



---

---

## **PDS-204GCO™ Web Management User Guide**

---

---

### **Introduction**

---

PDS-204GCO™ is a next-generation outdoor Power over Ethernet (PoE) switch for smart cities. It allows Wi-Fi® access points, security network cameras, and many other IoT devices to receive power and data over standard Ethernet cables, leaving network infrastructure completely unaltered.

This user guide describes the initial configuration of the PDS-204GCO™ network switch using the Web interface.

---

---

# Table of Contents

---

Introduction.....	1
1. Initial Configuration.....	4
1.1. Unit Default IP Address, Username, and Password Configuration.....	4
1.2. Setting Unit IP Address .....	4
1.3. Saving Configuration Changes.....	5
1.4. Avoiding Unit Network Management Connection Loss.....	5
2. Restoring PDS-204GCO Unit to Factory Default.....	6
2.1. Restoring Unit to Factory Default—Unknown Unit-IP, Username, or Unit Password.....	6
2.2. Restoring Unit to Factory Default From Web Interface.....	6
3. Web Interface.....	7
3.1. Home Web Page.....	7
4. Web Interface—Configuration.....	14
4.1. System Configuration.....	14
4.2. Green Ethernet—Port Power Saving Configuration.....	22
4.3. Port Configuration.....	23
4.4. Connectivity Fault Management (CFM) Configuration.....	24
4.5. APS Configuration.....	29
4.6. ERPS Configuration.....	30
4.7. DHCPv4 Snooping Configuration.....	31
4.8. DHCPv6 Snooping Configuration.....	32
4.9. Security Configuration.....	33
4.10. Security Aggregation Configuration.....	60
4.11. Loop Protection Configuration.....	62
4.12. Spanning Tree Configuration.....	62
4.13. LLDP Configuration.....	66
4.14. PoE Configuration.....	72
4.15. MAC Table Configuration.....	74
4.16. VLAN Configurations.....	75
4.17. QoS Configuration.....	77
4.18. Mirroring Configuration.....	85
4.19. UPnP Configuration.....	88
4.20. sFlow Configuration.....	88
5. Web Interface—Monitor.....	91
5.1. Monitor System.....	91
5.2. Monitor Green Ethernet Port Power Savings.....	94
5.3. Monitor Ports.....	95
5.4. Monitor CFM Status.....	101
5.5. Monitor APS.....	102
5.6. Monitor ERPS.....	104
5.7. Monitor DHCPv4.....	105
5.8. Monitor DHCPv6.....	106
5.9. Monitor Security.....	107

---



---

5.10. Monitor Aggregation.....	118
5.11. Monitor Loop Protection.....	120
5.12. Monitor Spanning Tree.....	120
5.13. Monitor LLDP.....	121
5.14. Monitor PoE.....	125
5.15. Monitor MAC Table.....	126
5.16. Monitor VLANs.....	127
5.17. Monitor sFlow.....	128
6. Web Interface—Diagnostics.....	130
6.1. Diagnostics Ping (IPv4).....	130
6.2. Diagnostics Ping (IPv6).....	131
6.3. Diagnostics—Traceroute (IPv4).....	131
6.4. Diagnostics—Traceroute (IPv6).....	132
6.5. Diagnostics VeriPHY.....	133
7. Web Interface—Maintenance.....	135
7.1. Restart Device.....	135
7.2. Factory Defaults.....	135
7.3. Maintenance Software.....	135
7.4. Maintenance—Configuration.....	136
8. Revision History.....	138
Microchip Information.....	139
The Microchip Website.....	139
Product Change Notification Service.....	139
Customer Support.....	139
Microchip Devices Code Protection Feature.....	139
Legal Notice.....	139
Trademarks.....	140
Quality Management System.....	141
Worldwide Sales and Service.....	142

## 1. Initial Configuration

You can configure the PDS-204GCO unit for the first time using a web interface or Telnet/SSH. Microchip recommends to using web interface to configure the unit easily.

For information regarding Telnet/SSH configuration, see the *CLI Commands User Manual*.

### 1.1 Unit Default IP Address, Username, and Password Configuration

The PDS-204GCO outdoor PoE switch is shipped with the following specifications:

- Default IP address: 192.168.0.50
- Username: admin
- Password: A unique random password is provided on the label attached to the left side of the device. It varies from unit to unit.

When you restore unit to factory default by using external loopback and no PoE Powered Devices (PDs) upon power up, the unit to IP address 192.168.0.50, username as admin, and same unique password (not to be confused with restoring the unit to factory default from the web which keeps the unit same IP address) are restored.

**Note:** User is responsible to keep a record of the unit's default unique password. The unit's unique password cannot be retrieved beyond the label on the left side of the device.

### 1.2 Setting Unit IP Address

The following figure and steps show how to set the unit IP address for the first time.

Figure 1-1. Unit IP Address Window

The screenshot shows the web interface for the PDS-204GCO Outdoor PoE-BT Switch. The left sidebar contains a navigation menu with 'Configuration' expanded and 'System' selected, with 'IP' highlighted. The main content area is titled 'IP Configuration' and includes the following sections:

- IP Configuration:** Fields for Domain Name, DNS Server 0, DNS Server 1, DNS Server 2, DNS Server 3, and DNS Proxy.
- IP Interfaces:** A table with columns: Delete, IF, Enable, Type, Client ID (Opt #61) (IFMac, ASCII, HEX), Hostname (Opt #12), Fallback, Current Lease, IPv4 Address, and Mask Length. The row for VLAN 1 shows IP address 192.168.0.50 and Mask Length 24.
- IP Routes (Default-Gateway):** A table with columns: Delete, Network, Mask Length, Gateway, Next Hop VLAN (IPv6), and Distance.

Yellow arrows point to the 'IP' menu item, the 'Address' and 'Mask Length' fields in the IP Interfaces table, and the 'Save' button at the bottom.

1. Navigate to unit IP address 192.168.0.50 using the username and password, as described in the preceding section.
2. Navigate to the web page **Configuration > System > IP** to modify the unit IP address.
3. Click **Save** to change the unit running IP address to the new address.
4. Press the upright storage icon to save `running-config` into `startup-config`.

### 1.3 Saving Configuration Changes

When you click **Save** on various configuration web pages, the modified parameter is immediately changed as part of `running-config`. However, it is not permanently saved until an explicit configuration save action is done.

The following are the three different ways to save `running-config` into `startup-config`:

- From the web browser, click the storage icon at top right: .
- From web browser, open the web page **Maintenance > Configuration > Save startup-config**.
- From Telnet/SSH, type the command: `copy running-config startup-config`.

**Figure 1-2. Save running-config to startup-config From Telnet/SSH CLI Interface**

```

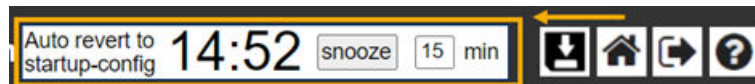
Username: admin
Password:
# copy running-config startup-config ←
Building configuration...
% Saving 887 bytes to flash:startup-config
#

```

### 1.4 Avoiding Unit Network Management Connection Loss

Besides restoring locally unit configuration to factory default to avoid connection loss (see 2. [Restoring PDS-204GCO Unit to Factory Default](#)), which requires being in front of the unit, a permanent configuration change takes place only after you copy `running-config` to `startup-config`. This means that even if configuration was invalid causing to Network connection loss, powering unit OFF and then back to ON must cause unit to revert to last saved valid configuration.

**Figure 1-3. Track Changes in running-config vs. startup-config**



As powering unit OFF and then back to ON cannot be easily done on already installed outdoor units, a protection mechanism is added to protect you (user) from losing unit connection while configuring unit from remote. When you start changing the unit configuration, the following window appears after several seconds to report that the unit will restart itself automatically, reverting to last saved configuration unless you save the modified configuration during the time left (default = 15 minutes). You can increase unsaved time up to 99 minutes at any given time. Saving modified configuration causes the window to disappear after several seconds. You can disable this feature.

## 2. Restoring PDS-204GCO Unit to Factory Default

This section describes the following two scenarios:

- Restoring the unit to factory default without knowing the unit IP, username, or password.
- Restoring the unit to factory default from within the unit web browser (after you have successfully logged in to the unit).

### 2.1 Restoring Unit to Factory Default—Unknown Unit-IP, Username, or Unit Password

Perform the following steps to reset the unit to factory default, restore unit IP to 192.168.0.50, username to admin, and password as per the label on the unit.

1. Turn OFF the unit power.
2. Disconnect from the unit all PoE devices.
3. Disconnect from the unit all ethernet connections.
4. Connect a single Ethernet cable to unit port #1 and the other cable end to port #2 (any two ports).
5. Turn the unit power ON and wait for 90s before turning the unit power OFF again, followed by disconnecting the Ethernet cable from ports #1 and #2.
6. Turn the unit ON and connect the Ethernet cable from your computer to one of the unit ports.

After approximately 40s from powering up, you can access the unit over IP 192.168.0.50 user as admin, and password as marked on the unit label.

### 2.2 Restoring Unit to Factory Default From Web Interface

This option must be used when you restore the unit to semi-factory default, leaving only the unit network access configuration unchanged.

By keeping the unit IP address unchanged, the remote user has the option to access the unit from the remote, although most other unit parameters are restored to factory default.

**Note:** Only `running-config` is restored to factory default. To make factory default parameter changes permanent, you must save `running-config` to `startup-config`.

1. Use the Web interface to access the web page **Maintenance > Factory Default** and initiate the factory default process.
2. Wait several seconds to let the Factory Default process finish followed by **Configuration Factory Reset Done**.
3. Save the new running default configuration by accessing the web page **Maintenance > Configuration > Save Startup-Config**.

### 3. Web Interface

This section provides a general description of the web interface and the home web page. The Web interface is constructed from three main panels. The top and left panel is stationary while the middle panel changes as per user action. See the following figure.

Figure 3-1. Unit Main Web Interface

**Port State Overview** Auto-refresh  Refresh

Hostname:

Gigabit PoE: LINK1, LINK2, LINK3, LINK4  
1G/2.5G SFP: LINK5, LINK6

**Ports - Network Status**

#	Local Link						Remote Network Device-LLDP/CDP		
	Type	Status	Speed	Aggr Ports	Transmit	Receive	System Name	System Description	IP Address
1	Copper	---	---	---	---	---	---	---	---
2	Copper	---	---	---	---	---	---	---	---
3	Copper	---	---	---	---	---	---	---	---
4	Copper	Up	1Gfdx	---	0.6 Kb/s	0 Kb/s	---	---	---
5	Sfp	---	---	---	---	---	---	---	---
6	Sfp	Up	1Gfdx	---	15.4 Kb/s	4 Kb/s	---	---	---

**Ports - PoE Status**

#	Local PoE Port Status							Remote PoE Device		
	PoE-BT Port Type	Power management Mode	Status	Requested Power	Assigned Power	Delivered Power	Assigned Class	PD Measured Class	PD Auto Class Support	PD Requested Power over LLDP
1	Type4 90[W]	Dynamic	On	30 [W]	30 [W]	1 [W]	3, 3	0, 0	---	---
2	Type4 90[W]	Dynamic	On	60 [W]	60 [W]	2.6 [W]	4, 4	4, 4	---	---
3	Type4 90[W]	Dynamic	On	90 [W]	90 [W]	0.5 [W]	5, 5	5, 5	---	---
4	Type4 90[W]	Dynamic	On	60 [W]	60 [W]	4 [W]	6	6	No	---

**System - Status**

Item	Value
Total Power Usage	8 [W]
Total Allocated Power	7 [W]
Free Available Power	144 [W]
Power Supply Voltage	53.5 [V]

- Left panel—Used to configure, monitor, diagnose, and perform unit maintenance.
- Top panel—Offers easy access to save the latest unit configuration, return to the main home page, log out, and provide help and information for the middle section web page.
- Middle panel—Varies based on the option the user selected from the left panel.

**Note:** Only single help web page can be opened at any given time. You must close the already opened help web page to open a new one.

#### 3.1 Home Web Page

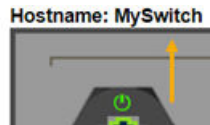
The home web page gets updated dynamically (if the **Auto-Refresh** check box is selected) and reports the unit's overall status. This saves you from switching between various status web pages.

**Note:** The log file is used to track various unit events, such as Ethernet link, PoE status change, and so on.

### 3.1.1 Hostname

User Hostname is reported on the top left, enabling easy differentiation between multiple similar units. The hostname can be easily configured through web interface **Configuration > System > Information** from CLI command *hostname*.

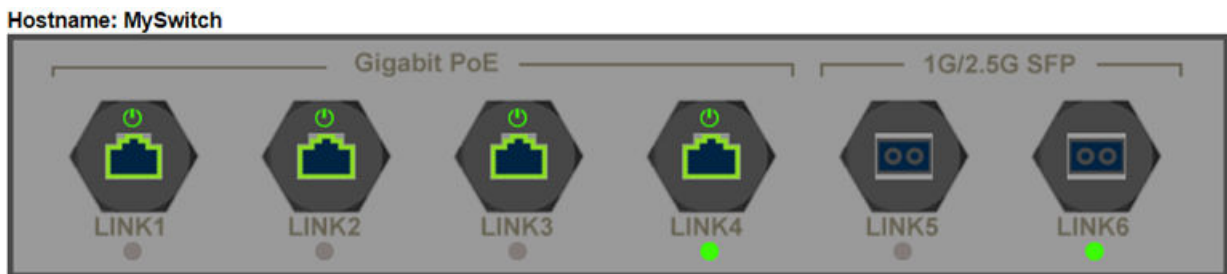
Figure 3-2. Unit Hostname



### 3.1.2 Ethernet, SFP, and PoE Port State

The following figure shows the unit front panel.

Figure 3-3. Unit Front Panel



Ethernet Link LED reports Network status which can be Up, Down, or Disabled.

Hovering over the Link LED with the mouse reports the link state. Pressing on the Link LED reports more details about the port Network traffic. PoE LED images report if power is being applied to the PD device. Ethernet RJ45 images report if PoE is enabled or disabled, and various possible PoE errors.

The following table lists Ethernet link LED images and their descriptions.





Table 3-1. Ethernet Link LED Images

Ethernet Link LED Images	Description
	The Ethernet link is up
	The Ethernet link is down
	The Ethernet link is disabled
	PoE is enabled (regardless of power)
	PoE is disabled
	PoE power applied to PoE-PD device
	No PoE power applied to the PoE-PD device
	The Small Form-factor Pluggable (SFP) Ethernet port is enabled
	The SFP Ethernet port is disabled







The following table lists the several possible PoE fault reports that might be present in the PoE ports.

**Table 3-2. PoE Fault States**





PoE Fault States LED Images	Description
	Fail to communicate with the PoE controller
	Fail to power PD. Insufficient free power [W]
	PoE fault—Fail to power PD
	PoE overload—PD power consumption exceeded the maximum limit.

The following table lists the additional information which can be accessed by hovering the mouse over LED, RJ45, and SFP images.

**Table 3-3. LED, RJ45, and SFP Images**

LED, RJ45, and SFP Images	Description
	PoE port status followed by PoE-Controller internal state index and its description. For example, PoE: On (ID = 0x89: 4P Pwr on 4P DSPD)
	Ethernet link status and speed
	PoE status and PD power consumption
	SFP Ethernet link state

The following table lists the images/icons, which redirect the user to the following web pages.

Web Pages Icons	Description
	Monitor—PoE Status web page
	Monitor—Detailed Port Statistics
	Monitor—PoE Status
	Monitor—Detailed Port Statistics

### 3.1.3 Ports—Network Status

Ports—Network Status provides important network information from the switch and end device.

**Table 3-4. Ports—Network Status**

#	Local Link						Remote Network Device—LLDP/CDP		
	Type	Status	Speed	Aggregate Ports	Transmit	Receive	System Name	System Description	IP Address
1	Copper	—	—	—	—	—	—	—	—

.....continued									
#	Local Link						Remote Network Device—LLDP/CDP		
	Type	Status	Speed	Aggregate Ports	Transmit	Receive	System Name	System Description	IP Address
2	Copper	—	—	—	—	—	—	—	—
3	Copper	—	—	—	—	—	—	—	—
4	Copper	Up	1 Gfdx	—	0 Kbps	0 Kbps	—	—	—
5	SFP	—	—	—	—	—	—	—	—
6	SFP	Up	1 Gfdx	—	8.4 Kbps	02.6 Kbps	—	—	—

- **#:** Unit logical port numbers 1–6. However, while using the CLI interface, the ports are named as following:
  - interface GigabitEthernet 1/1—interface GigabitEthernet 1/4
  - interface 2.5 GigabitEthernet 1/1—interface 2.5 GigabitEthernet 1/2
- **Type:** Copper/SFP. Ports 1–4 are Gb copper ports. Ports 5–6 are SFP 2.5 Gb SFP ports with a default of 1 Gb link speed. You must configure SFP port to 2.5 Gb when a dedicated 2.5G Gb SFP is in use.
- **Status:** Link port status:
  - —: Port is enabled. The link is down.
  - Up: Port is enabled. The link is up.
  - Disabled: Port is disabled.
- **Speed:** Port link speed—10 Mbps, 100 Mbps, 1 Gbps, and 2.5 Gbps.
 

**Note:** SFP ports use by default 1 Gigabit connection speed. For other SFP link speeds, such as 2.5 Gb or 100 Mb, manual configuration is required.
- **Aggregation Ports:** Report aggregated port numbers when port aggregation is in use. For example, P3 and P4 means that ports #3 and #4 are used as one logical aggregated port, doubling logical aggregated speed to 2 Gigabit.
- **Transmit:** Average transmits data rate in kbps/Mbps.
- **Receive:** Average receive data rate in kbps/Mbps.
- **System Name:** Remote network device system name as advertised over Link Layer Discovery Protocol (LLDP)/Cisco Discovery Protocol (CDP) (when enabled).
- **System Description:** Remote network device system description as advertised over LLDP/CDP (when enabled).
- **IP Address:** Remote network device IP address as advertised over LLDP/CDP (when enabled).

### 3.1.4 Ports—PoE Status

Ports—PoE Status reports major configurations and status PoE parameters. The following table lists the Switch PoE parameters (left columns) and the remote PD PoE parameters (right columns).

**Table 3-5. Ports—PoE Status**

#	Local PoE Port Status							Remote PoE Device		
	PoE-BT Port Type	Power Management Mode	Status	Requested Power	Assigned Power	Delivered Power	Assigned Class	PD Measured Class	PD Auto Class Support	PD Requested Power Over LLDP
1	Type4 90 [W]	Dynamic	On	30 [W]	30 [W]	1 [W]	3.3	0.0	—	—
2	Type4 90 [W]	Dynamic	On	60 [W]	30 [W]	2.6 [W]	4.4	4.4	—	—

.....continued										
#	Local PoE Port Status							Remote PoE Device		
	PoE-BT Port Type	Power Management Mode	Status	Requested Power	Assigned Power	Delivered Power	Assigned Class	PD Measured Class	PD Auto Class Support	PD Requested Power Over LLDP
3	Type4 90 [W]	Dynamic	On	90 [W]	30 [W]	0.5 [W]	5.5	5.5	—	—
4	Type4 90 [W]	Dynamic	On	60 [W]	30 [W]	4 [W]	6	6	No	—

- **#:** Unit logical port numbers 1–6. However, while using the CLI interface, the ports are named as the following:
  - interface GigabitEthernet 1/1—interface GigabitEthernet 1/4
  - interface 2.5 GigabitEthernet 1/1—interface 2.5 GigabitEthernet 1/2
- **PoE-BT Port Type:** PoE port maximum power configuration. Power to PD is shut down when PD attempts to exceed the limit.
  - Type4-90W: PoE-BT up to 90W on four pairs. Up to 45W on two pairs
  - Type3-60W: PoE-BT up to 60W on four pairs. Up to 30W on two pairs
  - Type3-30W: PoE-BT up to 30W on four pairs. Up to 30W on two pairs
  - Type3-15W: PoE-BT up to 15W on four pairs. Up to 15W on two pairs
- **Power Management Mode:** Power management configuration mode affects how PD class and power consumption affects the unit's overall free available power.
  - Dynamic: PoE port dynamic real-time power consumption is deducted from the overall PoE-free power budget, while ignoring PD class or PoE port maximum power.
  - Static: PoE port type power configuration (as Type4-90W) is deducted from the overall PoE free power budget after the PoE port is turned ON, while ignoring PD actual power consumption. Next, PD might not be turned ON when free available power is lower than PD requested power. Initial PD requested power is based on PD class and PD auto-class.
  - Hybrid: Mixture of dynamic and static power management based on PD advertising its power requirements by sending LLDP IEEE® 802.3 power through MDI TLV protocol. Every PoE port configured as Hybrid acts as if it is configured as Dynamic, if does not receive any Power Over-MDI TLV within the LLDP packet sent by the PD. After receiving IEEE 802.3 power through MDI TLV, the port also switches to Static Power mode, limiting PoE port maximum power as per the PD requested power plus user-configured cable loss based on user cable length configuration. Static PoE port maximum power might change based on PD LLDP IEEE 802.3 power through MDI TLV advertised values.
- **Status:** Reports the latest PoE port status.
  - —: PoE port is enabled. No PoE-PD.
  - On: PoE power is applied to PD.
  - Disabled: PoE is disabled (non-related to Ethernet data link state).
  - Overload: PD power consumption exceeded its maximum limit. Power is shut down.
  - Fault: Fails to turn ON the connected PD device. The following are the possible reasons:
    - Non-standard PD was connected.
    - PD class error
    - PD underload (PD power consumption is too low)
    - Shortage or invalid capacitor value
    - PD was disconnected (temporary recovery from underload)
    - PSE Fault. Not enough free power is available to turn ON the PD device. Other rare possible reasons: Power supply voltage is out of range, voltage is injected into the Ethernet port, and port over temperature.
- **Requested Power:** PoE PD requested power based on PD Class.
  - Class 8 = 90W

- Class 5, 5 = 90W
  - Class 6 = 60W
  - Class 4, 4 = 60W
  - Class 4 = 30W
  - Class 3 = 15W
  - Class 2 = 7W
  - Class 1 = 4W
  - Class 0 = 15W
- **Assigned Power:** The maximum power that was assigned to PD. Trying to consume above this limit causes the PD to be turned OFF. When enabling the Legacy PD\_Class mode, the assigned PD class might defer from the measured PD class, leading to Assigned-Power differing from Requested-Power. Assigned power might defer from requested power for the following reasons:
    - Demotion: Free available power is less than PD requested power. PoE-BT uses the demotion option to offer a lower power value to the PD. If PD agrees to the lower power value, then it is turned ON with a lower power limit.
    - PoE Port maximum Power: PoE port maximum power configuration is lower than the newly inserted PD power class. For example, a 90W PD class-8 is connected to a PoE port configured as Type3-60W.
  - **Delivered Power:** Temporarily PD power consumption.
  - **Assigned Class:** PD maximum power consumption is determined by the class it is being assigned by the PoE controller (8 = 90W/5, 5 = 90W/6 = 60W/4, 4 = 60W/4 = 30W/3 = 15W/2 = 7W/1 = 4W/0 = 15W). Mostly, the PD Assigned-Class matches with the PD-Measured-Class. The PD-Assigned-Class differs from the PD-Measured-Class in one of the following scenarios:
    - PoE Power Demotion: As per the IEEE 802.3bt specification, when the PoE port maximum available power is less than the PD requested power, the PoE port might offer the PD a lower maximum power value. It is up to the PD to decide to accept the new offer agreeing to consume less power.  
  
For example, PD class-8 (90W) is being connected while PoE-Port has only 60W spare power left. Here, the port offers PoE class-6 (60W). If PD accepts the offer, then Measured-Class is class-8 while Assigned-Class is class-6.
    - Legacy PD-Class Mode = PoH. Port Mode = Plus: PoE-AT DSPD PD class 4, 4 is given 90W as if it is class 5, 5 (2×45W). PoE-AT SSPD PD class 4 is given 45W as if it is class 5.
    - Legacy PD-Class Mode = Ignore PD-Class. Port Mode = Type4-90W: Any DSPD class-x, x is given 90W as if it is class 5, 5 (2×45W). SSPD PD class-x is given 45W as if it is class 5.
    - Legacy PD-Class Mode = Ignore PD-Class. Port Mode = Type3-60W: Any DSPD class-x, x is given 60W as if it is class 4, 4 (2×30W). SSPD PD class-x is given 30W as if it is class 4.
  - **PD Measured Class:** Remote PoE-PD measured classes 1–8 for SSPD, or class 0, 0–class 5, 5 for DSPD.
  - **PD Auto Class Support:** Report if the remote PoE-BT PD device advertises that it is supporting PoE Auto Class regardless of unit Auto Class configuration. When enabled and supported by the PoE-PD device, PoE port maximum power allocation is determined by the power consumed by the PD during the Auto Class negotiation phase instead of the PD class.
  - **PD Requested Power Over LLDP:** When supported by remote PoE-PD, report remote PoE PD requested power using LLDP Power Over-MDI. If PoE-LLDP is disabled, (N/A) appears to the right of PD request power, ignoring PD request power using only PD class for determining PoE power request. When PoE-LLDP is enabled, PD PoE power request over LLDP replaces the PoE PD class. However, it never exceeds the PD class maximum power. Cable loss based on cable length configuration is added on top of the PD LLDP requested power. PoE power management configuration mode controls the power deducted from unit-free available power.

### 3.1.5 System—Status

The following table lists the system power specifications.

**Table 3-6. System—Status**

Item	Value
Total power usage	8 [W]

---

---

.....continued	
Item	Value
Total allocated power	8 [W]
Free available power	143 [W]
power supply voltage	53.5 [W]

- **Total Power Usage:** Total power consumption by all PoE ports.
- **Total Allocated Power:** Total power allocated to all active PoE ports. PoE port power management mode configuration influences the total allocated power.
- **Free Available Power:** The free available power left to power additional PoE ports, or before turning OFF an active PoE PD due to lack of free available power.
- **Power Supply Voltage:** PoE power supply voltage.

## 4. Web Interface—Configuration

This section describes all unit configuration web pages.

**Note:** You must have administrator privilege to access all the web pages presented in this section.

### 4.1 System Configuration

The following sections describe the system configurations.

#### 4.1.1 System Information Configuration

This is used to configure switch Simple Network Management Protocol (SNMP) System-Contact, SNMP System-Location, and switch System-name.

**Figure 4-1. System Information Configuration**

**System Information Configuration**

<b>System Contact</b>	MyName
<b>System Name</b>	MySwitch
<b>System Location</b>	MyOffice

- **System Contact:** SNMP MIB-II system contact OID referring to the contact person responsible for the Network device. Textual identification of the contact person for this managed node. String length is 0 to 255, and valid ASCII characters range 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 drawn from the alphabet (A–Z, a–z), digits (0–9), minus sign (-). No space characters are permitted as part of a name. The first character must be an alpha character. 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 unit. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 32 to 126.

**Notes:**

- The System Name field is also used as unit Hostname for the CLI/Telnet/SSH interface.
- The System Name field is also used by DHCP when the hostname within VLAN DHCP configuration field is left blank.

#### 4.1.2 System IP Configuration

This is used to configure unit IP/DHCP, Default-gateway, DNS, management VLAN, and so on.

**Figure 4-2. IP Configuration**

IP Configuration

Domain Name	No Domain Name
DNS Server 0	No DNS server
DNS Server 1	No DNS server
DNS Server 2	No DNS server
DNS Server 3	
DNS Proxy	<input type="checkbox"/>

IP Interfaces

Delete	IP	Enable	Type	DHCPv4			Hostname (Opt #12)	Fallback	Current Lease	IPv4		DHCPv6		IPv6	
				Client ID (Opt #61)	MAC	HEX				Address	Mask Length	Enable	Rapid Commit	Current Lease	Address
<input type="checkbox"/>	VLAN 1	<input type="checkbox"/>	Auto	Port 1			0			192.168.0.50	24	<input type="checkbox"/>			
Delete		<input type="checkbox"/>	Auto	Port 1			0					<input type="checkbox"/>			

NOTE: To avoid potential DHCP address change, please avoid leaving DHCP Hostname (opt #12) blank, neither Client ID (opt#61) in AUTO mode.

Add Interface

IP Routes (Default-Gateway)

NOTE: To route all unknown destination IP to default gateway, please add the following:  
Network=0.0.0.0, Mask Length=0, Gateway=<Gateway-IP>, Distance=1

Delete	Network	Mask Length	Gateway	Next Hop VLAN (IPv6)	Distance
Delete				0	1

Add Route

Save Reset

- **Domain name:** The name string of local domain where the device belongs.
  - No Domain Name: No domain name is used.
  - Configured Domain Name: Explicitly specify the name of local domain.
  - From any DHCPv6 interfaces: The first domain name offered from a DHCPv6 lease to a DHCPv6-enabled interface is used.
  - From this DHCPv6 interface: Specify from which DHCPv6-enabled interface a provided domain name is preferred.
- **DNS Servers:** Controls the DNS name resolution done by the switch. Index #1 has the highest priority.
  - No DNS server: No DNS server is used.
  - Configured IPv4/IPv6: Explicitly provide the valid IPv4/v6 unicast address of the DNS Server. Ensure that the configured DNS server is reachable (for example, through PING) for activating DNS service.
  - From this DHCPv4/v6 interface: Specify from which DHCPv4-enabled interface a provided DNS server must be preferred.
  - From any DHCPv4/v6 interface: The first DNS server offered from a DHCPv4/v6 lease to a DHCPv4/v6-enabled interface is used.
- **DNS Proxy:** When DNS proxy is enabled, the system relays DNS requests to the currently configured DNS server and replies as a DNS resolver to the client devices on the network. Currently, Only IPv4 DNS proxy is supported.
- **Delete:** Select this option to delete an existing IP interface.
- **VLAN:** The VLAN associated with the IP interface. Only ports in this VLAN are 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 configures the IPv4 address and mask of the interface using the DHCPv4 protocol.
- **IPv4 DHCP Client Identifier Type:** This specifies which of the following three types are used for the Client Identifier. See RFC-2132 section 9.14.
  - IfMac: This is the interface name of DHCP client identifier. When DHCPv4 client is enabled and the client identifier type is **ifmac**, then the configured interface's hardware MAC address is used in the DHCP option 61 field.
  - ASCII: This is the ASCII string of DHCP client identifier. When DHCPv4 client is enabled and the client identifier type is **ascii**, the ASCII string is used in the DHCP option 61 field.
  - HEX: This is the hexadecimal string of DHCP client identifier. When DHCPv4 client is enabled and the client identifier type **hex**, the hexadecimal value is used in the DHCP option 61 field.
- **IPv4 DHCP Hostname:** The hostname of DHCP client. If DHCPv4 client is enabled, the configured hostname is used in the DHCP option 12 field. When this value is empty string, the field uses the configured system name and the latest three bytes of system MAC addresses as the hostname.
- **IPv4 DHCP Fallback Timeout:** The number of seconds for trying to obtain a DHCP lease. After this period expires, a configured IPv4 address is used as IPv4 interface address. A value of zero disables the fallback mechanism, such that DHCP keeps retrying until a valid lease is obtained. Legal values are 0 to 4294967295 seconds.
- **IPv4 DHCP Current Lease:** For DHCP interfaces with an active lease, this column shows the current interface address, as provided by the DHCP server.
- **IPv4 Address:** This is the IPv4 address of the interface. If DHCP is enabled, then 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:** The IPv4 network mask, in number of bits (*prefix length*). Valid values are between 0 and 30 bits for an IPv4 address. If DHCP is enabled, then 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.
- **DHCPv6 Enable:** Enable the DHCPv6 client by checking this box. If this option is enabled, then the system configures the IPv6 address of the interface using the DHCPv6 protocol.
- **DHCPv6 Rapid Commit:** Enable the DHCPv6 Rapid-Commit option by selecting this box. If this option is enabled, then the DHCPv6 client terminates the waiting process as soon as a Reply message with a Rapid Commit option is received. This option is only manageable when DHCPv6 client is enabled.
- **DHCPv6 Current Lease:** For DHCPv6 interface with an active lease, this column shows the interface address provided by the DHCPv6 server.

- **IPv6 Address:** The IPv6 address of the interface. 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.

System accepts the valid IPv6 unicast address only, except IPv4-Compatible address and IPv4-Mapped address. The field may be left blank if IPv6 operation on the interface is not desired.

- **IPv6 Mask:** The IPv6 network mask, in number of bits (*prefix length*). Valid values are between 1-bit and 128 bits for an IPv6 address. The field may be left blank if IPv6 operation on the interface is not desired.

### 4.1.3 System SNMP Configuration

The following sections describe the various system SNMP configurations.

#### 4.1.3.1 SNMP System Configuration

This configuration is used to Enable/Disable SNMP and set SNMPv3 engine ID.

Figure 4-3. SNMP System Configuration

The figure shows a web form titled "SNMP System Configuration". It contains two main input fields: "Mode" with a dropdown menu currently set to "Disabled", and "Engine ID" with a text input field containing the hexadecimal string "800019cb0300defdae1778". Below these fields are two buttons: "Save" and "Reset".

- **Mode:** Enable/Disable SNMP.
- **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, excluding all 0 or all F. Only users on this Engine ID can access the device (local users). Therefore, changing the Engine ID revokes access for all current local users.

#### 4.1.3.2 System SNMP Trap Configuration

The following sections describe the System SNMP Trap configurations.

##### 4.1.3.2.1 SNMP Trap Destinations Configuration

The following figure shows the SNMP Trap Configuration page.

Figure 4-4. SNMP Trap Configuration

The figure shows a web form titled "SNMP Trap Configuration". It consists of a table with the following fields: "Trap Config Name" (empty text input), "Trap Mode" (dropdown menu set to "Disabled"), "Trap Version" (dropdown menu set to "SNMP v2c"), "Trap Community" (text input with "public"), "Trap Destination Address" (empty text input), "Trap Destination Port" (text input with "162"), "Trap Inform Mode" (dropdown menu set to "Disabled"), "Trap Inform Timeout (seconds)" (text input with "3"), "Trap Inform Retry Times" (text input with "5"), "Trap Security Engine ID" (text input with "800019cb0300defdae1778"), and "Trap Security Name" (dropdown menu set to "None"). Below the table are "Save" and "Reset" buttons.

- **Trap Config Name:** Indicates the 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:** Enable/Disable from traps that the unit sends.
- **Trap Version:** Indicates the SNMP supported version. Possible versions are: SNMPv1, SNMPv2, and SNMPv3.
- **Trap Community:** Indicates the community access string when sending SNMP trap packet. The allowed string length is 0 to 63, and the allowed content is ASCII characters from 33 to 126.

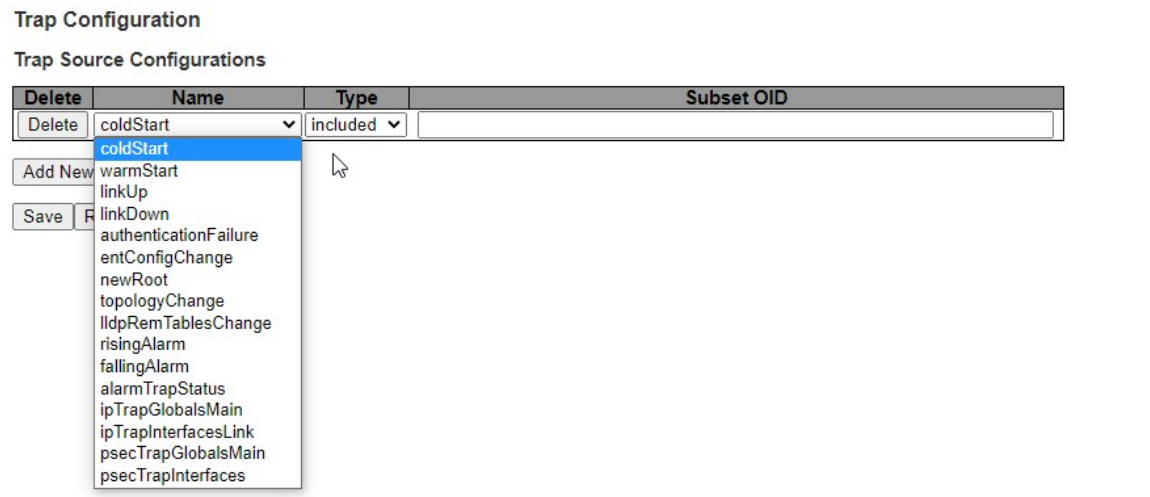
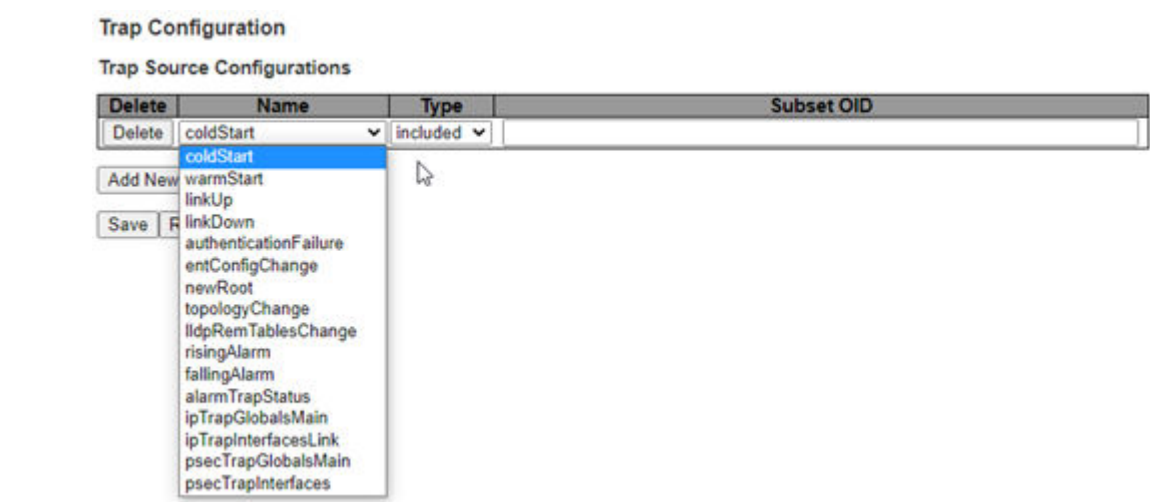


- **Trap Destination Address:** Indicates the SNMP trap destination address. It allows a valid IP address and a valid hostname.
- **Trap Destination Port:** Indicates the SNMP trap destination port. SNMP Agent will send SNMP message via this port; the port range is 1–65535.
- **Trap Inform Mode:** Indicates the SNMP trap inform mode operation. Possible modes are: Enabled/Disabled.
- **Trap Inform Timeout:** Indicates the SNMP trap inform timeout in seconds.
- **Trap Inform Retry Times:** Indicates the SNMP trap inform retry times
- **Trap Security Engine ID:** Indicates the SNMPv3 trap security engine ID.
- **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.

4.1.3.2.2 SNMP Trap Sources Configuration

This configuration provides SNMP trap source configurations. A trap is sent for the given trap source, if at least one filter with filter type included matches the filter.

Figure 4-5. SNMP Trap Source Configuration



- **Name:** For which event a trap must be sent. See the preceding figure.
- **Type:** Include/Exclude trap for the specified event.
- **Subset OID:** The subset OID for the entry. The value must depend on what kind of trap must be sent. For example, the **ifldex** is the subset OID of linkUp and linkDown. A valid subset OID is one or more digital numbers (0–4294967295) or asterisk (\*) which are separated by dots (.). The first character must not begin with asterisk (\*) and the maximum of OID count must not exceed 128.

### 4.1.3.3 SNMP Communities Configuration

Configure the SNMPv3 community table on this page. The entry index key is a Community.

Figure 4-6. SNMP Communities

#### SNMPv3 Community Configuration

Delete	Community name	Community secret	Source IP	Source Prefix
Delete	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

- **Delete:** Check to delete the entry. It will be deleted during the next save.
- **Community Name:** Indicates the security name to map the community to the SNMP Groups configuration. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.
- **Community Secret:** Indicates the community secret (access string) to permit access using SNMPv1 and SNMPv2c to the SNMP agent. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.
- **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 prefix.
- **Source Prefix:** Indicates the SNMP access source address prefix.

### 4.1.3.4 SNMP Users Configuration

Configure the SNMPv3 user table on this page. The entry index keys are Engine ID and Username.

Figure 4-7. Pv3 User Configuration

Delete	Engine ID	User Name	Security Level	Authentication Protocol	Authentication Password	Privacy Protocol	Privacy Password
Delete	800019cb0300defdae1778	<input type="text"/>	Auth. Priv	MD5	<input type="text"/>	DES	<input type="text"/>

- **Delete:** Check to delete the entry. It will be deleted during the next save.
- **Engine ID:** An octet string identifying the engine ID belonging to this entry. The string must contain an even number (in hexadecimal format) with number of digits between 10 and 64, but all-zeros and all Fs are not allowed.
- **User Name:** A string identifying the username belonging to this entry. 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 belonging to this entry. Possible security models are:
  - NoAuth, NoPriv: No authentication and no privacy.
  - Auth, NoPriv: Authentication and no privacy.
  - Auth, Priv: Authentication and privacy.
- **Authentication Protocol:** Indicates the authentication protocol of this entry. Possible authentication protocols 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.
- **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 belonging to this entry. Possible privacy protocols are:
  - None: No privacy protocol.
  - DES: An optional flag to indicate that this user uses DES authentication protocol.
  - SHA: When available, 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.

#### 4.1.3.5 SNMP Groups Configuration

Configure the SNMPv3 group table on this page. The entry index keys are Security Model and Security Name.

Figure 4-8. SNMPv3 Group Configuration

Delete	Security Model	Security Name	Group Name
<input type="checkbox"/>	v1	public	default_ro_group
<input type="checkbox"/>	v1	private	default_rw_group
<input type="checkbox"/>	v2c	public	default_ro_group
<input type="checkbox"/>	v2c	private	default_rw_group

- **Delete:** Check to delete the entry. It will be deleted during the next save.
- **Security Model:** Indicates the security model of this entry. Possible security models are:
  - **v1:** Reserved for SNMPv1.
  - **v2C:** Reserved for SNMPv2c.
  - **usm:** SNMPv3, User-based Security Model (USM).
- **Security Name:** A string identifying the security name belonging to this entry. 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 belonging to this entry. The allowed string length is 1 to 32 and the allowed content is ASCII characters from 33 to 126.

#### 4.1.3.6 SNMP Views Configuration

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

Figure 4-9. SNMPv3 View Configuration

Delete	View Name	View Type	OID Subtree
<input type="checkbox"/>	default_view	included	.1
<input type="button" value="Delete"/>		included	

- **Delete:** Check to delete the entry. It will be deleted during the next save.
- **View Name:** A string identifying the view name belonging to this entry. 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 belonging to this entry. Possible view types are:
  - Included: An optional flag to indicate that this view subtree must be included.
  - Excluded: An optional flag to indicate that this view subtree must be excluded.
- **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 (\*).

#### 4.1.3.7 SNMP Access Configuration

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

Figure 4-10. SNMP Access Configuration

Delete	Group Name	Security Model	Security Level	Read View Name	Write View Name
<input type="checkbox"/>	default_ro_group	any	NoAuth, NoPriv	default_view	None
<input type="checkbox"/>	default_rw_group	any	NoAuth, NoPriv	default_view	default_view

- **Delete:** Check to delete the entry. It will be deleted during the next save.
- **Group Name:** A string identifying the group name belonging to this entry. The allowed string length is 1 to 32 and the allowed content is ASCII characters from 33 to 126.
- **Security Model:** Indicates the security model belonging to this entry. Possible security models are:
  - any: Any security model accepted (v1|v2c|usm).
  - V1: Reserved for SNMPv1.

- V2c: Reserved for SNMPv2c.
- usm: SNMPv3, User-based Security Model (USM).
- **Security Level:** Indicates the security model belonging to this entry. Possible security models are:
  - NoAuth, NoPriv: No authentication and no privacy.
  - Auth, NoPriv: Authentication and no privacy.
  - Auth, Priv: Authentication and privacy.
- **Read View Name:** The name of the MIB view defining the MIB objects for which it 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.

### 4.1.4 System NTP Configuration

Configure IP address of NTP server offering advertising GMT time.

Figure 4-11. NTP Configuration

Mode	Disabled
Server 1	
Server 2	
Server 3	
Server 4	
Server 5	

Save Reset

- **Mode:** Indicates the NTP mode operation. The following are the possible modes:
  - **Enabled:** Enable NTP client mode operation.
  - **Disabled:** Disable NTP client mode operation.
- **Server:** Provide the IPv4/IPv6 or domain name address of NTP Server.

### 4.1.5 System Time Configuration

This page allows you to configure the Time Zone and Daylight-Saving Time.

Figure 4-12. Time Zone Configuration and Daylight-Saving Time

Time Zone Configuration

Time Zone Configuration	
Time Zone	(UTC) Coordinated Universal Time
Hours	0
Minutes	0
Acronym	( 0 - 16 characters )

Daylight Saving Time Configuration

Daylight Saving Time Mode	
Daylight Saving Time	Disabled

Start Time settings	
Month	Jan
Date	1
Year	2014
Hours	0
Minutes	0

End Time settings	
Month	Jan
Date	1
Year	2097
Hours	0
Minutes	0

Offset settings	
Offset	1 (1 - 1439) Minutes

Save Reset

- **Time Zone Configuration**

- Time Zone: Lists various Time Zones worldwide. Select appropriate Time Zone from the drop-down and click **Save** to set. The **Manual Setting** options is used for the specific time zone which is excluded from the options list.
- Hours: Number of hours offset from UTC. The field is only available when in time zone manual setting.
- Minutes: Number of minutes offset from UTC. The field only available when in time zone manual setting.
- Acronym: User can set the acronym of the time zone. This is a user configurable acronym to identify the time zone. Range is up to 16 characters.

**Note:** The string ' ' is a special syntax that is reserved for null input.

- **Daylight Saving Time:** This is used to set the clock forward or backward according to the following configurations set for a defined Daylight-Saving Time duration.
  - Disable: Disables the Daylight-Saving Time configuration.
  - Recurring: Repeats daylight saving every year.
  - Non-Recurring: For single time configuration.
- **Offset:** Enter the number of minutes to add during Daylight Saving Time. Range: 1 to 1439.

#### 4.1.6 System Log Configuration

Configure Syslog server IP address and log severity to be sent.

Figure 4-13. System Log Configuration

Server Mode	Disabled
Server Address	
Syslog Level	Warning

Save Reset

- **Server Mode:** Indicates the server mode operation. The syslog protocol is based on UDP communication and received on UDP port 514, and the syslog server does not send acknowledgments to sender, as UDP is a

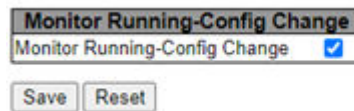
connectionless protocol and it does not provide acknowledgments. The syslog packet always sends out even if the syslog server does not exist. The following are the possible modes:

- Enabled: Enables server mode operation.
- Disabled: Disables server mode operation.
- **Server Address:** Indicates the IPv4 host address of syslog server. If the switch provides DNS feature, then it also can be a domain name.
- **Syslog Level:** Indicates what kind of message is sent to syslog server. The following are the possible modes:
  - Error: Send the specific messages regarding the severity code that is less than or equal to Error (3).
  - Warning: Send the specific messages regarding the severity code that is less than or equal to Warning (4).
  - Notice: Send the specific messages regarding severity code that is less than or equal to Notice (5).
  - Informational: Send the specific messages regarding severity code that is less than or equal to Informational (6).

### 4.1.7 System Monitor Unsaved Running-Config Configuration

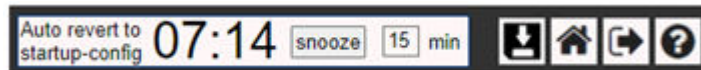
Changing the unit configuration remotely may stop the unit from being accessible, thereby preventing the user from saving the configuration (that is, unable to copy `running config` to `startup-config`), which most likely indicates incorrect new `running-configuration` setup. When enabled, the unit tracks the time since a new running-configuration was created, until it is saved, and performs a reset automatically after a given time (default 15 minutes). This allows for regaining remote access to the unit.

**Figure 4-14. Monitor Modified Unsaved running-config**



When unit configuration is changed while enabled, a warning top right window appears every time the user changes the unit configuration. The warning window disappears after running-configuration is saved. Restoring changed parameters to their previous values also removes the configuration changed window.

**Figure 4-15. Unsaved Warning Pop-Up Message**



- **Monitor Running-Config Change:** Enable/Disable monitoring unit unsaved changes.
- **Countdown Clock:** Time left before the unit resets, going back to its latest saved configuration.
- **Snooze:** Increase countdown clock by the number of minutes to the right (up to 99 minutes).
- **Minutes:** Number of minutes to increase the countdown timer, every time the Snooze button is pressed.

## 4.2 Green Ethernet—Port Power Saving Configuration

This page allows the user to configure the port power savings features.



Figure 4-16. Port Power Saving Configuration

Optimize EEE for Latency ▼

Port Configuration

Port	ActiPHY	PerfectReach	EEE	EEE Urgent Queues									
				1	2	3	4	5	6	7	8		
*	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Save Reset

EEE is a power saving option that reduces the power usage when there is low or no traffic utilization. EEE works by powering down circuits when there is no traffic. When a port gets the data transmitted, then all circuits are powered-up. EEE works for ports in Auto-Negotiation mode, where the port is negotiated to either 1G or 100 Mbit full Duplex mode.

- **Optimize EEE Mode:** The switch can be set to optimize EEE for either best power saving or least traffic latency.
- **Port:** The switch port number of the logical port.
- **ActiPHY:** Link down power savings enabled. ActiPHY works by lowering the power for a port when there is no link. The port is powered up for short moment to determine if the cable is inserted.
- **PerfectReach:** Cable length power savings enabled. PerfectReach works by determining the cable length and lowering the power for ports with short cables.
- **EEE:** Controls if EEE is enabled for this switch port. For maximizing power savings, the circuit is not started when transmit data is ready for a port but is queued until a burst of data is ready to be transmitted. This gives some traffic latency. If desired, it is possible to minimize the latency for specific frames by mapping the frames to a specific queue (mapping done with QOS), and then mark the queue as an urgent queue. When an urgent queue gets data to be transmitted, the circuits are powered-up at once and the latency is reduced to the wakeup time.
- **EEE Urgent Queues:** Queues that are set activate transmission of frames as soon as data is available. Otherwise, the queue postpones transmission until a burst of frames can be transmitted.

### 4.3 Port Configuration

This page displays current port configurations. Ports can also be configured here.

Figure 4-17. Port Configuration

Port	Link	Warning	Current	Speed Configured	Adv Duplex		Adv speed					Flow Control			PFC		Maximum Frame Size	Excessive Collision Mode	Frame Length Check	
					Fdx	Hdx	50M	100M	1G	2.5G	5G	10G	Enable	Curr Rx	Curr Tx	Enable				Priority
1	<span style="color:red">●</span>	<span style="color:gray">●</span>	Down	Automatic	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	5.7	10240	Discard	<input type="checkbox"/>
2	<span style="color:red">●</span>	<span style="color:gray">●</span>	Down	Automatic	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	5.7	10240	Discard	<input type="checkbox"/>
3	<span style="color:red">●</span>	<span style="color:gray">●</span>	Down	Automatic	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	5.7	10240	Discard	<input type="checkbox"/>
4	<span style="color:green">●</span>	<span style="color:gray">●</span>	10Gdx	Automatic	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	5.7	10240	Discard	<input type="checkbox"/>
5	<span style="color:red">●</span>	<span style="color:gray">●</span>	Down	2.5Gbps FDX	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	5.7	10240	Discard	<input type="checkbox"/>
6	<span style="color:green">●</span>	<span style="color:gray">●</span>	10Gdx	Automatic	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	5.7	10240	Discard	<input type="checkbox"/>

Save Reset

- **Port:** This is the logical port number for this row.
- **Link:** The current link state is displayed graphically. Green indicates that the link is up and red indicates that it is down.
- **Warning:** Operational warnings of the port.
  - Gray: No warnings
  - Yellow: There are warnings. Use tooltip to check.
- **Current Link Speed:** Provides the current link speed of the port.

- **Configured Link Speed:** Selects any available link speed for the given switch port. Only speeds supported by the specific port is shown. The following are the possible speeds:
  - Disabled: Disables the switch port operation.
  - Automatic: Port auto negotiating speed and duplex with the link partner and selects the highest speed that is compatible with the link partner.
  - 10 Mbps HDX: Forces the port in 10 Mbps half-duplex mode
  - 10 Mbps FDX: Forces the port in 10 Mbps full duplex mode
  - 100 Mbps HDX: Forces the port in 100 Mbps half-duplex mode
  - 100 Mbps FDX: Forces the port in 100 Mbps full duplex mode
  - 1 Gbps FDX: Forces the port in 1 Gbps full duplex mode
  - 2.5 Gbps FDX: Forces the port in 2.5 Gbps full duplex mode
- **Advertise Duplex:** When duplex is set as auto (auto negotiation), then the port only advertises the specified duplex as either Fdx or Hdx to the link partner. By default, the port advertises all the supported duplexes if the Duplex is Auto.
- **Advertise Speed:** When Speed is set as auto, that is (auto negotiation), then the port only advertises the specified speeds (10M, 100M, 1G, 2.5G, 5G, or 10G) to the link partner. By default, the port advertises all the supported speeds if the 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 if pause frames on the port are obeyed and the Current Tx column indicates if pause frames on the port are transmitted. The Rx and Tx settings are determined by the result of the last Auto Negotiation. Check the configured column to use the flow control. This setting is related to the setting for Configured Link Speed.
 

**Note:** The 100FX standard does not support Auto Negotiation. Therefore, when in 100FX mode, the flow control capabilities are always shown as **disabled**.
- **PFC:** When 802.1Qbb Priority Flow Control (PFC) is enabled on a port, then flow control on a priority level is enabled. Through the Priority field, range (one or more) of priorities can be configured. For example, '0–3, 7' which equals 0, 1, 2, 3, 7. PFC is not supported through auto negotiation. PFC and Flow control cannot be enabled on the same port.
- **Maximum Frame Size:** Enter the maximum frame size allowed for the switch port, including FCS. The range is 1518 bytes–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 are dropped. An Ethernet frame contains an **EtherType** field, 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, then 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, then frames with payload size less than 1536 bytes are dropped, if the **EtherType/Length** field does not match the actual payload length. If **frame length check** is disabled, then frames are not dropped due to frame length mismatch.
 

**Note:** No drop counters count frames dropped due to frame length mismatch.

## 4.4 Connectivity Fault Management (CFM) Configuration

The following sections describe the CFM configurations.

### 4.4.1 CFM Global Configuration

Connectivity Fault Management (CFM) is used to monitor connections for faults while Automatic Protection Switching (APS) is protecting. This web page configures CFM Global parameters.



Figure 4-18. CFM Global Configuration

Sender Id TLV	None
Port Status TLV	Enable
Interface Status TLV	Disable
Organisation Specific TLV	Disable
Organisation Specific TLV OUI	000000
Organisation Specific TLV Subtype	0
Organisation Specific TLV Value	

Save Reset

- **Sender Id TLV:** Choose whether and what to use as Sender ID TLVs in CCMs generated by this switch. This can be overridden by Domain and Service level configuration using one of the following options:
  - None
  - Chassis
  - Manage
  - ChassisManage
- **Port Status TLV:** Choose whether to send Port Status TLVs in CCMs generated by this switch. This can be overridden by Domain and Service level configuration.
  - Enable: Send Port Status TLVs in CCMs generated by this switch.
  - Disable: Do not send Port Status TLVs in CCMs generated by this switch.
- **Interface Status TLV:** Choose whether to send Interface Status TLVs in CCMs generated by this switch. This can be overridden by Domain and Service level configuration.
  - Enable: Send Interface Status TLVs in CCMs generated by this switch.
  - Disable: Do not Send Interface Status TLVs in CCMs generated by this switch.
- **Organization Specific TLV:** Choose whether to send Organization Specific TLVs in CCMs generated by this switch. This can be overridden by Domain and Service level configuration.
  - Enable: Send Organization Specific TLVs in CCMs generated by this switch.
  - Disable: Do not send Organization Specific TLVs in CCMs generated by this switch.
- **Organization Specific TLV OUI:** This is the three-bytes OUI transmitted with the Organization-Specific TLVs. Enter as 6 characters: 0–9, a–f.
- **Organization Specific TLV Subtype:** This is the subtype transmitted with the Organization-Specific TLV. This can be of any value in range [0–255].
- **Organization Specific TLV Value:** This is the value transmitted in the Organization-Specific TLVs. Value is a printable character string of length 0–63.

#### 4.4.2 CFM Domain Configuration

Configure CFM Domain parameters on this page.

Figure 4-19. CFM Domain Configuration

Delete	Domain	Format	Name	Level	TLV option select			
					Sender Id	Port Status	Interface Status	Org. Specific
Delete	domain	String	DEFAULT	0	Defer	Defer	Defer	Defer

Add New Entry

Save Reset

- **Delete:** Check to delete the entry. It will be deleted during the next save.
- **Domain:** Name of Domain. Value is a single word which begins with an alphabetic letter A–Z or a–z with length 1–15.
- **Format:** Select the MD name format. To mimic Y.1731 MEG IDs, use type None.
  - None
  - String

- **Name:** The contents of this parameter depend on the value of the format member. If format is None: Name is not used but is set to all-zeros behind the scenes. This format is typically used by Y.1731-kind-of-PDUs. If format is String: Name must contain a string from 1–43 characters long.
  - None: Name is not used but is set to all-zeros behind the scenes. This format is typically used by Y.1731-kind-of-PDUs.
  - String: Name must contain a string from 1–43 characters long.
- **Level:** MD/MEG level of this domain. Valid values are restricted to 0–7.
- **TLV Option Select:**
  - Sender Id: Default Sender ID TLV format to be used in CCMs generated by this domain (may be overridden in service).
    - None: Do not include Sender ID TLVs.
    - Chassis: Enable Sender ID TLV and send Chassis ID (MAC Address).
    - Manage: Enable Sender ID TLV and send Management address (IPv4 Address).
    - ChassisManage: Enable Sender ID TLV and send both Chassis ID (MAC Address) and Management Address (IPv4 Address).
    - Defer: Let the global configuration decide if Sender ID TLVs are included (may be overridden in service).
  - Port Status: Include or exclude Port Status TLV in CCMs generated by this Domain or let higher level determine (may be overridden in Service).
    - Disable: Do not include Port Status TLVs.
    - Enable: Include Port Status TLVs.
    - Defer: Let the global configuration decide if Port Status TLVs are included (may be overridden in Service).
  - Interface Status: Include or exclude Interface Status TLV in CCMs generated by this Domain or let higher level determine (may be overridden in Service).
    - Disable: Do not include Interface Status TLVs.
    - Enable: Include Interface Status TLVs.
    - Defer: Let the global configuration decide if Interface Status TLVs are included (may be overridden in Service).
  - Org. Specific: Exclude Organization-Specific TLV in CCMs generated by this Domain or let higher level determine (may be overridden in Service).
    - Disable: Do not include Organization-Specific TLVs.
    - Defer: Let the global configuration decide if Organization-Specific TLVs are included (may be overridden in Service).

### 4.4.3 CFM Services Configuration

Configure CFM Service parameters on this page.

**Figure 4-20. CFM Service Configuration**

Delete	Domain	Service	Format	Name	VLAN	CCM Interval	TLV option select			
							Sender Id	Port Status	Interface Status	Org. Specific
Delete			Primary Vid		0	1 sec	Defer	Defer	Defer	Defer

- **Delete:** Check to delete the entry. It will be deleted during the next save.
- **Domain:** Name of Domain under which this Service resides.
- **Service:** Name of Service. Value is a single word which begins with an alphabetic letter A–Z or a–z with length 1–15.
- **Format:** Select the short Service name format. This decides how the value of the Name parameter is interpreted. To mimic Y.1731 MEG IDs, create an MD instance with an empty name and use Y1731 ICC or Y1731 ICC CC.  
The following are the possible values (look under Name parameter for explanation):

- String
- Two Octets
- Y1731 ICC
- Y1731 ICC CC
- **Name:** The contents of this parameter depend on the value of the format member. Besides the limitations explained for each of them, the following applies in general:
  - If the Domain Format is None, the size of this cannot exceed 45 bytes. If the Domain format is not None, the size of this cannot exceed 44 bytes.
- If format is String, then the following applies:
  - Length must be in range [1–44]
  - Contents must be in range [32–126]
- If format is Two Octets, then the following applies:
  - Name [0] and Name [1] are interpreted as unsigned 8-bit integers (allowing a range of [0; 255]). Name [0] is placed in the PDU before Name [1].
  - The remaining available bytes in name are not used.
- If format is Y1731 ICC, then the following applies:
  - Length must be 13. Contents must be in range [a–z, A–Z, and 0–9].
  - Y.1731 specifies that it is a concatenation of ICC (ITU Carrier Code) and UMC (Unique MEG ID code):
    - ICC: 1–6 bytes
    - UMC: 7–12 bytes

In principle, UMC can be any value in range [1; 127], but API does not allow this for specifying length of ICC. Therefore, the underlying code does not know where ICC ends and UMC starts. The Domain Format must be None.
- If format is Y1731 ICC CC, then the following applies:
  - Length must be 15.
  - First 2 chars (CC): Must be amongst [A–Z]
  - Next 1–6 chars (ICC): Must be amongst [a–z, A–Z, 0–9]
  - Next 7–12 chars (UMC): Must be amongst [a–z, A–Z, 0–9]
  - There may be ONE (slash) present in name [3–7].
  - The Domain format must be None.
- **VLAN:** The MA's primary VID. A primary VID of 0 means that all MEPs created within this MA are created as port MEPs (interface MEPs). There can only be one port MEP per interface. A given port MEP may still be created with tags if that MEP's VLAN is non-zero. A non-zero primary VID means that all MEPs created within this MA are created as VLAN MEPs. A given MEP may be configured with another VLAN than the MA's primary VID, but it is impossible to have untagged VLAN MEPs.
- **CCM Interval:** The CCM rate of all MEPs bound to this Service.
- **TLV Option Select:**
  - Sender ID: Default Sender ID TLV format to be used in CCMs generated by this service.
    - None: Do not include Sender ID TLVs.
    - Chassis: Enables Sender ID TLV and send Chassis ID (MAC Address).
    - Manage: Enables Sender ID TLV and send Management address (IPv4 Address).
    - ChassisManage: Enables Sender ID TLV and send both Chassis ID (MAC Address) and Management Address (IPv4 Address).
    - Defer: Lets the Domain configuration decide if Sender ID TLVs are included.
  - Port Status: Include or exclude Port Status TLV in CCMs generated by this Service or let higher level determine.
    - Disable: Does not include Port Status TLVs.
    - Enable: Includes Port Status TLVs.
    - Defer: Let the Domain configuration decide if Port Status TLVs are included.
  - Interface Status: Include or exclude Interface Status TLV in CCMs generated by this Service or let higher level determine.

- Disable: Does not include Interface Status TLVs.
- Enable: Includes Interface Status TLVs.
- Defer: Lets the Domain configuration decide if Interface Status TLVs shall be included.
- Org. Specific: Excludes Organization-Specific TLV in CCMs generated by this service or let higher level determine.
  - Disable: Does not include Organization-Specific TLVs.
  - Defer: Lets the Domain configuration decide if Organization-Specific TLVs are included.

#### 4.4.4 CFM MEP Configuration

This switch supports two types of MEP: Port Down-MEPs and VLAN Down-MEPs. These MEPs can be configured from this web page.

Figure 4-21. CFM MEP Configuration

Delete	Domain	Service	MEPID	Direction	Port	VLAN	PCP	SMAC	Alarm Control			State Control		Remote MEPID
									Level	Present	Absent	CCM	Admin	
Delete	Select Service		1	Down	1	1	0	00:00:00:00:00:00	2	2500	10000	<input checked="" type="checkbox"/>	<input type="checkbox"/>	0

Add New Entry

Save Reset

##### Port Down-MEPs

In 802.1Q terminology, Port MEPs are located below the EISS entity, that is, closest to the physical port. Port MEPs are used by, for example, APS for protection purposes. Port MEPs are created when the encompassing service has type **Port**. Port MEPs may send OAM PDUs tagged or untagged. An OAM PDU is sent untagged only if the MEP's VLAN is set to **Inherit** (0). Any other value sends it tagged with the port's TPID, whether VLAN matches the port's PVID and that PVID is meant to be sent untagged.

##### VLAN Down-MEPs

In 802.1Q terminology, VLAN MEPs are located above the EISS entity. This means that tagging of OAM PDUs follows the port's VLAN configuration.

Therefore, if a VLAN MEP is created on the Port's PVID and PVID is configured to be untagged, OAM PDUs are transmitted untagged. VLAN MEPs are created when the encompassing service has type **VLAN**.

Following are the rules to follow while creating Down-MEPs:

- There can only be one Port MEP on the same port.
- There can only be one VLAN MEP on the same port and VLAN.
- A VLAN MEP must have a higher MD/MEG level than a Port MEP on the same port and VLAN.
- All port MEPs must have the same MD/MEG level.
- Any VLAN MEP must have an ME/MEG level higher than a Port MEP

These checks are performed automatically on administratively enabled MEPs. When you change a particular MEP, change the Service Type from Port to VLAN or vice-versa, or change the domain's MD/MEG level.

- **Delete:** Check to delete the entry. It will be deleted during the next save.
- **Domain:** Name of the domain under which this MEP resides.
- **Service:** Name of the service under which this MEP resides.
- **MEPID:** The identification of this MEP. Must be an integer [1..8091]
- **Direction:** Set whether this MEP is an Up- or a Down-MEP.
- **Port:** Port on which this MEP resides.
- **VLAN:** VLAN ID. Use the value 0 to indicate untagged traffic (implies a port MEP).
- **PCP:** Choose PCP value in PDUs' VLAN tag. Not used if untagged.
- **SMAC:** Set a Source MAC address to be used in CCM PDUs originating at this MEP. Must be a unicast address. Format is XX:XX:XX:XX:XX:XX. If all-zeros, then the switch port's MAC address is used.
- **Alarm Control:** Level—if a defect is detected with a priority higher than this level, a fault alarm notification is generated. Valid range is [1; 6] with 1 indicating that any defect can cause a fault alarm and 6 indicating that no

defect can cause a fault alarm. See 802.1Q-2018, clause 20.9.5, LowestAlarmPri. The following table lists the possible defects and their priorities.

**Table 4-1. List of Defects and Priorities**

Short Name	Description	Priority
DefRDICCM	Remote Defect Indication	1
DefMACstatus	MAC Status	2
DefRemoteCCM	Remote CCM	3
DefErrorCCM	Error CCM Received	4
DefXconCCM	Cross Connect CCM Received	5

**Present:** The time in milliseconds where defects must be present before a fault alarm notification is issued. Default is 2500 ms.

**Absent:** The time in milliseconds where defects must be absent before a fault alarm notification is reset. Default is 10000 ms.

- **State Control:** Enable or disable generation of Continuity-Check Messages (CCMs).
- **Admin:** Enable or disable this MEP. When this MEP is enabled, it checks received/missing CCMs and can raise defects.

## 4.5 APS Configuration

The APS module implements the protocol and linear protection switching mechanisms for point-to-point VLAN-based ETH SNC in Ethernet transport networks. Automatic Protection Switching is defined by the ITU G.8031 standard. This page allows the user to create and configure an APS Instance.

**Figure 4-22. APS Configuration**

APS #	Mode	SMAC	Level	VLAN	PCP	Rev	TxAps	WTR	HoldOff	Enable
0	1:1	00:00:00:00:00:00	0	0	7	<input type="checkbox"/>	<input type="checkbox"/>	300	0	<input type="checkbox"/>

**APS Signal Fail Trigger**

Working					Protecting				
Port	SF Type	Domain	Service	MEPID	Port	SF Type	Domain	Service	MEPID
1	Link			0	1	Link			0

Save Reset Cancel

- **APS #:** The ID of the APS. Maximum number of creatable APS instances is 6. Click on the link to get to APS instance page, reset counters, and issue commands.
- **Port:** The port this flow is attached to.
- **SF Trigger:** Selects whether Signal Fail (SF) comes from the link state of a given port or from a Down-MEP.
- **SF MEP:** The Domain::Service::MEPID refers to a MEP instance which represents the Working flow. Only used when SF Trigger is MEP. The selected MEP instance does not need to exist when this APS is configured.
- **Mode:** In the linear 1:1 protection switching architecture, the protection transport entity is dedicated to the working transport entity. However, the normal traffic is transported either on the working transport entity or on the protection transport entity using a selector bridge at the source of the protected domain. The selector at the sink of the protected domain selects the entity which carries the normal traffic.

In the linear 1+1 protection switching architecture, a protection transport entity is dedicated to each working transport entity. The normal traffic is copied and fed to both working and protection transport entities with a permanent bridge at the source of the protected domain. The traffic on working and protection transport entities is transmitted simultaneously to the sink of the protected domain, where a selection between the working and protection transport entities is made based on some predetermined criteria, such as server defect indication.

- 1+1 Uni: Creates a 1+1 Unidirectional APS.
- 1+1 Bi: Creates a 1+1 Bidirectional APS.

- **Level:** MD/MEG Level (0–7).
- **VLAN:** The VLAN ID used in the L-APS PDUs. 0 means untagged.
- **PCP:** PCP (priority) (default 7). The PCP value used in the VLAN tag unless the L-APS PDU is untagged. Must be a value in range 0–7.
- **SMAC:** Source MAC address used in L-APS PDUs. This must be a unicast address. If all-zeros, the switch port's MAC address is used.
- **Rev:** When checked, the port recovery mode is revertive, that is, traffic switches back to the working port after the condition(s) causing a switch has cleared. In case of clearing a command (for example, forced switch), this happens immediately. In case of clearing of a defect, this generally happens after the expiry of the Wait-To-Restore (WTR) timer. When unchecked, the port recovery mode is non-revertive and traffic is allowed to remain on the protect port after a switch reason has cleared.
- **TxAps:** Choose whether this end transmits APS PDUs. Only used for 1+1, unidirectional.
- **WTR:** When Rev is checked, WTR tells how many seconds to wait before restoring to the working port after a fault condition has cleared. Valid range is 1–720.
- **HoldOff:** When a new (or more severe) defect occurs, the hold-off timer is started, and the event is reported after the timer expires. HoldOff time is measured in milliseconds, and valid values are in the range 0–10000. Default is 0, which means immediate reporting of the defect.
- **Enable:** The administrative state of this APS instance. Check to make it function normally and uncheck to make it cease functioning.
- **Oper:** This field cannot be configured but shows the operational state. You can click on the link in the APS # field to get more details on the status.
  - ●: APS instance is functional.
  - ●: APS instance is not functional.
- **Warning:** If the operational state is Active, then the APS instance is active, but it may not run the way the administrator thinks because of configuration errors, which are reflected in the following warnings.

The following are the indication of warning information:

- ●: No warning
- ●: Warning

Use the tooltip to get the detailed warning information.

## 4.6 ERPS Configuration

The ERPS instances are configured on this page.

Figure 4-23. ERPS Configuration

ERPS Configuration

Configuration

ERPS #	Version	Type	VC	Interconnect		Port If		RingId	NodeId	Level	Control		Rev	Guard	WTR	HoldOff	Enable
				Instance	Prop	Port0	Port1				VLAN	PCP					
0	v2	Major	<input checked="" type="checkbox"/>	0	<input type="checkbox"/>	1	1	1	00:00:00:00:00:00	7	1	7	<input checked="" type="checkbox"/>	500	300	0	<input type="checkbox"/>

Signal Fail Trigger

Port0				Port1			
Type	Domain	Service	MEPID	Type	Domain	Service	MEPID
Link			0	Link			0

Protected VLANs

VLAN ID:

Ring Protection Link

RPL Mode:  RPL Port:

None | RingPort0

Save Reset Cancel

- **Configuration:**
  - ERPS #: The ID of ERPS. The allowed value is from 1:64.
  - Version: ERPS protocol version. v1 and v2 are supported.
  - Type: Type of ring. The following are the possible values:

- Major: ERPS major ring (G.8001-2016, clause 3.2.39)
- Sub: ERPS sub-ring (G.8001-2016, clause 3.2.66)
- InterSub: ERPS sub-ring on an interconnection node (G.8001-2016, clause 3.2.66).
- VC: Controls whether to use a Virtual Channel with a sub-ring.
- Interconnect Instance: For a sub-ring on an interconnection node, this must reference the instance ID of the ring to which this sub-ring is connected.
- Interconnect Prop: Controls whether the ring referenced by Interconnect Instance shall propagate R-APS flush PDUs whenever this sub-ring's topology changes.
- Ring ID: The Ring ID is used: Along with the control VLAN, this is used to identify R-APS PDUs as belonging to a particular ring.
- Node ID: The Node ID is used inside the R-APS specific PDU to uniquely identify this node (switch) on the ring.
- Level: MD/MEG Level of R-APS PDUs that are transmitted.
- Control VLAN: The VLAN on which R-APS PDUs are transmitted and received on the ring ports.
- Control PCP: The PCP value used in the VLAN tag of the R-APS PDUs.
- Rev: Revertive (true) or Non-Revertive (false) mode.
- Guard: Guard time in ms. Valid range is 10 ms–2000 ms.
- WTR: Wait-to-Restore time in seconds. Valid range 1s–720s.
- Hold Off: Hold off time in ms. Value is rounded down to 100 ms precision. Valid range is 0 ms–10000 ms.
- Enable: The administrative state of this ERPS. Check to make it function normally and uncheck to make it cease functioning.
- **Signal Fail Trigger**
  - Type: Selects whether Signal Fail (SF) comes from the link state of a given interface or from a Down-MEP.
  - Domain, Service, MEPID: Identification of the MEP instance to provide SF, if Type is MEP.
- **Protected VLANs:** VLANs, which are protected by this ring instance. At least one VLAN must be protected. Specify as a comma separated list of VLAN numbers or VLAN ranges. For example, 1, 4, 7, 30–70.
- **Ring Protection Link:**
  - RPL Mode: The following ring Protection Link modes are available:
    - None: This switch does not have the RPL port in the ring.
    - Owner: This switch is RPL owner for the ring (G.8001-2016, clause 3.2.61)
    - Neighbor: This switch is RPL neighbor for the ring (G.8001-2016, clause 3.2.60).
  - RPL Port: Indicates whether it is port0 or port1 that is the Ring Protection Link. This is not used if RPL mode is None.

## 4.7 DHCPv4 Snooping Configuration

Configure DHCP Snooping on this page.



Figure 4-24. DHCPv4 Snooping Configuration

**DHCP Snooping Configuration**

Snooping Mode Disabled ▾

**Port Mode Configuration**

Port	Mode
*	<> ▾
1	Trusted ▾
2	Trusted ▾
3	Trusted ▾
4	Trusted ▾
5	Trusted ▾
6	Trusted ▾

Save
Reset

- **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 are forwarded to trusted ports and only allow reply to packets from trusted ports.
  - Disabled: Disable DHCP snooping mode operation.
- **Port Mode Configuration:** Indicates the DHCP snooping port mode. The following are the possible port modes:
  - Trusted: Configures the port as trusted source of the DHCP messages.
  - Untrusted: Configures the port as untrusted source of the DHCP messages.

## 4.8 DHCPv6 Snooping Configuration

Configure DHCPv6 (that is, DHCP over IPv6) Snooping on this page.

Figure 4-25. DHCPv6 Snooping Configuration

**DHCPv6 Snooping Configuration**

**Switch Configuration**

Snooping Mode
Disabled ▾

Unknown IPv6 Next-Headers
Drop ▾

**Port Configuration**

Port	Trust Mode
*	<> ▾
Gi 1/1	Untrusted ▾
Gi 1/2	Untrusted ▾
Gi 1/3	Untrusted ▾
Gi 1/4	Untrusted ▾
2.5G 1/1	Untrusted ▾
2.5G 1/2	Untrusted ▾

- **Snooping Mode:** Indicates the DHCPv6 snooping mode operation. The following are the possible modes:
  - Enabled: Enable DHCPv6 snooping mode operation. When DHCPv6 snooping mode operation is enabled, the DHCPv6 client request messages are forwarded to trusted ports and only allow reply packets from trusted ports.
  - Disabled: Disable DHCP snooping mode operation.
- **Unknown IPv6 Next-Headers:** Indicates how Unknown IPv6 Next-Header values must be treated. The switch must parse all IPv6 packets to a DHCPv6 client to determine if it is a DHCPv6 message. If an unknown IPv6



extension header is encountered, then the parsing cannot continue. See RFC 7610, section 5, item 3 for details.

The following are the possible options:

- Drop: Drop packets with unknown IPv6 extension headers. This is the most secure option but may result in traffic disruptions.
- Allow: Allow packets with unknown IPv6 extension headers. This is a less secure option but prevents traffic disruptions.
- **Port Mode Configuration:** Indicates the DHCPv6 snooping port mode. Possible port modes are:
  - Trusted: Configures the port as trusted source of the DHCPv6 messages.
  - Untrusted: Configures the port as untrusted source of the DHCPv6 messages.

**Note:** Enabling this function requires changing the Key Type to **MAC and IP Address** for all ports that receive DHCPv6 packets. You can do this in the QoS Port Classification page.

## 4.9 Security Configuration

The following sections describe various security configurations.

### 4.9.1 Security Switch Configuration

The following sections describe the security switch configurations.

#### 4.9.1.1 Security Switch Users Configuration

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

**Figure 4-26. Users Configuration**

User Name	Privilege Level
admin	15

**Figure 4-27. Add User**

User Settings	
User Name	<input type="text"/>
Password	<input type="password"/>
Password (again)	<input type="password"/>
Privilege Level	0 <input type="button" value="v"/>

- **User Name:** The name identifying the user.
- **Privilege Level:** The privilege level of the user. The allowed range is 0–15. If the privilege level value is 15, it can access all groups, that is, it is granted the full control of the device. But the other value must refer to each group privilege level. User's privilege must be same or greater than the group privilege level to have the access of that group. By default setting, most group's 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) needs 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.

#### 4.9.1.2 Security Switch Privilege Level Configuration

This page provides an overview of the privilege levels.

Figure 4-28. Privilege Level Configuration

Group Name	Privilege Levels			
	Configuration Read-only	Configuration/Execute Read/write	Status/Statistics Read-only	Status/Statistics Read/write
Aggregation	5	10	5	10
Alarm	5	10	5	10
APS	5	10	5	10
CFM	5	10	5	10
Debug	15	15	15	15
DHCP	5	10	5	10
DHCPv6_Client	5	10	5	10
Diagnostics	5	10	5	10
ERPS	5	10	5	10
Firmware	5	10	5	10
Green_Ethernet	5	10	5	10
IP	5	10	5	10
LACP	5	10	5	10
LLDP	5	10	5	10
Loop_Protect	5	10	5	10
MAC_Table	5	10	5	10
Miscellaneous	15	15	15	15
NTP	5	10	5	10
POE	5	10	5	10
Ports	5	10	1	10
QoS	5	10	5	10
RMirror	5	10	5	10
Security(access)	10	10	5	10
Security(network)	5	10	5	10
sFlow	5	10	5	10
Spanning_Tree	5	10	5	10
System	5	10	1	10
uFDMA_AIL	5	10	5	10
uFDMA_CIL	5	10	5	10
UPnP	5	10	5	10
VLANs	5	10	5	10

Save Reset

- Group Name:** The name identifying the privilege group. In most cases, a privilege level group consists of a single module (for example, Link Aggregation Control Protocol (LACP), RSTP or QoS), but a few of them contains more than one. The following description defines these privilege level groups in detail:
  - System: Contact, Name, Location, Timezone, Daylight Saving Time, Log.
  - Security: Authentication, System Access Management, Port (contains Dot1x port, MAC based and the MAC Address Limit), Access Control List (ACL), HTTPS, SSH, and Address Resolution Protocol (ARP) Inspection.
  - IP: Everything except ping.
  - Port: Everything except VeriPHY.
  - Diagnostics: ping and VeriPHY.
  - Maintenance: CLI- System Reboot, System Restore Default, System Password, Configuration Save, Configuration Load, and Firmware Load. Web- Users, Privilege Levels, and everything in Maintenance.
  - Debug: Only present in CLI.
- Privilege Levels:** The Privilege Levels can be configured between 0–15 (where, 0 is lowest level and 15 is highest level). Every group has an authorization Privilege level for the following subgroups: configuration read-only, configuration/execute read-write, status/statistics read-only, and status/statistics read-write (for example, for clearing of statistics). User Privilege must be same or greater than the authorization Privilege level to have the access to that group.

#### 4.9.1.3 Security Switch Authentication Method Configuration

This section describes the security switch authentication method configuration.

Figure 4-29. Authentication Method Configuration

Authentication Method Configuration

Client	Methods		
console	local	no	no
telnet	local	no	no
ssh	local	no	no
http	local	no	no

Command Authorization Method Configuration

Client	Method	Cmd Lvl	Cfg Cmd
console	no	0	<input type="checkbox"/>
telnet	no	0	<input type="checkbox"/>
ssh	no	0	<input type="checkbox"/>

Accounting Method Configuration

Client	Method	Cmd Lvl	Exec
console	no		<input type="checkbox"/>
telnet	no		<input type="checkbox"/>
ssh	no		<input type="checkbox"/>

Save Reset

- **Authentication Method Configuration Help:** The authentication section allows you to configure how a user is authenticated when he logs into the switch through one of the management clients' interfaces. The table has one row for each client type and several columns, which are:
  - Client: The management client for which the configuration is applied; console, telnet, ssh, and HTTP.
  - Methods: Method can be set to one of the following values:
    - No: Command authorization is disabled. User is granted access to CLI commands according to his privilege level.
    - TACACS: Use remote TACACS+ server(s) for command authorization. If all remote servers are offline, the user is granted access to CLI commands according to his privilege level.
- **Command Authorization Method Configuration Help:** 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 several columns, which are:
  - Client: The management client for which the configuration is applied.
  - Method: Method can be set to one of the following values:
    - No: Command authorization is disabled. User is granted access to CLI commands according to his privilege level.
    - TACACS: Use remote TACACS+ server(s) for command authorization. If all remote servers are offline, the user is granted access to CLI commands according to his privilege level.
  - Cmd Lvl: Authorize 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 authorize configuration commands.
- **Accounting Method Configuration Help:** The accounting section allows you to configure command and exec (login) accounting. The table has one row for each client type and several columns, which are:
  - Client: The management client for which the configuration is applied.
  - Method: Method can be set to one of the following values:
    - No: Accounting is disabled.
    - TACACS: Use remote TACACS+ server (s) for accounting.
  - Cmd Lvl: Enable accounting 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.
  - Exec: Enable exec (login) accounting.

#### 4.9.1.4 Security Switch SSH Configuration

Configure SSH on this page.

Figure 4-30. SSH Configuration

The screenshot shows a configuration panel for SSH. At the top, there is a label 'Mode' followed by a dropdown menu currently set to 'Enabled'. Below this, there are two buttons: 'Save' and 'Reset'.

**Mode:** Indicates the SSH mode operation. The following are the possible modes:

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

#### 4.9.1.5 Security Switch HTTPS Configuration

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

Figure 4-31. HTTPS Configuration

The screenshot shows a configuration panel for HTTPS. It contains four rows of settings, each with a label and a dropdown menu or status field:
 

- Mode:** Disabled
- Automatic Redirect:** Disabled
- Certificate Maintain:** None
- Certificate Status:** Switch secure HTTP certificate is presented

 Below these settings are 'Save' and 'Reset' buttons.

- **Mode:** Indicate the HTTPS mode operation. The following are the possible modes:
  - Enable: Enable HTTPS mode operation.
  - Disabled: Disable HTTPS mode operation.
- **Automatic Redirect:** Indicates the HTTPS redirect mode operation. It is only significant when **HTTPS Mode Enabled** is selected. When the redirect mode is enabled, the HTTP connection is redirected to HTTPS connection automatically.

**Note:** 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. The following are the possible modes:

- Enabled: Enable HTTPS redirect mode operation.
- Disabled: Disable HTTPS redirect mode operation.
- **Certificate Maintain:** The operation of certificate maintenance. The following are the possible operations:
  - 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 must contain the certificate and private key together. If you have two separated files for saving certificate and private key, then use the Linux® `cat` command to combine them into a single PEM file. For example, `cat my.cert my.key > my.pem`

**Note:** The RSA certificate is recommended as most of the new versions of browsers do not support DSA in certificate. For example, Firefox v37 and Chrome v39.

The following are the possible methods:

- Web Browser: Upload a certificate via Web browser.
- URL: Upload a certificate through URL. The supported protocols are HTTP, HTTPS, TFTP, and FTP. The URL format is: `<protocol>://[<username>[:<password>]@]< host>[:<port>][/<path>]/<file_name>`. For example, `tftp://10.10.10.10/new_image_path/new_image.dat`, `http://username:password@10.10.10.10:80/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 (-), and under score (\_). The maximum length is 63 and a hyphen must not be first character. The file name content that only contains a dot (.) is not allowed.
- **Certificate Status:** Display the current status of certificate on the switch. The following are the possible statuses:

- Switch secure HTTP certificate is presented
- Switch secure HTTP certificate is not presented.
- Switch secure HTTP certificate is generating ....

#### 4.9.1.6 Security Switch Access Management Configuration

Configure access management table on this page. The maximum number of entries is 16. If the application's type matches any one of the access management entries, then it allows access to the switch.

Figure 4-32. Access Management Configuration

Mode: Disabled ▼

Delete	VLAN ID	Start IP Address	End IP Address	HTTP/HTTPS	SNMP	TELNET/SSH
Delete	1	0.0.0.0	0.0.0.0	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Add New Entry

Save Reset

- **Mode:** Indicates the access management mode operation. Possible modes are:
  - Enabled: Enable access management mode operation.
  - Disabled: Disable access management mode operation.
- **Delete:** Check to delete the entry. It will be deleted during the next save.
- **VLAN ID:** Indicates the VLAN ID for the access management entry.
- **Start IP Address:** Indicates the end IP unicast address for the access management entry.
- **End IP Address:** Indicates the end IP unicast 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.

#### 4.9.1.7 Security Switch RMON Configuration

The following sections describe the security switch RMON configuration.

##### 4.9.1.7.1 Switch RMON Statistics Configuration

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

Figure 4-33. RMON Statistics Configuration

Delete	ID	Data Source
Delete		.1.3.6.1.2.1.2.2.1.1 0

Add New Entry Save Reset

- **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 1–65535.
- **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, then the value is 2000005.

##### 4.9.1.7.2 Switch RMON History Configuration

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

Figure 4-34. RMON History Configuration

Delete	ID	Data Source	Interval	Buckets	Buckets Granted
Delete		.1.3.6.1.2.1.2.2.1.1 0	1800	50	

Add New Entry Save Reset

- **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 1–65535.
- **Data Source:** Indicates the port ID, which is 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, then the value is 2000005.
- **Interval:** Indicates the interval in seconds for sampling the history statistics data. The range is from 1–3600 and the default value is 1800s.
- **Buckets:** Indicates the maximum data entries associated with this History control entry stored in RMON. The range is from 1–3600 and the default value is 50.
- **Buckets Granted:** The number of data is saved in the RMON.

### 4.9.1.7.3 Switch RMON Alarm Configuration

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

**Figure 4-35. RMON Alarm Configuration**

RMON Alarm Configuration

Delete	ID	Interval	Variable	Sample Type	Value	Startup Alarm	Rising Threshold	Rising Index	Falling Threshold	Falling Index
Delete		30	1.3.6.1.2.1.2.2.1	0.0	Delta	0	RisingOrFalling	0	0	0

- **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 1–65535.
- **Interval:** Indicates the interval in seconds for sampling and comparing the rising and falling threshold. The range is from 1 to 2<sup>31</sup>-1.
- **Variable:** Indicates the variable to be sampled. The following is the list of possible variables.
  - InOctets: The total number of octets received on the interface, including framing characters.
  - InUcastPkts: The number of uni-cast packets delivered to a higher-layer protocol.
  - InNUcastPkts: The number of broad-cast and multi-cast packets delivered to a higher-layer protocol.
  - InDiscards: The number of inbound packets that are discarded even 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 broad-cast and multi-cast packets that request to transmit.
  - OutDiscards: The number of outbound packets that are discarded even if the packets are 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. The following is the list of sample types.
  - 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. The following is the list of sample types.
  - Rising: Trigger alarm when the first value is larger than the rising threshold.
  - Falling: Trigger alarm when the first value is less than the falling threshold.
  - RisingOrFalling: Trigger alarm when the first value is larger than the rising threshold or less than the falling threshold (default).
- **Rising Threshold:** Rising threshold value (–2147483648 to 2147483647).
- **Rising Index:** Rising event index (0–65535). If this value is zero, then no associated event is generated, as zero is not a valid event index.
- **Falling Threshold:** Falling threshold value (–2147483648 to 2147483647)



- **Falling Index:** Falling event index (0–65535). If this value is zero, no associated event is generated, as zero is not a valid event index.

#### 4.9.1.7.4 Switch RMON Event Configuration

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

Figure 4-36. RMON Event Configuration

Delete	ID	Desc	Type	Event Last Time
Delete			none	0

- **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 1–65535.
- **Desc:** Indicates this event. The string length is from 0–127, default is a null string.
- **Type:** Indicates the notification of the event. The following are the possible types.
  - None: No SNMP log is created; no SNMP trap is sent.
  - Log: Create SNMP log entry when the event is triggered.
  - Snmpttrap: Send SNMP trap when the event is triggered.
  - Logandtrap: Create SNMP log entry and sent SNMP trap when the event is triggered.
- **Event Last Time:** Indicates the value of sysUpTime at the time this event entry last generated an event.

### 4.9.2 Security Network Configuration

The following sections describe the security network configurations.

#### 4.9.2.1 Network Port Security Configuration

The following sections describe the network port security configurations.

##### 4.9.2.1.1 Port Security Configuration

This page allows you to configure the Port Security global and per-port settings. Port Security allows for limiting the number of users on a given port. A user is identified by a MAC address and VLAN ID. If Port Security is enabled on a port, the limit specifies the maximum number of users on the port. If this number is exceeded, then an action is taken depending on the violation mode. The violation mode can be one of the following options. The Port Security configuration consists of two sections, a global and a per-port.

Figure 4-37. Port Security Configuration

**Port Security Configuration**

**Global Configuration**

Aging Enabled	<input type="checkbox"/>
Aging Period	3600 seconds
Hold Time	300 seconds

**Port Configuration**

Port	Mode	Limit	Violation Mode	Violation Limit	Sticky	State
*	<>	4	<>	4	<input type="checkbox"/>	
1	Disabled	4	Protect	4	<input type="checkbox"/>	Disabled
2	Disabled	4	Protect	4	<input type="checkbox"/>	Disabled
3	Disabled	4	Protect	4	<input type="checkbox"/>	Disabled
4	Disabled	4	Protect	4	<input type="checkbox"/>	Disabled
5	Disabled	4	Protect	4	<input type="checkbox"/>	Disabled
6	Disabled	4	Protect	4	<input type="checkbox"/>	Disabled

- **Global Configuration**
  - **Aging Enabled:** If checked, the 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 functionality for securing MAC addresses, then they may have other

requirements to the aging period. The underlying functionality uses the shorter requested aging period of all modules that have aging enabled. The Aging Period can be set to a number between 10s–10000000s with a default of 3600s. To understand why aging may be desired, consider the following scenario: An end-host is connected to a third-party switch or hub, which in turn is connected to a port on this switch on which Port Security is enabled. The end-host is allowed to forward if the limit is not exceeded. Consider that the end-host logs off or powers down. If there is no aging, then the end-host continues to take up resources on this switch and is 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, then the end-host is disconnected, and the corresponding resources are freed on the switch.

- **Hold Time:** It is measured in seconds. The Hold Time is used to determine how long a MAC address is held in the MAC table if it has violated the limit. Valid range is between 10s–10000000s with a default of 300s. The reason for holding a violating MAC address in the MAC table is primarily to ensure that the same MAC address does not give rise to continuous notifications (if notifications on violation count is enabled).
- **Port Configuration:** The table has one row for each port on the switch and several columns, which are as follows:
  - Port: The port number to which the configuration below applies.
  - Mode: Controls whether Port Security is enabled on this port.
    - Note:** Other modules may still use the underlying port security features without enabling Port Security on a given port.
  - Limit: The maximum number of MAC addresses that can be secured on this port. This number cannot exceed 1023. Default is 4. If the limit is exceeded, then an action is taken corresponding to the mode. 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. As all ports draw from the same pool, a configured maximum might not be granted if the remaining ports have already used all available MAC addresses.
  - Violation Mode: If Limit is reached, then the switch can take one of the following actions:
    - Protect: Do not allow more than Limit MAC addresses on the port but take no further action.
    - Restrict: If Limit is reached, then the subsequent MAC addresses on the port are counted and marked as violating. Such MAC addresses are removed from the MAC table when the hold time expires. At the most, Violation Limit MAC addresses can be marked as violating at any given time.
    - Shutdown: If Limit is reached, then one additional MAC address causes the port to be shut down. This implies that all secured MAC addresses be removed from the port, and no new addresses be learned. There are three ways to re-open the port:
      - In the **Configuration > Ports** page's Configured column, disable the port and then restore the original mode.
      - Make a Port Security configuration change on the port.
      - Boot the switch.
- **Violation Limit:** The maximum number of MAC addresses that can be marked as violating on this port. This number cannot exceed 1023. Default is 4. It is only used when Violation mode is Restrict.
- **Sticky:** Enables sticky learning of MAC addresses on this port. When the port is in sticky mode, all MAC addresses that would otherwise have been learned as dynamic are learned as sticky. Sticky MAC addresses are part of the `running-config` and can therefore be saved to `startup-config`. Sticky MAC addresses survive link changes (in contrast to Dynamic, which will have to be learned again). They also survive reboots if `running-config` is saved to `startup-config`. A port can be Sticky-enabled whether Port Security is enabled on that interface. In that way, it is possible to add sticky MAC addresses management wise before enabling Port Security. To do that, use the **Configuration > Security > Port Security > MAC Addresses** page.
- **State:** This column shows the current Port Security state of the port. The state takes one of four values:
  - Disabled: Port Security is disabled on the port.
  - Ready: The limit is not yet reached. This can be shown for all violation modes.
  - Limit Reached: Indicates that the limit is reached on this port. This can be shown for all violation modes.
  - Shutdown: Indicates that the port is shut down by Port Security. This state can only be shown if violation mode is set to shut down.

### 4.9.2.1.2 Port MAC Address Configuration

On this page, you can add and delete static and sticky MAC addresses managed by Port Security.



Port security defines three types of MAC addresses, of which static and sticky can be added and removed on this page.

- **Dynamic:** A MAC address learned through learn frames coming to the Port Security module while the interface in question is not in sticky mode. Dynamic entries disappear if it ages out or if the interface link goes down.
- **Static:** A MAC address added by end-user through management. Static MAC addresses are not subject to aging and will be added to the MAC address table once Port Security gets enabled on the interface. Static entries are part of the `running-config` and survive interface link state changes. They reboot if saved to `startup-config`. Static entries can be added to the `running-config` at any time irrespective of Port Security being enabled.
- **Sticky:** When the interface is in the Sticky mode, then all entries that otherwise are learned as dynamic, are learned as sticky. Like static entries, sticky entries are part of the `running-config` and survive interface link state changes. They reboot if saved to the `startup-config`. Though it is not the intention with Sticky entries, they can be added by management to the `running-config` at any time irrespective of Port Security being enabled on the interface, if the interface is in the Sticky mode. Sticky entries disappear if the interface is taken out of the Sticky mode.

**Figure 4-38. Port Security Static and Sticky MAC Address**

Delete	Port	VLAN ID	MAC Address	Type
Delete	Select ... ▼	1	00:00:00:00:00:00	Static ▼

- **Delete:** Click to remove the entry from the MAC address table (if present) and the `running-config`.  
**Note:** Dynamic entries may be removed entirely on an interface through **Monitor > Security > Port Security > Switch** and one-by-one through **Monitor > Security > Port Security > Port**.
- **Port:** The port number to which this MAC address is bound.
- **VLAN ID and MAC Address:** The VLAN ID and MAC address in question.
- **Type:** Indicates the type of entry and may be either Static or Sticky.

### 4.9.2.2 Security Network 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 **Configuration > Security > AAA** page. The IEEE 802.1X standard defines port-based operation, but non-standard variants overcome security limitations. MAC-based authentication allows for authentication of more than one user on the same port and does not 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-wide and a port-wide.

Figure 4-39. Network Access Server Configuration

**Network Access Server Configuration**

**System Configuration**

Mode	Disabled <input type="button" value="v"/>	
Reauthentication Enabled	<input type="checkbox"/>	
Reauthentication Period	3600	seconds
EAPOL Timeout	30	seconds
Aging Period	300	seconds
Hold Time	10	seconds
RADIUS-Assigned QoS Enabled	<input type="checkbox"/>	
RADIUS-Assigned VLAN Enabled	<input type="checkbox"/>	
Guest VLAN Enabled	<input type="checkbox"/>	
Guest VLAN ID	1	
Max. Reauth. Count	2	
Allow Guest VLAN if EAPOL Seen	<input type="checkbox"/>	

**Port Configuration**

Port	Admin State	RADIUS-Assigned QoS Enabled	RADIUS-Assigned VLAN Enabled	Guest VLAN Enabled	Port State	Restart	
* <input type="button" value="v"/>		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>			
1	Force Authorized <input type="button" value="v"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate	Reinitialize
2	Force Authorized <input type="button" value="v"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate	Reinitialize
3	Force Authorized <input type="button" value="v"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate	Reinitialize
4	Force Authorized <input type="button" value="v"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate	Reinitialize
5	Force Authorized <input type="button" value="v"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate	Reinitialize
6	Force Authorized <input type="button" value="v"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate	Reinitialize

• **System Configuration:**

- Mode: Indicates if NAS is globally enabled or disabled on the switch. If globally disabled, then 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 does not imply that a client is still present on a port. See [Aging Period](#)).
- 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 selected. Valid values are in the range 1s–3600s.
- EAPOL Timeout: Determines the time for retransmission of Request Identity EAPOL frames. Valid values are in the range 1s–65535s. This has no effect for MAC-based ports.
- Aging Period: This setting applies to the following modes, that is, the 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 must check for activity on the MAC address in question at regular intervals and free resources if no activity is seen within a given period. This parameter controls exactly this period and can be set to a number between 10s–1000000s. If reauthentication is enabled and the port is in an 802.1X-based mode, then this is not so critical, as supplicants that are no longer attached to the port get removed upon the next reauthentication, which fails. 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 does not cause direct communication between the switch and the client. Therefore, it does not detect if 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, that is, 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 (according to the timeout specified on the **Configuration > Security > AAA** page), 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 ignores new frames coming from the client during the hold time. The Hold Time can be set to a number between 10s–1000000s.

- **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.

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 determines 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](#) 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 port's ditto setting determines whether RADIUS-assigned VLAN is enabled on that port. When unchecked, RADIUS-server assigned 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 entering the Guest VLAN, it first checks if this option is enabled or disabled. If disabled (unchecked; default), the switch only enters 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 considers 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 several columns, which are as follows:
  - Port: The port number for which the following configuration 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 sends one EAPOL Success frame when the port link comes up, and any client on the port is allowed network access without authentication.
    - Force Unauthorized: In this mode, the switch sends one EAPOL Failure frame when the port link comes up, and any client on the port is 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) does not 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 or block traffic on the switch port connected to the supplicant.

For example, if two backend servers are enabled and that the server timeout is configured to X seconds (using the Authentication, Authorization and Accounting (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 never gets authenticated, because the switch cancels on-going backend authentication server requests when it receives a new EAPOL Start frame from the supplicant. As the server has not yet failed (because the X seconds have not expired), the same server is contacted upon the next backend authentication server request from the switch. This scenario loops forever. Therefore, the server timeout must be smaller than the supplicant's EAPOL Start frame retransmission rate.

- **Single 802.1X:** In port-based 802.1X authentication, once a supplicant is successfully authenticated on a port, the whole port is opened for network traffic. This allows other clients that are connected to the port (for instance through a hub) to piggy-back on the successfully authenticated client and get network access even though they are not authenticated. To overcome this security breach, use the Single 802.1X variant. Single 802.1X is not an IEEE standard but features many of the same characteristics as does port-based 802.1X. In Single 802.1X, at most one supplicant can get authenticated on the port at a time. Normal EAPOL frames are used in the communication between the supplicant and the switch. If more than one supplicant is connected to a port, the one that comes first when the port's link comes up will be the first one considered. If that supplicant does not provide valid credentials within a certain amount of time, another supplicant will get a chance. Once a supplicant is successfully authenticated, only that supplicant is allowed access. This is the most secure of all the supported modes. In this mode, the Port Security module is used to secure a supplicant's MAC address once successfully authenticated.
- **Multi 802.1X:** Multi 802.1X is like Single 802.1X—it is not an IEEE standard, but a variant that features many of the same characteristics. In Multi 802.1X, one or more supplicants can get authenticated on the same port at the same time. Each supplicant is authenticated individually and secured in the MAC table using the Port Security module. In Multi 802.1X, it is not possible to use the multicast BPDU MAC address as destination MAC address for EAPOL frames sent from the switch towards the supplicant, as that causes all supplicants attached to the port to reply to requests sent from the switch. Instead, the switch uses the supplicant's MAC address, which is obtained from the first EAPOL Start or EAPOL Response Identity frame sent by the supplicant. An exception to this is when no supplicants are attached. In this case, the switch sends EAPOL Request Identity frames using the BPDU multicast MAC address as destination: to wake up any supplicants that might be on the port. The maximum number of supplicants that can be attached to a port can be limited using the Port Security Limit Control functionality.
- **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 or block traffic for that particular client, using the Port Security module. Only then, the frames from the client can 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.
- **RADIUS-Assigned QoS Enabled:** When RADIUS-Assigned QoS is both globally enabled and enabled (checked) on a given port, the switch reacts to QoS Class information carried in the RADIUS Access-

Accept packet transmitted by the RADIUS server when a supplicant is successfully authenticated. If present and valid, traffic received on the supplicant's port will be classified to the given QoS Class. If (re-)authentication fails or the RADIUS Access-Accept packet no longer carries a QoS Class or it's invalid, or the supplicant is otherwise no longer present on the port, the port's QoS Class is immediately reverted to the original QoS Class (which may be changed by the administrator in the meanwhile without affecting the RADIUS-assigned).

This option is only available for single-client modes:

- Port-based 802.1X
- Single 802.1X

### **RADIUS Attributes Used in Identifying a QoS Class**

The User-Priority-Table attribute defined in RFC4675 forms the basis for identifying the QoS Class in an Access-Accept packet. Only the first occurrence of the attribute in the packet is considered, and to be valid, it must follow this rule: All eight octets in the attribute's value must be identical and consist of ASCII characters in the range **0: 7**, which translates into the desired QoS Class in the range [0; 7].

- **RADIUS-Assigned VLAN Enabled:** When RADIUS-Assigned VLAN is both globally enabled and enabled (checked) for a given port, the switch reacts to VLAN ID information carried in the RADIUS Access-Accept packet transmitted by the RADIUS server when a supplicant is successfully authenticated. If present and valid, the port's Port VLAN ID is changed to this VLAN ID, the port is set to be a member of that VLAN ID, and the port is forced into VLAN unaware mode. Once assigned, all traffic arriving on the port is classified and switched on the RADIUS-assigned VLAN ID. If (re-)authentication fails or the RADIUS Access-Accept packet no longer carries a VLAN ID, it is invalid, or the supplicant is otherwise no longer present on the port, then the port's VLAN ID is immediately reverted to the original VLAN ID (which may be changed by the administrator in the meanwhile without affecting the RADIUS-assigned).

This option is only available for single-client modes:

- Port-based 802.1X
- Single 802.1X

For trouble shooting VLAN assignments, use the **Monitor > VLANs > VLAN Membership and VLAN Port** pages. These pages show which modules have (temporarily) overridden the current Port VLAN configuration.

### **RADIUS attributes used in identifying a VLAN ID:**

RFC2868 and RFC3580 form the basis for the attributes used in identifying a VLAN ID in an Access-Accept packet. The following criteria are used:

- The `Tunnel-Medium-Type`, `Tunnel-Type`, and `Tunnel-Private-Group-ID` attributes must all be present at least once in the Access-Accept packet.
- The switch looks for the first set of these attributes that have the same `Tag` value and fulfil the following requirements (if `Tag == 0` is used, the `Tunnel-Private-Group-ID` does not need to include a `Tag`):
  - Value of `Tunnel-Medium-Type` must be set to **IEEE-802** (ordinal 6).
  - Value of `Tunnel-Type` must be set to **VLAN** (ordinal 13).
  - Value of `Tunnel-Private-Group-ID` must be a string of ASCII chars in the range **0: 9**, which is interpreted as a decimal string representing the VLAN ID. Leading 0s are discarded. The final value must be in the range [1; 4095].
- **Guest VLAN Enabled:** When Guest VLAN is both globally enabled and enabled (checked) for a given port, then the switch considers moving the port into the Guest VLAN according to the following rules. This option is only available for EAPOL-based modes:
  - Port-based 802.1X
  - Single 802.1X
  - Multi 802.1X

For trouble shooting VLAN assignments, use the **Monitor > VLANs > VLAN Membership and VLAN Port** pages. These pages show which modules have (temporarily) overridden the current Port VLAN configuration.

### **Guest VLAN Operation**

When a Guest VLAN enabled port's link comes up, the switch starts transmitting EAPOL Request Identity frames. If the number of transmissions of such frames exceeds Max. Reauth. count and no EAPOL frames have been received, the switch considers entering the Guest VLAN. The interval between transmission of EAPOL Request Identity frames is configured with EAPOL Timeout. If **Allow Guest VLAN if EAPOL Seen** is enabled, then the port is placed in the Guest VLAN. If disabled, the switch first checks its history to see if an EAPOL frame has previously been received on the port (this history is cleared if the port link goes down or the port's Admin State is changed), and if not, the port is placed in the Guest VLAN. Otherwise, it does not move to the Guest VLAN but continue transmitting EAPOL Request Identity frames at the rate given by EAPOL Timeout. Once in the Guest VLAN, the port is considered authenticated, and all attached clients on the port are allowed access on this VLAN. The switch does not transmit an EAPOL Success frame when entering the Guest VLAN. While in the Guest VLAN, the switch monitors the link for EAPOL frames, and if one such frame is received, then the switch immediately takes the port out of the Guest VLAN and starts authenticating the supplicant according to the port mode. If an EAPOL frame is received, then the port is never able to go back into the Guest VLAN, if **Allow Guest VLAN if EAPOL Seen** is disabled.

- Port State: 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-supplicant mode and the supplicant is authorized.
  - Unauthorized: The port is in Force Unauthorized or a single-supplicant mode and the supplicant is not successfully authorized by the RADIUS server.
  - X Auth/Y Unauth: The port is in a multi-supplicant 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 transfer to the unauthorized state while the reauthentication is in progress.

### 4.9.2.3 Security Network ACL Configuration

The following section describes the security network ACL configurations.

#### 4.9.2.3.1 Network ACL Ports Configuration

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

Figure 4-40. ACL Ports Configuration

Port	Policy ID	Action	Rate Limiter ID	Port Redirect	Mirror	Logging	Shutdown	State	Counter
*	0	Permit	Disabled	Disabled	Disabled	Disabled	Disabled	Enabled	0
1	0	Permit	Disabled	Disabled	Disabled	Disabled	Disabled	Enabled	0
2	0	Permit	Disabled	Disabled	Disabled	Disabled	Disabled	Enabled	0
3	0	Permit	Disabled	Disabled	Disabled	Disabled	Disabled	Enabled	0
4	0	Permit	Disabled	Disabled	Disabled	Disabled	Disabled	Enabled	241
5	0	Permit	Disabled	Disabled	Disabled	Disabled	Disabled	Enabled	0
6	0	Permit	Disabled	Disabled	Disabled	Disabled	Disabled	Enabled	55603

Save Reset

- **Port:** The logical port for the settings contained in the same row.
- **Policy ID:** Select the policy to apply to this port. The allowed values are 0–63. The default value is 0.
- **Action:** Select if 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 1–16. The default value is **Disabled**.
- **Port Redirect:** Select which port frames are redirected. The allowed values are Disabled, or a specific port number and it cannot 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 does not 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:** The shutdown feature only works when the packet length is less than 1518 (without VLAN tags).
- **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.

#### 4.9.2.3.2 Network ACL Rate Limiters Configuration

Configure the rate limiter for the ACL of the switch on this page.



Figure 4-41. ACL Rate Limiter Configuration

Rate Limiter ID	Rate	Unit
*	1	<> ▾
1	1	pps ▾
2	1	pps ▾
3	1	pps ▾
4	1	pps ▾
5	1	pps ▾
6	1	pps ▾
7	1	pps ▾
8	1	pps ▾
9	1	pps ▾
10	1	pps ▾
11	1	pps ▾
12	1	pps ▾
13	1	pps ▾
14	1	pps ▾
15	1	pps ▾
16	1	pps ▾

Save Reset

- **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 0–99, 100, 200, 300, to 1092000 in pps or 0, 100, 200, 300, to 1000000 in Kbps.
- **Unit:** Specify the rate unit. The allowed values are:
  - pps: packets per second.
  - kbps: Kbits per second.

4.9.2.3.3 Network ACL Access Control List Configuration

Configure an Access Control Entry (ACE) on this page. An ACE consists of several parameters. These parameters vary according to the frame type that you select. First, select the ingress port for the ACE, and then select the frame type. Different parameter options are displayed depending on the frame type selected. A frame that hits this ACE matches the configuration that is defined here.

Figure 4-42. ACE Configuration—Global Parameters

Second Lookup	Disabled ▾	Action	Permit ▾
Ingress Port	All ▾ Port 1 Port 2 Port 3 Port 4 ▾	Rate Limiter	Disabled ▾
Policy Filter	Any ▾	Mirror	Disabled ▾
Frame Type	Any ▾	Logging	Disabled ▾
		Shutdown	Disabled ▾
		Counter	0

VLAN Parameters

802.1Q Tagged	Any ▾
VLAN ID Filter	Any ▾
Tag Priority	Any ▾

Save Reset Cancel

- **Global Configuration**
  - Second Lookup: Specify the second lookup operation of the ACE.
  - Ingress Port: Select the ingress port for which this ACE applies.
    - All: The ACE applies to all port.
    - Port n: The ACE applies to this port number, where n is the number of the switch port.
  - Policy Filter: Specify the policy number filter for this ACE.
    - Any: No policy filter is specified (policy filter status is **don't-care**.)



- Specific: If you want to filter a specific policy with this ACE, then choose this value. Two fields for entering the policy value and the bitmask appear.
- Policy Value: When **Specific** is selected for the policy filter, then you can enter a specific policy value. The allowed range is 0 to 63.
- Policy Bitmask: When **Specific** is selected for the policy filter, then you can enter a specific policy bitmask. The allowed range is 0x0 to 0x3f. While using bitmask, if the binary bit value is **0**, then it means this bit is **don't-care**. The real matched pattern is [policy\_value and policy\_bitmask]. For example, if the policy value is 3 and the policy bitmask is 0x10 (bit 0 is **don't-care** bit), then policies 2 and 3 are applied to this rule.
- Frame Type: Select the frame type for this ACE. These frame types are mutually exclusive.
  - Any: Any frame can match this ACE.
  - Ethernet Type: Only Ethernet Type frames can match this ACE. The IEEE 802.3 standard describes the value of Length/Type Field specifications to be greater than or equal to 1536 decimal (equal to 0600 hexadecimal) and the value must not be equal to 0x800 (IPv4), 0x806 (ARP), or 0x86DD (IPv6).
  - ARP: Only ARP frames can match this ACE.
 

**Note:** The ARP frames do not match the ACE with ethernet type.
  - IPv4: Only IPv4 frames can match this ACE.
 

**Note:** The IPv4 frames do not match the ACE with ethernet type.
  - IPv6: Only IPv6 frames can match this ACE.
 

**Note:** The IPv6 frames do not match the ACE with Ethernet type.
- **Action:** Specify the action to take with a frame that hits this ACE.
  - Permit: The frame that hits this ACE is granted permission for the ACE operation.
  - Deny: The frame that hits this ACE is dropped.
  - Filter: Frames matching the ACE are filtered.
- Rate Limiter: Specify the rate limiter in number of base units. The allowed range is 1–16. Disabled indicates that the rate limiter operation is disabled.
- Port Redirect: Frames that hit the ACE are redirected to the port number specified here. The rate limiter affects these ports. The allowed range is the same as the switch port number range. Disabled indicates that the port redirect operation is disabled, and the specific port number of **Port Redirect** cannot be set when action is permitted.
- Mirror: Specify the mirror operation of this port. Frames matching the ACE are mirrored to the destination mirror port. The rate limiter does not affect frames on the 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**.
- Logging: Specify the logging operation of the ACE.
 

**Note:** The logging message doesn't include the 4 bytes CRC information.

The allowed values are:

  - Enabled: Frames matching the ACE are stored in the System Log.
  - Disabled: Frames matching the ACE are not logged.

**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 the ACE. The allowed values are:
  - Enabled: If a frame matches the ACE, the ingress port will be disabled.
  - Disabled: Port shutdown is disabled for the ACE.

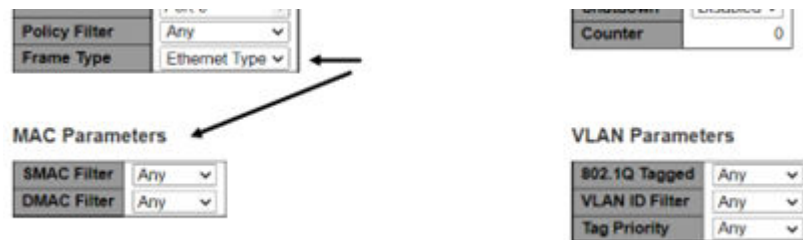
**Note:** The shutdown feature only works when the packet length is less than 1518 (without VLAN tags).
- Counter: The counter indicates the number of times the ACE was hit by a frame.
- **VLAN Parameters**
  - 802.1Q Tagged: Specify whether frames can hit the action according to the 802.1Q tagged. The allowed values are:

- Any: Any value is allowed (**don't-care**).
- Enabled: Tagged frame only.
- Disabled: Untagged frame only.

The default value is **Any**.

- VLAN ID Filter: Specify the VLAN ID filter for this ACE.
  - 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 with this ACE, then choose this value. A field for entering a VLAN ID number appears.
- VLAN ID: When **Specific** is selected for the VLAN ID filter, you can enter a specific VLAN ID number. The allowed range is 1 to 4095. A frame that hits this ACE matches this VLAN ID value.
- Tag Priority: Specify the tag priority for this ACE. A frame that hits this ACE matches this tag priority. The allowed number range is 0 to 7 or range 0–1, 2–3, 4–5, 6–7, 0–3, and 4–7. The value **Any** means that no tag priority is specified (tag priority is **don't-care**).
- **MAC Parameters:** The MAC parameters are Only displayed when the frame type is *Ethernet Type* or *ARP*.

Figure 4-43. ACE Configuration—MAC Parameters



- SMAC Filter: Specify the source MAC filter for this ACE.
  - Any: No SMAC filter is specified (SMAC filter status is **don't-care**).
  - Specific: If you want to filter a specific source MAC address with this ACE, choose this value. A field for entering a SMAC value appears.
- SMAC Value: When **Specific** is selected for the SMAC filter, you can enter a specific source MAC address. The legal format is `xx-xx-xx-xx-xx-xx` or `xx.xx.xx.xx.xx.xx` or `xxxxxxxxxxxx` (x is a hexadecimal digit). A frame that hits this ACE matches this SMAC value.
- DMAC Filter: Specify the destination MAC filter for this ACE.
  - Any: No DMAC filter is specified (DMAC filter status is **don't-care**).
  - MC: Frame must be multicast.
  - BC: Frame must be broadcast.
  - UC: Frame must be unicast.
  - Specific: If you want to filter a specific destination MAC address with this ACE, choose this value. A field for entering a DMAC value appears.
- DMAC Value: When **Specific** is selected for the DMAC filter, you can enter a specific destination MAC address. The legal format is `xx-xx-xx-xx-xx-xx` or `xx.xx.xx.xx.xx.xx` or `xxxxxxxxxxxx` (x is a hexadecimal digit). A frame that hits this ACE matches this DMAC value.
- **ARP Parameters:** The ARP parameters can be configured when Frame Type **ARP** is selected.

Figure 4-44. ACE Configuration—ARP Parameters

- ARP/RARP: Specify the available ARP/RARP opcode (OP) flag for this ACE.
  - Any: No ARP/RARP OP flag is specified (OP is **don't-care**).
  - ARP: Frame must have ARP opcode set to ARP.
  - RARP: Frame must have RARP opcode set to RARP.
  - Other: Frame has unknown ARP/RARP Opcode flag.
- Request/Reply: Specify the available Request/Reply opcode (OP) flag for this ACE.
  - Any: No Request/Reply OP flag is specified (OP is **don't-care**).
  - Request: Frame must have ARP Request or RARP Request OP flag set.
  - Reply: Frame must have ARP Reply or RARP Reply OP flag.
- Sender IP Filter: Specify the sender IP filter for this ACE.
  - Any: No sender IP filter is specified (sender IP filter is **don't-care**).
  - Host: Sender IP filter is set to Host. Specify the sender IP address in the SIP Address field that appears.
  - Network: Sender IP filter is set to Network. Specify the sender IP address and sender IP mask in the SIP Address and SIP Mask fields that appear.
- Sender IP Address: When Host or Network is selected for the sender IP filter, you can enter a specific sender IP address in dotted decimal notation.
 

**Note:** The invalid IP address configuration is also acceptable. For example, 0.0.0.0. Normally, an ACE with invalid IP address will explicitly deny action.
- Sender IP Mask: When Network is selected for the sender IP filter, you can enter a specific sender IP mask in dotted decimal notation.
- Target IP Filter: Specify the target IP filter for this specific ACE.
  - Any: No target IP filter is specified (target IP filter is **don't-care**).
  - Host: Target IP filter is set to Host. Specify the target IP address in the Target IP Address field that appears.
  - Network: Target IP filter is set to Network. Specify the target IP address and target IP mask in the Target IP Address and Target IP Mask fields that appear.
- Target IP Address: When Host or Network is selected for the target IP filter, you can enter a specific target IP address in dotted decimal notation.
 

**Note:** The invalid IP address configuration is also acceptable. For example, 0.0.0.0. Normally, an ACE with invalid IP address will explicitly deny action.
- Target IP Mask: When Network is selected for the target IP filter, you can enter a specific target IP mask in dotted decimal notation.
- ARP Sender MAC Match: Specify whether frames can hit the action according to their Sender Hardware Address (SHA) field settings.

- 0: ARP frames where SHA is not equal to the SMAC address.
- 1: ARP frames where SHA is equal to the SMAC address.
- Any: Any value is allowed (**don't-care**).
- RARP Target MAC Match: Specify whether frames can hit the action according to their Target Hardware Address (THA) field settings.
  - 0: RARP frames where THA is not equal to the target MAC address.
  - 1: RARP frames where THA is equal to the target MAC address.
  - Any: Any value is allowed (**don't-care**).
- IP/Ethernet Length: Specify whether frames can hit the action according to their ARP/RARP Hardware Address Length (HLN) and Protocol Address Length (PLN) settings.
  - 0: ARP/RARP frames where the HLN is not equal to Ethernet (0x06) or the (PLN) is not equal to IPv4 (0x04).
  - 1: ARP/RARP frames where the HLN is equal to Ethernet (0x06) and the (PLN) is equal to IPv4 (0x04).
  - Any: Any value is allowed (**don't-care**).
- IP: Specify whether frames can hit the action according to their ARP/RARP Hardware Address Space (HRD) settings.
  - 0: ARP/RARP frames where the HLD is not equal to Ethernet (1).
  - 1: ARP/RARP frames where the HLD is equal to Ethernet (1).
  - Any: Any value is allowed (**don't-care**).
- Ethernet: Specify whether frames can hit the action according to their ARP/RARP protocol address space (PRO) settings.
  - 0: ARP/RARP frames where the PRO is not equal to IP (0x800).
  - 1: ARP/RARP frames where the PRO is equal to IP (0x800).
  - Any: Any value is allowed (**don't-care**).
- **IP Parameters:** The IP parameters can be configured when Frame Type **IPv4** is selected.

**Figure 4-45. ACE Configuration IP Parameters**

The screenshot displays the configuration interface for an ACE. At the top, there are fields for 'Policy Filter' (set to 'Any'), 'Frame Type' (set to 'IPv4'), and 'Counter' (set to '0'). Below these are three sections of parameters:

- MAC Parameters:** 'DMAC Filter' is set to 'Any'.
- VLAN Parameters:** '802.1Q Tagged' is 'Any', 'VLAN ID Filter' is 'Any', and 'Tag Priority' is 'Any'.
- IP Parameters:** A table of dropdown menus:
 

IP Protocol Filter	Any
IP TTL	Any
IP Fragment	Any
IP Option	Any
SIP Filter	Any
DIP Filter	Any

At the bottom, there are 'Save', 'Reset', and 'Cancel' buttons. Arrows in the original image point to the 'Frame Type' and 'IP Protocol Filter' dropdowns.

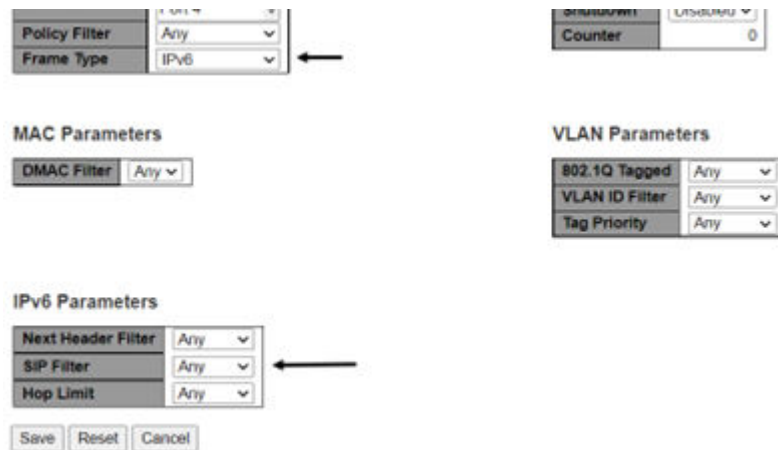
- **IP Protocol Filter:** Specify the IP protocol filter for this ACE.
  - Any: No IP protocol filter is specified (**don't-care**).
  - Specific: If you want to filter a specific IP protocol filter with this ACE, choose this value. A field for entering an IP protocol filter appears.
  - ICMP: Select ICMP to filter IPv4 ICMP protocol frames. Extra fields for defining ICMP parameters appear. These fields are explained later in this help file.
  - UDP: Select UDP to filter IPv4 UDP protocol frames. Extra fields for defining UDP parameters appear. These fields are explained later in this help file.

- TCP: Select TCP to filter IPv4 TCP protocol frames. Extra fields for defining TCP parameters appear. These fields are explained later in this help file.
- **IP Protocol Value:** When **Specific** is selected for the IP protocol value, you can enter a specific value. The allowed range is 0–255. A frame that hits this ACE matches this IP protocol value.
- **IP TTL:** Specify the Time-to-Live (TTL) settings for this ACE.
  - zero: IPv4 frames with a TTL field greater than zero must not be able to match this entry.
  - non-zero: IPv4 frames with a TTL field greater than zero must be able to match this entry.
  - Any: Any value is allowed (**don't-care**).
- **IP Fragment:** Specify the fragment offset settings for this ACE. This involves the settings for the More Fragments (MF) bit and the Fragment Offset (FRAG OFFSET) field for an IPv4 frame.
  - No: 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.
  - Yes: IPv4 frames where the MF bit is set or the FRAG OFFSET field is greater than zero must be able to match this entry.
  - Any: Any value is allowed (**don't-care**).
- **IP Option:** Specify the options flag setting for this ACE.
  - No: IPv4 frames where the options flag is set must not be able to match this entry.
  - Yes: IPv4 frames where the options flag is set must be able to match this entry.
  - Any: Any value is allowed (**don't-care**).
- **SIP Filter:** Specify the source IP filter for this ACE.
  - Any: No source IP filter is specified (source IP filter is **don't-care**).
  - Host: Source IP filter is set to Host. Specify the source IP address in the SIP Address field that appears.
  - Network: Source IP filter is set to Network. Specify the source IP address and source IP mask in the SIP Address and SIP Mask fields that appear.
- **SIP Address:** When Host or Network is selected for the source IP filter, you can enter a specific SIP address in dotted decimal notation.

**Note:** The invalid IP address configuration is also acceptable. For example, 0.0.0.0. Normally, an ACE with invalid IP address will explicitly adding deny action.
- **SIP Mask:** When Network is selected for the source IP filter, you can enter a specific SIP mask in dotted decimal notation.
- **DIP Filter:** Specify the destination IP filter for this ACE.
  - Any: No destination IP filter is specified (destination IP filter is **don't-care**).
  - Host: Destination IP filter is set to Host. Specify the destination IP address in the DIP Address field that appears.
  - Network: Destination IP filter is set to Network. Specify the destination IP address and destination IP mask in the DIP Address and DIP Mask fields that appear.
- **DIP Address:** When Host or Network is selected for the destination IP filter, you can enter a specific DIP address in dotted decimal notation.

**Note:** The invalid IP address configuration is also acceptable. For example, 0.0.0.0. Normally, an ACE with invalid IP address will explicitly adding deny action.
- **DIP Mask:** When Network is selected for the destination IP filter, you can enter a specific DIP mask in dotted decimal notation.
- **IPv6 Parameters:** The IPv6 parameters can be configured when Frame Type **IPv6** is selected.

Figure 4-46. ACE Configuration—IPv6 Parameters



- **Next Header Filter:** Specify the IPv6 next header filter for this ACE.
  - Any: No IPv6 next header filter is specified (**don't-care**).
  - Specific: If you want to filter a specific IPv6 next header filter with this ACE, choose this value. A field for entering an IPv6 next header filter appears.
  - ICMP: Select ICMP to filter IPv6 ICMP protocol frames. Extra fields for defining ICMP parameters will appear. These fields are explained later in this help file.
  - UDP: Select UDP to filter IPv6 UDP protocol frames. Extra fields for defining UDP parameters will appear. These fields are explained later in this help file.
  - TCP: Select TCP to filter IPv6 TCP protocol frames. Extra fields for defining TCP parameters will appear. These fields are explained later in this help file.
- **Next Header Value:** When **Specific** is selected for the IPv6 next header value, you can enter a specific value. The allowed range is 0 to 255. A frame that hits this ACE matches this IPv6 protocol value.
- **SIP Filter:** Specify the source IPv6 filter for this ACE.
  - Any: No source IPv6 filter is specified. (Source IPv6 filter is **don't-care**).
  - Specific: Source IPv6 filter is set to Network. Specify the source IPv6 address and source IPv6 mask in the SIP Address fields that appear.
- **SIP Address:** When **Specific** is selected for the source IPv6 filter, you can enter a specific SIPv6 address. The field only supported last 32 bits for IPv6 address.
- **SIP BitMask:** When **Specific** is selected for the source IPv6 filter, you can enter a specific SIPv6 mask. The field only supported last 32 bits for IPv6 address.
 

**Note:** The usage of bitmask, if the binary bit value is **0** means that this bit is **don't-care**. The real matched pattern is [sipv6\_address and sipv6\_bitmask] (last 32 bits). For example, if the SIPv6 address is 2001::3 and the SIPv6 bitmask is 0xFFFFFFFF (bit 0 is **don't-care** bit), then SIPv6 addresses 2001::2 and 2001::3 are applied to this rule.
- **Hop Limit:** Specify the hop limit settings for this ACE.
  - zero: IPv6 frames with a hop limit field greater than zero must not be able to match this entry.
  - non-zero: IPv6 frames with a hop limit field greater than zero must be able to match this entry.
  - Any: Any value is allowed (**don't-care**).

#### 4.9.2.3.4 Security Network IP Source Guard Configuration

The following sections describe the security network IP source guard configurations.

##### Network IP Source Guard Configuration

This page provides IP Source Guard related configuration.

Figure 4-47. IP Source Guard Configuration

**IP Source Guard Configuration**

Mode

Translate dynamic to static

**Port Mode Configuration**

Port	Mode	Max Dynamic Clients
*	<>	<>
1	Disabled	Unlimited
2	Disabled	Unlimited
3	Disabled	Unlimited
4	Disabled	Unlimited
5	Disabled	Unlimited
6	Disabled	Unlimited

- **Mode of IP Source Guard Configuration:** Enable the Global IP Source Guard or disable the Global IP Source Guard. All configured ACEs are lost when the mode is enabled.
- **Port Mode Configuration:** Specify IP Source Guard is enabled on which ports. Only when both Global mode and Port mode on a given port are enabled, IP Source Guard is enabled on this given port.
- **Maximum Dynamic Clients:** Specify the maximum number of dynamic clients that can be learned on given port. This value can be 0, 1, 2, or unlimited. If the Port mode is enabled and the value of maximum dynamic client is equal to 0, then it means that only those IP packets allowed for forwarding that are matched in static entries on the specific port.

**Network IP Source Guard Static Table Configuration**

This page shows the static IP Source Guard rules. The maximum number of rules is 112 on the switch.

Figure 4-48. Static IP Source Guard Table

Delete	Port	VLAN ID	IP Address	MAC address
Delete	1			

- **Delete:** Check to delete the entry. It will be deleted during the next save.
- **Port:** The logical port for the settings.
- **VLAN ID:** The VLAN ID for the settings.
- **IP Address:** Allowed Source IP address.
- **MAC Address:** Allowed Source MAC address.

**4.9.2.3.5 Security Network IPv6 Source Guard Configuration**

The following sections describe the security network IPv6 source guard configurations.

**Network IPv6 Source Guard Configuration**

This page provides IPv6 Source Guard related configuration.

Figure 4-49. IPv6 Source Guard Configuration

**Please note:**  
 Enabling this function requires you to change the *Key Type* to "MAC and IP Address" for all ports that will receive DHCPv6 packets.  
 You can do this in the [QoS Port Classification](#) page.

Mode: Disabled ▾

Translate dynamic to static

Port	Mode	Max Dynamic Clients
Gi 1/1	Disabled ▾	Unlimited ▾
Gi 1/2	Disabled ▾	Unlimited ▾
Gi 1/3	Disabled ▾	Unlimited ▾
Gi 1/4	Disabled ▾	Unlimited ▾
2.5G 1/1	Disabled ▾	Unlimited ▾
2.5G 1/2	Disabled ▾	Unlimited ▾

- **IPv6 Source Guard Mode Configuration:** Enable or disable the IPv6 Source Guard globally.
- **Port Mode Configuration:** The table shows all ports on the device. There IPv6 Source Guard can be enabled/ disabled on individual ports. Only when both Global mode and Port mode on a given port are enabled, IPv6 Source Guard is enabled on this given port.
- **Max Dynamic Clients:** Specify the maximum number of dynamic clients that can be learned on given port. This value can be 0, 1, 2, or unlimited. If the Port mode is enabled and the value of maximum dynamic client is equal to 0, then only IPv6 packets that are matched in static entries on the specific port are forwarded.

**Network IPv6 Source Guard Static Table Configuration**

This page shows the static IPv6 Source Guard entries. The maximum number of entries is 112 on the switch.

Figure 4-50. IPv6 Source Guard Static Table

Auto-refresh

Port: Gi 1/1 ▾ VLAN ID:  IP Address:  MAC Address:

Port	VLAN ID	IPv6 Address	MAC Address
------	---------	--------------	-------------

- **Delete:** Click entry **Delete** to delete the entry.
- **Port:** The logical port to which the entry is bound.
- **VLAN ID:** The VLAN ID for the entry. If no VLAN ID is associated with the entry, this field shows 0.
- **IPv6 Address:** Allowed Source IPv6 address.
- **Prefix Size:** Prefix size of the IPv6 address.
- **Mac Address:** Allowed Source MAC address.

**4.9.2.3.6 Security Network ARP Inspection Configuration**

The following sections describe the Security Network ARP Inspection configuration.

**Network ARP Inspection Port Configuration**

This page provides ARP Inspection related configuration.



Figure 4-51. ARP Inspection Configuration

**ARP Inspection Configuration**

Mode

**Port Mode Configuration**

Port	Mode	Check VLAN	Log Type
*	<>	<>	<>
1	Disabled	Disabled	None
2	Disabled	Disabled	None
3	Disabled	Disabled	None
4	Disabled	Disabled	None
5	Disabled	Disabled	None
6	Disabled	Disabled	None

- **ARP Inspection Configuration**
  - **Mode:** Enable the Global ARP Inspection or disable the Global ARP Inspection.
- **Port Mode Configuration**
  - **Mode:** Specify ARP Inspection is enabled on which ports. Only when both Global Mode and Port Mode on a given port are enabled, ARP Inspection is enabled on this given port. Possible modes are:
    - Enabled: Enable ARP Inspection operation.
    - Disabled: Disable ARP Inspection operation.
  - **Check VLAN:** If you want to inspect the VLAN configuration, you must enable the setting of **Check VLAN**. The default setting of **Check VLAN** is disabled. When the setting of **Check VLAN** is disabled, the log type of ARP Inspection refers to the port setting. Enable the setting of **Check VLAN**, so that the log type of ARP Inspection refers to the VLAN setting. Possible settings of **Check VLAN** are as follows:
    - Enable: Enable check VLAN operation.
    - Disabled: Disable check VLAN operation.
  - **Log Type:** Only the Global mode and Port mode on a given port are enabled, and the setting of **Check VLAN** is disabled, the log type of ARP Inspection will refer to the port setting. The following are the four log types and possible types:
    - None: Log nothing
    - Deny: Log denied entries
    - Permit: Log permitted entries
    - ALL: Log all entries

**Network ARP Inspection VLAN Configuration**

This page provides ARP Inspection related configuration. Each page shows up to 9999 entries from the VLAN table, default being 20, selected through the **entries per page** input field. When first visited, the web page shows the first 20 entries from the beginning of the VLAN table. The first displayed is the one with the lowest VLAN ID found in the VLAN table.

Figure 4-52. ARP Inspection—VLAN Configuration

Start from VLAN  with  entries per page.

Delete	VLAN ID	Log Type
Delete	<input type="text"/>	None

- **VLAN ID:** Specify for which VLAN ID ARP inspection must be done. First, you must enable the port setting on the Port mode configuration web page. Only when both Global mode and Port mode on a given port are

enabled, ARP Inspection is enabled on this given port. Second, you can specify which VLAN is inspected on VLAN mode configuration web page.

- **Log Type:** Log type must be configured for every VLAN ID.
  - None: Log nothing.
  - Deny: Log denied entries.
  - Permit: Log permitted entries.
  - ALL: Log all entries

### Network ARP Inspection Static Table Configuration

This page shows the static ARP Inspection rules. The maximum number of rules is 256 on the switch.

**Figure 4-53. Static ARP Inspection Table**

Delete	Port	VLAN ID	MAC Address	IP Address
Delete	1			

- **Delete:** Check to delete the entry. It will be deleted during the next save.
- **Port:** The logical port for the settings.
- **VLAN ID:** The VLAN ID for the settings.
- **MAC Address:** Allowed Source MAC address in ARP request packets.
- **IP Address:** Allowed Source IP address in ARP request packets.

### Network ARP Inspection Dynamic Table Configuration

Entries in the Dynamic ARP Inspection Table are shown on this page. The Dynamic ARP Inspection Table contains up to 256 entries, and is sorted in the following order:

1. Port
2. VLAN ID
3. MAC address
4. IP address

All dynamic entries are learning from DHCP Snooping.

**Figure 4-54. Dynamic ARP Inspection Table**

Auto-refresh   << >>

Start from  , VLAN  , MAC address  and IP address  with  entries per page.

Port	VLAN ID	MAC Address	IP Address	Translate to static
No more entries				

- **Port:** Switch Port Number for which the entries are displayed.
- **VLAN ID:** VLAN ID in which the ARP traffic is permitted.
- **MAC Address:** User MAC address of the entry.
- **IP Address:** User IP address of the entry.
- **Translate to Static:** Select the checkbox to translate the entry to static entry.

## 4.9.3 Security AAA Configuration

The following sections describe the Security AAA configurations.

### 4.9.3.1 AAA RADIUS Configuration

This page allows you to configure up to five RADIUS servers.

Figure 4-55. RADIUS Server Configuration

**RADIUS Server Configuration**

Global Configuration

Timeout	5	seconds
Retransmit	3	times
Deadtime	0	minutes
Change Secret Key	No <input type="checkbox"/>	
NAS-IP-Address		
NAS-IPv6-Address		
NAS-Identifier		

Server Configuration

Delete	Hostname	Auth Port	Acct Port	Timeout	Retransmit	Change Secret Key
<input type="checkbox"/>	Delete	1812	1813			

- **Global Configuration**

- Timeout: Timeout is the number of seconds, in the range 1–1000, to wait for a reply from a RADIUS server before retransmitting the request.
- Retransmit: Retransmit is the number of times, in the range 1–1000, 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 0–1440 minutes, is the period during which the switch does not send new requests to a server that has failed to respond to a previous request. This stops 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 (zero) enables this feature, but only if more than one server has been configured.
- Change Secret Key: Specify to change the secret key or not. When **Yes** is selected for the option, you can change 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-IPv6-Address (Attribute 95): The IPv6 address to be used as attribute 95 in RADIUS Access-Request packets. If this field is left blank, the IP address of the outgoing interface is used.
- NAS-Identifier (Attribute 32): This identifier is up to 253 characters long and used as attribute 32 in RADIUS Access-Request packets. If this field is left blank, then the NAS-Identifier is not included in the packet.

- **Server Configuration**

- Delete: To delete a RADIUS server entry, check this box. The entry will be deleted during the next Save.
- Hostname: The IPv4/IPv6 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.
- Change Secret Key: Specify to change the secret key or not. When the checkbox is checked, you can change the setting overrides the global key. Leaving it blank will use the global key.

#### 4.9.3.2 AAA TACACS++ Configuration

This page allows you to configure up to 5 TACACS++ servers.

Figure 4-56. TACACS Server Configuration

**TACACS+ Server Configuration**

Global Configuration

Timeout	5	seconds
Deadtime	0	minutes
Change Secret Key	No	

Server Configuration

Delete	Hostname	Port	Timeout	Change Secret Key
<input type="checkbox"/>		49		

- **Global Configuration**
  - Timeout: Timeout is the number of seconds in the range 1–1000, to wait for a reply from a TACACS+ server before it is dead.
  - Deadtime: Deadtime, which can be set to a number between 0–1440 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 (zero) enables this feature, but only if more than one server has been configured.
  - Change Secret Key: Specify to change the secret key or not. When **Yes** is selected for the option, you can change the secret key up to 63 characters long, shared between the TACACS+ server and the switch.
- **Server Configuration**
  - Delete: To delete a TACACS+ server entry, check this box. The entry is deleted during the next Save.
  - Hostname: The IPv4/IPv6 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.
  - Change Secret Key: Specify to change the secret key or not. When the checkbox is checked, you can change the setting overrides the global key. Leaving it blank will use the global key.

## 4.10 Security Aggregation Configuration

The following sections describe the Security Aggregation configurations.

### 4.10.1 Aggregation Common Configuration

This page is used to configure the Aggregation hash mode. This mode applies to the whole network element.

Figure 4-57. Common Aggregation Configuration

**Hash Code Contributors**

Source MAC Address	<input checked="" type="checkbox"/>
Destination MAC Address	<input type="checkbox"/>
IP Address	<input checked="" type="checkbox"/>
TCP/UDP Port Number	<input checked="" type="checkbox"/>

- **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.

### 4.10.2 Aggregation Groups Configuration

This page is used to configure the aggregation groups.

Figure 4-58. Aggregation Group Configuration

Group ID	Port Members						Group Configuration		
	1	2	3	4	5	6	Mode	Revertive	Max Bundle
Normal	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	Disabled	<input checked="" type="checkbox"/>	6
1	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Disabled	<input type="checkbox"/>	6
2	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Disabled	<input type="checkbox"/>	6
3	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Disabled	<input type="checkbox"/>	6

Save Reset

- **Group ID:** Indicates the aggregation 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.
- **Mode:** This parameter determines the mode for the aggregation group.
  - Disabled: The group is disabled.
  - Static: The group operates in static aggregation mode.
  - LACP (Active): The group operates in LACP active aggregation mode. See IEEE 801.AX-2014, section 6.4.1 for details.
  - LACL (Passive): The group operates in LACP passive aggregation mode. See IEEE 801.AX-2014, section 6.4.1 for details.
- **Revertive:** This parameter only applies to LACP-enabled groups. It determines if the group will perform automatic link (re-)calculation when links with higher priority becomes available.
- **Max Bundle:** This parameter only applies to LACP-enabled groups. It determines the maximum number of active bundled LACP ports allowed in an aggregation.

### 4.10.3 Aggregation LACP Configuration

This page allows the user to inspect the current LACP port configurations, and possibly change them.

Figure 4-59. LACP System Configuration

System Priority 32768

LACP Port Configuration

Port	LACP	Timeout	Prio
*	<input type="checkbox"/>	Fast	32768
1	No	Fast	32768
2	No	Fast	32768
3	No	Fast	32768
4	No	Fast	32768
5	No	Fast	32768
6	No	Fast	32768

Save Reset

- **Port:** The switch port number.
- **LACP:** Show whether LACP is currently enabled on this switch port.
- **Timeout:** The Timeout controls the period between BPDU transmissions. Fast transmits LACP packets each second, while Slow waits for 30s before sending a LACP packet.
- **Prio:** Controls the priority of the port, range 1–65535. If the LACP partner wants to form a larger group that is supported by this device, then this parameter controls which ports are active and which ports are in a backup role. Lower number means greater priority.

## 4.11 Loop Protection Configuration

This page allows the user to inspect the current Loop Protection configurations, and possibly change them.

Figure 4-60. Loop Protection Configuration

Global Configuration			
Enable Loop Protection	Disable		
Transmission Time	5	seconds	
Shutdown Time	180	seconds	

Port Configuration			
Port	Enable	Action	Tx Mode
*	<input checked="" type="checkbox"/>	<>	<>
1	<input checked="" type="checkbox"/>	Shutdown Port	Enable
2	<input checked="" type="checkbox"/>	Shutdown Port	Enable
3	<input checked="" type="checkbox"/>	Shutdown Port	Enable
4	<input checked="" type="checkbox"/>	Shutdown Port	Enable
5	<input checked="" type="checkbox"/>	Shutdown Port	Enable
6	<input checked="" type="checkbox"/>	Shutdown Port	Enable

Save Reset

- **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 1s–10s. Default value is 5s.
  - **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 180s.
- **Port Configuration**
  - **Port:** The switch port number of the port.
  - **Enable:** Controls whether loop protection is enabled on this switch port or not.
  - **Action:** Configures the action performed when a loop is detected on a port. Following are the valid values:
    - 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 PDUs.

## 4.12 Spanning Tree Configuration

The following sections describe the Spanning Tree configurations.

### 4.12.1 Spanning Tree Bridge Settings Configuration

Spanning Tree Protocol (STP) and its Rapid Spanning Tree Protocol (RSTP) and Multiple Spanning Tree Protocol (MSTP) variations are used mainly for the following reasons:

- To prevent possible network loops, which cause broadcast storming without STP.
- To offer redundancy path from Switch to Switch or path to path over multiple switches by supporting network loops under the control of STP. The STP algorithm ensures that at any given time, only one path out of multiple possible loops is active, allowing the switch to use multiple backup paths if the main connection path go down.

Figure 4-61. STP Bridge Configuration

Basic Settings	
Protocol Version	MSTP
Bridge Priority	32768
Hello Time	2
Forward Delay	15
Max Age	20
Maximum Hop Count	20
Transmit Hold Count	6

Advanced Settings	
Edge Port BPDU Filtering	<input type="checkbox"/>
Edge Port BPDU Guard	<input type="checkbox"/>
Port Error Recovery	<input type="checkbox"/>
Port Error Recovery Timeout	

Save Reset

- **STP Bridge Configuration**

- Protocol Version: The following spanning tree protocols are supported:
  - MSTP
  - RSTP
  - STP
- Bridge Priority: Controls the bridge priority. Lower numeric values have better priority. The bridge priority plus the Multiple Spanning Tree Instance (MSTI) 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.
- 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 4s–30s.
- Max Age: The maximum age of the information transmitted by the Bridge when it is the Root Bridge. Valid values are in the range 6s–40s, and maximum age must be  $\leq (\text{FwdDelay}-1) * 2$ .
- 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 BPDUs a bridge port can send per second. When exceeded, transmission of the next BPDU is delayed. Valid values are in the range 1–10 BPDUs per second.

- **Advanced Settings**

- Edge Port BPDU Filtering: Control whether a port explicitly configured as Edge transmits and receives BPDUs.
- Edge Port BPDU Guard: Control whether a port explicitly configured as Edge disables itself upon reception of a BPDU. The port enters the error-disabled state and is removed from the active topology.
- Port Error Recovery: Control whether a port in the *error-disabled* state is automatically enabled after a certain time. If recovery is not enabled, ports must 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 30s–86400s (24 hours).

#### 4.12.2 Spanning Tree MSTI Mapping Configuration

This page allows you to inspect the current STP MSTI bridge instance priority configurations, and possibly change them.



Figure 4-62. MSTI Configuration

Add VLANs separated by spaces or comma.  
 Unmapped VLANs are mapped to the CIST. (The default bridge instance).

Configuration Identification

Configuration Name: 00-de-f3-ae-17-78  
 Configuration Revision: 0

MSTI Mapping

MSTI	VLANs Mapped
MSTI1	
MSTI2	
MSTI3	
MSTI4	
MSTI5	
MSTI6	
MSTI7	
TE	

Save Reset

- **Configuration Identification**
  - Configuration Name: The name identifying the VLAN to MSTI mapping. Bridges must share the name and revision (see the following, and the VLAN-to-MSTI mapping configuration to share spanning trees for MSTIs (Intra-region). The name is maximum 32 characters.
  - Configuration Revision: The revision of the MSTI configuration named above. This must be an integer between 0–65535.
- **MSTI Mapping**
  - MSTI: The bridge instance. The CIST is not available for explicit mapping, as it receives the VLANs not explicitly mapped.  
**Note:** The Traffic Engineering (TE) instance is special, as it is not controlled by MSTP itself. The TE instance always forwards for all ports. The TE-MSTID is defined by IEEE 802.1Q-2018.
  - VLANs Mapped: The list of VLANs mapped to the MSTI. The VLANs can be given as a single (xx, xx being between 1–4094) 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 must be left empty (that is, not having any VLANs mapped to it). For example, 2, 5, 20–40.

### 4.12.3 Spanning Tree MSTI Priorities Configuration

This page allows you to inspect the current STP MSTI bridge instance priority configurations, and possibly change them.

Figure 4-63. MSTI Priorities Configuration

MSTI Priority Configuration

MSTI	Priority
*	<>
CIST	32768
MSTI1	32768
MSTI2	32768
MSTI3	32768
MSTI4	32768
MSTI5	32768
MSTI6	32768
MSTI7	32768

Save Reset

- **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*.

### 4.12.4 Spanning Tree CIST Ports Configuration

This page allows you to inspect the current STP CIST port configurations and set physical and aggregated ports.

Figure 4-64. STP CIST Port Configuration

CIST Aggregated Port Configuration									
Port	STP Enabled	Path Cost	Priority	Admin Edge	Auto Edge	Restricted Role	TCN	BPDU Guard	Point-to-point
-	<input checked="" type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Forced True

CIST Normal Port Configuration									
Port	STP Enabled	Path Cost	Priority	Admin Edge	Auto Edge	Restricted Role	TCN	BPDU Guard	Point-to-point
*	<input checked="" type="checkbox"/>	<>	<>	<>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<>
1	<input checked="" type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
2	<input checked="" type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
3	<input checked="" type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
4	<input checked="" type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
5	<input checked="" type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
6	<input checked="" type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto

Save Reset

- **CIST Aggregated/Normal Port Configuration**

- **Port:** The switch port number of the logical STP port.
- **STP Enabled:** Controls whether STP is enabled on this switch port.
- **Path Cost:** Controls the path cost incurred by the port. The Auto setting sets 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 favor of higher path cost ports. Valid values are in the range of 1–200000000.
- **Priority:** Controls the port priority. This can be used to control priority of ports having identical port cost. Lower priority is better.
- **Admin Edge:** Controls if the operEdge flag must start as set or cleared (the initial operEdge state when a port is initialized).
- **Auto Edge:** Controls if the bridge must enable automatic edge detection on the bridge port. This allows operEdge to be derived from whether BPDUs are received on the port or not.
- **Restricted Role:** If enabled, this 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 is 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, it causes the port not to propagate received topology change notifications and topology changes to other ports. If set it can cause temporary loss of connectivity after changes in a spanning tree's active topology because 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, it causes the port to disable itself upon receiving valid BPDUs. Contrary to the similar bridge setting, the port Edge status does not affect 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.

#### 4.12.5 Spanning Tree MSTI Ports Configuration

This page allows you to inspect the current STP MSTI port configurations, and possibly change them. 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.

Figure 4-65. MST1 MSTI Port Configuration

MSTI Aggregated Ports Configuration		
Port	Path Cost	Priority
-	Auto	128

MSTI Normal Ports Configuration		
Port	Path Cost	Priority
*	<>	<>
1	Auto	128
2	Auto	128
3	Auto	128
4	Auto	128
5	Auto	128
6	Auto	128

Save Reset

- **Port:** The switch port number of the corresponding STP CIST (and MSTI) port.
- **Path Cost:** Controls the path cost incurred by the port. The Auto setting sets 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 favor of higher path cost ports. Valid values are in the range of 1–200000000.
- **Priority:** Controls the port priority. This can be used to control priority of ports having identical port cost. Lower priority is better.

## 4.13 LLDP Configuration

The following sections describe the LLDP configurations.

### 4.13.1 LLDP Configuration

This page allows you to inspect and configure the current LLDP interface settings.

Figure 4-66. LLDP Configuration

#### LLDP Configuration

##### LLDP Parameters

Tx Interval	30	seconds
Tx Hold	4	times
Tx Delay	2	seconds
Tx Reinit	2	seconds

##### LLDP Interface Configuration

Interface	Mode	CDP aware	Trap	Optional TLVs				
				Port Descr	Sys Name	Sys Descr	Sys Capa	Mgmt Addr
*	<>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
GigabitEthernet 1/1	Enabled	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
GigabitEthernet 1/2	Enabled	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
GigabitEthernet 1/3	Enabled	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
GigabitEthernet 1/4	Enabled	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
2.5GigabitEthernet 1/1	Enabled	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
2.5GigabitEthernet 1/2	Enabled	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Save Reset

- **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 (for example, 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  $\frac{1}{4}$  of the Tx Interval value. Valid values are restricted to 1:8192 seconds.
  - Tx Reinit: When an 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 is not valid anymore. Tx Reinit controls the number 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 does not send LLDP information but LLDP information from neighbor units is analyzed.
      - Tx Only: The switch drops LLDP information received from neighbors but sends LLDP information.
      - Disabled: The switch does not send LLDP information and drops LLDP information received from neighbors.
      - Enabled: The switch sends LLDP information and analyzes LLDP information received from neighbors.
    - CDP Aware: The CDP operation is restricted to decoding incoming CDP frames (the switch does not 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:

      - 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 is not removed immediately but gets removed when the hold time is exceeded.
- Port Desc: When checked the **port description** is included in LLDP information transmitted.
  - Sys Name: When checked the **system name** is included in LLDP information transmitted.
  - Sys Desc: When checked the **system description** is included in LLDP information transmitted.
  - Sys Capa: When checked the **system capability** is included in LLDP information transmitted.
  - Mgmt Addr: When checked the **management address** is included in LLDP information transmitted.

### 4.13.2 LLDP LLDP-MED Configuration

This page allows you to configure the LLDP-MED. This function applies to VoIP devices which support LLDP-MED.

Figure 4-67. LLDP-MED Configuration

LLDP-MED Configuration

Fast Start Repeat Count

Fast start repeat count

LLDP-MED Interface Configuration

Interface	Transmit TLVs				Device Type
	Capabilities	Policies	Location	PoE	
GigabitEthernet 1/1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<>
GigabitEthernet 1/2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Connectivity
GigabitEthernet 1/3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Connectivity
GigabitEthernet 1/4	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Connectivity
2.5GigabitEthernet 1/1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Connectivity
2.5GigabitEthernet 1/2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Connectivity

Coordinates Location

Latitude  ° North Longitude  ° East Altitude  Meters Map Datum WGS84

Civic Address Location

Country code		State		County	
City		City district		Block (Neighborhood)	
Street		Leading street direction		Trailing street suffix	
Street suffix		House no.		House no. suffix	
Landmark		Additional location info		Name	
Zip code		Building		Apartment	
Floor		Room no.		Place type	
Postal community name		P.O. Box		Additional code	

Emergency Call Service

Emergency Call Service

Policies

Delete	Policy ID	Application Type	Tag	VLAN ID	L2 Priority	DSCP
No entries present						

Add New Policy

Save Reset

- **Fast start repeat count:** Rapid startup and Emergency Call Service Location Identification Discovery of endpoints is a critically important aspect of VoIP systems in general. In addition, it is best to advertise only those pieces of information which are specifically relevant to particular endpoint types (for example, only advertise the voice network policy to permitted voice-capable devices), to conserve the limited LLDPDU space and to reduce security and system integrity issues that can come with inappropriate knowledge of the network policy.

Therefore, LLDP-MED defines an LLDP-MED Fast Start interaction between the protocol and the application layers on top of the protocol, to achieve these related properties. Initially, a Network Connectivity Device only transmits LLDP TLVs in an LLDPDU. Only after an LLDP-MED Endpoint Device is detected, an LLDP-MED capable Network Connectivity Device starts to advertise LLDP-MED TLVs in outgoing LLDPDUs on the associated interface. The LLDP-MED application temporarily speeds up the transmission of the LLDPDU to start within a second, when a new LLDP-MED neighbor has been detected to share LLDP-MED information as fast as possible to new neighbors.

As there is a risk of an LLDP frame being lost during transmission between neighbors, it is recommended to repeat the fast start transmission multiple times to increase the possibility of the neighbors receiving the LLDP frame. With **Fast start repeat count**, it is possible to specify the number of times the fast start transmission is repeated. The recommended value is four times, given that four LLDP frames with a 1 second interval are transmitted, when an LLDP frame with new information is received.

**Note:** LLDP-MED and the LLDP-MED Fast Start mechanism is only intended to run on links between LLDP-MED Network Connectivity Devices and Endpoint Devices and does not apply to links between LAN infrastructure elements, including Network Connectivity Devices or other types of links.

- **LLDP-MED Interface Configuration**

- Interface: The interface name to which the configuration applies.
- Transmit TLVs Capabilities: When checked, the switch's capabilities are included in LLDP-MED information transmitted.
- Transmit TLVs Policies: When checked, the configured policies for the interface are included in LLDP-MED information transmitted.
- Transmit TLVs Location: When checked, the configured location information for the switch is included in LLDP-MED information transmitted.
- Transmit TLVs PoE: When checked, the configured PoE information for the interface is included in LLDP-MED information transmitted.
- Device Type: Any LLDP-MED Device is operating as a specific type of LLDP-MED Device, which may be either a Network Connectivity Device or a specific Class of Endpoint Device. A Network Connectivity Device is a LLDP-MED Device that provides access to the IEEE 802 based LAN infrastructure for LLDP-MED Endpoint Devices. An LLDP-MED Network Connectivity Device is a LAN access device based on any of the following technologies:
  - LAN Switch/Router
  - IEEE 802.1 Bridge
  - IEEE 802.3 Repeater (included for historical reasons)
  - IEEE 802.11 Wireless Access Point

Any device that supports the IEEE 802.1AB and MED extensions that can relay IEEE 802 frames via any method.

An Endpoint Device a LLDP-MED Device that sits at the network edge and provides some aspect of IP communications service, based on IEEE 802 LAN technology.

The main difference between a Network Connectivity Device and an Endpoint Device is that only an Endpoint Device can start the LLDP-MED information exchange.

Even though a switch must always be a Network Connectivity Device, it is possible to configure it to act as an Endpoint Device and thereby start the LLDP-MED information exchange (when two Network Connectivity Devices are connected).

- **Coordinates Location**

- Latitude: Latitude must be normalized to within 0–90 degrees with a maximum of four digits. It is possible to specify the direction to either **North** of the equator or **South** of the equator.
- Longitude: Longitude must be normalized to within 0–180 degrees with a maximum of four digits. It is possible to specify the direction to either **East** of the prime meridian or **West** of the prime meridian
- Altitude: Altitude must be normalized to within –2097151.9 to 2097151.9 with a maximum of 1 digit. It is possible to select between two altitude types (floors or meters).
  - Meters: Representing meters of Altitude defined by the vertical datum specified.
  - Floors: Representing altitude in a form more relevant in buildings which have different floor-to-floor dimensions. An altitude = 0.0 is meaningful even outside a building and represents ground level at the given latitude and longitude. Inside a building, 0.0 represents the floor level associated with ground level at the main entrance.
- Map Datum: The Map Datum is used for the coordinates given in these options:
  - WGS84 (Geographical 3D): World Geodesic System 1984, CRS Code 4327, Prime Meridian Name: Greenwich.
  - NAD83/NAVD88: North American Datum 1983, CRS Code 4269, Prime Meridian Name: Greenwich. The associated vertical datum is the North American Vertical Datum of 1988 (NAVD88). This datum pair is to be used when referencing locations on land, not near tidal water (which uses Datum = NAD83/MLLW).
  - NAD83/MLLW: North American Datum 1983, CRS Code 4269, Prime Meridian Name: Greenwich. The associated vertical datum is Mean Lower Low Water (MLLW). This datum pair is to be used when referencing locations on water/sea/ocean.
- Civic Address Location: IETF Geopriv Civic Address based Location Configuration Information (Civic Address LCI). The total number of characters for the combined civic address information must not exceed 250 characters. A couple of notes to the limitation of 250 characters.

If more than one civic address location is used, each of the additional civic address locations uses two extra characters in addition to the civic address location text.

The two-letter country code is not part of the 250 characters limitation.

- Country code: The two-letter ISO 3166 country code in capital ASCII letters. For example, DK, DE, or US.
- State: National subdivisions (state, canton, region, province, prefecture).
- Country: County, parish, gun (Japan), district.
- City: City, township, shi (Japan). For example, Copenhagen.
- City district: City division, borough, city district, ward, chou (Japan).
- Block: Neighborhood, block.
- Street: Street. For example, Poppelvej.
- Leading street direction: Street. For example, Poppelvej.
- Trailing street suffix: Trailing street suffix. For example, SW.
- Street suffix: Street suffix. For example, Ave, Platz.
- House no.: House number. For example, 21.
- House no. suffix: House number suffix. For example, A, 1/2.
- Landmark: Landmark or vanity address. For example, Columbia University.
- Additional location info: Additional location information. For example, South Wing.
- Name: Name (residence and office occupant). For example, Flemming Jahn.
- Zip code: Postal/zip code. For example, 2791.
- Building: Building (structure). For example, Low Library.
- Apartment: Unit (Apartment, suite). For example, Apt 42.
- Floor: Floor. For example, 4.
- Room no.: Room number. For example, 450F.
- Place type: Place type. For example, Office.
- Postal community name: Postal community name. For example, Leonia.
- P.O. Box: Post office box (P.O. BOX). For example, 12345.
- Additional Code: Additional code. For example, 1320300003.
- Emergency Call Services: For example, E911 and so on, as defined by TIA or NENA.
  - Emergency Call Service: ELIN identifier data format is defined to carry the ELIN identifier as used during emergency call setup to a traditional CAMA or ISDN trunk-based PSAP. This format consists of a numerical digit string, corresponding to the ELIN to be used for emergency calling.

Network Policy Discovery enables the efficient discovery and diagnosis of mismatch issues with the VLAN configuration, along with the associated Layer 2 and Layer 3 attributes, which apply for a set of specific protocol applications on that port. Improper network policy configurations are a very significant issue in VoIP environments that frequently result in voice quality degradation or loss of service.

Policies are only intended for use with applications that have specific real-time network policy requirements, such as interactive voice and/or video services. The network policy attributes advertised are:

- Layer 2 VLAN ID (IEEE 802.1Q-2003)
- Layer 2 priority value (IEEE 802.1D-2004)
- Layer 3 Diffserv code point (DSCP) value (IETF RFC 2474)

This network policy is potentially advertised and associated with multiple sets of application types supported on a given port. The application types specifically addressed are:

- i. Voice
- ii. Guest Voice
- iii. Softphone Voice
- iv. Video Conferencing
- v. Streaming Video
- vi. Control/Signaling (conditionally support a separate network policy for the media types above).



A large network may support multiple VoIP policies across the entire organization, and different policies per application type. LLDP-MED allows multiple policies to be advertised per port, each corresponding to a different application type. Different ports on the same Network Connectivity Device may advertise different sets of policies, based on the authenticated user identity or port configuration.

**Note:** LLDP-MED is not intended to run on links other than between Network Connectivity Devices and Endpoints, and therefore does not need to advertise the multitude of network policies that frequently run on an aggregated link interior to the LAN.

- Delete: Check to delete the policy. It will be deleted during the next save.
- Policy ID: ID for the policy. This is auto generated and shall be used when selecting the policies that shall be mapped to the specific interfaces.
- Application Type: Following are the uses of the application types:
  - Voice: For use by dedicated IP Telephony handsets and other similar appliances supporting interactive voice services. These devices are typically deployed on a separate VLAN for ease of deployment and enhanced security by isolation from data applications.
  - Voice Signaling (conditional): For use in network topologies that require a different policy for the voice signaling than for the voice media. This application type must not be advertised if all the same network policies apply as those advertised in the **Voice** application policy.
  - Guest Voice: Support a separate **limited feature-set** voice service for guest users and visitors with their own IP Telephony handsets and other similar appliances supporting interactive voice services.
  - Guest Voice Signaling (conditional): For use in network topologies that require a different policy for the guest voice signaling than for the guest voice media. This application type must not be advertised if all the same network policies apply as those advertised in the **Guest Voice** application policy.
  - Softphone Voice: For use by softphone applications on typical data centric devices, such as PCs or laptops. This class of endpoints frequently does not support multiple VLANs, if at all, and are typically configured to use an untagged VLAN or a single tagged data specific VLAN. When a network policy is defined for use with an untagged VLAN (see [Tagged flag](#)), then the L2 priority field is ignored and only the DSCP value has relevance.
  - Video Conferencing: For use by dedicated Video Conferencing equipment and other similar appliances supporting real-time interactive video/audio services.
  - Streaming Video: For use by broadcast or multicast-based on content distribution and other similar applications supporting streaming video services that require specific network policy treatment. Video applications relying on TCP with buffering would not be an intended use of this application type.
  - Video Signaling (conditional): For use in network topologies that require a separate policy for the video signaling than for the video media. This application type should not be advertised if all the same network policies apply as those advertised in the **Video Conferencing** application policy.
- Tag: Tag indicates if the specified application type is using a tagged or an untagged VLAN.
  - Untagged: Indicates that the device is using an untagged frame format and as such does not include a tag header as defined by IEEE 802.1Q-2003. In this case, both the VLAN ID and the Layer 2 priority fields are ignored and only the DSCP value has relevance.
  - Tagged: Indicates that the device is using the IEEE 802.1Q tagged frame format, and that both the VLAN ID and the Layer 2 priority values are being used, as well as the DSCP value. The tagged format includes an additional field, known as the tag header. The tagged frame format also includes priority tagged frames as defined by IEEE 802.1Q-2003.
- VLAN ID: VLAN Identifier (VID) for the interface, as defined in IEEE 802.1Q-2003.
- L2 Priority: L2 Priority is the Layer 2 priority to be used for the specified application type. **L2 Priority** may specify one of eight priority levels (0–7), as defined by IEEE 802.1D-2004. A value of 0 represents use of the default priority as defined in IEEE 802.1D-2004.
- **DSCP**: DSCP value is used to provide Diffserv node behavior for the specified application type as defined in IETF RFC 2474. **DSCP** may contain one of 64 code point values (0–63). A value of 0 represents use of the default DSCP value as defined in RFC 2475.
- **Policies Interface Configuration:** Every interface may advertise a unique set of network policies or different attributes for the same network policies, based on the authenticated user identity or interface configuration.
  - Interface: The interface name to which the configuration applies.

- Policy ID: The set of policies that shall apply to a given interface. The set of policies is selected by check marking the checkboxes that corresponds to the policies.

## 4.14 PoE Configuration

This page allows you to inspect and configure the current PoE port settings.

Figure 4-68. PoE Configuration

Power over Ethernet Configuration

System Configuration

Power supply	152	W
Interruptible power	Disabled ▾	
PD Auto-class request	Disabled ▾	
Legacy PD-Class Mode	Standard ▾	

**Note:**  
 - Legacy PD-Class Mode (standard / PoH / Ignore Pd-Class) configuration is applicable only to PoE ports configured as 'Plus' under the mode column.  
 - Legacy PD-Class Mode - 'Ignore Pd-Class' is applicable only for ports configured as Type3-60W, Type4-90W. Excluding Type3-15W, Type3-30W.

Port Configuration

Port	Type	Mode	Pwr Mng	Priority	LLDP	Cable Length
*	<> ▾	<> ▾	<> ▾	<> ▾	<> ▾	<> ▾
1	type4-90w ▾	plus ▾	dynamic ▾	low ▾	disable ▾	max-100 ▾
2	type4-90w ▾	plus ▾	dynamic ▾	low ▾	disable ▾	max-100 ▾
3	type4-90w ▾	plus ▾	dynamic ▾	low ▾	disable ▾	max-100 ▾
4	type4-90w ▾	plus ▾	dynamic ▾	low ▾	disable ▾	max-100 ▾

Save Reset

- **System Configuration**

- Power Supply: Report power supply maximum power capabilities.
- Interruptible power: Controls if PoE power should be interrupted (shut down for 5s) during unit software restart cycle or remain unchanged during the unit software restart cycle.
  - Disabled: PoE power remains unchanged during the entire unit software restart cycle.
  - Enabled: PoE power to already powered PD devices is turned OFF for 5s during unit software restart cycle.
- PD Auto-class request: PD Auto-class request is part of PoE IEEE 802.3bt in which the PD communicates its effective maximum power consumption to the PSE. The PoE port is to set its maximum allocated power in accordance with the maximum power consumed by the PD during the PD auto-class request negotiation cycle, instead the PD Class 0–8.

For example, a PD of type class-6 (60W) supporting PD Auto-Class request, may advertise through the PD Auto-Class request hardware handshake negotiation algorithm that it requires only 17W. As a result, PoE limits port maximum power to 17W although the PD is from type class-6 (60W).

- Disabled: PoE maximum power is determined based on PD class regardless of the PD advertising that it supports PD Auto-class.
- Enabled: PoE maximum power is determined based on the maximum power consumed by the PD during the PD auto-class request negotiation cycle.
- Legacy PD-Class Mode: Legacy PD-Class Mode (standard/PoH/Ignore Pd-Class) configuration is applicable only to PoE ports configured as Plus-Mode and is ignored for PoE ports configured as standard mode.
  - Standard: Extend PD detection resistance/capacitance range beyond IEEE 802.3bt specification. Power-Demotion, which means that PD is allocated power from a PSE that is lower than what the PD requested, is supported.
  - PoH: Same as Standard-Mode except for PoE-AT PDs advertising class 4, 4 (DSPD) or class 4 (SSPD). PoE-AT DSPD class 4, 4 is offered 90W (instead of 60W). PoE-AT SSPD class 4 is offered 45W (instead of 30W). No support for Power-Demotion.

**Note:** PoE-BT class 4, 4 PD is offered 60W, and PoE-BT SSPD class 4 is offered 30W.

- Ignore Pd-Class:
  - Port configured as Type4-90W is limited to 90W (DSPD) or 45W (SSPD) regardless of PD advertised class. No support for Power-Demotion.
  - Port configured as Type3-60W is limited to 60W (DSPD) or 30W (SSPD) regardless of PD advertised class. No support for Power-Demotion.
  - Port configured as Type3-30W/Type3-15W perform as if it is configured in Standard-Mode.
- **Port Configuration**
  - Port: Switch port number. Only PoE-capable ports are shown.
  - Type: Configure the maximum power the PoE port can deliver to the PD before shutting it down. Power demotion is however supported, and therefore a lower power may in effect be provided.
 

PoE Power demotion example: A PD advertise itself as class-8 90W, while the PoE port is either configured to Type3-60W offering up to class-6 60W, or due to limited free available power the PoE port is only allowed to offer up to class-6 60W. In either of these scenarios, the switch demotes the PD to class-6 60W. It is up to the PD to decide if to accept the 60W offer.

    - Type4-90W: PoE maximum power is limited to 90W/45W (four-pair/two-pair).
    - Type3-60W: PoE maximum power is limited to 60W/30W (four-pair/two-pair).
    - Type3-30W: PoE maximum power is limited to 30W.
    - Type3-15W: PoE maximum power is limited to 15W.
  - Mode: Configure PoE port to one of the following options.
    - Disabled: PoE port is disabled. Port becomes a non-PoE switch Ethernet port.
    - Standard: PoE port is enabled and compliant with IEEE 802.3bt specification.
    - Plus: PoE port is enabled and supports non-IEEE-802.3-af/at/bt PoE PDs.
  - Power Management Mode: Configure the method used for calculating the free available power for additional PDs. Whenever PoE LLDP is enabled, PoE port maximum power is determined by remote PD Power-Request over LLDP regardless to the Power Management mode.
    - Dynamic: Deduct from the free available power the actual PD power consumption, ignoring PD class.
    - Static: Use PD class to deduct from the free available power (SSPD class-8 = 90W, class7 = 75W, SSPD class-6 = 60W, and so on. DSPS class-5,5 = 90W, DSPD class 4,4 = 60W, and so on), considering power demotion, while ignoring actual PD power consumption. For PDs transmitting **Power Over-MDI** TLV in LLDP packet, free available power is deducted by the PD LLDP power-request value plus cable length power loss.
    - Hybrid: Mixture of dynamic and static power management. Any PoE port configured as Hybrid act as if it is configured to the dynamic mode unless it has negotiated a maximum power consumption over LLDP. A port that negotiates a successful maximum PoE power over LLDP is switched automatically to the static mode limited to the negotiated power.
  - Priority: PoE port priority controls the order of the PoE ports during Power-On sequence and during Power-Off sequence when overall power consumption exceeds the maximum available power. All ports configured as Critical are turned ON first, followed by all ports configured as High, and lastly all ports configured as Low. For all ports of the same priority, the lowest PoE switch port number is turned ON first, followed by the next highest PoE switch port number. For example, if all ports are set to priority-Low, then port #1 is turned ON first, followed by port #2, and so on. The highest PoE switch port number is the first port to be turned OFF when the overall power consumption exceeds the maximum available power, again in accordance with PoE port number, while giving priority to Critical over High and High over Low.
    - Critical: Highest level PoE port priority
    - High: Mid-level PoE port priority
    - Low: Lowest level PoE port priority
  - LLDP: The LLDP configures the PoE port behavior with respect to LLDP packets from PD.
    - Enable: Parameters as PD power-request received through LLDP are processed.
    - Disable: Parameters received through LLDP are ignored.
 

LLDP protocol is configured by its own configuration web page and transmission of PoE information through LLDP can be configured with the LLDP-MED configuration page.
  - Cable Length: Cable length assist port power optimization allocation to remote PD advertising their power requirement over LLDP. Cable power loss for PD Type4 requesting 71.3W is assumed to be 18.7W for

100m cable length. Therefore, port maximum power is set to 90W. However, if PD is located only 30m away then port maximum power can be lowered to 76W, freeing 14W for other PDs.

- max-10: Ethernet cable length is 10m or less.
- max-30: Ethernet cable length is 30m or less.
- max-60: Ethernet cable length is 60m or less.
- max-100: Ethernet cable length is 100m or less.

## 4.15 MAC Table Configuration

The MAC Address Table is configured on this page. Here, you can set timeouts for entries in the dynamic MAC table and configure the static MAC table.

Figure 4-69. MAC Address Table Configuration

- **Aging Configuration:** By default, dynamic entries are removed from the MAC table after 300s. This removal is also called aging. Configure aging time by entering a value here in seconds. The allowed range is 10s–1000000s.
- **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.

**Note:** Ensure 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 through the serial interface.
- **VLAN Learning Configuration:** This field shows the Learning-disabled VLANs. When a NEW MAC arrives at a learning-disabled VLAN, the MAC is not learnt. By default, the field is empty. More VLANs may be created by using a list syntax where the individual elements are separated by commas. Ranges are specified with a dash separating the lower and upper bound. The following example creates VLANs 1, 10, 11, 12, 13, 200, and 300: 1, 10-13, 200, 300. Spaces are allowed in between the delimiters.
- **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.

## 4.16 VLAN Configurations

The following sections describe the VLAN Configurations.

### 4.16.1 Controlling VLAN Configuration

This page allows for controlling VLAN configuration on the switch. The page is divided into a global section and a per-port configuration section.

Figure 4-70. Global VLAN Configuration

Global VLAN Configuration

Allowed Access VLANs	1
Ethertype for Custom S-ports	88A8

Port VLAN Configuration

Port	Mode	Port VLAN	Port Type	Ingress Filtering	Ingress Acceptance	Egress Tagging	Allowed VLANs	Forbidden VLANs
*	<>	1	<>	<input checked="" type="checkbox"/>	<>	<>	1	
1	Access	1	C-Port	<input type="checkbox"/>	Tagged and Untagged	Untag All	1	
2	Access	1	C-Port	<input type="checkbox"/>	Tagged and Untagged	Untag All	1	
3	Access	1	C-Port	<input type="checkbox"/>	Tagged and Untagged	Untag All	1	
4	Access	1	C-Port	<input type="checkbox"/>	Tagged and Untagged	Untag All	1	
5	Access	1	C-Port	<input type="checkbox"/>	Tagged and Untagged	Untag All	1	
6	Access	1	C-Port	<input type="checkbox"/>	Tagged and Untagged	Untag All	1	

Save Reset

- **Global VLAN Configuration**

- Allowed Access VLANs: This field shows the allowed Access VLANs, that is, it only affects ports configured as Access ports. Ports in other modes are members of the VLANs specified in the Allowed VLANs field. By default, only VLAN 1 is enabled. More VLANs may be created by using a list syntax where the individual elements are separated by commas. Ranges are specified with a dash separating the lower and upper bound.

The following example creates VLANs 1, 10, 11, 12, 13, 200, and 300: 1, 10-13, 200, 300. Spaces are allowed in between the delimiters.

- Ethertype for Custom S-ports: This field specifies the Ethertype/TPID (specified in hexadecimal) used for Custom S-ports. The setting is in force for all ports whose Port Type is set to S-Custom-Port.

- **Port VLAN Configuration**

- Port: This is the logical port number of this row.
- Mode: The port mode (default is Access) determines the fundamental behavior of the port in question. A port can be in one of three modes, as described in the following list. When a particular mode is selected, the remaining fields in that row are either grayed out or made changeable depending on the mode in question. Grayed out fields show the value that the port gets when the mode is applied.
  - Access: Access ports are normally used to connect to end stations. Dynamic features like Voice VLAN may add the port to more VLANs behind the scenes. Access ports have the following characteristics:
    - Member of exactly one VLAN, the Port VLAN (Access VLAN), which by default is 1.
    - Accepts untagged and C-tagged frames.
    - Discards all frames not classified to the Access VLAN.
    - On egress all frames are transmitted untagged.
  - Trunk: Trunk ports can carry traffic on multiple VLANs simultaneously and are normally used to connect to other switches. Trunk ports have the following characteristics:
    - By default, a trunk port is member of all VLANs (1–4095).
    - The VLANs that a trunk port is member of may be limited because of Allowed VLANs.

- Frames classified to a VLAN that the port is not a member of are discarded.
- By default, all frames but frames classified to the Port VLAN (that is, Native VLAN) get tagged on egress. Frames classified to the Port VLAN do not get C-tagged on egress.
- Egress tagging can be changed to tag all frames, in which case only tagged frames are accepted on ingress.
- Hybrid: Hybrid ports resemble trunk ports in many ways but adds additional port configuration features. In addition to the characteristics described for trunk ports, hybrid ports have these abilities:
  - Can be configured to be VLAN tag unaware, C-tag aware, S-tag aware, or S-custom-tag aware.
  - Ingress filtering can be controlled.
  - Ingress acceptance of frames and configuration of egress tagging can be configured independently.
- Port VLAN: Determines the port's VLAN ID (PVID). Allowed VLANs are in the range 1 through 4095, default being 1. On ingress, frames get classified to the Port VLAN if the port is configured as VLAN unaware, the frame is untagged, or VLAN awareness is enabled on the port, but the frame is priority tagged (VLAN ID = 0).

On egress, frames classified to the Port VLAN do not get tagged if Egress Tagging configuration is set to untag Port VLAN. The Port VLAN is called an **Access VLAN** for ports in Access mode and Native VLAN for ports in Trunk or Hybrid mode.
- Port Type: Ports in hybrid mode allow for changing the port type, that is, whether a frame's VLAN tag is used to classify the frame on ingress to a particular VLAN, and if so, which TPID it reacts on. Likewise, on egress, the Port Type determines the TPID of the tag, if a tag is required.
  - Unaware: On ingress, all frames, whether carrying a VLAN tag or not, get classified to the Port VLAN, and possible tags are not removed on egress.
  - C-Port: On ingress, frames with a VLAN tag with TPID = 0x8100 get classified to the VLAN ID embedded in the tag. If a frame is untagged or priority tagged, the frame gets classified to the Port VLAN. If frames must be tagged on egress, they will be tagged with a C-tag.
  - S-Port: On egress, if frames must be tagged, they will be tagged with an S-tag. On ingress, frames with a VLAN tag with TPID = 0x88A8 get classified to the VLAN ID embedded in the tag. Priority-tagged frames are classified to the Port VLAN. If the port is configured to accept Tagged Only frames (see [Ingress Acceptance](#)), frames without this TPID are dropped.

**Note:** If the S-port is configured to accept Tagged and Untagged frames (see [Ingress Acceptance](#)), frames with a C-tag are treated like frames with an S-tag.

If the S-port is configured to accept Untagged Only frames, S-tagged frames will be discarded (except for priority S-tagged frames). C-tagged frames are initially considered untagged and will therefore not be discarded. Later in the ingress classification process, they will get classified to the VLAN embedded in the tag instead of the port VLAN ID.
  - S-Custom-Port: On egress, if frames must be tagged, they will be tagged with the custom S-tag. On ingress, frames with a VLAN tag with a TPID equal to the Ethertype configured for Custom-S ports get classified to the VLAN ID embedded in the tag. Priority-tagged frames are classified to the Port VLAN. If the port is configured to accept Tagged Only frames (see [Ingress Acceptance](#)), frames without this TPID are dropped.

**Note:** If the custom S-port is configured to accept Tagged and Untagged frames (see [Ingress Acceptance](#)), frames with a C-tag are treated like frames with a custom S-tag.

If the Custom S-port is configured to accept Untagged Only frames, custom S-tagged frames will be discarded (except for priority custom S-tagged frames). C-tagged frames are initially considered untagged, and therefore, cannot be discarded. Later, in the ingress classification process, they are classified to the VLAN embedded in the tag instead of the port VLAN ID.
- Ingress Filtering: Hybrid ports allow for changing ingress filtering. Access and Trunk ports always have ingress filtering enabled. If ingress filtering is enabled (checkbox is checked), frames classified to a VLAN that the port is not a member of get discarded. If ingress filtering is disabled, frames classified to a VLAN that the port is not a member of are accepted and forwarded to the switch engine. However, the port never transmits frames classified to VLANs that it is not a member of.
- Ingress Acceptance: Hybrid ports allow for changing the type of frames that are accepted on ingress.



- Tagged and Untagged: Both tagged and untagged frames are accepted. See Port Type for a description of when a frame is considered tagged.
- Tagged Only: Only frames tagged with the corresponding Port Type tag is accepted on ingress.
- Untagged Only: Only untagged frames are accepted on ingress. See Port Type for a description of when a frame is considered untagged.
- Egress Tagging: Ports in Trunk and Hybrid mode may control the tagging of frames on egress.
  - Untag Port VLAN: Frames classified to the Port VLAN are transmitted untagged. Other frames are transmitted with the relevant tag.
  - Tag All: All frames, whether classified to the Port VLAN or not, are transmitted with a tag.
  - Untag All: All frames, whether classified to the Port VLAN or not, are transmitted without a tag. This option is only available for ports in Hybrid mode.
- Allowed VLANs: Ports in Trunk and Hybrid mode may control which VLANs they are allowed to become members of. Access ports can only be member of one VLAN, the Access VLAN. The field's syntax is identical to the syntax used in the Enabled VLANs field. By default, a Trunk or Hybrid port becomes member of all VLANs and is set to 1–4095. The field may be left empty, which means that the port does not become member of any VLANs.
- Forbidden VLANs: A port may be configured to never become member of one or more VLANs. This is particularly useful when dynamic VLAN protocols like MVRP and GVRP must be prevented from dynamically adding ports to VLANs. The trick is to mark such VLANs as forbidden on the port in question. The syntax is identical to the syntax used in the Enabled VLANs field. By default, the field is left blank, which means that the port may become a member of all possible VLANs.

#### 4.16.2 VLANs SVL (Shared VLAN Learning Configuration) Configuration

This page allows for controlling SVL configuration on the switch. In SVL, one or more VLANs map to a Filter ID (FID). By default, there is a one-to-one mapping from VLAN to FID, in which case the switch acts as an IVL bridge, but with SVL multiple VLANs may share the same MAC address table entries.

Figure 4-71. Shared VLAN Learning Configuration

Delete	FID	VLANs
Delete	1	

Add FID

Save Reset

- **Delete:** A previously allocated FID can be deleted using button.
- **FID:** FID is the ID that VLANs get learned on in the MAC table when SVL is in effect. No two rows in the table can have the same FID and the FID must be a number between 1–63.
- **VLANs:** List of VLANs is mapped into FID. The syntax is as follows: Individual VLANs are separated by commas. Ranges are specified with a dash separating the lower and upper bound. The following example maps VLANs 1, 10, 11, 12, 13, 200, and 300: 1, 10-13, 200, 300. Spaces are allowed in between the delimiters. The range of valid VLANs is 1–4095. The same VLAN can only be a member of one FID. A message is displayed if one VLAN is grouped into two or more FIDs. All VLANs must map to a particular FID, and by default VLAN x maps to FID x. This implies that if FID x is defined, then VLAN x is implicitly a member of FID x unless it is specified for another FID. If FID x does not exist, a confirmation message is displayed, asking whether to continue adding VLAN x implicitly to FID x.

### 4.17 QoS Configuration

The following sections describe the QoS configurations.

#### 4.17.1 QoS Port Classification Configuration

This page allows you to configure the basic QoS Classification settings for all switch ports.



Figure 4-72. QoS Port Classification

Port	Ingress							
	CoS	DPL	PCP	DEI	Tag Class.	DSCP Based	Key Type	Address Mode
*	<>	<>	<>	<>		<input type="checkbox"/>	<>	<>
1	0	0	0	0	Disabled	<input type="checkbox"/>	Normal	Source
2	0	0	0	0	Disabled	<input type="checkbox"/>	Normal	Source
3	0	0	0	0	Disabled	<input type="checkbox"/>	Normal	Source
4	0	0	0	0	Disabled	<input type="checkbox"/>	Normal	Source
5	0	0	0	0	Disabled	<input type="checkbox"/>	Normal	Source
6	0	0	0	0	Disabled	<input type="checkbox"/>	Normal	Source

Save Reset

- **Port:** The port number for which the configuration below applies.
- **CoS:** Controls the default CoS value. 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 DPL value. 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:** Shows the classification mode for 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 to configure the mode and/or mapping.  
**Note:** This setting has no effect if the port is VLAN unaware. 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.
- **Key Type:** The key type specifying the key generated for frames received on the port. The allowed values are:
  - Normal: Half key, match outer tag, SIP/DIP and SMAC/DMAC.
  - Double Tag: Quarter key, match inner and outer tag.
  - IP Address: Half key, match inner and outer tag, SIP and DIP. For non-IP frames, match outer tag only.
  - MAC and IP Address: Full key, match inner and outer tag, SMAC, DMAC, SIP and DIP. Filtering on DMAC type (unicast/multicast/broadcast) is supported for any key type.
- **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. This parameter is only used when the key type is Normal. The allowed values are:
  - Source: Enable SMAC/SIP matching.
  - Destination: Enable DMAC/DIP matching.

#### 4.17.2 QoS Port Policing Configuration

This page allows you to configure the Policer settings for all switch ports.

Figure 4-73. QoS Ingress Port Policer

Port	Enable	Rate	Unit	Flow Control
*	<input type="checkbox"/>	500	<> v	<input type="checkbox"/>
1	<input type="checkbox"/>	500	kbps v	<input type="checkbox"/>
2	<input type="checkbox"/>	500	kbps v	<input type="checkbox"/>
3	<input type="checkbox"/>	500	kbps v	<input type="checkbox"/>
4	<input type="checkbox"/>	500	kbps v	<input type="checkbox"/>
5	<input type="checkbox"/>	500	kbps v	<input type="checkbox"/>
6	<input type="checkbox"/>	500	kbps v	<input type="checkbox"/>

Save Reset

- **Port:** The port number for which the following configuration 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 the unit is kbps or fps, and 1–3276 when the 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 the Flow Control mode, then pause frames are sent instead of discarding frames.

### 4.17.3 QoS Queue Policing Configuration

This page allows you to configure the Queue Policer settings for all switch ports.

Figure 4-74. QoS Ingress Queue Policers

Port	Queue 0	Queue 1	Queue 2	Queue 3	Queue 4	Queue 5	Queue 6	Queue 7
	Enable	Enable	Enable	Enable	Enable	Enable	Enable	Enable
*	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Save Reset

- **Port:** The port number for which the following configuration applies.
- **Enable:** Enable or disable the queue policer for this switch port.

### 4.17.4 QoS Port Scheduler Configuration

This page provides an overview of QoS Egress Port Schedulers for all switch ports.

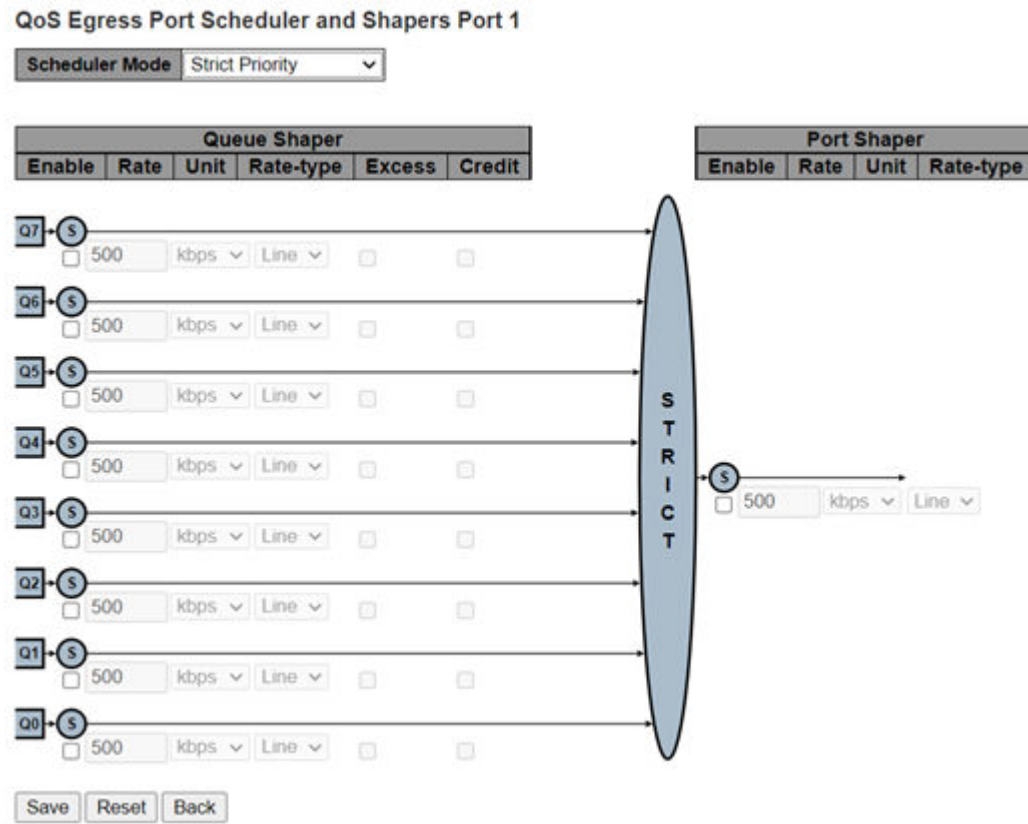
Figure 4-75. QoS Egress Port Scheduler

Port	Mode	Weight							
		Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7
1	Strict Priority	-	-	-	-	-	-	-	-
2	Strict Priority	-	-	-	-	-	-	-	-
3	Strict Priority	-	-	-	-	-	-	-	-
4	Strict Priority	-	-	-	-	-	-	-	-
5	Strict Priority	-	-	-	-	-	-	-	-
6	Strict Priority	-	-	-	-	-	-	-	-

- **Port:** The logical port for the settings contained in the same row. Click on the port number to configure the schedulers.
- **Mode:** Shows the scheduling mode for this port.
- **Qn:** Shows the weight for this queue and port.

Selecting port number opens the following web page that allows you to configure the Scheduler and Shapers for a specific port.

Figure 4-76. QoS Egress Port Scheduler and Shapers Port-X



- **Scheduler Mode:** Controls how many of the queues are scheduled as strict and how many are scheduled as weighted on this switch port.
- **Queue Shaper Enable:** Controls whether the queue shaper is enabled for this queue on this switch port.
- **Queue Shaper Rate:** Controls the rate for the queue shaper. This value is restricted to 100-3281943 when the unit is kbps, and 1–3281 when the unit is Mbps. The rate is internally rounded up to the nearest value supported by the queue shaper.
- **Queue Shaper Unit:** Controls the unit of measure for the queue shaper rate as kbps or Mbps.
- **Queue Shaper Rate-Type:** The rate type of the queue shaper. The allowed values are:
  - Line: Specify that this shaper operates online rate.
  - Data: Specify that this shaper operates on data rate.
- **Queue Shaper Excess:** Controls whether the queue is allowed to use excess bandwidth.
- **Queue Shaper Credit:** Controls whether the queue has credit-based shaper enabled.
- **Queue Scheduler Preemption:** Controls whether the queue has frame preemption enabled.
- **Queue Scheduler Weight:** Controls the weight for this queue. This value is restricted to 1-100. This parameter is only shown if **Scheduler Mode** is set to **Weighted**.
- **Queue Scheduler Percent:** Shows the weight in percent for this queue. This parameter is only shown if the **Scheduler Mode** is set to **Weighted**.
- **Port Shaper Enable:** Controls whether the port shaper is enabled for this switch port.
- **Port Shaper Rate:** Controls the rate for the port shaper. This value is restricted to 100-3281943 when the unit is kbps, and 1-3281 when unit is Mbps. The rate is internally rounded up to the nearest value supported by the port shaper.
- **Port Shaper Unit:** Controls the unit of measure for the port shaper rate as kbps or Mbps.
- **Port Shaper Rate-Type:** The rate type of the port shaper. The allowed values are:
  - Line: Specify that this shaper operates on line rate.
  - Data: Specify that this shaper operates on data rate.

#### 4.17.5 QoS Port Tag Remarking Configuration

This page provides an overview of QoS Egress Port Tag Remarking for all switch ports.

Figure 4-77. QoS Egress Port Tag Remarking

Port	Mode
1	Classified
2	Classified
3	Classified
4	Classified
5	Classified
6	Classified

- **Port:** The logical port for the settings contained in the same row. Click on the port number 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 CoS and DPL.

#### 4.17.6 QoS Port DSCP Configuration

This page allows you to configure the basic QoS Port DSCP Configuration settings for all switch ports.

Figure 4-78. QoS Port DSCP Configuration

Port	Ingress		Egress
	Translate	Classify	Rewrite
*	<input type="checkbox"/>	<>	<>
1	<input type="checkbox"/>	Disable	Disable
2	<input type="checkbox"/>	Disable	Disable
3	<input type="checkbox"/>	Disable	Disable
4	<input type="checkbox"/>	Disable	Disable
5	<input type="checkbox"/>	Disable	Disable
6	<input type="checkbox"/>	Disable	Disable

Save Reset

- **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 and Classify.
  - Translate: To Enable the Ingress Translation, click the checkbox.
  - Classify: Classification for a port have four 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: Classify all DSCP.
- **Egress:** Port Egress Rewriting can be one of the following:
  - Disable: No Egress rewrite.
  - Enable: Rewrite enabled 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 Translation > Egress Remap DP0** table.
  - Remap DP Aware: DSCP from analyzer is remapped and frame is remarked with remapped DSCP value. Depending on the DP level of the frame, the remapped DSCP value is either taken from the **DSCP Translation > Egress Remap DP0** table or from the **DSCP Translation > Egress Remap DP1** table.

#### 4.17.7 QoS DSCP-Based QoS Configuration

This page allows you to configure the basic QoS Port DSCP Configuration settings for all switch ports.

Figure 4-79. DSCP-Based QoS Ingress Classification

DSCP	Trust	CoS	DPL
*	<input type="checkbox"/>	<>	<>
0 (BE)	<input type="checkbox"/>	0	0
1	<input type="checkbox"/>	0	0
2	<input type="checkbox"/>	0	0
3	<input type="checkbox"/>	0	0
4	<input type="checkbox"/>	0	0
5	<input type="checkbox"/>	0	0
6	<input type="checkbox"/>	0	0
7	<input type="checkbox"/>	0	0
8 (CS1)	<input type="checkbox"/>	0	0
9	<input type="checkbox"/>	0	0
10 (AF11)	<input type="checkbox"/>	0	0
11	<input type="checkbox"/>	0	0
12 (AF12)	<input type="checkbox"/>	0	0

- **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 CoS and DPL. Frames with untrusted DSCP values are treated as a non-IP frame.
- **CoS:** CoS value can be in range of (0–7).
- **DPL:** Drop Precedence Level (0–1).

#### 4.17.8 QoS DSCP Translation Configuration

This page allows you to configure the basic QoS DSCP Translation settings for all switches. DSCP translation can be done in Ingress or Egress.

Figure 4-80. DSCP Translation

DSCP	Ingress		Egress	
	Translate	Classify	Remap DP0	Remap DP1
*	<>	<input type="checkbox"/>	<>	<>
0 (BE)	0 (BE)	<input type="checkbox"/>	0 (BE)	0 (BE)
1	1	<input type="checkbox"/>	1	1
2	2	<input type="checkbox"/>	2	2
3	3	<input type="checkbox"/>	3	3
4	4	<input type="checkbox"/>	4	4
5	5	<input type="checkbox"/>	5	5
6	6	<input type="checkbox"/>	6	6
7	7	<input type="checkbox"/>	7	7
8 (CS1)	8 (CS1)	<input type="checkbox"/>	8 (CS1)	8 (CS1)
9	9	<input type="checkbox"/>	9	9
10 (AF11)	10 (AF11)	<input type="checkbox"/>	10 (AF11)	10 (AF11)
11	11	<input type="checkbox"/>	11	11
12 (AF12)	12 (AF12)	<input type="checkbox"/>	12 (AF12)	12 (AF12)
13	13	<input type="checkbox"/>	13	13
14 (AF13)	14 (AF13)	<input type="checkbox"/>	14 (AF13)	14 (AF13)
15	15	<input type="checkbox"/>	15	15
16 (CS2)	16 (CS2)	<input type="checkbox"/>	16 (CS2)	16 (CS2)
17	17	<input type="checkbox"/>	17	17
18 (AF21)	18 (AF21)	<input type="checkbox"/>	18 (AF21)	18 (AF21)
19	19	<input type="checkbox"/>	19	19
20 (AF22)	20 (AF22)	<input type="checkbox"/>	20 (AF22)	20 (AF22)

- **DSCP:** Maximum number of supported DSCP values are 64 and valid DSCP value ranges from 0 to 63.
- **Ingress:** Ingress side DSCP can be first translated to new DSCP before using the DSCP for CoS and DPL map. There are two configuration parameters for DSCP Translation:
  - 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. Select the DSCP value from select menu to which you want to remap. DSCP value ranges from 0–63.
  - Remap DP1: Controls the remapping for frames with DP level 1. Select the DSCP value from select menu to which you want to remap. DSCP value ranges from 0–63.

#### 4.17.9 QoS DSCP Classification Configuration

This page allows you to configure the mapping of CoS and DPL to DSCP value.

Figure 4-81. DSCP Classification

CoS	DSCP DP0	DSCP DP1
+	<>	<>
0	0 (BE)	0 (BE)
1	0 (BE)	0 (BE)
2	0 (BE)	0 (BE)
3	0 (BE)	0 (BE)
4	0 (BE)	0 (BE)
5	0 (BE)	0 (BE)
6	0 (BE)	0 (BE)
7	0 (BE)	0 (BE)

Save Reset

- **CoS**: Actual Class of Service.
- **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.

#### 4.17.10 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 the plus icon to add a new QCE to the list.

Figure 4-82. QoS Control List Configuration

QCE	Port	DMAC	SMAC	Tag Type	VID	PCP	DEI	Frame Type	Action				
									CoS	DPL	DSCP	PCP	DEI
+													

Figure 4-83. QCE Configuration

QCE Configuration

Port Members

1	2	3	4	5	6
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Key Parameters

DMAC	Any
SMAC	Any
Tag	Any
VID	Any
PCP	Any
DEI	Any
Inner Tag	Any
Inner VID	Any
Inner PCP	Any
Inner DEI	Any
Frame Type	Any

Action Parameters

CoS	0
DPL	Default
DSCP	Default
PCP	Default
DEI	Default
Policy	

Save Reset Cancel

- **QCE**: Indicates the QCE id.
- **Port**: Indicates the list of ports configured with the QCE or **Any**.
- **DMAC**: Indicates the destination MAC address. Possible values are:
  - Any: Match any DMAC
  - Unicast: Match unicast DMAC
  - Multicast: Match multicast DMAC
  - Broadcast: Match broadcast DMAC
  - <MAC>: Match specific DMAC
- **SMAC**: Match specific source MAC address or **Any**.
- **Tag Type**: Indicates tag type. Possible values are:

- Any: Match tagged and untagged frames
- Untagged: Match untagged frames
- Tagged: Match tagged frames
- C-Tagged: Match C-tagged frames
- S-Tagged: Match S-tagged frames
- **VID:** Indicates (VLAN ID), either a specific VID or range of VIDs. VID can be in the range of 1–4095 or 'Any'.
- **PCP:** Priority Code Point. Valid values of PCP are specific (0, 1, 2, 3, 4, 5, 6, and 7) or range (0–1, 2–3, 4–5, 6–7, 0–3, and 4–7) or **Any**.
- **DEI:** Drop Eligible Indicator. Valid value of DEI is 0, 1 or **Any**.
- **Frame Type:** Indicates the type of frame. 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 the configured parameters are matched with the frame's content. The following are the possible actions:
  - 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

#### 4.17.11 QoS Storm Policing Configuration

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 flooded frames, that is, frames with a (VLAN ID, DMAC) pair not present in the MAC Address table.

Figure 4-84. Global Storm Policer Configuration

Frame Type	Enable	Rate	Unit
Unicast	<input type="checkbox"/>	1	fps ▾
Multicast	<input type="checkbox"/>	1	fps ▾
Broadcast	<input type="checkbox"/>	1	fps ▾

- **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 the unit is fps, and 1–1024 when the unit is kfps. The rate is internally rounded up to the nearest value supported by the global storm policer. Supported rates are 1, 2, 4, 8, 16, 32, 64, 128, 256, and 512 fps for rates ≤ 512 fps and 1, 2, 4, 8, 16, 32, 64, 128, 256, 512, and 1024 kfps for rates > 512 fps.
- **Unit:** Controls the unit of measure for the global storm policer rate as fps or kfps.

#### 4.17.12 QoS Weighted Random Early Detection (WRED) Configuration

This page allows you to configure the Random Early Detection (RED) settings. Through different RED configuration for the queues, it is possible to obtain Weighted Random Early Detection (WRED) operation between queues. The settings are global for all ports in the switch.



Figure 4-85. Weighted Random Early Detection Configuration

Queue	Enable	Min	Max	Max Unit
0	<input type="checkbox"/>	0	50	Drop Probability ▼
1	<input type="checkbox"/>	0	50	Drop Probability ▼
2	<input type="checkbox"/>	0	50	Drop Probability ▼
3	<input type="checkbox"/>	0	50	Drop Probability ▼
4	<input type="checkbox"/>	0	50	Drop Probability ▼
5	<input type="checkbox"/>	0	50	Drop Probability ▼
6	<input type="checkbox"/>	0	50	Drop Probability ▼
7	<input type="checkbox"/>	0	50	Drop Probability ▼

Save Reset

- **Queue:** The queue number (CoS) for which the configuration below applies.
- **Enable:** Controls if RED is enabled for this entry.
- **Min:** Controls the lower RED fill level threshold. If the queue filling level is below this threshold, the drop probability is zero. This value is restricted to 0%–100%.
- **Max:** Controls the upper RED drop probability or fill level threshold for frames marked with Drop Precedence Level > 0 (yellow frames). This value is restricted to 1%–100%
- **Max Unit:** Selects the unit for maximum possible values.
  - Drop Probability: Maximum controls the drop probability just below 100% fill level.
  - Fill Level: Maximum controls the fill level where drop probability reaches 100%.

## 4.18 Mirroring Configuration

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. Remote Mirroring is an extend function of Mirroring. It can extend the destination port in another switch so that the administrator can analyze the network traffic on the other switches. If you want to get the tagged mirrored traffic, you must set VLAN egress tagging as **Tag All** on the reflector port. On the other hand, if you want to get untagged mirrored traffic, you must set VLAN egress tagging as **Untag ALL** on the reflector port.

In the following figure, port #5 Tx and Rx are configured to be mirrored over port #1.

Figure 4-86. Mirror and RMirror Configuration Table

Session ID	Mode	Type	VLAN ID	Reflector Port
1	Enabled	Mirror	-	-
2	Disabled	Mirror	-	-
3	Disabled	Mirror	-	-
4	Disabled	Mirror	-	-
5	Disabled	Mirror	-	-

Figure 4-87. Mirror and RMirror Configuration

Mirror & RMirror Configuration

Global Settings

Session ID	1
Mode	Enabled
Type	Mirror
VLAN ID	200
ReflectorPort	Port 1

Source VLAN(s) Configuration

VLAN ID

Port Configuration

Port	Source	Destination
*	<>	<input checked="" type="checkbox"/>
Port 1	Disabled	<input checked="" type="checkbox"/>
Port 2	Disabled	<input type="checkbox"/>
Port 3	Disabled	<input type="checkbox"/>
Port 4	Disabled	<input type="checkbox"/>
Port 5	Both	<input type="checkbox"/>
Port 6	Disabled	<input type="checkbox"/>
CPU	Disabled	<input type="checkbox"/>

Save Reset Cancel

**Note:** Only hardware switched packets are mirrored. Software outgoing packets to port #5 (for the preceding example) as LLDP reply, spanning tree sent by the Switch, and so on, are sent to port #5 without being mirrored to port #1.

- **Global Settings**

- Session ID: Select session ID (not to be confused with port number) to configure.
- Mode: Enable/Disable session mirroring or Remote Mirroring session function.
- Type: Select switch mirror type.
  - Mirror: The switch is running on mirror mode. The source port(s) and destination port are located on this switch.
  - Source: The switch is a source node for monitor flow. The source port(s), reflector port are located on this switch.
  - Rmirror Destination: The switch is an end node for monitor flow. The destination port(s) is located on this switch.
- VLAN ID: The VLAN ID points out where the monitor packet will copy to. The default VLAN ID is 200.

- **ReflectorPort:** The reflector port is a method to redirect the traffic to Remote Mirroring VLAN. Any device connected to a port set as a reflector port loses connectivity until the Remote Mirroring is disabled. In the stacking mode, you need to select switch ID to select the correct device. If you shut down a port, it cannot be a candidate for reflector port. If you shut down the port which is a reflector port, then the remote mirror function cannot work.

**Notes:**

- The reflector port must select only on Source switch type.
- The reflector port must disable MAC Table learning and STP.
- The reflector port only supports on pure copper ports.
- **Source VLAN (s) Configuration:** The switch can support VLAN-based Mirroring. If you want to monitor some VLANs on the switch, you can set the selected VLANs on this field.
 

**Note:** The Mirroring session has either ports or VLANs as sources, but not both.
- **Remote Mirroring Port Configuration:** The following table is used for port role selecting.
  - Port: The logical port for the settings contained in the same row.
  - Source: Select mirror mode:
    - Disabled: Neither frames transmitted, nor frames received are mirrored.
    - Both: Frames received and frames transmitted are mirrored on the Destination port.
    - Rx only: Frames received on this port are mirrored on the Destination port. Frames transmitted are not mirrored.

- Tx Only: Frames transmitted on this port are mirrored on the Destination port. Frames received are not mirrored.
- **Destination:** Select destination port. This checkbox is designed for mirror or Remote Mirroring. The destination port is a switched port that you receive a copy of traffic from the source port.

**Notes:**

- On the Mirror mode, the device only supports one destination port.
- The destination port must disable MAC table learning.

### Configuration Guideline for All Features

When the switch is running on Remote Mirroring mode, the administrator must also check if other features are enabled or disabled. For example, the administrator is not disabled the MSTP on reflector port. All monitor traffic is blocked on reflector port. The following table lists all recommended settings.

**Table 4-2. Recommended Settings**

Network Feature	Impact <sup>3</sup>	Reflector Port	Intermediate Port	Destination Port	Remote Mirroring VLAN
arp_inspection	High	Disabled <sup>1</sup>	Disabled <sup>1</sup>	—	—
acl	Critical	Disabled <sup>1</sup>	Disabled <sup>1</sup>	Disabled <sup>1</sup>	—
dhcp_relay	High	Disabled <sup>1</sup>	Disabled <sup>1</sup>	—	—
dhcp_snooping	High	Disabled <sup>1</sup>	Disabled <sup>1</sup>	—	—
ip_source_guard	Critical	Disabled <sup>1</sup>	Disabled <sup>1</sup>	Disabled <sup>1</sup>	—
ipmc/igmpsnp	Critical	—	—	—	un-conflict
ipmc/mlidsnp	Critical	—	—	—	un-conflict
lACP	Low	—	—	Disabled <sup>2</sup>	—
lldp	Low	—	—	Disabled <sup>2</sup>	—
mac learning	Critical	Disabled <sup>1</sup>	Disabled <sup>1</sup>	Disabled <sup>1</sup>	—
mstp	Critical	Disabled	—	Disabled <sup>2</sup>	—
mvr	Critical	—	—	—	un-conflict
nas	Critical	Authorized <sup>1</sup>	Authorized <sup>1</sup>	Authorized <sup>1</sup>	—
psec	Critical	Disabled <sup>1</sup>	Disabled <sup>1</sup>	Disabled <sup>1</sup>	—
qos	Critical	Unlimited <sup>1</sup>	Unlimited <sup>1</sup>	Unlimited <sup>1</sup>	—
upnp	Low	—	—	Disabled <sup>2</sup>	—
mac-based vlan	Critical	Disabled <sup>1</sup>	Disabled <sup>1</sup>	—	—
protocol-based vlan	Critical	Disabled <sup>1</sup>	Disabled <sup>1</sup>	—	—
vlan_translation	Critical	Disabled <sup>1</sup>	Disabled <sup>1</sup>	Disabled <sup>1</sup>	—
voice_vlan	Critical	Disabled <sup>1</sup>	Disabled <sup>1</sup>	—	—
mrp	Low	—	—	Disabled <sup>2</sup>	—
mvrp	Low	—	—	Disabled <sup>2</sup>	—

**Notes:**

1. Must
2. Optional
3. Impact—Critical/High/Low
  - Critical 5 packets > 0 packet
  - High 5 packets > 4 packets
  - Low 5 packets > 6 packets

## 4.19 UPnP Configuration

Configure Universal Plug and Play (UPnP) on this page.

**Figure 4-88. UPnP Configuration**

Mode	Disabled ▾
TTL	4
Advertising Duration	100
IP Addressing Mode	Dynamic ▾
Static VLAN Interface ID	1

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

When the mode is enabled, two ACEs are added automatically to trap UPnP related packets to CPU. The ACEs are automatically removed when the mode is disabled.

- **TTL:** The TTL value is used by UPnP to send SSDP advertisement messages. Read only now.
- **Advertising Duration:** The duration, carried in SSDP packets, is used to inform a control point or control points how often it or they should receive an SSDP advertisement message from this switch. If a control point does not receive any message within the duration, it will think that the switch no longer exists. Due to the unreliable nature of UDP, in the standard it is recommended that such refreshing of advertisements to be done at less than one-half of the advertising duration. In the implementation, the switch sends SSDP messages periodically at the interval one-half of the advertising duration minus 30s. Valid values are in the range 100 to 86400. Specified in seconds.
- **IP Addressing Mode:** IP addressing mode provides two ways to determine IP address assignment:
  - Dynamic: Default selection for UPnP. UPnP module helps users choosing the IP address of the switch device. It finds the first available system IP address.
  - Static: User specifies the IP interface VLAN for choosing the IP address of the switch device.
- **Static VLAN Interface ID:** The index of the specific IP VLAN interface. It will only be applied when IP Addressing Mode is static. Valid configurable values range from 1–4095. Default value is 1.

## 4.20 sFlow Configuration

This page allows for configuring sFlow. The configuration is divided into two parts: Configuration of the sFlow receiver (that is, sFlow collector) and configuration of per-port flow and counter samplers.

sFlow configuration is not persisted to non-volatile memory, which means that a reboot disables sFlow sampling.

Figure 4-89. sFlow Configuration

**sFlow Configuration**

**Agent Configuration**

IP Address

**Receiver Configuration**

Owner	<none>	Release
IP Address/Hostname	0.0.0.0	
UDP Port	6343	
Timeout	0	seconds
Max. Datagram Size	1400	bytes

**Port Configuration**

Port	Flow Sampler			Counter Poller	
	Enabled	Sampling Rate	Max. Header	Enabled	Interval
*	<input type="checkbox"/>	0	128	<input type="checkbox"/>	0
1	<input type="checkbox"/>	0	128	<input type="checkbox"/>	0
2	<input type="checkbox"/>	0	128	<input type="checkbox"/>	0
3	<input type="checkbox"/>	0	128	<input type="checkbox"/>	0
4	<input type="checkbox"/>	0	128	<input type="checkbox"/>	0
5	<input type="checkbox"/>	0	128	<input type="checkbox"/>	0
6	<input type="checkbox"/>	0	128	<input type="checkbox"/>	0

• **Agent Configuration**

- IP Address: The IP address used as Agent IP address in sFlow datagrams. It serves as a unique key that identifies this agent over extended periods of time. Both IPv4 and IPv6 addresses are supported.

• **Receiver Configuration**

- Owner: Basically, sFlow can be configured in two ways: Through local management using the Web or CLI interface or through SNMP. This read-only field shows the owner of the current sFlow configuration and assumes values as follows:
  - If sFlow is currently unconfigured/unclaimed, Owner contains <none>.
  - If sFlow is currently configured through Web or CLI, Owner contains <Configured through local management>.
  - If sFlow is currently configured through SNMP, Owner contains a string identifying the sFlow receiver. If sFlow is configured through SNMP, all controls except for the Release button, are disabled to avoid inadvertent reconfiguration.

The RELEASE button allows for releasing the current owner and disable sFlow sampling. The button is disabled if sFlow is currently unclaimed. If configured through SNMP, the release must be confirmed (a confirmation request will appear).

- IP Address/Hostname: The IP address or hostname of the sFlow receiver. Both IPv4 and IPv6 addresses are supported.
- UDP Port: The UDP port on which the sFlow receiver listens to sFlow datagrams. If set to 0 (zero), the default port (6343) is used.
- Timeout: The number of seconds remaining before sampling stops and the current sFlow owner is released. While active, the current time left can be updated by clicking on **Refresh**. If locally managed, the timeout can be changed on the fly without affecting any other settings. Valid range is 0 to 2147483647 seconds.

- Max. Datagram Size: The maximum number of data bytes that can be sent in a single sample datagram. This should be set to a value that avoids fragmentation of the sFlow datagrams. Valid range is 200 to 1468 bytes with default being 1400 bytes.
- **Port Configuration**
  - Port: The port number for which the configuration below applies.
  - Flow Sampler Enabled: Enables/disables flow sampling on this port.
  - Flow Sampler Sampling Rate: The statistical sampling rate for packet sampling. Set to N to sample on average  $1/N^{\text{th}}$  of the packets transmitted/received on the port. Not all sampling rates are achievable. If an unsupported sampling rate is requested, the switch automatically adjusts it to the closest achievable. This is reported back in this field. Valid range is 1–4096.
  - Flow Sampler Max. Header: The maximum number of bytes that should be copied from a sampled packet to the sFlow datagram. Valid range is 14–200 bytes with default being 128 bytes.  
To have room for any frame, the maximum datagram size must be roughly 100 bytes larger than the maximum header size. If the maximum datagram size does not consider the maximum header size, samples may be dropped.
  - Counter Poller Enabled: Enables/disables counter polling on this port.
  - Counter Poller Interval: With counter polling enabled, this specifies the interval, in seconds, between counter poller samples. Valid range is 1s–3600s.

## 5. Web Interface—Monitor

This section provides information about all unit configuration web pages.

### 5.1 Monitor System

The following sections describe the Monitor system.

#### 5.1.1 Monitor System Information

This web page provides the switch system information.

**Figure 5-1. Monitor System Information**

System Information	
<b>System</b>	
Contact	
Name	
Location	
<b>Hardware</b>	
MAC Address	00-de-fd-ae-17-78
Serial Number	-----
Product Number	----
<b>Time</b>	
System Date	2022-11-15T17:50:50+00:00
System Uptime	1d 01:17:42
<b>Software</b>	
Software Version	PDS-204GCO-v1.08
Software Date	2022-11-14T16:33:37+02:00
Code Revision	001
Licenses	<a href="#">Details</a>

- **Contact:** Provides switch system information.
- **Name:** The system name configured in Configuration | System | Information | System Name.
- **Location:** The system location configured in Configuration | System | Information | System Location.
- **MAC Address:** The MAC Address of this switch.
- **Chip ID:** The Chip ID 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 the device has been operational.
- **Software Version:** The software version of this switch.
- **Software Date:** The date when the switch software was produced.
- **Code Revision:** The version control identifier of the switch software.

#### 5.1.2 Monitor CPU Load

This web page reports Switch internal CPU load. The load is measured as averaged over the last 100 ms, 1s, and 10s intervals. The last 120 samples are graphed, and the last numbers are displayed as text. To display the SVG graph, your browser must support the SVG format.



Figure 5-2. Monitor System CPU Load



### 5.1.3 Monitor System IP-Status

This page displays the status of the IP protocol layer. The status is defined by the IP interfaces, the IPv6 routes, and the neighbor cache (ARP cache) status.

Figure 5-3. Monitor System IP-Status

#### IP Interfaces

Interface	Type	Address	Status
VLAN 1	LINK	00-de-fd-ae-17-78	<UP BROADCAST MULTICAST>
VLAN 1	IPv4	192.168.0.50/24	
VLAN 1	IPv6	fe80::2de:fdff:feae:1778/64	

#### IP Routes

##### IPv4

Network	Gateway	Status
192.168.0.0/24	VLAN 1	<UP>

##### IPv6

Network	Gateway	Status
fe80::/64	VLAN 1	<UP>

#### Neighbor cache

##### IPv4

IP Address	Link Address
192.168.0.40	VLAN 1:00-0a-cd-2d-b1-ed

##### IPv6

IP Address	Link Address
------------	--------------

- **IP Interfaces**
  - Interface: The name of the interface.
  - Type: The address type of the entry. This may be LINK, IPv4, or IPv6.
  - 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 IPv4/IPv6 network or host address of this route.
  - Gateway: The gateway address of this route.
  - Status: The status flags of the route.
- **Neighbor Cache**
  - IP Address: The IPv4/IPv6 address of the entry.
  - Link Address: The Link (MAC) address for which a binding to the IP address given exist.

### 5.1.4 Monitor System IPv4 Routing Info. Base

This table provides IPv4 routing status. Each page shows up to 999 table entries, selected through the **entries per page** input field. When first visited, the web page shows the beginning entries of this table.

Figure 5-4. Routing Information Base

Routing Information Base 1 - 1 of 1 entry    Auto-refresh     Refresh    <<    <<    >>    >>|

Start from Network  /  Protocol  NextHop  with  entries per page.

Codes: C - connected, S - static, O - OSPF, R - RIP, \* - selected route, D - DHCP installed route

Protocol	Network/Prefix	NextHop	Distance	Metric	Interface	Uptime (hh:mm:ss)	State
C *	192.168.0.0/24	-	-	-	VLAN 1	1d 02:18:00	Active

- **Protocol:** The protocol that installed this route.
  - DHCP: The route is created by DHCP.
  - Connected: The destination network is connected directly.
  - Static: The route is created by user.
  - OSPF: The route is created by OSPF (NA for this product).
- **Network Prefix:** Network and prefix (for example, 10.0.0.0/16) of the given route entry.
- **Next Hop:** Next-hop IP address. All-zeroes indicates the link is directly connected.
- **Interface:** Next-hop interface
- **Distance:** Distance of the route
- **Metric:** Metric of the route
- **Uptime (hh:mm:ss):** Time (in seconds) since this route was created.
- **State:** Destination is active.

### 5.1.5 Monitor System IPv6 Routing Info. Base

This table provides IPv6 routing status. Each page shows up to 999 table entries, selected through the **entries per page** input field. When first visited, the web page shows the beginning entries of this table.

Figure 5-5. Routing Information Base

Routing Information Base 1 - 1 of 1 entry    Auto-refresh     Refresh    <<    <<    >>    >>|

Start from Network  /  Protocol  NextHop  with  entries per page.

Codes: C - connected, S - static, O - OSPF, R - RIP, \* - selected route, D - DHCP installed route

Protocol	Network/Prefix	NextHop	Distance	Metric	Interface	Uptime (hh:mm:ss)	State
C *	fe80::/64	::	-	-	VLAN 1	1d 02:28:00	Active

- **Protocol:** The protocol that installed this route.
  - DHCP: The route is created by DHCP.
  - Connected: The destination network is connected directly.
  - Static: The route is created by user.
  - OSPF: The route is created by OSPF (N/A for this product)
- **Network Prefix:** Network and prefix of the given route entry.
- **Next Hop:** Next-hop IP address. All-zeroes indicates the link is directly connected.
- **Interface:** Next-hop interface
- **Distance:** Distance of the route.
- **Metric:** Metric of the route.
- **Uptime (hh:mm:ss):** Time (in seconds) since this route was created
- **State:** Destination is active.

### 5.1.6 Monitor System Log

The switch system log information is provided here. Each page shows up to 999 table entries, selected through the **entries per page** input field. When first visited, the web page shows the beginning entries of this table. The **Level**

input field is used to filter the display system log entries. The **Clear Level** input field is used to specify which system log entries will be cleared. To clear specific system log entries: First, select the clear level, and then click on it.

The **Start from ID** input field allows you to change the starting point in this table. Clicking the button updates the displayed table starting from that or the closest next entry match. In addition, when clicked, these input fields consider the value of the first displayed entry, allowing for continuous refresh with the same start input field.

Figure 5-6. System Log Information

System Log Information Auto-refresh  Refresh Clear << >> >>|

Level: All  
Clear Level: All

The total number of entries is 8 for the given level.

Start from ID  with  entries per page.

ID	Level	Time	Message
1	Informational	2022-11-14T16:33:43+00:00	SYS-BOOTING: Switch just made a cool boot.
2	Notice	2022-11-14T16:33:43+00:00	LINK-UPDOWN: IP Interface VLAN 1 changed state to down.
3	Notice	2022-11-14T16:33:43+00:00	LINK-UPDOWN: IP Interface VLAN 1 changed state to down.
4	Notice	2022-11-14T16:33:45+00:00	POE-CONTROL: controller found
5	Notice	2022-11-14T16:33:46+00:00	LINK-UPDOWN: Interface 2.5GigabitEthernet 1/2, changed state to up.
6	Notice	2022-11-14T16:33:51+00:00	LINK-UPDOWN: IP Interface VLAN 1 changed state to up.
7	Notice	2022-11-14T16:33:56+00:00	POE-CONTROL: Port 1/3 changed from: NO_SUPP (0x00) to: PD_ON (0x89 DSPD)
8	Notice	2022-11-14T16:33:56+00:00	POE-CONTROL: Port 1/4 changed from: NO_SUPP (0x00) to: PD_ON (0x86 SSPD)

- **ID:** The identification of the system log entry.
- **Levels:** The level of the system log entry. Information: The system log entry belongs to information level.
  - Warning: The system log entry is belonged warning level.
  - Error: The system log entry is belonged error level.
- **Time:** The occurred time of the system log entry.
- **Message:** The detail message of the system log entry.

### 5.1.7 Monitor System Detailed Log

The switch system detailed log information is provided on this page.

Figure 5-7. Detailed System Log Information

Detailed System Log Information

ID:

Message

Level	Informational
Time	2022-11-14T16:33:43+00:00
Message	SYS-BOOTING: Switch just made a cool boot.

- **Level:** The severity level of the system log entry.
- **ID:** The ID ( $\geq 1$ ) of the system log entry.
- **Messages:** The detailed message of the system log entry.

## 5.2 Monitor Green Ethernet Port Power Savings

This page provides the current status for EEE power saving.

Figure 5-8. Port Power Savings Status

Port	Link	EEE Cap	EEE Ena	LP EEE Cap	EEE In power save	ActiPhy Savings	PerfectReach Savings
1	●	✓	✗	✗	✗	✗	✗
2	●	✓	✗	✗	✗	✗	✗
3	●	✓	✗	✗	✗	✗	✗
4	●	✓	✗	✗	✗	✗	✗
5	●	✗	✗	✗	✗	✗	✗
6	●	✗	✗	✗	✗	✗	✗

- **Port:** This is the logical port number for this row.
- **Link:** Shows if the link is up for the port (green = link up, red = link down).
- **EEE Cap:** Shows if the port is EEE capable.
- **EEE Ena:** Shows if EEE is enabled for the port (reflects the settings at the Port Power Savings configuration page).
- **LP EEE Cap:** Shows if the link partner is EEE capable.
- **EEE In Power Save:** Shows if the system is currently saving power due to EEE. When EEE is enabled, the system is powered down if no frame has been received or transmitted in 5  $\mu$ s.
- **ActiPhy Savings:** Shows if the system is currently saving power due to ActiPhy.
- **PerfectReach Savings:** Shows if the system is currently saving power due to PerfectReach.

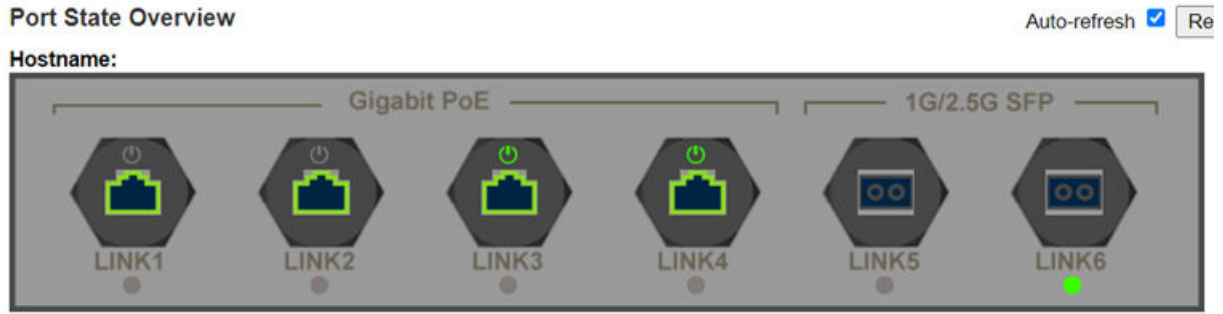
## 5.3 Monitor Ports

The following sections describe the Monitor ports.

### 5.3.1 Monitor Ports State

This page provides entire system overview in a single web page. It is the web page presented to the user when browsing to unit IP address.

Figure 5-9. Port State Overview



Ports - Network Status

#	Local Link						Remote Network Device-LLDP/CDP		
	Type	Status	Speed	Aggr Ports	Transmit	Receive	System Name	System Description	IP Address
1	Copper	---	---	---	---	---	---	---	---
2	Copper	---	---	---	---	---	---	---	---
3	Copper	---	---	---	---	---	---	---	---
4	Copper	---	---	---	---	---	---	---	---
5	Sfp	---	---	---	---	---	---	---	---
6	Sfp	Up	1Gfdx	---	8.4 Kb/s	2.8 Kb/s	---	---	---

Ports - PoE Status

#	Local PoE Port Status						Remote PoE Device			
	PoE-BT Port Type	Power management Mode	Status	Requested Power	Assigned Power	Delivered Power	Assigned Class	PD Measured Class	PD Auto Class Support	PD Requested Power over LLDP
1	Type4 90[W]	Dynamic	---	---	---	---	---	---	---	---
2	Type4 90[W]	Dynamic	---	---	---	---	---	---	---	---
3	Type4 90[W]	Dynamic	On	90 [W]	90 [W]	0.5 [W]	5, 5	5, 5	---	---
4	Type4 90[W]	Dynamic	On	60 [W]	60 [W]	4.2 [W]	6	6	No	---

System - Status

Item	Value
Total Power Usage	4 [W]
Total Allocated Power	4 [W]
Free Available Power	147 [W]
Power Supply Voltage	53.5 [V]

• Ports—Network Status

- #: Port number.
- Type: Copper/SFP. Ports 1–4 are Gigabit copper ports. Ports 5–6 are SFP 2.5 Gigabit SFP ports with default of 1-Gigabit link speed. User must configure SFP port to 2.5 Gigabit when a dedicated 2.5G Gigabit SFP is in use.
- Status:
  - ---: Port is enabled. Link is down.
  - Up: Port is enabled. Link is up
  - Disabled: Port is disabled
- Speed: Port link speed: 10 Mbps, 100 Mbps, 1 Gbps, and 2.5 Gbps.
- Aggregation Ports: Report configured aggregation ports. For example: P1, P2.
- Transmit: Average transmit data rate in Kbit, Mbit per second.
- Receive: Average receive data rate in Kbit, Mbit per second.
- System Name: Remote Network device name as advertised over LLDP/CDP.
- System Description: Remote Network system description as advertised over LLDP/CDP.
- IP Address: Remote Network device IP-Address as advertised over LLDP/CDP.

• Ports—PoE Status

- PoE-BT Port Type: PoE port maximum power configuration. Power to PD is shut down when PD tries to exceed the limit.

- Type4-90W: PoE-BT up to 90W on four pair. Up to 45W on two pair.
  - Type3-60W: PoE-BT up to 60W on four pair. Up to 30W on two pair.
  - Type3-30W: PoE-BT up to 30W on four pair. Up to 30W on two pair.
  - Type3-15W: PoE-BT up to 15W on four pair. Up to 15W on two pair.
- Power Management Mode: Power management configuration mode effecting how PD class, power consumption effects the unit overall free available power.
    - Dynamic: PoE port dynamic real time power consumption will be deducted from overall PoE free power budget ignoring PD class or PoE port maximum power.
    - Static: PoE port type power configuration (as Type4-90W) is deducted from overall PoE free power budget after PoE port is turned On, ignoring PD actual power consumption. Next PD may not be turned ON when free available power is lower than PD requested power. Initial PD requested power is based on PD class, PD Auto-Class.
    - Hybrid: Mixture of dynamic and static power management based on PD advertising its power requirements by sending LLDP IEEE 802.3 Power through MDI TLV protocol. Every PoE port configured as Hybrid acts as if it was configured as Dynamic, if it has not received any Power Over-MDI TLV within LLDP packet sent by the PD. After receiving IEEE 802.3 Power through MDI TLV, the port switches to Static Power mode limiting PoE port maximum power as per the PD requested power plus user configured cable loss based on user cable length configuration. Static PoE port maximum power may change based on PD LLDP IEEE 802.3 Power through MDI TLV advertised values.
  - Status—reports the latest PoE port status.
    - ---: PoE port is enabled. No PoE-PD
    - On: PoE power is applied to PD
    - Disabled: PoE is disabled (non-related to Ethernet data link state)
    - Overload: PD power consumption exceeded its maximum limit. Power was shut down
    - Fault: Fail to turn on connected PD device. The following are the possible reasons:
      - Non-standard PD is connected.
      - PD class error.
      - PD underload (PD power consumption is too low).
      - Shortage or invalid capacitor value.
      - PD was disconnected (temporary recovery from underload).
      - PSE Fault. Not enough free available power to turn on PD device. Other rare possible reason: Power supply voltage is out of range. Voltage is injected into the Ethernet port. Port over temperature.
  - Requested Power: PoE PD requested power based on PD Class. Class 8 = 90W, class 5, 5 = 90W, class 6 = 60W, class 4, 4 = 60W, class 4 = 30W, class 3 = 15W, class 2 = 7W, class 1 = 4W, class 0 = 15W.
  - Assigned Power: The maximum power that was assigned to the PD. Trying to consume above this limit causes the PD to be turned OFF. When enabling **Legacy PD\_Class Mode**, assigned PD class may defer from measured PD class, leading to Assigned-Power to differ from Requested-Power. Assigned power may defer from requested power from the following reasons.
    - Demotion: Free available power is less then PD requested power. PoE-BT will use the demotion option to offer a lower power value to the PD. If PD agree to the lower power value, then it will be turned ON with lower power limit.
    - PoE Port maximum Power: PoE port maximum power configuration lower then new inserted PD power class. For example, a 90W PD class-8 being connected to PoE port configured as Type3-60W.
    - Delivered Power: Temporarily PD power consumption.
    - Assigned Class: PD maximum power consumption is determined by the class it is being assigned by the PoE controller ( $8=90W/5$ ,  $5=90W/6 = 60W /4$ ,  $4 = 60W/4 = 30W/3 = 15W/2 = 7W/1=4W/0 = 15W$ ). Most of the time PD Assigned-Class matches PD-Measured-Class. PD-Assigned-Class differs from PD-Measured-Class in one of the following scenarios:
      - PoE Power Demotion: Per IEEE 802.3bt specification, when PoE port maximum available power is less then PD requested power, the PoE port may offer the PD a lower maximum power value. It is up to the PD to decide if to accept the new offer agreeing to consume less power. For example, PD class-8 (90W) is being connected while PoE-Port has only 60W spare power left. Port offers



PoE class-6 (60W). If PD accepts the offer, then Measured-Class is class-8 while Assigned-Class is class-6.

- Legacy PD-Class Mode = PoH. Port Mode = Plus. PoE-AT DSPD PD class 4, 4 is given 90W as if it is class 5, 5 (2x45W). PoE-AT SSPD PD class 4 is given 45W as if it is class 5.
  - Legacy PD-Class Mode = Ignore PD-Class. Port Mode =Type4-90W. Any DSPD class-x,x is given 90W as if it is class 5, 5 (2x45W). SSPD PD class-x is given 45W as if it is class 5.
  - Legacy PD-Class Mode = Ignore PD-Class. Port Mode=Type3-60W. Any DSPD Class-x, x is given 60W as if it is class 4, 4 (2x30W). SSPD PD class-x is given 30W as if it is class 4.
  - PD Measured Class: Remote PoE-PD measured Class 1–8 for SSPD, or Class 0,0, Class 5, 5 for DSPD
  - PD Auto Class Support: Report if remote PoE-BT PD device advertise it is supporting PoE Auto Class regardless to unit Auto Class configuration. When enabled and supported by the PoE-PD device, PoE port maximum power allocation is determined by the power consumed by PD during the Auto Class negotiation phase instead of the PD class.
  - PD Requested Power over LLDP: When supported by remote PoE-PD; Report remote PoE PD requested power using LLDP Power Over-MDI. If PoE-LLDP is disabled, (N/A) appears to the right of PD request power, ignoring PD request power using only PD class for determining PoE power request. When PoE-LLDP is enabled, PD PoE power request over LLDP replaces PoE PD class. However, it never exceeds the PD class maximum power. Cable loss based on cable length configuration is added on top of PD LLDP requested power. PoE power management configuration mode controls how much power is deducted from unit free available power.
- **System—Status**
    - Total Power Usage: Total power consumption by all PoE ports.
    - Total Allocated Power: Total power allocated to all active PoE ports. PoE port power management mode configuration effects the total allocated power.
    - Free Available Power: The free available power left to power additional PoE port, or before turning OFF active PoE PD due to lack of free available power.
    - Power Supply Voltage: PoE power supply voltage.

### 5.3.2 Monitor Ports Traffic Overview

This page provides an overview of general traffic statistics for all switch ports.

Figure 5-10. Port Statistics Overview

Port Statistics Overview Auto-refresh  Refresh Clear

Port	Packets		Bytes		Errors		Drops		Filtered
	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received
1	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0
6	101871	53401	14040481	13662872	0	0	0	0	62689

- **Port:** The logical port for the settings contained in the same row.
- **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.

### 5.3.3 Monitor Ports QoS Statistics

This page provides statistics for the different queues for all switch ports.



Figure 5-11. Queuing Counters

Queuing Counters

Port	Q0		Q1		Q2		Q3		Q4		Q5		Q6		Q7	
	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
6	48455	50189	0	0	0	0	0	0	0	0	0	0	0	0	0	3607

- **Port:** The logical port for the settings contained in the same row.
- **Qn:** There are eight QoS queues per port. Q0 is the lowest priority queue.
- **Rx/Tx:** The number of received and transmitted packets per queue.

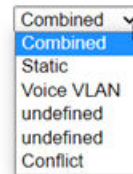
### 5.3.4 Monitor Ports QCL Status

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.

Figure 5-12. QoS Control List Status

QoS Control List Status

User	QCE	Port	Frame Type	Action						Conflict
				CoS	DPL	DSCP	PCP	DEI	Policy	
No entries										



- **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. 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 SCP value.
  - PCP: Classify PCP value.
  - DEI: Classify DEI value.
  - Policy: Classify ACL Policy number
- **Conflict:** Displays Conflict status of QCL entries. As hardware resources are shared by multiple applications, the resources required to add a QCE may not be available. In such a case, it shows conflict status as **Yes**. Otherwise, it is always **No**.

**Note:** Conflict can be resolved by releasing the hardware resources required to add QCL entry on clicking **Resolve Conflict**.

### 5.3.5 Monitor Ports Detailed 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.

Figure 5-13. Detailed Port Statistics

Detailed Port Statistics Port 6 Port 6

Receive Total		Transmit Total	
Rx Packets	103429	Tx Packets	54540
Rx Octets	14283552	Tx Octets	13929148
Rx Unicast	38964	Tx Unicast	50860
Rx Multicast	63371	Tx Multicast	3676
Rx Broadcast	1094	Tx Broadcast	4
Rx Pause	0	Tx Pause	0
Receive Size Counters		Transmit Size Counters	
Rx 64 Bytes	29308	Tx 64 Bytes	28412
Rx 65-127 Bytes	61555	Tx 65-127 Bytes	4804
Rx 128-255 Bytes	3818	Tx 128-255 Bytes	7256
Rx 256-511 Bytes	8462	Tx 256-511 Bytes	8624
Rx 512-1023 Bytes	286	Tx 512-1023 Bytes	1125
Rx 1024-1526 Bytes	0	Tx 1024-1526 Bytes	4319
Rx 1527- Bytes	0	Tx 1527- Bytes	0
Receive Queue Counters		Transmit Queue Counters	
Rx Q0	49069	Tx Q0	50904
Rx Q1	0	Tx Q1	0
Rx Q2	0	Tx Q2	0
Rx Q3	0	Tx Q3	0
Rx Q4	0	Tx Q4	0
Rx Q5	0	Tx Q5	0
Rx Q6	0	Tx Q6	0
Rx Q7	0	Tx Q7	3636
Receive Error Counters		Transmit Error Counters	
Rx Drops	0	Tx Drops	0
Rx CRC/Alignment	0	Tx Late/Exc. Coll.	0
Rx Undersize	0		
Rx Oversize	0		
Rx Fragments	0		
Rx Jabber	0		
Rx Filtered	63371		

- **Receive Total and Transmit Total**
  - Rx and Tx Packets: The number of received and transmitted (good and bad) packets
  - Rx and Tx Octets: The number of received and transmitted (good and bad) bytes. Includes FCS but excludes framing bits.
  - Rx and Tx Unicast: The number of received and transmitted (good and bad) unicast packets.
  - Rx and Tx Multicast: The number of received and transmitted (good and bad) multicast packets.
  - Rx and Tx Broadcast: The number of received and transmitted (good and bad) broadcast packets.
  - Rx and Tx Pause: A count of the MAC Control frames received or transmitted on this port that have an opcode indicating a PAUSE operation.
- Receive and Transmit Size Counters: The number of received and transmitted (good and bad) packets split into categories based on 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. Short frames are:
    - Short frames are frames that are smaller than 64 bytes.

- 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.
- **Receive MM Counters**
  - Rx MM Fragments: A count of received MAC frame fragments.
  - Rx MM Assembly OK: A count of MAC frames that were successfully reassembled and delivered to MAC.
  - Rx MM SMD Error: A count of MAC frames with reassembly errors. The counter is incremented when the ASSEMBLY\_ERROR state of the Receive Processing State Diagram is entered.
- **Transmit MM Counters**
  - Tx MM Fragments: A count of transmitted MAC frame fragments.
  - Tx MM Hold: A count of times MM\_CTL.request (HOLD) primitive assertion caused preemption of a preemptable MAC frame.

### 5.3.6 Monitor Ports Name Map

Many web pages use a port number to express an interface, whereas CLI uses interface names. The table on this page provides a means to convert from one to the other.

Figure 5-14. Interface Name to Port Number Map

**Interface Name to Port Number Map**

Interface Name	Port Number
Gi 1/1	1
Gi 1/2	2
Gi 1/3	3
Gi 1/4	4
2.5G 1/1	5
2.5G 1/2	6

## 5.4 Monitor CFM Status

See the Monitor CFM Status on this page.

Figure 5-15. CFM MEP Status

### CFM MEP Status

Domain	Service	MEPID	Port	State		SMAC	Defects		CCM Rx			CCM Tx
				Active	Fng		Highest	Defects	Valid	Invalid	Errors	
No entry exists												

- **Domain:** Name of Domain under which this MEP resides.
- **Services:** Name of Service under which this MEP resides.
- **MEPID:** The identification of this MEP.
- **Port:** Port on which this MEP resides.
- **State:**
  - Active: Operational state of the MEP.
    - ●: OFF. This indicates that the MEP Admin State is disabled.
    - ●: DOWN. The MEP Admin State is enabled, but an error state exists.
    - ●: UP. The MEP Admin State is enabled, and no errors and defects exist.
  - Fng: Holds the current state of the Fault Notification Generator State Machine. Values are one of the following options:
    - Reset: No defect has been present since reset timer expired or the State Machine was last reset.
    - Defect: A defect is present, but not for a long enough time to be reported.
    - reportDefect: A transient state during which the defect is reported.
    - defectReported: A defect is present, and some defect has been reported.

- defectClearing: No defect is present, but the ResetTime timer has not yet expired
- **SMAC**: This is MEP's MAC address.
- **Defects**
  - Highest: Highest priority defect that has been present since the MEP's fault notification generator state machine was last in the reset state.
  - Defects: A MEP can detect and report a number of defects, and multiple defects can be present at the same time. This is indicated the following letter code.

**Table 5-1. Letter Codes**

Code	Defect	Description
—	Defect not present	Defect not present
R	someRDIdefect	RDI received from at least one remote MEP
M	someMACstatusDefect	Received Port Status TLV != psUp or Interface Status TLV != isUp
C	someRMEPCCMdefec	Valid CCM is not received within 3.5 times CCM interval from at least one remote MEP
E	errorCCMdefect	Received CCM from an unknown remote MEP-ID or CCM interval mismatch
X	xconCCMdefect	Received CCM with an MD/MEG level smaller than configured or wrong MAID/MEGID (cross-connect)

- **CCM Rx**
  - Valid: Total number of CCMs that hit this MEP and pass the validation test.
  - Invalid: Total number of CCMs that hit this MEP and did not pass the validation test.
  - Errors: Total number of out-of-sequence errors seen from RMEPs.
- **CCM Tx**: Total number of CCM PDUs transmitted by this MEP.

## 5.5 Monitor APS

This page shows the status of the APS instances.

**Figure 5-16. APS Status**

APS Status

APS #	State			Defect state		TxAps			RxAps			Dfop				SMAC	TxCnt	RxCnt	
	Operational	Warning	Protection	Working	Protecting	Request	ReSignal	BrSignal	Request	ReSignal	BrSignal	CM	PM	NR	TO			Valid	Invalid
No entry exists																			

- **APS #**: The ID of the APS. Click on link to get to the APS instance page where you can reset counters and issue commands.
- **State**:
  - Operational: The operational state of the APS instance. There are many ways to not have the instance active. Each of them has its own value. The APS instance is active/up and running only when the state is Active. If the Operational state is not Active, then the remaining fields are invalid. The possible values of this field are:
    - Administratively disabled: Instance is inactive because it is administratively disabled.
    - Active: The instance is active and up and running.
    - Internal Error: Instance is inactive because an internal error has occurred.
    - Working MEP not Found: Instance is inactive because the Working MEP is not found.
    - Protecting MEP not Found: Instance is inactive because the Protecting MEP is not found.
    - Working MEP is not administrative active: Instance is inactive because the Working MEP is not admin enabled.

- Protecting MEP is not administrative active: Instance is inactive because the Protecting MEP is not admin enabled.
- Working MEP is not a Down MEP: Instance is inactive because the Working MEP is not a Down-MEP.
- Protecting MEP is not a Down MEP: Instance is inactive because the Protecting MEP is not a Down-MEP.
- Working and Protecting MEP use the same interface: Instance is inactive because both Working, and Protecting MEPs use the same I/F.
- Another instance uses the same Working port: Instance is inactive because another instance uses the same Working port.
- Warning: If the operational state is Active, the APS instance is active, but it might not run as the administrator thinks because of configuration errors. These errors are reflected in the following warnings. The Warning information is indicated by ●: no warning, ●: warning. Use the tooltip to get the detailed warning information.
- Protection: The possible protection group states. The letters refer to the state as described in G.8031 Annex.
  - No request Working: A.
  - No request Protecting: B.
  - Lockout: C.
  - Forced Switch: D.
  - Signal fail Working: E.
  - Signal fail Protecting: F.
  - Manual switch to Protecting: G.
  - Manual switch to Working: H.
  - Wait to restore: I.
  - Do not revert: J.
  - Exercise Working: K.
  - Exercise Protecting: L.
  - Reverse request Working: M.
  - Reverse request Protecting: N.
  - Signal degrade Working: P.
  - Signal degrade Protecting: Q.
- **Defect State:**
  - Working
    - Ok: The port defect state is OK
    - Sd: The port defect state is Signal Degrade
    - Sf: The port defect state is Signal Fail
  - Protection
    - Ok: The port defect state is OK
    - Sd: The port defect state is Signal Degrade
    - Sf: The port defect state is Signal Fail
- **TxAps:**
  - Request: The possible transmitted APS request according to G.8031, Table 11-1.
    - Nr: No Request.
    - Dnr: Do Not Revert.
    - Rr: Reverse Request.
    - Exer: Exercise.
    - Wtr: Wait-To-Restore.
    - Ms: Manual Switch.
    - Sd: Signal Degrade.
    - sfW: Signal Fail for Working.
    - Fs: Forced Switch.

- sfP: Signal Fail for Protect.
- Lo: Lockout.
- ReSignal: Transmitted requested signal according to G.8031 figure 11-2.
- BrSignal: Transmitted bridged signal according to G.8031 figure 11-2.
- **RxAps:**
  - Request: The possible received APS request according to G.8031, Table 11-1.
    - Nr: No Request.
    - Dnr: Do Not Revert.
    - Rr: Reverse Request.
    - Exer: Exercise.
    - Wtr: Wait-To-Restore.
    - Ms: Manual Switch.
    - Sd: Signal Degrade.
    - sfW: Signal Fail for Working.
    - Fs: Forced Switch.
    - sfP: Signal Fail for Protect.
    - Lo: Lockout.
  - ReSignal: Received requested signal according to G.8031 figure 11–2.
  - BrSignal: Received bridged signal according to G.8031 figure 11–2.
- **Dfop:** Dfop is Failure of Protocol defect. The presence of a defect is indicated by: ● no defect, ● defect.
  - CM: Configuration Mismatch (received APS PDU on working interface within last 17.5 seconds).
  - PM: Provisioning Mismatch (far and near ends are not using the same mode; bidir only).
  - NR: No Response (far end has not agreed on Requested Signal within 50 ms; bidir only).
  - TO: Time Out (near end has not received a valid APS PDU within last 17.5 seconds; bidir only).
- - SMAC: Source MAC address of last received APS PDU or all-zeros if no PDU has been received.
  - TxCnt: Number of APS PDU frames transmitted.
  - RxCnt:
    - Valid: Number of valid APS PDU frames received on the protect port.
    - Invalid: Number of invalid APS PDU frames received on the protect port.

## 5.6 Monitor ERPS

This page shows the status of the ERPS instances.

**Figure 5-17. ERPS Status**

ERPS Status

ERPS #	Oper	Warning	State	TxRapsActive	cFOPTo	Tx Info						
						UpdateTimeSecs	Request	Version	Rb	Dnf	Bpr	Node Id
No entry exists												

- **ERPS #:** The ID of the ERPS. Click on link to get to ERPS detailed instance page, you can reset counters and issue commands.
- **Oper:** The operational state of ERPS instance.
  - ●: Active.
  - ●: Disabled or Internal error.
- **Warning:** Operational warnings of ERPS instance.
  - ●: Active.
  - ●: Disabled or Internal error.
- **State:** Specifies protection/node state of ERPS.
- **TxRapsActive:** Specifies whether we are currently supposed to be transmitting R-APS PDUs on our ring ports.
- **cFOPTo:** Failure of Protocol:R-APS Rx Time Out.



- **Tx Info:**
  - UpdateTimeSecs: Time in seconds since boot that this structure was last updated.
  - Request: Request/state according to G.8032, table 10-3.
  - Version: Version of received/used R-APS Protocol. 0 means v1, 1 means v2, and so on
  - Rb: RB (RPL blocked) bit of R-APS info. See figure 10-3 of G.8032.
  - Dnf: DNF (Do Not Flush) bit of R-APS info. See figure 10-3 of G.8032.
  - Bpr: BPR (Blocked Port Reference) of R-APS info. See figure 10-3 of G.8032.
  - Node ID: Node ID of this request.
  - SMAC: The Source MAC address used in the request/state.

## 5.7 Monitor DHCPv4

This page shows the status of the DHCPv4 instances.

### 5.7.1 Monitor DHCPv4 Snooping Table

This page displays the dynamic IP assigned information after DHCP Snooping mode is disabled. All DHCP clients obtained the dynamic IP address from the DHCP server are listed in this table except for local VLAN interface IP addresses. Entries in the Dynamic DHCP snooping table are shown on this page. Each page shows up to 99 entries from the Dynamic DHCP snooping table, default being 20, selected through the **entries per page** input field. When first visited, the web page shows the first 20 entries from the beginning of the Dynamic DHCP Snooping table. The **MAC address** and **VLAN** input fields allow you to select the starting point in the Dynamic DHCP snooping table.

Figure 5-18. Dynamic DHCP Snooping Table

**Dynamic DHCP Snooping Table**

Start from MAC address  , VLAN  with  entries per page.

MAC Address	VLAN ID	Source Port	IP Address	IP Subnet Mask	DHCP Server
No more entries					

- **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 Address:** DHCP Server address of the entry.

### 5.7.2 Monitor DHCPv4 Detailed Statistics

This page provides statistics for DHCP snooping.

**Note:** The normal forward per-port TX statistics is not increased if the incoming DHCP packet is done by L3 forwarding mechanism. Clearing the statistics on specific port may not take effect on global statistics as it gathers the different layer overview.

Figure 5-19. DHCP Detailed Statistics

DHCP Detailed Statistics Port 6

Receive Packets		Transmit Packets	
Rx Discover	0	Tx Discover	0
Rx Offer	0	Tx Offer	0
Rx Request	0	Tx Request	0
Rx Decline	0	Tx Decline	0
Rx ACK	0	Tx ACK	0
Rx NAK	0	Tx NAK	0
Rx Release	0	Tx Release	0
Rx Inform	0	Tx Inform	0
Rx Lease Query	0	Tx Lease Query	0
Rx Lease Unassigned	0	Tx Lease Unassigned	0
Rx Lease Unknown	0	Tx Lease Unknown	0
Rx Lease Active	0	Tx Lease Active	0
Rx Discarded Checksum Error	0		
Rx Discarded from Untrusted	0		

Combined  
Combined  
Normal Forward  
Server  
Client  
Snooping  
Relay



- **Rx and Tx Discover:** The number of discover (option 53 with value 1) packets received and transmitted.
- **Rx and Tx Offer:** The number of offer (option 53 with value 2) packets received and transmitted.
- **Rx and Tx Request:** The number of request (option 53 with value 3) packets received and transmitted.
- **Rx and Tx Decline:** The number of decline (option 53 with value 4) packets received and transmitted.
- **Rx and Tx Ack:** The number of ACK (option 53 with value 5) packets received and transmitted.
- **Rx and Tx NAK:** The number of NAK (option 53 with value 6) packets received and transmitted.
- **Rx and Tx Release:** The number of release (option 53 with value 7) packets received and transmitted.
- **Rx and Tx Inform:** The number of inform (option 53 with value 8) packets received and transmitted.
- **Rx and Tx Lease Query:** The number of lease query (option 53 with value 10) packets received and transmitted.
- **Rx and Tx Lease Unassigned:** The number of lease unassigned (option 53 with value 11) packets received and transmitted.
- **Rx and Tx Unknown:** The number of lease unknown (option 53 with value 12) packets received and transmitted.
- **Rx and Tx Lease Active:** The number of lease active (option 53 with value 13) packets received and transmitted.
- **Rx Discarded checksum error:** The number of discard packet that IP/UDP checksum is error.
- **Rx Discarded from Untrusted:** The number of discarded packets coming from untrusted port.

## 5.8 Monitor DHCPv6

This page shows the status of the DHCPv6 instances.

### 5.8.1 Monitor DHCPv6 Snooping Table

This page displays the content of the current DHCPv6 snooping table.

**Figure 5-20. DHCPv6 Snooping Table**

#### DHCPv6 Snooping Table

This table display the currently known DHCPv6 clients and their assigned addresses.

Total entries: 0

Client DUID	MAC Address	Ingress Port	IAID	VLAN ID	Assigned Address	Lease Time	DHCP Server Address
-------------	-------------	--------------	------	---------	------------------	------------	---------------------

- **DUID:** The DHCP Unique Identifier (DUID) for the client. DHCPv6 uses this value to uniquely identify a client host instead of just using the MAC address of one of its interface ports (as DHCPv4 does).
- **MAC Address:** The MAC address for the client interface port that sent the DHCPv6 message.
- **VLAN ID:** The VLAN ID which is used by the client messages.
- **Local Ingress Port:** The local port on the snooping switch where client messages are received.
- **DHCPv6 Server Address:** The IPv6 address of the DHCP server which assigned the address to the client.
- **IAID:** Each client may contain multiple interfaces and may request addresses for each of these in the same DHCPv6 message. The Identity Association ID (IAID) value uniquely identifies the interface in the scope of the client.
- **Assigned Address:** The address assigned to the interface identified by the IAID value.
- **Lease Time:** The lease time associated with the assigned address in seconds.

### 5.8.2 Monitor DHCPv6 Snooping Statistics

This page provides statistics for DHCPv6 snooping.

Figure 5-21. DHCPv6 Snooping Statistics

DHCPv6 Snooping Statistics

Receive Packets		Transmit Packets	
Rx Solicit	0	Tx Solicit	0
Rx Request	0	Tx Request	0
Rx InfoRequest	0	Tx InfoRequest	0
Rx Confirm	0	Tx Confirm	0
Rx Renew	0	Tx Renew	0
Rx Rebind	0	Tx Rebind	0
Rx Decline	0	Tx Decline	0
Rx Advertise	0	Tx Advertise	0
Rx Reply	0	Tx Reply	0
Rx Reconfigure	0	Tx Reconfigure	0
Rx Release	0	Tx Release	0
Rx DiscardUntrust	0		

- **General Receive and Transmit Packets:** The page contains both RX and TX counters for all known DHCPv6 message types. See the RFC 3315 for details on the various DHCPv6 message types.
- **RxDiscardUntrust:** This indicates the number of received DHCP server packets that have been discarded due to the port being untrusted.

## 5.9 Monitor Security

The following sections describe the Monitor security.

### 5.9.1 Monitor Security Access Management Statistics

This page provides statistics for access management.

Figure 5-22. Access Management Statistics

Access Management Statistics

Interface	Received Packets	Allowed Packets	Discarded Packets
HTTP	0	0	0
HTTPS	0	0	0
SNMP	0	0	0
TELNET	0	0	0
SSH	0	0	0

- **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.

### 5.9.2 Monitor Security Network

The following sections describe the Monitor Security networks.

#### 5.9.2.1 Monitor Security Network Port Security

The following sections describe the Monitor Security network port security.

##### 5.9.2.1.1 Monitor Security Network Port Security Overview

This page shows the Port Security status. Port Security may be configured both administratively and indirectly through other software modules—the so-called 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, then it is 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.

Figure 5-23. Port Security Switch Status

Port Security Switch Status

User Module Legend

User Module Name	Abbr
Port Security (Admin)	P
802.1X	8

Port Status

Clear	Port	Users	Violation Mode	State	MAC Count		
					Current	Violating	Limit
Clear	1	--	Disabled	Disabled	-	-	-
Clear	2	--	Disabled	Disabled	-	-	-
Clear	3	--	Disabled	Disabled	-	-	-
Clear	4	--	Disabled	Disabled	-	-	-
Clear	5	--	Disabled	Disabled	-	-	-
Clear	6	--	Disabled	Disabled	-	-	-

- **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. This is used in the Users column in the port status table.
- **Port Status:** The table has one row for each port on the switch and several columns, which are as follows:
  - Clear: Click to remove all dynamic MAC addresses on all VLANs on this port. The button is only clickable if number of secured MAC addresses is non:zero.
  - 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 if that module has enabled Port Security. A (-) 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.
  - Violation Mode: Shows the configured Violation Mode of the port. It can take one of four values:
    - Disabled Port Security is not administratively enabled on this port.
    - Protect: Port Security is administratively enabled in Protect mode.
    - Restrict: Port Security is administratively enabled in Restrict mode.
    - Shutdown: Port Security is administratively enabled in Shutdown mode.
  - 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 administratively enabled, and the limit is reached.
    - Shut down: The Port Security service is administratively enabled, and the port is shut down. No MAC addresses can be learned on the port until it is administratively re-opened by administratively taking the port down and then back up on the **Configuration > Ports** page. Alternatively, the switch may be booted or reconfigured Port Security-wise.
    - MAC Count (Current, Violating, and Limit): The three columns indicate the number of currently learned MAC addresses (forwarding as well as blocked), the number of violating MAC address (only counting in Restrict mode) 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 shows a dash (-). If Port Security is not administratively enabled on the port, then the Violating and Limit columns show a dash (-).

#### 5.9.2.1.2 Network Port Security Details

This page shows the MAC addresses secured by the Port Security module. Port Security may be configured both administratively and indirectly through other software modules—the user modules. When a user module has enabled port security on a port, then 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 is blocked until that user module decides otherwise.

**Note:** If you have added static or sticky MAC addresses, then they show up on this page only if Port Security is enabled on the interface to which they pertain.

**Figure 5-24. Port Security Port Status All Ports**

Port Security Port Status All Ports

Delete	Port	VLAN ID	MAC Address	Type	State	Age/Hold
No MAC addresses attached						

- **Delete:** Click to remove this MAC address from MAC address table. The button is only clickable if the entry type is Dynamic. Use the **Configuration > Security > Port Security > MAC Addresses** page to remove Static and Sticky entries.
- **Port:** If all ports are shown (can be selected through the drop-down box on the top right), this one shows the port to which the MAC address is bound.
- **VLAN ID and MAC Address:** The VLAN ID and MAC address that is seen on this port. If no MAC addresses are learned, a single row stating **No MAC addresses** attached is displayed.
- **Type:** Indicates the type of entry. Takes one of three values:
  - Dynamic: The entry is learned through learn frames coming to the Port Security module while the port in question is not in sticky mode.
  - Static: The entry is entered by the end-user through management. Entry is not subject to aging.
  - Sticky: When the port is in sticky mode, all entries that would otherwise have been learned as dynamic are learned as sticky. Sticky entries are part of the `running-config` and can therefore be saved to `startup-config`. An important aspect of sticky MAC addresses is that they survive link changes (in contrast to Dynamic, which is learned again). They also survive reboots if running-config is saved to `startup-config`.
- **State:** Indicates whether the corresponding MAC address is violating (administrative user has configured the interface in the Restrict mode and the MAC address is blocked), blocked, or forwarding.
- **Age/Hold:** If at least one user module has decided to block this MAC address, it stays 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, then the Port Security module periodically checks that this MAC address still forwards traffic. If the age period (measured in seconds) expires and no frames have been seen, then the MAC address is removed from the MAC address table. Otherwise, a new age period begins. If aging is disabled or a user module has decided to hold the MAC address indefinitely, a dash (-) is shown.

### 5.9.2.2 Monitor Security Network NAS

The following sections describe the Monitor Security Network NAS.

#### 5.9.2.2.1 Monitor Security Network NAS Switch

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

**Figure 5-25. Network Access Server Switch Status**

Network Access Server Switch Status

Port	Admin State	Port State	Last Source	Last ID	QoS Class	Port VLAN ID
1	Force Authorized	Globally Disabled			-	
2	Force Authorized	Globally Disabled			-	
3	Force Authorized	Globally Disabled			-	
4	Force Authorized	Globally Disabled			-	
5	Force Authorized	Globally Disabled			-	
6	Force Authorized	Globally Disabled			-	

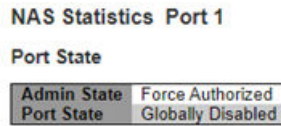
- **Port:** The switch port number. Click to navigate to detailed NAS statistics for this port.
- **Admin State:** The port's current administrative state. See NAS [Admin State](#) for a description of possible values.
- **Port State:** The current state of the port. See NAS [Port State](#) for a description 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 username (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 has put the 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. If the port is moved to the Guest VLAN, **Guest** is appended to the VLAN ID.

### 5.9.2.2.2 Monitor Security Network NAS Port

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.

Figure 5-26. NAS Statistics



- **Port State**
  - **Admin State:** The port's current administrative state. Refer to NAS Admin State for a description of possible values.
  - **Port State:** The current state of the port. Refer to NAS Port State for a description of the individual states.
  - **QoS:** The QoS class assigned by the RADIUS server. The field is blank if no QoS class is assigned.
  - **Port VLAN ID:** The VLAN ID that NAS has put the 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. If the port is moved to the Guest VLAN, **Guest** is appended to the VLAN ID.
- **Port Counters**
  - **EAPOL Counters:** These supplicant frame counters are available for the following administrative states:
    - Force Authorized
    - Force Unauthorized
    - Port-based 802.1X
    - Single 802.1X
    - Multi 802.1X

Figure 5-27. EAPOL Counters

EAPOL Counters			
Direction	Name	IEEE Name	Description
Rx	Total	dot1xAuthEapolFramesRx	The number of valid EAPOL frames of any type that have been received by the switch.
Rx	Response ID	dot1xAuthEapolRespIdFramesRx	The number of valid EAPOL Response Identity frames that have been received by the switch.
Rx	Responses	dot1xAuthEapolRespFramesRx	The number of valid EAPOL response frames (other than Response Identity frames) that have been received by the switch.
Rx	Start	dot1xAuthEapolStartFramesRx	The number of EAPOL Start frames that have been received by the switch.
Rx	Logoff	dot1xAuthEapolLogoffFramesRx	The number of valid EAPOL Logoff frames that have been received by the switch.
Rx	Invalid Type	dot1xAuthInvalidEapolFramesRx	The number of EAPOL frames that have been received by the switch in which the frame type is not recognized.
Rx	Invalid Length	dot1xAuthEapolLengthErrorFramesRx	The number of EAPOL frames that have been received by the switch in which the Packet Body Length field is invalid.
Tx	Total	dot1xAuthEapolFramesTx	The number of EAPOL frames of any type that have been transmitted by the switch.
Tx	Request ID	dot1xAuthEapolReqIdFramesTx	The number of EAPOL Request Identity frames that have been transmitted by the switch.
Tx	Requests	dot1xAuthEapolReqFramesTx	The number of valid EAPOL Request frames (other than Request Identity frames) that have been transmitted by the switch.

- **Backend Server Counters:** This backend (RADIUS) frame counters are available for the following administrative states:
  - Port-based 802.1X
  - Single 802.1X
  - Multi 802.1X
  - MAC-based Auth.

Figure 5-28. Backend Server Counters

Backend Server Counters			
Direction	Name	IEEE Name	Description
Rx	Access Challenges	dot1xAuthBackendAccessChallenges	802.1X based: Counts the number of times that the switch receives the first request from the backend server following the first response from the supplicant. Indicates that the backend server has communication with the switch. MAC based: Counts all Access Challenges received from the backend server for this port (left-most table) or client (right-most table).
Rx	Other Requests	dot1xAuthBackendOtherRequestsToSupplicant	802.1X based: Counts the number of times that the switch sends an EAP Request packet following the first to the supplicant. Indicates that the backend server chose an EAP method. MAC based: Not applicable.
Rx	Auth. Successes	dot1xAuthBackendAuthSuccesses	802.1X and MAC based: Counts the number of times that the switch receives a success indication. Indicates that the supplicant/client has successfully authenticated to the backend server.
Rx	Auth. Failures	dot1xAuthBackendAuthFails	802.1X and MAC based: Counts the number of times that the switch receives a failure message. This indicates that the supplicant/client has not authenticated to the backend server.
Tx	Responses	dot1xAuthBackendResponses	802.1X based: Counts the number of times that the switch attempts to send a supplicant's first response packet to the backend server. Indicates the switch attempted communication with the backend server. Possible retransmissions are not counted. MAC based: Counts all the backend server packets sent from the switch towards the backend server for a given port (left-most table) or client (right-most table). Possible retransmissions are not counted.

- **Last Supplicant/Client Info:** Information about the last supplicant/client that attempted to authenticate. This information is available for the following administrative states:
  - Port-based 802.1X



- Single 802.1X
- Multi 802.1X
- MAC-based Auth.

**Figure 5-29. Last Supplicant/Client Info**

Last Supplicant/Client Info		
Name	IEEE Name	Description
MAC Address	dot1xAuthLastEapolFrameSource	The MAC address of the last supplicant/client.
VLAN ID	-	The VLAN ID on which the last frame from the last supplicant/client was received. 802.1X-based:
Version	dot1xAuthLastEapolFrameVersion	The protocol version number carried in the most recently received EAPOL frame. MAC-based: Not applicable.
Identity	-	802.1X-based: The user name (supplicant identity) carried in the most recently received Response Identity EAPOL frame. MAC-based: Not applicable.

- **Selected Counters:** The Selected Counters table is visible when the port is in one of the following administrative states:
  - **Multi 802.1X**
  - **MAC-based Auth.**  
The table is identical to and is placed next to the Port Counters table, and will be empty if no MAC address is currently selected.
- **Attached MAC Addresses**
  - **Identity:** Shows the identity of the supplicant, as received in the Response Identity EAPOL frame. Clicking the link causes the supplicant's EAPOL and Backend Server counters to be shown in the Selected Counters table. If no supplicants are attached, it shows *No supplicants attached*. This column is not available for MAC-based Auth.
  - **MAC Address:** For Multi 802.1X, this column holds the MAC address of the attached supplicant. For MAC-based Auth., this column holds the MAC address of the attached client. Clicking the link causes the client's Backend Server counters to be shown in the Selected Counters table. If no clients are attached, it shows No clients attached.
  - **VLAN ID:** This column holds the VLAN ID that the corresponding client is currently secured through the Port Security module.
  - **State:** The client can either be authenticated or unauthenticated. In the authenticated state, it is allowed to forward frames on the port, and in the unauthenticated state, it is blocked. If the backend server hasn't successfully authenticated the client, it is unauthenticated. If an authentication fails for one or the other reason, the client will remain in the unauthenticated state for Hold Time seconds.
  - **Last Authentication:** Shows the date and time of the last authentication of the client (successful as well as unsuccessful).

### 5.9.2.3 Monitor Security Network 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 128 on each switch.

- **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: ACE matches any frame type.
  - EType: ACE matches Ethernet Type frames.  
**Note:** An Ethernet Type based ACE does not get matched by IP and ARP frames.
  - ARP: ACE matches ARP/RARP frames.
  - IPv4: ACE matches all IPv4 frames.
  - IPv4/ICMP: ACE matches IPv4 frames with ICMP protocol.
  - IPv4/UDP: ACE matches IPv4 frames with UDP protocol.
  - IPv4/TCP: ACE matches IPv4 frames with TCP protocol.
  - IPv4/Other: ACE matches IPv4 frames, which are not ICMP/UDP/TCP.
  - IPv6: ACE matches 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.
- **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.

#### 5.9.2.4 Monitor Security Network ARP Inspection

Entries in the Dynamic ARP Inspection Table are shown on this page. The Dynamic ARP Inspection Table contains up to 256 entries, and is sorted first by port, then by VLAN ID, then by MAC address, and then by IP address. All dynamic entries are learning from DHCP Snooping.

Figure 5-30. Dynamic ARP Inspection Table

Dynamic ARP Inspection Table

Start from  , VLAN  , MAC address  and IP address  with  entries per page.

Port	VLAN ID	MAC Address	IP Address
No more entries			

- **Port:** Switch Port Number for which the entries are displayed.
- **VLAN ID:** VLAN-ID in which the ARP traffic is permitted.
- **MAC Address:** User MAC address of the entry.
- **IP Address:** User IP address of the entry.

#### 5.9.2.5 Monitor Security Network IP Source Guard

Entries in the Dynamic IP Source Guard Table are shown on this page. The Dynamic IP Source Guard Table is sorted first by port, then by VLAN ID, then by IP address, and then by MAC address.

Figure 5-31. IP Source Guard

Dynamic IP Source Guard Table

Start from  , VLAN  and IP address  with  entries per page.

Port	VLAN ID	IP Address	MAC Address
No more entries			

- **Port:** Switch Port Number for which the entries are displayed.
- **VLAN ID:** VLAN-ID in which the IP traffic is permitted.
- **IP Address:** User IP address of the entry.
- **MAC Address:** Source MAC address.

#### 5.9.2.6 Monitor Security Network IPv6 Source Guard

Entries in the Dynamic IPv6 Source Guard Table are shown on this page.

Figure 5-32. IPv6 Source Guard Dynamic Table

IPv6 Source Guard Dynamic Table

Port	VLAN ID	IPv6 Address	MAC Address
------	---------	--------------	-------------

- **Port:** Switch Port Number to which the entries are bound.
- **VLAN ID:** VLAN-ID in which the IP traffic is permitted. If no VLAN-ID is associated with the entry, this field shows 0.
- **IPv6 Address:** Source IPv6 address of the entry.
- **MAC Address:** Source MAC address.



### 5.9.3 Monitor Security AAA

The following sections describe the Monitor Security AAA.

#### 5.9.3.1 Monitor Security AAA RADIUS Overview

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

**Figure 5-33. RADIUS Server Status Overview**

RADIUS Server Status Overview

#	IP Address	Authentication Port	Authentication Status	Accounting Port	Accounting Status
1			Disabled		Disabled
2			Disabled		Disabled
3			Disabled		Disabled
4			Disabled		Disabled
5			Disabled		Disabled

- **#:** 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:** UDP port number for accounting.
- **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.

#### 5.9.3.2 Monitor Security AAA RADIUS Details

This page provides detailed statistics for a particular RADIUS server. The statistics map closely to those specified in RFC4668—RADIUS Authentication Client MIB.

Figure 5-34. RADIUS Authentication Statistics

RADIUS Authentication Statistics for Server #1

Receive Packets		Transmit Packets	
Access Accepts	0	Access Requests	0
Access Rejects	0	Access Retransmissions	0
Access Challenges	0	Pending Requests	0
Malformed Access Responses	0	Timeouts	0
Bad Authenticators	0		
Unknown Types	0		
Packets Dropped	0		
Other Info			
IP Address			
State		Disabled	
Round-Trip Time		0 ms	

RADIUS Accounting Statistics for Server #1

Receive Packets		Transmit Packets	
Responses	0	Requests	0
Malformed Responses	0	Retransmissions	0
Bad Authenticators	0	Pending Requests	0
Unknown Types	0	Timeouts	0
Packets Dropped	0		
Other Info			
IP Address			
State		Disabled	
Round-Trip Time		0 ms	

- **RADIUS Authentication Packet Statistics:** For RADIUS authentication server packet counter, there are seven receive and four transmit counters.

Figure 5-35. Authentication Packet Counters

Direction	Name	RFC4668 Name	Description
Rx	Access Accepts	radiusAuthClientExtAccessAccepts	The number of RADIUS Access-Accept packets (valid or invalid) received from the server.
Rx	Access Rejects	radiusAuthClientExtAccessRejects	The number of RADIUS Access-Reject packets (valid or invalid) received from the server.
Rx	Access Challenges	radiusAuthClientExtAccessChallenges	The number of RADIUS Access-Challenge packets (valid or invalid) received from the server.
Rx	Malformed Access Responses	radiusAuthClientExtMalformedAccessResponses	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.
Rx	Bad Authenticators	radiusAuthClientExtBadAuthenticators	The number of RADIUS Access-Response packets containing invalid authenticators or Message Authenticator attributes received from the server.
Rx	Unknown Types	radiusAuthClientExtUnknownTypes	The number of RADIUS packets that were received with unknown types from the server on the authentication port and dropped.
Rx	Packets Dropped	radiusAuthClientExtPacketsDropped	The number of RADIUS packets that were received from the server on the authentication port and dropped for some other reason.
Tx	Access Requests	radiusAuthClientExtAccessRequests	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.

- **RADIUS Authentication Other Info:** This section contains information about the state of the server and the latest round-trip time.

Figure 5-36. RADIUS Authentication Statistics—Other Info

Name	RFC4668 Name	Description
IP Address	-	IP address and UDP port for the authentication server in question.
State	-	Shows the state of the server. It takes one of the following values: <b>Disabled</b> : The selected server is disabled. <b>Not Ready</b> : The server is enabled, but IP communication is not yet up and running. <b>Ready</b> : The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept access attempts. <b>Dead (X seconds left)</b> : 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	radiusAuthClientExtRoundTripTime	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 Packet Statistics** - The statistics map closely to those specified in RFC4670 - RADIUS Accounting Client MIB.

Figure 5-37. RADIUS Accounting Packet Statistics

Direction	Name	RFC4670 Name	Description
Rx	Responses	radiusAccClientExtResponses	The number of RADIUS packets (valid or invalid) received from the server.
Rx	Malformed Responses	radiusAccClientExtMalformedResponses	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 malformed access responses.
Rx	Bad Authenticators	radiusAccClientExtBadAuthenticators	The number of RADIUS packets containing invalid authenticators received from the server.
Rx	Unknown Types	radiusAccClientExtUnknownTypes	The number of RADIUS packets of unknown types that were received from the server on the accounting port.
Rx	Packets Dropped	radiusAccClientExtPacketsDropped	The number of RADIUS packets that were received from the server on the accounting port and dropped for some other reason.
Tx	Requests	radiusAccClientExtRequests	The number of RADIUS packets sent to the server. This does not include retransmissions.
Tx	Retransmissions	radiusAccClientExtRetransmissions	The number of RADIUS packets retransmitted to the RADIUS accounting server.
Tx	Pending Requests	radiusAccClientExtPendingRequests	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.
Tx	Timeouts	radiusAccClientExtTimeouts	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.

- **RADIUS Accounting Other Information:** This section contains information about the state of the server and the latest round-trip time.

Figure 5-38. RADIUS Accounting Statistics—Other Info

Name	RFC4670 Name	Description
IP Address	-	IP address and UDP port for the accounting server in question.
State	-	Shows the state of the server. It takes one of the following values: <b>Disabled</b> : The selected server is disabled. <b>Not Ready</b> : The server is enabled, but IP communication is not yet up and running. <b>Ready</b> : The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept accounting attempts. <b>Dead (X seconds left)</b> : 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.
Round-Trip Time	radiusAccClientExtRoundTripTime	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.

## 5.9.4 Monitor Security Switch

The following sections describe the Monitor Security switches.

### 5.9.4.1 Monitor Security Switch RMON

This section describes the Monitor Security switch RMON.

#### 5.9.4.1.1 Monitor Security Switch RMON Statistics

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. At the first visit, the web page shows the



first 20 entries from the beginning of the Statistics table. The first displayed are the ones with the lowest ID found in the Statistics table.

**Figure 5-39. RMON Statistics Status Overview**

RMON Statistics Status Overview

Start from Control Index  with  entries per page.

ID	Data Source (ifindex)	Drop	Octets	Pkts	Broad-cast	Multi-cast	CRC Errors	Under-size	Over-size	Frag.	Jabb.	Coll.	64 Bytes	65 ~ 127	128 ~ 255	256 ~ 511	512 ~ 1023	1024 ~ 1588
No more entries																		

- **ID:** Indicates the index of Statistics entry.
- **Data Source(ifindex):** The port ID which wants to be monitored.
- **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.
- **Pkts:** 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:** The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
- **Undersize:** The total number of packets received that were less than 64 octets.
- **Oversize:** 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.
- **64 Byte:** The total number of packets (including bad packets) received that were 64 octets in length.
- **65-127 Byte:** The total number of packets (including bad packets) received that were between 65 to 127 octets in length.
- **128-255 Byte:** The total number of packets (including bad packets) received that were between 128 to 255 octets in length.
- **256-511 Byte:** The total number of packets (including bad packets) received that were between 256 to 511 octets in length.
- **512-1023 Byte:** The total number of packets (including bad packets) received that were between 512 to 1023 octets in length.
- **1024-1588 Byte:** The total number of packets (including bad packets) received that were between 1024 to 1588 octets in length.

**5.9.4.1.2 Monitor Security Switch RMON History**

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.

**Figure 5-40. RMON History Overview**

RMON History Overview

Start from Control Index  and Sample Index  with  entries per page.

History Index	Sample Index	Sample Start	Drop	Octets	Pkts	Broad-cast	Multi-cast	CRC Errors	Under-size	Over-size	Frag.	Jabb.	Coll.	Utilization
No more entries														

- **History Index:** Indicates the index of History control entry.
- **Sample Index:** Indicates the index of the data entry associated with the control entry.
- **Sample Start:** The value of sysUpTime at the start of the interval over which this sample was measured.
- **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.

- **Pkts:** 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.
- **CRCErrors:** The total number of packets received that had a length (excluding framing bits but including FCS octets) of between 64 and 1518 octets, inclusive, but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
- **Undersize:** The total number of packets received that were less than 64 octets.
- **Oversize:** 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.

### 5.9.4.1.3 Monitor Security Switch RMON Alarm

This page provides an overview of RMON Alarm 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 Alarm table. The first displayed will be the one with the lowest ID found in the Alarm table.

Figure 5-41. RMON Alarm Overview

RMON Alarm Overview

Start from Control Index  with  entries per page.

ID	Interval	Variable	Sample Type	Value	Startup Alarm	Rising Threshold	Rising Index	Falling Threshold	Falling Index
No more entries									

- **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 variable to be sampled.
- **Sample Type:** The method of sampling the selected variable and calculating the value to be compared against the thresholds.
- **Values:** 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.

### 5.9.4.1.4 Monitor Security Switch RMON Event

This page provides an overview of RMON Event table 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.

Figure 5-42. RMON Event Overview

RMON Event Overview

Start from Control Index  and Sample Index  with  entries per page.

Event Index	LogIndex	LogTime	LogDescription
No more entries			

- **Event Index:** Indicates the index of the event entry.
- **Log Index:** Indicates the index of the log entry.
- **Log Time:** Indicates Event log time.

- **LogDescription:** Indicates the Event description.

## 5.10 Monitor Aggregation

The following sections describe the Monitor Aggregation.

### 5.10.1 Monitor Aggregation Status

This page is used to see the status of ports in Aggregation group.

Figure 5-43. Aggregation Status

Aggr ID	Name	Type	Speed	Configured Ports	Aggregated Ports
No aggregation groups					

- **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.

### 5.10.2 Monitor Aggregation LACP

The following sections describe the Monitor Aggregation LACP.

#### 5.10.2.1 Monitor Aggregation LACP System Status

This page provides a status overview for the system-level LACP information.

Figure 5-44. LACP System Status

#### LACP System Status

##### Local System ID

Priority	MAC Address
32768	00-de-fd-ae-17-78

##### Partner System Status

Aggr ID	Partner System ID	Partner Prio	Partner Key	Last Changed	Local Ports
No ports enabled or no existing partners					

- **Aggr ID:** The Aggregation ID associated with this aggregation instance.
- **Partner System ID:** The system ID (MAC address) of the aggregation partner.
- **Partner Prio:** The priority that the partner has assigned to this aggregation ID.
- **Partner Key:** The Key that the partner has assigned to this aggregation ID.
- **Last Changed:** The time since this aggregation changed.
- **Local Ports:** Shows which ports are a part of this aggregation for this switch.

#### 5.10.2.2 Monitor Aggregation LACP Internal Status

This page provides a status overview for the LACP internal (that is, the local system) status for all ports. Only ports that are part of an LACP group are shown. For details on the shown parameters, see the IEEE 801.AX-2014.

Figure 5-45. LACP Internal Port Status

Port	State	Key	Priority	Activity	Timeout	Aggregation	Synchronization	Collecting	Distributing	Defaulted	Expired
No LACP ports enabled											

- **Port:** The switch port number.
- **State:** The current port state:
  - Down: The port is not active.
  - Active: The port is in active state.

- Standby: The port is in standby state.
- **Key:** The key assigned to this port. Only ports with the same key can aggregate together.
- **Priority:** The priority assigned to this aggregation group.
- **Activity:** The LACP mode of the group (Active or Passive).
- **TimeOut:** The timeout mode configured for the port (Fast or Slow).
- **Aggregation:** Show whether the system considers this link to be **aggregateable**; that is, a potential candidate for aggregation.
- **Synchronization:** Show whether the system considers this link to be **IN\_SYNC**; that is, it has been allocated to the correct LAG, the group has been associated with a compatible Aggregator, and the identity of the LAG is consistent with the System ID and operational Key information transmitted.
- **Collecting:** Show if collection of incoming frames on this link is enabled.
- **Distributing:** Show if distribution of outgoing frames on this link is enabled.
- **Defaulted:** Show if the Actor's Receive machine is using Defaulted operational Partner information.
- **Expired:** Show if that the Actor's Receive machine is in the EXPIRED state.

### 5.10.2.3 Monitor Aggregation LACP Neighbor Status

This page provides a status overview for the LACP neighbor status for all ports. Only ports that are part of an LACP group are shown. For details on the shown parameters, see the IEEE 801.AX-2014.

Figure 5-46. LACP Neighbor Status

Port	State	Aggr ID	Partner Key	Partner Port	Partner Port Prio	Activity	Timeout	Aggregation	Synchronization	Collecting	Distributing	Defaulted	Expired
No LACP neighbor status available													

- **Port:** The switch port number.
- **State:** The current port state:
  - Down: The port is not active.
  - Active: The port is in active state.
  - Standby: The port is in standby state.
- **Aggr ID:** The aggregation group ID which the port is assigned to.
- **Partner Key:** The key assigned to this port by the partner.
- **Partner Port:** The partner port number associated with this link.
- **Partner Port Priority:** The priority assigned to this partner port.
- **Activity:** The LACP mode of the group (Active or Passive).
- **Timeout:** The timeout mode configured for the partner port (Fast or Slow).
- **Aggregation:** Show whether the partner considers this link to be **aggregateable**; that is, a potential candidate for aggregation.
- **Synchronization:** Show whether the partner considers this link to be **IN\_SYNC**; that is, it has been allocated to the correct LAG, the group has been associated with a compatible Aggregator, and the identity of the LAG is consistent with the System ID and operational Key information transmitted.
- **Collecting:** Show if collection of incoming frames on this link is enabled.
- **Distributing:** Show if distribution of outgoing frames on this link is enabled.
- **Defaulted:** Show if the partners Receive machine is using Defaulted operational Partner information.
- **Expired:** Show if that the partners Receive machine is in the EXPIRED state.

### 5.10.2.4 Monitor Aggregation LACP Port Statistics

This page provides an overview for LACP statistics for all ports.

Figure 5-47. LACP Statistics

Port	LACP		Discarded	
	Received	Transmitted	Unknown	Illegal
No ports enabled				

- **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.

## 5.11 Monitor Loop Protection

This page displays the loop protection port status the ports of the switch.

Figure 5-48. Loop Protection Status

Port	Action	Transmit	Loops	Status	Loop	Time of Last Loop
No ports enabled						

- **Port:** The switch port number of the logical port.
- **Action:** The currently configured port action.
- **Transmit:** The currently configured port transmit mode.
- **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.

## 5.12 Monitor Spanning Tree

The following sections describe the Monitor Spanning Tree configurations.

### 5.12.1 Monitor Spanning Tree Bridge Status

This page provides a status overview of all STP bridge instances.

Figure 5-49. STP Bridges

MSTI	Bridge ID	Root			Topology Flag	Topology Change Last
		ID	Port	Cost		
CIST	32768-00-DE-FD-AE-17-78	32768-00-59-88-44-AD-14	6	20000	Steady	3d 08:09:43

- **MSTI:** The Bridge Instance. This is also a link to the STP Detailed Bridge Status.
- **Bridge ID:** The Bridge ID of this Bridge instance.
- **Root ID:** The Bridge ID of the currently elected root bridge.
- **Root Port:** The switch port currently assigned the *root* port role.
- **Root Cost:** Root Path Cost. For the Root Bridge it is zero. For all other Bridges, it is the sum of the Port Path Costs on the least cost path to the Root Bridge.
- **Topology Flag:** The current state of the Topology Change Flag of this Bridge instance.
- **Topology Change Last:** The time since last Topology Change occurred.

### 5.12.2 Monitor Spanning Tree Port Status

This page displays the STP CIST port status for physical ports of the switch.

Figure 5-50. STP Port Status

Port	CIST Role	CIST State	Uptime
1	Disabled	Discarding	-
2	Disabled	Discarding	-
3	Disabled	Discarding	-
4	Disabled	Discarding	-
5	Disabled	Discarding	-
6	RootPort	Forwarding	3d 08:14:21

- **Port:** The switch port number of the logical STP port.
- **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, and Disabled.
- **CIST State:** The current STP port state of the CIST port. The port state can be one of the following values: Discarding, Learning, and Forwarding.

- **Uptime:** The time since the bridge port was last initialized.

### 5.12.3 Monitor Spanning Tree Port Statistics

This page displays the STP port statistics counters of bridge ports in the switch.

Figure 5-51. STP Statistics

Port	Transmitted				Received				Discarded	
	MSTP	RSTP	STP	TCN	MSTP	RSTP	STP	TCN	Unknown	Illegal
6	6	0	0	0	144441	0	0	0	0	0

- **Port:** The switch port number of the logical STP port.
- **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.

## 5.13 Monitor LLDP

The following sections describe the Monitor LLDPs.

### 5.13.1 Monitor LLDP Neighbors

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.

Figure 5-52. LLDP Neighbor Information

#### LLDP Neighbor Information

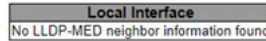
LLDP Remote Device Summary						
Local Interface	Chassis ID	Port ID	Port Description	System Name	System Capabilities	Management Address
No neighbor information found						

- **Local Interface:** The interface on which the LLDP frame was received.
  - **Chassis ID:** The Chassis ID is the identification of the neighbor's LLDP frames.
  - **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:
    - Other
    - Repeater
    - Bridge
    - WLAN Access Point
    - Router
    - Telephone
    - DOCSIS cable device
    - Station only
    - Reserved
- Note:** When a capability is enabled, the capability is followed by (+). If the capability is disabled, the capability 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 can, for example, hold the neighbor's IP address.

### 5.13.2 Monitor LLDP LLDP-MED Neighbors

This page provides a status overview of all LLDP-MED neighbors. The displayed table contains a row for each interface on which an LLDP neighbor is detected. This function applies to VoIP devices which support LLDP-MED.

**Figure 5-53. LLDP-MED Neighbor Information**



- **Interface:** The interface on which the LLDP frame was received.
- **Device Type:** LLDP-MED Devices are comprised of two primary device types: Network Connectivity Devices and Endpoint Devices.

**LLDP-MED Network Connectivity Device Definition:** LLDP-MED Network Connectivity Devices, as defined in TIA-1057, provide access to the IEEE 802 based LAN infrastructure for LLDP-MED Endpoint Devices. An LLDP-MED Network Connectivity Device is a LAN access device based on any of the following technologies:

- LAN Switch/Router
- IEEE 802.1 Bridge
- IEEE 802.3 Repeater (included for historical reasons)
- IEEE 802.11 Wireless Access Point
- Any device that supports the IEEE 802.1AB and MED extensions defined by TIA-1057 and can relay IEEE 802 frames via any method.

**LLDP-MED Endpoint Device Definition:** LLDP-MED Endpoint Devices, as defined in TIA-1057, are located at the IEEE 802 LAN network edge, and participate in IP communication service using the LLDP-MED framework. Within the LLDP-MED Endpoint Device category, the LLDP-MED scheme is broken into further Endpoint Device Classes, as defined in the following.

Each LLDP-MED Endpoint Device Class is defined to build upon the capabilities defined for the previous Endpoint Device Class. For-example will any LLDP-MED Endpoint Device claiming compliance as a Media Endpoint (Class II) also support all aspects of TIA-1057 applicable to Generic Endpoints (Class I), and any LLDP-MED Endpoint Device claiming compliance as a Communication Device (Class III) will also support all aspects of TIA-1057 applicable to both Media Endpoints (Class II) and Generic Endpoints (Class I).

**LLDP-MED Generic Endpoint (Class I):** The LLDP-MED Generic Endpoint (Class I) definition is applicable to all endpoint products that require the base LLDP discovery services defined in TIA-1057. However, they do not support IP media or act as an end-user communication appliance. Such devices may include (but are not limited to) IP Communication Controllers, other communication related servers, or any device requiring basic services as defined in TIA-1057.

Discovery services defined in this class include LAN configuration, device location, network policy, power management, and inventory management.

**LLDP-MED Media Endpoint (Class II):** The LLDP-MED Media Endpoint (Class II) definition is applicable to all endpoint products that have IP media capabilities however may or may not be associated with a particular end user. Capabilities include all the capabilities defined for the previous Generic Endpoint Class (Class I) and are extended to include aspects related to media streaming. Example product categories expected to adhere to this class include (but are not limited to) Voice/Media Gateways, Conference Bridges, Media Servers, and similar.

Discovery services defined in this class include media-type-specific network layer policy discovery.

**LLDP-MED Communication Endpoint (Class III):** The LLDP-MED Communication Endpoint (Class III) definition is applicable to all endpoint products that act as end user communication appliances supporting IP media. Capabilities include all the capabilities defined for the previous Generic Endpoint (Class I) and Media Endpoint (Class II) classes and are extended to include aspects related to end user devices. Example product categories expected to adhere to this class include (but are not limited to) end user communication appliances, such as IP Phones, PC-based softphones, or other communication appliances that directly support the end user.

Discovery services defined in this class include provision of location identifier (including ECS/E911 information), embedded L2 switch support, inventory management.

- **LLDP-MED Capabilities:** LLDP-MED Capabilities describes the neighbor unit's LLDP-MED capabilities. The possible capabilities are:
  - LLDP-MED capabilities

- Network Policy
- Location Identification
- Extended Power via MDI-PSE
- Extended Power via MDI-PD
- Inventory
- Reserved
- **Application Type:** Application Type indicating the primary function of the application(s) defined for this network policy, advertised by an Endpoint or Network Connectivity Device. The following are the possible application types:
  - Voice: for use by dedicated IP Telephony handsets and other similar appliances supporting interactive voice services. These devices are typically deployed on a separate VLAN for ease of deployment and enhanced security by isolation from data applications.
  - Voice Signaling: for use in network topologies that require a different policy for the voice signaling than for the voice media.
  - Guest Voice: to support a separate limited feature-set voice service for guest users and visitors with their own IP Telephony handsets and other similar appliances supporting interactive voice services.
  - Guest Voice Signaling: for use in network topologies that require a different policy for the guest voice signaling than for the guest voice media.
  - Softphone Voice: for use by softphone applications on typical data centric devices, such as PCs or laptops.
  - Video Conferencing: for use by dedicated Video Conferencing equipment and other similar appliances supporting real-time interactive video/audio services.
  - Streaming Video: for use by broadcast or multicast-based video content distribution and other similar applications supporting streaming video services that require specific network policy treatment. Video applications relying on TCP with buffering would not be an intended use of this application type.
  - Video Signaling: for use in network topologies that require a separate policy for the video signaling than for the video media.
- **Policy:** Policy indicates that an Endpoint Device wants to explicitly advertise that the policy is required by the device. Can be either Defined or Unknown
- **TAG:** TAG is indicative of whether the specified application type is using a tagged or an untagged VLAN. It can be Tagged or Untagged.
  - Untagged: The device is using an untagged frame format and as such does not include a tag header as defined by IEEE 802.1Q-2003.
  - Tagged: The device is using the IEEE 802.1Q tagged frame format.
- **VLAN ID:** VLAN ID is the VLAN identifier (VID) for the interface as defined in IEEE 802.1Q-2003. A value of 1 through 4094 is used to define a valid VLAN ID. A value of 0 (Priority Tagged) is used if the device is using priority tagged frames as defined by IEEE 802.1Q-2003, meaning that only the IEEE 802.1D priority level is significant and the default PVID of the ingress interface is used instead.
- **Priority:** Priority is the Layer 2 priority to be used for the specified application type. One of the eight priority levels (0 through 7).
- **DSCP:** DSCP is the DSCP value to be used to provide Diffserv node behavior for the specified application type as defined in IETF RFC 2474. Contain one of 64 code point values (0 through 63).
- **Auto-negotiation:** Auto-negotiation identifies if MAC/PHY auto-negotiation is supported by the link partner.
- **Auto-negotiation Status:** Auto-negotiation status identifies if auto-negotiation is currently enabled at the link partner. If Auto-negotiation is supported and Auto-negotiation status is disabled, then the 802.3 PMD operating mode is determined by the operational MAU type field value rather than by auto-negotiation.
- **Auto-negotiation Capabilities:** Auto-negotiation capabilities shows the link partners MAC/PHY capabilities.

### 5.13.3 Monitor LLDP PoE

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.

Figure 5-54. LLDP Neighbor PoE Information

Local Interface	Power Type	Power Source	Power Priority	Maximum Power
No PoE neighbor information found				

- **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**.
- **Power Source:** The Power Source represents the power source being utilized by a PSE or PD device. If the device is a PSE device, then 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 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.

### 5.13.4 Monitor LLDP EEE

By using EEE, power savings can be achieved at the expense of traffic latency. This latency occurs due to that the circuits EEE turn OFF to save power and need time to boot up before sending traffic over the link. This time is called wakeup time. To achieve minimal latency, devices can use LLDP to exchange information about their respective tx and rx wakeup time, to agree upon the minimum wakeup time they need.

If the interface does not support EEE, then it displays as **EEE not supported for this interface**. If EEE is not enabled on a particular interface, then it displays as **EEE not enabled for this interface**. If the link partner does not support EEE, then it displays as **Link partner is not EEE capable**.

Figure 5-55. LLDP Neighbors EEE Information

Local Interface	Tx Tw	Rx Tw	Fallback Receive Tw	Echo Tx Tw	Echo Rx Tw	Resolved Tx Tw	Resolved Rx Tw	EEE In Sync
No LLDP EEE Information found								

- **Local Interface:** The interface at which LLDP frames are received or transmitted.
- **Tx Tw:** The link partner's maximum time that transmit path can hold-off sending data after deassertion of LPI.
- **RxTw:** The link partner's time that receiver would like the transmitter to hold-off to allow time for the receiver to wake from sleep.
- **Fallback Received Tw:** The link partner's fallback receives Tw. A receiving link partner may inform the transmitter of an alternate desired Tw\_sys\_tx. As a receiving link partner might have discrete levels for savings, this provides the transmitter with additional information that it may use for a more efficient allocation. Systems that do not implement this option default the value to be the same as that of the Receive Tw\_sys\_tx.
- **Echo Tx Tw:** The link partner's Echo Tx Tw value. The respective echo values shall be defined as the local link partners reflection (echo) of the remote link partners respective values. When a local link partner receives its echoed values from the remote link partner it can determine if the remote link partner has received, registered, and processed its most recent values. For example, if the local link partner receives echoed parameters that do not match the values in its local MIB, then the local link partner infers that the remote link partners request was based on stale information.
- **Echo Rx Tw:** The link partner's Echo Rx Tw value.
- **Resolved Tx Tw:** The resolved Tx Tw for this link.  
**Note:** Not the link partner. The resolved value that is the actual tx wakeup time used for this link (based on EEE information exchanged through LLDP).
- **Resolved Rx Tw:** The resolved Rx Tw for this link.  
**Note:** Not the link partner. The resolved value that is the actual tx wakeup time used for this link (based on EEE information exchanged through LLDP).
- **EEE In Sync:** Shows whether the switch and the link partner have agreed on wake times.
  - Red: Switch and link partner have not agreed on wakeup times.
  - Green: Switch and link partner have agreed on wakeup times.

### 5.13.5 Monitor LLDP Port Statistics

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.

Figure 5-56. LLDP Global Counters

LLDP Global Counters

Global Counters	
Clear global counters	<input checked="" type="checkbox"/>
Neighbor entries were last changed	2022-11-14T16:33:09+00:00 (345720 secs. ago)
Total Neighbors Entries Added	0
Total Neighbors Entries Deleted	0
Total Neighbors Entries Dropped	0
Total Neighbors Entries Aged Out	0

LLDP Statistics Local Counters

Local Interface	Tx Frames	Rx Frames	Rx Errors	Frames Discarded	TLVs Discarded	TLVs Unrecognized	Org. Discarded	Age-Outs	Clear
GigabitEthernet 1/1	0	0	0	0	0	0	0	0	<input checked="" type="checkbox"/>
GigabitEthernet 1/2	0	0	0	0	0	0	0	0	<input checked="" type="checkbox"/>
GigabitEthernet 1/3	0	0	0	0	0	0	0	0	<input checked="" type="checkbox"/>
GigabitEthernet 1/4	0	0	0	0	0	0	0	0	<input checked="" type="checkbox"/>
2.5GigabitEthernet 1/1	0	0	0	0	0	0	0	0	<input checked="" type="checkbox"/>
2.5GigabitEthernet 1/2	11522	0	0	0	0	0	0	0	<input checked="" type="checkbox"/>

- **Global Counters**
  - Clear global counters: If checked the global counters are cleared when Clear is pressed.
  - 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 TLL expiring.
- **Local Counters**
  - 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 an error.
  - Frames Discarded: If a LLDP frame is received on an 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 Type Length Value (TLVs). If a TLV is malformed, then it is counted and discarded.
  - TLVs Unrecognized: The number of well-formed TLVs, but with an unknown type of 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, then 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 pressed.

### 5.14 Monitor PoE

This page allows the user to inspect the current status for all PoE ports.



Figure 5-57. Monitor PoE

Port	PD Class	Power Requested	Power Allocated	Power Used	Current Used	Priority	Port Status
1	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	---
2	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	---
3	5-5	90 [W]	90 [W]	0.5 [W]	11 [mA]	Low	On
4	6	60 [W]	60 [W]	4.1 [W]	78 [mA]	Low	On

- **Local Ports:** This is the logical port number for this row.
- **PD Class:** Each PD is classified according to a class that defines the maximum power used by the PD. The PD Class shows the PDs class. The following classes are defined:
  - Class 0: Max. power 15.4W
  - Class 1: Max. power 4.0W
  - Class 2: Max. power 7.0W
  - Class 3: Max. power 15.4W
  - Class 4: Max. power 30.0W
  - Class 5: Max. power 45.0W
  - Class 6: Max. power 60.0W
  - Class 7: Max. power 70.0W
  - Class 8: Max. power 90.0W
- **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:
  - On: A PD is detected for the port.
  - ---: No PD detected for the port.
  - Not Supported: PoE not supported for the port.
  - 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.
  - Off: PD is OFF.
  - Disabled: User has disabled PoE for the port.
  - Shutdown: The port is shut down.
  - Overload: The PD has requested or used more power than the port can deliver and is powered down.
  - Unknown: PD detected but is not working correctly.

## 5.15 Monitor MAC Table

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, and selected through the **entries per page** input field. When first visited, this web page shows the first 20 entries from the beginning of the MAC table. The first displayed is one with the lowest VLAN ID and the lowest MAC address found in the MAC table.

Figure 5-58. MAC Address Table

Start from VLAN  and MAC address  with  entries per page.

Type	VLAN	MAC Address	Port Members							
			CPU	1	2	3	4	5	6	
Dynamic	1	00-0A-CD-2D-B1-ED								✓
Dynamic	1	00-99-88-44-AD-1F								✓
Static	1	00-DE-FD-AE-17-78	✓							
Static	1	33-33-00-00-00-01	✓	✓	✓	✓	✓	✓	✓	✓
Static	1	33-33-FF-AE-17-78	✓	✓	✓	✓	✓	✓	✓	✓
Static	1	FF-FF-FF-FF-FF-FF	✓	✓	✓	✓	✓	✓	✓	✓

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



- **MAC Address:** The MAC address of the entry.
- **VLAN:** The VLAN ID of the entry.
- **Port Members:** The ports that are members of the entry.

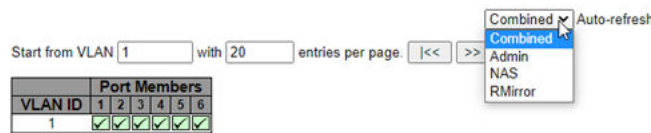
## 5.16 Monitor VLANs

The following sections describe the Monitor VLANs.

### 5.16.1 Monitor VLANs Membership

This page provides an overview of membership status of VLAN users. 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, this web page shows the first 20 entries from the beginning of the VLAN table. The one with the lowest VLAN ID found in the VLAN table are displayed first.

Figure 5-59. VLAN Membership Status for Combined Users



- **VLAN User:** Various internal software modules may use VLAN services to configure VLAN memberships on the fly. The drop-down list on the right allows for selecting between showing VLAN memberships as configured by an administrator (Admin) or as configured by one of these internal software modules. The **Combined** entry shows a combination of the administrator and internal software modules configuration, and basically reflects what is configured in hardware.
- **VLAN ID:** VLAN ID for which the Port members are displayed.
- **Port Members:** A row of check boxes for each port is displayed for each VLAN ID.
  - If a port is included in a VLAN, then the following image is displayed:
  - If a port is in the forbidden port list, then the following image is displayed:
  - If a port is in the forbidden port list and at the same time attempted included in VLAN, then the following image is displayed: . Here, the port is not a member of VLAN.

### 5.16.2 Monitor VLAN Ports

This page provides VLAN port status.

Figure 5-60. VLAN Port Status for Combined Users

Port	Port Type	Ingress Filtering	Frame Type	Port VLAN ID	Tx Tag	Untagged VLAN ID	Conflicts
1	C-Port	<input checked="" type="checkbox"/>	All	1	Untag All		No
2	C-Port	<input checked="" type="checkbox"/>	All	1	Untag All		No
3	C-Port	<input checked="" type="checkbox"/>	All	1	Untag All		No
4	C-Port	<input checked="" type="checkbox"/>	All	1	Untag All		No
5	C-Port	<input checked="" type="checkbox"/>	All	1	Untag All		No
6	C-Port	<input checked="" type="checkbox"/>	All	1	Untag All		No

- **VLAN User:** Various internal software modules may use VLAN services to configure VLAN port configuration on the fly. The drop-down list on the right allows for selecting between showing VLAN memberships as configured by an administrator (Admin) or as configured by one of these internal software modules. The **Combined** entry shows a combination of the administrator and internal software modules configuration, and basically reflects what is configured in the hardware.

If a given software modules has not overridden any of the port settings, the text **No data exists for the selected user** is shown in the table.

- **Port:** The logical port for the settings contained in the same row.
- **Port Type:** Shows the port type (Unaware, C-Port, S-Port, and S-Custom-Port.) that a given user wants to configure on the port. The field is empty if not overridden by the selected user.
- **Ingress Filtering:** Shows if a given user wants ingress filtering enabled. The field is empty if it is not overridden by the selected user.

- **Frame Type:** Shows the acceptable frame types (All, Tagged, and Untagged) that a given user wants to configure on the port. The field is empty if not overridden by the selected user.
- **Port VLAN ID:** Shows the Port VLAN ID (PVID) that a given user wants the port to have. The field is empty if not overridden by the selected user.
- **Tx Tag:** Shows the Tx Tag requirements (Tag All, Tag PVID, Tag UVID, Untag All, Untag PVID, and Untag UVID) that a given user has on a port. The field is empty if not overridden by the selected user.
- **Untagged VLAN ID:** If Tx Tag is overridden by the selected user and is set to Tag or Untag UVID, then this field shows the VLAN ID the user wants to tag or untag on egress. The field is empty if it is not overridden by the selected user.
- **Conflicts:** Two users may have conflicting requirements to a port's configuration. For instance, one user may require all frames to be tagged on egress while another requires all frames to be untagged on egress. Since both users cannot win, this gives rise to a conflict, which is solved in a prioritized way. The Administrator has the least priority. Other software modules are prioritized according to their position in the drop-down list: The higher in the list, the higher priority. If conflicts exist, it is displayed as **Yes** for the **Combined** user and the offending software module. The **Combined** user reflects what is configured in hardware.

## 5.17 Monitor sFlow

This page shows receiver and per-port sFlow statistics.

Figure 5-61. sFlow Statistics

**sFlow Statistics**

**Receiver Statistics**

Owner	<none>
IP Address/Hostname	0.0.0.0
Timeout	0
Tx Successes	0
Tx Errors	0
Flow Samples	0
Counter Samples	0

**Port Statistics**

Port	Flow Samples	Counter Samples
1	0	0
2	0	0
3	0	0
4	0	0
5	0	0
6	0	0

- **Receiver Statistics**
  - **Owner:** This field shows the current owner of the sFlow configuration. It considers one of the following three values:
    - If sFlow is currently unconfigured/unclaimed, then Owner contains <none>.
    - If sFlow is currently configured through Web or CLI, Owner contains <Configured through local management>.
    - If sFlow is currently configured through SNMP, Owner contains a string identifying the sFlow receiver.
  - **IP Address/Hostname:** The IP address or hostname of the sFlow receiver.
  - **Timeout:** The number of seconds remaining before sampling stops and the current sFlow owner is released.
  - **Tx Successes:** The number of UDP datagrams successfully sent to the sFlow receiver.
  - **Tx Errors:** The number of UDP datagrams that has failed transmission. The most common source of errors is invalid sFlow receiver IP/hostname configuration. To diagnose, paste the receiver's IP address/hostname into the Ping Web page (Diagnostics → Ping/Ping6)
  - **Flow Samples:** The total number of flow samples sent to the sFlow receiver.
  - **Counter Samples:** The total number of counter samples sent to the sFlow receiver.

- **Port Statistics**

- **Port:** The port number for which the following statistics applies.
- **Flow Samples:** The number of flow samples sent to the sFlow receiver originating from this port.
- **Counter Samples:** The total number of counter samples sent to the sFlow receiver originating from this port.

## 6. Web Interface—Diagnostics

This section describes the Network assist tools, such as ping and trace rout.

### 6.1 Diagnostics Ping (IPv4)

This page allows you to issue ICMP (IPv4) PING packets to troubleshoot IP connectivity issues.

**Figure 6-1. Ping (IPv4)**

Fill in the parameters as needed and press "Start" to initiate the Ping session.

Hostname or IP Address	<input type="text"/>	
Payload Size	<input type="text" value="56"/>	bytes
Payload Data Pattern	<input type="text" value="0"/>	(single byte value, integer or hex with prefix '0x')
Packet Count	<input type="text" value="5"/>	packets
TTL Value	<input type="text" value="64"/>	
VID for Source Interface	<input type="text"/>	
Source Port Number	<input type="text"/>	
IP Address for Source Interface	<input type="text"/>	
Quiet (only print result)	<input type="checkbox"/>	

You can configure the following parameters for the test:

- **Hostname or IP Address:** The address of the destination host, either as a symbolic hostname or an IP Address.
- **Payload Size:** Determines the size of the ICMP data payload in bytes (excluding the size of Ethernet, IP, and ICMP headers). The default value is 56 bytes. The valid range is 2 bytes–1452 bytes.
- **Payload Data Pattern:** Determines the pattern used in the ICMP data payload. The default value is 0. The valid range is 0–255.
- **Packet Count:** Determines the number of PING requests sent. The default value is 5. The valid range is 1–60.
- **TTL Value:** Determines the TTL field value in the IPv4 header. The default value is 64. The valid range is 1–255.
- **VID for Source Interface:** This field can be used to force the test to use a specific local VLAN interface as the source interface. Leave this field empty for automatic selection based on routing configuration.  
**Note:** You may only specify either the VID or the IP Address for the source interface.
- **Source Port Number:** This field can be used to force the test to use a specific local interface with the specified port number as the source interface. The specified port must be configured with a suitable IP address. Leave this field empty for automatic selection based on routing configuration.  
**Note:** You may only specify either the Source Port Number or the IP Address for the source interface
- **Address for Source Interface:** This field can be used to force the test to use a specific local interface with the specified IP address as the source interface. The specified IP address must be configured on a local interface. Leave this field empty for automatic selection based on routing configuration.  
**Note:** You may only specify either the VID or the IP Address for the source interface.
- **Quiet (Only Print Result):** Checking this option does not print the result of each ping request but only shows the result.

The following figure shows the ping result output.

**Figure 6-2. IPv4 Ping Example**

```

PING 2001::01 (2001::1) from 2001::3: 56 data bytes
64 bytes from 2001::1: seq=0 ttl=64 time=2.118 ms
64 bytes from 2001::1: seq=1 ttl=64 time=2.009 ms
64 bytes from 2001::1: seq=2 ttl=64 time=1.852 ms
64 bytes from 2001::1: seq=3 ttl=64 time=2.869 ms
64 bytes from 2001::1: seq=4 ttl=64 time=1.845 ms

--- 2001::01 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 1.845/2.138/2.869 ms

```

## 6.2 Diagnostics Ping (IPv6)

This page allows you to issue ICMPv6 PING packets to troubleshoot IPv6 connectivity issues.

Figure 6-3. Ping (IPv6)

**Ping (IPv6)**

Fill in the parameters as needed and press "Start" to initiate the Ping session.

Hostname or IP Address	<input type="text"/>	
Payload Size	<input type="text" value="56"/>	bytes
Payload Data Pattern	<input type="text" value="0"/>	(single byte value; integer or hex with prefix '0x')
Packet Count	<input type="text" value="5"/>	packets
VID for Source Interface	<input type="text"/>	
Source Port Number	<input type="text"/>	
IP Address for Source Interface	<input type="text"/>	
Quiet (only print result)	<input type="checkbox"/>	

You can configure the following parameters for the test:

- **Hostname or IP Address:** The address of the destination host, either as a symbolic hostname or an IP address.
- **Payload Size:** Determines the size of the ICMP data payload in bytes (excluding the size of Ethernet, IP, and ICMP headers). The default value is 56 bytes. The valid range is 2 bytes–1452 bytes.
- **Payload Data Pattern:** Determines the pattern used in the ICMP data payload. The default value is 0. The valid range is 0–255.
- **Packet Count:** Determines the number of PING requests sent. The default value is 5. The valid range is 1–60.
- **VID for Source Interface:** This field can be used to force the test to use a specific local VLAN interface as the source interface. Leave this field empty for automatic selection based on routing configuration.  
**Note:** You may only specify either the VID or the IP address for the source interface.
- **Source Port Number:** This field can be used to force the test to use a specific local interface with the specified port number as the source interface. The specified port must be configured with a suitable IP address. Leave this field empty for automatic selection based on routing configuration.  
**Note:** You may only specify either the Source Port Number or the IP address for the source interface.
- **Address for Source Interface:** This field can be used to force the test to use a specific local interface with the specified IP address as the source interface. The specified IP address must be configured on a local interface. Leave this field empty for automatic selection based on routing configuration.  
**Note:** You may only specify either the VID or the IP address for the source interface.
- **Quiet (Only Print Result):** Checking this option does not print the result of each ping request but only shows the result.

The following figure shows the ping result output.

Figure 6-4. Ping IPv6

```
PING 2001::01 (2001::1) from 2001::3: 56 data bytes
64 bytes from 2001::1: seq=0 ttl=64 time=2.118 ms
64 bytes from 2001::1: seq=1 ttl=64 time=2.009 ms
64 bytes from 2001::1: seq=2 ttl=64 time=1.852 ms
64 bytes from 2001::1: seq=3 ttl=64 time=2.869 ms
64 bytes from 2001::1: seq=4 ttl=64 time=1.845 ms

--- 2001::01 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 1.845/2.138/2.869 ms
```

## 6.3 Diagnostics—Traceroute (IPv4)

This page allows you to perform a Traceroute test over IPv4 towards a remote host. Traceroute is a diagnostic tool for displaying the route and measuring transit delays of packets across an IPv4 network.

Figure 6-5. Traceroute (IPv4)

Fill in the parameters as needed and press "Start" to initiate the Traceroute session.

Hostname or IP Address	<input type="text"/>	
DSCP Value	<input type="text" value="0"/>	
Number of Probes Per Hop	<input type="text" value="3"/>	packets
Response Timeout	<input type="text" value="3"/>	seconds
First TTL Value	<input type="text" value="1"/>	
Max TTL Value	<input type="text" value="30"/>	
VID for Source Interface	<input type="text"/>	
IP Address for Source Interface	<input type="text"/>	
Use ICMP instead of UDP	<input type="checkbox"/>	
Print Numeric Addresses	<input type="checkbox"/>	

You can configure the following parameters for the test:

- **Hostname or IP Address:** The destination IP Address.
- **DSCP Value:** This value is used for the DSCP value in the IPv4 header. The default value is 0. The valid range is 0–63.
- **Number of Probes Per Hop:** Determines the number of probes (packets) sent for each hop. The default value is 3. The valid range is 1–60.
- **Response Timeout:** Determines the number of seconds to wait for a reply to a sent request. The default number is 3. The valid range is 1–86400.
- **First TTL Value:** Determines the value of the TTL field in the IPv4 header in the first packet sent. The default number is 1. The valid range is 1–30.
- **Max TTL Value:** Determines the maximum value of the TTL field in the IPv4 header. If this value is reached before the specified remote host is reached the test stops. The default number is 30. The valid range is 1–255.
- **VID for Source Interface:** This field can be used to force the test to use a specific local VLAN interface as the source interface. Leave this field empty for automatic selection based on routing configuration.  
**Note:** You may only specify either the VID or the IP Address for the source interface.
- **Address for Source Interface:** This field can be used to force the test to use a specific local interface with the specified IP address as the source interface. The specified IP address must be configured on a local interface. Leave this field empty for automatic selection based on routing configuration.  
**Note:** You may only specify either the VID or the IP Address for the source interface.
- **Use ICMP instead of UDP:** By default, the `traceroute` command uses UDP datagrams. Selecting this option forces it to use ICMP ECHO packets instead.
- **Print Numeric Address:** By default, the `traceroute` command prints out hop information using a reverse DNS lookup for the acquired host IP addresses. This may slow down the display if the DNS information is not available. Selecting this option prevents the reverse DNS lookup and forces the `traceroute` command to print numeric IP addresses.

## 6.4 Diagnostics—Traceroute (IPv6)

This page allows you to perform a traceroute test over IPv6 towards a remote host. Traceroute is a diagnostic tool for displaying the route and measuring transit delays of packets across an IPv6 network.

Figure 6-6. Traceroute (IPv6)

Fill in the parameters as needed and press "Start" to initiate the Traceroute session.

Hostname or IP Address	<input type="text"/>	
DSCP Value	<input type="text" value="0"/>	
Number of Probes Per Hop	<input type="text" value="3"/>	packets
Response Timeout	<input type="text" value="3"/>	seconds
Max TTL Value	<input type="text" value="30"/>	
VID for Source Interface	<input type="text"/>	
IP Address for Source Interface	<input type="text"/>	
Print Numeric Addresses	<input type="checkbox"/>	

You can configure the following parameters for the test:

- **Hostname or IP Address:** The destination IP Address.
- **DSCP Value:** This value is used for the DSCP value in the IPv4 header. The default value is 0. The valid range is 0–255.
- **Number of Probes Per Hop:** Determines the number of probes (packets) sent for each hop. The default value is 3. The valid range is 1–60.
- **Response Timeout:** Determines the number of seconds to wait for a reply to a sent request. The default number is 3. The valid range is 1–86400.
- **Max TTL Value:** Determines the maximum value of the TLL field in the IPv4 header. If this value is reached before the specified remote host is reached the test stops. The default number is 255. The valid range is 1–255.
- **VID for Source Interface:** This field can be used to force the test to use a specific local VLAN interface as the source interface. Leave this field empty for automatic selection based on routing configuration.  
**Note:** You may only specify either the VID or the IP Address for the source interface.
- **Address for Source Interface:** This field can be used to force the test to use a specific local interface with the specified IP address as the source interface. The specified IP address must be configured on a local interface. Leave this field empty for automatic selection based on routing configuration.  
**Note:** You may only specify either the VID or the IP Address for the source interface.
- **Print Numeric Address:** By default, the `tracert` command prints out hop information using a reverse DNS lookup for the acquired host IP addresses. This may slow down the display if the DNS information is not available. Selecting this option prevents the reverse DNS lookup and forces the `tracert` command to print numeric IP addresses.

## 6.5 Diagnostics VeriPHY

This page is used for running the VeriPHY Cable Diagnostics for 10/100 and 1G copper ports. Click **Start** to run the diagnostics. This takes approximately 10 seconds. If all ports are selected, then this can take approximately 30 seconds. When completed, the page refreshes automatically, and you can view the cable diagnostics results in the cable status table.

**Note:** VeriPHY is only accurate for cables of length 7m–140m. 10 Mbps and 100 Mbps ports are linked down while running VeriPHY. Therefore, running VeriPHY on a 10 Mbps or 100 Mbps management port causes the switch to stop responding until VeriPHY is complete.

Figure 6-7. Diagnostics VeriPHY

Cable Status								
Port	Pair A	Length A	Pair B	Length B	Pair C	Length C	Pair D	Length D
1	--	--	--	--	--	--	--	--
2	--	--	--	--	--	--	--	--
3	--	--	--	--	--	--	--	--
4	--	--	--	--	--	--	--	--

- **Port:** Port Number.
- **Cable Status:**
  - **Port:** 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:** The length (in meters) of the cable pair. The resolution is 3m.

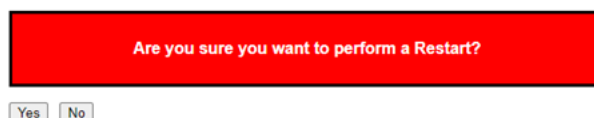
## 7. Web Interface—Maintenance

This section describes maintenance activities, such as resetting the device, restore configuration to factory default, software update, and unit configuration.

### 7.1 Restart Device

You can restart the switch on this page. After the restart, the switch boots normally.

Figure 7-1. Restart Device



### 7.2 Factory Defaults

You can reset configuration of the switch on this page. Only the IP configuration is retained. The new configuration is available immediately, which means that restart is not necessary.

Figure 7-2. Factory Defaults



### 7.3 Maintenance Software

The following sections describe the maintenance software.

#### 7.3.1 Software Upload

This page facilitates an update of the firmware controlling the switch. After the software image is uploaded, a page announces that the firmware update is initiated. After about a minute, the firmware is updated and the switch restarts.

Figure 7-3. Software Upload



#### 7.3.2 Image Select

This page provides information about the active and alternate (backup) firmware images in the device and allows you to revert to the alternate image. The web page displays two tables with information about the active and alternate firmware images.

- If the active firmware image is the alternate image, only the **Active Image** table is shown. In this case, the **Activate Alternate Image** button is also disabled.
- If the alternate image is active (due to a corruption of the primary image or by manual intervention), uploading a new firmware image to the device automatically uses the primary image slot and activates this.
- The firmware version and date information may be empty for older firmware releases. This does not constitute an error.

Figure 7-4. Software Image Selection

Active Image	
Image	PDS-204G_v1.08.mfi
Version	PDS-204GCO-v1.08
Date	2022-11-14T16:33:37+02:00

Alternate Image	
Image	PDS-204G_v1.07.mfi
Version	v1.07
Date	2022-11-10T13:06:42+02:00

- **Image:** The file name of the firmware image, from when the image was last updated.
- **Version:** The version of the firmware image.
- **Date:** The date where the firmware was produced.

## 7.4 Maintenance—Configuration

The following sections describe the maintenance configurations.

### 7.4.1 Configuration Save startup-config

This copies `running-config` to `startup-config` and ensures that the currently active configuration is used at the next reboot.

Figure 7-5. Save Running Configuration to startup = config

Please note: The generation of the configuration file may be time consuming, depending on the amount of non-default configuration.

### 7.4.2 Configuration Download

You can download unit configuration file to local computer for later use or modify manually by the user.

Figure 7-6. Download Configuration

Select configuration file to save.

Please note: `running-config` may take a while to prepare for download.

File Name
<input type="radio"/> <code>running-config</code>
<input type="radio"/> <code>default-config</code>
<input type="radio"/> <code>startup-config</code>

- **File Name (configuration file type to be download)**
  - `running-config`: The active in-use configuration file.
  - `default-config`: Unit configuration as it was released by the factory.
  - `startup-config`: Unit configuration upon power up or software restart.

**Note:** `startup-config` and `running-config` must be the same if you have saved its latest configuration changes.

### 7.4.3 Configuration Upload

You can upload unit configuration file from the web browser to the unit.

Figure 7-7. Upload Configuration

File To Upload  
 No file chosen

Destination File

File Name	Parameters
<input type="radio"/> running-config	<input checked="" type="radio"/> Replace <input type="radio"/> Merge
<input type="radio"/> startup-config	
<input checked="" type="radio"/> Create new file	<input type="text"/>

The following file types can be selected:

- **running-config:** The file is applied to the switch configuration. This can be done in the following ways:
  - **Replace mode:** The current configuration is fully replaced with the configuration in the uploaded file.
  - **Merge mode:** The uploaded file is merged into `running-config`.

**Note:** Unit may keep up to 32 different configuration files.

#### 7.4.4 Configuration Activate

Select configuration file to activate. The previous configuration is completely replaced, potentially leading to a loss of management connectivity.

**Note:** The activated configuration file is not saved to `startup-config` automatically.

Figure 7-8. Active Configuration

Select configuration file to activate. The previous configuration will be completely replaced, potentially leading to loss of management connectivity.  
 Please note: The activated configuration file will **not** be saved to `startup-config` automatically.

File Name
<input type="radio"/> default-config
<input checked="" type="radio"/> startup-config

#### 7.4.5 Delete Configuration File

You can 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, then the switch to default configuration is effectively reset.

Figure 7-9. Delete Configuration File

File Name
<input checked="" type="radio"/> startup-config

### 8. Revision History

The revision history describes the changes that were implemented in the document. The changes are listed by revision, starting with the most current publication.

Revision	Date	Description
A	01/2023	Initial Revision

---

## Microchip Information

---

### The Microchip Website

---

Microchip provides online support via our website at [www.microchip.com/](http://www.microchip.com/). This website is used to make files and information easily available to customers. Some of the content available includes:

- **Product Support** – Data sheets and errata, application notes and sample programs, design resources, user's guides and hardware support documents, latest software releases and archived software
- **General Technical Support** – Frequently Asked Questions (FAQs), technical support requests, online discussion groups, Microchip design partner program member listing
- **Business of Microchip** – Product selector and ordering guides, latest Microchip press releases, listing of seminars and events, listings of Microchip sales offices, distributors and factory representatives

### Product Change Notification Service

---

Microchip's product change notification service helps keep customers current on Microchip products. Subscribers will receive email notification whenever there are changes, updates, revisions or errata related to a specified product family or development tool of interest.

To register, go to [www.microchip.com/pcn](http://www.microchip.com/pcn) and follow the registration instructions.

### Customer Support

---

Users of Microchip products can receive assistance through several channels:

- Distributor or Representative
- Local Sales Office
- Embedded Solutions Engineer (ESE)
- Technical Support

Customers should contact their distributor, representative or ESE for support. Local sales offices are also available to help customers. A listing of sales offices and locations is included in this document.

Technical support is available through the website at: [www.microchip.com/support](http://www.microchip.com/support)

### Microchip Devices Code Protection Feature

---

Note the following details of the code protection feature on Microchip products:

- Microchip products meet the specifications contained in their particular Microchip Data Sheet.
- Microchip believes that its family of products is secure when used in the intended manner, within operating specifications, and under normal conditions.
- Microchip values and aggressively protects its intellectual property rights. Attempts to breach the code protection features of Microchip product is strictly prohibited and may violate the Digital Millennium Copyright Act.
- Neither Microchip nor any other semiconductor manufacturer can guarantee the security of its code. Code protection does not mean that we are guaranteeing the product is "unbreakable". Code protection is constantly evolving. Microchip is committed to continuously improving the code protection features of our products.

### Legal Notice

---

This publication and the information herein may be used only with Microchip products, including to design, test, and integrate Microchip products with your application. Use of this information in any other manner violates these terms. Information regarding device applications is provided only for your convenience and may be superseded

---

by updates. It is your responsibility to ensure that your application meets with your specifications. Contact your local Microchip sales office for additional support or, obtain additional support at [www.microchip.com/en-us/support/design-help/client-support-services](http://www.microchip.com/en-us/support/design-help/client-support-services).

THIS INFORMATION IS PROVIDED BY MICROCHIP "AS IS". MICROCHIP MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WHETHER EXPRESS OR IMPLIED, WRITTEN OR ORAL, STATUTORY OR OTHERWISE, RELATED TO THE INFORMATION INCLUDING BUT NOT LIMITED TO ANY IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY, AND FITNESS FOR A PARTICULAR PURPOSE, OR WARRANTIES RELATED TO ITS CONDITION, QUALITY, OR PERFORMANCE.

IN NO EVENT WILL MICROCHIP BE LIABLE FOR ANY INDIRECT, SPECIAL, PUNITIVE, INCIDENTAL, OR CONSEQUENTIAL LOSS, DAMAGE, COST, OR EXPENSE OF ANY KIND WHATSOEVER RELATED TO THE INFORMATION OR ITS USE, HOWEVER CAUSED, EVEN IF MICROCHIP HAS BEEN ADVISED OF THE POSSIBILITY OR THE DAMAGES ARE FORESEEABLE. TO THE FULLEST EXTENT ALLOWED BY LAW, MICROCHIP'S TOTAL LIABILITY ON ALL CLAIMS IN ANY WAY RELATED TO THE INFORMATION OR ITS USE WILL NOT EXCEED THE AMOUNT OF FEES, IF ANY, THAT YOU HAVE PAID DIRECTLY TO MICROCHIP FOR THE INFORMATION.

Use of Microchip devices in life support and/or safety applications is entirely at the buyer's risk, and the buyer agrees to defend, indemnify and hold harmless Microchip from any and all damages, claims, suits, or expenses resulting from such use. No licenses are conveyed, implicitly or otherwise, under any Microchip intellectual property rights unless otherwise stated.

## Trademarks

---

The Microchip name and logo, the Microchip logo, Adaptec, AVR, AVR logo, AVR Freaks, BesTime, BitCloud, CryptoMemory, CryptoRF, dsPIC, flexPWR, HELDO, IGLOO, JukeBlox, KeeLoq, Kleer, LANCheck, LinkMD, maXStylus, maXTouch, MediaLB, megaAVR, Microsemi, Microsemi logo, MOST, MOST logo, MPLAB, OptoLyzer, PIC, picoPower, PICSTART, PIC32 logo, PolarFire, Prochip Designer, QTouch, SAM-BA, SenGenuity, SpyNIC, SST, SST Logo, SuperFlash, Symmetricom, SyncServer, Tachyon, TimeSource, tinyAVR, UNI/O, Vectron, and XMEGA are registered trademarks of Microchip Technology Incorporated in the U.S.A. and other countries.

AgileSwitch, APT, ClockWorks, The Embedded Control Solutions Company, EtherSynch, Flashtec, Hyper Speed Control, HyperLight Load, Libero, motorBench, mTouch, Powermite 3, Precision Edge, ProASIC, ProASIC Plus, ProASIC Plus logo, Quiet-Wire, SmartFusion, SyncWorld, Temux, TimeCesium, TimeHub, TimePictra, TimeProvider, TrueTime, and ZL are registered trademarks of Microchip Technology Incorporated in the U.S.A.

Adjacent Key Suppression, AKS, Analog-for-the-Digital Age, Any Capacitor, AnyIn, AnyOut, Augmented Switching, BlueSky, BodyCom, Clockstudio, CodeGuard, CryptoAuthentication, CryptoAutomotive, CryptoCompanion, CryptoController, dsPICDEM, dsPICDEM.net, Dynamic Average Matching, DAM, ECAN, Espresso T1S, EtherGREEN, GridTime, IdealBridge, In-Circuit Serial Programming, ICSP, INICnet, Intelligent Paralleling, IntellIMOS, Inter-Chip Connectivity, JitterBlocker, Knob-on-Display, KoD, maxCrypto, maxView, memBrain, Mindi, MiWi, MPASM, MPF, MPLAB Certified logo, MPLIB, MPLINK, MultiTRAK, NetDetach, Omniscient Code Generation, PICDEM, PICDEM.net, PICkit, PICtail, PowerSmart, PureSilicon, QMatrix, REAL ICE, Ripple Blocker, RTAX, RTG4, SAM-ICE, Serial Quad I/O, simpleMAP, SimpliPHY, SmartBuffer, SmartHLS, SMART-I.S., storClad, SQL, SuperSwitcher, SuperSwitcher II, Switchtec, SynchroPHY, Total Endurance, Trusted Time, TSHARC, USBCheck, VariSense, VectorBlox, VeriPHY, ViewSpan, WiperLock, XpressConnect, and ZENA are trademarks of Microchip Technology Incorporated in the U.S.A. and other countries.

SQTP is a service mark of Microchip Technology Incorporated in the U.S.A.

The Adaptec logo, Frequency on Demand, Silicon Storage Technology, and Symmcom are registered trademarks of Microchip Technology Inc. in other countries.

GestIC is a registered trademark of Microchip Technology Germany II GmbH & Co. KG, a subsidiary of Microchip Technology Inc., in other countries.

All other trademarks mentioned herein are property of their respective companies.

© 2023, Microchip Technology Incorporated and its subsidiaries. All Rights Reserved.

ISBN: 978-1-6683-1844-7



---

---

## Quality Management System

---

For information regarding Microchip's Quality Management Systems, please visit [www.microchip.com/quality](http://www.microchip.com/quality).

## Worldwide Sales and Service

AMERICAS	ASIA/PACIFIC	ASIA/PACIFIC	EUROPE
<p><b>Corporate Office</b> 2355 West Chandler Blvd. Chandler, AZ 85224-6199 Tel: 480-792-7200 Tel: 480-792-7277 Technical Support: <a href="http://www.microchip.com/support">www.microchip.com/support</a> Web Address: <a href="http://www.microchip.com">www.microchip.com</a></p> <p><b>Atlanta</b> Duluth, GA Tel: 678-957-9614 Fax: 678-957-1455</p> <p><b>Austin, TX</b> Tel: 512-257-3370</p> <p><b>Boston</b> Westborough, MA Tel: 774-760-0087 Fax: 774-760-0088</p> <p><b>Chicago</b> Itasca, IL Tel: 630-285-0071 Fax: 630-285-0075</p> <p><b>Dallas</b> Addison, TX Tel: 972-818-7423 Fax: 972-818-2924</p> <p><b>Detroit</b> Novi, MI Tel: 248-848-4000</p> <p><b>Houston, TX</b> Tel: 281-894-5983</p> <p><b>Indianapolis</b> Noblesville, IN Tel: 317-773-8323 Fax: 317-773-5453 Tel: 317-536-2380</p> <p><b>Los Angeles</b> Mission Viejo, CA Tel: 949-462-9523 Fax: 949-462-9608 Tel: 951-273-7800</p> <p><b>Raleigh, NC</b> Tel: 919-844-7510</p> <p><b>New York, NY</b> Tel: 631-435-6000</p> <p><b>San Jose, CA</b> Tel: 408-735-9110 Tel: 408-436-4270</p> <p><b>Canada - Toronto</b> Tel: 905-695-1980 Fax: 905-695-2078</p>	<p><b>Australia - Sydney</b> Tel: 61-2-9868-6733</p> <p><b>China - Beijing</b> Tel: 86-10-8569-7000</p> <p><b>China - Chengdu</b> Tel: 86-28-8665-5511</p> <p><b>China - Chongqing</b> Tel: 86-23-8980-9588</p> <p><b>China - Dongguan</b> Tel: 86-769-8702-9880</p> <p><b>China - Guangzhou</b> Tel: 86-20-8755-8029</p> <p><b>China - Hangzhou</b> Tel: 86-571-8792-8115</p> <p><b>China - Hong Kong SAR</b> Tel: 852-2943-5100</p> <p><b>China - Nanjing</b> Tel: 86-25-8473-2460</p> <p><b>China - Qingdao</b> Tel: 86-532-8502-7355</p> <p><b>China - Shanghai</b> Tel: 86-21-3326-8000</p> <p><b>China - Shenyang</b> Tel: 86-24-2334-2829</p> <p><b>China - Shenzhen</b> Tel: 86-755-8864-2200</p> <p><b>China - Suzhou</b> Tel: 86-186-6233-1526</p> <p><b>China - Wuhan</b> Tel: 86-27-5980-5300</p> <p><b>China - Xian</b> Tel: 86-29-8833-7252</p> <p><b>China - Xiamen</b> Tel: 86-592-2388138</p> <p><b>China - Zhuhai</b> Tel: 86-756-3210040</p>	<p><b>India - Bangalore</b> Tel: 91-80-3090-4444</p> <p><b>India - New Delhi</b> Tel: 91-11-4160-8631</p> <p><b>India - Pune</b> Tel: 91-20-4121-0141</p> <p><b>Japan - Osaka</b> Tel: 81-6-6152-7160</p> <p><b>Japan - Tokyo</b> Tel: 81-3-6880-3770</p> <p><b>Korea - Daegu</b> Tel: 82-53-744-4301</p> <p><b>Korea - Seoul</b> Tel: 82-2-554-7200</p> <p><b>Malaysia - Kuala Lumpur</b> Tel: 60-3-7651-7906</p> <p><b>Malaysia - Penang</b> Tel: 60-4-227-8870</p> <p><b>Philippines - Manila</b> Tel: 63-2-634-9065</p> <p><b>Singapore</b> Tel: 65-6334-8870</p> <p><b>Taiwan - Hsin Chu</b> Tel: 886-3-577-8366</p> <p><b>Taiwan - Kaohsiung</b> Tel: 886-7-213-7830</p> <p><b>Taiwan - Taipei</b> Tel: 886-2-2508-8600</p> <p><b>Thailand - Bangkok</b> Tel: 66-2-694-1351</p> <p><b>Vietnam - Ho Chi Minh</b> Tel: 84-28-5448-2100</p>	<p><b>Austria - Wels</b> Tel: 43-7242-2244-39 Fax: 43-7242-2244-393</p> <p><b>Denmark - Copenhagen</b> Tel: 45-4485-5910 Fax: 45-4485-2829</p> <p><b>Finland - Espoo</b> Tel: 358-9-4520-820</p> <p><b>France - Paris</b> Tel: 33-1-69-53-63-20 Fax: 33-1-69-30-90-79</p> <p><b>Germany - Garching</b> Tel: 49-8931-9700</p> <p><b>Germany - Haan</b> Tel: 49-2129-3766400</p> <p><b>Germany - Heilbronn</b> Tel: 49-7131-72400</p> <p><b>Germany - Karlsruhe</b> Tel: 49-721-625370</p> <p><b>Germany - Munich</b> Tel: 49-89-627-144-0 Fax: 49-89-627-144-44</p> <p><b>Germany - Rosenheim</b> Tel: 49-8031-354-560</p> <p><b>Israel - Ra'anana</b> Tel: 972-9-744-7705</p> <p><b>Italy - Milan</b> Tel: 39-0331-742611 Fax: 39-0331-466781</p> <p><b>Italy - Padova</b> Tel: 39-049-7625286</p> <p><b>Netherlands - Drunen</b> Tel: 31-416-690399 Fax: 31-416-690340</p> <p><b>Norway - Trondheim</b> Tel: 47-72884388</p> <p><b>Poland - Warsaw</b> Tel: 48-22-3325737</p> <p><b>Romania - Bucharest</b> Tel: 40-21-407-87-50</p> <p><b>Spain - Madrid</b> Tel: 34-91-708-08-90 Fax: 34-91-708-08-91</p> <p><b>Sweden - Gothenberg</b> Tel: 46-31-704-60-40</p> <p><b>Sweden - Stockholm</b> Tel: 46-8-5090-4654</p> <p><b>UK - Wokingham</b> Tel: 44-118-921-5800 Fax: 44-118-921-5820</p>