tr>
<tr>
<td>8</td>
</tr>
<tr>
<td>9</td>
</tr>
<tr>
<td>10</td>
</tr>
<tr>
<td>11</td>
</tr>
<tr>
<td>12</td>
</tr>
</tbody>
</table>

[Save] [Reset]
Global Configurations

Alarm Mode
Enable relay alarm or not, options as follows:
- Enable
- Disable

Power Mode Configuration

Power
Display power supply of the device, value is 1 or 2.

Mode
Enable the power supply alarm or not, options as follows:
- Enable: when the power supply fails, power supply alarm will be triggered.
- Disable

Status
Connection status of power supply, the device will automatically recognize and display, values include:
- Fault
- Normal.

Port Mode Configuration

Port
Displays the port number of the device.

Mode
Enable the port alarm or not, options as follows:
- Enable: when the port is disconnected, port alarm will be triggered.
- Disable

Link
Connection status of the port, the device will automatically recognize and display, values include:
- Up
- Down

Buttons
Save: Click to save changes.
Reset: Click to undo any changes made locally and revert to previously saved values.
3.4 IO Alarm

On the page of “IO Alarm”, user can enable IO alarm and configure IO alarm information.

<table>
<thead>
<tr>
<th>IO</th>
<th>Mode</th>
<th>Type</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Disabled</td>
<td>Close</td>
<td>Open</td>
</tr>
<tr>
<td>2</td>
<td>Disabled</td>
<td>Close</td>
<td>Open</td>
</tr>
</tbody>
</table>

**IO**

Display IO number of the device, value is 1 or 2.

**Mode**

Enable the IO alarm or not, options as follows:
- Enabled
- Disabled

**Type**

Configure the type of enabling IO alarm, when input state conforms to the value of Type, IO alarm will be triggered. Type options as follows:
- Open
- Close
- Both

**State**

IO input state, the device will automatically recognize and display, values as follows:
- Open
- Close

**Buttons**

Save: Click to save changes.
Reset: Click to undo any changes made locally and revert to previously saved values.
4.1 User Configuration

This option provides an overview of the current users. Currently, the only way to log in as another user on the web server is to close and reopen the browser.

<table>
<thead>
<tr>
<th>User Name</th>
<th>Privilege Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>admin</td>
<td>15</td>
</tr>
</tbody>
</table>

The values displayed by each user are:

**User Name**

The name identifying the user. This is also a link to edit a user.

**Privilege Level**

The privilege level of the user. The allowed range is 0 to 15. If the privilege level value is 15, it can access all groups, that is, that is granted the fully control of the device. But others value need to refer to each group privilege level. User's privilege should be same or greater than the group privilege level to have the access of that group. By default setting, most groups privilege level 5 has the read-only access and privilege level 10 has the read-write access. And the system maintenance (software upload, factory defaults, and so on) need user privilege level 15. Generally, the privilege level 15 can be used for an administrator account, privilege level 10 for a standard user account and privilege level 5 for a guest account.
Buttons

Add new user: Click this button to add a new user.

This page configures a user.

<table>
<thead>
<tr>
<th>Add User</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>User Settings</strong></td>
</tr>
<tr>
<td><strong>User Name</strong></td>
</tr>
<tr>
<td><strong>Password</strong></td>
</tr>
<tr>
<td><strong>Password (again)</strong></td>
</tr>
<tr>
<td><strong>Privilege Level</strong></td>
</tr>
</tbody>
</table>

Buttons

Save: Click to save changes.

User Name

A string identifying the user name that this entry should belong to. The allowed string length is 1 to 31. The valid user name allows letters, numbers and underscores.

Password

The password of the user. The allowed string length must be greater than or equal to 8. Passwords contain at least two of uppercase letters, lowercase letters, numbers or special characters.

Privilege Level

The privilege level of the user. The allowed range is 0 to 15. If the privilege level value is 15, it can access all groups, i.e. that is granted the fully control of the device. But others value need to refer to each group privilege level. User’s privilege should be same or greater than the group privilege level to have the access of that group. By default setting, most groups privilege level 5 has the read-only access and privilege level 10 has the read-write access. And the system maintenance (software upload, factory defaults and etc.) need user privilege level 15. Generally, the privilege level 15 can be used for an administrator account, privilege level 10 for a standard user account and privilege level 5 for a guest account.
Reset: Click to undo any changes made locally and revert to previously saved values.
Back: Click to undo any changes made locally and return to the Users.
Delete user: Delete the current user. This button is not available for new configurations (Add new user)

4.2 Privilege Level

This option provides an overview of the privilege levels configuration.

<table>
<thead>
<tr>
<th>Group Name</th>
<th>Privilege Levels</th>
<th>Configuration/Execute Read/write</th>
<th>Status/Statistics Read-only</th>
<th>Status/Statistics Read/write</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aggregation</td>
<td>5</td>
<td>10 •</td>
<td>5 •</td>
<td>10 •</td>
</tr>
<tr>
<td>DDMI</td>
<td>5</td>
<td>10 •</td>
<td>5 •</td>
<td>10 •</td>
</tr>
<tr>
<td>Debug</td>
<td>15 •</td>
<td>10 •</td>
<td>15 •</td>
<td>10 •</td>
</tr>
<tr>
<td>DHCP</td>
<td>5 •</td>
<td>10 •</td>
<td>5 •</td>
<td>10 •</td>
</tr>
<tr>
<td>Diagnostics</td>
<td>5 •</td>
<td>10 •</td>
<td>5 •</td>
<td>10 •</td>
</tr>
<tr>
<td>ERPS</td>
<td>5 •</td>
<td>10 •</td>
<td>5 •</td>
<td>10 •</td>
</tr>
<tr>
<td>EVC</td>
<td>5 •</td>
<td>10 •</td>
<td>5 •</td>
<td>10 •</td>
</tr>
<tr>
<td>IO_Alarm</td>
<td>5 •</td>
<td>10 •</td>
<td>5 •</td>
<td>10 •</td>
</tr>
<tr>
<td>IP</td>
<td>5 •</td>
<td>10 •</td>
<td>5 •</td>
<td>10 •</td>
</tr>
<tr>
<td>IPMC_Snooping</td>
<td>5 •</td>
<td>10 •</td>
<td>5 •</td>
<td>10 •</td>
</tr>
<tr>
<td>JSON_RPC</td>
<td>5 •</td>
<td>10 •</td>
<td>5 •</td>
<td>10 •</td>
</tr>
<tr>
<td>JSON_RPC_Notification</td>
<td>5 •</td>
<td>10 •</td>
<td>5 •</td>
<td>10 •</td>
</tr>
<tr>
<td>LACP</td>
<td>5 •</td>
<td>10 •</td>
<td>5 •</td>
<td>10 •</td>
</tr>
<tr>
<td>LLDP</td>
<td>5 •</td>
<td>10 •</td>
<td>5 •</td>
<td>10 •</td>
</tr>
<tr>
<td>Loop_Protect</td>
<td>5 •</td>
<td>10 •</td>
<td>5 •</td>
<td>10 •</td>
</tr>
<tr>
<td>MAC_Table</td>
<td>5 •</td>
<td>10 •</td>
<td>5 •</td>
<td>10 •</td>
</tr>
<tr>
<td>Maintenance</td>
<td>15 •</td>
<td>15 •</td>
<td>15 •</td>
<td>15 •</td>
</tr>
<tr>
<td>Mirroring</td>
<td>5 •</td>
<td>10 •</td>
<td>5 •</td>
<td>10 •</td>
</tr>
<tr>
<td>NTP</td>
<td>5 •</td>
<td>10 •</td>
<td>5 •</td>
<td>10 •</td>
</tr>
<tr>
<td>POE</td>
<td>5 •</td>
<td>10 •</td>
<td>5 •</td>
<td>10 •</td>
</tr>
<tr>
<td>Ports</td>
<td>5 •</td>
<td>10 •</td>
<td>1 •</td>
<td>10 •</td>
</tr>
<tr>
<td>QoS</td>
<td>5 •</td>
<td>10 •</td>
<td>5 •</td>
<td>10 •</td>
</tr>
<tr>
<td>Relay</td>
<td>5 •</td>
<td>10 •</td>
<td>5 •</td>
<td>10 •</td>
</tr>
<tr>
<td>Ring</td>
<td>5 •</td>
<td>10 •</td>
<td>5 •</td>
<td>10 •</td>
</tr>
<tr>
<td>Security</td>
<td>5 •</td>
<td>10 •</td>
<td>5 •</td>
<td>10 •</td>
</tr>
<tr>
<td>Spanning_Tree</td>
<td>5 •</td>
<td>10 •</td>
<td>5 •</td>
<td>10 •</td>
</tr>
<tr>
<td>System</td>
<td>5 •</td>
<td>10 •</td>
<td>1 •</td>
<td>10 •</td>
</tr>
<tr>
<td>VLANs</td>
<td>5 •</td>
<td>10 •</td>
<td>5 •</td>
<td>10 •</td>
</tr>
</tbody>
</table>

Group Name

The name identifying the privilege group. In most cases, a privilege level group consists of a single module (for example, LACP, RSTP or QoS), but a few of them contains more than one. The following description defines these privilege level groups in details:

- System: Contact, Name, Location, Time Zone, Log.
- Security: Authentication, System Access Management, Port (including Dot1x port, MAC based and the MAC Address Limit), ACL, HTTPS, SSH, ARP Inspection, IP source guard.
- IP: Everything except ping.
- Port: Everything except VeriPHY.
- Diagnostics: Ping and VeriPHY.
- Debug: Only present in CLI.

Privilege Level

Every group has an authorization Privilege level for the following sub groups: configuration read-only, configuration/execute read-write, status/statistics read-only, status/statistics read-write (for example, for clearing of statistics). User Privilege should be same or greater than the authorization Privilege level to have the access to that group.

Buttons

Save: Click to save changes.
Undo: Click to undo any changes made locally and revert to previously saved values.

4.3 Authentication method

Authentication Method Configuration

This option allows you to configure how a user is authenticated when he logs into the switch via one of the management client interfaces.
The table has one row for each client type and a number of columns which are as follows:

**Client**

The management client for which the configuration below applies.

**Method**

Method can be set to one of the following values:
- no: Authentication is disabled and login is not possible.
- local: Use the local user database on the switch for authentication.
- radius: Uses one or more of the remote RADIUS servers for authentication.
- tacacs: Uses one or more of the remote TACACS+ servers for authentication.

Methods that involves remote servers are timed out if the remote servers are offline. In this case the next method is tried. Each method is tried from left to right and continues until a method either approves or rejects a user. If a remote server is used for primary authentication it is recommended to configure secondary authentication.
as local. This will enable the management client to log in via the local user database if none of the configured authentication servers are alive.

**Command Authorization Method Configuration**

The command authorization section allows you to limit the CLI commands available to a user. The table has one row for each client type and a number of columns which are as follows:

**Client**

The management client for which the configuration below applies.

**Method**

Method can be set to one of the following values:
- no: disable command authorization. User is granted access to CLI commands according to his privilege level.
- tacacs: Uses one or more of the remote TACACS+ servers for command authorization. If all remote servers are offline, the user is granted access to CLI commands according to his privilege level.

**Cmd Lvl**

Authorizes all commands with a privilege level higher than or equal to this level. Valid values are in the range 0 to 15.

**Cfg Cmd**

Also, authorizes configuration commands.

**Accounting Method Configuration**

The accounting section allows you to configure command and exec (login) accounting. The table has one row for each client type and a number of columns which are as follows:

**Client**

The management client for which the configuration below applies.

**Method**

Method can be set to one of the following values:
- no: disable authentication.
- tacacs: Uses one or more of the remote TACACS+ servers for accounting.

**Cmd Lvl**

Enable statistics of all commands with a privilege level higher than or equal to this level. Valid values are in the range 0 to 15. Leave the field empty to disable command accounting.
4. Exec

Enables exec (login) accounting.

Buttons

Save: Click to save changes.
Reset: Click to undo any changes made locally and revert to previously saved values.

4.4 SSH Configuration

This option allows you to configure SSH.

Mode

The Mode option indicates the SSH mode operation. Possible modes are:

- Enabled: Enables SSH mode operation.
- Disabled: Disables SSH mode operation.

Buttons

Save: Click to save changes.
Reset: Click to undo any changes made locally and revert to previously saved values.

4.4.1 HTTPS Setting

This page allows you to configure the HTTPS settings and maintain the current certificate on the switch.
Mode

Indicate the HTTPS mode operation.
Possible modes are:
- **Enabled**: Enable HTTPS mode operation.
- **Disabled**: Disable HTTPS mode operation.

Automatic Redirect

Indicate the HTTPS redirect mode operation. It is only significant when "HTTPS Mode Enabled" is selected. When the redirect mode is enabled, the HTTP connection will be redirected to HTTPS connection automatically.
Notice that the browser may not allow the redirect operation due to the security consideration unless the switch certificate is trusted to the browser. You need to initialize the HTTPS connection manually for this case.
Possible modes are:
- **Enabled**: Enable HTTPS redirect mode operation.
- **Disabled**: Disable HTTPS redirect mode operation.

Certificate Maintain

The operation of certificate maintenance.
Possible operations are:
- **None**: No operation.
- **Delete**: Delete the current certificate.
- **Upload**: Upload a certificate PEM file. Possible methods are: Web Browser or URL.
- **Generate**: Generate a new self-signed RSA certificate.

Certificate Pass Phrase

Enter the pass phrase in this field if your uploading certificate is protected by a specific passphrase.
Certificate Upload

Upload a certificate PEM file into the switch. The file should contain the certificate and private key together. If you have two separated files for saving certificate and private key, Use the Linux cat command to combine them into a single PEM file. For example, cat my.cert my.key > my.pem

Notice that the RSA certificate is recommended since most of the new version of browsers has removed support for DSA in certificate, e.g. Firefox v37 and Chrome v39.

Possible methods are:
- **Web Browser:** Upload a certificate via Web browser.
- **URL:** Upload a certificate via URL, the supported protocols are HTTP, HTTPS, TFTP and FTP. URL format: <protocol>://[<username>[:<password>[@]<host>[:<port>]]/<path>/]<file_name>. For example, tftp://10.10.10.10/new_image_path/new_image.dat, http://username:password@10.10.10.80/new_image_path/new_image.dat. A valid file name is a text string drawn from alphabet (A-Z, a-z), digits (0-9), dot (.), hyphen (-), under score(_). The maximum length is 63 and hyphen must not be first character. The file name content that only contains '.' is not allowed.

Certificate Status

Display the current status of certificate on the switch.

Possible statuses are:
- The device security HTTP certificate has been submitted.
- The device security HTTP certificate has not been submitted.
- The device security HTTP certificate is generating ...

Buttons

Save: Click to save changes.
Reset: Click to undo any changes made locally and revert to previously saved values.

4.5 Access Management

4.5.1 Access Management Configuration

This option allows you to configure access management. The maximum number of entries is 16. If the type of the application matches any one of the access management entries, it allows access to the switch.
**Mode**

Indicates the access management mode operation. Possible modes are:
- Enabled: Enables access management mode operation.
- Disabled: Disables access management mode operation.

**Delete**

Check the corresponding check box to delete an entry. It will be deleted during the next Save operation.

**VLAN ID**

Indicates the VLAN ID for the access management entry.

**Start IP Address**

Indicates the start IP address for the access management entry.

**End IP Address**

Indicates the end IP address for the access management entry.

**HTTP/HTTPS**

Indicates that the host can access the switch from HTTP/HTTPS interface if the host IP address matches the IP address range provided in the entry.

**SNMP**

Indicates that the host can access the switch from SNMP interface if the host IP address matches the IP address range provided in the entry.

**TELNET/SSH**

Indicates that the host can access the switch from TELNET/SSH interface if the host IP address matches the IP address range provided in the entry.

**Buttons**

Add new entry: Click to add a new access management entry.
Save: Click to save changes.
Reset: Click to undo any changes made locally and revert to previously saved values.

4.5.2 Access Management Statistics Monitoring

This page provides statistics for access management.

<table>
<thead>
<tr>
<th>Interface</th>
<th>Received Packets</th>
<th>Allowed Packets</th>
<th>Discarded Packets</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>HTTPS</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>SSH</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Telnet</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Interface
The interface type through which the remote host can access the switch.

Received Packets
Number of received packets from the interface when access management mode is enabled.

Allowed Packets
Number of allowed packets from the interface when access management mode is enabled.

Discarded Packets
Number of discarded packets from the interface when access management mode is enabled.

Buttons
Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
Refresh: Click to refresh the page immediately.
Clear: Clear all statistics.

4.6 SNMP

4.6.1 System Configuration

This option allows you to system configure the SNMP feature.
**Mode**

Indicates the SNMP mode operation. Possible modes are:
- **Enabled**: Enables SNMP mode operation.
- **Disabled**: Disables SNMP mode operation.

**Version**

Indicates the SNMP supported version. Possible versions are:
- **SNMP v1**: Set SNMP supported version 1.
- **SNMP v2c**: Set SNMP supported version 2c.
- **SNMP v3**: Set version 3 supported by SNMP.

**Read Community**

Indicates the community read access string to permit access to SNMP agent. The allowed string length is 1 to 255, and the allowed content is the ASCII characters from 33 to 126. The field is applicable only when SNMP version is SNMPv1 or SNMPv2c. If SNMP version is SNMPv3, the community string is associated with SNMPv3 communities table. It provides more flexibility to configure security name than a SNMPv1 or SNMPv2c community string. In addition to community string, a particular range of source addresses can be used to restrict source subnet.

**Write Community**

Indicates the community write access string to permit access to SNMP agent. The allowed string length is 1 to 255, and the allowed content is the ASCII characters from 33 to 126. The field is applicable only when SNMP version is SNMPv1 or SNMPv2c. If SNMP version is SNMPv3, the community string is associated with SNMPv3 communities table. It provides more flexibility to configure security name than a SNMPv1 or SNMPv2c community string. In addition to community string, a particular range of source addresses can be used to restrict source subnet.

**Engine ID**

Indicates the SNMPv3 engine ID. The string must contain an even number (in hexadecimal format) with number of digits between 10 and 64, but all-zeros and all-‘F’s are not allowed. Change of the Engine ID will clear all original local users.
Buttons

Save: Click to save changes.
Reset: Click to undo any changes made locally and revert to previously saved values.

4.6.2 Trap Configuration

This option allows you to configure the SNMP trap feature.

Global Settings

Mode
Indicates the Trap mode operation. Possible modes are as follows:
- Enabled: Enables SNMP trap mode operation.
- Disabled: Disables SNMP trap mode operation.

Trap Destination Configurations
Configure Trap destinations on this page.

Name
Indicates the name of the Trap configuration.

Enable
Indicates the trap destination mode operation. Possible modes are as follows:
- Enabled: Enables SNMP trap mode operation.
- Disabled: Disables SNMP trap mode operation.

Version
Indicates the SNMP trap supported version. Possible versions are as follows:
- SNMPv1: Sets SNMP trap supported version 1.
- SNMPv2c: Sets SNMP trap supported version 2c.
- SNMPv3: Set SNMP trap supported version 3.
Destination Address
Indicates the SNMP trap destination address. It allows a valid IP address in dotted decimal notation ('x.y.z.w') as well as a valid hostname. A valid host name is a string extracted from alphabet (A-Z, a-z), number (09), dot (.) and dash (-). Spaces are not allowed, the first character must be an alpha character, and the first and last characters must not be a dot or a dash. Indicates the SNMP trap destination IPv6 address. A IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example, 'fe80::215:c5ff:fe03:4dc7'. The symbol is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can appear only once. It can also represent a legally valid IPv4 address. For example, '::192.1.2.34'.

Destination Port
Indicates the SNMP trap destination port. SNMP Agent sends an SNMP message via this port. The port range is 1~65535.

Buttons
Add new entry: Click to add a new user.
Save: Click to save changes.
Reset: Click to undo any changes made locally and revert to previously saved values.

4.6.2.1 SNMP Trap Configuration
Configure SNMP trap on this page.
**SNMP Trap Configuration**

- **Trap Config Name**: Indicates which trap Configuration's name for configuring. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.

- **Trap Mode**: Indicates the SNMP mode operation. Possible modes are:
  - Enabled: Enable SNMP mode operation.
  - Disabled: Disable SNMP mode operation.

- **Trap Version**: Indicates the SNMP supported version. Possible versions are:

---

**Trap Config Name**

Indicates which trap Configuration's name for configuring. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.

**Trap Mode**

Indicates the SNMP mode operation. Possible modes are:
- Enabled: Enable SNMP mode operation.
- Disabled: Disable SNMP mode operation.

**Trap Version**

Indicates the SNMP supported version. Possible versions are:
- SNMP v1: Set SNMP supported version 1.
- SNMP v2c: Set SNMP supported version 2c.
- SNMP v3: Set version 3 supported by SNMP.

**Trap Community**
Indicates the community access string when sending SNMP trap packet. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 33 to 126.

**Trap Destination Address**
Indicates the SNMP trap destination address. It allows a valid IP address in dotted decimal notation ('x.y.z.w').
And it also allows a valid hostname. A valid host name is a string extracted from alphabet (A-Z, a-z), number (09), dot (.) and dash (-). Spaces are not allowed, the first character must be an alpha character, and the first and last characters must not be a dot or a dash.
Indicates the SNMP trap destination IPv6 address. A IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example, 'fe80::215:c5ff:fe03:4dc7'. The symbol is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can appear only once. It can also represent a legally valid IPv4 address. For example, "::192.1.2.34".

**Trap Destination Port**
Indicates the SNMP trap destination port. SNMP Agent will send SNMP message via this port, the port range is 1~65535.

**Trap Inform Mode**
Indicates the SNMP trap inform mode operation. Possible modes are:
- Enabled: Enable SNMP trap inform mode operation.
- Disabled: Disable SNMP trap inform mode operation.

**Trap Inform Timeout (seconds)**
Indicates the SNMP trap inform timeout. The allowed range is 0 to 2147.

**Trap Inform Retry Times**
Indicates the SNMP trap inform retry times. The allowed range is 0 to 255.

**Trap Probe Security Engine ID**
Indicates the SNMP trap probe security engine ID mode of operation. Possible values are:
- Enabled: Enable SNMP trap probe security engine ID mode of operation.
- Disabled: Disable SNMP trap probe security engine ID mode of operation.
Trap Security Engine ID
Indicates the SNMP trap security engine ID. SNMPv3 sends traps and informs using USM for authentication and privacy. A unique engine ID for these traps and informs is needed. When "Trap Probe Security Engine ID" is enabled, the ID will be probed automatically. Otherwise, the ID specified in this field is used. The string must contain an even number (in hexadecimal format) with number of digits between 10 and 64, but all-zeros and all-'F's are not allowed.

Trap Security Name
Indicates the SNMP trap security name. SNMPv3 traps and informs using USM for authentication and privacy. A unique security name is needed when traps and informs are enabled.

SNMP Trap Event
Configure SNMP trap on this page.

System
Enable/disable that the Interface group's traps. Possible traps are:
- Warm Start: Enable/disable Warm Start trap.
- Cold Start: Enable/disable Cold Start trap.

Interface
Indicates that the Interface group's Traps. Possible traps are: Indicates that the SNMP entity is permitted to generate authentication failure traps. Possible modes are:
- Link Up: Enable/disable Link up trap.
- Link Down: Enable/disable Link down trap.
- LLDP: Enable/disable LLDP trap.

Authentication
Indicates that the authentication group's Traps. Possible traps are:
- SNMP authentication failure: Enable/disable SNMP trap authentication failure trap.

Switch
Indicates that the Switch group's traps. Possible traps are:
- STP: Enable/disable STP trap.
- RMON: Enable/disable RMON trap.
4.6.3 Community Configuration

This option allows you to configure SNMPv3 community table. The entry index key is Community.

Delete
Check the corresponding check box to delete an entry. It will be deleted during the next Save operation.

Community
Indicates the community access string to permit access to SNMPv3 agent. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126. The community string will be treated as security name and map a SNMPv1 or SNMPv2c community string.

Source IP
Indicates the SNMP access source address. A particular range of source addresses can be used to restrict source subnet when combined with source mask.

Source Mask
Indicates the SNMP access source address mask.

Buttons
Add new community entry: Click to add a new community entry.
Save: Click to save changes.
Reset: Click to undo any changes made locally and revert to previously saved values.

4.6.4 User Configuration

This option allows you to configure SNMPv3 user table. The entry index keys are Engine ID and User Name.
Delete

Check the corresponding check box to delete an entry. It will be deleted during the next Save operation.

Engine ID

An octet string identifying the engine ID that this entry should belong to. The string must contain an even number (in hexadecimal format) with number of digits between 10 and 64, but all-zeros and all-‘F’s are not allowed. The SNMPv3 architecture uses the User-based Security Model (USM) for message security and the View-based Access Control Model (VACM) for access control. For the USM entry, the usmUserEngineID and usmUserName are the entry's keys. In a simple agent, usmUserEngineID is always that agent's own snmpEngineID value. The value can also take the value of the snmpEngineID of a remote SNMP engine with which this user can communicate. In other words, if user engine ID equal system engine ID then it is a local user; otherwise it is a remote user.

Username

A string identifying the user name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.

Security Level

Indicates the security model that this entry should belong to. Possible security models are:

- NoAuth, NoPriv: No authentication and no encryption.
- Auth, NoPriv: Authentication and no encryption.
- Auth, Priv: Authentication and encryption.

The value of security level cannot be modified if entry already exists. That means must first ensure that the value is set correctly.

Authentication Protocol

Indicates the authentication protocol that this entry should belong to. Possible modes are:

- None: No authentication protocol.
- MD5: An optional flag to indicate that this user uses MD5 authentication protocol.
- SHA: An optional flag to indicate that this user uses SHA authentication protocol.

The value of security level cannot be modified if entry already exists. That means must first ensure that the value is set correctly.
Authentication Password
A string identifying the authentication password phrase. For MD5 authentication protocol, the allowed string length is 8 to 32. For SHA authentication protocol, the allowed string length is 8 to 40. The allowed content is ASCII characters from 33 to 126.

Privacy Protocol
Indicates the privacy protocol that this entry should belong to. Possible privacy protocols are:
- None: No privacy protocol.
- DES: An optional flag to indicate that this user uses DES authentication protocol.
- AES: An optional flag to indicate that this user uses AES authentication protocol.

Privacy Password
A string identifying the privacy password phrase. The allowed string length is 8 to 32, and the allowed content is ASCII characters from 33 to 126.

Buttons
Add New Entry: Click to add new entry.
Save: Click to save changes.
Reset: Click to undo any changes made locally and revert to previously saved values.

4.6.5 Group Configuration
This option allows you to configure the SNMPv3 group table. The entry index keys are Security Model and Security Name.

Delete
Check the corresponding check box to delete an entry. It will be deleted during the next Save operation.
Security Model
Indicates the security model that this entry should belong to. Possible security models are as follows:
- v1: Reserved for SNMPv1.
- v2c: Reserved for SNMPv2c.

Security Name
A string identifying the security name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.

Group Name
A string identifying the group name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.

Buttons
Add new group entry: Click to add a new community entry.
Save: Click to save changes.
Reset: Click to undo any changes made locally and revert to previously saved values.

4.6.6 View Configuration
Configure SNMPv3 view table on this page. The entry index keys are View Name and OID Subtree.

Delete
Check to delete the entry. It will be deleted during the next save.

View Name
A string identifying the view name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.

View Type
Indicates the view type that this entry should belong to. Possible view types are:
- included: An optional flag to indicate that this view subtree should be included.
- excluded: An optional flag to indicate that this view subtree should be excluded.
In general, if a view entry's view type is 'excluded', there should be another view entry existing with view type as 'included' and it's OID subtree should overstep the 'excluded' view entry.

**OID Subtree**

The OID defining the root of the subtree to add to the named view. The allowed OID length is 1 to 128. The allowed string content is digital number or asterisk (*).

**Buttons**

Add new view entry: click to add a new view entry.
Save: Click to save changes.
Reset: Click to undo any changes made locally and revert to previously saved values.

### 4.6.7 Access Configuration

Configure SNMPv3 access table on this page. The entry index keys are Group Name, Security Model and Security Level.

<table>
<thead>
<tr>
<th>Security Model</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>any</td>
<td>v1,v2c,usm</td>
</tr>
<tr>
<td>v1</td>
<td>Reserved for SNMPv1.</td>
</tr>
<tr>
<td>v2c</td>
<td>Reserved for SNMPv2c.</td>
</tr>
<tr>
<td>usm</td>
<td>User-based Security Model (USM).</td>
</tr>
</tbody>
</table>

**Group Name**

A string identifying the group name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.
Security Level

Indicates the security model that this entry should belong to. Possible security models are:
- NoAuth, NoPriv: No authentication and no encryption.
- Auth, NoPriv: Authentication and no encryption.
- Auth, Priv: Authentication and encryption.

Read View Name

The name of the MIB view defining the MIB objects for which this request may request the current values. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.

Write View Name

The name of the MIB view defining the MIB objects for which this request may potentially set new values. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.

Buttons

Add new access entry: click to add a new access entry.
Save: Click to save changes.
Reset: Click to undo any changes made locally and revert to previously saved values.

4.7 RMON

4.7.1 Statistics Configuration

Configure RMON Statistics table on this page. The entry index key is ID.

Delete

Check to delete the entry. It will be deleted during the next save.

ID

Indicates the index of the entry. The range is from 1 to 65535.
**Data Source**

Indicates the port ID which wants to be monitored. If in stacking switch, the value must add 1000000*(switch ID-1), for example, if the port is switch 3 port 5, the value is 2000005.

**Buttons**

Add new entry: Click to add a new community entry.
Save: Click to save changes.
Reset: Click to undo any changes made locally and revert to previously saved values.

**4.7.2 History Configuration**

Configure RMON History table on this page. The entry index key is ID.

**Delete**

Check to delete the entry. It will be deleted during the next save.

**ID**

Indicates the index of the entry. The range is from 1 to 65535.

**Data Source**

Indicates the port ID which wants to be monitored. If in stacking switch, the value must add 1000000*(switch ID-1), for example, if the port is switch 3 port 5, the value is 2000005.

**Interval**

Indicates the interval in seconds for sampling the history statistics data. The range is from 1 to 3600, default value is 1800 seconds.

**Buckets**

Indicates the maximum data entries associated this History control entry stored in RMON. The range is from 1 to 3600, default value is 50.

**Buckets Granted**

The number of data shall be saved in the RMON.
Buttons

Add new entry: Click to add a new community entry.
Save: Click to save changes.
Reset: Click to undo any changes made locally and revert to previously saved values.

4.7.3 Alarm Configuration

Configure RMON alarm table on this page. The entry index key is ID.

Delete

Check to delete the entry. It will be deleted during the next save.

ID

Indicates the index of the entry. The range is from 1 to 65535.

Interval

Indicates the interval in seconds for sampling and comparing the rising and falling threshold. The range is from 1 to $2^{31}-1$.

Variable

Indicates the particular variable to be sampled, the possible variables are:

- **InOctets**: The total number of octets received on the interface, including framing characters.
- **InUcastPkts**: The number of unicast packets delivered to a higher-layer protocol.
- **InNUcastPkts**: The number of broadcast and multi-cast packets delivered to a higher-layer protocol.
- **InDiscards**: The number of inbound packets that are discarded even if the packets are normal.
- **InErrors**: The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
- **InUnknownProtos**: the number of the inbound packets that were discarded because of the unknown or un-support protocol.
- **OutOctets**: The number of octets transmitted out of the interface, including framing characters.
- **OutUcastPkts**: The number of uni-cast packets that request to transmit.
- **OutNUcastPkts**: The number of broadcast and multi-cast packets that request
to transmit.

- OutDiscards: The number of outbound packets that are discarded event the packets is normal.
- OutErrors: The number of outbound packets that could not be transmitted because of errors.
- OutQLen: The length of the output packet queue (in packets).

Sample Type

The method of sampling the selected variable and calculating the value to be compared against the thresholds, possible sample types are:

- Absolute: Get the sample directly.
- Delta: Calculate the difference between samples (default).

Value

The value of the statistic during the last sampling period.

Startup Alarm

The method of sampling the selected variable and calculating the value to be compared against the thresholds, possible sample types are:

- RisingTrigger alarm when the first value is larger than the rising threshold.
- FallingTrigger alarm when the first value is less than the falling threshold.
- RisingOrFallingTrigger alarm when the first value is larger than the rising threshold or less than the falling threshold (default).

Rising Threshold

Rising threshold value (-2147483648-2147483647).

Rising Index

Rising event index (1-65535).

Falling Threshold

Falling threshold value (-2147483648-2147483647).

Falling Index

Falling event index (1-65535).

Buttons

Add new entry: Click to add a new community entry.

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.
4.7.4 Link Event Configuration

Configure RMON Event table on this page. The entry index key is ID.

Delete

Check to delete the entry. It will be deleted during the next save.

ID

Indicates the index of the entry. The range is from 1 to 65535.

Description

Indicates this event, the string length is from 0 to 127, default is a null string.

Type

Indicates the notification of the event, the possible types are:
- none: No operations.
- Log: When an event is triggered, create SNMP log entries.
- snmptrap: send SNMP trap when an event is triggered.
- Logandtrap: Create SNMP log entry and send SNMP trap when an event is triggered.

Community

Specify the community when trap is sent, the string length is from 0 to 127, default is "public".

Event Last Time

Indicates the value of sysUpTime at the time this event entry last generated an event.

Buttons

Add new entry: Click to add a new community entry.
Save: Click to save changes.
Reset: Click to undo any changes made locally and revert to previously saved values.

4.7.5 Statistics Monitoring

This page provides an overview of RMON Statistics entries. Each page shows up to 99 entries from the Alarm table, default being 20, selected through the "entries per
page" input field. When first visited, the WEB page will show the first 20 entries from the beginning of the Statistics table. The first displayed will be the one with the lowest ID found in the Statistics table.

The “Start from Control Index” allows the user to select the starting point in the Alarm table. Clicking the “Refresh” button will update the displayed table starting from that or the next closest Statistics table match.

This “>>” button will use the last entry of the currently displayed entry as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the “|<<” button to start over.

The displayed counters are:

<table>
<thead>
<tr>
<th>ID</th>
<th>Data Source(ifIndex)</th>
<th>Drop</th>
<th>Octets</th>
<th>Packets</th>
<th>Broadcast</th>
<th>Multicast</th>
</tr>
</thead>
<tbody>
<tr>
<td>Indication the index of Statistics entry.</td>
<td>The port ID which wants to be monitored.</td>
<td>The total number of events in which packets were dropped by the probe due to lack of resources.</td>
<td>The total number of octets of data (including those in bad packets) received on the network.</td>
<td>The total number of packets (including bad packets, broadcast packets, and multicast packets) received.</td>
<td>The total number of good packets received that were directed to the broadcast address.</td>
<td>The total number of good packets received that were directed to a multicast address.</td>
</tr>
</tbody>
</table>
**CRC Errors**

Total number of packets received. Eight-bit byte with length (excluding the frame part, but including FCS octets) between 64 and 1518, but there is an integer (FCS error) bad frame check sequence (FCS) of eight-bit byte or a bad FCS eight-bit byte which is not an integer (alignment error).

**Under-size**

The total number of packets received that were less than 64 octets.

**Over-size**

The total number of packets received that were longer than 1518 octets.

**Frag**

The number of frames which size is less than 64 octets received with invalid CRC.

**Jabb**

The number of frames which size is larger than 64 octets received with invalid CRC.

**Coll**

The best estimate of the total number of collisions on this Ethernet segment.

**Bytes**

The total number of packets (including bad packets) received that were 64 octets in length.

**65~127**

The total number of packets (including bad packets) received that were between 65 to 127 octets in length.

**128~255**

The total number of packets (including bad packets) received that were between 128 to 255 octets in length.

**256~511**

The total number of packets (including bad packets) received that were between 256 to 511 octets in length.

**512~1023**

The total number of packets (including bad packets) received that were between 512 to 1023 octets in length.

**1024~1588**

The total number of packets (including bad packets) received that were between 1024 to 1588 octets in length.
Buttons

Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page immediately.

|<<: Updates the table starting from the first entry in the Statistics table, i.e. the entry with the lowest ID.

>>: Updates the table, starting with the entry after the last entry currently displayed.

4.7.6 History Monitoring

This page provides an overview of RMON History entries. Each page shows up to 99 entries from the History table, default being 20, selected through the "entries per page" input field. When first visited, the WEB page will show the first 20 entries from the beginning of the History table. The first displayed will be the one with the lowest History Index and Sample Index found in the History table.

"Start from Control Index" allows the user to select a starting point in the history table. Clicking the "Refresh" button will update the displayed table starting from that or the next closest History table match.

This “>>” button will use the last entry of the currently displayed entry as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the "|<<" button to start over.

The displayed fields are:

Interval

Indicates the interval in seconds for sampling and comparing the rising and falling threshold.

Variable

Indicates the particular variable to be sampled

Sample Type

The method of sampling the selected variable and calculating the value to be compared against the thresholds.
Drop
The total number of events in which packets were dropped by the probe due to lack of resources.

Octets
The total number of octets of data (including those in bad packets) received on the network.

Packets
The total number of packets (including bad packets, broadcast packets, and multicast packets) received.

Broadcast
The total number of good packets received that were directed to the broadcast address.

Multicast
The total number of good packets received that were directed to a multicast address.

CRC Errors
Total number of packets received. Eight-bit byte with length (excluding the frame part, but including FCS octets) between 64 and 1518, but there is an integer (FCS error) bad frame check sequence (FCS) of eight-bit byte or a bad FCS eight-bit byte which is not an integer (alignment error).

Under-size
The total number of packets received that were less than 64 octets.

Over-size
The total number of packets received that were longer than 1518 octets.

Frag
The number of frames which size is less than 64 octets received with invalid CRC.

Jabb
The number of frames which size is larger than 64 octets received with invalid CRC.

Coll
The best estimate of the total number of collisions on this Ethernet segment.

Utilization
The best estimate of the mean physical layer network utilization on this interface during this sampling interval, in hundredths of a percent.
Buttons

Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
Refresh: Click to refresh the page immediately.
|<<: Updates the table starting from the first entry in the Statistics table, i.e. the entry with the lowest ID.
>>: Updates the table, starting with the entry after the last entry currently displayed.

4.7.7 Alarm Monitoring

This page provides an overview of RMON Statistics entries. Each page shows up to 99 entries from the Statistics table, default being 20, selected through the “entries per page” input field. When first visited, the WEB page will show the first 20 entries from the beginning of the Statistics table. The first displayed will be the one with the lowest ID found in the Statistics table.

The “Start from Control Index” allows the user to select the starting point in the Alarm table. Clicking the “Refresh” button will update the displayed table starting from that or the next closest Statistics table match.

This “>>” button will use the last entry of the currently displayed entry as a basis for the next lookup. When the end is reached the text “No more entries” is shown in the displayed table. Use the “|<<” button to start over.

The displayed fields are:

<table>
<thead>
<tr>
<th>ID</th>
<th>Interval</th>
<th>Variable</th>
</tr>
</thead>
</table>

ID

Indicates the index of Alarm control entry.

Interval

Indicates the interval in seconds for sampling and comparing the rising and falling threshold.

Variable

Indicates the particular variable to be sampled
Sample Type
The method of sampling the selected variable and calculating the value to be compared against the thresholds.

Value
The value of the statistic during the last sampling period.

Startup Alarm
The alarm that may be sent when this entry is first set to valid.

Rising Threshold
Rising threshold value.

Rising Index
Rising event index.

Falling Threshold
Falling threshold value.

Falling Index
Falling event index.

Buttons
Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
Refresh: Click to refresh the page immediately.
|<<: Updates the table starting from the first entry in the Statistics table, i.e. the entry with the lowest ID.
>>: Updates the table, starting with the entry after the last entry currently displayed.

4.7.8 Event Monitoring
This page provides an overview of RMON event entries. Each page shows up to 99 entries from the event table, default being 20, selected through the "entries per page" input field. When first visited, the WEB page will show the first 20 entries from the beginning of the Event table. The first displayed will be the one with the lowest Event Index and Log Index found in the Event table. The "Start from Control Index and Sample Index" input field allows the user to select a starting point in the Event table. Clicking the "Refresh" button will update the displayed table starting from that or the next closest Event table match.
This “>>” button will use the last entry of the currently displayed entry as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the “|<|” button to start over.

The displayed fields are:

**Event Index**
- Indicates the index of the event entry.

**Log Index**
- Indicates the index of the log entry.

**Log Time**
- Indicates Event log time

**Log Description**
- Indicates the Event description.

**Buttons**
- Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
- Refresh: Click to refresh the page immediately.
- |<<: Updates the table starting from the first entry in the Event Table, i.e. the entry with the lowest Event Index and Log Index.
- >>: Updates the table, starting with the entry after the last entry currently displayed.
5.1 Port Limit Control

This page allows you to configure the Port Security Limit Control system and port settings.
Limit Control allows for limiting the number of users on a specified port. A user is identified by a MAC address and VLAN ID. If Limit Control is enabled on a port, the limit specifies the maximum number of users on the port. If this number is exceeded, an action is taken. The action can be one of the four different actions as described below.
The Limit Control module utilizes a lower-layer module, Port Security module, which manages MAC addresses learnt on the port.
The Limit Control configuration consists of two sections, a system- and a port-wide.
System Configuration

Mode
Indicates if Limit Control is globally enabled or disabled on the switch. If globally disabled, other modules may still use the underlying functionality, but limit checks and corresponding actions are disabled.

Aging Enabled
If checked, secured MAC addresses are subject to aging as discussed under Aging Period.
Aging Period

If Aging Enabled is checked, then the aging period is controlled with this input. If other modules are using the underlying port security for securing MAC addresses, they may have other requirements to the aging period. The underlying port security will use the shorter requested aging period of all modules that use the functionality. The Aging Period can be set to a number between 10 and 10,000,000 seconds.

To understand why aging may be desired, consider the following scenario: Suppose an end-host is connected to a 3rd party switch or hub, which in turn is connected to a port on this switch on which Limit Control is enabled. The end-host will be allowed to forward if the limit is not exceeded. Now suppose that the end-host logs off or powers down. If it wasn't for aging, the end-host would still take up resources on this switch and will be allowed to forward. To overcome this situation, enable aging. With aging enabled, a timer is started once the end-host gets secured. When the timer expires, the switch starts looking for frames from the end-host, and if such frames are not seen within the next Aging Period, the end-host is assumed to be disconnected, and the corresponding resources are freed on the switch.

Port Configuration

The table has one row for each port on the switch and a number of columns, which are:

Port
The port number for which the configuration below applies.

Mode
Controls whether Limit Control is enabled on this port. Both this and the Global Mode must be set to Enabled for Limit Control to be in effect. Notice that other modules may still use the underlying port security features without enabling Limit Control on a given port.

Limit
The maximum number of MAC addresses that can be secured on this port. This number cannot exceed 1024. If the limit is exceeded, the corresponding action is taken.

The switch is "born" with a total number of MAC addresses from which all ports draw whenever a new MAC address is seen on a Port Security-enabled port. Since all ports draw from the same pool, it may happen that a configured maximum cannot be granted, if the remaining ports have already used all available MAC addresses.
Action

If Limit is reached, the switch can take one of the following actions:

- None: Do not allow more than Limit MAC addresses on the port, but take no further action.
- Trap: If Limit +1 MAC addresses is seen on the port, send an SNMP trap. If Aging is disabled, only one SNMP trap will be sent, but with Aging enabled, new SNMP traps will be sent every time the limit gets exceeded.
- Shutdown: If Limit +1 MAC addresses is seen on the port, shut down the port. This implies that all secured MAC addresses will be removed from the port, and no new address will be learned. Even if the link is physically disconnected and reconnected on the port (by disconnecting the cable), the port will remain shut down. There are three ways to re-open the port:
  1) Boot the switch,
  2) Disable and re-enable Limit Control on the port or the switch,
  3) Click the Reopen button.
- Trap & Shutdown: If Limit + 1 MAC addresses is seen on the port, both the "Trap" and the "Shutdown" actions described above will be taken.

State

This column shows the current state of the port as seen from the Limit Control's point of view. The state takes one of four values:

- Disabled: Limit Control is either globally disabled or disabled on the port.
- Ready: The limit is not yet reached. This can be shown for all actions.
- Limit Reached: Indicates that the limit is reached on this port. This state can only be shown if Action is set to None or Trap.
- Shutdown: Indicates that the port is shut down by the Limit Control module. This state can only be shown if Action is set to Shutdown or Trap & Shutdown.

Re-open Button

If a port is shut down by this module, you may reopen it by clicking this button, which will only be enabled if this is the case.

Note that clicking the "Reopen" button will refresh the page, so uncommitted changes will be lost.

Buttons

Save: Click to save changes.
Reset: Click to undo any changes made locally and revert to previously saved values.
5.2 Port Security

5.2.1 Switch Monitoring

This page shows the Port Security status. Port Security is a module with no direct configuration. Configuration comes indirectly from other modules - the user modules. When a user module has enabled port security on a port, the port is set up for software-based learning. In this mode, frames from unknown MAC addresses are passed on to the port security module, which in turn asks all user modules whether to allow this new MAC address to forward or block it. For a MAC address to be set in the forwarding state, all enabled user modules must unanimously agree on allowing the MAC address to forward. If only one chooses to block it, it will be blocked until that user module decides otherwise.

The status page is divided into two sections - one with a legend of user modules and one with the actual port status.

<table>
<thead>
<tr>
<th>Port Security Switch Status</th>
<th>Switch Monitor</th>
<th>Port Monitor</th>
<th>Auto-refresh</th>
<th>Refresh</th>
</tr>
</thead>
</table>

### User Module

<table>
<thead>
<tr>
<th>User Module Name</th>
<th>Abbr</th>
</tr>
</thead>
<tbody>
<tr>
<td>Limit Control</td>
<td>L</td>
</tr>
<tr>
<td>802.1X</td>
<td>8</td>
</tr>
</tbody>
</table>

### Port Status

<table>
<thead>
<tr>
<th>Port</th>
<th>Users</th>
<th>State</th>
<th>MAC Count</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>Current</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Limit</td>
</tr>
<tr>
<td>1</td>
<td>—</td>
<td>Disabled</td>
<td>—</td>
</tr>
<tr>
<td>2</td>
<td>—</td>
<td>Disabled</td>
<td>—</td>
</tr>
<tr>
<td>3</td>
<td>—</td>
<td>Disabled</td>
<td>—</td>
</tr>
<tr>
<td>4</td>
<td>—</td>
<td>Disabled</td>
<td>—</td>
</tr>
<tr>
<td>5</td>
<td>—</td>
<td>Disabled</td>
<td>—</td>
</tr>
<tr>
<td>6</td>
<td>—</td>
<td>Disabled</td>
<td>—</td>
</tr>
<tr>
<td>7</td>
<td>—</td>
<td>Disabled</td>
<td>—</td>
</tr>
<tr>
<td>8</td>
<td>—</td>
<td>Disabled</td>
<td>—</td>
</tr>
<tr>
<td>9</td>
<td>—</td>
<td>Disabled</td>
<td>—</td>
</tr>
<tr>
<td>10</td>
<td>—</td>
<td>Disabled</td>
<td>—</td>
</tr>
<tr>
<td>11</td>
<td>—</td>
<td>Disabled</td>
<td>—</td>
</tr>
<tr>
<td>12</td>
<td>—</td>
<td>Disabled</td>
<td>—</td>
</tr>
</tbody>
</table>
User Module Legend
The legend shows all user modules that may request Port Security services.

User Module Name
The full name of a module that may request Port Security services.

Abbr
A one-letter abbreviation of the user module. Used in the user column of the port status table.

Port Status
The table has one row for each port on the switch and a number of columns, which are:

Port
The port number for which the status applies. Click the port number to see the status for this particular port.

Users
Each of the user modules has a column that shows whether that module has enabled Port Security or not. '-' means that the corresponding user module is not enabled, whereas a letter indicates that the user module abbreviated by that letter (see Abbr) has enabled port security.

State
Shows the current state of the port. It can take one of four values:

- Disabled: No user modules are currently using the Port Security service.
- Ready: The Port Security service is in use by at least one user module, and is awaiting frames from unknown MAC addresses to arrive.
- Limit Reached: The Port Security service is enabled by at least the Limit Control user module, and that module has indicated that the limit is reached and no more MAC addresses should be taken in.
- Shutdown: The Port Security service is enabled by at least the Limit Control user module, and that module has indicated that the limit is exceeded. No MAC addresses can be learned on the port until it is administratively re-opened on the Limit Control configuration Web-page.

MAC Count (Current, Limit)
The two columns indicate the number of currently learned MAC addresses (forwarding as well as blocked) and the maximum number of MAC addresses that can be learned on the port, respectively.

If no user modules are enabled on the port, the Current column will show a dash (-).
If the restriction control user module is not enabled on the port, the restriction column will display a dash (-).

**Buttons**

- **Auto-refresh**: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
- **Refresh**: Click to refresh the page immediately.

### 5.2.2 Port Monitoring

This page shows the MAC addresses secured by the Port Security module. Port Security is a module with no direct configuration. Configuration comes indirectly from other modules - the user modules. When a user module has enabled port security on a port, the port is set-up for software-based learning. In this mode, frames from unknown MAC addresses are passed on to the port security module, which in turn asks all user modules whether to allow this new MAC address to forward or block it. For a MAC address to be set in the forwarding state, all enabled user modules must unanimously agree on allowing the MAC address to forward. If only one chooses to block it, it will be blocked until that user module decides otherwise.

<table>
<thead>
<tr>
<th>MAC Address</th>
<th>VLAN ID</th>
<th>State</th>
<th>Time of Addition</th>
<th>Age/Hold</th>
</tr>
</thead>
</table>

**MAC Address & VLAN ID**

The MAC address and VLAN ID that is seen on this port. If no MAC addresses are learned, a single row stating "No MAC addresses attached" is displayed.

**State**

Indicates whether the corresponding MAC address is blocked or forwarding. In the blocked state, it will not be allowed to transmit or receive traffic.

**Time of Addition**

Shows the date and time when this MAC address was first seen on the port.

**Age/Hold**

If at least one user module has decided to block this MAC address, it will stay in the blocked state until the hold time (measured in seconds) expires. If all user modules have decided to allow this MAC address to forward, and aging is enabled, the Port Security module will periodically check that this MAC address still forwards traffic.
the age period (measured in seconds) expires and no frames have been seen, the MAC address will be removed from the MAC table. Otherwise a new age period will begin.
If aging is disabled or a user module has decided to hold the MAC address indefinitely, a dash (-) will be shown.

**Buttons**

Use the port select box to select which port to show status for.
Auto-refresh: Check this box to enable an automatic refresh. Automatic refresh occurs every 3 seconds.
Refresh: Click to refresh the page immediately.

### 5.3 NAS

#### 5.3.1 NAS Configuration

This page allows you to configure the IEEE 802.1X and MAC-based authentication system and port settings.

The IEEE 802.1X standard defines a port-based access control procedure that prevents unauthorized access to a network by requiring users to first submit credentials for authentication. One or more central servers, the backend servers, determine whether the user is allowed access to the network. These backend (RADIUS) servers are configured on the "Security Network" page. The IEEE802.1X standard defines port-based operation, but non-standard variants overcome security limitations as shall be explored below.

MAC-based authentication allows for authentication of more than one user on the same port, and doesn't require the user to have special 802.1X supplicant software installed on his system. The switch uses the user's MAC address to authenticate against the backend server. Intruders can create counterfeit MAC addresses, which makes MAC-based authentication less secure than 802.1X authentication.

The NAS configuration consists of two sections, a system- and a port-wide.
System Configuration

Mode

Indicates if NAS is globally enabled or disabled on the switch. If globally disabled, all ports are allowed forwarding of frames.

Reauthentication Enabled

If checked, successfully authenticated supplicants/clients are reauthenticated after the interval specified by the Reauthentication Period. Reauthentication for 802.1X-enabled ports can be used to detect if a new device is plugged into a switch port or if a supplicant is no longer attached.

For MAC-based ports, reauthentication is only useful if the RADIUS server configuration has changed. It does not involve communication between the switch and the client, and therefore doesn’t imply that a client is still present on a port (see Aging Period below).
**Reauthentication Period**

Determines the period, in seconds, after which a connected client must be reauthenticated. This is only active if the Reauthentication Enabled checkbox is checked. Valid values are in the range 1 to 3600 seconds.

**EAPOL Timeout**

Determines the time for retransmission of Request Identity EAPOL frames. Valid values are in the range 1 to 65535 seconds. This has no effect for MAC-based ports.

**Aging Period**

This setting applies to the following modes, i.e. modes using the Port Security functionality to secure MAC addresses:
- Single 802.1X
- Multi 802.1X
- MAC-Based Auth.

When the NAS module uses the Port Security module to secure MAC addresses, the Port Security module needs to check for activity on the MAC address in question at regular intervals and free resources if no activity is seen within a given period of time. This parameter controls exactly this period and can be set to a number between 10 and 1000000 seconds.

If reauthentication is enabled and the port is in an 802.1X-based mode, this is not so critical, since supplicants that are no longer attached to the port will get removed upon the next reauthentication, which will fail. But if reauthentication is not enabled, the only way to free resources is by aging the entries.

For ports in MAC-based Auth. mode, reauthentication doesn't cause direct communication between the switch and the client, so this will not detect whether the client is still attached or not, and the only way to free any resources is to age the entry.

**Hold Time**

This setting applies to the following modes, i.e. modes using the Port Security functionality to secure MAC addresses:
- Single 802.1X
- Multi 802.1X
- MAC-Based Auth.

If a client is denied access - either because the RADIUS server denies the client access or because the RADIUS server request times out - the client is put on hold in the Unauthorized state. The hold timer does not count during an on-going authentication.
In MAC-based Auth. mode, the switch will ignore new frames coming from the client during the hold time.
The Hold Time can be set to a number between 10 and 1000000 seconds.

**RADIUS-Assigned QoS Enabled**

RADIUS-assigned QoS provides a means to centrally control the traffic class to which traffic coming from a successfully authenticated supplicant is assigned on the switch. The RADIUS server must be configured to transmit special RADIUS attributes to take advantage of this feature (see RADIUS-Assigned QoS Enabled below for a detailed description).

The “RADIUS-Assigned QoS Enabled” checkbox provides a quick way to globally enable/disable RADIUS-server assigned QoS Class functionality. When checked, the individual ports' ditto setting determine whether RADIUS-assigned QoS Class is enabled on that port. When unchecked, RADIUS-server assigned QoS Class is disabled on all ports.

**RADIUS-Assigned VLAN Enabled**

RADIUS-assigned VLAN provides a means to centrally control the VLAN on which a successfully authenticated supplicant is placed on the switch. Incoming traffic will be classified to and switched on the RADIUS-assigned VLAN. The RADIUS server must be configured to transmit special RADIUS attributes to take advantage of this feature (see RADIUS-Assigned VLAN Enabled below for a detailed description).

The “RADIUS-Assigned VLAN Enabled” checkbox provides a quick way to globally enable/disable RADIUS-server assigned VLAN functionality. When checked, the individual ports' ditto setting determine whether RADIUS-assigned VLAN is enabled on that port. When unchecked, RADIUS-server assigned VLAN is disabled on all ports.

**Guest VLAN Enabled**

A Guest VLAN is a special VLAN - typically with limited network access - on which 802.1X-unaware clients are placed after a network administrator-defined timeout.

The switch follows a set of rules for entering and leaving the Guest VLAN as listed below.

The “Guest VLAN Enabled” checkbox provides a quick way to globally enable/disable Guest VLAN functionality. When checked, the individual ports' ditto setting determines whether the port can be moved into Guest VLAN. When unchecked, the ability to move to the Guest VLAN is disabled on all ports.
Guest VLAN ID
This is the value that a port's Port VLAN ID is set to if a port is moved into the Guest VLAN. It is only changeable if the Guest VLAN option is globally enabled.
Valid values are in the range \([1; 4095]\).

Max. Reauth. Count
The number of times the switch transmits an EAPOL Request Identity frame without response before considering entering the Guest VLAN is adjusted with this setting. The value can only be changed if the Guest VLAN option is globally enabled.
Valid values are in the range \([1; 255]\).

Allow Guest VLAN if EAPOL Seen
The switch remembers if an EAPOL frame has been received on the port for the lifetime of the port. Once the switch considers whether to enter the Guest VLAN, it will first check if this option is enabled or disabled. If disabled (unchecked; default), the switch will only enter the Guest VLAN if an EAPOL frame has not been received on the port for the lifetime of the port. If enabled (checked), the switch will consider entering the Guest VLAN even if an EAPOL frame has been received on the port for the lifetime of the port.
The value can only be changed if the Guest VLAN option is globally enabled.

Port Configuration
The table has one row for each port on the switch and a number of columns, which are:

Port
The port number for which the configuration below applies.

Admin State
If NAS is globally enabled, this selection controls the port's authentication mode. The following modes are available:
- Force Authorized
  In this mode, the switch will send one EAPOL Success frame when the port link comes up, and any client on the port will be allowed network access without authentication.
- Force Unauthorized
  In this mode, the switch will send one EAPOL Failure frame when the port link comes up, and any client on the port will be disallowed network access.
- Port-based 802.1X
  In the 802.1X-world, the user is called the supplicant, the switch is the authenticator, and the RADIUS server is the authentication server. The
authenticator acts as the man-in-the-middle, forwarding requests and responses between the supplicant and the authentication server. Frames sent between the supplicant and the switch are special 802.1X frames, known as EAPOL (EAP Over LANs) frames. EAPOL frames encapsulate EAP PDUs (RFC3748). Frames sent between the switch and the RADIUS server are RADIUS packets. RADIUS packets also encapsulate EAP PDUs together with other attributes like the switch's IP address, name, and the supplicant's port number on the switch. EAP is very flexible, in that it allows for different authentication methods, like MD5-Challenge, PEAP, and TLS. The important thing is that the authenticator (the switch) doesn't need to know which authentication method the supplicant and the authentication server are using, or how many information exchange frames are needed for a particular method. The switch simply encapsulates the EAP part of the frame into the relevant type (EAPOL or RADIUS) and forwards it. When authentication is complete, the RADIUS server sends a special packet containing a success or failure indication. Besides forwarding this decision to the supplicant, the switch uses it to open up or block traffic on the switch port connected to the supplicant.

Note:
Suppose two backend servers are enabled and that the server timeout is configured to X seconds (using the AAA configuration page), and suppose that the first server in the list is currently down (but not considered dead). Now, if the supplicant retransmits EAPOL Start frames at a rate faster than X seconds, then it will never get authenticated, because the switch will cancel on-going backend authentication server requests whenever it receives a new EAPOL Start frame from the supplicant. And since the server hasn't yet failed (because the X seconds haven't expired), the same server will be contacted upon the next backend authentication server request from the switch. This scenario will loop forever. Therefore, the server timeout should be smaller than the supplicant's EAPOL Start frame retransmission rate.

• MAC-based Auth.

Unlike port-based 802.1X, MAC-based authentication is not a standard, but merely a best-practices method adopted by the industry. In MAC-based authentication, users are called clients, and the switch acts as the supplicant on behalf of clients. The initial frame (any kind of frame) sent by a client is snooped by the switch, which in turn uses the client's MAC address as both username and password in the subsequent EAP exchange with the RADIUS server. The 6-byte MAC address is converted to a string on the following form "xx-xx-xx-xx-xx-xx", that is, a dash (-) is used as separator between the lower-cased hexadecimal digits. The switch only supports the MD5-Challenge authentication method, so the RADIUS server must be configured accordingly. When authentication is complete, the RADIUS server sends a success or failure indication, which in turn causes the switch to open up or block traffic for that
particular client, using the Port Security module. Only then will frames from the client be forwarded on the switch. There are no EAPOL frames involved in this authentication, and therefore, MAC-based Authentication has nothing to do with the 802.1X standard.

The advantage of MAC-based authentication over 802.1X-based authentication is that the clients don’t need special supplicant software to authenticate. The disadvantage is that MAC addresses can be spoofed by malicious users - equipment whose MAC address is a valid RADIUS user can be used by anyone. Also, only the MD5-Challenge method is supported. The maximum number of clients that can be attached to a port can be limited using the Port Security Limit Control functionality.

**Port Status**

The current state of the port. It can undertake one of the following values:

- Globally Disabled: NAS is globally disabled.
- Link Down: NAS is globally enabled, but there is no link on the port.
- Authorized: The port is in Force Authorized or a single-suppliant mode and the supplicant is authorized.
- Unauthorized: The port is in Force Unauthorized or a single-suppliant mode and the supplicant is not successfully authorized by the RADIUS server.
- X Auth/Y Unauth: The port is in a multi-suppliant mode. Currently X clients are authorized and Y are unauthorized.

**Restart**

Two buttons are available for each row. The buttons are only enabled when authentication is globally enabled and the port's Admin State is in an EAPOL-based or MAC-based mode.

Clicking these buttons will not cause settings changed on the page to take effect.

- Reauthenticate: Schedules a reauthentication whenever the quiet-period of the port runs out (EAPOL-based authentication). For MAC-based authentication, reauthentication will be attempted immediately.
  The button only has effect for successfully authenticated clients on the port and will not cause the clients to get temporarily unauthorized.
- Reinitialize: Forces a reinitialization of the clients on the port and thereby a reauthentication immediately. The clients will transfer to the unauthorized state while the reauthentication is in progress.

**Buttons**

Save: Click to save changes.
Reset: Click to undo any changes made locally and revert to previously saved values.
5.3.2 Device Monitoring

This page provides an overview of the current NAS port states.

<table>
<thead>
<tr>
<th>Port</th>
<th>Admin State</th>
<th>Port State</th>
<th>Last Source</th>
<th>Last ID</th>
<th>QoS Class</th>
<th>Port VLAN ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Force Authorized</td>
<td>Globally Disabled</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>2</td>
<td>Force Authorized</td>
<td>Globally Disabled</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>3</td>
<td>Force Authorized</td>
<td>Globally Disabled</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>4</td>
<td>Force Authorized</td>
<td>Globally Disabled</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>5</td>
<td>Force Authorized</td>
<td>Globally Disabled</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>6</td>
<td>Force Authorized</td>
<td>Globally Disabled</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>7</td>
<td>Force Authorized</td>
<td>Globally Disabled</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>8</td>
<td>Force Authorized</td>
<td>Globally Disabled</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>9</td>
<td>Force Authorized</td>
<td>Globally Disabled</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>10</td>
<td>Force Authorized</td>
<td>Globally Disabled</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>11</td>
<td>Force Authorized</td>
<td>Globally Disabled</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>12</td>
<td>Force Authorized</td>
<td>Globally Disabled</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

Port

The switch port number. Click to navigate to detailed NAS statistics for this port.

Admin State

The port's current administrative state. Refer to NAS Admin State for a description of possible values.

Port Status

The current state of the port. Refer to NAS Port State for a description of the individual states.

Last Source

The source MAC address carried in the most recently received EAPOL frame for EAPOL-based authentication, and the most recently received frame from a new client for MAC-based authentication.

Last ID

The user name (supplicant identity) carried in the most recently received Response Identity EAPOL frame for EAPOL-based authentication, and the source MAC address from the most recently received frame from a new client for MAC-based authentication.

QoS Class

QoS Class assigned to the port by the RADIUS server if enabled.
Port VLAN ID

The VLAN ID that NAS places port in. The field is blank, if the Port VLAN ID is not overridden by NAS.
If the VLAN ID is assigned by the RADIUS server, "(RADIUS-assigned)" is appended to the VLAN ID. Read more about RADIUS-assigned VLANs here.
If the port is moved to the Guest VLAN, "(Guest)" is appended to the VLAN ID. Read more about Guest VLANs here.

Buttons

Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
Refresh: Click to refresh the page immediately.

5.3.3 Port Monitoring

This page provides detailed NAS statistics for a specific switch port running EAPOL-based IEEE 802.1X authentication. For MAC-based ports, it shows selected backend server (RADIUS Authentication Server) statistics only.
Use the port select box to select which port details to be displayed.

<table>
<thead>
<tr>
<th>Port State</th>
<th>Admin State</th>
<th>Port State</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Force Authorized</td>
<td>Globally Disabled</td>
</tr>
</tbody>
</table>

Port State

Admin State

The port's current administrative state. Refer to NAS Configuration Admin State for a description of possible values.

Port State

The current state of the port. Refer to NAS Configuration Admin State for a description of possible values.
5.4 ACL

5.4.1 Port Configuration

Configure the ACL parameters (ACE) of each switch port. These parameters will affect frames received on a port unless the frame matches a specific ACE.

### Port Configuration

<table>
<thead>
<tr>
<th>Port</th>
<th>Policy ID</th>
<th>Action</th>
<th>Rate Limit ID</th>
<th>EVC Policer</th>
<th>EVC Policer ID</th>
<th>Port Redirect</th>
<th>Mirror</th>
<th>Logging</th>
<th>Shutdown</th>
<th>State</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0</td>
<td>Permit</td>
<td>Disabled</td>
<td>Disabled</td>
<td>1</td>
<td>Disabled</td>
<td>Port 1 Port 2</td>
<td>Disabled</td>
<td>Disabled</td>
<td>Disabled</td>
<td>Enabled</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>Permit</td>
<td>Disabled</td>
<td>Disabled</td>
<td>1</td>
<td>Disabled</td>
<td>Port 1 Port 2</td>
<td>Disabled</td>
<td>Disabled</td>
<td>Disabled</td>
<td>Enabled</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>Permit</td>
<td>Disabled</td>
<td>Disabled</td>
<td>1</td>
<td>Disabled</td>
<td>Port 1 Port 2</td>
<td>Disabled</td>
<td>Disabled</td>
<td>Disabled</td>
<td>Enabled</td>
</tr>
<tr>
<td>4</td>
<td>0</td>
<td>Permit</td>
<td>Disabled</td>
<td>Disabled</td>
<td>1</td>
<td>Disabled</td>
<td>Port 1 Port 2</td>
<td>Disabled</td>
<td>Disabled</td>
<td>Disabled</td>
<td>Enabled</td>
</tr>
<tr>
<td>5</td>
<td>0</td>
<td>Permit</td>
<td>Disabled</td>
<td>Disabled</td>
<td>1</td>
<td>Disabled</td>
<td>Port 1 Port 2</td>
<td>Disabled</td>
<td>Disabled</td>
<td>Disabled</td>
<td>Enabled</td>
</tr>
<tr>
<td>6</td>
<td>0</td>
<td>Permit</td>
<td>Disabled</td>
<td>Disabled</td>
<td>1</td>
<td>Disabled</td>
<td>Port 1 Port 2</td>
<td>Disabled</td>
<td>Disabled</td>
<td>Disabled</td>
<td>Enabled</td>
</tr>
<tr>
<td>7</td>
<td>0</td>
<td>Permit</td>
<td>Disabled</td>
<td>Disabled</td>
<td>1</td>
<td>Disabled</td>
<td>Port 1 Port 2</td>
<td>Disabled</td>
<td>Disabled</td>
<td>Disabled</td>
<td>Enabled</td>
</tr>
<tr>
<td>8</td>
<td>0</td>
<td>Permit</td>
<td>Disabled</td>
<td>Disabled</td>
<td>1</td>
<td>Disabled</td>
<td>Port 1 Port 2</td>
<td>Disabled</td>
<td>Disabled</td>
<td>Disabled</td>
<td>Enabled</td>
</tr>
<tr>
<td>9</td>
<td>0</td>
<td>Permit</td>
<td>Disabled</td>
<td>Disabled</td>
<td>1</td>
<td>Disabled</td>
<td>Port 1 Port 2</td>
<td>Disabled</td>
<td>Disabled</td>
<td>Disabled</td>
<td>Enabled</td>
</tr>
<tr>
<td>10</td>
<td>0</td>
<td>Permit</td>
<td>Disabled</td>
<td>Disabled</td>
<td>1</td>
<td>Disabled</td>
<td>Port 1 Port 2</td>
<td>Disabled</td>
<td>Disabled</td>
<td>Disabled</td>
<td>Enabled</td>
</tr>
<tr>
<td>11</td>
<td>0</td>
<td>Permit</td>
<td>Disabled</td>
<td>Disabled</td>
<td>1</td>
<td>Disabled</td>
<td>Port 1 Port 2</td>
<td>Disabled</td>
<td>Disabled</td>
<td>Disabled</td>
<td>Enabled</td>
</tr>
<tr>
<td>12</td>
<td>0</td>
<td>Permit</td>
<td>Disabled</td>
<td>Disabled</td>
<td>1</td>
<td>Disabled</td>
<td>Port 1 Port 2</td>
<td>Disabled</td>
<td>Disabled</td>
<td>Disabled</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

**Port**

The switch port number.

**Policy ID**

Select the policy to apply to this port. The allowed values are 0 through 255. The default value is 0.

**Action**

Select whether forwarding is permitted ("Permit") or denied ("Deny"). The default value is "Permit".
Rate Limiter ID
Select which rate limiter to apply on this port. The allowed values are Disabled or the values 1 through 16. The default value is "Disabled".

EVC Policer
Select whether EVC policer is enabled or disabled. The default value is "Disabled". Note that ACL rate limiter and EVC policer can not both be enabled.

EVC Policer ID
Select which EVC policer ID to apply on this port. The allowed values are Disabled or the values 1 through 256.

Re-mirror Port
Select which port frames are redirected on. The allowed values are Disabled or a specific port number and it can't be set when action is permitted. The default value is "Disabled".

Mirror
Specify the mirror operation of this port. The allowed values are:
- Enabled: Frames received on the port are mirrored.
- Disabled: Frames received on the port are not mirrored.
The default value is "Disabled".

Logging
Specify the logging operation of this port. Notice that the logging message doesn't include the 4 bytes CRC. The allowed values are:
- Enabled: Frames received on the port are stored in the System Log.
- Disabled: Frames received on the port are not logged.
The default value is "Disabled".

Note:
The logging feature only works when the packet length is less than 1518(without VLAN tags) and the System Log memory size and logging rate is limited.

Shutdown
Specify the port shut down operation of this port. The allowed values are:
- Enabled: If a frame is received on the port, the port will be disabled.
- Disabled: Port shut down is disabled.
The default value is "Disabled".

Note:
Only when the packet length is less than 1518 (without VLAN tag), the shutdown function is effective.
State

Specify the port state of this port. The allowed values are:

- **Enabled**: To reopen ports by changing the volatile port configuration of the ACL user module.
- **Disabled**: To close ports by changing the volatile port configuration of the ACL user module.

The default value is "Enabled".

Counter

Counts the number of frames that match this ACE.

Buttons

Save: Click to save changes.
Reset: Click to undo any changes made locally and revert to previously saved values.
Refresh: Click to refresh the page; any changes made locally will be undone.
Clear: Click to clear the counters.

5.4.2 Rate Limiter Configuration

Configure the rate limiter for the ACL of the switch.
**Rate Limiter ID**

The rate limiter ID for the settings contained in the same row and its range is 1 to 16.

**Rate**

The valid rate is 0-3276700pps.
Or 0,100,200,300, ..., 1000000kbps.

**Unit**

Specify the rate unit. The allowed values are:
- pps: packets per second.
- kbps: Kbits per second.

**Buttons**

Save: Click to save changes.
Reset: Click to undo any changes made locally and revert to previously saved values.

### 5.4.3 Access Control List Configuration

This page shows the Access Control List (ACL), which is made up of the ACEs defined on this switch. Each row describes the ACE that is defined. The maximum number of ACEs is 256 on each switch.

Click on the lowest plus sign to add a new ACE to the list. The reserved ACEs used for internal protocol, cannot be edited or deleted, the order sequence cannot be changed and the priority is highest.

**ACE**

Indicates the ACE ID.

**Ingress Port**

Indicates the ingress port of the ACE. Possible values are:
- All: The ACE will match all ingress port.
- Port: The ACE will match a specific ingress port.

**Policy / Bitmask**

Indicates the policy number and bitmask of the ACE.

**Frame Type**

Indicates the frame type of the ACE. Possible values are:
• Any: The ACE will match any frame type.
• EType: The ACE will match Ethernet Type frames.
  Note:
  Ethernet Type based ACE will not get matched by IP and ARP frames.
• ARP: The ACE will match ARP/RARP frames.
• IPv4: The ACE will match all IPv4 frames.
• IPv4/ICMP: The ACE will match IPv4 frames with ICMP protocol.
• IPv4/UDP: The ACE will match IPv4 frames with UDP protocol.
• IPv4/TCP: The ACE will match IPv4 frames with TCP protocol.
• IPv4/Other: The ACE will match IPv4 frames, which are not ICMP/UDP/TCP.
• IPv6: The ACE will match all IPv6 standard frames.

Action
Indicates the forwarding action of the ACE.
• Permit: Frames matching the ACE may be forwarded and learned.
• Deny: Frames matching the ACE are dropped.
• Filter: Frames matching the ACE are filtered.

Rate Limiter
Indicates the rate limiter number of the ACE. The allowed range is 1 to 16. When Disabled is displayed, the rate limiter operation is disabled.

Port Redirect
Indicates the port redirect operation of the ACE. Frames matching the ACE are redirected to the port number. The allowed values are Disabled or a specific port number. When Disabled is displayed, the port redirect operation is disabled.

Mirror
Specify the mirror operation of this port. Frames matching the ACE are mirrored to the destination mirror port. The allowed values are:
• Enabled: Frames received on the port are mirrored.
• Disabled: Frames received on the port are not mirrored.

The default value is "Disabled".

Counter
The counter indicates the number of times the ACE was hit by a frame.

Modification Buttons
You can modify each ACE (Access Control Entry) in the table using the following buttons:

Add: Insert a new ACE before the current row.
Edit: Edit the ACE row.
5.4.4 ACL Status

This page shows the ACL status by different ACL users. Each row describes the ACE that is defined. It is a conflict if a specific ACE is not applied to the hardware due to hardware limitations. The maximum number of ACEs is 256 on each switch.

<table>
<thead>
<tr>
<th>User</th>
<th>ACE</th>
<th>Frame Type</th>
<th>Action</th>
<th>Rate Limiter</th>
<th>Mirror</th>
<th>CPU</th>
<th>Counter</th>
<th>Conflict</th>
</tr>
</thead>
<tbody>
<tr>
<td>netmanager 1</td>
<td>IPv4/UDP 65535:65534</td>
<td>Permit</td>
<td>Disabled</td>
<td>Disabled</td>
<td>Yes</td>
<td>0</td>
<td>0</td>
<td>No</td>
</tr>
<tr>
<td>ring 1</td>
<td>ARP</td>
<td>Permit</td>
<td>Disabled</td>
<td>Disabled</td>
<td>No</td>
<td>0</td>
<td>0</td>
<td>No</td>
</tr>
<tr>
<td>ring 2</td>
<td>LLC</td>
<td>Permit</td>
<td>Disabled</td>
<td>Disabled</td>
<td>No</td>
<td>0</td>
<td>0</td>
<td>No</td>
</tr>
</tbody>
</table>

**User**
Indicates the ACL user.

**ACE**
Indicates the ACE ID on local switch.

**Frame Type**
Indicates the frame type of the ACE. Possible values are:
- **Any**: The ACE will match any frame type.
- **EType**: The ACE will match Ethernet Type frames. Note that an Ethernet Type based ACE will not get matched by IP and ARP frames.
- **ARP**: The ACE will match ARP/RARP frames.
- **IPv4**: The ACE will match all IPv4 frames.
- **IPv4/ICMP**: The ACE will match IPv4 frames with ICMP protocol.
- **IPv4/UDP**: The ACE will match IPv4 frames with UDP protocol.
- **IPv4/TCP**: The ACE will match IPv4 frames with TCP protocol.
- **IPv4/Other**: The ACE will match IPv4 frames, which are not ICMP/UDP/TCP.
- **IPv6**: The ACE will match all IPv6 standard frames.

**Action**
Indicates the forwarding action of the ACE.
- **Allow**: frames matching ACE can be forwarded and learned.
- **Reject**: frames matching ACE are deleted.
• Filter: Frames matching the ACE are filtered.

**Rate Limiter**
Indicates the rate limiter number of the ACE. The allowed range is 1 to 16. When Disabled is displayed, the rate limiter operation is disabled.

**CPU**
Forward packet that matched the specific ACE to CPU.

**Counter**
The counter indicates the number of times the ACE was hit by a frame.

**Conflict**
Indicates the hardware status of the specific ACE. The specific ACE is not applied to the hardware due to hardware limitations.

**Buttons**
The select box determines which ACL user is affected by clicking the buttons.

Auto-refresh: Check this box to enable an automatic refresh. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page.

### 5.5 Ethernet Services

#### 5.5.1 Port Configuration

This page displays current EVC port configurations. The settings can also be configured here.
Port

The switch port number.

DEI Mode

The DEI mode for an NNI port determines whether frames transmitted on the port will have the DEI field in the outer tag marked based on the colour of the frame. The allowed values are:
- Coloured: The DEI is 1 for yellow frames and 0 for green frames.
- Fixed: The DEI value is determined by ECE rules.

Tag Mode

The tag mode specifying whether the EVC classification must be based on the outer or inner tag. This can be used on NNI ports connected to another service provider, where an outer "tunnel" tag is added together with the inner tag identifying the EVC. The allowed values are:
- Inner: Enable inner tag in EVC classification.
- Outer: Enable outer tag in EVC classification.

Address Mode

The IP/MAC address mode specifying whether the EVC classification must be based on source (SMAC/SIP) or destination (DMAC/DIP) addresses. The allowed values are:
- Source: Enable SMAC/SIP matching.
- Destination: Enable DMAC/DIP matching.

Buttons

Save: Click to save changes.
Reset: Click to undo any changes made locally and revert to previously saved values.

5.5.2 L2CP Configuration

This page displays current EVC L2CP configurations. The settings can also be configured here.
DMAC

The destination BPDU MAC addresses (01-80-C2-00-00-0X) and GARP (01-80-C2-00-00-2X) MAC addresses for the settings contained in the same row.

L2CP Mode

The L2CP mode for the specific port. Possible values are:

- **Peer**: Allow to peer L2CP frames.
- **Forward**: Allow to forward L2CP frames.

Buttons

- **Port 1 ▼**: the port select box determines which port is affected by clicking the buttons.
- **Refresh**: Click to refresh the page.
- **Save**: Click to save changes.
- **Reset**: Click to undo any changes made locally and revert to previously saved values.

5.5.3 Bandwidth Limitation Subset

This page displays current EVC ingress bandwidth profile configurations. These policers may be used to limit the traffic received on UNI ports. The settings can also be configured here.
Start from Policer ID
The start Policer ID for displaying the table entries. The allowed range is from 1 through 256.

Entry
The number of entries per page. The allowed range is from 2 through 256.

Policer ID
The Policer ID is used to identify one of the 256 policers.

State
The administrative state of the bandwidth profile. The allowed values are:
- Enabled: The bandwidth profile enabled.
- Disabled: The bandwidth profile is disabled.

Type
The policer type of the bandwidth profile. The allowed values are:
- MEF: MEF ingress bandwidth profile.
- Single: Single bucket policer.

Policer Mode
The colour mode of the bandwidth profile. The allowed values are:
- Coupled: Colour-aware mode with coupling enabled.
- Aware: Colour-aware mode with coupling disabled.

Rate Type
The rate type of the bandwidth profile. The allowed values are:
- Data: Specify that this bandwidth profile operates on data rate.
- Line: Specify that this bandwidth profile operates on line rate.
### CIR

The Committed Information Rate of the bandwidth profile. The allowed range is from 0 through 10000000 kilobit per second.

### CBS

The Committed Burst Size of the bandwidth profile. The allowed range is from 0 through 100000 bytes.

### EIR

The Excess Information Rate for MEF type bandwidth profile. The allowed range is from 0 through 10000000 kilobit per second.

### EBS

The Excess Burst Size for MEF type bandwidth profile. The allowed range is from 0 through 100000 bytes.

### Buttons

- **Refresh**: Refresh the displayed table starting from the input fields.
- **<<**: Updates the table, starting with the first entry in the table.
- **<<**: Updates the table, ending at the entry before the first entry currently displayed.
- **>>**: Updates the table, starting with the entry after the last entry currently displayed.
- **>>|**: Updates the table, ending at the last entry in the table.

**Save**: Click to save changes.

**Reset**: Click to undo any changes made locally and revert to previously saved values.

### 5.5.4 EVCs Configuration

This page displays current EVC configurations. On this system, only Provider Bridge based EVCs are supported.

#### EVC ID

The EVC ID identifies the EVC. The range is from 1 through 256.

#### Name

The name for the EVC.
**VID**

The VLAN ID in the PB network. It may be inserted in a C-tag, S-tag or S-custom tag depending on the NNI port VLAN configuration. The range is from 1 through 4095.

**IVID**

The Internal/classified VLAN ID in the PB network. The range is from 1 through 4095.

**Learning**

The learning mode for the EVC controls whether source MAC addresses are learned for frames matching the EVC. Learning may be disabled if the EVC only includes two UNI/NNI ports. Possible values are:
- Enabled: Learning is enabled (MAC addresses are learned).
- Disabled: Learning is disabled (MAC addresses are not learned).

**Inner Tag Type**

The inner tag type is used to determine whether an inner tag is inserted in frames forwarded to NNI ports. Possible values are:
- None: An inner tag is not inserted.
- C-tag: An inner C-tag is inserted.
- S-tag: An inner S-tag is inserted.
- S-custom-tag: An inner tag is inserted and the tag type is determined by the VLAN port configuration of the NNI.

**Inner Tag VID Mode**

The inner VID Mode affects the VID in the inner and outer tag. Possible values are:
- Normal: The VID of the two outer tags aren't swapped.
- Tunnel: The VID of the two outer tags are swapped, so that the VID of the outer tag is taken from the Inner Tag configuration and the VID of the inner tag is the EVC VID. In this mode, the NNI ports are normally configured to do EVC classification based on the inner tag.

**Inner Tag VID**

The Inner tag VLAN ID. The allowed range is from 0 through 4095.

**Inner Tag PCP/DEI Preservation**

The inner tag PCP and DEI preservation. Possible values are:
- Preserved: The inner tag PCP and DEI is preserved.
- Fixed: The inner tag PCP and DEI is fixed.

**Inner Tag PCP**

The inner tag PCP value. The allowed range is from 0 through 7.

**Inner Tag DEI**

The inner tag DEI value. The allowed value is 0 or 1.
Outer Tag VID
The EVC outer tag VID for UNI ports. The allowed range is from 0 through 4095.

NNI Ports
The list of Network to Network Interfaces for the EVC.

Modification Buttons
You can modify each EVC in the table using the following buttons:

- Edit the EVC entry.
- Delete the EVC entry.
- Add new EVC entry.

Buttons
Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
Refresh: Click to refresh the page.
Remove all: Click to remove all EVCs.

This page displays current EVC configurations. The settings can also be configured here.
**NNI Ports**

The list of Network to Network Interfaces for the EVC.

**EVC ID**

The EVC ID identifies the EVC. The allowed range is from 1 through 256.

**Name**

The name for the EVC. It is case sensitive and can contain up to 256 characters combination of alphanumeric and special characters.

**VID**

The VLAN ID in the PB network. It may be inserted in a C-tag, S-tag or S-custom tag depending on the NNI port VLAN configuration. The allowed range is from 1 through 4095.

**IVID**

The Internal/classified VLAN ID in the PB network. The allowed range is from 1 through 4095.
Learning
The learning mode for the EVC controls whether source MAC addresses are learned for frames matching the EVC. Learning may be disabled if the EVC only includes two UNI/NNI ports. Possible values are:
- Enabled: Learning is enabled (MAC addresses are learned).
- Disabled: Learning is disabled (MAC addresses are not learned).

Inner Tag Type
The inner tag type is used to determine whether an inner tag is inserted in frames forwarded to NNI ports. Possible values are:
- None: An inner tag is not inserted.
- C-tag: An inner C-tag is inserted.
- S-tag: An inner S-tag is inserted.
- S-custom-tag: An inner tag is inserted and the tag type is determined by the VLAN port configuration of the NNI.

VID Mode
The inner VID Mode affects the VID in the inner and outer tag. Possible values are:
- Normal: The VID of the two outer tags aren't swapped.
- Tunnel: The VID of the two outer tags are swapped, so that the VID of the outer tag is taken from the Inner Tag configuration and the VID of the inner tag is the EVC VID. In this mode, the NNI ports are normally configured to do EVC classification based on the inner tag.

VLAN ID
The Inner tag VLAN ID. The allowed range is from 1 through 4095.

PCP/DEI Preservation
The inner tag PCP and DEI preservation. Possible values are:
- Preserved: The inner tag PCP and DEI is preserved.
- Fixed: The inner tag PCP and DEI is fixed.

PCP
The inner tag PCP value. The allowed range is from 0 through 7.

DEI
The inner tag DEI value. The allowed value is 0 or 1.

Outer Tag VLAN ID
The EVC outer tag VID for UNI ports. The allowed range is from 1 through 4095.
Buttons

Save: Click to save changes.
Reset: Click to undo any changes made locally and revert to previously saved values.
Cancel: Return to the previous page; any changes made locally will be undone.

5.5.5 ECEs Configuration

This page displays the current EVC Control Entries (ECEs). The settings can also be configured here.

ECE ID

The ECE ID identifies the ECE. Unique ECE IDs are automatically assigned to ECEs added. The possible range is from 1 through 256.

Ingress Matching

UNI Ports

The list of User Network Interfaces for the ECE.

Tag Type

The tag type for the ECE. Possible values are:
- Any: The ECE will match both tagged and untagged frames.
- Untagged: The ECE will match untagged frames only.
- C-Tagged: The ECE will match custom tagged frames only.
- S-Tagged: The ECE will match service tagged frames only.
- Tagged: The ECE will match tagged frames only.

VID

The VLAN ID for the ECE. It only significant if tag type 'Tagged' is selected. Possible values are:
- Specific: The range is from 0 through 4095.
- Any: The ECE will match any VLAN ID.

PCP

The PCP value for the ECE. It only significant if tag type 'Tagged' is selected. Possible values are:
Specific: The ECE will match a specific PCP in the range 0 through 7.
Range: The ECE will match PCP values in the selected range 0-1, 2-3, 4-5, 6-7, 0-3 or 4-7.
Any: The ECE will match any PCP value.

**DEI**

The DEI value for the ECE. It only significant if tag type ‘Tagged’ is selected. The possible values is: 0, 1 or Any.

**Frame Type**

The frame type for the ECE. Possible values are:
- Any: The ECE will match any frame type.
- IPv4: The ECE will match IPv4 frames only.
- IPv6: The ECE will match IPv6 frames only.

**Actions**

**Direction**

The EVCs and ECEs are used to setup flows in one or both directions as determined by the ECE Direction parameter. If the ECE is bidirectional, the ingress rules of the NNI ports will be setup to match the traffic being forwarded to NNI ports. Possible values are:
- Both: Bidirectional.
- UNI-to-NNI: Unidirectional from UNI to NNI.
- NNI-to-UNI: Unidirectional from NNI to UNI.

**EVC ID**

The EVC ID for the ECE. The ECE is only active when mapping to an existing EVC. Possible values are:
- Specific: The range is from 1 through 256.
- None: The ECE does not map to an EVC.

**Tag Pop Count**

The ingress tag pop count for the ECE. The possible range is from 0 through 2.

**Policy ID**

The ACL Policy ID for the ECE. The range is from 0 through 255.

**Class**

The traffic class for the ECE. The range is from 0 through 7.

**Egress Outer Tag Mode**

The outer tag for nni-to-uni direction for the ECE. Possible values are:
- Enable: Enable outer tag for nni-to-uni direction for the ECE.
• Disable: Disable outer tag for nni-to-uni direction for the ECE.

**PEC/DEI Preservation**

The outer tag PCP and DEI preservation for the ECE. Possible values are:

- Preserved: The outer tag PCP and DEI are preserved.
- Fixed: The outer tag PCP and DEI are fixed.

**PCP**

The outer tag PCP value for the ECE. The possible range is from 0 through 7.

**DEI**

The outer tag DEI value for the ECE. The possible value is 0 or 1.

**Conflict**

Indicates the hardware status of the specific ECE. The specific ECE is not applied to the hardware due to hardware limitations.

**Modification Buttons**

You can modify each ECE (EVC Control Entry) in the table using the following buttons:

- (+) Inserts a new ECE before the current row.
- (•) Edits the ECE row.
- (<) Moves the ECE up the list.
- (>) Moves the ECE down the list.
- (X) Deletes the ECE.
- (+) The lowest plus sign adds a new entry at the bottom of the ECE listings.

**Buttons**

Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page.

Remove all: Click to remove all ECEs.

This page displays current ECE configurations. The settings can also be configured here.
UNI Ports

The list of User Network Interfaces for the ECE.

Ingress Matching

Tag Type

The tag type for matching the ECE. Possible values are:

- Any: The ECE will match both tagged and untagged frames.
- Untagged: The ECE will match untagged frames only.
- C-Tagged: The ECE will match custom tagged frames only.
- S-Tagged: The ECE will match service tagged frames only.
- Tagged: The ECE will match tagged frames only.

VLAN ID Filter

The VLAN ID filter for matching the ECE. It only significant if tag type 'Tagged' is selected. Possible values are:

- Any: No VLAN ID filter is specified. (VLAN ID filter status is "don't-care".)
Specific: If you want to filter a specific VLAN ID value with this ECE, choose this value. A field for entering a specific value appears.

Range: If you want to filter a specific VLAN ID range filter with this ECE, choose this value. A field for entering a range appears.

VLAN ID Value
When "Specific" is selected for the VLAN ID filter, you can enter a specific value. The allowed value is from 0 through 4095.

VLAN ID Range
When "Range" is selected for the VLAN ID filter, you can enter a specific range. The allowed range is from 0 through 4095.

PCP
The PCP value for matching the ECE. It only significant if tag type 'Tagged' is selected. Possible values are:
- Any: The ECE will match any PCP value.
- Specific: The ECE will match a specific PCP in the range 0 through 7.
- Range: The ECE will match PCP values in the selected range 0-1, 2-3, 4-5, 6-7, 0-3 or 4-7.

DEI
The DEI value for matching the ECE. It only significant if tag type 'Tagged' is selected. The allowed value is: 0, 1 or Any.

Frame Type
The frame type for the ECE. Possible values are:
- Any: The ECE will match any frame type.
- IPv4: The ECE will match IPv4 frames only.
- IPv6: The ECE will match IPv6 frames only.

IP Parameters

Protocol
The IP protocol for matching the ECE. Possible values are:
- Any: No protocol filter is specified. (Protocol filter status is "don't-care").
- UDP: Specify the UDP for matching the ECE.
- TCP: Specify the TCP for matching the ECE.
- Other: If you want to filter a specific protocol value with this ECE, choose this value. A field for entering a specific value appears.

Protocol Value
When "other" is selected for the protocol filter, you can enter a specific value. The allowed value is from 0 through 255.
SIP/DIP Filter

The source/destination IP address for matching the ECE. It depend on by the port address mode, when port address mode is set to 'Source' then the field is used for source address. Similarly when port address mode is set to 'Destination' then the field is used for destination address. Possible values are:

- **Any**: No SIP/DIP filter is specified. (SIP/DIP filter status is "don't-care").
- **Host**: When "IPv4" is selected for the Frame Type, if you want to filter a specific host address with this ECE, choose this value. A field for entering a host address appears.
- **Network**: When "IPv4" is selected for the Frame Type, if you want to filter a specific network address with this ECE, choose this value. Two fields for entering a specific network address and network mask appears.
- **Specific**: When "IPv6" is selected for the Frame Type, if you want to filter a specific network address with this ECE, choose this value. Two fields for entering a specific network address and network mask appears.

SIP/DIP Address

When "IPv4" is selected for the Frame Type and "Host" or "Network" is selected for the SIP/DIP filter, you can enter a specific host or network address. When "IPv6" is selected for the Frame Type, the field only supported 32 bits for IPv6 address.

SIP/DIP Mask

When "IPv4" is selected for the Frame Type and "Host" or "Network" is selected for the SIP/DIP filter, you can enter a specific network mask. When "IPv6" is selected for the Frame Type, the field only supported 32 bits for IPv6 address mask.

DSCP Filter

The DSCP filter for matching the ECE. Possible values are:

- **Any**: No DSCP filter is specified. (DSCP filter status is "don't-care").
- **Specific**: If you want to filter a specific DSCP value with this ECE, choose this value. A field for entering a specific value appears.
- **Range**: If you want to filter a specific DSCP range filter with this ECE, choose this value. A field for entering a range appears.

DSCP Value

When "Specific" is selected for the DSCP filter, you can enter a specific value. The allowed value is from 0 through 63.

DSCP Range

When "Range" is selected for the DSCP filter, you can enter a specific range. The allowed range is from 0 through 63.
**Fragment**

The IPv4 Fragment for matching the ECE. This involves the settings for the More Fragments (MF) bit and the Fragment Offset (FRAG OFFSET) field for an IPv4 frame. Possible values are:

- **Any:** The ECE will match any MF bit.
- **Non-Fragment:** IPv4 frames where the MF bit is set or the FRAG OFFSET field is greater than zero must not be able to match this entry.
- **Fragment:** IPv4 frames where the MF bit is set or the FRAG OFFSET field is greater than zero must be able to match this entry.

**UDP/TCP Parameters**

**Source Port Filter**

The TCP/UDP source port for matching the ECE. It only significant if protocol filter 'UDP' or 'TCP' is selected. Possible values are:

- **Any:** No TCP/UDP source port filter is specified. (Source port filter status is "don't-care".)
- **Specific:** If you want to filter a specific TCP/UDP source port No. Use this ECE, choose this value. A field for entering a specific No. appears.
- **Range:** If you want to filter a specific TCP/UDP source port range filter with this ECE, choose this value. A field for entering a range appears.

**Source Port No.**

When "Specific" is selected for the source port filter, you can enter a specific value. The allowed value is from 0 through 65535.

**Source Port Range**

When "Range" is selected for the source port filter, you can enter a specific range. The allowed range is from 0 through 65535.

**Destination Port Filter**

The TCP/UDP destination port for matching the ECE. It only significant if protocol filter 'UDP' or 'TCP' is selected. The possible values are:

- **Any:** No TCP/UDP destination port filter is specified. (Destination port filter status is "don't-care".)
- **Specific:** If you want to filter a specific TCP/UDP destination port No. Use this ECE, choose this value. A field for entering a specific No. appears.
- **Range:** If you want to filter a specific TCP/UDP destination port range filter with this ECE, choose this value. A field for entering a range appears.
**Destination Port No.**
When "Specific" is selected for the destination port filter, you can enter a specific value. The allowed value is from 0 through 65535.

**Destination Port Range**
When "Range" is selected for the destination port filter, you can enter a specific range. The allowed range is from 0 through 65535.

**MAC Parameters**

**SMAC Filter**
The source MAC address for matching the ECE. Possible values are:
- Any: No SMAC filter is specified. (SMAC filter status is "don't-care").
- Specific: If you want to filter a specific SMAC value with this ECE, choose this value. A field for entering a specific value appears.

**SMAC Value**
When "Specific" is selected for the SMAC filter, you can enter a specific value. The legal format is "xx-xx-xx-xx-xx-xx" or "xx.xx.xx.xx.xx.xx" or "xxxxxxxxxxxx" (x is a hexadecimal digit).

**DMAC Type**
The destination MAC address type for matching the ECE. Possible values are:
- Any: No DMAC type is specified. (DMAC filter status is "don't-care").
- Unicast: Frame must be unicast.
- Multicast: Frame must be multicast.
- Broadcast: Frame must be broadcast.

**Action**

**Direction**
The EVCs and ECEs are used to setup flows in one or both directions as determined by the ECE Direction parameter. If the ECE is bidirectional, the ingress rules of the NNI ports will be setup to match the traffic being forwarded to NNI ports. Possible values are:
- Both: Bidirectional.
- UNI-to-NNI: Unidirectional from UNI to NNI.
- NNI-to-UNI: Unidirectional from NNI to UNI.

**EVC ID Filter**
The EVC ID for the ECE. The ECE is only active when mapping to an existing EVC. Possible values are:
- Any: No EVC ID filter is specified. (EVC ID filter status is "don't-care").
- Specific: If you want to filter a specific EVC ID with this ECE, choose this value.
A field for entering a specific value appears.

EVC ID Value
When “Specific” is selected for the VLAN ID filter, you can enter a specific value. The allowed value is from 1 through 256.

Tag Pop Count
The ingress tag pop count for the ECE. The allowed range is from 0 through 2.

Policy ID
The ACL Policy ID for the ECE for matching ACL rules. The allowed range is from 0 through 255.

Class
The traffic class for the ECE. The allowed range is from 0 through 7 or disabled.

Egress Outer Tag
Mode
The outer tag for nni-to-uni direction for the ECE. Possible values are:
- Enable: Enable outer tag for nni-to-uni direction for the ECE.
- Disable: Disable outer tag for nni-to-uni direction for the ECE.

PEC/DEI Preservation
The outer tag PCP and DEI preservation for the ECE. Possible values are:
- Preserved: The outer tag PCP and DEI is preserved.
- Fixed: The outer tag PCP and DEI is fixed.

PCP
The outer tag PCP value for the ECE. The allowed range is from 0 through 7.

DEI
The outer tag DEI value for the ECE. The allowed value is 0 or 1.

Buttons
Save: Click to save changes.
Reset: Click to undo any changes made locally and revert to previously saved values.
Cancel: Return to the previous page; any changes made locally will be undone.

5.5.6 EVC Statistics
This page provides NNI port traffic statistics for the selected EVC. It also shows counters for UNI ports of ECEs mapping to the EVC. And the MPLS Pseudo-Wires counters are included when the PW ID is attached to the selected EVC.
**Class**

The traffic class for the EVC.

**Green Frames Rx**

The number of green received.

**Green Frames Tx**

The number of green transmitted.

**Yellow Frames Rx**

The number of yellow received.

**Yellow Frames Tx**

The number of yellow transmitted.

**Red Frames Rx**

The number of red received.

**Discarded Frames Green**

The number of discarded in the green color.

**Discarded Frames Yellow**

The number of discarded in the yellow color.

**Buttons**

Port 1▼: The port select box determines which port is affected by clicking the buttons.

Auto-refresh: Check this box to enable an automatic refresh. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page immediately.

Clear: Clears the counters for the selected port.

### 5.6 RADIUS

#### 5.6.1 RADIUS Server Configuration

This page allows you to configure the RADIUS servers.
Global Configuration

These setting are common for all of the RADIUS servers.

Timeout

Timeout is the number of seconds, in the range 1 to 1000, to wait for a reply from a RADIUS server before retransmitting the request.

Retransmit

Retransmit is the number of times, in the range 1 to 1000, a RADIUS request is retransmitted to a server that is not responding. If the server has not responded after the last retransmit it is considered to be dead.

Deadtime

Deadtime, which can be set to a number between 0 to 1440 分, is the period during which the switch will not send new requests to a server that has failed to respond to a previous request. This will stop the switch from continually trying to contact a server that it has already determined as dead.

Setting the Deadtime to a value greater than 0 (0) will enable this feature, but only if more than one server has been configured.

Key

The secret key - up to 63 characters long - shared between the RADIUS server and the switch.
**NAS-IP-Address (Attribute 4)**

The IPv4 address to be used as attribute 4 in RADIUS Access-Request packets. If this field is left blank, the IP address of the outgoing interface is used.

**NAS-Identifier (Attribute 32)**

The identifier - up to 253 characters long - to be used as attribute 32 in RADIUS Access-Request packets. If this field is left blank, the NAS-Identifier is not included in the packet.

**Server Configuration**

The table has one row for each RADIUS server and a number of columns, which are:

**Delete**

To delete a RADIUS server entry, check this box. The entry will be deleted during the next Save.

**Hostname**

The IP address or hostname of the RADIUS server.

**Auth Port**

The UDP port to use on the RADIUS server for authentication. Set to 0 to disable authentication.

**Acct Port**

The UDP port to use on the RADIUS server for accounting. Set to 0 to disable accounting.

**Timeout**

This optional setting overrides the global timeout value. Leaving it blank will use the global timeout value.

**Retransmit**

This optional setting overrides the global retransmit value. Leaving it blank will use the global retransmit value.

**Key**

This optional setting overrides the global key. Leaving it blank will use the global key.

**Adding New Server**

Click “Add New Server” to add a new RADIUS server. An empty row is added to the table, and the RADIUS server can be configured as needed. Up to 5 servers are supported.

The “Delete” button can be used to undo the addition of the new server.
**Buttons**

Save: Click to save changes.
Reset: Click to undo any changes made locally and revert to previously saved values.

**5.6.2 RADIUS Server Status Overview Monitoring**

This page provides an overview of RADIUS server status. This server is configurable on the Authentication configuration page.

<table>
<thead>
<tr>
<th>#</th>
<th>Host Name</th>
<th>Authentication Port</th>
<th>Authentication Status</th>
<th>Accounting Port</th>
<th>Accounting Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td>Disabled</td>
<td></td>
<td>Disabled</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td>Disabled</td>
<td></td>
<td>Disabled</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td>Disabled</td>
<td></td>
<td>Disabled</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td>Disabled</td>
<td></td>
<td>Disabled</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td></td>
<td>Disabled</td>
<td></td>
<td>Disabled</td>
<td></td>
</tr>
</tbody>
</table>

**RADIUS Servers#**

The RADIUS server number. Click to navigate to detailed statistics for this server.

**IP Address**

The IP address of this server.

**Authentication Port**

UDP port number for authentication.

**Authentication Status**

The current status of the server. This field takes one of the following values:

- Disabled: The server is disabled.
- Not Ready: The server is enabled, but IP communication is not yet up and running.
- Ready: The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept access attempts.
- Dead (X seconds left): Access attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.

**Accounting Port**

Billing UDP port number.
Accounting Status

The current status of the server. This field takes one of the following values:

- Disabled: The server is disabled.
- Not Ready: The server is enabled, but IP communication is not yet up and running.
- Ready: The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept access attempts.
- Dead (X seconds left): Access attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.

Buttons

Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
Refresh: Click to refresh the page immediately.

5.6.3 RADIUS Authentication Statistics Link Monitoring

This page provides detailed statistics for a particular RADIUS server.
RADIUS Authentication Statistics

The statistics map closely to those specified in RFC4668 – RADIUS Authentication Client MIB.

Use the server select box to switch between the backend servers to show details for.

Packet Counters

RADIUS authentication server packet counter. There are seven receive and four transmit counters.

<table>
<thead>
<tr>
<th>Direction</th>
<th>Name</th>
<th>RFC4668 Name</th>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rx</td>
<td>Access Accepts</td>
<td>radiusAuthClientExtAccessAccepts</td>
<td>The number of RADIUS Access-Accept packets (valid or invalid) received from the server.</td>
</tr>
<tr>
<td>Rx</td>
<td>Access Rejects</td>
<td>radiusAuthClientExtAccessRejects</td>
<td>The number of RADIUS Access-Reject packets (valid or invalid) received from the server.</td>
</tr>
<tr>
<td>Rx</td>
<td>Access Challenges</td>
<td>radiusAuthClientExtAccessChallenges</td>
<td>The number of RADIUS Access-Challenge packets (valid or invalid) received from the server.</td>
</tr>
<tr>
<td>Rx</td>
<td>Malformed access response</td>
<td>radiusAuthClientExtMalformedAccessResponses</td>
<td>The number of malformed RADIUS Access-Response packets received from the server. Malformed packets include packets with an invalid length. Bad authenticators or Message Authenticator attributes or unknown types are not included as malformed access responses.</td>
</tr>
<tr>
<td>Rx</td>
<td>Bad authenticators</td>
<td>radiusAuthClientExtBadAuthenticators</td>
<td>The number of RADIUS Access-Response packets containing invalid authenticators or Message Authenticator attributes received from the server.</td>
</tr>
<tr>
<td>Rx</td>
<td>Unknown types</td>
<td>radiusAuthClientExtUnknownTypes</td>
<td>The number of RADIUS packets that were received with unknown types from the server on the authentication port and dropped.</td>
</tr>
<tr>
<td>Rx</td>
<td>Packets Dropped</td>
<td>radiusAuthClientExtPacketsDropped</td>
<td>The number of RADIUS packets that were received from the server on the authentication port and dropped.</td>
</tr>
</tbody>
</table>
Direction | Name | RFC4668 Name | Note
--- | --- | --- | ---
| | d | | authentication port and dropped for some other reason.

Tx | Access Requests | radiusAuthClientExtAccessRequest | The number of RADIUS Access-Request packets sent to the server. This does not include retransmissions.

Tx | Access Retransmissions | radiusAuthClientExtAccessRetransmissions | The number of RADIUS Access-Request packets retransmitted to the RADIUS authentication server.

Tx | Pending Requests | radiusAuthClientExtPendingRequests | The number of RADIUS Access-Request packets destined for the server that have not yet timed out or received a response. This variable is incremented when an Access-Request is sent and decremented due to receipt of an Access-Accept, Access-Reject, Access-Challenge, timeout, or retransmission.

Tx | Timeouts | radiusAuthClientExtTimeouts | The number of authentication timeouts to the server. After a timeout, the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as a Request as well as a timeout.

### Other Info

This section contains information about the state of the server and the latest round-trip time.

<table>
<thead>
<tr>
<th>Name</th>
<th>RFC4668 Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td></td>
<td>IP address and UDP port number of the related authentication server</td>
</tr>
</tbody>
</table>
| State | | Shows the state of the server. It adopts one of the following values:  
  - Disabled: The selected server is disabled.  
  - Not Ready: The server is enabled, but IP |
Name | RFC4668 Name | Description
---|---|---
| | | communication is not yet up and running.
| | | • Ready: The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept access attempts.
| | | • Dead (X seconds left): Access attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.

| Round-trip time | radiusAuthClientExt RoundTripTime | The time interval (measured in milliseconds) between the most recent Access-Reply/Access-Challenge and the Access-Request that matched it from the RADIUS authentication server. The granularity of this measurement is 100 ms. A value of 0 ms indicates that there hasn't been round-trip communication with the server yet.

**RADIUS Accounting Statistics**

The statistics map closely to those specified in RFC4670-RADIUS Accounting Client MIB.

Use the server select box to switch between the backend servers to show details for.

**Packet Counters**

RADIUS accounting server packet counter. There are five receive and four transmit counters.

<table>
<thead>
<tr>
<th>Direction</th>
<th>Name</th>
<th>RFC4670 Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rx</td>
<td>Responses</td>
<td>radiusAccClient ExtResponses</td>
<td>The number of RADIUS packets (valid or invalid) received from the server.</td>
</tr>
<tr>
<td>Rx</td>
<td>Malformed Response</td>
<td>radiusAccClient ExtMalformedResponses</td>
<td>The number of malformed RADIUS packets received from the server. Malformed packets include packets with an invalid length. Bad authenticators or unknown types are not included as</td>
</tr>
<tr>
<td>Direction</td>
<td>Name</td>
<td>RFC4670 Name</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-----------------------</td>
<td>-------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Rx</td>
<td>Bad authenticators</td>
<td>radiusAcctClient</td>
<td>malformed access responses.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ExtBadAuthenticators</td>
<td></td>
</tr>
<tr>
<td>Rx</td>
<td>Unknown type</td>
<td>radiusAcctClient</td>
<td>The number of RADIUS packets containing invalid authenticators received from the server.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ExtUnknownTypes</td>
<td></td>
</tr>
<tr>
<td>Rx</td>
<td>Packets Dropped</td>
<td>radiusAcctClient</td>
<td>The number of RADIUS packets of unknown types that were received from the server on the accounting port.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ExtPacketsDropped</td>
<td></td>
</tr>
<tr>
<td>Tx</td>
<td>Requests</td>
<td>radiusAcctClient</td>
<td>The number of RADIUS packets sent to the server. This does not include retransmissions.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ExtRequests</td>
<td></td>
</tr>
<tr>
<td>Tx</td>
<td>Retransmissions</td>
<td>radiusAcctClient</td>
<td>The number of RADIUS packets retransmitted to the RADIUS accounting server.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ExtRetransmissions</td>
<td></td>
</tr>
<tr>
<td>Tx</td>
<td>Pending Requests</td>
<td>radiusAcctClient</td>
<td>The number of RADIUS packets destined for the server that have not yet timed out or received a response. This variable is incremented when a Request is sent and decremented due to receipt of a Response, timeout, or retransmission.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ExtPendingRequests</td>
<td></td>
</tr>
<tr>
<td>Tx</td>
<td>Timeout</td>
<td>radiusAcctClient</td>
<td>The number of accounting timeouts to the server. After a timeout, the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as a Request as well as a timeout.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ExtTimeouts</td>
<td></td>
</tr>
</tbody>
</table>
Other Info

This section contains information about the state of the server and the latest round-trip time.

<table>
<thead>
<tr>
<th>Name</th>
<th>RFC4670 Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>-</td>
<td>IP address and UDP port for the accounting server in question.</td>
</tr>
<tr>
<td>State</td>
<td>-</td>
<td>Shows the state of the server. It takes one of the following values:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Disabled: The selected server is disabled.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Not Ready: The server is enabled, but IP communication is not yet up and running.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Ready: The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept accounting attempts.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Dead (X seconds left): Accounting attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.</td>
</tr>
<tr>
<td>Round-trip time</td>
<td>radiusAccClientExtRoundTripTime</td>
<td>The time interval (measured in milliseconds) between the most recent Response and the Request that matched it from the RADIUS accounting server. The granularity of this measurement is 100 ms. A value of 0 ms indicates that there hasn't been round-trip communication with the server yet.</td>
</tr>
</tbody>
</table>

Buttons

The server select box determines which server is affected by clicking the buttons.
Auto-refresh: Check this box to enable an automatic refresh. Automatic refresh occurs every 3 seconds.
Refresh: Click to refresh the page immediately.
Clear: Clears the counters for the selected server. The "Pending Requests" counter will not be cleared by this operation.
5.7 TACACS+ Server Configuration

This page allows you to configure the TACACS+ servers.

<table>
<thead>
<tr>
<th>TACACS+ Server Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Global Configuration</strong></td>
</tr>
<tr>
<td><strong>Timeout</strong></td>
</tr>
<tr>
<td><strong>Deadtime</strong></td>
</tr>
<tr>
<td><strong>Key</strong></td>
</tr>
</tbody>
</table>

**Server Configuration**

- **Delete**
- **Hostname**
- **Port**
- **Timeout**
- **Key**

**Add New Entry**

**Save**

**Reset**

**Global Configuration**

These settings are common for all of the TACACS+ servers.

**Timeout**

Timeout is the number of seconds, in the range 1 to 1000, to wait for a reply from a TACACS+ server before it is considered to be dead.

**Deadtime**

Deadtime, which can be set to a number between 0 to 1440 minutes, is the period during which the switch will not send new requests to a server that has failed to respond to a previous request. This will stop the switch from continually trying to contact a server that it has already determined as dead.

Setting the Deadtime to a value greater than 0 (0) will enable this feature, but only if more than one server has been configured.

**Key**

The secret key - up to 63 characters long - shared between the TACACS+ server and the switch.
Server Configuration

The table has one row for each TACACS+ server and a number of columns, which are:

Delete
To delete a TACACS+ server entry, check this box. The entry will be deleted during the next Save.

Hostname
The IP address or hostname of the TACACS+ server.

Port
The TCP port to use on the TACACS+ server for authentication.

Timeout
This optional setting overrides the global timeout value. Leaving it blank will use the global timeout value.

Key
This optional setting overrides the global key. Leaving it blank will use the global key.

Add New Entry
Click “Add new entry” to add a new TACACS+ server. An empty row is added to the table, and the TACACS+ server can be configured as needed. Up to 5 servers are supported.
The “Delete” button can be used to undo the addition of the new server.

Buttons
Save: Click to save changes.
Reset: Click to undo any changes made locally and revert to previously saved values.
6.1 MAC Address Table

6.1.1 MAC Address Table Configuration

Aging Configuration

Disable Automatic Aging

Aging Time: 300 seconds

MAC Table Learning

Static MAC Table Configuration

Add New Static Entry

Save Reset
The MAC Address Table is configured on this page. Set timeouts for entries in the dynamic MAC Table and configure the static MAC table here.

**Aging Configuration**

By default, dynamic entries are removed from the MAC table after 300 seconds. This removal is also called aging.

Configure aging time by entering a value here in seconds; for example, Age time seconds.

"Aging time": the allowed range is 0.1 to 1 million seconds.

"Disable Auto Aging": disable the auto aging function of dynamic entries by checking Disable Auto Aging.

**MAC Table Learning**

If the learning mode for a given port is greyed out, another module is in control of the mode, so that it cannot be changed by the user. An example of such a module is the MAC-Based Authentication under 802.1X.

Each port can do learning based upon the following settings:

**Auto**

Learning is done automatically as soon as a frame with unknown SMAC is received.

**Disable**

No learning is done.

**Secure**

Only static MAC entries are learned, all other frames are dropped.

Notice:

Make sure that the link used for managing the switch is added to the Static Mac Table before changing to secure learning mode, otherwise the management link is lost and can only be restored by using another non-secure port or by connecting to the switch via the serial interface.

**Static MAC Table Configuration**

The static entries in the MAC table are shown in this table. The static MAC table can contain 64 entries.

The MAC table is sorted first by VLAN ID and then by MAC address.

**Delete**

Check to delete the entry. It will be deleted during the next save.

**VLAN ID**

The VLAN ID of the entry.
MAC Address
The MAC address of the entry.

Port Members
Checkmarks indicate which ports are members of the entry. Check or uncheck as needed to modify the entry.

Add New Static Entry
Click "add new static entry" to add a new MAC table entry. Specify the VLAN ID, MAC address, and port members for the new entry. Click "Apply".

Buttons
Save: Click to save changes.
Reset: Click to undo any changes made locally and revert to previously saved values.

6.1.2 MAC Address Table Monitoring
Entries in the MAC Table are shown on this page. The MAC Table contains up to 8192 entries, and is sorted first by VLAN ID, then by MAC address.

Each page shows up to 999 entries from the MAC table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the MAC Table. The first displayed will be the one with the lowest VLAN ID and the lowest MAC address found in the MAC Table.

The Start "MAC address" and "VLAN" input fields allow the user to select the starting point in the MAC Table. Clicking the "Refresh" button will update the displayed table starting from that or the closest next MAC Table match. In addition, the two input
fields will - upon a “Refresh” button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address. The “>>” button will use the last entry of the currently displayed entry as a basis for the next lookup. When the end is reached the text “No more entries” is shown in the displayed table. Use the “|<<” button to start over.

**MAC Address Table**

**Type**
Indicates whether the entry is a static or a dynamic entry.

**VLAN**
The VLAN ID of the entry.

**MAC Address**
The MAC address of the entry.

**Port Members**
The ports that are members of the entry.

**Buttons**
- **Auto-refresh**: Automatic refresh occurs every 3 seconds.
- **Refresh**: Refreshes the displayed table starting from the “Start from MAC address” and “VLAN” input fields.
- **Clear**: refresh all dynamic entries.
- **|<<**: Updates the table starting from the first entry in the MAC Table, i.e. the entry with the lowest VLAN ID and MAC address.
- **>>**: Updates the table, starting with the entry after the last entry currently displayed.

### 6.2 VLAN

### 6.2.1 VLAN

On this page, users can create VLAN and edit VLAN description.
VLAN
VLAN ID number, value range is 1-4094.

Description
Description information of VLAN.

Untagged Port
Untagged port member to conduct untagged process to sending data frame.

Tagged Port
Tag port member to conduct tagged process to sending data frame.

State
State type:
- Static;
- Dynamic.

Buttons
Add: click to add VLAN.
Delete: Click to delete the selected VLAN.

6.2.2 Access interface
On this page, users can configure the port VLAN mode (access, trunk, Hybrid), and port PVID.
Port

The corresponding port name of the device Ethernet port.

PVID

PVID value, it defaults to 1, value range is 1-4094. Each port has a PVID property, when the port receives Untag messages, it adds Tag mark on them according to PVID. When the port transmits data message with the same Tag mark as PVID, it would erase the Tag mark and then transmit the message. The PVID of all ports default to 1.

Buttons

Set: Click to configure the PVID of the selected port.
Mode: Click to configure the port mode of the selected port.

There are three port link types that the switch supports:
- Access: port only belongs to 1 VLAN(which is the default VLAN), all ports of the switch are Access mode by default and all PVID are 1.
- Trunk: port can belong to multiple VLANs, Trunk port can allow the messages of multiple VLANs to pass with Tag, but only allow the messages of one VLAN to transmit without tag (strip Tag) from this kind of interface. Commonly used in the connection between network devices.

- Hybrid: port can belong to multiple VLANs, Hybrid port allows messages of multiple VLANs to pass with tag, and allows the messages sent from this kind of interface to configure whether the messages of some VLANs is with tag (not strip Tag) or not (strip Tag). It could be used in the connection between network devices, as well as user devices.

If the port mode is set to Trunk or Hybrid, the port display will be updated to the tab corresponding to “Trunk” or “Hybrid”.

### 6.2.3 Trunk

On this page, user can configure the relevant parameters of Trunk port mode.

<table>
<thead>
<tr>
<th>VLAN</th>
<th>VLAN</th>
<th>Access</th>
<th>Trunk</th>
<th>Hybrid</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>Trunk set</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>SET</td>
<td>MODE</td>
</tr>
<tr>
<td>Port</td>
<td>PVID</td>
<td>Tag VLAN</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Port**

The corresponding port name of the device Ethernet port.

**PVID**

The PVID number of the port, ranging from 1-4094.

**TagVLAN**

VLAN ID number with TAG allowed by interface, a single value or range (“-“indicates the range). For example: 9 or 10-15.

**Buttons**

Set: Check the entries that need to be reconfigured, click "Set" to reset PVID value and TagVLAN parameters.
Mode: Click “Mode” to set the mode to Access or Hybrid. If the port mode is set to Access or Hybrid, the port display will be updated to the tab corresponding to Access or Hybrid.

6.2.4 Hybrid

On this page, user can configure the relevant parameters of Hybrid port mode.

<table>
<thead>
<tr>
<th>VLAN</th>
<th>Access</th>
<th>Trunk</th>
<th>Hybrid</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hybrid set</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Port**
The corresponding port name of the device Ethernet port.

**PVID**
The PVID number of the port, ranging from 1-4094.

**Untag Vlan**
The VLAN ID number that the port allows to pass without tags.

**Allow Vlan**
The VLAN ID number that the port allows to pass, a single value or range (the range is indicated by "-"). For example: 9 or 10-15.

**Egress Tagging**
Processing mode of Hybrid interface for marking of exit message;
- UntagPortVLAN:PVID is not tagged;
- TagAll: Tag all VLAN;
- UntagAll: Untag all VLAN.
### Process for Port Receiving Message

<table>
<thead>
<tr>
<th>Interface type</th>
<th>Process for Receiving Untagged Message</th>
<th>Process for Receiving Tagged Message</th>
</tr>
</thead>
</table>
| Access interface | Receive this message and tag it with default VLAN ID. | • Receive the message when the VLAN ID is the same as default VLAN ID.  
• Discard the message when the VLAN ID is different from the default VLAN ID. |
| Trunk | Receive this message and tag it with default VLAN ID. | • Receive this message when the VLAN ID is in the list of VLAN ID that allow to pass through the interface.  
• Discard this message when the VLAN ID is not in the list of VLAN ID that allow to pass through the interface. |
| Hybrid | | |

### Process for Port Sending Message

<table>
<thead>
<tr>
<th>Interface type</th>
<th>The process of transmit frame</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access interface</td>
<td>Strip the PVID Tag of the message first, then transmit it.</td>
</tr>
</tbody>
</table>
| Trunk | • When the VLAN ID is the same as the default VLAN ID, and it is the VLAN ID allowed to pass through the interface, it would strip the Tag and send this message.  
• When the VLAN ID is different from the default VLAN ID, and it’s the VLAN ID allowed to pass through the interface, it would remain its original Tag and send the message. |
| Hybrid | When the VLAN ID is the one allowed to pass through the interface, it would send this message. It could be set to whether to carry Tag during transmission. |
6.3 DHCP Server

6.3.1 Mode Setting

This page configures global mode and VLAN mode to enable/disable DHCP server per system and per VLAN.

Global Mode

Configure operation mode to enable/disable DHCP server per system.

Mode

Configure the operation mode per system. Possible modes are:
- Enabled: Enable DHCP server per system.
- Disabled: Disable DHCP server per system.

VLAN Mode

Configure operation mode to enable/disable DHCP server per VLAN.

VLAN Range

Indicate the VLAN range in which DHCP server is enabled or disabled. The first VLAN ID must be smaller than or equal to the second VLAN ID. BUT, if the VLAN range contains only 1 VLAN ID, then you can just input it into either one of the first and second VLAN ID or both.

On the other hand, if you want to disable existed VLAN range, then you can follow the steps.
1. Click “add VLAN range” to add a new VLAN range.
2. Input the VLAN range that you want to disable.
3. Choose Mode to be disabled.
4. Press "Apply" to apply the changes.
Then, you will see the disabled VLAN range is removed from the DHCP Server mode configuration page.

**Mode**

Indicate the operation mode per VLAN. Possible modes are:
- **Enabled**: Enable DHCP server per VLAN.
- **Disabled**: Disable DHCP server per VLAN.

**Buttons**

- Add VLAN range: click to add new VLAN range.
- Apply: Click to save changes.
- Reset: Click to undo any changes made locally and revert to previously saved values.

### 6.3.2 Reserve IP Address Configuration

This page configures excluded IP addresses. DHCP server will not allocate these excluded IP addresses to DHCP client.

#### Excluded IP Address

Configure excluded IP addresses.

#### IP Range

Define the IP range to be excluded IP addresses. The first excluded IP must be smaller than or equal to the second excluded IP. BUT, if the IP range contains only 1 excluded IP, then you can just input it to either one of the first and second excluded IP or both.

**Buttons**

- Add IP range: Click to add a new excluded IP range.
- Save: Click to save changes.
- Reset: Click to undo any changes made locally and revert to previously saved values.
6.3.3 DHCP Pool Configuration

This page manages DHCP pools. According to the DHCP pool, DHCP server will allocate IP address and deliver configuration parameters to DHCP client.

Pool Setting

Delete

Add or delete pools.
Adding a pool and giving a name is to create a new pool with "default" configuration. If you want to configure all settings including type, IP subnet mask and lease time, you can click the pool name to go into the configuration page.

Name

Configure the pool name that accepts all printable characters, except white space. If you want to configure the detail settings, you can click the pool name to go into the configuration page.

Type

Display which type of the pool is.
- Network: the pool defines a pool of IP addresses to service more than one DHCP client.
- Host: the pool services for a specific DHCP client identified by client identifier or hardware address.
If "-" is displayed, it means not defined.

IP

Display network number of the DHCP address pool.
If "-" is displayed, it means not defined.

Subnet Mask

Display subnet mask of the DHCP address pool.
If "-" is displayed, it means not defined.
Lease Time
Display lease time of the pool.

Buttons
Add new pool: click to add a DHCP pool.
Save: Click to save changes.
Reset: Click to undo any changes made locally and revert to previously saved values.

6.3.3.1 Add a new DHCP pool

This page configures all settings of a DHCP pool.
<table>
<thead>
<tr>
<th>Pool Name</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>IP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Subnet Mask</td>
<td></td>
<td>days (0-365)</td>
</tr>
<tr>
<td>Lease Time</td>
<td>0</td>
<td>hours (0-23)</td>
</tr>
<tr>
<td>Domain Name</td>
<td></td>
<td>minutes (0-59)</td>
</tr>
<tr>
<td>Broadcast Address</td>
<td>0.0.0.0</td>
<td></td>
</tr>
<tr>
<td>Default Router</td>
<td>0.0.0.0</td>
<td></td>
</tr>
<tr>
<td>DNS Server</td>
<td>0.0.0.0</td>
<td></td>
</tr>
<tr>
<td>NTP Server</td>
<td>0.0.0.0</td>
<td></td>
</tr>
</tbody>
</table>
### Pool
Select a pool to configure the settings.

### Name
Select a pool by pool name.

### Setting
Configure pool settings.
**Pool Name**

Display the selected pool name.

**Type**

Specify which type of the pool is.
- Network: the pool defines a pool of IP addresses to service more than one DHCP client.
- Host: the pool services for a specific DHCP client identified by client identifier or hardware address.

**IP**

Specify network number of the DHCP address pool.

**Subnet Mask**

DHCP option 1.
Specify subnet mask of the DHCP address pool.

**Lease Time**

DHCP option 51, 58 and 59.
Specified Lease Time. Allow the client to request a lease time for the IP address. If all are 0's, then it means the lease time is infinite.

**Domain Name**

DHCP option 15.
Specify domain name that client should use when resolving hostname via DNS.

**Broadcast Address**

DHCP option 28.
Specify the broadcast address in use on the client's subnet.

**Default Router**

DHCP option 3.
Specify a list of IP addresses for routers on the client's subnet.

**DNS Server**

DHCP option 6.
Specify a list of Domain Name System name servers available to the client.

**NTP Server**

DHCP option 42.
Specify a list of IP addresses indicating NTP servers available to the client.

**NetBIOS Node Type**

DHCP option 46.
Specify NetBIOS node type option to allow Netbios over TCP/IP clients which are configurable to be configured as described in RFC 1001/1002.

**NetBIOS Scope**

DHCP option 47.
Specify the NetBIOS over TCP/IP scope parameter for the client as specified in RFC 1001/1002.

**NetBIOS Name Server**

DHCP option 44.
Specify a list of NBNS name servers listed in order of preference.

**NIS Domain Name**

DHCP option 40.
Specify the name of the client's NIS domain.

**NIS Server**

DHCP option 41.
Specify a list of IP addresses indicating NIS servers available to the client.

**Client Identifier**

DHCP option 61.
Specify client's unique identifier to be used when the pool is the type of host.

**Hardware Address**

Specify client's hardware(MAC) address to be used when the pool is the type of host.

**Client Name**

DHCP option 12.
Specify the name of client to be used when the pool is the type of host.

**Vendor / Class Identifier**

DHCP option 60.
Specify to be used by DHCP client to optionally identify the vendor type and configuration of a DHCP client. DHCP server will deliver the corresponding option 43 specific information to the client that sends option 60 vendor class identifier.

**Vendor / Specific Information**

DHCP option 43.
Specify vendor specific information according to option 60 vendor class identifier.

**Buttons**

Save: Click to save changes.
Reset: Click to undo any changes made locally and revert to previously saved values.

6.3.4 Statistics Monitoring

DHCP Server Statistics
This page displays the database counters and the number of DHCP messages sent and received by DHCP server.

Database Counters
Display counters of various databases.

Pool
Number of pools.

Excluded IP Address
Number of excluded IP address ranges.

Declined IP Address
Number of declined IP addresses.

Binding Counters
Display counters of various databases.

Automatic Binding
Number of bindings with network-type pools.

Manual Binding
Number of bindings that administrator assigns an IP address to a client. That is, the pool is of host type.
Expired Binding
   Number of bindings that their lease time expired or they are cleared from Automatic/Manual type bindings.

DHCP Message Received Counters
   Display counters of DHCP messages received by DHCP server.

   DISCOVER
      Number of DHCP DISCOVER messages received.

   REQUEST
      Number of DHCP REQUEST messages received.

   DECLINE
      Number of DHCP DECLINE messages received.

   RELEASE
      Number of DHCP RELEASE messages received.

   INFORM
      Number of DHCP INFORM messages received.

DHCP Message Sent Counters
   Display counters of DHCP messages sent by DHCP server.

   OFFER
      Number of DHCP OFFER messages sent.

   ACK
      Number of DHCP ACK messages sent.

   NAK
      Number of DHCP NAK messages sent.

Buttons
   Save: Click to save changes.
   Undo: Click to undo any changes made locally and revert to previously saved values.

6.3.5 Binding Monitoring

DHCP Server Binding IP
   This page displays bindings generated for DHCP clients.
**Binding IP Address**

Display all bindings.

**IP**

IP address allocated to DHCP client.

**Type**

Type of binding. Possible types are Automatic, Manual, Expired.

**State**

State of binding. Possible states are Committed, Allocated, Expired.

**Pool Name**

The pool that generates the binding.

**Server ID**

Server IP address to service the binding.

**Buttons**

Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page immediately.

Clear selected: Click to clear selected bindings. If the selected binding is Automatic or Manual, then it is changed to be Expired. If the selected binding is Expired, then it is freed.

Clear Automatic: Click to clear all automatic bindings and change them to expired bindings.

Clear Manual: Click to clear all manual bindings and change them to expired bindings.

Clear Expired: Click to clear all expired bindings and free them.

### 6.3.6 Conflict Monitoring

This page displays declined IP addresses.
Declined IP Address
Display IP addresses declined by DHCP clients.

Declined IP
List of IP addresses declined.

Buttons
Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
Refresh: Click to refresh the page immediately.

6.4 DHCP Snooping

6.4.1 Snooping Configuration
Configure DHCP Snooping on this page.
### Snooping Mode

Indicates the DHCP snooping mode operation. Possible modes are:

- **Enabled**: Enable DHCP snooping mode operation. When DHCP snooping mode operation is enabled, the DHCP request messages will be forwarded to trusted ports and only allow reply packets from trusted ports.
- **Disabled**: Disable DHCP snooping mode operation.

### Port Mode Configuration

Indicates the DHCP snooping port mode. Possible port modes are:

- **Trusted**: Configures the port as trusted source of the DHCP messages.
- **Untrusted**: Configures the port as untrusted source of the DHCP messages.

### Buttons

- **Save**: Click to save changes.
- **Reset**: Click to undo any changes made locally and revert to previously saved values.

---

### Port Mode Configuration Table

<table>
<thead>
<tr>
<th>Port</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>&lt;&gt;</td>
</tr>
<tr>
<td>1</td>
<td>Trusted</td>
</tr>
<tr>
<td>2</td>
<td>Trusted</td>
</tr>
<tr>
<td>3</td>
<td>Trusted</td>
</tr>
<tr>
<td>4</td>
<td>Trusted</td>
</tr>
<tr>
<td>5</td>
<td>Trusted</td>
</tr>
<tr>
<td>6</td>
<td>Trusted</td>
</tr>
<tr>
<td>7</td>
<td>Trusted</td>
</tr>
<tr>
<td>8</td>
<td>Trusted</td>
</tr>
<tr>
<td>9</td>
<td>Trusted</td>
</tr>
<tr>
<td>10</td>
<td>Trusted</td>
</tr>
<tr>
<td>11</td>
<td>Trusted</td>
</tr>
<tr>
<td>12</td>
<td>Trusted</td>
</tr>
</tbody>
</table>
6.4.2 Snooping Table Monitor

This page display the dynamic IP assigned information after DHCP Snooping mode is disabled. All DHCP clients obtained the dynamic IP address from the DHCP server will be listed in this table except for local VLAN interface IP addresses. Entries in the Dynamic DHCP snooping Table are shown on this page.

<table>
<thead>
<tr>
<th>MAC Address</th>
<th>VLAN ID</th>
<th>Source Port</th>
<th>IP Address</th>
<th>IP Subnet Mask</th>
<th>DHCP Server</th>
</tr>
</thead>
</table>

Navigating the DHCP snooping Table

Each page shows up to 99 entries from the Dynamic DHCP snooping table, default being 20, selected through the "per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the Dynamic DHCP snooping Table.

The "MAC address" and "VLAN" input fields allows the user to select the starting point in the Dynamic DHCP snooping Table. Clicking the "Refresh" button will update the displayed table starting from that or the closest next Dynamic DHCP snooping Table match. In addition, the two input fields will - upon a "Refresh" button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

">>" will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the "<<" button to start over.

DHCP Snooping Table Columns

MAC Address
User MAC address of the entry.

VLAN ID
VLAN-ID in which the DHCP traffic is permitted.

Source Port
Switch Port Number for which the entries are displayed.

IP Address
User IP address of the entry.
**IP Subnet Mask**  
User IP subnet mask of the entry.

**DHCP Server**  
DHCP Server address of the entry.

**Buttons**  
Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.  
Refresh: Refresh the displayed table starting from the input fields.  
|<<: Updates the table starting from the first entry in the Dynamic DHCP snooping Table.  
|>>: Updates the table, starting with the entry after the last entry currently displayed.

### 6.5 DHCP Relay

#### 6.5.1 Relay Configuration

A DHCP relay agent is used to forward and to transfer DHCP messages between the clients and the server when they are not in the same subnet domain. It stores the incoming interface IP address in the GIADDR field of the DHCP packet. The DHCP server can use the value of GIADDR field to determine the assigned subnet. For such condition, please make sure the switch configuration of VLAN interface IP address and PVID (Port VLAN ID) correctly.

<table>
<thead>
<tr>
<th>DHCP Relay Configuration</th>
<th>Relay Configuration</th>
<th>Relay Statistics Monitor</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Relay Mode</strong></td>
<td>Disabled</td>
<td></td>
</tr>
<tr>
<td><strong>Relay Server</strong></td>
<td>0.0.0.0</td>
<td></td>
</tr>
<tr>
<td><strong>Relay Information Mode</strong></td>
<td>Disabled</td>
<td></td>
</tr>
<tr>
<td><strong>Relay Information Policy</strong></td>
<td>Keep</td>
<td></td>
</tr>
</tbody>
</table>

**Relay Mode**  
Indicates the DHCP relay mode operation. Possible modes are:
- **Enabled**: Enable DHCP relay mode operation. When DHCP relay mode operation is enabled, the agent forwards and transfers DHCP messages between the clients and the server when they are not in the same subnet domain. And the DHCP broadcast message won't be flooded for security considerations.
- **Disabled**: Disable DHCP relay mode operation.

**Relay Server**
Indicates the DHCP relay server IP address.

**Relay Information Mode**
Indicates the DHCP relay information mode option operation. The option 82 circuit ID format as "[vlan_id][module_id][port_no]". The first four characters represent the VLAN ID, the fifth and sixth characters are the module ID (in standalone device it always equal 0, in stackable device it means switch ID), and the last two characters are the port number. For example, "00030108" means the DHCP message receive form VLAN ID 3, switch ID 1, port No 8. And the option 82 remote ID value is equal the switch MAC address.

Possible modes are:
- **Enabled**: Enable DHCP relay information mode operation. When DHCP relay information mode operation is enabled, the agent inserts specific information (option 82) into a DHCP message when forwarding to DHCP server and removes it from a DHCP message when transferring to DHCP client. It only works when DHCP relay operation mode is enabled.
- **Disabled**: Disable DHCP relay information mode operation.

**Relay Information Policy**
Indicates the DHCP relay information option policy. When DHCP relay information mode operation is enabled, if the agent receives a DHCP message that already contains relay agent information it will enforce the policy. The 'Replace' policy is invalid when relay information mode is disabled. Possible policies are:
- **Replace**: Replace the original relay information when a DHCP message that already contains it is received.
- **Keep**: Keep the original relay information when a DHCP message that already contains it is received.
- **Drop**: Drop the package when a DHCP message that already contains relay information is received.

**Buttons**
Save: Click to save changes.
Reset: Click to undo any changes made locally and revert to previously saved values.

6.5.2 Relay Statistics Monitoring

This page provides statistics for DHCP relay.

Server Statistics
Transmit to Server
The number of packets that are relayed from client to server.

Transmit Error
The number of packets that resulted in errors while being sent to clients.

Receive from Server
The number of packets received from server.

Receive Missing Agent Option
The number of packets received without agent information options.

Receive Missing Circuit ID
The number of packets received with the Circuit ID option missing.

Receive Missing Remote ID
The number of packets received with the Remote ID option missing.

Receive Bad Circuit ID
The number of packets whose Circuit ID option did not match known circuit ID.

Receive Bad Remote ID
The number of packets whose Remote ID option did not match known Remote ID.

Client Statistics
Transmit to Client
The number of relayed packets from server to client.
**Transmit Error**

The number of packets that resulted in error while being sent to servers.

**Receive from Client**

The number of received packets from server.

**Receive Agent Option**

The number of received packets with relay agent information option.

**Replace Agent Option**

The number of packets which were replaced with relay agent information option.

**Keep Agent Option**

The number of packets whose relay agent information was retained.

**Drop Agent Option**

The number of packets that were dropped which were received with relay agent information.

**Buttons**

- **Auto-refresh**: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
- **Refresh**: Click to refresh the page immediately.
- **Clear**: Clear all statistics.

**6.6 DHCP Detailed Statistics**

This page provides statistics for DHCP snooping. Notice that the normal forward per-port TX statistics isn't increased if the incoming DHCP packet is done by L3 forwarding mechanism. And clear the statistics on specific port may not take effect on global statistics since it gathers the different layer overview.
### Receive and Transmit Packets

#### Rx and Tx Discover
Number of Discover (option 53 with a value of 1) packets received and sent.

#### Rx and Tx Offer
Number of offer (option 53, value 2) packets received and sent.

#### Rx and Tx Request
Number of requests received and sent (option 53, value 3)

#### Rx and Tx Decline
Number of falling packets (option 53, value 4) received and sent.

#### Rx and Tx ACK
Number of ACK (option 53 with a value of 5) packets received and sent.

#### Rx and Tx NAK
Number of NAK (option 53 with a value of 6) packets received and sent.

#### Rx and Tx Release
Number of release packets received and sent (option 53, value 7).

#### Rx and Tx Inform
Number of information packets received and sent (option 53, value 8).

#### Rx and Tx Lease Query
Number of lease request packages received and sent (option 53, value 10).

#### Rx and Tx Lease Unassigned
Number of unallocated lease received and sent (option 53, value 11).

#### Rx and Tx Lease Unknown
Unknown number of leases received and sent (option 53, value 12).
Rx and Tx Lease Active
Number of lease activity packages received and sent (option 53 with a value of 13).

Rx Discarded Checksum Error
The number of discard packet that IP/UDP checksum is error.

Rx Discarded from Untrusted
The number of discarded packet that are coming from untrusted port.

Buttons
The DHCP user select box determines which user is affected by clicking the buttons.
The port select box determines which port is affected by clicking the buttons.
Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
Refresh: Click to refresh the page immediately.
Clear: clear the counters of all ports.

6.7 LLDP

6.7.1 LLDP Configuration
This page allows the user to inspect and configure the current LLDP interface settings.
LLDP Parameters

Tx Interval

The switch periodically transmits LLDP frames to its neighbors for having the network discovery information up-to-date. The interval between each LLDP frame is determined by the Tx Interval value. Valid values are restricted to 5 - 32768 seconds.

Tx Hold

Each LLDP frame contains information about how long time the information in the LLDP frame shall be considered valid. The LLDP information valid period is set to Tx Hold multiplied by Tx Interval seconds. Valid values are restricted to 2 - 10 times.

Tx Delay

If some configuration is changed (e.g. the IP address) a new LLDP frame is transmitted, but the time between the LLDP frames will always be at least the value of Tx Delay seconds. Tx Delay cannot be larger than 1/4 of the Tx Interval value. Valid values are restricted to 1 - 8192 seconds.
**Tx Reinit**

When a interface is disabled, LLDP is disabled or the switch is rebooted, a LLDP shutdown frame is transmitted to the neighboring units, signaling that the LLDP information isn't valid anymore. Tx Reinit controls the amount of seconds between the shutdown frame and a new LLDP initialization. Valid values are restricted to 1 - 10 seconds.

**LLDP Interface Configuration**

**Interface**

The switch interface name of the logical LLDP interface.

**Mode**

Select LLDP mode.
- Rx only: The switch will not send out LLDP information, but LLDP information from neighbor units is analyzed.
- Tx only: The switch will drop LLDP information received from neighbors, but will send out LLDP information.
- Disabled: The switch will not send out LLDP information, and will drop LLDP information received from neighbors.
- Tx and Rx: The switch will send out LLDP information, and will analyze LLDP information received from neighbors.

**CDP Aware**

Select CDP awareness.

The CDP operation is restricted to decoding incoming CDP frames (The switch doesn't transmit CDP frames). CDP frames are only decoded if LLDP on the interface is enabled.

Only CDP TLVs that can be mapped to a corresponding field in the LLDP neighbors' table are decoded. All other TLVs are discarded (Unrecognized CDP TLVs and discarded CDP frames are not shown in the LLDP statistics.). CDP TLVs are mapped onto LLDP neighbors' table as shown below.

- CDP TLV "Device ID" is mapped to the LLDP "Chassis ID" field.
- CDP TLV "Address" is mapped to the LLDP "Management Address" field. The CDP address TLV can contain multiple addresses, but only the first address is shown in the LLDP neighbors table.
- CDP TLV "Port ID" is mapped to the LLDP "Port ID" field.
- CDP TLV "Version and Platform" is mapped to the LLDP "System Description" field.
Both the CDP and LLDP support "system capabilities", but the CDP capabilities cover capabilities that are not part of the LLDP. These capabilities are shown as "others" in the LLDP neighbors' table.

If all interfaces have CDP awareness disabled the switch forwards CDP frames received from neighbor devices. If at least one interface has CDP awareness enabled all CDP frames are terminated by the switch.

Note:
When CDP awareness on an interface is disabled the CDP information isn't removed immediately, but gets removed when the hold time is exceeded.

**Port Descr**
Optional TLV: When checked the "port description" is included in LLDP information transmitted.

**System Name**
Optional TLV: When checked the "system name" is included in LLDP information transmitted.

**System Description**
Optional TLV: When checked the "system description" is included in LLDP information transmitted.

**System Capabilities**
Optional TLV: When checked the "system capability" is included in LLDP information transmitted.

**Management Address**
Optional TLV: When checked the "management address" is included in LLDP information transmitted.

**Buttons**
Save: Click to save changes.
Reset: Click to undo any changes made locally and revert to previously saved values.

### 6.7.2 LLDP Neighbor Information

This page provides a status overview for all LLDP neighbors. The displayed table contains a row for each interface on which an LLDP neighbor is detected. The columns hold the following information:
Local interface
The interface on which the LLDP frame was received.

Chassis ID
The chassis ID is the identification of the neighbor LLDP frame.

Port ID
The port ID is the identification of the neighbor port.

Port Description
Port Description is the port description advertised by the neighbor unit.

System Name
System Name is the name advertised by the neighbor unit.

System Capabilities
System Capabilities describes the neighbor unit's capabilities. The possible capabilities are:
- 1other
- 2Repeater
- 3Bridge
- 4Wireless network node
- 5Router
- 6Telephone
- 7DOCSIS cable device
- 8Station only
- 9Reserved
When a function is enabled, the function is followed by (+). If the function is disabled, the function is followed by (-).

Management Address
Management Address is the neighbor unit's address that is used for higher layer entities to assist discovery by the network management. This could for instance hold the neighbor's IP address.
Buttons

Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
Refresh: Click to refresh the page.

6.7.3 PoE Monitoring

This page provides a status overview for all LLDP PoE neighbors. The displayed table contains a row for each interface on which an LLDP PoE neighbor is detected. The columns hold the following information:

Local interface
The interface for this switch on which the LLDP frame was received.

Power Type
The Power Type represents whether the device is a Power Sourcing Entity (PSE) or Power Device (PD).
If the Power Type is unknown it is represented as "Reserved".

Energy Source
The Power Source represents the power source being utilized by a PSE or PD device.
If the device is a PSE device it can either run on its Primary Power Source or its Backup Power Source. If it is unknown whether the PSE device is using its Primary Power Source or its Backup Power Source it is indicated as "Unknown"
If the device is a PD device it can either run on its local power supply or it can use the PSE as power source. It can also use both its local power supply and the PSE.
If it is unknown what power supply the PD device is using it is indicated as "Unknown"

Power Priority
Power Power Priority represents the priority of the PD device, or the power priority associated with the PSE type device’s interface that is sourcing the power. There are three levels of power priority. The three levels are: Critical, High and Low.
If the power priority is unknown it is indicated as "Unknown"
Maximum Power
The Maximum Power Value contains a numerical value that indicates the maximum power in watts required by a PD device from a PSE device, or the minimum power a PSE device is capable of sourcing over a maximum length cable based on its current configuration.
The maximum allowed value is 102.3 W. If the device indicates value higher than 102.3 W, it is represented as "reserved"

Buttons
Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
Refresh: Click to refresh the page.

6.7.4 Port Statistics Monitoring
This page provides an overview of all LLDP traffic.
Two types of counters are shown. Global counters are counters that refer to the whole switch, while local counters refer to per interface counters for the currently selected switch.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Global Counters</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Clear global counters</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Neighbor entries were last changed</td>
<td>1970-01-01T00:00:00+00:00 (30549 secs ago)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Total Neighbors Entries Added</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Total Neighbors Entries Deleted</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Total Neighbors Entries Dropped</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Total Neighbors Entries Aged Out</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>LLDP Statistics: Local Counters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local Interface</td>
</tr>
<tr>
<td>-----------------</td>
</tr>
<tr>
<td>GigabitEthernet 1/1</td>
</tr>
<tr>
<td>GigabitEthernet 1/2</td>
</tr>
<tr>
<td>GigabitEthernet 1/3</td>
</tr>
<tr>
<td>GigabitEthernet 1/4</td>
</tr>
<tr>
<td>GigabitEthernet 1/5</td>
</tr>
<tr>
<td>GigabitEthernet 1/6</td>
</tr>
<tr>
<td>GigabitEthernet 1/7</td>
</tr>
<tr>
<td>GigabitEthernet 1/8</td>
</tr>
<tr>
<td>GigabitEthernet 1/9</td>
</tr>
<tr>
<td>2.5GigabitEthernet 1/10</td>
</tr>
<tr>
<td>GigabitEthernet 1/11</td>
</tr>
<tr>
<td>GigabitEthernet 1/12</td>
</tr>
</tbody>
</table>
Global Counter

Clear global counters
If checked the global counters are cleared when “Clear” is clicked.

Neighbor entries were last changed
Shows the time when the last entry was last deleted or added. It also shows the time elapsed since the last change was detected.

Total Neighbors Entries Added
Shows the number of new entries added since switch reboot.

Total Neighbors Entries Deleted
Shows the number of new entries deleted since switch reboot.

Total Neighbors Entries Dropped
Shows the number of LLDP frames dropped due to the entry table being full.

Total Neighbors Entries Aged Out
Shows the number of entries deleted due to Time-To-Live expiring.

LLDP Statistics Local Counter
The displayed table contains a row for each interface. The columns hold the following information:

Local Interface
The interface on which LLDP frames are received or transmitted.

Tx Frames
The number of LLDP frames transmitted on the interface.

Rx Frames
The number of LLDP frames received on the interface.

Rx Errors
The number of received LLDP frames containing some kind of error.

Frames Discarded
If a LLDP frame is received on a interface, and the switch's internal table has run full, the LLDP frame is counted and discarded. This situation is known as "Too Many Neighbors" in the LLDP standard. LLDP frames require a new entry in the table when the Chassis ID or Remote Port ID is not already contained within the table. Entries are removed from the table when a given interface's link is down, an LLDP shutdown frame is received, or when the entry ages out.
**TLVs Discarded**
Each LLDP frame can contain multiple pieces of information, known as TLVs (TLV is short for “Type Length Value”). If a TLV is malformed, it is counted and discarded.

**TLVs Unrecognized**
The number of well-formed TLVs, but with an unknown type value.

**Org. Discarded**
If LLDP frame is received with an organizationally TLV, but the TLV is not supported the TLV is discarded and counted.

**Age-Outs**
Each LLDP frame contains information about how long time the LLDP information is valid (age-out time). If no new LLDP frame is received within the age out time, the LLDP information is removed, and the Age-Out counter is incremented.

**Clear**
If checked the counters for the specific interface are cleared when “Clear” is clicked.

**Buttons**
Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
Refresh: Click to refresh the page.
Clear: Clear the counters which have the corresponding checkbox checked.

### 6.8 Storm Suppression
Global storm policers for the switch are configured on this page.
There is a unicast storm policer, multicast storm policer, and a broadcast storm policer.
These only affect flooding frames, that is, (VLAN ID, DMAC) paired frames do not exist in the MAC address table.
The displayed settings are:
Frame Type

The frame type for which the configuration below applies.

Enable

Enable or disable the global storm policer for the given frame type.

Rate

Controls the rate for the global storm policer. This value is restricted to 1-1024000 when "Unit" is fps, and 1-1024 when "Unit" is kfps. The rate is internally rounded up to the nearest value supported by the global storm policer.

Unit

Controls the unit of measure for the global storm policer rate as fps or kfps.

Buttons

Save: Click to save changes.
Reset: Click to undo any changes made locally and revert to previously saved values.

6.9 Loop Protection

6.9.1 Loop Protection Configuration

This page allows the user to inspect the current Loop Protection configurations, and possibly change them as well.
General Settings

Enable Loop Protection
Controls whether loop protections is enabled (as a whole).

Transmission Time
The interval between each loop protection PDU sent on each port. Valid values are 1 to 10 seconds. Default value is 5 seconds.

Shutdown Time
The period (in seconds) for which a port will be kept disabled in the event of a loop is detected (and the port action shuts down the port). Valid values are 0 to 604800
seconds (7 days). A value of zero will keep a port disabled (until next device restart). Default value is 180 seconds.

**Port Configuration**

**Port**

The switch port number.

**Enable**

Controls whether loop protection is enabled on this switch port.

**Action**

Configures the action performed when a loop is detected on a port. Valid values are
- Shutdown Port
- Shutdown Port and Log
- Log Only

**Tx Mode**

Controls whether the port is actively generating loop protection PDU's, or whether it is just passively looking for looped PDU's.

**Buttons**

Save: Click to save changes.
Reset: Click to undo any changes made locally and revert to previously saved values.

### 6.9.2 Loop Protection Status

This page displays the loop protection port status the ports of the switch.

Loop protection port status is:

<table>
<thead>
<tr>
<th>Port</th>
<th>Action</th>
<th>Tx Mode</th>
<th>Loops</th>
<th>Status</th>
<th>Loop</th>
<th>Time of Last Loop</th>
</tr>
</thead>
</table>

**Port**

The switch port number of the logical port.

**Action**

The currently configured port action.

**Tx Mode**

Status of port active protection.
Loops
   The number of loops detected on this port.

Status
   The current loop protection status of the port.

Loop
   Whether a loop is currently detected on the port.

Time of Last Loop
   The time of the last loop event detected.

Buttons
   Refresh: Click to refresh the page immediately.
   Auto-refresh: Check this box to enable an automatic refresh of the page at regular intervals.

6.10 Static Aggregation

6.10.1 Static Link Aggregation Mode Configuration
   This page is used to configure the aggregation mode and the aggregation group.
Hash Code Contributors

Source MAC Address

The Source MAC address can be used to calculate the destination port for the frame. Check to enable the use of the Source MAC address, or uncheck to disable. By default, Source MAC Address is enabled.

Destination MAC Address

The Destination MAC Address can be used to calculate the destination port for the frame. Check to enable the use of the Destination MAC Address, or uncheck to disable. By default, Destination MAC Address is disabled.

IP Address

The IP address can be used to calculate the destination port for the frame. Check to enable the use of the IP Address, or uncheck to disable. By default, IP Address is enabled.
TCP/UDP Port Number

The TCP/UDP port number can be used to calculate the destination port for the frame. Check to enable the use of the TCP/UDP Port Number, or uncheck to disable. By default, TCP/UDP Port Number is enabled.

Aggregation Group Configuration

Group ID

Indicates the group ID for the settings contained in the same row. Group ID "Normal" indicates there is no aggregation. Only one group ID is valid per port.

Port Members

Each switch port is listed for each group ID. Select a radio button to include a port in an aggregation, or clear the radio button to remove the port from the aggregation. By default, no ports belong to any aggregation group. Only full duplex ports can join an aggregation and ports must be in the same speed in each group.

Buttons

Save: Click to save changes.
Reset: Click to undo any changes made locally and revert to previously saved values.

6.10.2 Link Aggregation Status Monitoring

This page is used to see the status of ports in Aggregation group.

Aggregation Group Status

Aggr ID

The Aggregation ID associated with this aggregation instance.

Name

Name of the Aggregation group ID.

Type

Type of the Aggregation group(Static or LACP).

Speed

Speed of the Aggregation group.
Configured Ports
Configured member ports of the Aggregation group.

Aggregated Ports
Aggregated member ports of the Aggregation group.

Buttons
Refresh: Click to refresh the page immediately.
Auto-refresh: Automatic refresh occurs every 3 seconds.

6.11 LACP

6.11.1 LACP Configuration

This page allows the user to inspect the current LACP port configurations, and possibly change them as well.

<table>
<thead>
<tr>
<th>Port</th>
<th>LACP Enabled</th>
<th>Key</th>
<th>Role</th>
<th>Timeout</th>
<th>Prio</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Auto</td>
<td>Active</td>
<td>Fast</td>
<td>32768</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Auto</td>
<td>Active</td>
<td>Fast</td>
<td>32768</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Auto</td>
<td>Active</td>
<td>Fast</td>
<td>32768</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Auto</td>
<td>Active</td>
<td>Fast</td>
<td>32768</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Auto</td>
<td>Active</td>
<td>Fast</td>
<td>32768</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Auto</td>
<td>Active</td>
<td>Fast</td>
<td>32768</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Auto</td>
<td>Active</td>
<td>Fast</td>
<td>32768</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Auto</td>
<td>Active</td>
<td>Fast</td>
<td>32768</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>Auto</td>
<td>Active</td>
<td>Fast</td>
<td>32768</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>Auto</td>
<td>Active</td>
<td>Fast</td>
<td>32768</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>Auto</td>
<td>Active</td>
<td>Fast</td>
<td>32768</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>Auto</td>
<td>Active</td>
<td>Fast</td>
<td>32768</td>
<td></td>
</tr>
</tbody>
</table>

Port
The switch port number.

LACP Enabled
Controls whether LACP is enabled on this switch port. LACP will form an aggregation when 2 or more ports are connected to the same partner.
**Key**

The Key value incurred by the port, range 1-65535. The Auto setting will set the key as appropriate by the physical link speed, 10Mb=1, 100mb=2, 1gb=3. Using the Specific setting, a user-defined value can be entered. Ports with the same Key value can participate in the same aggregation group, while ports with different keys cannot.

**Role**

The Role shows the LACP activity status. The Active will transmit LACP packets each second, while Passive will wait for a LACP packet from a partner (speak if spoken to).

**Timeout**

The Timeout controls the period between BPDU transmissions. Fast will transmit LACP packets each second, while Slow will wait for 30 seconds before sending a LACP packet.

**Prio**

The priority of the control port, range 1-65535. If the LACP partner wants to form a larger group than is supported by this device then this parameter will control which ports will be active and which ports will be in a backup role. Lower number means greater priority.

**Buttons**

Save: Click to save changes.
Reset: Click to undo any changes made locally and revert to previously saved values.

### 6.11.2 System Status Monitoring

This page provides a status overview for all LACP instances.

#### Aggr ID

The Aggregation ID associated with this aggregation instance. For LLAG, id is shown as ‘isid:aggr-id’ and for GLAGs as ‘aggr-id’.
**Partner System ID**

The system ID (MAC address) of the aggregation partner.

**Partner Key**

The key that the partner has assigned to this aggregation ID.

**Partner Prio**

Port priority of aggregation partner.

**Last Changed**

The time since this aggregation changed.

**Local Ports**

Shows which ports are a part of this aggregation for this switch.

**Buttons**

Refresh: Click to refresh the page immediately.  
Auto-refresh: Automatic refresh occurs every 3 seconds.

### 6.11.3 Port State Monitoring

This page provides a status overview for LACP status for all ports.

<table>
<thead>
<tr>
<th>Port</th>
<th>LACP</th>
<th>Key</th>
<th>Aggr ID</th>
<th>Partner System ID</th>
<th>Partner Port</th>
<th>Partner Prio</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>No</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>2</td>
<td>No</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>3</td>
<td>No</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>4</td>
<td>No</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>5</td>
<td>No</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>6</td>
<td>No</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>7</td>
<td>No</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>8</td>
<td>No</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>9</td>
<td>No</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>10</td>
<td>No</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>11</td>
<td>No</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>12</td>
<td>No</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

**Port**

The switch port number.

**LACP**

‘Yes’ means that LACP is enabled and the port link is up. ‘No’ means that LACP is not enabled or that the port link is down. ‘Backup’ means that the port could not join the aggregation group but will join if other port leaves. Meanwhile it’s LACP status is disabled.
**Key**

The key assigned to this port. Only ports with the same key can aggregate together.

**Aggr ID**

The Aggregation ID assigned to this aggregation group.

**Partner System ID**

The system ID (MAC address) of the partner.

**Partner Port**

The partner's port number connected to this port.

**Partner Prio**

The partner's port priority.

**Buttons**

- Refresh: Click to refresh the page immediately.
- Auto-refresh: Automatic refresh occurs every 3 seconds.

### 6.11.4 Port Statistics Monitoring

This page provides an overview for LACP statistics for all ports.

<table>
<thead>
<tr>
<th>Port</th>
<th>LACP Received</th>
<th>LACP Transmitted</th>
<th>Discarded</th>
<th>Unknown</th>
<th>Illegal</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>5</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>6</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>7</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>8</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>9</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>10</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>11</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>12</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

**Port**

The switch port number.

**LACP Received**

Shows how many LACP frames have been received at each port.

**LACP Transmitted**

Shows how many LACP frames have been sent from each port.
Discarded

Shows how many unknown or illegal LACP frames have been discarded at each port.

Buttons

Auto-refresh: Automatic refresh occurs every 3 seconds.
Refresh: Click to refresh the page immediately.
Clear: Clears the counters for all ports.

6.12 Spanning Tree

6.12.1 Bridge Setting Configuration

This page allows you to configure STP system settings. The settings are used by all STP Bridge instances in the Switch.

Basic Settings

Protocol Version

The MSTP/RSTP/STP protocol version setting. Valid values are STP, RSTP and MSTP.

Bridge Priority

Controls the bridge priority. Lower numeric values have better priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch forms a Bridge Identifier.
For MSTP operation, this is the priority of the CIST. Otherwise, this is the priority of the STP/RSTP bridge.
Hello Time
The interval between sending STP BPDU's. Valid values are in the range 1 to 10 seconds, default is 2 seconds.

Note
Changing this parameter from the default value is not recommended, and may have adverse effects on your network.

Forward Delay
The delay used by STP Bridges to transit Root and Designated Ports to Forwarding (used in STP compatible mode). Valid values are in the range 4 to 30 seconds.

Max Age
The maximum age of the information transmitted by the Bridge when it is the Root Bridge. Valid values are in the range 6 to 40 seconds, and MaxAge must be <= (FwdDelay-1)*2.

Maximum Hop Count
This defines the initial value of remaining Hops for MSTI information generated at the boundary of an MSTI region. It defines how many bridges a root bridge can distribute its BPDU information to. Valid values are in the range 6 to 40 hops.

Transmit Hold Count
The number of BPDU's a bridge port can send per second. When exceeded, transmission of the next BPDU will be delayed. Valid values are in the range 1 to 10 BPDU's per second.

Advanced Settings

Edge Port BPDU Filtering
Control whether a port explicitly configured as Edge will transmit and receive BPDUs.

Edge Port BPDU Guard
Control whether a port explicitly configured as Edge will disable itself upon reception of a BPDU. The port will enter the error-disabled state, and will be removed from the active topology.

Port Error Recovery
Control whether a port in the error-disabled state automatically will be enabled after a certain time. If recovery is not enabled, ports have to be disabled and re-enabled for normal STP operation. The condition is also cleared by a system reboot.
Port Error Recovery Timeout

The time to pass before a port in the error-disabled state can be enabled. Valid values are between 30 and 86400 seconds (24 hours).

Buttons

Save: Click to save changes.
Reset: Click to undo any changes made locally and revert to previously saved values.

6.12.2 MSTI Mapping Configuration

This page allows the user to inspect the current STP MSTI bridge instance priority configurations, and possibly change them as well.

![Configuration Identification](image)

Configuration Identification

Configuration Name

The name identifying the VLAN to MSTI mapping. Bridges must share the name and revision (see below), as well as the VLAN-to-MSTI mapping configuration in order to share spanning trees for MSTI's (Intra-region). The name is at most 32 characters.

Configuration Revision

The revision of the MSTI configuration named above. This must be an integer between 0 and 65535.
MSTI Mapping

MSTI

The Bridge Instance. The CIST is not available for explicit mapping, as it will receive the VLANs not explicitly mapped.

VLANs Mapped

The list of VLANs mapped to the MSTI. The VLANs can be given as a single (xx, xx being between 1 and 4094) VLAN, or a range (xx-yy), each of which must be separated with comma and/or space. A VLAN can only be mapped to one MSTI. An unused MSTI should just be left empty. (I.e. not having any VLANs mapped to it.) Example: 2, 5, 20-40.

Buttons

Save: Click to save changes.
Reset: Click to undo any changes made locally and revert to previously saved values.

6.12.3 MSTI Priority Configuration

This page allows the user to inspect the current STP MSTI bridge instance priority configurations, and possibly change them as well.

MSTI

The Bridge Instance. The CIST is the default instance, which is always active.

Priority

Controls the bridge priority. Lower numeric values have better priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch forms a Bridge Identifier.

Buttons

Save: Click to save changes.
Reset: Click to undo any changes made locally and revert to previously saved values.

6.12.4 CIST Port Configuration

This page allows the user to inspect the current STP CIST port configurations, and possibly change them as well.

This page contains settings for physical and aggregated ports.

Port

The switch port number.

STP Enabled

Controls whether STP is enabled on this switch port.

Path Cost

Controls the path cost incurred by the port. The Auto setting will set the path cost as appropriate by the physical link speed, using the 802.1D recommended values. Using the Specific setting, a user-defined value can be entered. The path cost is used when establishing the active topology of the network. Lower path cost ports are chosen as forwarding ports in favour of higher path cost ports. Valid values are in the range 1 to 20000000.

Priority

Controls the port priority. This can be used to control priority of ports having identical port cost.
Admin Edge
Controls whether the operEdge flag should start as set or cleared. (The initial operation edge state when a port is initialized).

Auto Edge
Controls whether the bridge should enable automatic edge detection on the bridge port. This allows operEdge to be derived from whether BPDU's are received on the port or not.

Restricted Role
If enabled, causes the port not to be selected as 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. If set, it can cause lack of spanning tree connectivity. It can be set by a network administrator to prevent bridges external to a core region of the network influence the spanning tree active topology, possibly because those bridges are not under the full control of the administrator. This feature is also known as Root Guard.

Restricted TCN
If enabled, 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 persistently incorrect learned station location information. It is set by a network administrator to prevent bridges external to a core region of the network, causing address flushing in that region, possibly because those bridges are not under the full control of the administrator or the physical link state of the attached LANs transits frequently.

BPDU Guard
If enabled, causes the port to disable itself upon receiving valid BPDU's. Contrary to the similar bridge setting, the port Edge status does not effect this setting. A port entering error-disabled state due to this setting is subject to the bridge Port Error Recovery setting as well.

Point-to-Point
Controls whether the port connects to a point-to-point LAN rather than to a shared medium. This can be automatically determined, or forced either true or false. Transition to the forwarding state is faster for point-to-point LANs than for shared media.

Buttons
Save: Click to save changes.
Reset: Click to undo any changes made locally and revert to previously saved values.

### 6.12.5 MSTI port configuration

This page allows the user to inspect the current STP MSTI port configurations, and possibly change them as well. An MSTI port is a virtual port, which is instantiated separately for each active CIST (physical) port for each MSTI instance configured on and applicable to the port. The MSTI instance must be selected before displaying actual MSTI port configuration options. This page contains MSTI port settings for physical and aggregated ports.

<table>
<thead>
<tr>
<th>Port</th>
<th>The switch port number of the corresponding STP CIST (and MSTI) port.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Path Cost</td>
<td>Controls the path cost incurred by the port. The Auto setting will set the path cost as appropriate by the physical link speed, using the 802.1D recommended values. Using the Specific setting, a user-defined value can be entered. The path cost is used when establishing the active topology of the network. Lower path cost ports are chosen as forwarding ports in favour of higher path cost ports. Valid values are in the range 1 to 200000000.</td>
</tr>
<tr>
<td>Priority</td>
<td>Controls the port priority. This can be used to control priority of ports having identical port cost. (See above).</td>
</tr>
</tbody>
</table>

**Buttons**

- **Get**: Click to retrieve settings for a specific MSTI.
- **Save**: Click to save changes.
- **Reset**: Click to undo any changes made locally and revert to previously saved values.
6.12.6 Bridge Status Monitoring

This page provides a status overview of all STP bridge instances. The displayed table contains a row for each STP bridge instance, where the column displays the following information:

<table>
<thead>
<tr>
<th>MSTI</th>
<th>Bridge ID</th>
<th>Root ID</th>
<th>Root Port</th>
<th>Root Cost</th>
<th>Topology Flag</th>
<th>Topology Change Last Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Bridge Instance. This is also a link to the STP Detailed Bridge Status.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The Bridge ID of this Bridge instance.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The Bridge ID of the currently elected root bridge.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The switch port currently assigned the root port role.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Root Path Cost. For the Root Bridge this is zero. For all other Bridges, it is the sum of the Port Path Costs on the least cost path to the Root Bridge.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The current state of the Topology Change Flag of this Bridge instance.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The time since last Topology Change occurred.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Buttons**

- **Refresh**: Click to refresh the page immediately.
- **Auto-refresh**: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
**STP Bridge Status**

**Bridge Instance**
Bridge Instance - CIST, MST1, ......

**Bridge ID**
The Bridge ID of this Bridge instance.

**Root ID**
The Bridge ID of the currently elected root bridge.

**Root Cost**
Root Path Cost. For the Root Bridge this is zero. For all other Bridges, it is the sum of the Port Path Costs on the least cost path to the Root Bridge.

**Root Port**
The switch port currently assigned the root port role.

**Regional Root**
The Bridge ID of the currently elected regional root bridge, inside the MSTP region of this bridge. (For the CIST instance only).

**Internal Root Cost**
The Regional Root Path Cost. For the Regional Root Bridge this is zero. For all other CIST instances in the same MSTP region, it is the sum of the Internal Port Path Costs on the least cost path to the Internal Root Bridge. (For the CIST instance only).

**Topology Flag**
The current state of the Topology Change Flag of this Bridge instance.

**Topology Change Count**
The number of times where the topology change flag has been set (during a one-second interval).

**Topology Change Last Time**
The time passed since the Topology Flag was last set.

**CSTI Ports & Sggregation State**

**Port**
The switch port number.

**Port ID**
The port id as used by the STP protocol. This is the priority part and the logical port index of the bridge port.
Role
The current STP port role. The port role can be one of the following values: Alternate Port, Backup Port, Root Port, Designated Port.

State
The current STP port state. The port state can be one of the following values: Discarding Learning Forwarding.

Path Cost
The current STP port path cost. This will either be a value computed from the Auto setting, or any explicitly configured value.

Edge
The current STP port (operational) Edge Flag. An Edge Port is a switch port to which no Bridges are attached. The flag may be automatically computed or explicitly configured. Each Edge Port transits directly to the Forwarding Port State, since there is no possibility of it participating in a loop.

Point-to-Point
The current STP port point-to-point flag. A point-to-point port connects to a non-shared LAN media. The flag may be automatically computed or explicitly configured. The point-to-point properties of a port affect how fast it can transit to STP state.

Uptime
The time since the bridge port was last initialized.

Buttons
Refresh: Click to refresh the page immediately.
Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

6.12.7 Port State Monitoring
This page displays the STP CIST port status for physical ports of the switch. STP port state:
Port
The switch port number.

CIST Role
The current STP port role of the CIST port. The port role can be one of the following values: AlternatePort BackupPort RootPort DesignatedPort Disabled.

CIST State
The current STP port state of the CIST port. The port state can be one of the following values: Discarding Learning Forwarding.

Uptime
The time since the bridge port was last initialized.

Buttons
Refresh: Click to refresh the page immediately.
Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

6.12.8 Port Statistics Monitoring

This page displays the STP port statistics counters of bridge ports in the switch.
The STP port statistics counters are:

<table>
<thead>
<tr>
<th>Port</th>
<th>MSTP</th>
<th>RSTP</th>
<th>STP</th>
<th>TCN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>Number</td>
<td>Number</td>
<td>Number</td>
<td>Number</td>
</tr>
</tbody>
</table>

Port
The switch port number.

MSTP
The number of MSTP BPDU's received/transmitted on the port.

RSTP
The number of RSTP BPDU's received/transmitted on the port.

STP
The number of legacy STP Configuration BPDU's received/transmitted on the port.

TCN
The number of (legacy) Topology Change Notification BPDU's received/transmitted on the port.
Discarded Unknown
The number of unknown Spanning Tree BPDU's received (and discarded) on the port.

Discarded Illegal
The number of illegal Spanning Tree BPDU's received (and discarded) on the port.

Buttons
Refresh: Click to refresh the page immediately.
Clear: click to reset the counts.
Auto-refresh: Check this box to enable an automatic refresh. Automatic refresh occurs every 3 seconds.

6.13 Ring

6.13.1 Ring Configuration
This page provides ring related configurations.
It provides automatic recovery and reconnection mechanism for the disconnected Ethernet network, which has link redundancy and self-recovery ability in case of network interruption or network failure.

<table>
<thead>
<tr>
<th>Ring</th>
<th>Ring Configuration</th>
<th>Ring Monitor</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Global Mode

Mode: Disabled

Ring Mode

<table>
<thead>
<tr>
<th>Delete</th>
<th>Group</th>
<th>Network ID</th>
<th>Type</th>
<th>Port1</th>
<th>Port2</th>
<th>Hello Time</th>
<th>Master/Slave</th>
</tr>
</thead>
</table>

Add New Entry

Save  Reset
Global Mode

Mode

Enable/Disable the Global mode.
The ring configuration only takes effect when the global mode is enabled.

Ring Mode

Delete

Check the corresponding check box to delete an entry. It will be deleted during the next Save operation.

Group

Support ring group 1-4, it can create 4 ring networks at the same time.

Network ID

When multiple switch devices constitute a ring network, the current ring identification of the ring is network identification; the network identifications of different ring network are different.

Type

According to the scene environment requirement, choose different ring type.
- Single: Single ring, it adopts a continuous ring to connect each device together.
- Couple: Coupling ring is a redundant structure proposed to connect two independent networks.
- Chain: The chain, it enhances the flexibility that user builds any type of redundant network topology structure via a kind of advanced software technology.
- Dual-homing: Two adjacent rings share a switch; users can carry the same switch on two different networks or two different switching devices on the same network.

Port1

The network port 1 on the switch device used to form the ring network.

Port2

The network port 2 on the switch device used to form the ring network.

Hello time

Hello_time is the sending time interval of Hello packet; via the ring port, CPU sends information packet to adjacent device for confirming the connection is normal or not.

Master/Slave

Single ring has master/slave device option. One-Master Multi-Slave mode is recommended in one single ring. When the device is set as master device and one
end of it is backup link, it can enable backup link to ensure the normal operation of
the network when failure occurs in ring network.

Note:
Some products don’t support Master-slave option, so their ring network is non-master station
structure.

Buttons
Add new entry: Click to add a new loop entry. Specify the ID and configure the new
entry. Click “Save”.
Save: Click to save changes.
Reset: Click to undo any changes made locally and revert to previously saved values.

6.13.2 Loop Monitoring
This page displays the ring status.

Group ID
Group ID of the ring network.

Network ID
The current ring identification of the ring is network ID.

Master/Slave
Single ring has master/slave device option. One-Master Multi-Slave mode is
recommended in one single ring. When the device is set as master device and one
end of it is backup link, it can enable backup link to ensure the normal operation of
the network when failure occurs in ring network.

Note:
Some products don’t support Master-slave option, so their ring network is non-master station
structure.

Port1
The network port 1 on the switch device used to form the ring network.
Port2
The network port 2 on the switch device used to form the ring network.

Port1 Status
The status of network port 1 on the switch device used to form the ring network.

Port2 Status
The status of network port 2 on the switch device used to form the ring network.

Buttons
Auto-refresh: Automatic refresh occurs every 3 seconds.
Refresh: Click to refresh the page immediately.

6.14 MEP
The Maintenance Entity Point instances are configured here.

Delete
This box is used to mark a MEP for deletion in next Save operation.

Instance
The ID of the MEP. Click on the ID of a MEP to enter the configuration page. The range is from 1 through 100.

Domain
- Port: This is a MEP in the Port Domain.
- EVC: This is a MEP in the EVC Domain. 'Flow Instance' is an EVC. The EVC must be created
- VLAN: This is a MEP in the VLAN Domain. 'Flow Instance' is a VLAN. In case of Up-MEP the VLAN must be created

Mode
- MEP: This is a Maintenance Entity End Point.
- MIP: This is a Maintenance Entity Intermediate Point.

Direction
- Down: This is a Down MEP - monitoring ingress OAM and traffic on 'Residence Port'.
• Up: This is a Up MEP - monitoring ingress OAM and traffic on 'Residence Port'.

**Residence Port**

The port where MEP is monitoring - see 'Direction'. For a EVC MEP the port must be a port in the EVC. For a VLAN MEP the port must be a VLAN member.

**Level**

The MEG level of this MEP.

**Flow Instance**

The MEP is related to this flow - See 'Domain'. This is not relevant and not shown in case of Port MEP.

**Tagged VID**

- Port MEP: An outer C/S-tag (depending on VLAN Port Type) is added with this VID. Entering '0' means no TAG added.
- EVC MEP: This is not used.
- VLAN MEP: This is not used.
- EVC MIP: On Serval, this is the Subscriber VID that identifies the subscriber flow in this EVC where the MIP is active.

**This MAC**

The MAC of this MEP - can be used by other MEP when unicast is selected (Info only).

**Alarm**

There is an active alarm on the MEP.

**Buttons**

Add new MEP: Click to add a new MEP entry.
Refresh: Click to refresh the page immediately.
Save: Click to save changes.
Reset: Click to undo any changes made locally and revert to previously saved values.

This page allows the user to inspect and configure the current MEP Instance.
Instance Data

MEP Instance

The ID of the MEP.

Domain

- **Port**: This is a MEP in the Port Domain.
- **EVC**: This is a MEP in the EVC Domain. 'Flow Instance' is an EVC. The EVC must be created
- **VLAN**: This is a MEP in the VLAN Domain. 'Flow Instance' is a VLAN. In case of Up-MEP the VLAN must be created

Mode

- **MEP**: This is a Maintenance Entity End Point.
- **MIP**: This is a Maintenance Entity Intermediate Point.

Direction

- **Down**: this is an egress OAM and flow of downlink MEP-monitoring "monitoring port".
- **Up**: this is an egress OAM and flow of uplink MEP-monitoring "monitoring port".

Residence Port

The port where MEP is monitoring - see 'Direction'. For a EVC MEP the port must be a port in the EVC. For a VLAN MEP the port must be a VLAN member.
Flow Instance

The MEP is related to this flow - See 'Domain'. This is not relevant and not shown in case of Port MEP.

Tagged VID

- Port MEP: An outer C/S-tag (depending on VLAN Port Type) is added with this VID. Entering '0' means no TAG added.
- EVC MEP: This is not used.
- VLAN MEP: This is not used.
- EVC MIP: On Serval, this is the Subscriber VID that identifies the subscriber flow in this EVC where the MIP is active.

This MAC

The MAC of this MEP - can be used by other MEP when unicast is selected (Info only).

Instance Configuration

EVC QoS

This is only relevant for a EVC MEP. This is the Qos of the EVC and used for getting QoS counters for Loss Measurement.

Level

The MEG level of this MEP.

Format

This is the configuration of the two possible Maintenance Association Identifier formats.

- ITU ICC: This is defined by ITU (Y1731 Fig. A3). 'Domain Name' is not used. 'MEG id' must be max. 13 char.
- IEEE String: This is defined by IEEE (802.1ag Section 21.6.5). 'Domain Name' can be max. 16 char. 'MEG id' (Short MA Name) can be max. 16 char.
- ITU CC ICC: This is defined by ITU (Y1731 Fig. A5). 'Domain Name' is not used. 'MEG id' must be max. 15 char.

Domain Name

This is the IEEE Maintenance Domain Name and is only used in case of 'IEEE String' format. This string can be empty giving Maintenance Domain Name Format 1 - Not present. This can be max 16 char.

MEG Id

This is either ITU MEG ID or IEEE Short MA Name - depending on 'Format'. See 'Format'. In case of ITU ICC format this must be 13 char. In case of ITU CC ICC format this must be 15 char. In case of IEEE String format this can be max 16 char.
**MEP Id**

This value will become the transmitted two byte CCM MEP ID.

**Tagged VID**

This value will be the VID of a TAG added to the OAM PDU.

**VOE**

This will attempt to utilize VOE HW for MEP implementation. Not all platforms support VOE.

**cLevel**

Fault Cause indicating that a CCM is received with a lower level than the configured for this MEP.

**cMEG**

Fault Cause indicating that a CCM is received with a MEG ID different from configured for this MEP.

**cMEP**

Fault Cause indicating that a CCM is received with a MEP ID different from all 'Peer MEP ID' configured for this MEP.

**cAIS**

Fault Cause indicating that AIS PDU is received.

**cLCK**

Fault Cause indicating that LCK PDU is received.

**cDEG**

Fault Cause indicating that server layer is indicating Signal Degraded.

**cSSF**

Fault Cause indicating that server layer is indicating Signal Fail.

**aBLK**

The consequent action of blocking service frames in this flow is active.

**aTSD**

The consequent action of indicating Trail Signal Degrade is calculated.

**aTSF**

The consequent action of indicating Trail Signal Fail to-wards protection is active.
Peer MEP Configuration

Delete
This box is used to mark a Peer MEP for deletion in next Save operation.

Peer MEP ID
This value will become an expected MEP ID in a received CCM - see 'cMEP'.

Unicast Peer MAC
This MAC will be used when unicast is selected with this peer MEP. Also this MAC is used to create HW checking of receiving CCM PDU (LOC detection) from this MEP.

cLOC
Fault Cause indicating that no CCM has been received (in 3.5 periods) - from this peer MEP.

cRDI
Fault Cause indicating that a CCM is received with Remote Defect Indication - from this peer MEP.

cPeriod
Fault Cause indicating that a CCM is received with a period different what is configured for this MEP - from this peer MEP.

cPriority
Fault Cause indicating that a CCM is received with a priority different what is configured for this MEP - from this peer MEP.

Buttons
Add New Peer MEP: Click to add a new peer MEP.

Function Configuration

Continuity Check
Enable
Continuity Check based on transmitting/receiving CCM PDU can be enabled/disabled. The CCM PDU is always transmitted as Multi-cast Class 1.

Priority
The priority to be inserted as PCP bits in TAG (if any). In case of enable of Continuity Check and Loss Measurement both implemented on SW based CCM, 'Priority' has to be the same.
Frame rate
Selecting the frame rate of CCM PDU. This is the inverse of transmission period as described in Y.1731.: This value has the following uses:
- The transmission rate of the CCM PDU.
- Fault Cause cLOC is declared if no CCM PDU has been received within 3.5 periods - see ‘cLOC’.
- Fault Cause cPeriod is declared if a CCM PDU has been received with different period - see ‘cPeriod’.
Selecting 300f/sec or 100f/sec will configure HW based CCM (if possible). Selecting other frame rates will configure SW based CCM. In case of enable of Continuity Check and Loss Measurement both implemented on SW based CCM, ‘Frame Rate’ has to be the same.

TLV
Enable/disable of TLV insertion in the CCM PDU.

APS Protocol
Enable
Automatic Protection Switching protocol information transportation based on transmitting/receiving R-APS/L-APS PDU can be enabled/disabled. Must be enabled to support ERPS/ELPS implementing APS. This is only valid with one Peer MEP configured.

Priority
The priority to be inserted as PCP bits in TAG (if any).

Cast
Selection of APS PDU transmitted unicast or multi-cast. The unicast MAC will be taken from the ‘Unicast Peer MAC’ configuration. Unicast is only valid for L-APS - see ‘Type’. The R-APS PDU is always transmitted with multi-cast MAC described in G.8032.

Type
R-APS: APS PDU is transmitted as R-APS - this is for ERPS.
L-APS: APS PDU is transmitted as L-APS - this is for ELPS.

Last Octet
This is the last octet of the transmitted and expected RAPS multi-cast MAC. In G.8031(03/2010), RAPS multicast MAC is defined as 01-19-A7-00-00-XX. In current standard the value for this last octet is ‘01’ and the usage of other values is for further study.
TLV Configuration
Configuration of the OAM PDU TLV. Currently only TLV in the CCM is supported.

Organization Specific - OUI First
The transmitted first value in the OS TLV OUI field.

Organization Specific - OUI Second
The transmitted second value in the OS TLV OUI field.

Organization Specific - OUI Third
The transmitted third value in the OS TLV OUI field.

Organization Specific - Sub-Type
The transmitted value in the OS TLV Sub-Type field.

Organization Specific - Value
The transmitted value in the OS TLV Value field.

TLV Status
Display of the last received TLV. Currently only TLV in the CCM is supported.

CC Organization Specific - OUI First
The last received first value in the OUI field.

CC Organization Specific - OUI Second
The last received second value in the OS TLV OUI field.

CC Organization Specific - OUI Third
The last received third value in the OS TLV OUI field.

CC Organization Specific - Sub-Type
The last received value in the OS TLV Sub-Type field.

CC Organization Specific - Value
The last received value in the OS TLV Value field.

CC Organization Specific - Last RX
OS TLV was received in the last received CCM PDU.

CC Port Status - Value
The last received value in the PS TLV Value field.

CC Port Status - Last RX
PS TLV was received in the last received CCM PDU.

CC Interface Status - Value
The last received value in the IS TLV Value field.
**CC Interface Status - Last RX**

IS TLV was received in the last received CCM PDU.

**Link State Tracking**

**Enable**

When LST is enabled in an instance, Local SF or received 'isDown' in CCM Interface Status TLV, will bring down the residence port. Only valid in Up-MEP. The CCM rate must be 1 f/s or faster.

**Buttons**

Fault management: Click to enter Fault Management page.

Performance Monitoring: Click to go to Performance Monitor page.

Refresh: Click to refresh the page immediately.

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

This page allows the user to inspect and configure the Fault Management of the current MEP Instance.

<table>
<thead>
<tr>
<th>Loop Back</th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable</td>
<td>DEI</td>
<td>Priority</td>
<td>Cost</td>
<td>Peer MEP</td>
<td>Unicast MAC</td>
<td>To Send</td>
</tr>
<tr>
<td>✓</td>
<td>0</td>
<td>Multi</td>
<td>1</td>
<td>00-00-00-00-00-00</td>
<td>00-00-00-00-00-00-00</td>
<td>10</td>
</tr>
</tbody>
</table>

**Loop Back State**

Transaction | Transmitted | Reply MAC | Received | Out Of Order |  |
---|---|---|---|---|---|
1 | 00-00-00-00-00-00 | 00-00-00-00-00-00 | 0 | 0 |

| Link Trace |  |  |  |  |  |  |
| Enable | Priority | Peer MEP | Unicast MAC | Time To Live |  |
| ✓ | 1 | 00-00-00-00-00-00 | 00-00-00-00-00-00 | 1 |  |

**Link Trace State**

<table>
<thead>
<tr>
<th>Transaction ID</th>
<th>Time To Live</th>
<th>Mode</th>
<th>Direction</th>
<th>Forwarded</th>
<th>Relay</th>
<th>Last MAC</th>
<th>Next MAC</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No Transactions</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Test Signal**

<table>
<thead>
<tr>
<th>Tx</th>
<th>Rx</th>
<th>DEI</th>
<th>Priority</th>
<th>Peer MEP</th>
<th>Rate</th>
<th>Size</th>
<th>Pattern</th>
<th>Sequence Number</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>6-4</td>
<td>All Zero</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Test Signal State**

<table>
<thead>
<tr>
<th>TX frame count</th>
<th>RX frame count</th>
<th>RX rate</th>
<th>Test time</th>
<th>Clear</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>
Loop Back

Enable

Loop Back based on transmitting/receiving LBM/LBR PDU can be enabled/disabled. Loop Back is automatically disabled when all 'To Send' LBM PDU has been transmitted - waiting 5 sec. for all LBR from the end.

DEI

The DEI to be inserted as PCP bits in TAG (if any).

Priority

The priority to be inserted as PCP bits in TAG (if any).

Cast

Selection of LBM PDU transmitted unicast or multi-cast. The unicast MAC will be configured through 'Peer MEP' or 'Unicast Peer MAC'. To-wards MIP only unicast Loop Back is possible.

Peer MEP

This is only used if the 'Unicast MAC' is configured to all zero. The LBM unicast MAC will be taken from the 'Unicast Peer MAC' configuration of this peer.

Unicast MAC

This is only used if NOT configured to all zero. This will be used as the LBM PDU unicast MAC. This is the only way to configure Loop Back to-wards a MIP.

To Send

The number of LBM PDU to send in one loop test. The value 0 indicate infinite transmission (test behaviour). This is HW based LBM/LBR and Requires VOE.
**Size**

The LBM frame size. This is entered as the wanted size (in bytes) of a un-tagged frame containing LBM OAM PDU - including CRC (four bytes).

Example when 'Size' = 64 => Un-tagged frame size = DMAC(6) + SMAC(6) + TYPE(2) + TST PDU LENGTH(46) + CRC(4) = 64 bytes

The transmitted frame will be four bytes longer for each tag added - 8 bytes in case of a tunnel EVC.

There are two frame MAX sizes to consider.

Switch RX frame MAX size: The MAX frame size (all inclusive) accepted on the switch port of 9600 Bytes

CPU RX frame MAX size: The MAX frame size (all inclusive) possible to copy to CPU of 1526 Bytes

Consider that the Peer MEP must be able to handle the selected frame size.

Consider that In case of SW based MEP, the received LBR PDU must be copied to CPU

Warning will be given if selected frame size exceeds the CPU RX frame MAX size

Frame MIN Size is 64 Bytes.

**Interval**

The interval between transmitting LBM PDU. In 10 ms. If 'To Send' != 0 (max 100 - '0' is as fast as possible) in 1us.

**Loop Back State**

**Transaction**

The transaction id of the first LBM transmitted. For each LBM transmitted the transaction ID in the PDU is incremented.

**Transmitted**

The total number of LBM PDU transmitted.

**Reply MAC**

The MAC of the replying MEP/MIP. In case of multicast LBM, replies from all peer MEP in the group can be received. This MAC is not shown in case of 'To Send' == 0.

**Received**

The total number of LBR PDU received from this 'Reply MAC'.

**Out Of Order**

The number of LBR PDU received from this 'Reply MAC' with incorrect 'Transaction ID'.

**Link Trace**

**Enable**

Link Trace based on transmitting/receiving LTM/LTR PDU can be enabled/disabled. Link Trace is automatically disabled when all 5 transactions are done with 5 sec. interval - waiting 5 sec. for all LTR in the end. The LTM PDU is always transmitted as Multi-cast Class 2.

**Priority**

The priority to be inserted as PCP bits in TAG (if any).

**Peer MEP**

This is only used if the 'Unicast MAC' is configured to all zero. The Link Trace Target MAC will be taken from the 'Unicast Peer MAC' configuration of this peer.

**Unicast MAC**

This is only used if NOT configured to all zero. This will be used as the Link Trace Target MAC. This is the only way to configure a MIP as Target MAC.

**Time To Live**

This is the LTM PDU TTL value as described in Y.1731. This value is decremented each time forwarded by a MIP. Will not be forwarded reaching zero.

**Link Trace State**

**Transaction ID**

The transaction id is incremented for each LTM send. This value is inserted the transmitted LTM PDU and is expected to be received in the LTR PDU. Received LTR with wrong transaction id is ignored. There are five transactions in one Link Trace activated.

**Time To Live**

This is the TTL value taken from the LTM received by the MIP/MEP sending this LTR - decremented as if forwarded.

**Mode**

Indicating if is was a MEP/MIP sending this LTR.

**Direction**

Indicating if MEP/MIP sending this LTR is ingress/egress.

**Forwarded**

Indicating if MEP/MIP sending this LTR has forwarded the LTM.
Relay
The Relay action can be one of the following:
- MAC: This is a hit on the LT Target MAC.
- FDB: LTM is forwarded based on hit in the Filtering DB.
- MFDB: LTM is forwarded based on hit in the MIP CCM DB.

Last MAC
The MAC identifying the last sender of the LBM causing this LTR - initiating MEP or previous MIP forwarding.

Next MAC
The MAC identifying the next sender of the LBM causing this LTR - MIP forwarding or terminating MEP.

Test Signal
Tx
Sending Test Signal based on transmitting TST PDU can be enabled/disabled.

Tx
Receiving Test Signal based on transmitting TST PDU can be enabled/disabled.

DEI
The DEI to be inserted as PCP bits in TAG (if any).

Priority
The priority to be inserted as PCP bits in TAG (if any).

Peer MEP
The TST frame destination MAC will be taken from the 'Unicast Peer MAC' configuration of this peer.

Rate
The TST frame transmission bit rate - in Mega bits pr. second. Limit is 400 Mbps. This is the bit rate of a standard frame without any encapsulation. If 1 Mbps rate is selected in a EVC MEP, the added tag will give a higher bitrate on the wire.

Size
The TST frame size. This is entered as the wanted size (in bytes) of a un-tagged frame containing TST OAM PDU - including CRC (four bytes).
Example when 'Size' = 64 => Un-tagged frame size = DMAC(6) + SMAC(6) + TYPE(2) + TST PDU LENGTH(46) + CRC(4) = 64 bytes
The transmitted frame will be four bytes longer for each tag added - 8 bytes in case of a tunnel EVC.
There are two frame MAX sizes to consider.

Switch RX frame MAX size: The MAX frame size (all inclusive) accepted on the switch port of 9600 Bytes
CPU RX frame MAX size: The MAX frame size (all inclusive) possible to copy to CPU of 1526 Bytes
Consider that the Peer MEP must be able to handle the selected frame size.
Consider that in order to calculate the ‘RX rate’ a received TST PDU must be copied to CPU
Warning will be given if selected frame size exceeds the CPU RX frame MAX size
Frame MIN Size is 64 Bytes.

**Pattern**

The ‘empty’ TST PDU has the size of 12 bytes. In order to achieve the configured frame size a data TLV will be added with a pattern.
Example when ‘Size’ = 64 => Un-tagged frame size = DMAC(6) + SMAC(6) + TYPE(2) + TST PDU LENGTH(46) + CRC(4) = 64 bytes
The TST PDU needs to be 46 bytes so a pattern of 46-12=34 bytes will be added.
- All Zero: Pattern will be ‘00000000’
- All 1: the mode is “11111111”
- 10101010: Pattern will be ‘10101010’

**Test Signal State**

**TX frame count**
The number of transmitted TST frames since last ‘Clear’.

**RX frame count**
The number of received TST frames since last ‘Clear’.

**RX rate**
The current received TST frame bit rate in Kbps. This is calculated on a 1 s. basis, starting when first TST frame is received after ‘Clear’. The frame size used for this calculation is the first received after ‘Clear’

**Test time**
The number of seconds passed since first TST frame received after last ‘Clear’.

**Clear**
This will clear all Test Signal State. Transmission of TST frame will be restarted. Calculation of ‘Rx frame count’, ‘RX rate’ and ‘Test time’ will be started when receiving first TST frame.
**Client Configuration**

Only a Port MEP is able to be a server MEP with flow configuration. The Priority in the client flow is always the highest priority configured in the EVC.

**Domain**

The domain of the client layer flow.

**Instance**

Client layer flow instance numbers.

**Level**

Client layer level - AIS and LCK PDU transmitted in this client layer flow will be on this level.

**AIS Prio**

The priority to be used when transmitting AIS in each client flow. Priority resulting in highest possible PCP can be selected.

**LCK Prio**

The priority to be used when transmitting LCK in each client flow. Priority resulting in highest possible PCP can be selected.

**AIS**

**Enable**

Insertion of AIS signal (AIS PDU transmission) in client layer flows, can be enable/disabled.

**Frame Rate**

Selecting the frame rate of AIS PDU. This is the inverse of transmission period as described in Y.1731.: 

**Protection**

Selecting this means that the first 3 AIS PDU is transmitted as fast as possible - in case of using this for protection in the end point.

**LOCK**

**Enable**

Insertion of LOCK signal (LCK PDU transmission) in client layer flows, can be enable/disabled.

**Frame Rate**

Selecting the frame rate of LCK PDU. This is the inverse of transmission period as described in Y.1731.:
### Buttons

Back: Click to go back to this MEP instance main page.

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

This page allows the user to inspect and configure the performance monitor of the current MEP Instance.
### Performance Monitoring Data Set

#### Enable

When enabled this MEP instance will contribute to the 'PM Data Set' gathered by the PM Session.

#### Loss Measurement

##### Tx

Loss Measurement initiator is enabled/disabled. Initiator is transmitting/receiving CCM or LMM/LMR or SLM/SLR/1SL PDUs - see 'Synthetic' and 'Ended'.

Service frame LM (not 'Synthetic') is only allowed with one Peer MEP configured.

Synthetic frame LM is allowed with multiple Peer MEPs configured.

##### Rx

Enable loss calculation when receiving LM PDUs (LMM/SLM/1SL). This is ignored when LM initiator is enabled.
Priority
The priority to be inserted as PCP bits in TAG (if any). In case of enable of Continuity Check and Loss Measurement both implemented on SW based CCM, 'Priority' has to be the same.

Cast
Selection of LM PDU transmitted unicast or multicast. The unicast MAC will be taken from the 'Unicast Peer MAC' database. In case of enable of Continuity Check and dual ended Loss Measurement both implemented on SW based CCM, 'Cast' has to be the same.

Peer MEP
Peer MEP-ID for unicast LM. The MAC is taken from the 'Unicast Peer MAC' database. Only used in case of multiple peers ('Synthetic' LM).

Speed
Selecting the frame rate of LM PDU. This is the inverse of transmission period as described in Y.1731
Selecting 100f/sec is only valid in case of 'Synthetic' LM.
Selecting 6f/min is not valid in case of dual ended 'Service frame' LM (CCM PDU based).
In case of enable of Continuity Check and Loss Measurement both implemented on SW based CCM, 'Frame Rate' has to be the same.

Size
The 'Synthetic' SLM/1SL frame size. This is entered as the wanted size (in bytes) of an un-tagged frame containing LM OAM PDU - including CRC (four bytes).
Example when 'Size' = 64 => Un-tagged frame size = DMAC(6) + SMAC(6) + TYPE(2) + TST PDU LENGTH(46) + CRC(4) = 64 bytes
The transmitted frame will be four bytes longer for each tag added - 8 bytes in case of a tunnel EVC.
There are two frame MAX sizes to consider.
Switch RX frame MAX size: The MAX frame size (all inclusive) accepted on the switch port of Bytes
CPU RX frame MAX size: The MAX frame size (all inclusive) possible to copy to CPU of Bytes
Consider that the Peer MEP must be able to handle the selected frame size.
Consider that the received SLR PDU must be copied to CPU
Warning will be given if selected frame size exceeds the CPU RX frame MAX size
Frame MIN Size is 64 Bytes.
Synthetic frame LM is enabled. This is SLM/SLR/1SL PDU based LM.

**Ended**

Single: Single ended Loss Measurement implemented on LMM/LMR or SLM/SLR.
Dual: Dual ended Loss Measurement implemented on SW based CCM or 1SL.

**FLR Interval**

This is the interval in number of measurement intervals where the interval Frame Loss Ratio is calculated.

**Meas Interval**

This is the 'synthetic' LM measurement interval in milliseconds. This must be a whole number of the LM PDU transmission interval (inverse 'Rate'). This is the interval in time where the loss and FLR is calculated based on the counted number of SL OAM PDUs. It is in this interval that the calculated FLR is checked against availability, high loss and degraded FLR threshold.

For example: 'Rate' = 100f/sec => 'Meas Interval' = N*10 milliseconds.
For example: 'Rate' = 10f/sec => 'Meas Interval' = N*100 milliseconds.
In case of service frame based LM this attribute is not used and the measurement interval is always the LM PDU transmission interval.

**Loss Threshold**

Far end loss threshold count is incremented if a loss measurement is above this threshold.

**SLM Test ID**

The Test ID value to use in SLM PDUs (see G.8013, section 9.22.1). The default value is 0.

**Loss Measurement State**

**Peer MEP**

The Peer MEP ID that the following state relates to.

**Tx**

The accumulated transmitted LM PDUs - since last 'clear'.

**Rx**

The accumulated received LM PDUs - since last 'clear'.

**Near End Loss Count**

The accumulated near end frame loss count - since last 'clear'.

---

Indu-Sol proprietary and confidential
Copyright © Indu-Sol GmbH
Far End Loss Count
The accumulated far end frame loss count - since last 'clear'.

Interval Elapsed
The accumulated number of 'FLR Interval' elapsed - since last 'clear'.

Interval Near End Loss Ratio
The near end frame loss ratio calculated based on the near end frame loss count and far end frame transmitted - in the latest 'FLR Interval'. This is shown in \((\text{Loss/Tx}) \times 10000\). Same as 1/100 Percent.

Interval Far End Loss Ratio
The far end frame loss ratio calculated based on the far end frame loss count and near end frame transmitted - in the latest 'FLR Interval'. This is shown in \((\text{Loss/Tx}) \times 10000\). Same as 1/100 Percent.

Total Near End Loss Ratio
The near end frame loss ratio calculated based on the near end frame loss count and far end frame transmitted - since last 'clear'. This is shown in \((\text{Loss/Tx}) \times 10000\). Same as 1/100 Percent.

Total Far End Loss Ratio
The far end frame loss ratio calculated based on the far end frame loss count and near end frame transmitted - since last 'clear'. This is shown in \((\text{Loss/Tx}) \times 10000\). Same as 1/100 Percent.

Clear
Set of this check and save will clear the accumulated counters and restart ratio calculation.

Loss Measurement Availability

Enable
Enable/disable of loss measurement availability.

Interval
Availability interval - number of measurements with same availability in order to change availability state.

FLR Threshold
Availability frame loss ratio threshold in per mile.

Maintenance
Enable/disable of loss measurement availability maintenance.
Loss Measurement Availability Status

Near Avail Count
Near end availability count.

Far Avail Count
Far end availability count.

Near Unavail Count
Near end unavailability count.

Far Unavail Count
Far end unavailability count.

Near State
Near end availability state.

Far State
Far end availability state.

Loss Measurement High Loss Interval

Enable
Enable/disable of loss measurement high loss interval.

FLR Threshold
High Loss Interval frame loss ratio threshold in per mile.

Consecutive Interval
High Loss Interval consecutive interval (number of measurements).

Loss Measurement High Loss Interval Status

Near Count
Near end high loss interval count (number of measurements where availability state is available and FLR is above high loss interval FLR threshold).

Far Count
Far end high loss interval count (number of measurements where availability state is available and FLR is above high loss interval FLR threshold).

Near Consecutive Count
Near end high loss interval consecutive count.

Far Consecutive Count
Far end high loss interval consecutive count.
Loss Measurement Signal Degrade

Enable
Enable/disable of loss measurement signal degrade.

TX Minimum
Minimum number of frames that must be transmitted in a measurement before frame loss ratio is tested against loss ratio threshold.

FLR Threshold
Signal Degraded frame loss ratio threshold in per mile.

Bad Threshold
Number of consecutive bad interval measurements required to set degrade state.

Good Threshold
Number of consecutive good interval measurements required to clear degrade state.

Delay Measurement

Enable
Delay Measurement based on transmitting 1DM/DMM PDU can be enabled/disabled.
Delay Measurement based on receiving and handling 1DM/DMR PDU is always enabled.

Priority
The priority to be inserted as PCP bits in TAG (if any).

Cast
Selection of 1DM/DMM PDU transmitted unicast or multicast. The unicast MAC will be configured through 'Peer MEP'.

Peer MEP
This is only used if the 'Cast' is configured to Uni. The 1DM/DMR unicast MAC will be taken from the 'Unicast Peer MAC' configuration of this peer.

Ended
Single: Single ended Delay Measurement implemented on DMM/DMR.
Dual: Dual ended Delay Measurement implemented on 1DM.

Tx Mode
Standardize: Y.1731 standardize way to transmit 1DM/DMR.
Proprietary: Proprietary way with follow-up packets to transmit 1DM/DMR.

Counter
This is only used if the 'Ended' is configured to single ended.
Round trip: The frame delay calculated by the transmitting and receiving timestamps of initiators. Frame Delay = RxTimeb-TxTimeStamp

Flow: The frame delay calculated by the transmitting and receiving timestamps of initiators and remotes. Frame Delay = (RxTimeb-TxTimeStamp)-(TxTimeStampb-RxTimeb).

**Gap**

The gap between transmitting 1DM/DMM PDU in 10ms. The range is 10 to 65535.

**Count**

The number of last records to calculate. The range is 10 to 2000.

**Unit**

The time resolution.

**Synchronized**

Enable to use DMM/DMR packet to calculate dual ended DM. If the option is enabled, the following action will be taken. When DMR is received, two-way delay (roundtrip or flow) and both near-end-to-far-end and far-end-to-near-end one-way delay are calculated. When DMM or 1DM is received, only far-end-to-near-end one-way delay is calculated.

**Counter Overflow Action**

The action to counter when overflow happens.

**Delay Measurement State**

**Tx**

The accumulated transmit count - since last 'clear'.

**Rx**

The accumulated receive count - since last 'clear'.

**Rx Timeout**

The accumulated receive timeout count for two-way only - since last 'clear'.

**Rx Error**

The accumulated receive error count - since last 'clear'. This is counting if the frame delay is larger than 1 second or if far end residence time is larger than the round trip time.

**Av Delay Tot**

The average total delay - since last 'clear'.
**Av Delay last N**

The average delay of the last n packets - since last 'clear'.

**Delay Min.**

The minimum delay - since last 'clear'.

**Delay Max.**

The maximum delay - since last 'clear'.

**Av Delay-Var Tot**

The average total delay variation - since last 'clear'.

**Av Delay-Var last N**

The average delay variation of the last n packets - since last 'clear'.

**Delay-Var Min.**

The minimum delay variation - since last 'clear'.

**Delay-Var Max.**

The maximum delay variation - since last 'clear'.

**Overflow**

The number of counter overflow - since last 'clear'.

**Clear**

Set of this check and save will clear the accumulated counters.

**Far-end-to-near-end one-way delay**

The one-way delay is from remote devices to the local devices. Here are the conditions to calculate this delay. DM received by 1. 2DMM received with Synchronized enabled. 3DMR received with Synchronized enabled.

**Near-end-to-far-end one-way delay**

The one-way delay is from the local devices to remote devices. The only case to calculate this delay is below. DMR received with Synchronized enabled.

**Delay Measurement Bins**

A Measurement Bin is a counter that stores the number of delay measurements falling within a specified range, during a Measurement Interval.

**Measurement Bins for FD**

Configurable number of Frame Delay Measurement Bins per Measurement Interval. The minimum number of FD Measurement Bins per Measurement Interval supported is 2.
The maximum number of FD Measurement Bins per Measurement Interval supported is 10.
The default number of FD Measurement Bins per Measurement Interval supported is 3.

**Measurement Bins for IFDV**
Configurable number of Inter-Frame Delay Variation Measurement Bins per Measurement Interval.
The minimum number of FD Measurement Bins per Measurement Interval supported is 2.
The maximum number of FD Measurement Bins per Measurement Interval supported is 10.
The default number of FD Measurement Bins per Measurement Interval supported is 2.

**Measurement Threshold**
Configurable the Measurement Threshold for each Measurement Bin.
The unit for a measurement threshold is in microseconds (us).
The default configured measurement threshold for a Measurement Bin is an increment of 5000 us.

**Delay Measurement Bins for FD**
A Measurement Bin is a counter that stores the number of delay measurements falling within a specified range, during a Measurement Interval.
If the measurement threshold is 5000 us and the total number of Measurement Bins is four, we can give an example as follows.

<table>
<thead>
<tr>
<th>Bin</th>
<th>Threshold</th>
<th>Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>bin0</td>
<td>0 us</td>
<td>0 us &lt;= measurement &lt; 5,000 us</td>
</tr>
<tr>
<td>bin1</td>
<td>5,000 us</td>
<td>5,000 us &lt;= measurement &lt; 10,000 us</td>
</tr>
<tr>
<td>bin2</td>
<td>10,000 us</td>
<td>10,000 us &lt;= measurement &lt; 15,000 us</td>
</tr>
<tr>
<td>bin3</td>
<td>15,000 us</td>
<td>15,000 us &lt;= measurement &lt; infinite us</td>
</tr>
</tbody>
</table>

**Delay Measurement Bins for IFDV**
A Measurement Bin is a counter that stores the number of delay measurements falling within a specified range, during a Measurement Interval.
If the measurement threshold is 5000 us and the total number of Measurement Bins is four, we can give an example as follows.

<table>
<thead>
<tr>
<th>Bin</th>
<th>Threshold</th>
<th>Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>bin0</td>
<td>0 us</td>
<td>0 us &lt;= measurement &lt; 5,000 us</td>
</tr>
<tr>
<td>bin1</td>
<td>5,000 us</td>
<td>5,000 us &lt;= measurement &lt; 10,000 us</td>
</tr>
</tbody>
</table>
Buttons

Back: Click to go back to this MEP instance main page.
Save: Click to save changes.
Reset: Click to undo any changes made locally and revert to previously saved values.

6.15 ERPS

The ERPS instances are configured here.

Delete

This box is used to mark an ERPS for deletion in next save operation.

ERPS ID

The ID of the created Protection group. It must be an integer value between 1 and 64. The maximum numbers of ERPS Protection Groups that can be created are 64. Click on the ID of a Protection group to enter the configuration page.

Port 0

This will create a Port 0 of the switch in the ring.

Port 1

This will create "Port 1" of the switch in the Ring. As interconnected sub-ring will have only one ring port, "Port 1" is configured as "0" for interconnected sub-ring. "0" in this field indicates that no "Port 1" is associated with this instance.

Port 0 SF MEP

The Port 0 Signal Fail reporting MEP.

Port 1 SF MEP

The Port 1 Signal Fail reporting MEP. As only one SF MEP is associated with interconnected sub-ring without virtual channel, it is configured as "0" for such ring instances. "0" in this field indicates that no Port 1 APS MEP is associated with this instance.
Port 0 APS MEP
The Port 0 APS PDU handling MEP.

Port 1 APS MEP
The Port 1 APS PDU handling MEP. As only one APS MEP is associated with interconnected sub-ring without virtual channel, it is configured as "0" for such ring instances. "0" in this field indicates that no Port 1 APS MEP is associated with this instance.

Ring Type
Type of Protecting ring. It can be either major ring or sub-ring.

Interconnected Node
Interconnected Node indicates that the ring instance is interconnected. Click on the checkbox to configure this. "Yes" indicates it is an interconnected node for this instance. "No" indicates that the configured instance is not interconnected.

Virtual Channel
Sub-rings can either have virtual channel or not on the interconnected node. This is configured using "Virtual Channel" checkbox. "Yes" indicates it is a sub-ring with virtual channel. "No" indicates, sub-ring doesn't have virtual channel.

Major Ring ID
Major ring group ID for the interconnected sub-ring. It is used to send topology change updates on major ring. If ring is major, this value is same as the protection group ID of this ring.

Alarm
There is an active alarm on the ERPS.

Buttons
Add new protection group: Click to add a new protection group entry.
Refresh: Click to refresh the page immediately.
Protect: Click to save changes.
Reset: Click to undo any changes made locally and revert to previously saved values.

This page allows the user to inspect and configure the current ERPS Instance.
### Instance Data

#### ERPS ID

The ID of the Protection group.

#### Port 0

This will create a Port 0 of the switch in the ring.

#### Port 1

This will create "Port 1" of the switch in the Ring. As interconnected sub-ring will have only one ring port, "Port 1" is configured as "0" for interconnected sub-ring. "0" in this field indicates that no "Port 1" is associated with this instance.

#### Port 0 SF MEP

The Port 0 Signal Fail reporting MEP.

#### Port 1 SF MEP

The Port 1 Signal Fail reporting MEP. As only one SF MEP is associated with interconnected sub-ring without virtual channel, it is configured as "0" for such ring instances. "0" in this field indicates that no Port 1 APS MEP is associated with this instance.

#### Port 0 APS MEP

The Port 0 APS PDU handling MEP.

#### Port 1 APS MEP

The Port 1 APS PDU handling MEP. As only one APS MEP is associated with interconnected sub-ring without virtual channel, it is configured as "0" for such ring instances. "0" in this field indicates that no Port 1 APS MEP is associated with this instance.
Ring Type
Type of Protecting ring. It can be either major ring or sub-ring.

Instance Configuration

Configured
Red: This ERPS is only created and has not yet been configured - is not active.
Green: This ERPS is configured - is active.

Guard Time
Guard timeout value to be used to prevent ring nodes from receiving outdated R-APS messages.
The period of the guard timer can be configured in 10 ms steps between 10 ms and 2 seconds. The default value is 500 ms.

WTR Time
The Wait To Restore timing value to be used in revertive switching.
The period of the WTR time can be configured by the operator in 1 minute steps between 5 and 12 minutes. The default value is 5 minutes.

Hold Off Time
The timing value to be used to make persistent check on Signal Fail before switching.
The range of the hold off timer is 0 to 10 seconds in steps of 100 ms

Version
ERPS Protocol Version - v1 or v2

Revertive
In Revertive mode, after the conditions causing a protection switch has cleared, the traffic channel is restored to the working transport entity, i.e., blocked on the RPL.
In Non-Revertive mode, the traffic channel continues to use the RPL, if it is not failed, after a protection switch condition has cleared.

VLAN config
VLAN configuration of the Protection Group. Click on the "VLAN Config" link to configure VLANs for this protection group.

RPL Configuration

RPL Role
It can be either RPL owner or RPL Neighbor.

RPL Port
This allows to select the east port or west port as the RPL block.
Clear
If the owner has to be changed, then the clear check box allows to clear the RPL owner for that ERPS ring.

Sub-Ring Configuration

Topology Change
Clicking this checkbox indicates that the topology changes in the sub-ring are propagated in the major ring.

Instance Command

Command
Administrative command. A port can be administratively configured to be in either manual switch or forced switch state.

Forced Switch
Forced Switch command forces a block on the ring port where the command is issued.

Manual Switch
In the absence of a failure or FS, Manual Switch command forces a block on the ring port where the command is issued.

Clear
The Clear command is used for clearing an active local administrative command (e.g., Forced Switch or Manual Switch).

Port
Port selection - Port0 or Port1 of the protection Group on which the command is applied.

Instance State

Protection State
ERPS state according to State Transition Tables in G.8032.

Port 0
OK: State of East port is ok
SF: State of East port is Signal Fail

Port 1
OK: State of West port is ok.
SF: State of West port is Signal Fail.
**Transmit APS**

The transmitted APS according to State Transition Tables in G.8032.

**Port 0 Receive APS**

The received APS on Port 0 according to State Transition Tables in G.8032.

**Port 1 Receive APS**

The received APS on Port 1 according to State Transition Tables in G.8032.

**WTR Remaining**

Remaining WTR timeout in milliseconds.

**RPL Un-blocked**

APS is received on the working flow.

**No APS Received**

RAPS PDU is not received from the other end.

**Port 0 Block Status**

Block status for Port 0 (Both traffic and R-APS block status). R-APS channel is never blocked on sub-rings without virtual channel.

**Port 1 Block Status**

Block status for Port 1 (Both traffic and R-APS block status). R-APS channel is never blocked on sub-rings without virtual channel.

**FOP Alarm**

Failure of Protocol Defect (FOP) status. If FOP is detected, red LED glows; else green LED glows.

**Buttons**

Save: Click to save changes.

Auto-refresh: Check this box to enable an automatic refresh. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page immediately.

Reset: Click to undo any changes made locally and revert to previously saved values.
Delete

To delete a VLAN entry, check this box. The entry will be deleted during the next Save.

VLAN ID

Indicates the ID of this particular VLAN.

Adding New Entry

Click “Add New Entry” to add a new VLAN ID. Legal values for a VLAN ID are 1 through 4095.
The VLAN is enabled when you click “Save”. A VLAN without any port members will be deleted when you click “Save”.
The “Delete” button can be used to delete the added vlan.

Buttons

Save: Click to save changes.
Reset: Click to undo any changes made locally and revert to previously saved values.
Back: Click to go back to this MEP instance main page.
Refresh: Refreshes the displayed table starting from the “VLAN ID” input fields.
7.1 IGMP Snooping

7.1.1 Basic Configuration

This page provides IGMP Snooping related configuration.

### Global Configuration

**Snooping Enabled**

Enable the Global IGMP Snooping.
Unregistered IPMCv4 Flooding Enabled

Enable unregistered IPMCv4 traffic flooding.
The flooding control takes effect only when IGMP Snooping is enabled.
When IGMP Snooping is disabled, unregistered IPMCv4 traffic flooding is always active in spite of this setting.

Port-related Configuration

Router Port

Specify which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or IGMP querier.
If an aggregation member port is selected as a router port, the whole aggregation will act as a router port.

Fast Leave

Enable the fast leave on the port.

Throttling

Enable to limit the number of multicast groups to which a switch port can belong.

Buttons

Save: Click to save changes.
Reset: Click to undo any changes made locally and revert to previously saved values.

7.1.2 VLAN Configuration

Navigating the IGMP Snooping VLAN Table

Each page shows up to 99 entries from the VLAN table, default being 20, selected through the "__ entries per page" input field. When first visited, the WEB page will show the first 20 entries from the beginning of the VLAN Table. The first displayed will be the one with the lowest VLAN ID found in the VLAN Table.
The "VLAN" input fields allow the user to select the starting point in the VLAN Table. Clicking the "Refresh" button will update the displayed table starting from that or the closest next VLAN Table match. In addition, the two input fields will - upon a button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.
Pressing the "|<<" button will use the last entry of the currently displayed entry as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the "|<<" button to start over.
Delete

Check to delete the entry. The designated entry will be deleted during the next save.

VLAN ID

The VLAN ID of the entry.

Enable Listening

Enable the per-VLAN IGMP Snooping. Up to 32 VLANs can be selected for IGMP Snooping.

Querier Election

Enable to join IGMP Querier election in the VLAN. Disable to act as an IGMP Non-Querier.

Querier Address

Define the IPv4 address as source address used in IP header for IGMP Querier election.

When the Querier address is not set, system uses IPv4 management address of the IP interface associated with this VLAN.

When the IPv4 management address is not set, system uses the first available IPv4 management address.

Otherwise, system uses a pre-defined value. By default, this value will be 192.0.2.1.

IGMP Versions

Compatibility is maintained by hosts and routers taking appropriate actions depending on the versions of IGMP operating on hosts and routers within a network.

The allowed selection is IGMP-Auto, Forced IGMPv1, Forced IGMPv2, Forced IGMPv3, default compatibility value is IGMP-Auto.

Buttons

Refresh: Refreshes the displayed table starting from the "VLAN" input fields.
<<: Updates the table starting from the first entry in the VLAN Table, i.e. the entry with the lowest VLAN ID.
>>: Updates the table, starting with the entry after the last entry currently displayed.
Add New IGMP VLAN: click here to add new IGMP VLAN. Specify the VID and configure the new entry. Click "Save". The specific IGMP VLAN starts working after the corresponding static VLAN is also created.

Save: Click to save changes.
Reset: Click to undo any changes made locally and revert to previously saved values.

### 7.1.3 Status Monitoring

This page provides IGMP Snooping status.

<table>
<thead>
<tr>
<th>Statistics</th>
<th>VLAN ID</th>
<th>Querier Version</th>
<th>Host Version</th>
<th>Querier Status</th>
<th>Queries Transmitted</th>
<th>Queries Received</th>
<th>V1 Reports Received</th>
<th>V2 Reports Received</th>
<th>V3 Reports Received</th>
<th>V2 Leaves Received</th>
</tr>
</thead>
<tbody>
<tr>
<td>IGMP Snooping &gt;</td>
<td>Basic Configuration</td>
<td>VLAN Configuration</td>
<td>Status Monitor</td>
<td>Groups Information Monitor</td>
<td>IP4 SFM Information Monitor</td>
<td>Auto-refresh</td>
<td>Refresh</td>
<td>Clear</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### VLAN ID

The VLAN ID of the entry.

#### Querier Version

Working Querier Version currently.

#### Host Version

Working Host Version currently.

#### Query Status

Shows the Querier status is "ACTIVE" or "IDLE".
"DISABLE" denotes the specific interface is administratively disabled.

#### Queries Transmitted

The number of Transmitted Queries.

#### Queries Received

The number of Received Queries.
V1 Reports Received
The number of Received V1 Reports.

V2 Reports Received
The number of Received V2 Reports.

V3 Reports Received
The number of Received V3 Reports.

V2 Leaves Received
The number of Received V2 Leaves.

Router Port
Display which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or IGMP querier.
Static denotes the specific port is configured to be a router port.
Dynamic denotes the specific port is learnt to be a router port.
Both denote the specific port is configured or learnt to be a router port.

Port
The switch port number.

Status
Indicate whether specific port is a router port or not.

Buttons
Auto-refresh: Automatic refresh occurs every 3 seconds.
Refresh: Click to refresh the page immediately.
Clear: Clears all Statistics counters.

7.1.4 Group Information Monitoring
Entries in the IGMP Group Table are shown on this page. The IGMP Group Table is sorted first by VLAN ID, and then by group.
Navigating the IGMP Group Table

Each page shows up to 99 entries from the IGMP Group table, default being 20, selected through the "__ entries per page" input field. When first visited, the WEB page will show the first 20 entries from the beginning of the IGMP Group Table. The "Start from VLAN__", and "group" input fields allow the user to select the starting point in the IGMP Group Table. Clicking the “Refresh” button will update the displayed table starting from that or the closest next IGMP Group Table match. In addition, the two input fields will - upon a “Refresh” button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address. “>>” will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached the text “No more entries” is shown in the displayed table. Use the “|<<” button to start over.

IGMP Group Table Columns

VLAN ID
VLAN ID of the group.

Group
Group address of the group displayed.

Port Members
Ports under this group.

Buttons
Auto-refresh: Automatic refresh occurs every 3 seconds.
Refresh: Refresh the displayed table starting from the input fields.
|<<: Updates the table, starting with the first entry in the IGMP Group Table.
>>: Updates the table, starting with the entry after the last entry currently displayed.

7.1.5 IPv4 SFM Information Monitoring

Entries in the IGMP SFM Information Table are shown on this page. The IGMP SFM (Source-Filtered Multicast) Information Table also contains the SSM (Source-Specific Multicast) information. This table is sorted first by VLAN ID, then by group, and then by Port. Different source addresses belong to the same group are treated as single entry.
Navigating the IGMP SFM Information Table

Each page shows up to 99 entries from the IGMP SFM Information Table, default being 20, selected through the "entries per page" input field. When first visited, the WEB page will show the first 20 entries from the beginning of the IGMP SFM Information Table.

The "Start from VLAN__and Group__" input fields allow the user to select the starting point in the IGMP SFM Information Table. Clicking the “Refresh” button will update the displayed table starting from that or the closest next IGMP SFM Information Table match. In addition, the two input fields will - upon a "Refresh" button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

">>" will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the "|<<" button to start over.

IGMP SFM Information Table Columns

**VLAN ID**
VLAN ID of the group.

**Group**
Group address of the group displayed.

**Port**
The switch port number.

**Mode**
Indicates the filtering mode maintained per (VLAN ID, port number, Group Address) basis. It can be either Include or Exclude.

**Source Address**
IP Address of the source.
Currently, the maximum number of IPv4 source address for filtering (per group) is 8. When there is no any source filtering address, the text "None" is shown in the Source Address field.

**Type**
Indicates the Type. It can be either Allow or Deny.
Hardware Filter/Switch

Indicates whether data plane destined to the specific group address from the source IPv4 address could be handled by chip or not.

Buttons

Auto-refresh: Automatic refresh occurs every 3 seconds.
Refresh: Refresh the displayed table starting from the input fields.
|<<: Updates the table starting from the first entry in the IGMP SFM Information Table.
>>: Updates the table, starting with the entry after the last entry currently displayed.

7.2 Multicast MAC

Static multicast MAC address could be added on this page.

Delete

Click the “Delete” button to delete the current entry.

VLAN ID

The VLAN ID of the entry.

MAC Address

The multicast MAC address of the entry, such as “01-00-5E-XX-XX-XX”.

Port Members

The ports that are members of the entry.

Buttons

Add new static entry: click to add a new static multicast MAC address entry.
Save: Click to save changes.
Reset: Click to undo any changes made locally and revert to previously saved values.
8.1 Global Configuration

8.1.1 PoE Configuration

This page allows the user to inspect and configure the current PoE port settings.
There are three modes for configuring how the ports/PDs may reserve power.

- **Allocated mode**: In this mode the user allocates the amount of power that each port may reserve. The allocated/reserved power for each port/PD is specified in the Maximum Power fields.
- **Class mode**: In this mode each port automatically determines how much power to reserve according to the class the connected PD belongs to, and reserves the power accordingly. Four different port classes exist and one for 4, 7, 15.4 or 30 Watts. In this mode the Maximum Power fields have no effect.
- **LLDP-MED mode**: This mode is similar to the Class mode expect that each port determine the amount power it reserves by exchanging PoE information using the LLDP protocol and reserves power accordingly. If no LLDP information is

---

Reserved Power determined by

- **Allocated mode**: In this mode the user allocates the amount of power that each port may reserve. The allocated/reserved power for each port/PD is specified in the Maximum Power fields.
- **Class mode**: In this mode each port automatically determines how much power to reserve according to the class the connected PD belongs to, and reserves the power accordingly. Four different port classes exist and one for 4, 7, 15.4 or 30 Watts. In this mode the Maximum Power fields have no effect.
- **LLDP-MED mode**: This mode is similar to the Class mode expect that each port determine the amount power it reserves by exchanging PoE information using the LLDP protocol and reserves power accordingly. If no LLDP information is

---

Reserved Power determined by

There are three modes for configuring how the ports/PDs may reserve power.

- **Allocated mode**: In this mode the user allocates the amount of power that each port may reserve. The allocated/reserved power for each port/PD is specified in the Maximum Power fields.
- **Class mode**: In this mode each port automatically determines how much power to reserve according to the class the connected PD belongs to, and reserves the power accordingly. Four different port classes exist and one for 4, 7, 15.4 or 30 Watts. In this mode the Maximum Power fields have no effect.
- **LLDP-MED mode**: This mode is similar to the Class mode expect that each port determine the amount power it reserves by exchanging PoE information using the LLDP protocol and reserves power accordingly. If no LLDP information is
available for a port, the port will reserve power using the class mode. In this mode, the Maximum Power fields have no effect.

For all modes: If a port uses more power than the reserved power for the port, the port is shut down.

**Power Management Mode**

There are 2 modes for configuring when to shut down the ports:

- **Actual Consumption**: In this mode, the ports are shut down when the actual power consumption for all ports exceeds the amount of power that the power supply can deliver or if the actual power consumption for a given port exceeds the reserved power for that port. The ports are shut down according to the ports priority. If two ports have the same priority, the port with the highest port number is shut down.

- **Reserved Power**: In this mode, the ports are shut down when the total reserved power exceeds the amount of power that the power supply can deliver. In this mode, the port power is not turned on if the PD requests more power than available from the power supply.

**Capacitor Detection**

Controls capacitor detection for legacy PD devices.

- **Disabled**: This feature is disabled.
- **Enabled**: This feature is enabled.

**PoE Power Supply Configuration**

**Primary Power Supply [W]**

For being able to determine the amount of power the PD may use, it must be defined what amount of power a power source can deliver.

Valid values are in the range 0 to 240 Watts.

**PoE Port Configuration**

**Port**

This is the logical port number for this row.

Ports that are not PoE-capable are grayed out and thus impossible to configure PoE for.

**PoE Mode**

The PoE Mode represents the PoE operating mode for the port.

- **Disabled**: PoE disabled for the port.
- **PoE**: Enables PoE IEEE 802.3af (Class 4 PDs limited to 15.4W)
- **PoE+**: Enables PoE+ IEEE 802.3at (Class 4 PDs limited to 30W)
**Priority**

The Priority represents the ports priority. There are three levels of power priority named Low, High and Critical.
The priority is used in the case where the remote device requires more power than the power supply can deliver. In this case the port with the lowest priority will be turned off starting from the port with the highest port number.

**Maximum Power [W]**

The Maximum Power value contains a numerical value that indicates the maximum power in watts that can be delivered to a remote device.
The maximum allowed value is 30 W.

**Buttons**

Save: Click to save changes.
Reset: Click to undo any changes made locally and revert to previously saved values.

### 8.1.2 Power Over Ethernet Status

This page allows the user to inspect the current status for all PoE ports.

<table>
<thead>
<tr>
<th>Local Port</th>
<th>PD Class</th>
<th>Power Requested</th>
<th>Power Allocated</th>
<th>Power Used</th>
<th>Current Used</th>
<th>Priority</th>
<th>Port Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0 [W]</td>
<td>0 [W]</td>
<td>0 [W]</td>
<td>0 [mA]</td>
<td>Low</td>
<td>No PD detected</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>0 [W]</td>
<td>0 [W]</td>
<td>0 [W]</td>
<td>0 [mA]</td>
<td>Low</td>
<td>No PD detected</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>0 [W]</td>
<td>0 [W]</td>
<td>0 [W]</td>
<td>0 [mA]</td>
<td>Low</td>
<td>No PD detected</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>0 [W]</td>
<td>0 [W]</td>
<td>0 [W]</td>
<td>0 [mA]</td>
<td>Low</td>
<td>No PD detected</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>0 [W]</td>
<td>0 [W]</td>
<td>0 [W]</td>
<td>0 [mA]</td>
<td>Low</td>
<td>No PD detected</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>0 [W]</td>
<td>0 [W]</td>
<td>0 [W]</td>
<td>0 [mA]</td>
<td>Low</td>
<td>No PD detected</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>0 [W]</td>
<td>0 [W]</td>
<td>0 [W]</td>
<td>0 [mA]</td>
<td>Low</td>
<td>No PD detected</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>0 [W]</td>
<td>0 [W]</td>
<td>0 [W]</td>
<td>0 [mA]</td>
<td>Low</td>
<td>No PD detected</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>0 [W]</td>
<td>0 [W]</td>
<td>0 [W]</td>
<td>0 [mA]</td>
<td>Low</td>
<td>No PD detected</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>0 [W]</td>
<td>0 [W]</td>
<td>0 [W]</td>
<td>0 [mA]</td>
<td>Low</td>
<td>PoE not available - No PoE chip found</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>0 [W]</td>
<td>0 [W]</td>
<td>0 [W]</td>
<td>0 [mA]</td>
<td>Low</td>
<td>PoE not available - No PoE chip found</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>0 [W]</td>
<td>0 [W]</td>
<td>0 [W]</td>
<td>0 [mA]</td>
<td>Low</td>
<td>PoE not available - No PoE chip found</td>
<td></td>
</tr>
<tr>
<td>Total</td>
<td>0 [W]</td>
<td>0 [W]</td>
<td>0 [W]</td>
<td>0 [mA]</td>
<td>Low</td>
<td>PoE not available - No PoE chip found</td>
<td></td>
</tr>
</tbody>
</table>

**Local Port**

This is the logical port number for this row.

**PD Class**

Each PD is classified according to a class that defines the maximum power the PD will use. The PD Class shows the PDs class.
Five Classes are defined:
- **Class 0:** the maximum supported power is 15.4W.
- Class 1: the maximum supported power is 4.0W.
- Class 2: the maximum supported power is 7.0W.
- Class 3: the maximum supported power is 15.4W.
- Class 4: the maximum supported power is 30.0W.

**Power Requested**
The Power Requested shows the requested amount of power the PD wants to be reserved.

**Power Allocated**
The Power Allocated shows the amount of power the switch has allocated for the PD.

**Power Used**
The Power Used shows how much power the PD currently is using.

**Current Used**
The Power Used shows how much current the PD currently is using.

**Priority**
The Priority shows the port's priority configured by the user.

**Port Status**
The Port Status shows the port's status. The status can be one of the following values:
- PoE not available - No PoE chip found - PoE not supported for the port.
- PoE turned OFF - PoE disabled : PoE is disabled by user.
- PoE turned OFF - Power budget exceeded - The total requested or used power by the PDs exceeds the maximum power the Power Supply can deliver, and port(s) with the lowest priority is/are powered down.
- No PD detected - No PD detected for the port.
- PoE turned OFF - PD overload - The PD has requested or used more power than the port can deliver, and is powered down.
- PoE turned OFF - PD is off.
- Invalid PD - PD detected, but is not working correctly.

**Buttons**
Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
Refresh: Click to refresh the page.
8.2 PoE power delay

This page is used to set PoE power supply delay time, which can prevent the instant power supply shock when the device is powered on. After the device is powered on, the PoE port first waits for Delay Time, and then powers the PD.

Delay Mode

Enable Delay Mode or not, options as follows:
- Enable
- Disable

Delay Time

Delay power supply of PoE port.

Buttons

Save: Click to save changes.
Reset: Click to undo any changes made locally and revert to previously saved values.
8.3 Policy Configuration

8.3.1 Policy Configuration

When PoE scheduling rule is valid only for a certain period of time, user can set time-based scheduling configuration. Therefore, first user can configure one or more time periods, and then reference the time periods in the rule, the rule will be valid only for the specified time period.

Users that adopt the same name can configure multiple time segments with different contents. After gain the union of each cycle time period and each absolute time period, the intersection of each union will become the final valid time range.

Delete

Delete one scheduling user record.

Name

Username. This is also a link to edit a name. Click the user name to enter the policy subset configuration page.
On the policy subset configuration page, you can set the following items:

- **Type**: the type of scheduling scheme, which can be divided into Periodic scheduling or Absolute scheduling.
- **PStartTime**: Starting time of relative time, format: HH:MM (Hour: Minute).
- **PEndTime**: End time of relative time, format: HH:MM (Hour: Minute).
- **PWeek**: Cycle date of relative time, take one week as a cycle.
- **AStartTime**: Starting time of absolute time, format: HH:MM (Hour: Minute).
- AStartYear: Start date of absolute time, format: YYYY-MM-DD (Year-month-day).
- AEndTime: End time of absolute time, format: HH:MM (Hour: Minute).
- AEndYear: End date of absolute time, format: YYYY-MM-DD (Year-month-day).

**Buttons**

Save: Click to save changes.
Reset: Click to undo any changes made locally and revert to previously saved values.

**State**

User’s current status, it could be Inactive or active.

**Type**

The type of scheduling policy, Periodic scheduling or Absolute scheduling.

**Time-range**

Plan time.

**Buttons**

Add new name: click to add new name.
Save: Click to save changes.
Reset: Click to undo any changes made locally and revert to previously saved values.

### 8.3.2 PoE Policy Binding Configuration

This page can configure the port to bind PoE scheduling scheme.
Mode

Enable Mode or not, options as follows:
- Enable
- Disable

Scheduling

Select an existing scheduling scheme and bind it to the port.

Buttons

Save: Click to save changes.
Reset: Click to undo any changes made locally and revert to previously saved values.

8.4 Auto check

This page can automatically monitor the PoE status of the port.
Ping Check

Global switch for PoE auto-check, options are as follows:

- Enabled
- Disabled

Ping IP Address

Ping the IP address of the remote device.

Startup Time

Startup time (reserved, not enabled).

Interval Time(sec)

Detection interval.

Retry Time

Check the number of fault retries.

Failure Log

Failure log.

Failure Action

Troubleshooting.

Reboot Time(sec)

Restart delay time.

Buttons

Save: Click to save changes.
Reset: Click to undo any changes made locally and revert to previously saved values.
9 Service Quality

9.1 Port Classification

This page allows you to configure the basic QoS Ingress Classification settings for all switch ports.

The displayed settings are:

<table>
<thead>
<tr>
<th>Port</th>
<th>CoS</th>
<th>DPL</th>
<th>PCP</th>
<th>DEI</th>
<th>Tag Class</th>
<th>DSCP Based</th>
<th>Address Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>⇧</td>
<td>⇧</td>
<td>⇧</td>
<td>⇧</td>
<td>Disabled</td>
<td></td>
<td>Source</td>
</tr>
<tr>
<td>2</td>
<td>⇧</td>
<td>⇧</td>
<td>⇧</td>
<td>⇧</td>
<td>Disabled</td>
<td></td>
<td>Source</td>
</tr>
<tr>
<td>3</td>
<td>⇧</td>
<td>⇧</td>
<td>⇧</td>
<td>⇧</td>
<td>Disabled</td>
<td></td>
<td>Source</td>
</tr>
<tr>
<td>4</td>
<td>⇧</td>
<td>⇧</td>
<td>⇧</td>
<td>⇧</td>
<td>Disabled</td>
<td></td>
<td>Source</td>
</tr>
<tr>
<td>5</td>
<td>⇧</td>
<td>⇧</td>
<td>⇧</td>
<td>⇧</td>
<td>Disabled</td>
<td></td>
<td>Source</td>
</tr>
<tr>
<td>6</td>
<td>⇧</td>
<td>⇧</td>
<td>⇧</td>
<td>⇧</td>
<td>Disabled</td>
<td></td>
<td>Source</td>
</tr>
<tr>
<td>7</td>
<td>⇧</td>
<td>⇧</td>
<td>⇧</td>
<td>⇧</td>
<td>Disabled</td>
<td></td>
<td>Source</td>
</tr>
<tr>
<td>8</td>
<td>⇧</td>
<td>⇧</td>
<td>⇧</td>
<td>⇧</td>
<td>Disabled</td>
<td></td>
<td>Source</td>
</tr>
<tr>
<td>9</td>
<td>⇧</td>
<td>⇧</td>
<td>⇧</td>
<td>⇧</td>
<td>Disabled</td>
<td></td>
<td>Source</td>
</tr>
<tr>
<td>10</td>
<td>⇧</td>
<td>⇧</td>
<td>⇧</td>
<td>⇧</td>
<td>Disabled</td>
<td></td>
<td>Source</td>
</tr>
<tr>
<td>11</td>
<td>⇧</td>
<td>⇧</td>
<td>⇧</td>
<td>⇧</td>
<td>Disabled</td>
<td></td>
<td>Source</td>
</tr>
<tr>
<td>12</td>
<td>⇧</td>
<td>⇧</td>
<td>⇧</td>
<td>⇧</td>
<td>Disabled</td>
<td></td>
<td>Source</td>
</tr>
</tbody>
</table>

Save    Reset

Port

The port number for which the configuration below applies.
CoS

Controls the default class of service. All frames are classified to a CoS. There is a one to one mapping between CoS, queue and priority. A CoS of 0 (zero) has the lowest priority.

If the port is VLAN aware, the frame is tagged and Tag Class. is enabled, then the frame is classified to a CoS that is mapped from the PCP and DEI value in the tag. Otherwise the frame is classified to the default CoS.

The classified CoS can be overruled by a QCL entry.

Note:
If the default CoS has been dynamically changed, then the actual default CoS is shown in parentheses after the configured default CoS.

DPL

Controls the default drop precedence level. All frames are classified to a drop precedence level.

If the port is VLAN aware, the frame is tagged and Tag Class. is enabled, then the frame is classified to a DPL that is mapped from the PCP and DEI value in the tag. Otherwise the frame is classified to the default DPL.

The classified DPL can be overruled by a QCL entry.

PCP

Controls the default PCP value. All frames are classified to a PCP value.

If the port is VLAN aware and the frame is tagged, then the frame is classified to the PCP value in the tag. Otherwise the frame is classified to the default PCP value.

DEI

Controls the default DEI value. All frames are classified to a DEI value.

If the port is VLAN aware and the frame is tagged, then the frame is classified to the DEI value in the tag. Otherwise the frame is classified to the default DEI value.

Tag Class

Display the classification mode of label frames on this port. Display the label classification of tagged frames on this port.

- Disabled: Use default CoS and DPL for tagged frames.
- Enabled: Use mapped versions of PCP and DEI for tagged frames.

Click on the mode in order to configure the mode and/or mapping.

Note:
This setting has no effect if the port can’t identify VLAN. Tagged frames received on VLAN
unaware ports are always classified to the default CoS and DPL.

**DSCP-based**

Click to Enable DSCP Based QoS Ingress Port Classification.

**Address Mode**

The IP/MAC address mode specifying whether the QCL classification must be based on source (SMAC/SIP) or destination (DMAC/DIP) addresses on this port. The allowed values are:

- **Source**: Enable SMAC/SIP matching.
- **Destination**: Enable DMAC/DIP matching.

**Buttons**

- **Save**: Click to save changes.
- **Reset**: Click to undo any changes made locally and revert to previously saved values.

### 9.2 Ingress Policy

This page allows you to configure the Policer settings for all switch ports.

The displayed settings are:
Port

The port number for which the configuration below applies.

Enable

Enable or disable the port policer for this switch port.

Rate

Controls the rate for the port policer. This value is restricted to 100-3276700 when "Unit" is kbps or fps, and 1-3276 when "Unit" is Mbps or kfps. The rate is internally rounded up to the nearest value supported by the port policer.

Unit

Controls the unit of measure for the port policer rate as kbps, Mbps, fps or kfps.

Flow Control

If flow control is enabled and the port is in flow control mode, then pause frames are sent instead of discarding frames.

Buttons

Save: Click to save changes.
Reset: Click to undo any changes made locally and revert to previously saved values.
## 9.3 Queue Strategy

This page allows you to configure the Queue Policer settings for all switch ports. The displayed settings are:

<table>
<thead>
<tr>
<th>Port</th>
<th>Queue 0</th>
<th>Queue 1</th>
<th>Queue 2</th>
<th>Queue 3</th>
<th>Queue 4</th>
<th>Queue 5</th>
<th>Queue 6</th>
<th>Queue 7</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>Enable</td>
<td>Enable</td>
<td>Enable</td>
<td>Enable</td>
<td>Enable</td>
<td>Enable</td>
<td>Enable</td>
<td>Enable</td>
</tr>
<tr>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Port**

The port number for which the configuration below applies.

**Enable**

Enable or disable the queue policer for this switch port.

**Rate**

Controls the rate for the queue policer. This value is restricted to 100-3276700 when "Unit" is kbps, and 1-3276 when "Unit" is Mbps. The rate is internally rounded up to the nearest value supported by the queue policer.

This field is only shown if at least one of the queue policers are enabled.

**Unit**

Controls the unit of measure for the queue policer rate as kbps or Mbps.

This field is only shown if at least one of the queue policers are enabled.
Buttons

Save: Click to save changes.
Reset: Click to undo any changes made locally and revert to previously saved values.

9.4 Egress Scheduling

This page provides an overview of QoS Egress Port Schedulers for all switch ports.
The displayed settings are:

<table>
<thead>
<tr>
<th>Port</th>
<th>Mode</th>
<th>Weight</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Q0 Q1 Q2 Q3 Q4 Q5</td>
</tr>
<tr>
<td>1</td>
<td>Strict Priority</td>
<td>- - - - - -</td>
</tr>
<tr>
<td>2</td>
<td>Strict Priority</td>
<td>- - - - - -</td>
</tr>
<tr>
<td>3</td>
<td>Strict Priority</td>
<td>- - - - - -</td>
</tr>
<tr>
<td>4</td>
<td>Strict Priority</td>
<td>- - - - - -</td>
</tr>
<tr>
<td>5</td>
<td>Strict Priority</td>
<td>- - - - - -</td>
</tr>
<tr>
<td>6</td>
<td>Strict Priority</td>
<td>- - - - - -</td>
</tr>
<tr>
<td>7</td>
<td>Strict Priority</td>
<td>- - - - - -</td>
</tr>
<tr>
<td>8</td>
<td>Strict Priority</td>
<td>- - - - - -</td>
</tr>
<tr>
<td>9</td>
<td>Strict Priority</td>
<td>- - - - - -</td>
</tr>
<tr>
<td>10</td>
<td>Strict Priority</td>
<td>- - - - - -</td>
</tr>
<tr>
<td>11</td>
<td>Strict Priority</td>
<td>- - - - - -</td>
</tr>
<tr>
<td>12</td>
<td>Strict Priority</td>
<td>- - - - - -</td>
</tr>
</tbody>
</table>

Port

The switch port number.
Click on the port number in order to configure the schedulers.

Mode

Shows the scheduling mode for this port.

Qn

Shows the weight for this queue and port.

9.5 Egress Shaping

This page provides an overview of QoS Egress Port Shapers for all switch ports.
The displayed settings are:

<table>
<thead>
<tr>
<th>Port</th>
<th>Q0</th>
<th>Q1</th>
<th>Q2</th>
<th>Q3</th>
<th>Q4</th>
<th>Q5</th>
<th>Q6</th>
<th>Q7</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>2</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>3</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>4</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>5</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>6</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>7</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>8</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>9</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>10</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>11</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>12</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

**Port**

The switch port number.

Click on the port number in order to configure the shapers.

**Qn**

Shows "-" for disabled or actual queue shaper rate - e.g. "800 Mbps".

**Port**

Shows "-" for disabled or actual port shaper rate - e.g. "800 Mbps".

### 9.6 Egress Relabeling

This page provides an overview of QoS Egress Port Tag Remarking for all switch ports.

The displayed settings are:
Port

The switch port number.
Click on the port number in order to configure tag remarking.

Mode

Shows the tag remarking mode for this port.
- Classified: Use classified PCP/DEI values.
- Default: Use default PCP/DEI values.
- Mapped: Use mapped versions of QoS class and DP level.

9.7 Port DSCP

This page allows you to configure the basic QoS Port DSCP Configuration settings for all switch ports.
The displayed settings are:
Port

The Port column shows the list of ports for which you can configure dscp ingress and egress settings.

Ingress

In Ingress settings you can change ingress translation and classification settings for individual ports.

There are two configuration parameters available in Ingress:

- Translate
- Classify

Translate

To Enable the Ingress Translation click the checkbox.

Classify

Classification for a port have 4 different values.

- Disable: No Ingress DSCP Classification.
- DSCP=0: Classify if incoming (or translated if enabled) DSCP is 0.
- Selected: Classify only selected DSCP for which classification is enabled as specified in DSCP Translation window for the specific DSCP.
- All: all DSCP are classified.

**Egress**

Port Egress Rewriting can be one of:

- Disabled: no egress rewrite.
- Enable: enable rewrite without remapping.
- Remap DP Unaware: DSCP from analyzer is remapped and frame is remarked with remapped DSCP value. The remapped DSCP value is always taken from the “DSCP Conversion > Egress Remap DP0” table.
- Remap DP Aware: DSCP from analyzer is remapped and frame is remarked with remapped DSCP value. According to the DP level of the frame, the remapped DSCP value can be obtained from either the “DSCP Conversion > Egress Remap DP0” table or the “DSCP Conversion > Egress Remap DP1” table.

**Buttons**

Save: Click to save changes.
Reset: Click to undo any changes made locally and revert to previously saved values.

### 9.8 DSCP-based QoS

This page allows you to configure basic QoS DSCP ingress classification settings based on QoS DSCP for all switches.

The displayed settings are:
<table>
<thead>
<tr>
<th>DSCP</th>
<th>Trust</th>
<th>QoS Class</th>
<th>DPL</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>0 (BE)</td>
<td>☐</td>
<td>0 ▼</td>
<td>0 ▼</td>
</tr>
<tr>
<td>1</td>
<td>☐</td>
<td>0 ▼</td>
<td>0 ▼</td>
</tr>
<tr>
<td>2</td>
<td>☐</td>
<td>0 ▼</td>
<td>0 ▼</td>
</tr>
<tr>
<td>3</td>
<td>☐</td>
<td>0 ▼</td>
<td>0 ▼</td>
</tr>
<tr>
<td>4</td>
<td>☐</td>
<td>0 ▼</td>
<td>0 ▼</td>
</tr>
<tr>
<td>5</td>
<td>☐</td>
<td>0 ▼</td>
<td>0 ▼</td>
</tr>
<tr>
<td>6</td>
<td>☐</td>
<td>0 ▼</td>
<td>0 ▼</td>
</tr>
<tr>
<td>7</td>
<td>☐</td>
<td>0 ▼</td>
<td>0 ▼</td>
</tr>
<tr>
<td>8 (CS1)</td>
<td>☐</td>
<td>0 ▼</td>
<td>0 ▼</td>
</tr>
<tr>
<td>9</td>
<td>☐</td>
<td>0 ▼</td>
<td>0 ▼</td>
</tr>
<tr>
<td>10 (AF11)</td>
<td>☐</td>
<td>0 ▼</td>
<td>0 ▼</td>
</tr>
<tr>
<td>11</td>
<td>☐</td>
<td>0 ▼</td>
<td>0 ▼</td>
</tr>
<tr>
<td>12 (AF12)</td>
<td>☐</td>
<td>0 ▼</td>
<td>0 ▼</td>
</tr>
<tr>
<td>13</td>
<td>☐</td>
<td>0 ▼</td>
<td>0 ▼</td>
</tr>
<tr>
<td>14 (AF13)</td>
<td>☐</td>
<td>0 ▼</td>
<td>0 ▼</td>
</tr>
<tr>
<td>15</td>
<td>☐</td>
<td>0 ▼</td>
<td>0 ▼</td>
</tr>
<tr>
<td>16 (CS2)</td>
<td>☐</td>
<td>0 ▼</td>
<td>0 ▼</td>
</tr>
<tr>
<td>17</td>
<td>☐</td>
<td>0 ▼</td>
<td>0 ▼</td>
</tr>
<tr>
<td>18 (AF21)</td>
<td>☐</td>
<td>0 ▼</td>
<td>0 ▼</td>
</tr>
<tr>
<td>19</td>
<td>☐</td>
<td>0 ▼</td>
<td>0 ▼</td>
</tr>
<tr>
<td>20 (AF22)</td>
<td>☐</td>
<td>0 ▼</td>
<td>0 ▼</td>
</tr>
<tr>
<td>21</td>
<td>☐</td>
<td>0 ▼</td>
<td>0 ▼</td>
</tr>
<tr>
<td>22 (AF23)</td>
<td>☐</td>
<td>0 ▼</td>
<td>0 ▼</td>
</tr>
<tr>
<td>23</td>
<td>☐</td>
<td>0 ▼</td>
<td>0 ▼</td>
</tr>
<tr>
<td>24 (CS3)</td>
<td>☐</td>
<td>0 ▼</td>
<td>0 ▼</td>
</tr>
<tr>
<td>25</td>
<td>☐</td>
<td>0 ▼</td>
<td>0 ▼</td>
</tr>
<tr>
<td>26 (AF31)</td>
<td>☐</td>
<td>0 ▼</td>
<td>0 ▼</td>
</tr>
<tr>
<td>27</td>
<td>☐</td>
<td>0 ▼</td>
<td>0 ▼</td>
</tr>
<tr>
<td>28 (AF32)</td>
<td>☐</td>
<td>0 ▼</td>
<td>0 ▼</td>
</tr>
<tr>
<td>29</td>
<td>☐</td>
<td>0 ▼</td>
<td>0 ▼</td>
</tr>
<tr>
<td>30 (AF33)</td>
<td>☐</td>
<td>0 ▼</td>
<td>0 ▼</td>
</tr>
<tr>
<td>31</td>
<td>☐</td>
<td>0 ▼</td>
<td>0 ▼</td>
</tr>
<tr>
<td>32 (CS4)</td>
<td>☐</td>
<td>0 ▼</td>
<td>0 ▼</td>
</tr>
<tr>
<td>33</td>
<td>☐</td>
<td>0 ▼</td>
<td>0 ▼</td>
</tr>
<tr>
<td>34 (AF41)</td>
<td>☐</td>
<td>0 ▼</td>
<td>0 ▼</td>
</tr>
</tbody>
</table>
**DSCP**

Maximum number of supported DSCP values are 64.

**Trust**

Controls whether a specific DSCP value is trusted. Only frames with trusted DSCP values are mapped to a specific QoS class and Drop Precedence Level. Frames with untrusted DSCP values are treated as a non-IP frame.

**QoS Class**

QoS class value can be any of (0-7).
DPL

Drop Precedence Level (0-1).

Buttons

Save: Click to save changes.
Reset: Click to undo any changes made locally and revert to previously saved values.

9.9 DSCP Conversion

This page allows you to configure the basic QoS DSCP Translation settings for all switches. DSCP translation can be done in Ingress or Egress.
The displayed settings are:
## DSCP Translation

<table>
<thead>
<tr>
<th>DSCP</th>
<th>Ingress</th>
<th>Egress</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Translate</td>
<td>Classify</td>
</tr>
<tr>
<td>*</td>
<td>&lt;= ▼</td>
<td>□</td>
</tr>
<tr>
<td>0 (BE)</td>
<td>▼ 0 (BE) ▼</td>
<td>□</td>
</tr>
<tr>
<td>1</td>
<td>▼ 1 ▼</td>
<td>□</td>
</tr>
<tr>
<td>2</td>
<td>▼ 2 ▼</td>
<td>□</td>
</tr>
<tr>
<td>3</td>
<td>▼ 3 ▼</td>
<td>□</td>
</tr>
<tr>
<td>4</td>
<td>▼ 4 ▼</td>
<td>□</td>
</tr>
<tr>
<td>5</td>
<td>▼ 5 ▼</td>
<td>□</td>
</tr>
<tr>
<td>6</td>
<td>▼ 6 ▼</td>
<td>□</td>
</tr>
<tr>
<td>7</td>
<td>▼ 7 ▼</td>
<td>□</td>
</tr>
<tr>
<td>8 (CS1)</td>
<td>▼ 8 (CS1) ▼</td>
<td>□</td>
</tr>
<tr>
<td>9</td>
<td>▼ 9 ▼</td>
<td>□</td>
</tr>
<tr>
<td>10 (AF1)</td>
<td>▼ 10 (AF1) ▼</td>
<td>□</td>
</tr>
<tr>
<td>11</td>
<td>▼ 11 ▼</td>
<td>□</td>
</tr>
<tr>
<td>12 (AF2)</td>
<td>▼ 12 (AF2) ▼</td>
<td>□</td>
</tr>
<tr>
<td>13</td>
<td>▼ 13 ▼</td>
<td>□</td>
</tr>
<tr>
<td>14 (AF3)</td>
<td>▼ 14 (AF3) ▼</td>
<td>□</td>
</tr>
<tr>
<td>15</td>
<td>▼ 15 ▼</td>
<td>□</td>
</tr>
<tr>
<td>16 (CS2)</td>
<td>▼ 16 (CS2) ▼</td>
<td>□</td>
</tr>
<tr>
<td>17</td>
<td>▼ 17 ▼</td>
<td>□</td>
</tr>
<tr>
<td>18 (AF4)</td>
<td>▼ 18 (AF4) ▼</td>
<td>□</td>
</tr>
<tr>
<td>19</td>
<td>▼ 19 ▼</td>
<td>□</td>
</tr>
<tr>
<td>20 (AF5)</td>
<td>▼ 20 (AF5) ▼</td>
<td>□</td>
</tr>
<tr>
<td>21</td>
<td>▼ 21 ▼</td>
<td>□</td>
</tr>
<tr>
<td>22 (AF6)</td>
<td>▼ 22 (AF6) ▼</td>
<td>□</td>
</tr>
<tr>
<td>23</td>
<td>▼ 23 ▼</td>
<td>□</td>
</tr>
<tr>
<td>24 (CS3)</td>
<td>▼ 24 (CS3) ▼</td>
<td>□</td>
</tr>
<tr>
<td>25</td>
<td>▼ 25 ▼</td>
<td>□</td>
</tr>
<tr>
<td>26 (AF7)</td>
<td>▼ 26 (AF7) ▼</td>
<td>□</td>
</tr>
<tr>
<td>27</td>
<td>▼ 27 ▼</td>
<td>□</td>
</tr>
<tr>
<td>28 (AF8)</td>
<td>▼ 28 (AF8) ▼</td>
<td>□</td>
</tr>
<tr>
<td>29</td>
<td>▼ 29 ▼</td>
<td>□</td>
</tr>
<tr>
<td>30 (AF9)</td>
<td>▼ 30 (AF9) ▼</td>
<td>□</td>
</tr>
<tr>
<td>31</td>
<td>▼ 31 ▼</td>
<td>□</td>
</tr>
<tr>
<td>32 (CS4)</td>
<td>▼ 32 (CS4) ▼</td>
<td>□</td>
</tr>
<tr>
<td>33</td>
<td>▼ 33 ▼</td>
<td>□</td>
</tr>
<tr>
<td>34 (AF10)</td>
<td>▼ 34 (AF10) ▼</td>
<td>□</td>
</tr>
<tr>
<td>35</td>
<td>▼ 35 ▼</td>
<td>□</td>
</tr>
<tr>
<td>36 (AF11)</td>
<td>▼ 36 (AF11) ▼</td>
<td>□</td>
</tr>
<tr>
<td>37</td>
<td>▼ 37 ▼</td>
<td>□</td>
</tr>
<tr>
<td>38 (AF12)</td>
<td>▼ 38 (AF12) ▼</td>
<td>□</td>
</tr>
<tr>
<td>39</td>
<td>▼ 39 ▼</td>
<td>□</td>
</tr>
<tr>
<td>40 (CS5)</td>
<td>▼ 40 (CS5) ▼</td>
<td>□</td>
</tr>
</tbody>
</table>
DSCP

Maximum number of supported DSCP values are 64 and valid DSCP value ranges from 0 to 63.

Ingress

Before using DSCP to realize QoS class and DPL mapping, the DSCP at the entrance can be converted into a new DSCP.

There are two configuration parameters for DSCP mapping:
- Translate
- Classify

Translate

DSCP at Ingress side can be translated to any of (0-63) DSCP values.

Classify

Click to enable Classification at Ingress side.

Egress

There are the following configurable parameters for Egress side:
- Remap DP0: Controls the remapping for frames with DP level 0.
- Remap DP1: Controls the remapping for frames with DP level 1.

**Remap DP0**

Select the DSCP value from the drop-down list that needs to be remapped. DSCP value ranges from 0 to 63.

**Remap DP1**

Select the DSCP value from the drop-down list that needs to be remapped. DSCP value ranges from 0 to 63.

**Buttons**

Save: Click to save changes.
Reset: Click to undo any changes made locally and revert to previously saved values.

### 9.10 DSCP Classification

This page allows you to configure the mapping of QoS class and Drop Precedence Level to DSCP value.

The displayed settings are:

<table>
<thead>
<tr>
<th>QoS Class</th>
<th>DSCP DP0</th>
<th>DSCP DP1</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0 (BE)</td>
<td>0 (BE)</td>
</tr>
<tr>
<td>1</td>
<td>0 (BE)</td>
<td>0 (BE)</td>
</tr>
<tr>
<td>2</td>
<td>0 (BE)</td>
<td>0 (BE)</td>
</tr>
<tr>
<td>3</td>
<td>0 (BE)</td>
<td>0 (BE)</td>
</tr>
<tr>
<td>4</td>
<td>0 (BE)</td>
<td>0 (BE)</td>
</tr>
<tr>
<td>5</td>
<td>0 (BE)</td>
<td>0 (BE)</td>
</tr>
<tr>
<td>6</td>
<td>0 (BE)</td>
<td>0 (BE)</td>
</tr>
<tr>
<td>7</td>
<td>0 (BE)</td>
<td>0 (BE)</td>
</tr>
</tbody>
</table>

**QoS Class**

Actual QoS class.

**DSCP DP0**

Select the classified DSCP value (0-63) for Drop Precedence Level 0.
DSCP DP1
Select the classified DSCP value (0-63) for Drop Precedence Level 1.

Buttons
Save: Click to save changes.
Reset: Click to undo any changes made locally and revert to previously saved values.

9.11 QoS Control List

QoS Control List Configuration
This page shows the QoS Control List (QCL), which is made up of the QCEs. Each row describes a QCE that is defined. The maximum number of QCEs is 256 on each switch.
Click on the lowest plus sign to add a new QCE to the list.

<table>
<thead>
<tr>
<th>QCE</th>
<th>Port</th>
<th>DMAC</th>
<th>SMAC</th>
<th>Tag Type</th>
<th>VID</th>
<th>PCP</th>
<th>DEI</th>
<th>Frame Type</th>
<th>CoS</th>
<th>DPL</th>
<th>DSCP</th>
<th>PCP</th>
<th>DEI</th>
<th>Policy</th>
</tr>
</thead>
</table>

QCE
Indicates the QCE id.

Port
Indicates the list of ports configured with the QCE or 'Any'.

DMAC
Indicates the destination MAC address. The possible values are:
- Any: Match any DMAC.
- Unicast: Match unicast DMAC.
- Multicast: Match multicast DMAC.
- Broadcast: Match broadcast DMAC.
The default value is 'Any'.

SMAC
Match specific source MAC address or 'Any'.
If a port is configured to match on destination addresses, this field indicates the DMAC.
Tag Type

Indicates tag type. The possible values are:
- Any: Match tagged and untagged frames.
- Untagged: Match untagged frames.
- Tagged: Match tagged frames.
The default value is 'Any'.

VID

Indicates (VLAN ID), either a specific VID or range of VIDs. The range of VID can be 1-4095 or "any".

PCP

Priority Code Point: Valid values of PCP are specific (0, 1, 2, 3, 4, 5, 6, 7) or range (0-1, 2-3, 4-5, 6-7, 0-3, 4-7) or 'Any'.

DEI

Drop Eligible Indicator: Valid value of DEI are 0, 1 or 'Any'.

Frame Type

Indicates the type of frame. The possible values are:
- Any: Match any frame type.
- Ethernet: Match EtherType frames.
- LLC: Match (LLC) frames.
- SNAP: Match (SNAP) frames.
- IPv4: Match IPv4 frames.
- IPv6: Match IPv6 frames.

Action

Indicates the classification action taken on ingress frame if parameters configured are matched with the frame's content.
Possible actions are:
- CoS: Classify Class of Service.
- DPL: Classify Drop Precedence Level.
- DSCP: Classify DSCP value.
- PCP: Classify PCP value.
- DEI: Classify DEI value.
- Policy: Classify ACL Policy number.

Modification Buttons

You can modify each QCE (QoS Control Entry) in the table using the following buttons:

➕: Insert a new QCE before the current row.
9.12 QoS Statistics

This page provides statistics for the different queues for all switch ports. The displayed counters are:

<table>
<thead>
<tr>
<th>Port</th>
<th>Q0 Rx</th>
<th>Q0 Tx</th>
<th>Q1 Rx</th>
<th>Q1 Tx</th>
<th>Q2 Rx</th>
<th>Q2 Tx</th>
<th>Q3 Rx</th>
<th>Q3 Tx</th>
<th>Q4 Rx</th>
<th>Q4 Tx</th>
<th>Q5 Rx</th>
<th>Q5 Tx</th>
<th>Q6 Rx</th>
<th>Q6 Tx</th>
<th>Q7 Rx</th>
<th>Q7 Tx</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>5</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>6</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>7</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>8</td>
<td>7355</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>9</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>10</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>11</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>12</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

**Port**

The switch port number.

**Qn**

There are 8 QoS queues per port. Q0 is the lowest priority queue.

**Rx/Tx**

The number of received and transmitted packets per queue.
Buttons

Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
Refresh: Click to refresh the page immediately.
Clear: Clears the counters for all ports.

9.13 QCL Status

QCL Status

This page shows the QCL status by different QCL users. Each row describes the QCE that is defined. It is a conflict if a specific QCE is not applied to the hardware due to hardware limitations. The maximum number of QCEs is 256 on each switch.

<table>
<thead>
<tr>
<th>User</th>
<th>QCE</th>
<th>Port</th>
<th>Frame Type</th>
<th>Action</th>
<th>Conflict</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

User

Indicates the QCL user.

QCE

Indicates the QCE id.

Port

Indicates the list of ports configured with the QCE.

Frame Type

Indicates the type of frame. The possible values are:
- Any: Match any frame type.
- Ethernet: Match EtherType frames.
- LLC: Match (LLC) frames.
- SNAP: Match (SNAP) frames.
- IPv4: Match IPv4 frames.
- IPv6: Match IPv6 frames.

Action

Indicates the classification action taken on ingress frame if parameters configured are matched with the frame's content.
Possible actions are:

- **CoS**: Classify Class of Service.
- **DPL**: Classify Drop Precedence Level.
- **DSCP**: Classify DSCP value.
- **PCP**: Classify PCP value.
- **DEI**: Classify DEI value.
- **Policy**: Classify ACL Policy number.

**Conflict**

Displays Conflict status of QCL entries. As H/W resources are shared by multiple applications. It may happen that resources required to add a QCE may not be available, in that case it shows conflict status as ‘Yes’, otherwise it is always ‘No’. Please note that conflict can be resolved by releasing the H/W resources required to add QCL entry on pressing ‘Resolve Conflict’ button.

**Buttons**

Select QCL status from the drop-down list.

Auto-refresh: Check this box to enable an automatic refresh. Automatic refresh occurs every 3 seconds.

Resolve Conflict: Click to release the resources required to add QCL entry, in case the conflict status for any QCL entry is ‘yes’.

Refresh: Click to refresh the page.
10 System Diagnosis

10.1 Mirroring

Mirroring is a feature for switched port analyzer. The administrator can use the Mirroring to debug network problems. The selected traffic can be mirrored or copied on a destination port where a network analyzer can be attached to analyze the network traffic.

If you want to get the tagged mirrored traffic, you have to set VLAN egress tagging as "Tag All" on the reflector port. On the other hand, if you want to get untagged mirrored traffic, you have to set VLAN egress tagging as "Untag ALL" on the reflector port.
Mirror Configuration

Port to mirror to

This checkbox is designed for selecting destination port. The destination port is a switched port that you receive a copy of traffic from the source port.

Notice:
- On mirror mode, the device only supports one destination port.
- The destination port needs to disable MAC Table learning.

Mirror Port Configuration

Port

The switch port number.

Mode

Enable/disable Mirroring function.

Buttons

Save: Click to save changes.
Reset: Click to undo any changes made locally and revert to previously saved values.

10.2 Ping

This page allows you to issue ICMP PING packets to troubleshoot IP connectivity issues.

![ICMP Ping Table]

After pressing “Start”, ICMP packet is sent, and serial number and round trip time are displayed after receiving reply. The amount of data received in an IP packet of ICMP ECHO_REPLY type is always 8 bytes more than the requested data space (ICMP header). The page refreshes automatically until responses to all packets are received, or until a timeout occurs.

PING server 192.168.1.61, 56 bytes of data.
64 bytes from 192.168.1.61: icmp_seq=0, time=0ms
64 bytes from 192.168.1.61: icmp_seq=1, time=0ms
64 bytes from 192.168.1.61: icmp_seq=2, time=0ms
64 bytes from 192.168.1.61: icmp_seq=3, time=0ms
64 bytes from 192.168.1.61: icmp_seq=4, time=0ms
Sent 5 packets, received 5 OK, 0 bad

You can configure the following properties of the issued ICMP packets:

**IP Address**

The destination IP Address.

**Ping Length**

The payload size of the ICMP packet. Values range from 2 bytes to 1452 bytes.

**Ping Count**

The count of the ICMP packet. Values range from 1 time to 60 times.
Ping Interval

The interval of the ICMP packet. Values range from 0 second to 30 seconds.

Buttons

Start: Click Start to send ICMP data package.
New Ping: Click to restart diagnostics with PING.

10.3 Cable Detection

This page is used for running the VeriPHY Cable Diagnostics for 10/100 and 1G copper ports.

<table>
<thead>
<tr>
<th>Cable Diagnostics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Cable Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
</tr>
<tr>
<td>------</td>
</tr>
<tr>
<td>1</td>
</tr>
<tr>
<td>2</td>
</tr>
<tr>
<td>3</td>
</tr>
<tr>
<td>4</td>
</tr>
<tr>
<td>5</td>
</tr>
<tr>
<td>6</td>
</tr>
<tr>
<td>7</td>
</tr>
<tr>
<td>8</td>
</tr>
</tbody>
</table>

Press "Start" to run diagnostics. This will take approximately 5 seconds. If all ports are selected, this can take approximately 15 seconds. When completed, the page refreshes automatically, and you can view the cable diagnostics results in the cable status table. Please note that VeriPHY is only applicable to cables with a length of 7-140m.

10 and 100 Mbps ports will be linked down while running VeriPHY. Therefore, running VeriPHY on a 10 or 100 Mbps management port will cause the switch to stop responding until VeriPHY is complete.
Port

The port where you are requesting VeriPHY Cable Diagnostics.

Cable Status

Port

Switch port number.

Pair

The status of the cable pair.
OK - Correctly terminated pair
Open - Open pair
Short - Shorted pair
Short A - Cross-pair short to pair A
Short B - Cross-pair short to pair B
Short C - Cross-pair short to pair C
Short D - Cross-pair short to pair D
Cross A - Abnormal cross-pair coupling with pair A
Cross B - Abnormal cross-pair coupling with pair B
Cross C - Abnormal cross-pair coupling with pair C
Cross D - Abnormal cross-pair coupling with pair D

Length

Length of cable pair (m). The resolution is 3m.
11 System Maintenance

11.1 Restart Device

You can restart the switch on this page. After restart, the switch will boot normally.

![Restart Device]

**Buttons**

Yes: Click to restart the device.
No: Click to return to the port status page without restarting.

11.2 Restore Factory Settings

You can reset the configuration of the switch on this page. Only the IP configuration is retained.
The new configuration is available immediately, which means that no restart is necessary.
11.3 Upgrade

This page facilitates an update of the firmware controlling the switch.

"Choose File" in the software firmware, and then click "Update". After uploading the software firmware, the page will announce to start the firmware update. After about a minute, the firmware is updated and the switch restarts.

Warning:

When firmware is being updated, network access seems to be unavailable. The front LED flashes Green/Off with a frequency of 10 Hz while the firmware update is in progress. Do not restart or power off the device at this time or the switch may fail to function afterwards.
11.4 Firmware Selection

This page provides information about the active and standby (backup) firmware in the device, and allows recovery to the standby firmware.

The WEB page displays two tables containing information about the active firmware and the standby firmware.

| Image File name of firmware, starting from the time when firmware was last updated. |
| Version | The version of the firmware. |
| Date | The date where the firmware was produced. |
| Buttons | Activate alternate firmware: click to use alternate image. This button may be disabled depending on system state. Undo: deactivate the backup image. Navigates away from this page. |

Note:
- If the active firmware is an alternate image, only the “Active Firmware” table is displayed. In this case, the activate standby firmware button is also disabled.
- If the standby firmware is active (due to damage to the main firmware or manual intervention), uploading new firmware to the device will automatically use the main firmware slot and activate it.
- The firmware version and date information may be empty for older firmware releases. This does not constitute an error.
The switch stores its configuration in a number of text files in CLI format. These files are either virtual (based on RAM) or stored in Flash on the switch.

Available documents are:

- running-config: representing the virtual file currently configured by the activity on the switch. This file is volatile.
- startup-config: The startup configuration for the switch, read at boot time. If this file doesn't exist at boot time, the switch will start up in default configuration.
- default-config: A read-only file with vendor-specific configuration. This file is read when the system is restored to default settings.
- Up to 31 other files, typically used for configuration backups or alternative configurations.

12.1 Save startup-config

This will copy running-config to startup-config, thus ensuring that the currently active configuration will be used on the next restart.
12.2 Download

It is possible to download any of the files on the switch to the WEB browser. Select the file and click “Download Configuration File”. Running-config download may take some time to complete, because files must be prepared for download.

12.3 Upload

It is possible to upload a file from the WEB browser to all the files on the switch, except default-config which is read-only. Select the file to upload, select the target file on the target file, and then click “Upload Configuration”.
If the target is running-config, the file will be applied to the switch configuration. This can be achieved in two ways:

- Replace mode: the current configuration is completely replaced with the configuration in the uploaded file.
- Merge mode: the uploaded files are merged into running-config.

If the Flash file system is full (that is, it contains the default configuration and 32 other files, usually including startup-config), it is impossible to create a new file. Instead an existing file must be overwritten or another file must be deleted.

### 12.4 Activate

You can activate any configuration file on the switch, except that running-config represents the currently active configuration.
Select the file to activate and click "Activate Configuration". This will initiate the process of completely replacing the existing configuration with that of the selected file.

**12.5 Delete**

It is possible to delete any of the writable files stored in Flash, including startup-config. If this is done and the switch is rebooted without a prior Save operation, this effectively resets the switch to default configuration.
13 FAQ

13.1 Sign in Problems

1. Why the web page display abnormally when browsing the configuration via WEB?
   Before accessing the WEB, please eliminate IE cache buffer and cookies. Otherwise, the web page will display abnormally.

2. What should I do if I forget my login password?
   If you forget the login password, you can initialize the password by restoring the factory settings, and the device can be initialized by using the function of restoring the factory settings through the network management software. In the first minute when the switch is restarted, a physical loopback is made between port 1 and port 2, which can also restore the device to the factory settings. The factory setting can also be restored by setting the corresponding factory setting switch to the ON position.

13.2 Configuration Problem

1. Why the bandwidth can’t be increased after configuring Trunking (port aggregation) function?
   Check whether the port attributes set to Trunking are consistent, such as rate, duplex mode, VLAN and other attributes.

2. How to deal with the problem that part of switch ports are impassable?
   When some ports on the switch are impassable, it may be network cable, network adapter and switch port faults. User can locate the faults via following tests:
   - Keep connected computer and switch ports unchanged, change other network cables;
- Keep connected network cable and switch port unchanged, change other computers;
- Keep connected network cable and computer unchanged, change other switch port;
- If the switch port faults are confirmed, please contact supplier for maintenance.

3. **How about the order of port self-adaption state detection?**
   The port self-adaption state detection is conducted according to following order: 1000Mbps full duplex, 100Mbps full duplex, 100Mbps half-duplex, 10Mbps full duplex, 10Mbps half-duplex, detect from high to low, connect automatically in supported highest speed.

### 13.3 Indicator Problem

1. **Why is the power supply indicator off?**
   Possible reasons include:
   - Not connected to the power socket; troubleshooting, connected to the power socket.
   - Power supply or indicators faults; troubleshooting, change the power supply or device test.
   - Power supply voltage can't meet the device requirements; troubleshooting, configure the power supply voltage according to the device manual.

2. **Link/Act indicator isn't bright, what's the reason?**
   Possible reasons include:
   - The network cable portion of Ethernet copper port is disconnected or bad contact; troubleshooting, connect the network cable again.
   - Ethernet terminal device or network card works abnormally; troubleshooting, eliminate the terminal device fault.
   - Not connected to the power socket; troubleshooting, connected to the power socket.
   - Interface rate doesn't match the pattern; troubleshooting, examine whether the device transmission speed matches the duplex mode.

3. **Ethernet copper port and fiber port indicator are connected normally, but can't transmit data, what's the reason?**
When the system is power on or network configuration changes, the device and switch configuration in the network will need some time. Troubleshooting, after the device and switch configuration are completed, Ethernet data can be transmitted; if it's impassable, power off the system, and power on again.

4. Why does the communication crashes after a period of time, namely, it cannot communicate, and it returns to normal after restarting?

Reasons may include:
- Surrounding environment disturbs the product; troubleshooting, product grounding adopts shielding line or shields the interference source.
- Site wiring is not normative; Troubleshooting, optical fiber, network cable, optical cable cannot be arranged with power line and high-voltage line.
- Network cable is disturbed by static electricity or surge; Troubleshooting, change the shielded cable or install a lightning protector.
- High and low temperature influence; troubleshooting, check the device temperature usage range.
14 Maintenance and Service

Since the date of product delivery, our company provides 5-year product warranty. According to our company's product specification, during the warranty period, if the product exists any failure or functional operation fails, our company will repair or replace the product for users free of charge. However, the commitments above do not cover damage caused by improper usage, accident, natural disaster, incorrect operation or improper installation.

In order to ensure that consumers benefit from our company's managed switch products, consumers can get help and solutions in the following ways:

- Internet Service;
- Service Hotline;
- Product repair or replacement;

14.1 Internet Service

More useful information and tips are available via our company website.
Website: http://www.indu-sol.com

14.2 Service Hotline

Users of our company's products could call technical support office for help. Our company has professional technical engineers to answer your questions and help you to solve the product or usage problems ASAP. Free service hotline: +49 34491 58014
14.3 Product Repair or Replacement

As for the product repair, replacement or return, customers should firstly confirm with the company's technical staff, and then contact the salesmen to solve the problem. According to the company's handling procedure, customers should negotiate with our company's technical staff and salesmen to complete the product maintenance, replacement or return.