24-PORT GIGABIT ETHERNET POE+ LAYER2+ MANAGED SWITCH WITH 10 GBE UPLINK
USER MANUAL

Model 561105

Version 2.0

FCC/CE Mark Warning

FCC Warning

This Equipment has been tested and found to comply with the limits for a Class-A digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy. It may cause harmful interference to radio communications if the equipment is not installed and used in accordance with the instructions. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

CE Mark Warning

This is a Class-A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

Table of Contents

Table of Contents

Table of Contents

Table of Contents

Table of Contents

Table of Contents

Table of Contents

Table of Contents

Before Starting

In Before Starting:

This section contains introductory information, which includes:

- **Intended Readers**
- **Icons for Note, Caution, and Warning**
- **Product Package Contents**

Intended Readers

This manual provides information regarding to all the aspects and functions needed to install, configure, use, and maintain the product you've purchased.

This manual is intended for technicians who are familiar with in-depth concepts of networking management and terminologies.

Icons for Note, Caution, and Warning

To install, configure, use, and maintain this product properly, please pay attention when you see these icons in this manual:

A **Note** icon indicates important information which will guide you to use this product properly.

A **Caution** icon indicates either a potential for hardware damage or data loss, including information that will guide you to avoid these situations.

A **Warning** icon indicates potentials for property damage and personal injury.

Before Starting

Product Package Contents

Before starting install this product, please check and verify the contents of the product package, which should include the following items:

	One Network Switch
	One Power Cord
	One User Manual CD
	One pair Rack-mount kit + 8 Screws

Note: If any item listed in this table above is missing or damaged, please contact your distributor or retailer as soon as possible.

Chapter 1:

Product Overview

In Product Overview:

This section will give you an overview of this product, including its feature functions and hardware/software specifications.

- **Product Brief Description**
- **Product Specification**
- **Hardware Description**
- **Hardware Installation**

1.1. Product Brief Description

Introduction

The switch is 24-port 10/100/1000Base-T + 4 10G SFP+ Open Slot Rack-mount L2+ Full Management Network Switch that is designed for medium or large network environment to strengthen its network connection. The switch supports 128G non-blocking switch fabric, the 24 gigabit ports and 4 10G ports can transmit and receive data traffic without any lost. The EEE feature reduces the power consumption when there is no traffic forwarding even port is still connected. The 10G uplink port design is available and important for high bandwidth uplink request when cascaded with other switch. The switch also supports Layer 2+ full management software features. These features are powerful to provide network control, management, monitor and security feature requests. Including rack-mount brackets, the 19" size fits into your rack environment. It is a superb choice to boost your network with better performance and efficiency.

4 10 Gigabit SFP+ Open Slots

The switch equips with 4 10G SFP+ open slots as the uplink ports, the 10G uplink design provides an excellent solution for expanding your network from 1G to 10G. By 10G speed, this product provides high flexibility and high bandwidth connectivity to another 10G switch or the Servers, Workstations and other attached devices which support 10G interface. The user can also aggregate the 10G ports as Trunk group to enlarge the bandwidth.

Full Layer 2 Management Features

The switch includes full Layer 2+ Management features. The software set includes up to 4K 802.1Q VLAN and advanced Protocol VLAN, Private VLAN, MVR…features. There are 8 physical queues Quality of Service, IPv4/v6 Multicast filtering, Rapid Spanning Tree protocol to avoid network loop, Multiple Spanning Tree Protocol to integrate VLAN and Spanning Tree, LACP, LLDP; sFlow, port mirroring, cable diagnostic and advanced Network Security features. It also provides Console CLI for out of band management and SNMP, Web GUI for in band Management.

1.2. Product Specification

Interface		
10/100/1000 Base RJ45 Ports		24
10G Uplink SFP+ Slot		4
Console Port for CLI Management		1
System Performance		
Packet Buffer		32Mb
MAC Address Table Size		32K
Switching Capacity		128Gbps
Forwarding Rate		95.2Mpps
PoE Features		
IEEE 802.3 af/at		IEEE 802.3 af/at
Number of PSE Ports		24
Max. Power Consumption		500W
External/Internal Power		Internal Power
Power Feeding Detecting Capability on PD		•
PD Alive Check		•
PD Classification		•
Power Management (per-port)	Enable/Disable PoE Per Port	•
	Priority Setting Per Port	•
	Power Level Setting Per Port	•
	Overloading Protection	•
L2 Features		
Auto-negotiation		•
Auto MDI/MDIX		•
Flow Control (duplex)	802.3x (Full)	•
	Back-Pressure (Half)	•
Spanning Tree	IEEE 802.1D (STP)	•
	IEEE 802.1w (RSTP)	•
	IEEE 802.1s (MSTP)	•
VLAN	VLAN Group	4K
	Tagged Based	•
	Port-based	•
Link Aggregation	IEEE 802.3ad with LACP	•
	Static Trunk	•
	Max. LACP Link Aggregation Group	12
IGMP Snooping	IGMP Snooping v1/v2/v3	•
	IPv6 MLD Snooping	•
	Querier, Immediate Leave	•
Storm Control (Broadcast/Multi-cast/Un-known Unicast)		•
Jumbo Frame Support		10K

QoS Features		
Number of priority queue		8 queues/port
Rate Limiting	Ingress	Yes, 1KBps/1pps
	Egress	Yes, 1KBps/1pps
DiffServ (RFC2474 Remarking)		•
Scheduling (WRR, Strict, Hybrid)		•
CoS	IEEE 802.1p	•
	IP ToS precedence, IP DSCP	•
Security		
Management System User Name/Password Protection		•
User Privilege		Set user privilege up to 15 Level
Port Security (MAC-based)		•
IEEE 802.1x Port-based Access Control		•
ACL (L2/L3/L4)		•
IP Source Guard		•
RADIUS (Authentication, Authorization, Accounting)		•
TACACS+		•
HTTP & SSL (Secure Web)		•
SSH v2.0 (Secured Telnet Session)		•
MAC/IP Filter		•
Management		
Command Line Interface (CLI)		•
Web Based Management		•
Telnet		•
Access Management Filtering		SNMP/WEB/SSH/TELNET
Firmware Upgrade via HTTP		•
Dual Firmware Images		•
Configuration Download/Upload		•
SNMP (v1/v2c/v3)		•
RMON (1,2,3,&9 groups)		•
DHCP (Client/Relay/Option82/Snooping)		•
System Event/Error Log		•
NTP/LLDP		•
Cable Diagnostics		•
IPv6 Configuration		•
Port Mirroring		One to One or Many to One
Mechanical		
Power Input		100~240VAC
Dimension (H*W*D)		44*440*220 mm
LED		Power, 10/100/1000M, PoE, SFP
Operating Temperature		0~45°C
Operating Humidity		5~90% (non-condensing)
Weight		3 KG
Certification		CE, FCC Class A

Product Specification

Standard	
IEEE 802.3 – 10BaseT	•
IEEE 802.3u - 100BaseTX	•
IEEE 802.3ab - 1000BaseT	•
IEEE 802.3z 1000BaseSX/LX	•
IEEE 802.3af Power over Ethernet (PoE)	•
IEEE 802.3at Power over Ethernet (PoE+)	•
IEEE 802.3az - Energy Efficient Ethernet (EEE)	•
IEEE 802.3x - Flow Control	•
IEEE 802.1Q - VLAN	•
IEEE802.1v - Protocol VLAN	•
IEEE 802.1p - Class of Service	•
IEEE 802.1D - Spanning Tree	•
IEEE 802.1w - Rapid Spanning Tree	•
IEEE 802.1s - Multiple Spanning Tree	•
IEEE 802.3ad - Link Aggregation Control Protocol (LACP)	•
IEEE 802.1AB - LLDP (Link Layer Discovery Protocol)	•
IEEE 802.1X - Access Control	•

1.3. Hardware Description

This section mainly describes the hardware of Full-Management PoE switch and gives a physical and functional overview on the certain switch.

Front Panel

The front panel of the Full-Management PoE switch consists of 24 10/100/1000 Base-TX RJ-45 ports, 2 gigabit uplink SFP ports, and 2 10G SFP+ stacking ports. The LED Indicators are also located on the front panel.
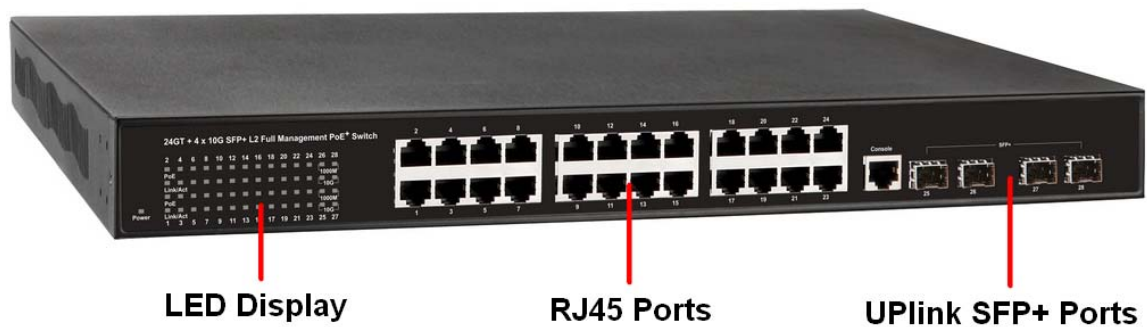
LED Indicators

The LED Indicators present real-time information of systematic operation status. The following table provides description of LED status and their meaning.

LED	Color / Status	Description	No. of LEDs
Power	Amber On	Power on	Power
10/100/1000M	Green On	Link Up	24(1~24)
	Green Blinking	Data Activating	
SFP	Green On	linked to Power Device	25~26
	Green Blinking	Data Activating	25~26

Rear Panel

The rear panel of the Full-Management PoE switch contains 2 ventilation fans, a power switch, and an IEC 60320 plug for power supply.

1.4. Hardware Installation

To install the Full-Management PoE switch, please place it on a large flat surface with a power socket close by. This surface should be clean, smooth, and level. Also, please make sure that there is enough space around the Full-Management PoE switch for RJ45 cable, power cord and ventilation.

If you're installing this Full-Management PoE switch on a 19-inch rack, please make sure to use the rack-mount kit (L brackets) and screws come with the product package. All screws must be fastened so the rack-mount kit and your product are tightly conjoined before installing it on your 19-inch rack.

Ethernet cable Request

The wiring cable types are as below:

- 10 Base-T: 2-pair UTP/STP CAT. 3, 4, 5 cable, EIA/TIA-568 100-ohm (Max. 100m)
- 100 Base-TX: 2-pair UTP/STP CAT. 5 cable, EIA/TIA-568 100-ohm (Max. 100m)
- 1000 Base-T: 4-pair UTP/STP CAT. 5 cable, EIA/TIA-568 100-ohm (Max. 100m)
- PoE: To delivery power properly, it is recommended to use CAT 5e and CAT 6 cable. Ethernet cables of higher qualities can reduce the power lost during transmission.

SFP Installation

While install the SFP transceiver, make sure the SFP type of the 2 ends is the same and the transmission distance, wavelength, fiber cable can meet your request. It is suggested to purchase the SFP transceiver with the switch provider to avoid any incompatible issue.

The way to connect the SFP transceiver is to Plug in SFP fiber transceiver fist. The SFP transceiver has 2 plug for fiber cable, one is TX (transmit), the other is RX (receive). Cross-connect the transmit channel at each end to the receive channel at the opposite end.

For more information regarding to the product safety and maintenance guide, please refer to **Appendix A: Product Safety**.

Chapter 2:

Preparing for Management

In Preparing for Management:
This section will guide your how to manage this product via serial console, management web page, and Telnet/SSH interface.

The switch provides both *out-of-band* and *in-band* managements.

Out-of-band Management: You can configure the switch via RS232 console cable without having the switch or your PC connecting to a network. Out-of-band management provides a dedicated and secure way for switch management.

In-Band Management: In-band management allows you to manage your switch with a web browser (such as Microsoft IE, Mozilla Firefox, or Google Chrome) as long as your PC and the switch are connected to the same network.

- **Preparation for Serial Console**
- **Preparation for Web Interface**
- **Preparation for Telnet/SSH Interface**

2.1. Preparation for Serial Console

Inside the product package, you can find an RS-232 console cable. Before managing your switch via out-of-band management, please attach this cable's RJ45 connector to your switch's console port and its RS-232 female connector to your PC's COM port.

To access this switch's out-of-band management CLI (Command Line Interface), your PC must have terminal emulator software such as HyperTerminal or PuTTY installed. Some operating systems (such as Microsoft Windows XP) have HyperTerminal already installed. If your PC does not have any terminal emulator software installed, please download and install a terminal emulator software on your PC.

The following section will use HyperTerminal as an example.

1. Run HyperTerminal on your PC.
2. Give a name to the new console connection.

3. Choose the COM port that is connected to the switch.

4. Set the serial port settings as: **Baud Rate:** 115200, **Data Bit:** 8, **Parity:** None, **Stop Bit:** 1, **Row Control:** None.
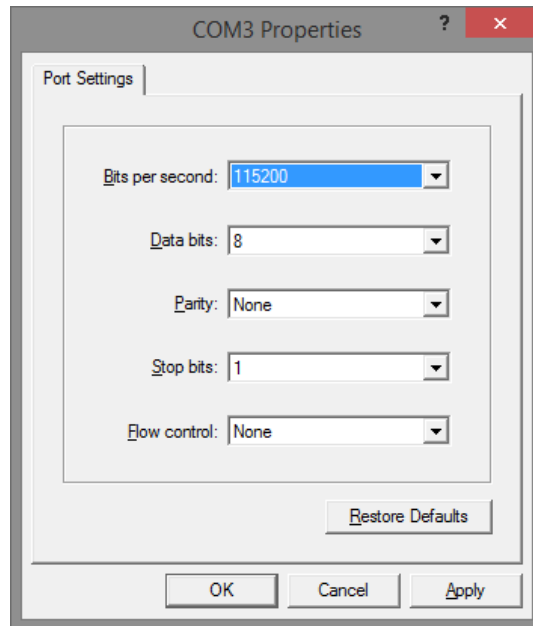
5. The system will prompt you to login the out-of-band management CLI. The default username/password is **admin**/**admin**.
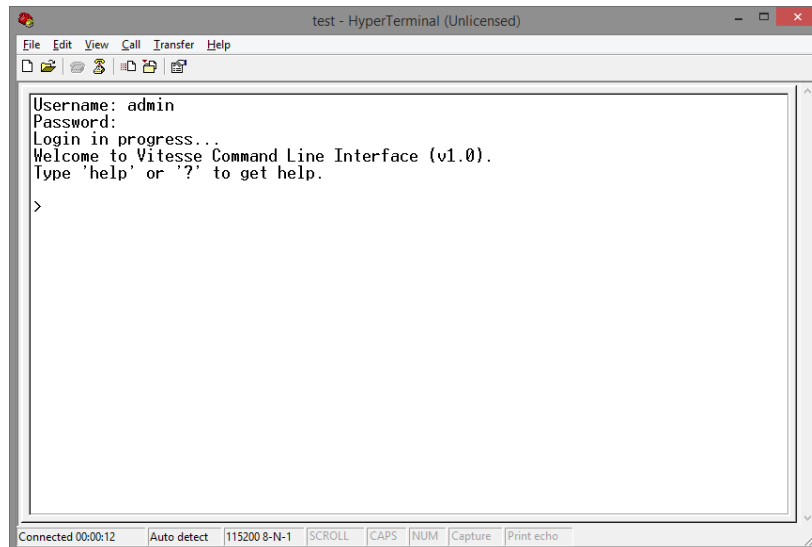
2.2. Preparation for Web Interface

The management web page allows you to use a web browser (such as Microsoft IE, Google Chrome, or Mozilla Firefox) to configure and monitor the switch from anywhere on the network.

Before using the web interface to manage your switch, please verify that your switch and your PC are on the same network. Please follow the steps down below to configure your PC properly:

1. Verify that the network interface card (NIC) of your PC is operational and properly installed, and that your operating system supports TCP/IP protocol.
2. Connect your PC with the switch via an RJ45 cable.
3. The default IP address of the switch is **192.168.2.1**. The switch and your PC should locate within the same IP Subnet. Change your PC's IP address to 192.168.2.X, where X can be any number from 2 to 254. Please make sure that the IP address you've assigned to your PC cannot be the same with the switch.
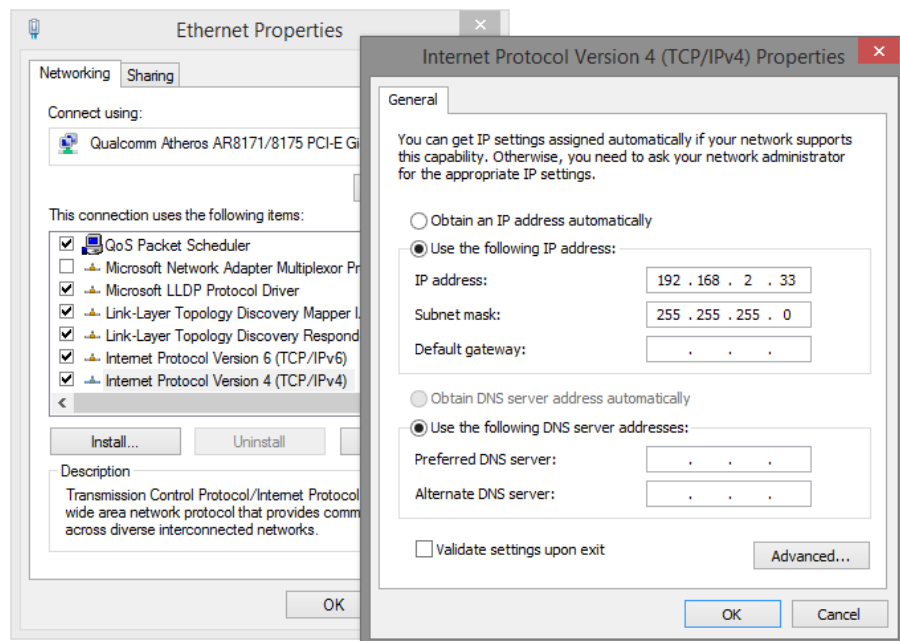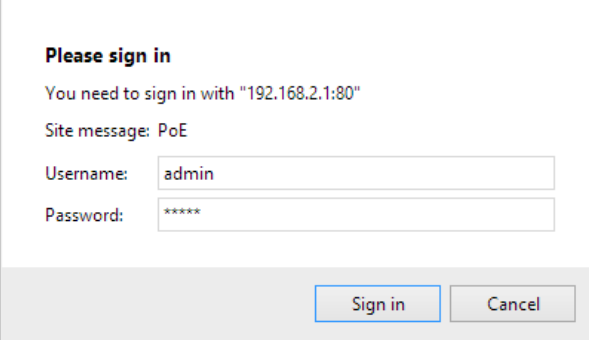
4. Launch the web browser (IE, Firefox, or Chrome) on your PC.
5. Type **192.168.2.1** (or the IP address of the switch) in the web browser's URL field, and press Enter.
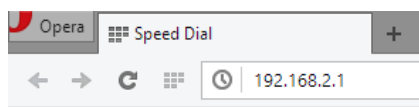
6.   The web browser will prompt you to sign in. The default username/password for the configuration web page is **admin**/**admin**.

For more information, please refer to **Appendix B: IP Configuration for Your PC**.

2.3. Preparation for Telnet/SSH Interface

Both telnet and SSH (Secure Shell) are network protocols that provide a text-based command line interface (CLI) for in-band system management. However, only SSH provides a secure channel over an un-secured network, where all transmitted data are encrypted.

This switch support both telnet and SSH management CLI. In order to access the switch's CLI via telnet or SSH, both your PC and the switch must be in the same network. Before using the switch's telnet/SSH management CLI, please set your PC's network environment according to the previous chapter (**2.2. Preparation for Web Interface**).

Telnet interface can be accessed via Microsoft "CMD" command. However, SSH interface can only be accessed via dedicated SSH terminal simulator. The following section will use *PuTTY* as an example to demonstrate how to connect to the switch's SSH CLI, since both telnet and SSH uses the same way (though using different terminal simulator software) to access in-band management CLI.

Access SSH via Putty:
A "PuTTY Configuration" window will pop up after you run PuTTY.

1. Input the IP address of the switch in the "**Host Name (or IP address)**" field. The default IP address of the switch if **192.168.2.1**.

2. Choose "SSH" on the "**Connection type**" section, then press "Enter"**.**
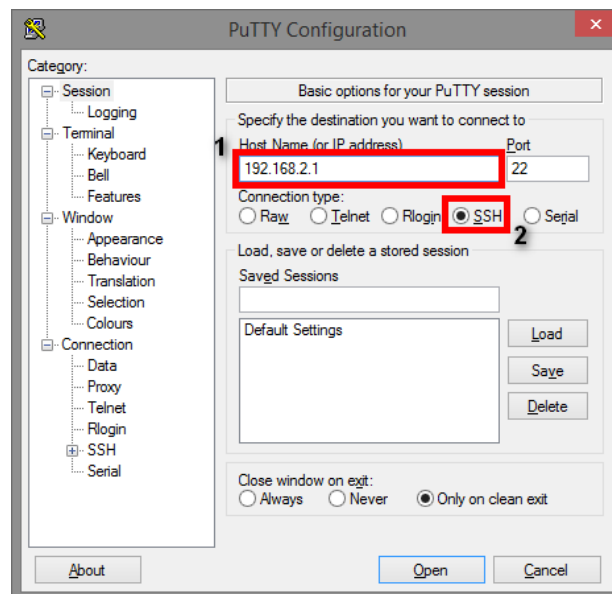
3. If you're connecting to the switch via SSH for the first time, a "**PuTTY Security Alert**" window will pop up. Please press "**Yes**" to continue. This window won't pop up if you're using telnet to connect to the in-band management CLI.
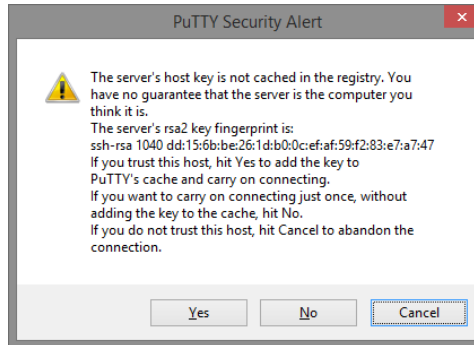
4. PuTTY will prompt you to login after the telnet/SSH connection is established. The default username/password is **admin**/**admin**.
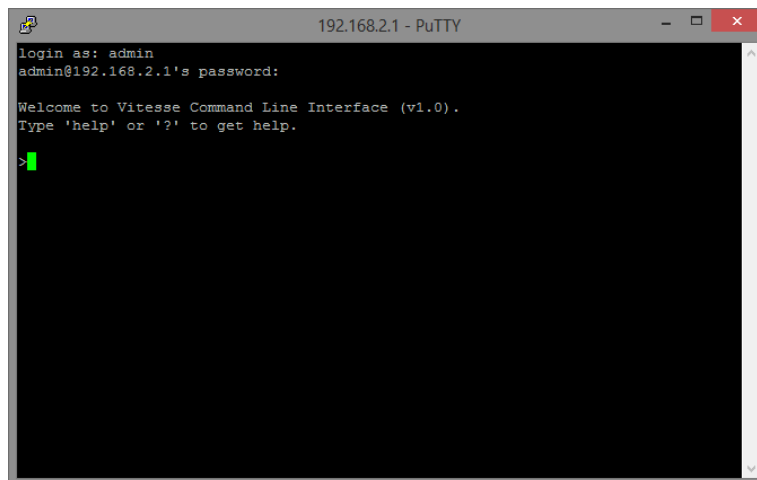
Chapter 3:

Web Management

In Web Management:

As mentioned in *Chapter 2.2. Preparation for Web Interface*, This switch provides a web-based management interface. You can make all settings and monitor system status with this management web page.

Configuration/Monitor options included in the management web page can be divided into the following 4 categories, which will be discussed in detail in this chapter:

- **Web Management - Configure**
- **Web Management - Monitor**
- **Web Management - Diagnostic**
- **Web Management - Maintenance**

3.1. Web Management - Configure

In here you can access all the configuration options of the switch. The configuration options here include:

- **System:** Here you can configure basic system settings such as system information, switch IP, NTP, system time and log.

- **Power Reduction:** You can enable EEE (Energy Efficient Ethernet) function on each port to conserve and save power used by the switch.

- **Ports:** You can view the connection status of all the ports on the switch, as well as set port connection speed, flow control, maximum frame length, and power control mode.

- **Security:** The Security option allows you to make settings that secures both the switch itself or your network.

- **Aggregation:** Aggregation allows you to combine multiple physical ports into a logical port, thus allows the transmitting speed exceeding the limit of a single port.

- **Loop Protection:** A network loop might cause broadcast storm and paralyze your entire network. You can enable loop protection function here to prevent network loop.

- **Spanning Tree:** Spanning Tree Protocol is a network designed to ensure a loop-free network and provide redundant links that serve as automatic backup paths if an active link fails. This switch supports STP, RSTP (Rapid STP), and MSTP (Multiple STP).

- **MVR:** MVR stands for Multiple VLAN Registration, a protocol that allows sharing multicast VLAN information and configuring it dynamically when needed.

- **IPMC:** Here you can set IGMP snooping (for IPv4) or MLD snooping (for IPv6). These protocols can reduce the network loading while running band-width demanding applications such as streaming videos by eliminating excessive data transmitting.

- **LLDP:** LLDP stands for Link Layer Discovery Protocol, a protocol that allows the switch to advertise its identity, capabilities, and neighbors on the network.

- **PoE:** Here you can enable/disable the PoE function on each port or assign the power (in Watt) for each port.

- **MAC Table:** When a network device is connected to the switch, the switch will keep its MAC address on the MAC table. This section provides settings for the switch's MAC address table.

- **VLANs:** VLAN stands for Virtual LAN, which allows you to separate ports into different VLAN groups. Only member of the same VLAN group can transmit/receive packets among each other, while other ports in different VLAN group can't. Here you can set port-based VLAN.

- **Private VLANs:** Also known as port isolation. Only the same member in the private VLAN can communicate with each other.

- **VCL:** Here you can set MAC-based VLAN, Protocol-based VLAN, and IP Subnet-based VLAN.
- **Voice VLAN:** Voice VLAN is a specific VLAN for voice communication (such as VoIP phones) that can ensure the transmission priority of voice traffic and voice quality.
- **QoS:** QoS stands for Quality of Service, which allows you to control the network priority (which packet gets top priority to transmit and which gets low priority) via IEEE 802.1p or DSCP.
- **Mirroring:** For purposes such as network diagnostics, you can direct packets transmitted/received to/from a port (or multiple ports) to a designated port.
- **UPnP:** UPnP stands for Universal Plug and Play, a protocol that allows all the devices on the same network can discover each other and establishing network services such as data sharing. You can set UPnP here in this management page.
- **sFlow:** sFlow is an industry standard technology for monitoring switched networks through random sampling of packets on switch ports and time-based sampling of port counters. The sampled packets will be sent to the designated sFlow receiver (host) for system administrator for analysis.

3.1.1. Configuration - System

3.1.1.1. System - Information

System Information Configuration

System Contact	
System Name	
System Location	

Save   Reset

The switch system information is provided here.

System Contact

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

System Name

You can input an assigned name for this switch. By convention, this is the switch'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. And the first or last character must not be a minus sign. The allowed string length is 0 to 255.

System Location

The physical location of this node(e.g., telephone closet, 3rd floor). The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 32 to 126.

Buttons

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

3.1.1.2. System - IP

IP Configuration

	Configured	Current
DHCP Client	☐	Renew
IP Address	192.168.2.1	192.168.2.1
IP Mask	255.255.255.0	255.255.255.0
IP Router	0.0.0.0	0.0.0.0
VLAN ID	1	1
DNS Server	0.0.0.0	0.0.0.0

IP DNS Proxy Configuration

DNS Proxy	☐

Save Reset

This page allows you to view and set configurations regarding to the switch's IP setting. The left part (Configured) is for changing settings and the right part (Current) displays the current setting.

DHCP Client

Enable the DHCP client by checking this box. If DHCP fails and the configured IP address is zero, DHCP will retry. If DHCP server does not respond around 35 seconds and the configured IP address is not zero, DHCP will stop and the configured IP settings will be used. The DHCP client will announce the configured System Name as hostname for DNS lookup.

IP Address

Provide the IP address of this switch in dotted decimal notation.

IP Mask

Provide the IP mask of this switch dotted decimal notation.

IP Router

Provide the IP address of the router in dotted decimal notation.

VLAN ID

Provide the managed VLAN ID. The allowed range is 1 to 4095.

DNS Server

Provide the IP address of the DNS Server in dotted decimal notation.

DNS Proxy

When DNS proxy is enabled, DUT will relay DNS requests to the current configured DNS server on DUT, and reply as a DNS resolver to the client device on the network.

Buttons

- **Save:** Click to save changes.
- **Reset:** Click to undo any changes made locally and revert to previously saved values.
- **Renew:** Click to renew DHCP. This button is only available if DHCP is enabled.

3.1.1.3. System - IPv6

IPv6 Configuration

	Configured	Current
Auto Configuration	☑	Renew
Address	::192.168.2.1	::192.168.2.1 Link-Local Address: fe80::203:ceff:fe11:1111
Prefix	96	96
Router	::	::

Save Reset

This page allows you to view and set configurations regarding to the switch's IPv6 setting. The left part (Configured) is for changing settings and the right part (Current) displays the current setting.

Auto Configuration

Enable IPv6 auto-configuration by checking this box. If system cannot obtain the stateless address in time, the configured IPv6 settings will be used. The router may delay responding to a router solicitation for a few seconds, the total time needed to complete auto-configuration can be significantly longer.

Address

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

Prefix

Provide the IPv6 Prefix of this switch. The allowed range is 1 to 128.

Router

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

Buttons

- **Save:** Click to save changes.
- **Reset:** Click to undo any changes made locally and revert to previously saved values.
- **Renew:** Click to renew IPv6 AUTOCONF. This button is only available if IPv6 AUTOCONF is enabled.

3.1.1.4. System - NTP

NTP Configuration

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

Save   Reset

NTP stands for Network Time Protocol, which allows switch to perform clock synchronization with the NTP server.

Mode

You can enable or disable NTP function on this switch:

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

Server 1~5

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

Also, you can just input NTP server's URL here as well.

Buttons

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

3.1.1.5. System - Time

Time Zone Configuration

Time Zone Configuration	
Time Zone	None
Acronym	(0 - 16 characters)

This page allows you to configure the Time Zone and daylight saving time.

Time Zone Configuration

- **Time Zone:** Lists various Time Zones world wide. Select appropriate Time Zone from the drop down and click Save to set.

- **Acronym:** User can set the acronym of the time zone. This is a User configurable acronym to identify the time zone. You can use up to 16 alphanumeric characters and punctuations such as "-", "_", and ".".

Daylight Saving Time Configuration

Daylight Saving Time Mode	
Daylight Saving Time	Disabled

Start Time settings	
Month	Jan
Date	1
Year	2000
Hours	0
Minutes	0

End Time settings	
Month	Jan
Date	1
Year	2000
Hours	0
Minutes	0

Offset settings	
Offset	1 (1 - 1440) Minutes

Save   Reset

Daylight Saving Time Configuration

When enabled, the switch will set the clock forward or backward according to the configurations set below for a defined Daylight Saving Time duration.

- **Disable:** Disable the Daylight Saving Time configuration. This is the default setting.

- **Recurring:** The configuration of the daylight saving time duration will be applied every year.

- **Non-Recurring**: The configuration of the daylight saving time duration will be applied only once.

Start time settings

- **Week** - Select the starting week number.
- **Day** - Select the starting day.
- **Month** - Select the starting month.
- **Hours** - Select the starting hour.
- **Minutes** - Select the starting minute.

End time settings

- **Week** - Select the ending week number.
- **Day** - Select the ending day.
- **Month** - Select the ending month.
- **Hours** - Select the ending hour.
- **Minutes** - Select the ending minute.

Offset settings

- **Offset** - Enter the number of minutes to add during Daylight Saving Time. (Range: 1 to 1440)

Buttons

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

3.1.1.6. System - Log

System Log Configuration

Server Mode	Disabled ▾
Server Address	
Syslog Level	Info ▾

Save   Reset

Configure System Log on this page.

Server Mode

When enabled, the system log message will be sent out to the system log server you set here. The system log protocol is based on UDP communication and received on UDP port 514 and the system log server will not send acknowledgments back sender since UDP is a connectionless protocol and it does not provide acknowledgments. The system log packet will always send out even if the system log server does not exist. Possible modes are:

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

Server Address

Indicates the IPv4 host address of system log server. If the switch provide DNS feature, it also can be a host name.

System log Level

Indicates what kind of message will send to system log server. Possible modes are:

- **Info:** Send information, warnings and errors.
- **Warning:** Send warnings and errors.
- **Error:** Send errors.

Buttons

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

3.1.2. Configuration - Power Reduction

3.1.2.1. Power Reduction - EEE

EEE Configuration for Switch 1

Port	Enabled
*	☐
1	☐
2	☐
3	☐
4	☐
5	☐
6	☐
7	☐
8	☐

Save   Reset

EEE (Energy-Efficient Ethernet) is a power saving option that reduces the power usage when there is low or no traffic utilization by powering down circuits when there is no traffic. When a port gets data to be transmitted all circuits are powered up. The time it takes to power up the circuits is named wakeup time. The default wakeup time is 17 us for 1Gbit links and 30 us for other link speeds.

EEE devices must agree upon the value of the wakeup time in order to make sure that both the receiving and transmitting device has all circuits powered up when traffic is transmitted. The devices can exchange wakeup time information using the LLDP protocol.

EEE works for ports in auto-negotiation mode, where the port is negotiated to either 1G or 100 Mbit full duplex modes.

Ports that are not EEE-capable are grayed out and thus impossible to enable EEE.
The EEE port settings relate to the currently selected stack unit, as reflected by the page header.

Port

The switch port number of the logical EEE port.

Enabled

Controls whether EEE is enabled for this switch port.

Buttons

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

3.1.3. Configuration - Ports

Port Configuration for Switch 1   Refresh

| Port | Link | Speed | | Flow Control | | | Maximum Frame Size | Excessive Collision Mode | Power Control |
		Current	Configured	Current Rx	Current Tx	Configured			
*			<>			☐	10056	<>	<>
1	●	Down	Auto	✗	✗	☐	10056	Discard	Disabled
2	●	Down	Auto	✗	✗	☐	10056	Discard	Disabled
3	●	Down	Auto	✗	✗	☐	10056	Discard	Disabled
4	●	Down	Auto	✗	✗	☐	10056	Discard	Disabled
5	●	Down	Auto	✗	✗	☐	10056	Discard	Disabled
25	●	Down	10Gbps FDX	✗	✗	☐	10056		
26	●	Down	10Gbps FDX	✗	✗	☐	10056		

Save   Reset

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

The port settings relate to the currently selected stack unit, as reflected by the page header.

Port

This is the logical port number for this row.

Link

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

Current Link Speed

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. Possible speeds are:

- **Disabled** - Disables the switch port operation.
- **Auto** - Cu port auto negotiating speed with the link partner and selects the highest speed that is compatible with the link partner.
- **10Mbps HDX** - Forces the cu port in 10Mbps half duplex mode.
- **10Mbps FDX** - Forces the cu port in 10Mbps full duplex mode.
- **100Mbps HDX** - Forces the cu port in 100Mbps half duplex mode.
- **100Mbps FDX** - Forces the cu port in 100Mbps full duplex mode.
- **1Gbps FDX** - Forces the cu port in 1Gbps full duplex mode.

Flow Control

When Auto Speed is selected on a port, this section indicates the flow control capability that is advertised to the link partner.

When a fixed-speed setting is selected, that is what is used. The Current Rx column indicates whether pause frames on the port are obeyed, and the Current Tx column indicates whether pause frames on the port are transmitted. The Rx and Tx settings are determined by the result of the last Auto-Negotiation.

Check the configured column to use flow control. This setting is related to the setting for Configured

Link Speed.

Maximum Frame Size

Enter the maximum frame size allowed for the switch port, including FCS.

Excessive Collision Mode

Configure port transmit collision behavior.

- **Discard:** Discard frame after 16 collisions (default).
- **Restart:** Restart backoff algorithm after 16 collisions.

Power Control

The Usage column shows the current percentage of the power consumption per port. The Configured column allows for changing the power savings mode parameters per port.

- **Disabled:** All power savings mechanisms disabled.
- **ActiPHY:** Link down power savings enabled.
- **PerfectReach:** Link up power savings enabled.
- **Enabled:** Both link up and link down power savings enabled.

Buttons

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

3.1.4. Configuration - Security

This section provides settings regarding to the switch's security functions. Settings provided here can be divided into 3 categories:

- **Switch:** Here you can make security settings regarding to the switch itself.
- **Network:** Providing security settings regarding to the network.
- **AAA:** Here you can set RADIUS and TACACS+ authentication settings.

3.1.4.1. Security - Switch - Users

Users Configuration

User Name	Privilege Level
admin	15

Add New User

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.

User Name

The name of the user. You can also click on the link to configure user account.

Privilege Level

The privilege level of the user. The allowed range is 1 to 15. If the privilege level value is 15, it can access all groups, i.e. that is granted the fully control of the device. But others value need to refer to each group privilege level. User's privilege should be same or greater than the group privilege level to have the access of that group. By default setting, most groups privilege level 5 has the read-only access and privilege level 10 has the read-write access. And the system maintenance (software upload, factory defaults and etc.) need user privilege level 15. Generally, the privilege level 15 can be used for an administrator account, privilege level 10 for a standard user account and privilege level 5 for a guest account.

Buttons

- **Add New User:** Click to add a new user.

Edit User

User Settings	
User Name	Test
Password	••••
Password (again)	••••
Privilege Level	15

Save   Reset   Cancel

Delete User

This page configures a user.

User Name

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

Password

The password of the user. The allowed string length is 0 to 31.

Privilege Level

The privilege level of the user. The allowed range is 1 to 15. If the privilege level value is 15, it can access all groups, i.e. that is granted the fully control of the device. But others value need to refer to each group privilege level. User's privilege should be same or greater than the group privilege level to have the access of that group.

By default setting, most groups privilege level 5 has the read-only access and privilege level 10 has the read-write access. And the system maintenance (software upload, factory defaults and etc.) need user privilege level 15. Generally, the privilege level 15 can be used for an administrator account, privilege level 10 for a standard user account and privilege level 5 for a guest account.

Buttons

- **Save:** Click to save changes.
- **Reset:** Click to undo any changes made locally and revert to previously saved values.
- **Cancel:** Click to undo any changes made locally and return to the Users.
- **Delete User:** Delete the current user. Please note that the default user (admin) cannot be deleted.

3.1.4.2. Security - Switch - Privilege Level

Privilege Level Configuration

Group Name	Configuration Read-only	Configuration/Execute Read/write	Status/Statistics Read-only	Status/Statistics Read/write
Aggregation	5	10	5	10
Debug	15	15	15	15
Diagnostics	5	10	5	10
EEE	5	10	5	10
IP	5	10	5	10
IPMC_LIB	5	10	5	10
IPMC_Snooping	5	10	5	10
LACP	5	10	5	10
LLDP	5	10	5	10
LLDP_MED	5	10	5	10
Loop_Protect	5	10	5	10
MAC_Table	5	10	5	10
MVR	5	10	5	10
Maintenance	15	15	15	15
Mirroring	5	10	5	10
PHY	5	10	5	10
POE	5	10	5	10
Port_Security	5	10	5	10
Ports	5	10	1	10
Private_VLANs	5	10	5	10
QoS	5	10	5	10
SNMP	5	10	5	10
Security	5	10	5	10
Spanning_Tree	5	10	5	10
Stack	5	10	1	10
System	5	10	1	10
Timer	5	10	5	10
UPnP	5	10	5	10
VCL	5	10	5	10
VLANs	5	10	5	10
Voice_VLAN	5	10	5	10
sFlow	5	10	5	10

Save Reset

This page provides an overview of the privilege levels.

Group Name

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

- **System:** Contact, Name, Location, Timezone, Daylight Saving Time, Log.
- **Security:** Authentication, System Access Management, Port (contains Dot1x port, MAC based and the MAC Address Limit), ACL, HTTPS, SSH, ARP Inspection, IP source guard.
- **IP:** Everything except 'ping'.
- **Port:** Everything except 'VeriPHY'.
- **Diagnostics:** 'ping' and 'VeriPHY'.
- **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

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

Buttons

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

3.1.4.3. Security - Switch - Authentication Method

Authentication Method Configuration

Client	Authentication Method	Fallback
console	local ⌄	☐
telnet	local ⌄	☐
ssh	local ⌄	☐
web	local ⌄	☐

Save Reset

This page allows you to configure how a user is authenticated when he logs into the stack via one of the management client interfaces.

Client

The management client for which the configuration below applies.

Authentication Method

Authentication Method can be set to one of the following values:

- **None:** authentication is disabled and login is not possible.
- **Local:** use the local user database on the stack for authentication.
- **RADIUS:** use a remote RADIUS server for authentication.
- **TACACS+:** use a remote TACACS+ server for authentication.

Fallback

Enable fallback to local authentication by checking this box.

If none of the configured authentication servers are alive, the local user database is used for authentication.

This is only possible if the Authentication Method is set to a value other than 'none' or 'local'.

Buttons

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

3.1.4.4. Security - Switch - SSH

SSH Configuration

Mode	Enabled ⌄

Save   Reset

Configure SSH on this page.

Mode

Indicates the SSH mode operation. Possible modes are:

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

Buttons

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

3.1.4.5. Security - Switch - HTTPS

HTTPS Configuration

Mode	Enabled ∨
Automatic Redirect	Disabled ∨

Save   Reset

Configure HTTPS on this page.

Mode

Indicates the HTTPS mode operation. When the current connection is HTTPS, to apply HTTPS disabled mode operation will automatically redirect web browser to an HTTP connection. Possible modes are:

- **Enabled:** Enable HTTPS mode operation.
- **Disabled:** Disable HTTPS mode operation.

Automatic Redirect

Indicates the HTTPS redirect mode operation. Automatically redirects web browser to an HTTPS connection when both HTTPS mode and Automatic Redirect are enabled. Possible modes are:

- **Enabled:** Enable HTTPS redirect mode operation.
- **Disabled:** Disable HTTPS redirect mode operation.

Buttons

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

3.1.4.6. Security - Switch - Access Management

Access Management Configuration

Mode | Disabled ∨

Delete	Start IP Address	End IP Address	HTTP/HTTPS	SNMP	TELNET/SSH
Delete	0.0.0.0	0.0.0.0	☐	☐	☐

Add New Entry

Save | Reset

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

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.

Start IP address

Indicates the start IP address for the access management entry.

End IP address

Indicates the end IP address for the access management entry.

HTTP/HTTPS

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

SNMP

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

TELNET/SSH

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

Buttons

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

3.1.4.7. Security - Switch - SNMP

3.1.4.7.1. Security - Switch - SNMP - System

SNMP System Configuration

Mode	Enabled
Version	SNMP v2c
Read Community	public
Write Community	private
Engine ID	800007e5017f000001

Configure SNMP on this page.

Mode

Indicates the SNMP mode operation. Possible modes are:

- **Enabled:** Enable SNMP mode operation.
- **Disabled:** Disable SNMP mode operation.

Version

Indicates the SNMP supported version. Possible versions are:

- **SNMP v1:** Set SNMP supported version 1.
- **SNMP v2c:** Set SNMP supported version 2c.
- **SNMP v3:** Set SNMP supported version 3.

Read Community

Indicates the community read access string to permit access to SNMP agent. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 33 to 126.

The field is applicable only when SNMP version is SNMPv1 or SNMPv2c. If SNMP version is SNMPv3, the community string will be associated with SNMPv3 communities table. It provides more flexibility to configure security name than a SNMPv1 or SNMPv2c community string. In addition to community string, a particular range of source addresses can be used to restrict source subnet.

Write Community

Indicates the community write access string to permit access to SNMP agent. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 33 to 126.

The field is applicable only when SNMP version is SNMPv1 or SNMPv2c. If SNMP version is SNMPv3, the community string will be associated with SNMPv3 communities table. It provides more flexibility to configure security name than a SNMPv1 or SNMPv2c community string. In addition to community string, a particular range of source addresses can be used to restrict source subnet.

Engine ID

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

SNMP Trap Configuration

Trap Mode	Disabled
Trap Version	SNMP v1
Trap Community	public
Trap Destination Address	
Trap Destination IPv6 Address	::
Trap Authentication Failure	Enabled
Trap Link-up and Link-down	Enabled
Trap Inform Mode	Enabled
Trap Inform Timeout (seconds)	1
Trap Inform Retry Times	5

Save   Reset

SNMP Trap Configuration

Configure SNMP trap on this page.

Trap Mode

Indicates the SNMP trap mode operation. Possible modes are:

- **Enabled:** Enable SNMP trap mode operation.
- **Disabled:** Disable SNMP trap mode operation.

Trap Version

Indicates the SNMP trap supported version. Possible versions are:

- **SNMP v1:** Set SNMP trap supported version 1.
- **SNMP v2c:** Set SNMP trap supported version 2c.
- **SNMP v3:** Set SNMP trap supported version 3.

Trap Community

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

Trap Destination Address

Indicates the SNMP trap destination address. It allow a valid IP address in dotted decimal notation ('x.y.z.w').

And it also allow a valid hostname. A valid hostname is a string drawn from the alphabet (A-Za-z), digits (0-9), dot (.), dash (-). Spaces are not allowed, the first character must be an alpha character, and the first and last characters must not be a dot or a dash.

Trap Destination IPv6 Address

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

Trap Authentication Failure

Indicates that the SNMP entity is permitted to generate authentication failure traps. Possible modes are:

- **Enabled:** Enable SNMP trap authentication failure.
- **Disabled:** Disable SNMP trap authentication failure.

Trap Link-up and Link-down

Indicates the SNMP trap link-up and link-down mode operation. Possible modes are:

- **Enabled:** Enable SNMP trap link-up and link-down mode operation.
- **Disabled:** Disable SNMP trap link-up and link-down mode operation.

Trap Inform Mode

Indicates the SNMP trap inform mode operation. Possible modes are:

- **Enabled:** Enable SNMP trap inform mode operation.
- **Disabled:** Disable SNMP trap inform mode operation.

Trap Inform Timeout (seconds)

Indicates the SNMP trap inform timeout. The allowed range is 0 to 2147.

Trap Inform Retry Times

Indicates the SNMP trap inform retry times. The allowed range is 0 to 255.

Trap Probe Security Engine ID

Indicates the SNMP trap probe security engine ID mode of operation. Possible values are:

- **Enabled:** Enable SNMP trap probe security engine ID mode of operation.
- **Disabled:** Disable SNMP trap probe security engine ID mode of operation.

Trap Security Engine ID

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

Trap Security Name

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

Buttons

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

3.1.4.7.2. Security - Switch - SNMP - Community

SNMPv3 Community Configuration

Delete	Community	Source IP	Source Mask
☐	public	0.0.0.0	0.0.0.0
☐	private	0.0.0.0	0.0.0.0

Add New Entry   Save   Reset

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

Delete

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

Community

Indicates the community access string to permit access to SNMPv3 agent. The allowed string

length is 1 to 32, and the allowed content is ASCII characters from 33 to 126. The community string

will be treated as security name and map a SNMPv1 or SNMPv2c community string.

Source IP

Indicates the SNMP access source address. A particular range of source addresses can be used to

restrict source subnet when combined with source mask.

Source Mask

Indicates the SNMP access source address mask.

Buttons

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

3.1.4.7.3. Security - Switch - SNMP - User

SNMPv3 User Configuration

Delete	Engine ID	User Name	Security Level	Authentication Protocol	Authentication Password	Privacy Protocol	Privacy Password
☐	800007e5017f000001	default_user	NoAuth, NoPriv	None	None	None	None

Add New Entry   Save   Reset

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

Delete

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

Engine ID

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

User Name

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

Security Level

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

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

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

Authentication Protocol

Indicates the authentication protocol that this entry should belong to. 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.

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

Authentication Password

A string identifying the authentication password phrase. For MD5 authentication protocol, the allowed string length is 8 to 32. For SHA authentication protocol, the allowed string length is 8 to 40. The allowed content is ASCII characters from 33 to 126.

Privacy Protocol

Indicates the privacy protocol that this entry should belong to. Possible privacy protocols are:

- **None:** No privacy protocol.
- **DES:** An optional flag to indicate that this user uses DES authentication protocol.

Privacy Password

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

Buttons

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

3.1.4.7.4. Security - Switch - SNMP - Groups

SNMPv3 Group Configuration

Delete	Security Model	Security Name	Group Name
☐	v1	public	default_ro_group
☐	v1	private	default_rw_group
☐	v2c	public	default_ro_group
☐	v2c	private	default_rw_group
☐	usm	default_user	default_rw_group

Add New Entry   Save   Reset

Configure SNMPv3 group table on this page.

Delete

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

Security Model

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

- **v1:** Reserved for SNMPv1.

- **v2c:** Reserved for SNMPv2c.

- **usm:** User-based Security Model (USM).

Security Name

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

Group Name

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

Buttons

- **Add New Entry:** Click to add a new community entry.

- **Save:** Click to save changes.

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

3.1.4.7.5. Security - Switch - SNMP - Views

SNMPv3 View Configuration

Delete	View Name	View Type	OID Subtree
☐	default_view	included ⌄	.1

[Add New Entry] [Save] [Reset]

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

Delete

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

View Name

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

View Type

Indicates the view type that this entry should belong to. Possible view types are:

- **included:** An optional flag to indicate that this view subtree should be included.
- **excluded:** An optional flag to indicate that this view subtree should be excluded.

In general, if a view entry's view type is 'excluded', there should be another view entry existing with view type as 'included' and it's OID subtree should overstep the 'excluded' view entry.

OID Subtree

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

Buttons

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

3.1.4.7.6. Security - Switch - SNMP - Access

SNMPv3 Access Configuration

Delete	Group Name	Security Model	Security Level	Read View Name	Write View Name
☐	default_ro_group	any	NoAuth, NoPriv	default_view ▾	None ▾
☐	default_rw_group	any	NoAuth, NoPriv	default_view ▾	default_view ▾

[Add New Entry] [Save] [Reset]

Configure SNMPv3 access table on this page.

Delete

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

Group Name

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

Security Model

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

- **any:** Any security model accepted(v1|v2c|usm).
- **v1:** Reserved for SNMPv1.
- **v2c:** Reserved for SNMPv2c.
- **usm:** User-based Security Model (USM).

Security Level

Indicates the security model that this entry should belong to. 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 this request may request the current values. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.

Write View Name

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

Buttons

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

3.1.4.8. Security - Switch - RMON

3.1.4.8.1. Security - Switch - RMON - Statistics

RMON Statistics Configuration

Delete	ID	Data Source
Delete		.1.3.6.1.2.1.2.2.1.1. 0

Add New Entry   Save   Reset

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

Delete

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

ID

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

Data Source

Indicates the port ID which wants to be monitored. If in stacking switch, the value must add

1000*(switch ID-1), for example, if the port is switch 3 port 5, the value is 2005

Buttons

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

3.1.4.8.2. Security - Switch - RMON - History

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

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

Delete

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

ID

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

Data Source

Indicates the port ID which wants to be monitored. If in stacking switch, the value must add 1000*(switch ID-1), for example, if the port is switch 3 port 5, the value is 2005.

Interval

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

Buckets

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

Buckets Granted

The number of data shall be saved in the RMON.

Buttons

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

3.1.4.8.3. Security - Switch - RMON - Alarm

RMON Alarm Configuration

Delete	ID	Interval	Variable	Sample Type	Value	Startup Alarm	Rising Threshold	Rising Index	Falling Threshold	Falling Index

Add New Entry   Save   Reset

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

Delete

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

ID

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

Interval

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

Variable

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

- **InOctets:** The total number of octets received on the interface, including framing characters.
- **InUcastPkts:** The number of 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 event the packets are normal.
- **OutErrors:** The The number of outbound packets that could not be transmitted because of errors.
- **OutQLen:** The length of the output packet queue (in packets).

Sample Type

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

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

Value

The value of the statistic during the last sampling period.

Startup Alarm

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

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

Rising Threshold

Rising threshold value (-2147483648-2147483647).

Rising Index

Rising event index (1-65535).

Falling Threshold

Falling threshold value (-2147483648-2147483647)

Falling Index

Falling event index (1-65535).

Buttons

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

3.1.4.8.4. Security - Switch - RMON - Event

RMON Event Configuration

Delete	ID	Desc	Type	Community	Event Last Time

Add New Entry   Save   Reset

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

Delete

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

ID

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

Desc

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

Type

Indicates the notification of the event, the possible types are:

- **None:** The total number of octets received on the interface, including framing characters.
- **Log:** The number of uni-cast packets delivered to a higher-layer protocol.
- **snmptrap:** The number of broad-cast and multi-cast packets delivered to a higher-layer protocol.
- **logandtrap:** The number of inbound packets that are discarded even the packets are normal.

Community

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

Event Last Time

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

Buttons

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

3.1.4.9. Security - Network - Limit Control

This page allows you to configure the Port Security Limit Control system and port settings.

Limit Control allows for limiting the number of users on a given port. A user is identified by a MAC address and VLAN ID. If Limit Control is enabled on a port, the limit specifies the maximum number of users on the port. If this number is exceeded, an action is taken. The action can be one of the four different actions as described below.

The Limit Control module utilizes a lower-layer module, Port Security module, which manages MAC addresses learnt on the port.

The Limit Control configuration consists of two sections, a system- and a port-wide.

System Configuration

Mode

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

Aging Enabled

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

Aging Period

If Aging Enabled is checked, then the aging period is controlled with this input. If other modules are using the underlying port security for securing MAC addresses, they may have other requirements to the aging period. The underlying port security will use the shorter requested aging period of all modules that use the functionality.

The Aging Period can be set to a number between 10 and 10,000,000 seconds.

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

Port Configuration

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

Port

The port number to which the configuration below applies.

Mode

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

Limit

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

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

Action

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

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

State

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

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

Re-open Button

If a port is shutdown by this module, you may reopen it by clicking this button, which will only be enabled if this is the case. For other methods, refer to Shutdown in the Action section.

Note that clicking the reopen button causes the page to be refreshed, so non-committed changes will be lost.

Buttons

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

3.1.4.10. Security - Network - NAS (Network Access Server)

Network Access Server Configuration   [Refresh]

System Configuration (Stack Global)

Mode	Disabled	
Reauthentication Enabled	☐	
Reauthentication Period	3600	seconds
EAPOL Timeout	30	seconds
Aging Period	300	seconds
Hold Time	10	seconds
RADIUS-Assigned QoS Enabled	☐	
RADIUS-Assigned VLAN Enabled	☐	
Guest VLAN Enabled	☐	
Guest VLAN ID	1	
Max. Reauth. Count	2	
Allow Guest VLAN if EAPOL Seen	☐	

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 IEEE802.1X standard defines port-based operation, but non-standard variants overcome security limitations as shall be explored below.

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

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

System Configuration

Mode

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

Re-authentication Enabled

If checked, successfully authenticated supplicants/clients are re-authenticated after the interval specified by the Re-authentication Period. Re-authentication 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, re-authentication is only useful if the RADIUS server configuration has changed. It does not involve communication between the switch and the client, and therefore doesn't imply that a client is still present on a port (see Aging Period below).

Re-authentication Period

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

EAPOL Timeout

Determines the time for retransmission of Request Identity EAPOL frames.

Valid values are in the range 1 to 65535 seconds. This has no effect for MAC-based ports.

Aging Period

This setting applies to the following modes, i.e. modes using the Port Security functionality to secure MAC addresses:

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

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

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

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

Hold Time

This setting applies to the following modes, i.e. modes using the Port Security functionality to secure MAC addresses:

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

If a client is denied access - either because the RADIUS server denies the client access or because the RADIUS server request times out (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 will ignore new frames coming from the client during the hold time. The Hold Time can be set to a number between 10 and 1000000 seconds.

RADIUS-Assigned QoS Enabled

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

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

RADIUS-Assigned VLAN Enabled

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

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

Guest VLAN Enabled

A Guest VLAN is a special VLAN - typically with limited network access - on which 802.1X-unaware clients are placed after a network administrator-defined timeout. The switch follows a set of rules for entering and leaving the Guest VLAN as listed below.

The "Guest VLAN Enabled" checkbox provides a quick way to globally enable/disable Guest VLAN functionality. When checked, the individual ports' ditto setting determines whether the port can be moved into Guest VLAN. When unchecked, the ability to move to the Guest VLAN is disabled on all ports.

Guest VLAN ID

This is the value that a port's Port VLAN ID is set to if a port is moved into the Guest VLAN. It is only changeable if the Guest VLAN option is globally enabled.

Valid values are in the range [1; 4095].

Max. Reauth. Count

The number of times the switch transmits an EAPOL Request Identity frame without response before considering entering the Guest VLAN is adjusted with this setting. The value can only be changed if the Guest VLAN option is globally enabled.

Valid values are in the range [1; 255].

Allow Guest VLAN if EAPOL Seen

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

The value can only be changed if the Guest VLAN option is globally enabled.

Port Configuration for Switch 1

Port	Admin State	RADIUS-Assigned QoS Enabled	RADIUS-Assigned VLAN Enabled	Guest VLAN Enabled	Port State	Restart	
*	<>	☐	☐	☐			
1	Force Authorized	☐	☐	☐	Globally Disabled	Reauthenticate	Reinitialize
2	Force Authorized	☐	☐	☐	Globally Disabled	Reauthenticate	Reinitialize
3	Force Authorized	☐	☐	☐	Globally Disabled	Reauthenticate	Reinitialize
4	Force Authorized	☐	☐	☐	Globally Disabled	Reauthenticate	Reinitialize
5	Force Authorized	☐	☐	☐	Globally Disabled	Reauthenticate	Reinitialize
6	Force Authorized	☐	☐	☐	Globally Disabled	Reauthenticate	Reinitialize
7	Force Authorized	☐	☐	☐	Globally Disabled	Reauthenticate	Reinitialize
8	Force Authorized	☐	☐	☐	Globally Disabled	Reauthenticate	Reinitialize
9	Force Authorized	☐	☐	☐	Globally Disabled	Reauthenticate	Reinitialize
10	Force Authorized	☐	☐	☐	Globally Disabled	Reauthenticate	Reinitialize
11	Force Authorized	☐	☐	☐	Globally Disabled	Reauthenticate	Reinitialize
12	Force Authorized	☐	☐	☐	Globally Disabled	Reauthenticate	Reinitialize
13	Force Authorized	☐	☐	☐	Globally Disabled	Reauthenticate	Reinitialize
14	Force Authorized	☐	☐	☐	Globally Disabled	Reauthenticate	Reinitialize
15	Force Authorized	☐	☐	☐	Globally Disabled	Reauthenticate	Reinitialize
16	Force Authorized	☐	☐	☐	Globally Disabled	Reauthenticate	Reinitialize
17	Force Authorized	☐	☐	☐	Globally Disabled	Reauthenticate	Reinitialize
18	Force Authorized	☐	☐	☐	Globally Disabled	Reauthenticate	Reinitialize
19	Force Authorized	☐	☐	☐	Globally Disabled	Reauthenticate	Reinitialize
20	Force Authorized	☐	☐	☐	Globally Disabled	Reauthenticate	Reinitialize
21	Force Authorized	☐	☐	☐	Globally Disabled	Reauthenticate	Reinitialize
22	Force Authorized	☐	☐	☐	Globally Disabled	Reauthenticate	Reinitialize
23	Force Authorized	☐	☐	☐	Globally Disabled	Reauthenticate	Reinitialize
24	Force Authorized	☐	☐	☐	Globally Disabled	Reauthenticate	Reinitialize
25	Force Authorized	☐	☐	☐	Globally Disabled	Reauthenticate	Reinitialize
26	Force Authorized	☐	☐	☐	Globally Disabled	Reauthenticate	Reinitialize

Save   Reset

Port Configuration

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

Port

The port number for which the configuration below applies.

Admin State

If NAS is globally enabled, this selection controls the port's authentication mode. The following modes are available:

Force Authorized

In this mode, the switch will send one EAPOL Success frame when the port link comes up, and any client on the port will be allowed network access without authentication.

Force Unauthorized

In this mode, the switch will send one EAPOL Failure frame when the port link comes up, and any client on the port will be disallowed network access.

Port-based 802.1X

In the 802.1X-world, the user is called the supplicant, the switch is the authenticator, and the RADIUS server is the authentication server. The authenticator acts as the man-in-the-middle, forwarding

requests and responses between the supplicant and the authentication server. Frames sent between the supplicant and the switch are special 802.1X frames, known as EAPOL (EAP Over LANs) frames. EAPOL frames encapsulate EAP PDUs (RFC3748). Frames sent between the switch and the RADIUS server are RADIUS packets. RADIUS packets also encapsulate EAP PDUs together with other attributes like the switch's IP address, name, and the supplicant's port number on the switch. EAP is very flexible, in that it allows for different authentication methods, like MD5-Challenge, PEAP, and TLS. The important thing is that the authenticator (the switch) doesn't need to know which authentication method the supplicant and the authentication server are using, or how many information exchange frames are needed for a particular method. The switch simply encapsulates the EAP part of the frame into the relevant type (EAPOL or RADIUS) and forwards it.

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

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 connected to the port (for instance through a hub) to piggy-back on the successfully authenticated client and get network access even though they really aren't authenticated. To overcome this security breach, use the Single 802.1X variant.

Single 802.1X is really 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 doesn't provide valid credentials within a certain amount of time, another supplicant will get a chance. Once a supplicant is successfully

authenticated, only that supplicant will be 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 - 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, since that would cause 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 up or block traffic for that particular client, using the Port Security module. Only then will frames from the client be forwarded on the switch. There are no EAPOL frames involved in this authentication, and therefore, MAC-based Authentication has nothing to do with the 802.1X standard.

The advantage of MAC-based authentication over 802.1X-based authentication is that the clients don't need special supplicant software to authenticate. The disadvantage is that MAC addresses can

be spoofed by malicious users - equipment whose MAC address is a valid RADIUS user can be used by anyone. Also, only the MD5-Challenge method is supported. The maximum number of clients that can be attached to a port can be limited using the Port Security Limit Control functionality.

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, i.e.

- 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 will be considered, and to be valid, it must follow this rule:

- All 8 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 will be changed to this VLAN ID, the port will be set to be a member of that VLAN ID, and the port will be forced into VLAN unaware mode. Once assigned, all traffic arriving on the port will be 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 or it's invalid, or the supplicant is otherwise no longer present on the port, 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, i.e.
- 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 '0's 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, the switch considers moving the port into the Guest VLAN according to the rules outlined below.This option is only available for EAPOL-based modes, i.e.:
- 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 in the meanwhile, 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, the port will now be placed in the Guest VLAN. If disabled, the switch will first check 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 will be placed in the Guest VLAN. Otherwise it will 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 will 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, 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, the port will never be able to go back into the Guest VLAN if the "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.

- **Re-authenticate:** Schedules a re-authentication whenever the quiet-period of the port runs out (EAPOL-based authentication). For MAC-based authentication, re-authentication 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 re-authentication immediately. The clients will transfer to the unauthorized state while the re-authentication is in progress.

Buttons

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

3.1.4.11. Security - Network - ACL

3.1.4.11.1. Security - Network - ACL - Ports

ACL Ports Configuration for Switch 1   Refresh   Clear

Port	Policy ID	Action	Rate Limiter ID	Port Redirect	Logging	Shutdown	State	Counter
*	0	<>	<>	<>	<>	<>	<>	*
1	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
2	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
3	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
4	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
5	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
6	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
7	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
8	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
9	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
10	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
11	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
12	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
13	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
14	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
15	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
16	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
17	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
18	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
19	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
20	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
21	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
22	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
23	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	138997
24	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
25	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0
26	0	Permit	Disabled	Disabled	Disabled	Disabled	Enabled	0

Save   Reset

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

The settings relate to the currently selected stack unit, as reflected by the page header.

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 through 255. The default value is 0.

Action

Select whether forwarding is permitted ("Permit") or denied ("Deny"). The default value is "Permit".

Rate Limiter ID

Select which rate limiter to apply on this port. The allowed values are Disabled or the values 1 through 16. The default value is "Disabled".

Port Redirect

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

Logging

Specify the logging operation of this port. 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". Please note that 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".

State

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

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

The default value is "Enabled".

Counter

Counts the number of frames that match this ACE.

Buttons

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

3.1.4.11.2. Security - Network - ACL - Rate Limiter

ACL Rate Limiter Configuration

Rate Limiter ID	Rate (pps)
*	1
1	1
2	1
3	1
4	1
5	1
6	1
7	1
8	1
9	1
10	1
11	1
12	1
13	1
14	1
15	1
16	1

Save | Reset

Configure the rate limiter for the ACL of the switch.

Rate Limiter ID

The rate limiter ID for the settings contained in the same row.

Rate

The allowed values are: 0-131071 in pps

Buttons

- **Save:** Click to save changes.

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

3.1.4.11.3. Security - Network - ACL - Access Control List

Access Control List Configuration   Auto-refresh ☐ Refresh Clear Remove All

Ingress Port	Policy / Bitmask	Frame Type	Action	Rate Limiter	Port Redirect	Counter	
							⊕

This page shows the Access Control List (ACL), which is made up of the ACEs defined on this switch. Each row describes the ACE that is defined. The maximum number of ACEs is 512 on each switch. Click on the lowest plus sign to add a new ACE to the list. The reserved ACEs used for internal protocol, cannot be edited or deleted, the order sequence cannot be changed and the priority is highest.

Notice: the ACE won't apply to any stacking or none existing port.

Ingress Port

Indicates the ingress port of the ACE. Possible values are:

- **All:** The ACE will match all ingress port.
- **Port:** The ACE will match a specific ingress port.

Policy / Bitmask

Indicates the policy number and bitmask of the ACE.

Frame Type

Indicates the frame type of the ACE. Possible values are:

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

Action

Indicates the forwarding action of the ACE.

- **Permit:** Frames matching the ACE may be forwarded and learned.
- **Deny:** Frames matching the ACE are dropped.

Rate Limiter

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

Port Redirect

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

Counter

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

Modification Buttons

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

- ⊕: Inserts a new ACE before the current row.
- ⓔ: Edits the ACE row.
- ⬆: Moves the ACE up the list.
- ⬇: Moves the ACE down the list.
- ⊗: Deletes the ACE.
- ⊕: The lowest plus sign adds a new entry at the bottom of the ACE listings.

Buttons

- **Auto-refresh:** Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
- **Refresh:** Click to refresh the page; any changes made locally will be undone.
- **Clear:** Click to clear the counters.
- **Remove All:** Click to remove all ACEs.

ACE Configuration

Ingress Port	All
Policy Filter	Specific
Policy Value	0
Policy Bitmask	0x 0
Switch	Any
Frame Type	Any

Action	Permit
Rate Limiter	Disabled
Port Redirect	Disabled
Logging	Disabled
Shutdown	Disabled
Counter	0

Configure an ACE (Access Control Entry) 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.

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, choose this value. Two field for entering an policy value and bitmask appears.

Policy Value

When "Specific" is selected for the policy filter, you can enter a specific policy value. The allowed range is 0 to 255.

Policy Bitmask

When "Specific" is selected for the policy filter, you can enter a specific policy bitmask. The allowed range is 0x0 to 0xff.

Switch

Select the switch to which this ACE applies.

- **Any:** The ACE applies to any port.
- **Switch n:** The ACE applies to this switch number, where n is the number of the switch.

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 describes the value of Length/Type Field specifications to be greater than or equal to 1536 decimal (equal to 0600 hexadecimal).
- **ARP:** Only ARP frames can match this ACE. Notice the ARP frames won't match the ACE with ethernet type.
- **IPv4:** Only IPv4 frames can match this ACE. Notice the IPv4 frames won't match the ACE with ethernet type.
- **IPv6:** Only IPv6 frames can match this ACE. Notice the IPv6 frames won't 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.

Rate Limiter

Specify the rate limiter in number of base units. The allowed range is 1 to 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 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' can't be set when action is permitted.

Logging

Specify the logging operation of the ACE. The allowed values are:
- **Enabled:** Frames matching the ACE are stored in the System Log.
- **Disabled:** Frames matching the ACE are not logged.

Please note that 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 shut down is disabled for the ACE.

Counter

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

MAC Parameters

SMAC Filter	Specific
SMAC Value	00-00-00-00-00-01
DMAC Filter	Specific
DMAC Value	00-00-00-00-00-02

MAC Parameters

SMAC Filter

(Only displayed when the frame type is Ethernet Type or ARP.)

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 an 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.

VLAN Parameters

VLAN ID Filter	Specific
VLAN ID	1
Tag Priority	0

VLAN Parameters

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, 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. The value Any means that no tag priority is specified (tag priority is "don't-care".)

ARP Parameters

The ARP parameters can be configured when Frame Type "ARP" is selected.

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.

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.

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 field (SHA) 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 field (THA) 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

IP Protocol Filter	Other
IP Protocol Value	255
IP TTL	Any
IP Fragment	Any
IP Option	Any
SIP Filter	Network
SIP Address	0.0.0.0
SIP Mask	255.255.255.0
DIP Filter	Network
DIP Address	0.0.0.0
DIP Mask	255.255.255.0

IP Parameters

The IP parameters can be configured when Frame Type "IPv4" is selected.

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 will 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 will 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 will 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 to 255. A frame that hits this ACE matches this IP protocol value.

IP TTL

Specify the Time-to-Live settings for this ACE.

- **zero:** IPv4 frames with a Time-to-Live field greater than zero must not be able to match this entry.
- **non-zero:** IPv4 frames with a Time-to-Live 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.

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.

DIP Mask

When "Network" is selected for the destination IP filter, you can enter a specific DIP mask in dotted decimal notation.

ICMP Parameters

ICMP Type Filter

Specify the ICMP filter for this ACE.

- **Any:** No ICMP filter is specified (ICMP filter status is "don't-care").

- **Specific:** If you want to filter a specific ICMP filter with this ACE, you can enter a specific ICMP value. A field for entering an ICMP value appears.

ICMP Type Value

When "Specific" is selected for the ICMP filter, you can enter a specific ICMP value. The allowed range is 0 to 255. A frame that hits this ACE matches this ICMP value.

ICMP Code Filter

Specify the ICMP code filter for this ACE.

- **Any:** No ICMP code filter is specified (ICMP code filter status is "don't-care").

- **Specific:** If you want to filter a specific ICMP code filter with this ACE, you can enter a specific ICMP code value. A field for entering an ICMP code value appears.

ICMP Code Value

When "Specific" is selected for the ICMP code filter, you can enter a specific ICMP code value. The allowed range is 0 to 255. A frame that hits this ACE matches this ICMP code value.

UDP Parameters

Source Port Filter	Specific ⌄
Source Port No.	0
Dest. Port Filter	Specific ⌄
Dest. Port No.	0

UDP Parameters

Source Port Filter	Range ⌄	
Source Port Range	0	-65535
Dest. Port Filter	Range ⌄	
Dest. Port Range	0	-65535

TCP Parameters

Source Port Filter	Specific ⌄
Source Port No.	0
Dest. Port Filter	Specific ⌄
Dest. Port No.	0
TCP FIN	Any ⌄
TCP SYN	Any ⌄
TCP RST	Any ⌄
TCP PSH	Any ⌄
TCP ACK	Any ⌄
TCP URG	Any ⌄

TCP Parameters

Source Port Filter	Range ⌄	
Source Port Range	0	-65535
Dest. Port Filter	Range ⌄	
Dest. Port Range	0	-65535
TCP FIN	Any ⌄	
TCP SYN	Any ⌄	
TCP RST	Any ⌄	
TCP PSH	Any ⌄	
TCP ACK	Any ⌄	
TCP URG	Any ⌄	

TCP/UDP Parameters

TCP/UDP Source Filter

Specify the TCP/UDP source filter for this ACE.

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

TCP/UDP Source No.

When "Specific" is selected for the TCP/UDP source filter, you can enter a specific TCP/UDP source value. The allowed range is 0 to 65535. A frame that hits this ACE matches this TCP/UDP source value.

TCP/UDP Source Range

When "Range" is selected for the TCP/UDP source filter, you can enter a specific TCP/UDP source range value. The allowed range is 0 to 65535. A frame that hits this ACE matches this TCP/UDP source value.

TCP/UDP Destination Filter

Specify the TCP/UDP destination filter for this ACE.

- **Any:** No TCP/UDP destination filter is specified (TCP/UDP destination filter status is "don't-care").
- **Specific: I**f you want to filter a specific TCP/UDP destination filter with this ACE, you can

enter a specific TCP/UDP destination value. A field for entering a TCP/UDP destination value appears.

- **Range:** If you want to filter a specific range TCP/UDP destination filter with this ACE, you can enter a specific TCP/UDP destination range value. A field for entering a TCP/UDP destination value appears.

TCP/UDP Destination Number

When "Specific" is selected for the TCP/UDP destination filter, you can enter a specific TCP/UDP destination value. The allowed range is 0 to 65535. A frame that hits this ACE matches this TCP/UDP destination value.

TCP/UDP Destination Range

When "Range" is selected for the TCP/UDP destination filter, you can enter a specific TCP/UDP destination range value. The allowed range is 0 to 65535. A frame that hits this ACE matches this TCP/UDP destination value.

TCP FIN

Specify the TCP "No more data from sender" (FIN) value for this ACE.

- **0:** TCP frames where the FIN field is set must not be able to match this entry.
- **1:** TCP frames where the FIN field is set must be able to match this entry.
- **Any:** Any value is allowed ("don't-care").

TCP SYN

Specify the TCP "Synchronize sequence numbers" (SYN) value for this ACE.

- **0:** TCP frames where the SYN field is set must not be able to match this entry.
- **1:** TCP frames where the SYN field is set must be able to match this entry.
- **Any:** Any value is allowed ("don't-care").

TCP RST

Specify the TCP "Reset the connection" (RST) value for this ACE.

- **0:** TCP frames where the RST field is set must not be able to match this entry.
- **1:** TCP frames where the RST field is set must be able to match this entry.
- **Any:** Any value is allowed ("don't-care").

TCP PSH

Specify the TCP "Push Function" (PSH) value for this ACE.

- **0:** TCP frames where the PSH field is set must not be able to match this entry.
- **1:** TCP frames where the PSH field is set must be able to match this entry.
- **Any:** Any value is allowed ("don't-care").

TCP ACK

Specify the TCP "Acknowledgment field significant" (ACK) value for this ACE.

- **0:** TCP frames where the ACK field is set must not be able to match this entry.
- **1:** TCP frames where the ACK field is set must be able to match this entry.
- **Any:** Any value is allowed ("don't-care").

TCP URG

Specify the TCP "Urgent Pointer field significant" (URG) value for this ACE.

- **0:** TCP frames where the URG field is set must not be able to match this entry.
- **1:** TCP frames where the URG field is set must be able to match this entry.
- **Any:** Any value is allowed ("don't-care").

Ethernet Type Parameters

EtherType Filter	Specific ⌄
Ethernet Type Value	0x FFFF

Save　Reset　Cancel

Ethernet Type Parameters

The Ethernet Type parameters can be configured when Frame Type "Ethernet Type" is selected.

EtherType Filter

Specify the Ethernet type filter for this ACE.

- **Any:** No EtherType filter is specified (EtherType filter status is "don't-care").
- **Specific:** If you want to filter a specific EtherType filter with this ACE, you can enter a specific EtherType value. A field for entering a EtherType value appears.

Ethernet Type Value

When "Specific" is selected for the EtherType filter, you can enter a specific EtherType value. The allowed range is 0x600 to 0xFFFF but excluding 0x800(IPv4), 0x806(ARP) and 0x86DD(IPv6). A frame that hits this ACE matches this EtherType value.

Buttons

- **Save:** Click to save changes.
- **Reset:** Click to undo any changes made locally and revert to previously saved values.
- **Cancel:** Return to the previous page.

3.1.4.12. Security - Network - DHCP

3.1.4.12.1. Security - Network - DHCP - Snooping

DHCP Snooping Configuration

Stack Global Settings

Snooping Mode	Disabled ▼

Port Mode Configuration for Switch 1

Port	Mode	
*	<>	▼
1	Trusted	▼
2	Trusted	▼
3	Trusted	▼
25	Trusted	▼
26	Trusted	▼

Save   Reset

Configure DHCP Snooping on this page.

Snooping Mode

Indicates the DHCP snooping mode operation. Possible modes are:

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

Port Mode Configuration

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

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

Buttons

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

3.1.4.12.2. Security - Network - DHCP - Relay

DHCP Relay Configuration

Relay Mode	Disabled
Relay Server	0.0.0.0
Relay Information Mode	Enabled
Relay Information Policy	Replace

Save   Reset

Configure DHCP Relay on this page.

Relay Mode

Indicates the DHCP relay mode operation. Possible modes are:

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

- **Disabled:** Disable DHCP relay mode operation.

Relay Server

Indicates the DHCP relay server IP address. A DHCP relay agent is used to forward and to transfer DHCP messages between the clients and the server when they are not in the same subnet domain.

Relay Information Mode

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

Possible modes are:

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

- **Disabled:** Disable DHCP relay information mode operation.

Relay Information Policy

Indicates the DHCP relay information option policy. When DHCP relay information mode operation is enabled, if agent receives a DHCP message that already contains relay agent information it will enforce the policy. The 'Replace' option is invalid when relay information mode is disabled. Possible policies are:

- **Replace:** Replace the original relay information when a DHCP message that already contains it is received.
- **Keep:** Keep the original relay information when a DHCP message that already contains it is received.
- **Drop:** Drop the package when a DHCP message that already contains relay information is received.

Buttons

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

3.1.4.13. Security - Network - IP Source Guard

3.1.4.13.1. Security - Network - IP Source Guard - Configuration

This page provides IP Source Guard related configuration.

Mode of IP Source Guard Configuration

Enable the Global IP Source Guard or disable the Global IP Source Guard. All configured ACEs will be 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.

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 max dynamic client is equal to 0, it means only allow the IP packets forwarding that are matched in static entries on the specific port.

Buttons

- **Save:** Click to save changes.
- **Reset:** Click to undo any changes made locally and revert to previously saved values.
- **Translate Dynamic to Static**: Click to translate all dynamic entries to static entries.

3.1.4.13.2. Security - Network - IP Source Guard - Static Table

Static IP Source Guard Table for Switch 1

Delete	Port	VLAN ID	IP Address	IP Mask
Delete	1 ∨			

Add New Entry

Save | Reset

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.

IP Mask

It can be used for calculating the allowed network with IP address.

Buttons

- **Add New Entry:** Click to add a new entry to the Static IP Source Guard table.
- **Save:** Click to save changes.
- **Reset:** Click to undo any changes made locally and revert to previously saved values.

3.1.4.14. Security - Network - ARP Inspection

3.1.4.14.1. Security - Network - ARP Inspection - Configuration

ARP Inspection Configuration

Stack Global Settings

| Mode | Disabled ⌄ |

Translate dynamic to static

Port Mode Configuration for Switch 1

Port	Mode
*	<> ⌄
1	Disabled ⌄
2	Disabled ⌄
3	Disabled ⌄
4	Disabled ⌄
5	Disabled ⌄
25	Disabled ⌄
26	Disabled ⌄

Save Reset

This page provides ARP Inspection related configuration.

Mode of ARP Inspection Configuration

Enable the Global ARP Inspection or disable the Global ARP Inspection.

Port Mode Configuration

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.

Buttons

- **Save:** Click to save changes.
- **Reset:** Click to undo any changes made locally and revert to previously saved values.
- **Translate Dynamic to Static**: Click to translate all dynamic entries to static entries.

3.1.4.14.2. Security - Network - ARP Inspection - Static Table

Static ARP Inspection Table for Switch 1

Delete	Port	VLAN ID	MAC Address	IP Address
Delete	1 ∨			

Add New Entry

Save   Reset

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.

Buttons

- **Add New Entry:** Click to add a new entry to the Static IP Source Guard table.
- **Save:** Click to save changes.
- **Reset:** Click to undo any changes made locally and revert to previously saved values.

3.1.4.15. Security - AAA

Authentication Server Configuration

Common Server Configuration

Timeout	15	seconds
Dead Time	300	seconds

Common Server Configuration

These setting are common for all of the Authentication Servers.

Timeout

The Timeout, which can be set to a number between 3 and 3600 seconds, is the maximum time to wait for a reply from a server.

If the server does not reply within this time frame, we will consider it to be dead and continue with the next enabled server (if any).

RADIUS servers are using the UDP protocol, which is unreliable by design. In order to cope with lost frames, the timeout interval is divided into 3 subintervals of equal length. If a reply is not received within the subinterval, the request is transmitted again. This algorithm causes the RADIUS server to be queried up to 3 times before it is considered to be dead.

Dead Time

The Dead Time, which can be set to a number between 0 and 3600 seconds, 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 Dead Time to a value greater than 0 (zero) will enable this feature, but only if more than one server has been configured.

RADIUS Authentication Server Configuration

#	Enabled	IP Address/Hostname	Port	Secret
1	☐		1812	
2	☐		1812	
3	☐		1812	
4	☐		1812	
5	☐		1812	

RADIUS Authentication Server Configuration

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

#

The RADIUS Authentication Server number for which the configuration below applies.

Enabled

Enable the RADIUS Authentication Server by checking this box.

IP Address/Hostname

The IP address or hostname of the RADIUS Authentication Server. IP address is expressed in dotted decimal notation.

Port

The UDP port to use on the RADIUS Authentication Server. If the port is set to 0 (zero), the default port (1812) is used on the RADIUS Authentication Server.

Secret

The secret - up to 29 characters long - shared between the RADIUS Authentication Server and the stack.

RADIUS Accounting Server Configuration

#	Enabled	IP Address/Hostname	Port	Secret
1	☐		1813	
2	☐		1813	
3	☐		1813	
4	☐		1813	
5	☐		1813	

RADIUS Accounting Server Configuration

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

#

The RADIUS Accounting Server number for which the configuration below applies.

Enabled

Enable the RADIUS Accounting Server by checking this box.

IP Address/Hostname

The IP address or hostname of the RADIUS Accounting Server. IP address is expressed in dotted decimal notation.

Port

The UDP port to use on the RADIUS Accounting Server. If the port is set to 0 (zero), the default port (1813) is used on the RADIUS Accounting Server.

Secret

The secret - up to 29 characters long - shared between the RADIUS Accounting Server and the stack.

TACACS+ Authentication Server Configuration

#	Enabled	IP Address/Hostname	Port	Secret
1	☐		49	
2	☐		49	
3	☐		49	
4	☐		49	
5	☐		49	

Save   Reset

TACACS+ Authentication Server Configuration

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

#

The TACACS+ Authentication Server number for which the configuration below applies.

Enabled

Enable the TACACS+ Authentication Server by checking this box.

IP Address/Hostname

The IP address or hostname of the TACACS+ Authentication Server. IP address is expressed in dotted decimal notation.

Port

The TCP port to use on the TACACS+ Authentication Server. If the port is set to 0 (zero), the default port (49) is used on the TACACS+ Authentication Server.

Secret

The secret - up to 29 characters long - shared between the TACACS+ Authentication Server and the stack.

Buttons

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

3.1.5. Configuration - Aggregation

3.1.5.1. Aggregation - Static

This page is used to configure the Aggregation hash mode and the aggregation group.

Hash Code Contributors

Source MAC Address

The Source MAC address can be used to calculate the destination port for the frame. Check to enable the use of the Source MAC address, or uncheck to disable. By default, Source MAC Address is enabled.

Destination MAC Address

The Destination MAC Address can be used to calculate the destination port for the frame. Check to enable the use of the Destination MAC Address, or uncheck to disable. By default, Destination MAC Address is disabled.

IP Address

The IP address can be used to calculate the destination port for the frame. Check to enable the use of the IP Address, or uncheck to disable. By default, IP Address is enabled.

TCP/UDP Port Number

The TCP/UDP port number can be used to calculate the destination port for the frame. Check to enable the use of the TCP/UDP Port Number, or uncheck to disable. By default, TCP/UDP Port Number is enabled.

Aggregation Group Configuration

Locality

Indicates the aggregation group type. This field is only valid for stackable switches.

- **Global:** The group members may reside on different units in the stack. Each global aggregation may consist of up to 8 members.

- **Local:** The group members reside on the same unit. Each local aggregation may consist of up to 16 members.

Group ID

Indicates the group ID for the settings contained in the same row. Group ID "Normal" indicates there is no aggregation. Only one group ID is valid per port.

Port Members

Each switch port is listed for each group ID. Select a radio button to include a port in an aggregation, or clear the radio button to remove the port from the aggregation. By default, no ports belong to any aggregation group. Only full duplex ports can join an aggregation and ports must be in the same speed in each group.

Buttons

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

3.1.5.2. Aggregation - LACP

LACP Port Configuration for Switch 1

Port	LACP Enabled	Key		Role		Timeout		Prio
*	☐	<>	∨	<>	∨	<>	∨	32768
1	☐	Auto	∨	Active	∨	Fast	∨	32768
2	☐	Auto	∨	Active	∨	Fast	∨	32768
3	☐	Auto	∨	Active	∨	Fast	∨	32768
4	☐	Auto	∨	Active	∨	Fast	∨	32768
5	☐	Auto	∨	Active	∨	Fast	∨	32768
6	☐	Auto	∨	Active	∨	Fast	∨	32768
7	☐	Auto	∨	Active	∨	Fast	∨	32768
8	☐	Auto	∨	Active	∨	Fast	∨	32768
9	☐	Auto	∨	Active	∨	Fast	∨	32768
10	☐	Auto	∨	Active	∨	Fast	∨	32768
11	☐	Auto	∨	Active	∨	Fast	∨	32768
12	☐	Auto	∨	Active	∨	Fast	∨	32768
13	☐	Auto	∨	Active	∨	Fast	∨	32768
14	☐	Auto	∨	Active	∨	Fast	∨	32768
15	☐	Auto	∨	Active	∨	Fast	∨	32768
16	☐	Auto	∨	Active	∨	Fast	∨	32768
17	☐	Auto	∨	Active	∨	Fast	∨	32768
18	☐	Auto	∨	Active	∨	Fast	∨	32768
19	☐	Auto	∨	Active	∨	Fast	∨	32768
20	☐	Auto	∨	Active	∨	Fast	∨	32768
21	☐	Auto	∨	Active	∨	Fast	∨	32768
22	☐	Auto	∨	Active	∨	Fast	∨	32768
23	☐	Auto	∨	Active	∨	Fast	∨	32768
24	☐	Auto	∨	Active	∨	Fast	∨	32768
25	☐	Auto	∨	Active	∨	Fast	∨	32768
26	☐	Auto	∨	Active	∨	Fast	∨	32768

Save Reset

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

The LACP port settings relate to the currently selected stack unit, as reflected by the page header.

Port
The switch port number.

LACP Enabled
Controls whether LACP is enabled on this switch port. LACP will form an aggregation when 2 or more ports are connected to the same partner. LACP can form max 12 LLAGs per switch and 2 GLAGs per stack.

Key
The Key value incurred by the port, range 1-65535 . The Auto setting will set the key as appropriate by the physical link speed, 10Mb = 1, 100Mb = 2, 1Gb = 3. Using the Specific setting, a user-defined value can be entered. Ports with the same Key value can participate in the same aggregation group, while ports with different keys cannot.

Role
The Role shows the LACP activity status. The Active will transmit LACP packets each second, while Passive will wait for a LACP packet from a partner (speak if spoken to).

Timeout

The Timeout controls the period between BPDU transmissions. Fast will transmit LACP packets each second, while Slow will wait for 30 seconds before sending a LACP packet.

Prio

The Prio controls the priority of the port. If the LACP partner wants to form a larger group than is supported by this device then this parameter will control which ports will be active and which ports will be in a backup role. Lower number means greater priority.

Buttons

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

3.1.6. Configuration - Loop Protection

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

General Settings

Enable Loop Protection

Controls whether loop protections is enabled (as a whole).

Transmission Time

The interval between each loop protection PDU sent on each port. valid values are 1 to 10 seconds.

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).

Port Configuration

Port

The switch port number of the port.

Enable

Controls whether loop protection is enabled on this switch port.

Action

Configures the action performed when a loop is detected on a port. Valid values are Shutdown Port, Shutdown Port and Log or Log Only.

Tx Mode

Controls whether the port is actively generating loop protection PDU's, or whether it is just passively looking for looped PDU's.

Buttons

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

3.1.7. Configuration - Spanning Tree

3.1.7.1. Spanning Tree - Bridge Settings

STP Bridge Configuration

Basic Settings

Protocol Version	MSTP
Bridge Priority	32768
Forward Delay	15
Max Age	20
Maximum Hop Count	20
Transmit Hold Count	6

Advanced Settings

Edge Port BPDU Filtering	☐
Edge Port BPDU Guard	☐
Port Error Recovery	☐
Port Error Recovery Timeout	

Save   Reset

This page allows you to configure STP system settings. The settings are used by all STP Bridge instances in the Switch Stack.

Basic Settings

Protocol Version

The MSTP / RSTP / STP protocol version setting. Valid values are STP, RSTP and MSTP.

Bridge Priority

Controls the bridge priority. Lower numeric values have better priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch forms a **Bridge Identifier.**

For MSTP operation, this is the priority of the CIST. Otherwise, this is the priority of the STP/RSTP bridge.

Forward Delay

The delay used by STP Bridges to transit Root and Designated Ports to Forwarding (used in STP compatible mode). Valid values are in the range 4 to 30 seconds.

Max Age

The maximum age of the information transmitted by the Bridge when it is the Root Bridge. Valid values are in the range 6 to 40 seconds, and MaxAge must be <= (FwdDelay-1)*2.

Maximum Hop Count

This defines the initial value of remaining Hops for MSTI information generated at the boundary of an MSTI region. It defines how many bridges a root bridge can distribute its BPDU information to. Valid values are in the range 6 to 40 hops.

Transmit Hold Count

The number of BPDU's a bridge port can send per second. When exceeded, transmission of the next BPDU will be delayed. Valid values are in the range 1 to 10 BPDU's per second.

Advanced Settings

Edge Port BPDU Filtering

Control whether a port explicitly configured as Edge will transmit and receive BPDUs.

Edge Port BPDU Guard

Control whether a port explicitly configured as Edge will disable itself upon reception of a BPDU. The port will enter the error-disabled state, and will be removed from the active topology.

Port Error Recovery

Control whether a port in the error-disabled state automatically will be enabled after a certain time. If recovery is not enabled, ports have to be disabled and re-enabled for normal STP operation. The condition is also cleared by a system reboot.

Port Error Recovery Timeout

The time to pass before a port in the error-disabled state can be enabled. Valid values are between 30 and 86400 seconds (24 hours).

Buttons

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

3.1.7.2. Spanning Tree - MSTI Mapping

MSTI Configuration

Add VLANs separated by spaces or comma.

Unmapped VLANs are mapped to the CIST. (The default bridge instance).

Configuration Identification	
Configuration Name	00-03-ce-11-11-11
Configuration Revision	0

MSTI Mapping

MSTI	VLANs Mapped
MSTI1	
MSTI2	
MSTI3	
MSTI4	
MSTI5	
MSTI6	
MSTI7	

Save   Reset

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

Configuration Identification

Configuration Name

The name identifying the VLAN to MSTI mapping. Bridges must share the name and revision (see below), as well as the VLAN-to-MSTI mapping configuration in order to share spanning trees for MSTI's (Intra-region). The name is at most 32 characters.

Configuration Revision

The revision of the MSTI configuration named above. This must be an integer between 0 and 65535.

MSTI Mapping

MSTI

The bridge instance. The CIST is not available for explicit mapping, as it will receive the VLANs not explicitly mapped.

VLANs Mapped

The list of VLANs mapped to the MSTI. The VLANs can be given as a single (xx, xx being between 1 and 4094) VLAN, or a range (xx-yy), each of which must be separated with comma and/or space. A VLAN can only be mapped to one MSTI. An unused MSTI should just be left empty. (I.e. not having any VLANs mapped to it.) Example: 2,5,20-40.

Buttons

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

3.1.7.3. Spanning Tree - MSTI Priorities

MSTI Configuration

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

Save   Reset

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

MSTI

The bridge instance. The CIST is the default instance, which is always active.

Priority

Controls the bridge priority. Lower numeric values have better priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch forms a Bridge Identifier.

Buttons

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

3.1.7.4. Spanning Tree - CIST Ports

STP CIST Port Configuration

CIST Aggregated Port Configuration (Stack Global)

Port	STP Enabled	Path Cost		Priority	Admin Edge	Auto Edge	Restricted		BPDU Guard	Point-to-point
							Role	TCN		
-	☑	Auto	⌄	128 ⌄	Non-Edge ⌄	☑	☐	☐	☐	Forced True ⌄

CIST Normal Port Configuration for Switch 1

Port	STP Enabled	Path Cost		Priority	Admin Edge	Auto Edge	Restricted		BPDU Guard	Point-to-point
							Role	TCN		
*	☑	<>	⌄	<> ⌄	<> ⌄	☑	☐	☐	☐	<> ⌄
1	☑	Auto	⌄	128 ⌄	Non-Edge ⌄	☑	☐	☐	☐	Auto ⌄
2	☑	Auto	⌄	128 ⌄	Non-Edge ⌄	☑	☐	☐	☐	Auto ⌄
3	☑	Auto	⌄	128 ⌄	Non-Edge ⌄	☑	☐	☐	☐	Auto ⌄
4	☑	Auto	⌄	128 ⌄	Non-Edge ⌄	☑	☐	☐	☐	Auto ⌄
5	☑	Auto	⌄	128 ⌄	Non-Edge ⌄	☑	☐	☐	☐	Auto ⌄
6	☑	Auto	⌄	128 ⌄	Non-Edge ⌄	☑	☐	☐	☐	Auto ⌄
7	☑	Auto	⌄	128 ⌄	Non-Edge ⌄	☑	☐	☐	☐	Auto ⌄
8	☑	Auto	⌄	128 ⌄	Non-Edge ⌄	☑	☐	☐	☐	Auto ⌄
9	☑	Auto	⌄	128 ⌄	Non-Edge ⌄	☑	☐	☐	☐	Auto ⌄
10	☑	Auto	⌄	128 ⌄	Non-Edge ⌄	☑	☐	☐	☐	Auto ⌄
11	☑	Auto	⌄	128 ⌄	Non-Edge ⌄	☑	☐	☐	☐	Auto ⌄
12	☑	Auto	⌄	128 ⌄	Non-Edge ⌄	☑	☐	☐	☐	Auto ⌄
13	☑	Auto	⌄	128 ⌄	Non-Edge ⌄	☑	☐	☐	☐	Auto ⌄
14	☑	Auto	⌄	128 ⌄	Non-Edge ⌄	☑	☐	☐	☐	Auto ⌄
15	☑	Auto	⌄	128 ⌄	Non-Edge ⌄	☑	☐	☐	☐	Auto ⌄
16	☑	Auto	⌄	128 ⌄	Non-Edge ⌄	☑	☐	☐	☐	Auto ⌄
17	☑	Auto	⌄	128 ⌄	Non-Edge ⌄	☑	☐	☐	☐	Auto ⌄
18	☑	Auto	⌄	128 ⌄	Non-Edge ⌄	☑	☐	☐	☐	Auto ⌄
19	☑	Auto	⌄	128 ⌄	Non-Edge ⌄	☑	☐	☐	☐	Auto ⌄
20	☑	Auto	⌄	128 ⌄	Non-Edge ⌄	☑	☐	☐	☐	Auto ⌄
21	☑	Auto	⌄	128 ⌄	Non-Edge ⌄	☑	☐	☐	☐	Auto ⌄
22	☑	Auto	⌄	128 ⌄	Non-Edge ⌄	☑	☐	☐	☐	Auto ⌄
23	☑	Auto	⌄	128 ⌄	Non-Edge ⌄	☑	☐	☐	☐	Auto ⌄
24	☑	Auto	⌄	128 ⌄	Non-Edge ⌄	☑	☐	☐	☐	Auto ⌄
25	☑	Auto	⌄	128 ⌄	Non-Edge ⌄	☑	☐	☐	☐	Auto ⌄
26	☑	Auto	⌄	128 ⌄	Non-Edge ⌄	☑	☐	☐	☐	Auto ⌄

Save   Reset

This page allows the user to inspect the current STP CIST port configurations, and possibly change them as well.

This page contains settings for physical and aggregated ports. The aggregation settings are stack global.

The STP port settings relate to the currently selected stack unit, as reflected by the page header.

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 will set the path cost as appropriate by the physical link speed, using the 802.1D recommended values. Using the Specific setting, a user-defined value can be entered. The path cost is used when establishing the active topology of the network. Lower path cost ports are chosen as forwarding ports in favour of higher path cost ports. Valid values are in the range 1 to 200000000.

Priority

Controls the port priority. This can be used to control priority of ports having identical port cost. (See above).

operEdge (state flag)

Operational flag describing whether the port is connecting directly to edge devices. (No Bridges attached). Transition to the forwarding state is faster for edge ports (having operEdge true) than for other ports. The value of this flag is based on AdminEdge and AutoEdge fields. This flag is displayed as Edge in Monitor->Spanning Tree -> STP Detailed Bridge Status.

AdminEdge

Controls whether the operEdge flag should start as set or cleared. (The initial operEdge state when a port is initialized).

AutoEdge

Controls whether the bridge should enable automatic edge detection on the bridge port. This allows operEdge to be derived from whether BPDU's are received on the port or not.

Restricted Role

If enabled, causes the port not to be selected as Root Port for the CIST or any MSTI, even if it has the best spanning tree priority vector. Such a port will be selected as an Alternate Port after the Root Port has been selected. If set, it can cause lack of spanning tree connectivity. It can be set by a network administrator to prevent bridges external to a core region of the network influence the spanning tree active topology, possibly because those bridges are not under the full control of the administrator. This feature is also known as Root Guard.

Restricted TCN

If enabled, causes the port not to propagate received topology change notifications and topology changes to other ports. If set it can cause temporary loss of connectivity after changes in a spanning tree's active topology as a result of persistently incorrect learned station location information. It is set by a network administrator to prevent bridges external to a core region of the network, causing address flushing in that region, possibly because those bridges are not under the full control of the administrator or the physical link state of the attached LANs transits frequently.

BPDU Guard

If enabled, causes the port to disable itself upon receiving valid BPDU's. Contrary to the similar bridge setting, the port Edge status does not effect this setting.

A port entering error-disabled state due to this setting is subject to the bridge Port Error Recovery setting as well.

Point-to-Point

Controls whether the port connects to a point-to-point LAN rather than to a shared medium. This can be automatically determined, or forced either true or false. Transition to the forwarding state is faster for point-to-point LANs than for shared media.

Buttons

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

3.1.7.5. Spanning Tree - MSTI Ports

MSTI Port Configuration

Select MSTI

MST1 [ ] Get

MST1 MSTI Port Configuration

MSTI Aggregated Ports Configuration (Stack Global)

Port	Path Cost	Priority
-	Specific	128

MSTI Normal Ports Configuration for Switch 1

Port	Path Cost		Priority
*	<>		<>
1	Auto		128
2	Auto		128
3	Auto		128
4	Auto		128
5	Auto		128
6	Auto		128
7	Auto		128
8	Auto		128
9	Auto		128
10	Auto		128
11	Auto		128
12	Auto		128
13	Auto		128
14	Auto		128
15	Auto		128
16	Auto		128
17	Auto		128
18	Auto		128
19	Auto		128
20	Auto		128
21	Auto		128
22	Auto		128
23	Auto		128
24	Auto		128
25	Auto		128
26	Auto		128

Save   Reset

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

An MSTI port is a virtual port, which is instantiated separately for each active CIST (physical) port for each MSTI instance configured on and applicable to the port. The MSTI instance must be selected before displaying actual MSTI port configuration options.

This page contains MSTI port settings for physical and aggregated ports. The aggregation settings are stack global.

Apart from the selected MSTI, the STP MSTI port settings also relate to the currently selected stack unit, as reflected by the page header.

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 will set the path cost as appropriate by the physical link speed, using the 802.1D recommended values. Using the Specific setting, a user-defined value can be entered. The path cost is used when establishing the active topology of the network. Lower path cost ports are chosen as forwarding ports in favour of higher path cost ports. Valid values are in the range 1 to 200000000.

Priority

Controls the port priority. This can be used to control priority of ports having identical port cost. (See above).

Buttons

- **Get:** Click to retrieve settings for a specific MSTI.
- **Save:** Click to save changes.
- **Reset:** Click to undo any changes made locally and revert to previously saved values.

3.1.8. Configuration - MVR

MVR Configurations

Global Setting

MVR Mode   Enabled ⌄

VLAN Interface Setting for Switch 1 (Role [I:Inactive / S:Source / R:Receiver])

Delete	MVR VID	MVR Name	Mode	Tagging	Priority	LLQI	Interface Channel Setting
Delete			Dynamic ⌄	Tagged ⌄	0	5	
Port	1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28						
Role							

Add New MVR VLAN

This page provides MVR related configurations.

Most of the settings are global, whereas the Immediate Leave and MVR Port-Role configuration is related to the current selecting stack unit, as reflected by the page header.

The MVR feature enables multicast traffic forwarding on the Multicast VLANs. In a multicast television application, a PC or a network television or a set-top box can receive the multicast stream. Multiple set-top boxes or PCs can be connected to one subscriber port, which is a switch port configured as an MVR receiver port. When a subscriber selects a channel, the set-top box or PC sends an IGMP/MLD report message to Switch A to join the appropriate multicast group address. Uplink ports that send and receive multicast data to and from the multicast VLAN are called MVR source ports. It is allowed to create at maximum 8 MVR VLANs with corresponding channel settings for each Multicast VLAN. There will be totally at maximum 256 group addresses for channel settings.

MVR Mode

Enable/Disable the Global MVR.

The Unregistered Flooding control depends on the current configuration in IGMP/MLD Snooping.

It is suggested to enable Unregistered Flooding control when the MVR group table is full.

Delete

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

MVR VID

Specify the Multicast VLAN ID.

Note: MVR source ports are not recommended to be overlapped with management VLAN ports.

MVR Name

MVR Name is an optional attribute to indicate the name of the specific MVR VLAN. Maximum length of the MVR VLAN Name string is 32. MVR VLAN Name can only contain alphabets or numbers. When the optional MVR VLAN name is given, it should contain at least one alphabet. MVR VLAN name can be edited for the existing MVR VLAN entries or it can be added to the new entries.

Mode

Specify the MVR mode of operation. In Dynamic mode, MVR allows dynamic MVR membership reports on source ports. In Compatible mode, MVR membership reports are forbidden on source ports. The default is Dynamic mode.

Tagging

Specify whether the traversed IGMP/MLD control frames will be sent as Untagged or Tagged with MVR VID. The default is Tagged.

Priority

Specify how the traversed IGMP/MLD control frames will be sent in prioritized manner. The default Priority is 0.

LLQI

Define the maximum time to wait for IGMP/MLD report memberships on a receiver port before removing the port from multicast group membership. The value is in units of tenths of a seconds. The range is from 0 to 31744. The default LLQI is 5 tenths or one-half second.

Interface Channel Setting

When the MVR VLAN is created, click the Edit symbol ⓔ to expand the corresponding multicast channel settings for the specific MVR VLAN. Summary about the Interface Channel Setting (of the MVR VLAN) will be shown besides the Edit symbol.

Detail information regarding to the Interface Channel Setting will be covered on page 122.

Port

The logical port for the settings.

Port Role

Configure an MVR port of the designated MVR VLAN as one of the following roles.

- **Inactive (I):** The designated port does not participate MVR operations.
- **Source (S):** Configure uplink ports that receive and send multicast data as source ports. Subscribers cannot be directly connected to source ports.
- **Receiver (R):** Configure a port as a receiver port if it is a subscriber port and should only receive multicast data. It does not receive data unless it becomes a member of the multicast group by issuing IGMP/MLD messages.

Note: MVR source ports are not recommended to be overlapped with management VLAN ports.

Select the port role by clicking the Role symbol to switch the setting.

Immediate Leave Setting for Switch 1

Port	Immediate Leave
1	Disabled
2	Disabled
3	Disabled
4	Disabled
5	Disabled
6	Disabled
7	Disabled
8	Disabled
9	Disabled
10	Disabled
11	Disabled
12	Disabled
13	Disabled
14	Disabled
15	Disabled
16	Disabled
17	Disabled
18	Disabled
19	Disabled
20	Disabled
21	Disabled
22	Disabled
23	Disabled
24	Disabled
25	Disabled
26	Disabled
27	Disabled
28	Disabled

Save   Reset

Immediate Leave

Enable the fast leave on the port.

Buttons

- **Add New NVR VLAN:** Click to add new MVR VLAN. Specify the VID and configure the new entry. Click "Save".
- **Save:** Click to save changes.
- **Reset:** Click to undo any changes made locally and revert to previously saved values.

MVR Channel Configuration   Refresh |<<   >>

Navigate Channel Setting with MVR VID 1   by 16   entries per page.

| Delete | VLAN ID | VLAN Name | Start Address | End Address | Channel Name |

Add New MVR Channel

Save   Reset

This page provides MVR channel settings for a specific MVR VLAN.

Delete

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

VLAN ID

Display the specific Multicast VLAN ID. This field is not editable.

VLAN Name

Display the name of the specific Multicast VLAN. This field is not editable.

Start Address

The starting IPv4/IPv6 Multicast Group Address that will be used as a streaming channel.

End Address

The ending IPv4/IPv6 Multicast Group Address that will be used as a streaming channel.

Channel Name

Indicate the name of the Channel of the specific Multicast VLAN. Maximum length of the Channel Name string is 32. Channel Name can only contain alphabets or numbers. Channel name should contain at least one alphabet. Channel name can be edited for the existing Channel entries or it can be added to the new entries.

Buttons

- **Add New MVR Channel:** Click to add new Channel for a given MVR VLAN. Specify the Address and configure the new entry. Click "Save"
- **Save:** Click to save changes.
- **Reset:** Click to undo any changes made locally and revert to previously saved values.
- **Refresh:** Refreshes the displayed table starting from the input fields.
- **|<<:** Updates the table starting from the first entry in the MVR Channel Configuration for a specific MVR VLAN.
- **>>:** Updates the table, starting with the entry after the last entry currently displayed.

3.1.9. Configuration - IPMC

3.1.9.1. IPMC - IGMP Snooping

3.1.9.1.1. IPMC - IGMP Snooping - Basic Configuration

IGMP Snooping Configuration

Stack Global Settings

Global Configuration	
Snooping Enabled	☐
Unregistered IPMCv4 Flooding Enabled	☑
IGMP SSM Range	232.0.0.0 / 8
Leave Proxy Enabled	☐
Proxy Enabled	☐

Port Related Configuration for Switch 1

Port	Router Port	Fast Leave	Throttling
*	☐	☐	<>
1	☐	☐	unlimited
2	☐	☐	unlimited
3	☐	☐	unlimited
4	☐	☐	unlimited
5	☐	☐	unlimited
25	☐	☐	unlimited
26	☐	☐	unlimited

Save Reset

This page provides IGMP Snooping related configuration.

Most of the settings are global, whereas the Router Port configuration is related to the currently selected stack unit, as reflected by the page header.

Snooping Enabled

Enable the Global IGMP Snooping.

Unregistered IPMCv4 Flooding Enabled

Enable unregistered IPMCv4 traffic flooding.

The flooding control takes effect only when IGMP Snooping is enabled.

When IGMP Snooping is disabled, unregistered IPMCv4 traffic flooding is always active in spite of this setting.

IGMP SSM Range

SSM (Source-Specific Multicast) Range allows the SSM-aware hosts and routers run the SSM service model for the groups in the address range.

Leave Proxy Enabled

Enable IGMP Leave Proxy. This feature can be used to avoid forwarding unnecessary leave messages to the router side.

Proxy Enabled

Enable IGMP Proxy. This feature can be used to avoid forwarding unnecessary join and leave messages to the router side.

Router Port

Specify which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or IGMP querier.

If an aggregation member port is selected as a router port, the whole aggregation will act as a router port.

Fast Leave

Enable the fast leave on the port.

Throttling

Enable to limit the number of multicast groups to which a switch port can belong.

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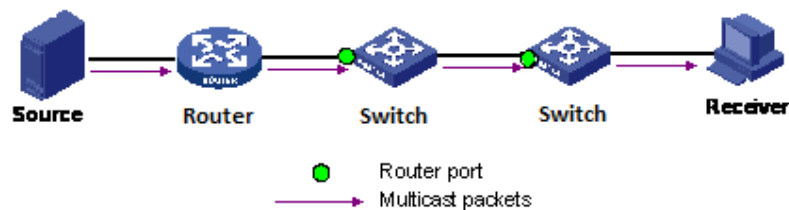
- **Save:** Click to save changes.
- **Reset:** Click to undo any changes made locally and revert to previously saved values.

3.1.9.1.2. IPMC - IGMP Snooping - VLAN Configuration

IGMP Snooping VLAN Configuration   Refresh |<<   >>

Start from VLAN 1   with 20   entries per page.

Delete	VLAN ID	Snooping Enabled	IGMP Querier	Compatibility	RV	QI (sec)	QRI (0.1 sec)	LLQI (0.1 sec)	URI (sec)

Add New IGMP VLAN

Save   Reset

Each page shows up to 99 entries from the VLAN table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the VLAN Table. The first displayed will be the one with the lowest VLAN ID found in the VLAN Table.

The "VLAN" input fields allow the user to select the starting point in the VLAN Table. Clicking the **Refresh** button will update the displayed table starting from that or the next closest VLAN Table match.

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

IGMP Snooping VLAN Table Columns

Delete

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

VLAN ID

The VLAN ID of the entry.

IGMP Snooping Enabled

Enable the per-VLAN IGMP Snooping. Up to 32 VLANs can be selected for IGMP Snooping.

IGMP Querier

Enable the IGMP Querier in the VLAN.

Compatibility

Compatibility is maintained by hosts and routers taking appropriate actions depending on the versions of IGMP operating on hosts and routers within a network. The allowed selection is IGMP-Auto, Forced IGMPv1, Forced IGMPv2, Forced IGMPv3, default compatibility value is IGMP-Auto.

RV

Robustness Variable. The Robustness Variable allows tuning for the expected packet loss on a network. The allowed range is 1 to 255, default robustness variable value is 2.

QI

Query Interval. The Query Interval is the interval between General Queries sent by the Querier. The allowed range is 1 to 31744 seconds, default query interval is 125 seconds.

QRI

Query Response Interval. The Maximum Response Delay used to calculate the Maximum Response Code inserted into the periodic General Queries. The allowed range is 0 to 31744 in tenths of seconds, default query response interval is 100 in tenths of seconds (10 seconds).

LLQI (LMQI for IGMP)

Last Member Query Interval. The Last Member Query Time is the time value represented by the Last Member Query Interval, multiplied by the Last Member Query Count. The allowed range is 0 to 31744 in tenths of seconds, default last member query interval is 10 in tenths of seconds (1 second).

URI

Unsolicited Report Interval. The Unsolicited Report Interval is the time between repetitions of a host's initial report of membership in a group. The allowed range is 0 to 31744 seconds, default unsolicited report interval is 1 second.

Buttons

- **Refresh:** Refreshes the displayed table starting from the "VLAN" input fields.
- **|<<:** Updates the table starting from the first entry in the VLAN Table, i.e. the entry with the lowest VLAN ID.
- **>>:** Updates the table, starting with the entry after the last entry currently displayed.
- **Add New IGMP VLAN:** Click to add new IGMP VLAN. Specify the VID and configure the new entry. Click "Save". The specific IGMP VLAN starts working after the corresponding static VLAN is also created.
- **Save:** Click to save changes.
- **Reset:** Click to undo any changes made locally and revert to previously saved values.

3.1.9.1.3. IPMC - IGMP Snooping - Port Group Filtering

IGMP Snooping Port Group Filtering Configuration for Switch 1

Delete	Port	Filtering Groups
Delete	1 ⌄	

Add New Filtering Group

Save   Reset

Delete

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

Port

The logical port for the settings.

Filtering Groups

The IP Multicast Group that will be filtered.

Add New Filtering Group

Click "**Add New Filtering Group**" button to add a new entry to the Group Filtering table. Specify

the Port, and Filtering Group of the new entry. Click "Save".

Buttons

- **Add New Filtering Group:** Click to add a new entry to the Group Filtering table.

- **Save:** Click to save changes.

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

3.1.9.2. IPMC - MLD Snooping

3.1.9.2.1. IPMC - MLD Snooping - Basic Configuration

MLD Snooping Configuration

Stack Global Settings

Global Configuration	
Snooping Enabled	☐
Unregistered IPMCv6 Flooding Enabled	☑
MLD SSM Range	ff3e:: / 96
Leave Proxy Enabled	☐
Proxy Enabled	☐

Port Related Configuration for Switch 1

Port	Router Port	Fast Leave	Throttling
*	☐	☐	<>
1	☐	☐	unlimited
2	☐	☐	unlimited
3	☐	☐	unlimited
25	☐	☐	unlimited
26	☐	☐	unlimited

Save   Reset

This page provides MLD Snooping related configuration.

Most of the settings are global, whereas the Router Port configuration is related to the currently selected stack unit, as reflected by the page header.

Snooping Enabled

Enable the Global MLD Snooping.

Unregistered IPMCv6 Flooding Enabled

Enable unregistered IPMCv6 traffic flooding.

The flooding control takes effect only when MLD Snooping is enabled.

When MLD Snooping is disabled, unregistered IPMCv6 traffic flooding is always active in spite of this setting.

MLD SSM Range

SSM (Source-Specific Multicast) Range allows the SSM-aware hosts and routers run the SSM service model for the groups in the address range.

Leave Proxy Enabled

Enable MLD Leave Proxy. This feature can be used to avoid forwarding unnecessary leave messages to the router side.

Proxy Enabled

Enable MLD Proxy. This feature can be used to avoid forwarding unnecessary join and leave

messages to the router side.

Router Port

Specify which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or MLD querier.

If an aggregation member port is selected as a router port, the whole aggregation will act as a router port.

Fast Leave

Enable the fast leave on the port.

Throttling

Enable to limit the number of multicast groups to which a switch port can belong.

Buttons

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

3.1.9.2.2. IPMC - MLD Snooping - VLAN Configuration

Each page shows up to 99 entries from the VLAN table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the VLAN Table. The first displayed will be the one with the lowest VLAN ID found in the VLAN Table.

The "VLAN" input fields allow the user to select the starting point in the VLAN Table. Clicking the **Refresh** button will update the displayed table starting from that or the next closest VLAN Table match.

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

MLD Snooping VLAN Table Columns

Delete

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

VLAN ID

The VLAN ID of the entry.

MLD Snooping Enabled

Enable the per-VLAN MLD Snooping. Up to 32 VLANs can be selected for MLD Snooping.

MLD Querier

Enable the IGMP Querier in the VLAN.

Compatibility

Compatibility is maintained by hosts and routers taking appropriate actions depending on the versions of MLD operating on hosts and routers within a network. The allowed selection is MLD-Auto, Forced MLDv1, Forced MLDv2, default compatibility value is MLD-Auto.

RV

Robustness Variable. The Robustness Variable allows tuning for the expected packet loss on a link. The allowed range is 1 to 255, default robustness variable value is 2.

QI

Query Interval. The Query Interval is the interval between General Queries sent by the Querier.

The allowed range is 1 to 31744 seconds, default query interval is 125 seconds.

QRI

Query Response Interval. The Maximum Response Delay used to calculate the Maximum Response Code inserted into the periodic General Queries. The allowed range is 0 to 31744 in tenths of seconds, default query response interval is 100 in tenths of seconds (10 seconds).

LLQI

Last Listener Query Interval. The Last Listener Query Interval is the Maximum Response Delay used to calculate the Maximum Response Code inserted into Multicast Address Specific Queries sent in response to Version 1 Multicast Listener Done messages. It is also the Maximum Response Delay used to calculate the Maximum Response Code inserted into Multicast Address and Source Specific Query messages. The allowed range is 0 to 31744 in tenths of seconds, default last listener query interval is 10 in tenths of seconds (1 second).
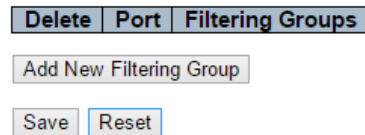
URI

Unsolicited Report Interval. The Unsolicited Report Interval is the time between repetitions of a node's initial report of interest in a multicast address. The allowed range is 0 to 31744 seconds, default unsolicited report interval is 1 second.

Buttons

- **Refresh:** Refreshes the displayed table starting from the "VLAN" input fields.
- **|<<:** Updates the table starting from the first entry in the VLAN Table, i.e. the entry with the lowest VLAN ID.
- **>>:** Updates the table, starting with the entry after the last entry currently displayed.
- **Add New MLD VLAN:** Click to add new MLD VLAN. Specify the VID and configure the new entry. Click "Save". The specific MLD VLAN starts working after the corresponding static VLAN is also created.
- **Save:** Click to save changes.
- **Reset:** Click to undo any changes made locally and revert to previously saved values.

3.1.9.2.3. IPMC - MLD Snooping - Port Group Filtering

MLD Snooping Port Group Filtering Configuration for Switch 1

| Delete | Port | Filtering Groups |

Add New Filtering Group

Save   Reset

Delete

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

Port

The logical port for the settings.

Filtering Groups

The IP Multicast Group that will be filtered.

Add New Filtering Group

Click "**Add New Filtering Group**" button to add a new entry to the Group Filtering table. Specify the Port, and Filtering Group of the new entry. Click "Save".

Buttons

- **Add New Filtering Group:** Click to add a new entry to the Group Filtering table.
- **Save:** Click to save changes.
- **Reset:** Click to undo any changes made locally and revert to previously saved values.

3.1.10. Configuration - LLDP

3.1.10.1. LLDP - LLDP

LLDP Configuration

LLDP Parameters

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

LLDP Port Configuration for Switch 1

Port	Mode	CDP aware	Optional TLVs				
			Port Descr	Sys Name	Sys Descr	Sys Capa	Mgmt Addr
*	<>	☐	✔	✔	✔	✔	✔
1	Enabled	☐	✔	✔	✔	✔	✔
2	Enabled	☐	✔	✔	✔	✔	✔
3	Enabled	☐	✔	✔	✔	✔	✔
4	Enabled	☐	✔	✔	✔	✔	✔
5	Enabled	☐	✔	✔	✔	✔	✔
6	Enabled	☐	✔	✔	✔	✔	✔
7	Enabled	☐	✔	✔	✔	✔	✔
25	Enabled	☐	✔	✔	✔	✔	✔
26	Enabled	☐	✔	✔	✔	✔	✔

Save   Reset

This page allows the user to inspect and configure the current LLDP port settings.

LLDP Parameters

Tx Interval

The switch periodically transmits LLDP frames to its neighbors for having the network discovery information up-to-date. The interval between each LLDP frame is determined by the Tx Interval value. Valid values are restricted to 5 - 32768 seconds.

Tx Hold

Each LLDP frame contains information about how long the information in the LLDP frame shall be considered valid. The LLDP information valid period is set to Tx Hold multiplied by Tx Interval seconds. Valid values are restricted to 2 - 10 times.

Tx Delay

If some configuration is changed (e.g. the IP address) a new LLDP frame is transmitted, but the time between the LLDP frames will always be at least the value of Tx Delay seconds. Tx Delay cannot be larger than 1⁄4 of the Tx Interval value. Valid values are restricted to 1 - 8192 seconds.

Tx Reinit

When a port is disabled, LLDP is disabled or the switch is rebooted, an LLDP shutdown frame is transmitted to the neighboring units, Signaling that the LLDP information isn't valid anymore. Tx Reinit controls the amount of seconds between the shutdown frame and a new LLDP initialization. Valid values are restricted to 1 - 10 seconds.

LLDP Port Configuration

The LLDP port settings relate to the currently selected stack unit, as reflected by the page header.

Port

The switch port number of the logical LLDP port.

Mode

Select LLDP mode.

Rx only The switch will not send out LLDP information, but LLDP information from neighbor units is analyzed.

Tx only The switch will drop LLDP information received from neighbors, but will send out LLDP information.

Disabled The switch will not send out LLDP information, and will drop LLDP information received from neighbors.

Enabled The switch will send out LLDP information, and will analyze LLDP information received from neighbors.

CDP Aware

Select CDP awareness.

The CDP operation is restricted to decoding incoming CDP frames (The switch doesn't transmit CDP frames). CDP frames are only decoded if LLDP on the port is enabled.

Only CDP TLVs that can be mapped to a corresponding field in the LLDP neighbors' table are decoded. All other TLVs are discarded (Unrecognized CDP TLVs and discarded CDP frames are not shown in the LLDP statistics.). CDP TLVs are mapped onto LLDP neighbors' table as shown below.

CDP TLV "Device ID" is mapped to the LLDP "Chassis ID" field.

CDP TLV "Address" is mapped to the LLDP "Management Address" field. The CDP address TLV can contain multiple addresses, but only the first address is shown in the LLDP neighbors table.

CDP TLV "Port ID" is mapped to the LLDP "Port ID" field.

CDP TLV "Version and Platform" is mapped to the LLDP "System Description" field.

Both the CDP and LLDP support "system capabilities", but the CDP capabilities cover capabilities that are not part of the LLDP. These capabilities are shown as "others" in the LLDP neighbors' table.

If all ports have CDP awareness disabled the switch forwards CDP frames received from neighbor devices. If at least one port has CDP awareness enabled all CDP frames are terminated by the switch.

Note: When CDP awareness on a port is disabled the CDP information isn't removed immediately, but gets removed when the hold time is exceeded.

Port Descr

Optional TLV: When checked the "port description" is included in LLDP information transmitted.

Sys Name

Optional TLV: When checked the "system name" is included in LLDP information transmitted.

Sys Descr

Optional TLV: When checked the "system description" is included in LLDP information transmitted.

Sys Capa

Optional TLV: When checked the "system capability" is included in LLDP information transmitted.

Mgmt Addr

Optional TLV: When checked the "management address" is included in LLDP information transmitted.

Buttons

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

3.1.10.2. LLDP - LLDP-MED

LLDP-MED Configuration

Fast Start Repeat Count

Fast start repeat count	4

Coordinates Location

| Latitude | 0 | ° | North | ⌄ | Longitude | 0 | ° | East | ⌄ | Altitude | 0 | | Meters | ⌄ | Map Datum | WGS84 | ⌄ |

Civic Address Location

Country code		State		County	
City		City district		Block (Neighbourhood)	
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

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

Fast start repeat count

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), both in order to conserve the limited LLDPU space and to reduce security and system integrity issues that can come with inappropriate knowledge of the network policy.

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

Because 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 would be repeated. The recommended value is 4 times, given that 4 LLDP frames with a 1 second interval will be transmitted, when an LLDP frame with new information is received.

It should be noted that 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 as such does not apply to links between LAN infrastructure elements, including Network Connectivity Devices, or other types of links.

Coordinates Location

Latitude

Latitude SHOULD be normalized to within 0-90 degrees with a maximum of 4 digits. It is possible to specify the direction to either North of the equator or South of the equator.

Longitude

Longitude SHOULD be normalized to within 0-180 degrees with a maximum of 4 digits. It is possible to specify the direction to either East of the prime meridian or West of the prime meridian.

Altitude

Altitude SHOULD be normalized to within -32767 to 32767 with a maximum of 4 digits.

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 would use 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).

Country code

The two-letter ISO 3166 country code in capital ASCII letters - Example: DK, DE or US.

State

National subdivisions (state, canton, region, province, prefecture).

County

County, parish, gun (Japan), district.

City

City, township, shi (Japan) - Example: Copenhagen.

City district

City division, borough, city district, ward, chou (Japan).

Block (Neighborhood)

Neighborhood, block.

Street

Street - Example: Poppelvej.

Leading street direction

Leading street direction - Example: N.

Trailing street suffix

Trailing street suffix - Example: SW.

Street suffix

Street suffix - Example: Ave, Platz.

House no.

House number - Example: 21.

House no. suffix

House number suffix - Example: A, 1/2.

Landmark

Landmark or vanity address - Example: Columbia University.

Additional location info

Additional location info - Example: South Wing.

Name

Name (residence and office occupant) - Example: Flemming Jahn.

Zip code

Postal/zip code - Example: 2791.

Building

Building (structure) - Example: Low Library.

Apartment

Unit (Apartment, suite) - Example: Apt 42.

Floor

Floor - Example: 4.

Room no.

Room number - Example: 450F.

Place type

Place type - Example: Office.

Postal community name

Postal community name - Example: Leonia.

P.O. Box

Post office box (P.O. BOX) - Example: 12345.

Additional code

Additional code - Example: 1320300003.

Emergency Call Service

Emergency Call Service (e.g. E911 and others), such as defined by TIA or NENA.

Emergency Call Service

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.

Policies

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:

1. Layer 2 VLAN ID (IEEE 802.1Q-2003)
2. Layer 2 priority value (IEEE 802.1D-2004)
3. 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:

1. Voice
2. Guest Voice
3. Softphone Voice
4. Video Conferencing
5. Streaming Video
6. 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.

It should be noted that 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 polices that shall be mapped to the specific ports.

Application Type

Intended use of the application types:

1. 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.

2. 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 should not be advertised if all the same network policies apply as those advertised in the Voice application policy.

3. 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.

4. 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 should not be advertised if all the same network policies apply as those advertised in the Guest Voice application policy.

5. 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 below), then the L2 priority field is ignored and only the DSCP value has relevance.

6. Video Conferencing - for use by dedicated Video Conferencing equipment and other similar appliances supporting real-time interactive video/audio services.

7. 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.

8. 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 indicating whether 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 port 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 through 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 to be used to provide Diffserv node behaviour for the specified application type as defined in IETF RFC 2474. DSCP may contain one of 64 code point values (0 through 63). A value of 0 represents use of the default DSCP value as defined in RFC 2475.

Adding a new policy

Click "**Add New Policy**" to add a new policy. Specify the Application type, Tag, VLAN ID, L2 Priority and DSCP for the new policy. Click "Save".

The number of policies supported is 32

Port Policies Configuration

Every port may advertise a unique set of network policies or different attributes for the same network policies, based on the authenticated user identity or port configuration.

Port

The port number to which the configuration applies.

Policy Id

The set of policies that shall apply to a given port. The set of policies is selected by check marking the checkboxes that corresponds to the policies.

Buttons

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

3.1.11. Configuration - PoE

Power Over Ethernet Configuration

Reserved Power determined by	◉ Class	○ Allocation	○ LLDP-MED
Power Management Mode	○ Actual Consumption	◉ Reserved Power	

PoE Power Supply Configuration for Switch 1

Primary Power Supply [W]
400

PoE Port Configuration for Switch 1

Port	PoE Mode	Priority	Maximum Power [W]
*	<>	<>	15.4
1	PoE+	Low	15.4
2	PoE+	Low	15.4
3	PoE+	Low	15.4
4	PoE+	Low	15.4
23	PoE+	Low	15.4
24	PoE+	Low	15.4

Save   Reset

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

Power over Ethernet Configuration

Reserved Power determined by

There are three modes for configuring how the ports/PDs may reserve power.

1. Allocated mode: In this mode the user allocates the amount of power that each port may reserve. The allocated/reserved power for each port/PD is specified in the Maximum Power fields.

2. Class mode: In this mode each port automatically determines how much power to reserve according to the class the connected PD belongs to, and reserves the power accordingly. Four different port classes exist and one for 4, 7, 15.4 or 30 Watts. In this mode the Maximum Power fields have no effect.

3. LLDP-MED mode: This mode is similar to the Class mode expect that each port determine the amount power it reserves by exchanging PoE information using the LLDP protocol and reserves power accordingly. If no LLDP information is available for a port, the port will reserve power using the class mode. In this mode the Maximum Power fields have no effect

For all modes: If a port uses more power than the reserved power for the port, the port is shut down.

Power Management Mode

There are 2 modes for configuring when to shut down the ports:

1. Actual Consumption: In this mode the ports are shut down when the actual power consumption for all ports exceeds the amount of power that the power supply can deliver or if the actual power consumption for a given port exceeds the reserved power for that port. The ports are shut down according to the ports priority. If two ports have the same priority the port with the highest port number is shut down.

2. Reserved Power: In this mode the ports are shut down when total reserved powered exceeds the amount of power that the power supply can deliver. In this mode the port power is not turned on if the PD requests more power than available from the power supply.

Power Supply Configuration

Primary and Backup Power Source

Some switches support having two PoE power supplies. One is used as primary power source, and one as backup power source. If the switch doesn't support backup power supply only the primary power supply settings will be shown. In case that the primary power source fails the backup power source will take over. For being able to determine the amount of power the PD may use, it must be defined what amount of power the primary and backup power sources can deliver.

Valid values are in the range 0 to 2000 Watts.

Port Configuration

Port

This is the logical port number for this row.

Ports that are not PoE-capable are grayed out and thus impossible to configure PoE for.

PoE Mode

The PoE Mode represents the PoE operating mode for the port.
- **Disabled:** PoE disabled for the port.
- **PoE:** Enables PoE IEEE 802.3af (Class 4 PDs limited to 15.4W)
- **PoE+**: Enables PoE+ IEEE 802.3at (Class 4 PDs limited to 30W)

Priority

The Priority represents the ports priority. There are three levels of power priority named Low, High and Critical.

The priority is used in the case where the remote devices requires more power than the power supply can deliver. In this case the port with the lowest priority will be turn off starting from the port with the highest port number.

Maximum Power

The Maximum Power value contains a numerical value that indicates the maximum power in watts that can be delivered to a remote device.

The maximum allowed value is 30 W.

Buttons

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

3.1.12. Configuration - MAC Table

MAC Address Table Configuration

Stack Aging Configuration

Disable Automatic Aging	☐
Aging Time	300 seconds

MAC Table Learning for Switch 1

	Port Members
	1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26
Auto	⦿ ⦿
Disable	○ ○
Secure	○ ○

Static MAC Table Configuration for Switch 1

			Port Members
Delete	VLAN ID	MAC Address	1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26

Add New Static Entry

Save Reset

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

Aging Configuration

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

Configure aging time by entering a value here in seconds. The allowed range is 10 to 1000000 seconds.

Disable the automatic aging of dynamic entries by checking the "**Disable automatic aging**" checkbox. .

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

Static MAC Table Configuration

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

The maximum of 64 entries is for the whole stack, and not per switch.

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.

Adding a New Static Entry

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

Buttons

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

3.1.13. Configuration - VLANs

3.1.13.1. VLANs - VLAN Membership

The VLAN membership configuration for the selected stack switch unit can be monitored and modified here. Up to 4096 VLANs are supported. This page allows for adding and deleting VLANs as well as adding and deleting port members of each VLAN.

Navigating the VLAN Table

Each page shows up to 99 entries from the VLAN table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the VLAN Table. The first displayed will be the one with the lowest VLAN ID found in the VLAN Table.

The "VLAN" input fields allow the user to select the starting point in the VLAN Table. Clicking the "**Refresh**" button will update the displayed table starting from that or the closest next VLAN Table match. The "**>>**" will use the last entry of the currently displayed VLAN entry as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the "**|<<**" button to start over.

Delete

To delete a VLAN entry, check this box. The entry will be deleted on the selected switch in the stack. If none of the ports of this switch are members of a VLAN then the delete checkbox will be greyed out (you cannot delete that entry. during the next Save.

VLAN ID

Indicates the ID of this particular VLAN.

VLAN Name

Indicates the name of the VLAN. Maximum length of the VLAN Name String is 32. VLAN Name can be null. If it is not null, it must contain alphabets or numbers. At least one alphabet must be present in a non-null VLAN name. VLAN name can be edited for the existing VLAN entries or it can be added to the new entries.

Port Members

A row of check boxes for each port is displayed for each VLAN ID.

To include a port in a VLAN, check the box as port.

To include a port in a forbidden port list, check the box as shown forbid.

To remove or exclude the port from the VLAN, make sure the box is unchecked as shown menu_o.

By default, no ports are members, and for every new VLAN entry all boxes are unchecked.

Adding a New VLAN

Click "**Add New VLAN**" to add a new VLAN ID. An empty row is added to the table, and the VLAN can be configured as needed. Legal values for a VLAN ID are 1 through 4095.

The VLAN is enabled on the selected stack switch unit when you click on "Save". The VLAN is thereafter present on the other stack switch units, but with no port members. The check box is greyed out when VLAN is displayed on other stacked switches, but user can add member ports to it.

The "**Delete**" button can be used to undo the addition of new VLANs.

Buttons

- **Save:** Click to save changes.
- **Reset:** Click to undo any changes made locally and revert to previously saved values.
- **Refresh:** Refreshes the displayed table starting from the "VLAN ID" input fields.
- **>>|:** Updates the table starting from the first entry in the VLAN Table, i.e. the entry with the lowest VLAN ID.
- **<<:** Updates the table, starting with the entry after the last entry currently displayed.

3.1.13.2. VLANs - Ports

Ethertype for Custom S-ports 0x 88A8   Auto-refresh ☐ Refresh

VLAN Port Configuration for Switch 1

Port	Port Type	Ingress Filtering	Frame Type	Port VLAN Mode	ID	Tx Tag
*	<>	☐	<>	<>	1	<>
1	Unaware	☐	All	Specific	1	Untag_pvid
2	Unaware	☐	All	Specific	1	Untag_pvid
3	Unaware	☐	All	Specific	1	Untag_pvid
4	Unaware	☐	All	Specific	1	Untag_pvid
25	Unaware	☐	All	Specific	1	Untag_pvid
26	Unaware	☐	All	Specific	1	Untag_pvid

Save   Reset

This page is used for configuring the selected stack switch unit port VLAN.

Ethertype for Custom S-ports

This field specifies the ether type used for Custom S-ports. This is a global setting for all the Custom S-ports.

Port

This is the logical port number of this row.

Port Type

Port can be one of the following types: Unaware, Customer port(C-port), Service port(S-port),

Custom Service port(S-custom-port)

If Port Type is Unaware, all frames are classified to the Port VLAN ID and tags are not removed.

Ingress Filtering

Enable ingress filtering on a port by checking the box. This parameter affects VLAN ingress processing. If ingress filtering is enabled and the ingress port is not a member of the classified VLAN of the frame, the frame is discarded. By default, ingress filtering is disabled (no checkmark).

Frame Type

Determines whether the port accepts all frames or only tagged/untagged frames. This parameter affects VLAN ingress processing. If the port only accepts tagged frames, untagged frames received on the port are discarded. By default, the field is set to All.

Port VLAN Mode

Configures the Port VLAN Mode. The allowed values are None or Specific. This parameter affects VLAN ingress and egress processing.

If None is selected, a VLAN tag with the classified VLAN ID is inserted in frames transmitted on the port. This mode is normally used for ports connected to VLAN aware switches. Tx tag should be set to

Untag_pvid when this mode is used.

If Specific (the default value) is selected, a Port VLAN ID can be configured (see below). Untagged frames received on the port are classified to the Port VLAN ID. If VLAN awareness is disabled, all frames received on the port are classified to the Port VLAN ID. If the classified VLAN ID of a frame transmitted on the port is different from the Port VLAN ID, a VLAN tag with the classified VLAN ID is inserted in the frame.

Port VLAN ID

Configures the VLAN identifier for the port. The allowed values are from 1 through 4095. The default value is 1.

Note: The port must be a member of the same VLAN as the Port VLAN ID.

Tx Tag

Determines egress tagging of a port. Untag_pvid - All VLANs except the configured PVID will be tagged. Tag_all - All VLANs are tagged. Untag_all - All VLANs are untagged.

Buttons

- **Auto-refresh:** Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
- **Refresh:** Click to refresh the page immediately.
- **Save:** Click to save changes.
- **Reset:** Click to undo any changes made locally and revert to previously saved values.

3.1.14. Configuration - Private VLAN

3.1.14.1. Private VLAN - Port Isolation

Overview

This page is used for enabling or disabling port isolation on ports in a Private VLAN.

A port member of a VLAN can be isolated to other isolated ports on the same VLAN.

The port settings relate to the currently selected stack unit, as reflected by the page header.

This feature works across the stack.

Configuration

Port Members

A check box is provided for each port of a private VLAN.

When checked, port isolation is enabled on that port.

When unchecked, port isolation is disabled on that port.

By default, port isolation is disabled on all ports.

Buttons

- **Auto-refresh:** Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
- **Refresh:** Click to refresh the page immediately.
- **Save:** Click to save changes.
- **Reset:** Click to undo any changes made locally and revert to previously saved values.

3.1.15. Configuration - VCL

3.1.15.1. VCL - MAC-based VLAN

The MAC-based VLAN entries can be configured here. This page allows for adding and deleting MAC-based VLAN entries and assigning the entries to different ports. This page shows only static entries.

Delete

To delete a MAC-based VLAN entry, check this box and press save. The entry will be deleted on the selected switch in the stack.

MAC Address

Indicates the MAC address.

VLAN ID

Indicates the VLAN ID.

Port Members

A row of check boxes for each port is displayed for each MAC-based VLAN entry. To include a port in a MAC-based VLAN, check the box. To remove or exclude the port from the MAC-based VLAN, make sure the box is unchecked. By default, no ports are members, and all boxes are unchecked.

Adding a New MAC-based VLAN

Click "**Adding New Entry**" to add a new MAC-based VLAN entry. An empty row is added to the table, and the MAC-based VLAN entry can be configured as needed. Any unicast MAC address can be configured for the MAC-based VLAN entry. No broadcast or multicast MAC addresses are allowed. Legal values for a VLAN ID are 1 through 4095.

The MAC-based VLAN entry is enabled on the selected stack switch unit when you click on "Save". A MAC-based VLAN without any port members on any stack unit will be deleted when you click "Save".

The "**Delete**" button can be used to undo the addition of new MAC-based VLANs. The maximum possible MAC-based VLAN entries are limited to 256.

Buttons

- **Save:** Click to save changes.

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

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

- **Refresh:** Click to refresh the page immediately.

- **|<<:** Updates the table starting from the first entry in the MAC-based VLAN Table.

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

3.1.15.2. VCL - Port-based VLAN

3.1.15.2.1. VCL - Port-based VLAN - Protocol to Group

Protocol to Group Mapping Table Auto-refresh ☐ Refresh

Delete	Frame Type	Value	Group Name
Delete	Ethernet ∨	Etype: 0x 0800	

Add New Entry

Save   Reset

This page allows you to add new protocols to Group Name (unique for each Group) mapping entries as well as allow you to see and delete already mapped entries for the selected stack switch unit.

Delete

To delete a Protocol to Group Name map entry, check this box. The entry will be deleted on the switch during the next Save.

Frame Type

Frame Type can have one of the following values:

1. Ethernet
2. LLC
3. SNAP

Note: On changing the Frame type field, valid value of the following text field will vary depending on the new frame type you selected.

Value

Valid value that can be entered in this text field depends on the option selected from the the preceding Frame Type selection menu.

Below is the criteria for three different Frame Types:

1. For Ethernet: Values in the text field when Ethernet is selected as a Frame Type is called etype. Valid values for etype ranges from 0x0600-0xffff
2. For LLC: Valid value in this case is comprised of two different sub-values.
   a. **DSAP:** 1-byte long string (0x00-0xff)
   b. **SSAP:** 1-byte long string (0x00-0xff)
3. For SNAP: Valid value in this case also is comprised of two different sub-values.
   a. **OUI:** OUI (Organizationally Unique Identifier) is value in format of xx-xx-xx where each pair (xx) in string is a hexadecimal value ranges from 0x00-0xff.
   b. **PID:** If the OUI is hexadecimal 000000, the protocol ID is the Ethernet type (EtherType) field

value for the protocol running on top of SNAP; if the OUI is an OUI for a particular organization, the protocol ID is a value assigned by that organization to the protocol running on top of SNAP.

In other words, if value of OUI field is 00-00-00 then value of PID will be etype (0x0600-0xffff) and if value of OUI is other than 00-00-00 then valid value of PID will be any value from 0x0000 to 0xffff.

Group Name

A valid Group Name is a unique 16-character long string for every entry which consists of a combination of alphabets (a-z or A-Z) and integers(0-9).

Note: special character and underscore(_) are not allowed.

Adding a New Group to VLAN mapping entry

Click "**Add New Entry**" to add a new entry in mapping table. An empty row is added to the table; Frame Type, Value and the Group Name can be configured as needed.

The "**Delete**" button can be used to undo the addition of new entry. The maximum possible Protocol to Group mappings are limited to 128.

Buttons

- **Save:** Click to save changes.
- **Reset:** Click to undo any changes made locally and revert to previously saved values.
- **Auto-refresh:** Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
- **Refresh:** Click to refresh the page immediately.

3.1.15.2.2. VCL - Port-based VLAN - Group to VLAN

This page allows you to map an already configured Group Name to a VLAN for the selected stack switch unit.

Delete

To delete a Group Name to VLAN map entry, check this box. The entry will be deleted on the switch during the next Save

Group Name

A valid Group Name is a string at the most 16 characters which consists of a combination of alphabets (a-z or A-Z) and integers(0-9), no special character is allowed. Whichever Group name you try map to a VLAN must be present in Protocol to Group mapping table and must not be pre-used by any other existing mapping entry on this page.

VLAN ID

Indicates the ID to which Group Name will be mapped. A valid VLAN ID ranges from 1-4095.

Port Members

A row of check boxes for each port is displayed for each Group Name to VLAN ID mapping. To include a port in a mapping, check the box. To remove or exclude the port from the mapping, make sure the box is unchecked. By default, no ports are members, and all boxes are unchecked.

Adding a New Group to VLAN mapping entry

Click "**Add New Entry**" to add a new entry in mapping table. An empty row is added to the table, the Group Name, VLAN ID and port members can be configured as needed. Legal values for a VLAN ID are 1 through 4095.

The "**Delete**" button can be used to undo the addition of new entry. The maximum possible Group to VLAN mappings are limited to 64.

Buttons

- **Save:** Click to save changes.
- **Reset:** Click to undo any changes made locally and revert to previously saved values.
- **Auto-refresh:** Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
- **Refresh:** Click to refresh the page immediately.

3.1.15.3. VCL - IP Subnet-based VLAN

IP Subnet-based VLAN Membership Configuration for Switch 1   Auto-refresh ☐   Refresh

Delete	VCE ID	IP Address	Mask Length	VLAN ID	Port Members 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26
Currently no entries present					

Add New Entry

Save   Reset

The IP subnet-based VLAN entries can be configured here. This page allows for adding, updating and deleting IP subnet-based VLAN entries and assigning the entries to different ports. This page shows only static entries.

Delete

To delete a IP subnet-based VLAN entry, check this box and press save. The entry will be deleted on the selected switch in the stack.

VCE ID

Indicates the index of the entry. It is user configurable. It's value ranges from 0-128. If a VCE ID is 0, application will auto-generate the VCE ID for that entry. Deletion and lookup of IP subnet-based VLAN are based on VCE ID.

IP Address

Indicates the IP address.

Mask Length

Indicates the network mask length.

VLAN ID

Indicates the VLAN ID. VLAN ID can be changed for the existing entries.

Port Members

A row of check boxes for each port is displayed for each IP subnet-based VLAN entry. To include a port in a IP subnet-based VLAN, check the box. To remove or exclude the port from the IP subnet-based VLAN, make sure the box is unchecked. By default, no ports are members, and all boxes are unchecked.

Adding a New IP subnet-based VLAN

Click "**Add New Entry**" to add a new IP subnet-based VLAN entry. An empty row is added to the table, and the IP subnet-based VLAN entry can be configured as needed. Any IP address/mask can be configured for the IP subnet-based VLAN entry. Legal values for a VLAN ID are 1 through 4095.

The IP subnet-based VLAN entry is enabled on the selected stack switch unit when you click on "Save". The "**Delete**" button can be used to undo the addition of new IP subnet-based VLANs. The maximum possible IP subnet-based VLAN entries are limited to 128.

Buttons

- **Save:** Click to save changes.

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

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

- **Refresh:** Refreshes the displayed table.

3.1.16. Configuration - Voice VLAN

3.1.16.1. Voice VLAN - Configuration

Voice VLAN Configuration

Stack Global Settings

Mode	Disabled
VLAN ID	1000
Aging Time	86400	seconds
Traffic Class	7 (High)

Port Configuration for Switch 1

Port	Mode	Security	Discovery Protocol
*	<>	<>	<>
1	Disabled	Disabled	OUI
2	Disabled	Disabled	OUI
3	Disabled	Disabled	OUI
24	Disabled	Disabled	OUI
25	Disabled	Disabled	OUI
26	Disabled	Disabled	OUI

Save   Reset

The Voice VLAN feature enables voice traffic forwarding on the Voice VLAN, then the switch can classify and schedule network traffic. It is recommended that there be two VLANs on a port - one for voice, one for data. Before connecting the IP device to the switch, the IP phone should configure the voice VLAN ID correctly. It should be configured through its own GUI.

Mode

Indicates the Voice VLAN mode operation. We must disable MSTP feature before we enable Voice VLAN. It can avoid the conflict of ingress filtering. Possible modes are:

- **Enabled:** Enable Voice VLAN mode operation.
- **Disabled:** Disable Voice VLAN mode operation.

VLAN ID

Indicates the Voice VLAN ID. It should be a unique VLAN ID in the system and cannot equal each port PVID. It is a conflict in configuration if the value equals management VID, MVR VID, PVID etc. The allowed range is 1 to 4095.

Aging Time

Indicates the Voice VLAN secure learning aging time. The allowed range is 10 to 10000000 seconds. It is used when security mode or auto detect mode is enabled. In other cases, it will be based on hardware aging time. The actual aging time will be situated between the [age_time; 2 * age_time] interval.

Traffic Class

Indicates the Voice VLAN traffic class. All traffic on the Voice VLAN will apply this class.

Port Mode

Indicates the Voice VLAN port mode.

Possible port modes are:

- **Disabled:** Disjoin from Voice VLAN.
- **Auto:** Enable auto detect mode. It detects whether there is VoIP phone attached to the specific port and configures the Voice VLAN members automatically.
- **Forced:** Force join to Voice VLAN.

Port Security

Indicates the Voice VLAN port security mode. When the function is enabled, all non-telephonic MAC addresses in the Voice VLAN will be blocked for 10 seconds. Possible port modes are:

- **Enabled:** Enable Voice VLAN security mode operation.
- **Disabled:** Disable Voice VLAN security mode operation.

Port Discovery Protocol

Indicates the Voice VLAN port discovery protocol. It will only work when auto detect mode is enabled. We should enable LLDP feature before configuring discovery protocol to "LLDP" or "Both". Changing the discovery protocol to "OUI" or "LLDP" will restart auto detect process. Possible discovery protocols are:

- **OUI:** Detect telephony device by OUI address.
- **LLDP:** Detect telephony device by LLDP.
- **Both:** Both OUI and LLDP.

Buttons

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

3.1.16.2. Voice VLAN - OUI

Voice VLAN OUI Table

Delete	Telephony OUI	Description
☐	00-01-e3	Siemens AG phones
☐	00-03-6b	Cisco phones
☐	00-0f-e2	H3C phones
☐	00-60-b9	Philips and NEC AG phones
☐	00-d0-1e	Pingtel phones
☐	00-e0-75	Polycom phones
☐	00-e0-bb	3Com phones

Add New Entry

Save   Reset

Configure VOICE VLAN OUI table on this page. The maximum number of entries is 16. Modifying the OUI table will restart auto detection of OUI process.

Delete

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

Telephony OUI

A telephony OUI address is a globally unique identifier assigned to a vendor by IEEE. It must be 6 characters long and the input format is "xx-xx-xx" (x is a hexadecimal digit).

Description

The description of OUI address. Normally, it describes which vendor telephony device it belongs to. The allowed string length is 0 to 32.

Buttons

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

3.1.17. Configuration - QoS

3.1.17.1. QoS - Port Classification

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

The settings relate to the currently selected stack unit, as reflected by the page header.

Port

The port number for which the configuration below applies.

QoS class

Controls the default QoS class.

All frames are classified to a QoS class. There is a one to one mapping between QoS class, queue and priority. A QoS class of 0 (zero) has the lowest priority.

If the port is VLAN aware and the frame is tagged, then the frame is classified to a QoS class that is based on the PCP value in the tag as shown below. Otherwise the frame is classified to the default QoS class.

PCP value: 0   1   2   3   4   5   6   7
QoS class: 1   0   2   3   4   5   6   7

The classified QoS class can be overruled by a QCL entry.

Note: If the default QoS class has been dynamically changed, then the actual default QoS class is shown in parentheses after the configured default QoS class.

DP level

Controls the default Drop Precedence Level.

All frames are classified to a DP level.

If the port is VLAN aware and the frame is tagged, then the frame is classified to a DP level that is equal to the DEI value in the tag. Otherwise the frame is classified to the default DP level.

The classified DP level can be overruled by a QCL entry.

DSCP Based

Click to Enable DSCP Based QoS Ingress Port Classification.

Buttons

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

3.1.17.2. QoS - Port Policing

QoS Ingress Port Policers for Switch 1

Port	Enabled	Rate	Unit	Flow Control
*	☐	500	<> ⌄	☐
1	☐	500	kbps ⌄	☐
2	☐	500	kbps ⌄	☐
3	☐	500	kbps ⌄	☐
4	☐	500	kbps ⌄	☐
5	☐	500	kbps ⌄	☐
24	☐	500	kbps ⌄	☐
25	☐	500	kbps ⌄	☐
26	☐	500	kbps ⌄	☐

Save   Reset

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

The settings relate to the currently selected stack unit, as reflected by the page header.

Port

The port number for which the configuration below applies.

Enabled

Controls whether the policer is enabled on this switch port.

Rate

Controls the rate for the policer. The default value is 500. This value is restricted to 100-1000000 when the "Unit" is "kbps" or "fps", and it is restricted to 1-13200 when the "Unit" is "Mbps" or "kfps".

Unit

Controls the unit of measure for the policer rate as kbps, Mbps, fps or kfps . The default value is "kbps".

Flow Control

If flow control is enabled and the port is in flow control mode, then pause frames are sent instead of discarding frames.

Buttons

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

3.1.17.3. QoS - Port Scheduler

QoS Egress Port Schedulers for Switch 1

Port	Mode	Weight					
		Q0	Q1	Q2	Q3	Q4	Q5
1	Strict Priority	-	-	-	-	-	-
2	Strict Priority	-	-	-	-	-	-
3	Strict Priority	-	-	-	-	-	-
4	Strict Priority	-	-	-	-	-	-
5	Strict Priority	-	-	-	-	-	-
6	Strict Priority	-	-	-	-	-	-
7	Strict Priority	-	-	-	-	-	-
8	Strict Priority	-	-	-	-	-	-
9	Strict Priority	-	-	-	-	-	-
10	Strict Priority	-	-	-	-	-	-
11	Strict Priority	-	-	-	-	-	-
12	Strict Priority	-	-	-	-	-	-
13	Strict Priority	-	-	-	-	-	-
14	Strict Priority	-	-	-	-	-	-
15	Strict Priority	-	-	-	-	-	-
16	Strict Priority	-	-	-	-	-	-
17	Strict Priority	-	-	-	-	-	-
18	Strict Priority	-	-	-	-	-	-
19	Strict Priority	-	-	-	-	-	-
20	Strict Priority	-	-	-	-	-	-
21	Strict Priority	-	-	-	-	-	-
22	Strict Priority	-	-	-	-	-	-
23	Strict Priority	-	-	-	-	-	-
24	Strict Priority	-	-	-	-	-	-
25	Strict Priority	-	-	-	-	-	-
26	Strict Priority	-	-	-	-	-	-

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

The ports belong to the currently selected stack unit, as reflected by the page header.

Port

The logical port for the settings contained in the same row.

Click on the port number in order to configure the schedulers.

Mode

Shows the scheduling mode for this port.

Qn

Shows the weight for this queue and port.

This page allows you to configure the Scheduler and Shapers for a specific port.

The settings relate to the currently selected stack unit, as reflected by the page header.

Scheduler Mode

Controls whether the scheduler mode is "Strict Priority" or "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. The default value is 500. This value is restricted to 100-1000000 when the "Unit" is "kbps", and it is restricted to 1-13200 when the "Unit" is "Mbps".

Queue Shaper Unit

Controls the unit of measure for the queue shaper rate as "kbps" or "Mbps". The default value is "kbps".

Queue Shaper Excess

Controls whether the queue is allowed to use excess bandwidth.

Queue Scheduler Weight

Controls the weight for this queue. The default value is "17". 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 "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. The default value is 500. This value is restricted to 100-1000000 when the "Unit" is "kbps", and it is restricted to 1-13200 when the "Unit" is "Mbps".

Port Shaper Unit

Controls the unit of measure for the port shaper rate as "kbps" or "Mbps". The default value is "kbps".

Buttons

- **Save:** Click to save changes.
- **Reset:** Click to undo any changes made locally and revert to previously saved values.
- **Cancel:** Click to undo any changes made locally and return to the previous page.

This page allows you to configure the Scheduler and Shapers for a specific port.

The settings relate to the currently selected stack unit, as reflected by the page header.

Scheduler Mode

Controls whether the scheduler mode is "Strict Priority" or "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. The default value is 500. This value is restricted to 100-1000000 when the "Unit" is "kbps", and it is restricted to 1-13200 when the "Unit" is "Mbps".

Queue Shaper Unit

Controls the unit of measure for the queue shaper rate as "kbps" or "Mbps". The default value is "kbps".

Queue Shaper Excess

Controls whether the queue is allowed to use excess bandwidth.

Queue Scheduler Weight

Controls the weight for this queue. The default value is "17". 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 "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. The default value is 500. This value is restricted to 100-1000000 when the "Unit" is "kbps", and it is restricted to 1-13200 when the "Unit" is "Mbps".

Port Shaper Unit

Controls the unit of measure for the port shaper rate as "kbps" or "Mbps". The default value is "kbps".

Buttons

- **Save:** Click to save changes.
- **Reset:** Click to undo any changes made locally and revert to previously saved values.
- **Cancel:** Click to undo any changes made locally and return to the previous page.

3.1.17.4. QoS - Port Shaping

QoS Egress Port Shapers for Switch 1

Port	Shapers								Port
	Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Port
1	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
2	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
3	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
4	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
5	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
6	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
7	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
8	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
9	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
10	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
11	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
12	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
13	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
14	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
15	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
16	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
17	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
18	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
19	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
20	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
21	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
22	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
23	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
24	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
25	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
26	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled

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

The ports belong to the currently selected stack unit, as reflected by the page header.

Port

The logical port for the settings contained in the same row.

Click on the port number in order to configure the shapers.

Qn

Shows "disabled" or actual queue shaper rate - e.g. "800 Mbps".

Port

Shows "disabled" or actual port shaper rate - e.g. "800 Mbps".

This page allows you to configure the Scheduler and Shapers for a specific port.

The settings relate to the currently selected stack unit, as reflected by the page header.

Scheduler Mode

Controls whether the scheduler mode is "Strict Priority" or "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. The default value is 500. This value is restricted to 100-1000000 when the "Unit" is "kbps", and it is restricted to 1-13200 when the "Unit" is "Mbps".

Queue Shaper Unit

Controls the unit of measure for the queue shaper rate as "kbps" or "Mbps". The default value is "kbps".

Queue Shaper Excess

Controls whether the queue is allowed to use excess bandwidth.

Queue Scheduler Weight

Controls the weight for this queue. The default value is "17". 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 "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. The default value is 500. This value is restricted to 100-1000000 when the "Unit" is "kbps", and it is restricted to 1-13200 when the "Unit" is "Mbps".

Port Shaper Unit

Controls the unit of measure for the port shaper rate as "kbps" or "Mbps". The default value is "kbps".

Buttons

- **Save:** Click to save changes.
- **Reset:** Click to undo any changes made locally and revert to previously saved values.
- **Cancel:** Click to undo any changes made locally and return to the previous page.

This page allows you to configure the Scheduler and Shapers for a specific port.

The settings relate to the currently selected stack unit, as reflected by the page header.

Scheduler Mode

Controls whether the scheduler mode is "Strict Priority" or "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. The default value is 500. This value is restricted to 100-1000000 when the "Unit" is "kbps", and it is restricted to 1-13200 when the "Unit" is "Mbps".

Queue Shaper Unit

Controls the unit of measure for the queue shaper rate as "kbps" or "Mbps". The default value is "kbps".

Queue Shaper Excess

Controls whether the queue is allowed to use excess bandwidth.

Queue Scheduler Weight

Controls the weight for this queue. The default value is "17". 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 "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. The default value is 500. This value is restricted to 100-1000000 when the "Unit" is "kbps", and it is restricted to 1-13200 when the "Unit" is "Mbps".

Port Shaper Unit

Controls the unit of measure for the port shaper rate as "kbps" or "Mbps". The default value is "kbps".

Buttons

- **Save:** Click to save changes.
- **Reset:** Click to undo any changes made locally and revert to previously saved values.
- **Cancel:** Click to undo any changes made locally and return to the previous page.

3.1.17.5. QoS - Port Tag Remarking

QoS Egress Port Tag Remarking for Switch 1

Port	Mode
1	Classified
2	Classified
3	Classified
4	Classified
5	Classified
6	Classified
7	Classified
8	Classified
9	Classified
10	Classified
11	Classified
12	Classified
13	Classified
14	Classified
15	Classified
16	Classified
17	Classified
18	Classified
19	Classified
20	Classified
21	Classified
22	Classified
23	Classified
24	Classified
25	Classified
26	Classified

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

The ports belong to the currently selected stack unit, as reflected by the page header.

Port

The logical port for the settings contained in the same row.

Click on the port number in order to configure tag remarking.

Mode

Shows the tag remarking mode for this port.

- **Classified:** Use classified PCP/DEI values.

- **Default:** Use default PCP/DEI values.

- **Mapped:** Use mapped versions of QoS class and DP level.

The QoS Egress Port Tag Remarking for a specific port are configured on this page.

Mode

Controls the tag remarking mode for this port.

- **Classified:** Use classified PCP/DEI values.
- **Default:** Use default PCP/DEI values.
- **Mapped:** Use mapped versions of QoS class and DP level.

PCP/DEI Configuration

Controls the default PCP and DEI values used when the mode is set to Default.

DP level Configuration

Controls the Drop Precedence level translation table when the mode is set to Mapped.

The purpose of this table is to reduce the 2 bit classified DP level to a 1 bit DP level used in the (QoS class, DP level) to (PCP, DEI) mapping process.

(QoS class, DP level) to (PCP, DEI) Mapping

Controls the mapping of the classified (QoS class, DP level) to (PCP, DEI) values when the mode is set to Mapped.

Buttons

- **Save:** Click to save changes.
- **Reset:** Click to undo any changes made locally and revert to previously saved values.
- **Cancel:** Click to undo any changes made locally and return to the previous page.

3.1.17.6. QoS - Port DSCP

QoS Port DSCP Configuration for Switch 1

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

The settings relate to the currently selected stack unit, as reflected by the page header.

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:

1. Translate
2. Classify

1. Translate

To Enable the Ingress Translation click the checkbox.

2. Classify

Classification for a port have 4 different values.

- **Disable:** No Ingress DSCP Classification.
- **DSCP=0:** Classify if incoming (or translated if enabled) DSCP is 0.
- **Selected:** Classify only selected DSCP for which classification is enabled as specified in DSCP Translation window for the specific DSCP.
- **All:** Classify all DSCP.

Egress

Port Egress Rewriting can be one of -

- **Disable:** No Egress rewrite.
- **Enable:** Rewrite enabled without remapping.
- **Remap:** DSCP from analyzer is remapped and frame is remarked with remapped DSCP value.

Buttons

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

3.1.17.7. QoS - DSCP-Based QoS

This page allows you to configure the basic QoS DSCP based QoS Ingress Classification settings for all switches.

DSCP

Maximum number of supported DSCP values are 64.

Trust

Controls whether a specific DSCP value is trusted. Only frames with trusted DSCP values are mapped to a specific QoS class and Drop Precedence Level. Frames with untrusted DSCP values are treated as a non-IP frame.

QoS Class

QoS class value can be any of (0-7)

DPL

Drop Precedence Level (0-3)

Buttons

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

3.1.17.8. QoS - DSCP Translation

DSCP Translation

DSCP	Ingress		Egress
	Translate	Classify	Remap
*	<>	☐	<>
0 (BE)	0 (BE)	☐	0 (BE)
1	1	☐	1
2	2	☐	2
3	3	☐	3
4	4	☐	4
62	62	☐	62
63	63	☐	63

Save Reset

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

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 QoS class and DPL map.

There are two configuration parameters for DSCP Translation -

1. Translate
2. Classify

1. Translate

DSCP at Ingress side can be translated to any of (0-63) DSCP values.

2. Classify

Click to enable Classification at Ingress side.

Egress

There is the following configurable parameter for Egress side -

- Remap

Remap

Select the DSCP value from select menu to which you want to remap. DSCP value ranges form 0 to 63.

Buttons

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

3.1.17.9. QoS - DSCP Classification

DSCP Classification

QoS Class	DSCP
*	<>
0	0 (BE)
1	0 (BE)
2	0 (BE)
3	0 (BE)
4	0 (BE)
5	0 (BE)
6	0 (BE)
7	0 (BE)

Save   Reset

This page allows you to configure the mapping of QoS class to DSCP value.

The settings relate to the currently selected stack unit, as reflected by the page header.

QoS Class

Actual QoS class.

DSCP

Select the classified DSCP value (0-63).

Buttons

- **Save:** Click to save changes.

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

3.1.17.10. QoS - Storm Control

QoS Port Storm Control for Switch 1

Port	Unicast Frames			Broadcast Frames			Unknown Frames		
	Enabled	Rate	Unit	Enabled	Rate	Unit	Enabled	Rate	Unit
*	☐	500	<>	☐	500	<>	☐	500	<>
1	☐	500	kbps	☐	500	kbps	☐	500	kbps
2	☐	500	kbps	☐	500	kbps	☐	500	kbps
3	☐	500	kbps	☐	500	kbps	☐	500	kbps
26	☐	500	kbps	☐	500	kbps	☐	500	kbps

Save   Reset

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

There is a storm rate control for unicast frames, broadcast frames and unknown (flooded) frames.

The settings relate to the currently selected stack unit, as reflected by the page header.

Port

The port number for which the configuration below applies.

Enabled

Controls whether the storm control is enabled on this switch port.

Rate

Controls the rate for the storm control. The default value is 500. This value is restricted to 100-1000000 when the "Unit" is "kbps" or "fps", and it is restricted to 1-13200 when the "Unit" is "Mbps" or "kfps".

Unit

Controls the unit of measure for the storm control rate as kbps, Mbps, fps or kfps . The default value is "kbps".

Buttons

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

3.1.17.11. QoS - WRED

Weighted Random Early Detection Configuration

Queue	Enable	Min. Threshold	Max. DP 1	Max. DP 2	Max. DP 3
0	☐	0	1	5	10
1	☐	0	1	5	10
2	☐	0	1	5	10
3	☐	0	1	5	10
4	☐	0	1	5	10
5	☐	0	1	5	10

Save   Reset

This page allows you to configure the Random Early Detection (RED) settings for queue 0 to 5.

RED cannot be applied to queue 6 and 7.

Through different RED configuration for the queues (QoS classes) it is possible to obtain Weighted Random Early Detection (WRED) operation between queues.

The settings are global for all ports in the stack.

Queue

The queue number (QoS class) for which the configuration below applies.

Enable

Controls whether RED is enabled for this queue.

Min. Threshold

Controls the lower RED threshold. If the average queue filling level is below this threshold, the drop probability is zero. This value is restricted to 0-100.

Max. DP 1

Controls the drop probability for frames marked with Drop Precedence Level 1 when the average queue filling level is 100%. This value is restricted to 0-100.

Max. DP 2

Controls the drop probability for frames marked with Drop Precedence Level 2 when the average queue filling level is 100%. This value is restricted to 0-100.

Max. DP 3

Controls the drop probability for frames marked with Drop Precedence Level 3 when the average queue filling level is 100%. This value is restricted to 0-100.

RED Drop Probability Function
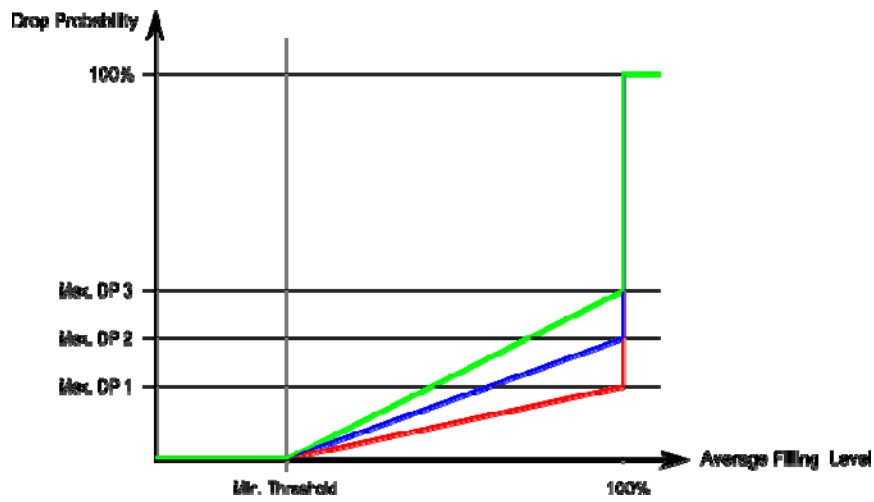
The following illustration shows the drop probability function with associated parameters.

RED Drop Probability Function

Max. DP 1-3 is the drop probability when the average queue filling level is 100%. Frames marked with Drop Precedence Level 0 are never dropped. Min. Threshold is the average queue filling level where the queues randomly start dropping frames. The drop probability for frames marked with Drop Precedence Level n increases linearly from zero (at Min. Threshold average queue filling level) to Max. DP n (at 100% average queue filling level).

Buttons

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

3.1.18. Configuration - Mirroring

Mirror Configuration

Port to mirror to	Disabled
Switch to mirror to	Switch 1

Mirror Port Configurationfor Switch 1

Port	Mode
*	<>
1	Disabled
2	Disabled
3	Disabled
24	Disabled
25	Disabled
26	Disabled

Save   Reset

Configure port Mirroring on this page.

To debug network problems, selected traffic can be copied, or mirrored, on a mirror port where a frame analyzer can be attached to analyze the frame flow.

The traffic to be copied on the mirror port is selected as follows:

- All frames received on a given port (also known as ingress or source mirroring).
- All frames transmitted on a given port (also known as egress or destination mirroring).

Port to mirror to

Port to mirror also known as the mirror port. Frames from ports that have either source (rx) or destination (tx) mirroring enabled are mirrored on this port. Disabled disables mirroring.

Switch to mirror to

Frames from ports that have either source (rx) or destination (tx) mirroring enabled are mirrored to this switch.

Mirror Port Configuration

The following table is used for Rx and Tx enabling.

Port

The logical port for the settings contained in the same row.

Mode

Select mirror mode.

- **Rx only:** Frames received on this port are mirrored on the mirror port. Frames transmitted are not mirrored.

- **Tx only:** Frames transmitted on this port are mirrored on the mirror port. Frames received are not mirrored.

- **Disabled:** Neither frames transmitted nor frames received are mirrored.

- **Enabled:** Frames received and frames transmitted are mirrored on the mirror port.

Note: For a given port, a frame is only transmitted once. It is therefore not possible to mirror mirror port Tx frames. Because of this, mode for the selected mirror port is limited to **Disabled** or **Rx only**.

Buttons

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

3.1.19. Configuration - UPnP

UPnP Configuration

Mode	Disabled
TTL	4
Advertising Duration	100

Save   Reset

Configure UPnP on this page.

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. Valid values are in the range 1 to 255.

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 30 seconds. Valid values are in the range 100 to 86400.

Buttons

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

3.1.20. Configuration - sFlow

sFlow Configuration   Refresh

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 for Switch 1

Port	Flow Sampler			Counter Poller	
	Enabled	Sampling Rate	Max. Header	Enabled	Interval
*	☐	0	128	☐	0
1	☐	0	128	☐	0
2	☐	0	128	☐	0
3	☐	0	128	☐	0
25	☐	0	128	☐	0
26	☐	0	128	☐	0

Save   Reset

This page allows for configuring sFlow. The configuration is divided into two parts: Configuration of the sFlow receiver (a.k.a. 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 or master change will disable sFlow sampling.

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 with a click on the Refresh-button. If locally managed, the timeout can be changed on the fly without affecting any other settings.

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/Nth of the packets transmitted/received on the port.

Not all sampling rates are achievable. If an unsupported sampling rate is requested, the switch will automatically adjust it to the closest achievable. This will be reported back in this field.

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 to 200 bytes with default being 128 bytes.

If the maximum datagram size does not take into account 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.

Buttons

- **Release:** See description under Owner.

- **Refresh:** Click to refresh the page. Note that unsaved changes will be lost.

- **Save:** Click to save changes. Note that sFlow configuration is not persisted to non-volatile memory.

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

3.2. Web Management - Monitor

You can monitor and view system status here. Also, all the settings you've made in the Configuration section of the management web page can be viewed here as well.

3.2.1. Monitor - System

3.2.1.1. System - Information

The switch system information is provided here.

Contact

The system contact configured in Configuration | System | Information | System Contact.

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.

System Date

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

System Uptime

The period of time the device has been operational.

Switch ID

The switch ID.

Chip ID

The Chip ID of this switch.

Software Version

The software version of this switch.

Software Date

The date when the switch software was produced.

Buttons

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

- **Refresh:** Click to refresh the page.

3.2.1.2. System - CPU Load
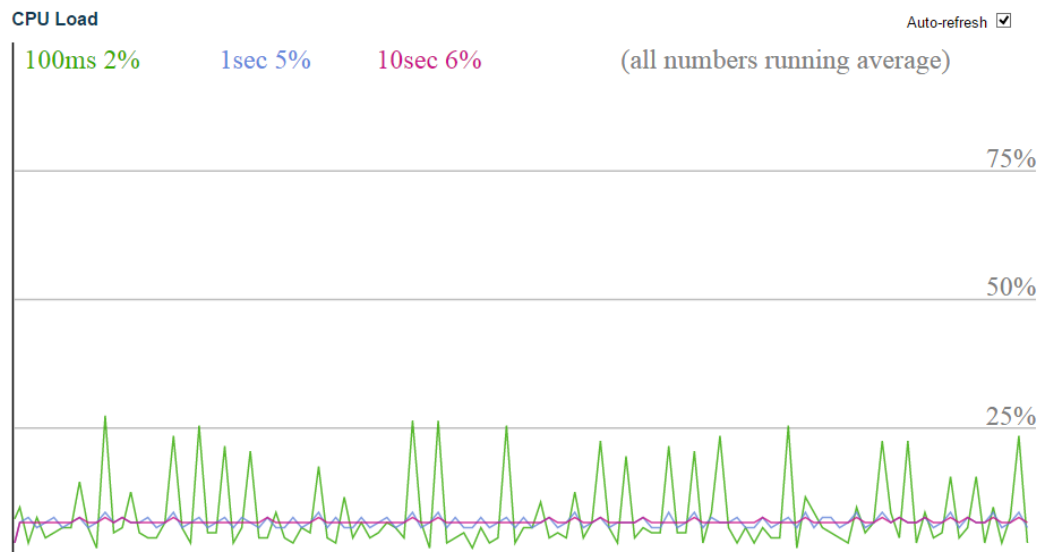
This page displays the CPU load, using an SVG graph.

The load is measured as averaged over the last 100ms, 1sec and 10 seconds intervals. The last 120 samples are graphed, and the last numbers are displayed as text as well.

In order to display the SVG graph, your browser must support the SVG format. Consult the SVG Wiki for more information on browser support. Specifically, at the time of writing, Microsoft Internet Explorer will need to have a plugin installed to support SVG.

Buttons

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

3.2.1.3. System - Log

The switch system log information is provided here.

ID

The ID (>= 1) of the system log entry.

Level

The level of the system log entry. The following level types are supported:

- **Info:** Information level of the system log.

- **Warning:** Warning level of the system log.

- **Error:** Error level of the system log.

- **All:** All levels.

Time

The time of the system log entry.

Message

The message of the system log entry.

Buttons

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

- **Refresh:** Updates the system log entries, starting from the current entry ID.

- **Clear:** Flushes the selected log entries.

- **|<<:** Updates the system log entries, starting from the first available entry ID.

- **<<**: Updates the system log entries, ending at the last entry currently displayed.

- **>>:** Updates the system log entries, starting from the last entry currently displayed.

- **>>|:** Updates the system log entries, ending at the last available entry ID.

3.2.1.4. System - Detailed Log

The switch system detailed log information is provided here.

ID

The ID (>= 1) of the system log entry.

Message

The detailed message of the system log entry.

Buttons

- **Refresh:** Updates the system log entry to the current entry ID.

- **|<<:** Updates the system log entry to the first available entry ID.

- **<<:** Updates the system log entry to the previous available entry ID.

- **>>:** Updates the system log entry to the next available entry ID.

- **>>|:** Updates the system log entry to the last available entry ID.

3.2.2. Monitor - Ports

3.2.2.1. Ports - State
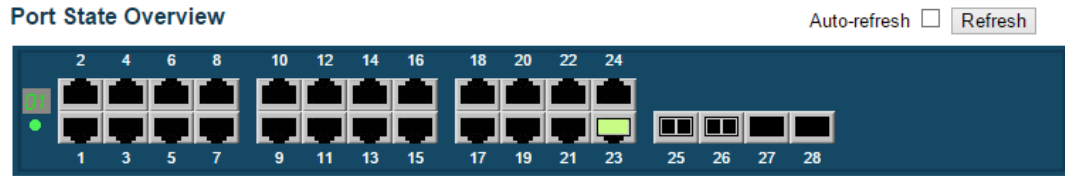
This page provides an overview of the current switch port states.

The port states are illustrated as follows:

Status	Disabled	Down	Link
RJ45 ports			
SFP ports			
X2 ports			

Buttons

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

3.2.2.2. Ports - Traffic Overview

Port Statistics Overview for Switch 1   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	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0	0
13	0	0	0	0	0	0	0	0	0
14	0	0	0	0	0	0	0	0	0
15	0	0	0	0	0	0	0	0	0
16	0	0	0	0	0	0	0	0	0
17	0	0	0	0	0	0	0	0	0
18	0	0	0	0	0	0	0	0	0
19	0	0	0	0	0	0	0	0	0
20	0	0	0	0	0	0	0	0	0
21	0	0	0	0	0	0	0	0	0
22	0	0	0	0	0	0	0	0	0
23	89368	2067	28900058	322487	0	0	53965	0	53965
24	0	0	0	0	0	0	0	0	0
25	0	0	0	0	0	0	0	0	0
26	0	0	0	0	0	0	0	0	0
27	0	1683	0	127908	0	0	0	0	0
28	238	1683	131532	127908	238	0	225	0	225

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

The ports belong to the currently selected stack unit, as reflected by the page header.

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.

Buttons

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

3.2.2.3. Ports - QoS Statistics

Queuing Counters for Switch 1   Auto-refresh ☐ | Refresh | Clear |

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	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
13	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
14	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
15	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
17	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
18	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
19	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
20	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
21	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
22	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
23	37261	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2139
24	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
25	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
26	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
27	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1758
28	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1758

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

The ports belong to the currently selected stack unit, as reflected by the page header.

Port

The logical port for the settings contained in the same row.

Qn

There are 8 QoS queues per port. Q0 is the lowest priority queue.

Rx/Tx

The number of received and transmitted packets per queue.

Buttons

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

3.2.2.4. Ports - Detailed Statistics

Detailed Port Statistics for Switch 1 Port 23 [Port 23 ▾] Auto-refresh ☐ [Refresh] [Clear]

Receive Total		Transmit Total	
Rx Packets	96661	Tx Packets	2233
Rx Octets	30693055	Tx Octets	355217
Rx Unicast	21445	Tx Unicast	2068
Rx Multicast	42544	Tx Multicast	159
Rx Broadcast	32672	Tx Broadcast	6
Rx Pause	0	Tx Pause	0
Receive Size Counters		**Transmit Size Counters**	
Rx 64 Bytes	33185	Tx 64 Bytes	403
Rx 65-127 Bytes	16942	Tx 65-127 Bytes	824
Rx 128-255 Bytes	6966	Tx 128-255 Bytes	322
Rx 256-511 Bytes	29784	Tx 256-511 Bytes	667
Rx 512-1023 Bytes	2899	Tx 512-1023 Bytes	5
Rx 1024-1526 Bytes	6885	Tx 1024-1526 Bytes	12
Rx 1527- Bytes	0	Tx 1527- Bytes	0
Receive Queue Counters		**Transmit Queue Counters**	
Rx Q0	38922	Tx Q0	0
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	2233
Receive Error Counters		**Transmit Error Counters**	
Rx Drops	57739	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	57739		

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 selected port belongs to the currently selected stack unit, as reflected by the page header.

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.

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.

> **Note 1:** Short frames are frames that are smaller than 64 bytes.

> **Note 2:** Long frames are frames that are longer than the configured maximum frame length for this port.

Transmit Error Counters

Tx Drops

The number of frames dropped due to output buffer congestion.

Tx Late/Exc. Coll.

The number of frames dropped due to excessive or late collisions.

Buttons

- **Refresh:** Click to refresh the page immediately.

- **Clear:** Clears the counters for the selected port.

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

   Note: The port select box determines which port is affected by clicking the buttons.

3.2.3. Monitor - Security

3.2.3.1. Security - Access Management Statistics

This page provides statistics for access management.

Interface

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

Received Packets

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

Allowed Packets

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

Discarded Packets

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

Buttons

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

3.2.3.2. Security - Network

3.2.3.2.1. Security - Network - Port Security - Switch

Port Security Switch Status Auto-refresh ☐ Refresh

User Module Legend

User Module Name	Abbr
Limit Control	L
802.1X	8
DHCP Snooping	D
Voice VLAN	V

Port Status for Switch 1

Port	Users	State	MAC Count Current	MAC Count Limit
1	- - - -	Disabled	-	-
2	- - - -	Disabled	-	-
3	- - - -	Disabled	-	-
4	- - - -	Disabled	-	-
5	- - - -	Disabled	-	-
6	- - - -	Disabled	-	-
7	- - - -	Disabled	-	-
8	- - - -	Disabled	-	-
9	- - - -	Disabled	-	-
10	- - - -	Disabled	-	-
11	- - - -	Disabled	-	-
12	- - - -	Disabled	-	-
13	- - - -	Disabled	-	-
14	- - - -	Disabled	-	-
15	- - - -	Disabled	-	-
16	- - - -	Disabled	-	-
17	- - - -	Disabled	-	-
18	- - - -	Disabled	-	-
19	- - - -	Disabled	-	-
20	- - - -	Disabled	-	-
21	- - - -	Disabled	-	-
22	- - - -	Disabled	-	-
23	- - - -	Disabled	-	-
24	- - - -	Disabled	-	-
25	- - - -	Disabled	-	-
26	- - - -	Disabled	-	-

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

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

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 selected switch in the stack and a number of columns.

Port

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

Users

Each of the user modules has a column that shows whether that module has enabled Port Security or not. 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.

State

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

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

MAC Count (Current, Limit)

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

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

Buttons

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

- **Refresh:** Click to refresh the page immediately.

3.2.3.2.2. Security - Network - Port Security - Port

Port Security Port Status for Switch 1 Port 1 | Port 1 ▾ | Auto-refresh ☐ | Refresh

MAC Address	VLAN ID	State	Time of Addition	Age/Hold
No MAC addresses attached				

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

MAC Address & VLAN ID

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

State

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

Time of Addition

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

Age/Hold

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

If aging is disabled or a user module has decided to hold the MAC address indefinitely, a dash (-) will be shown.

Buttons

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

3.2.3.2.3. Security - Network - NAS - Switch

Network Access Server Switch Status for Switch 1   Auto-refresh ☐ Refresh

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				
7	Force Authorized	Globally Disabled				
8	Force Authorized	Globally Disabled				
9	Force Authorized	Globally Disabled				
10	Force Authorized	Globally Disabled				
11	Force Authorized	Globally Disabled				
12	Force Authorized	Globally Disabled				
13	Force Authorized	Globally Disabled				
14	Force Authorized	Globally Disabled				
15	Force Authorized	Globally Disabled				
16	Force Authorized	Globally Disabled				
17	Force Authorized	Globally Disabled				
18	Force Authorized	Globally Disabled				
19	Force Authorized	Globally Disabled				
20	Force Authorized	Globally Disabled				
21	Force Authorized	Globally Disabled				
22	Force Authorized	Globally Disabled				
23	Force Authorized	Globally Disabled				
24	Force Authorized	Globally Disabled				
25	Force Authorized	Globally Disabled				
26	Force Authorized	Globally Disabled				

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

Port

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

Admin State

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

Port State

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

Last Source

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

Last ID

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

QoS Class

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

Port VLAN ID

The VLAN ID that NAS 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. Read more about RADIUS-assigned VLANs here.

If the port is moved to the Guest VLAN, "(Guest)" is appended to the VLAN ID. Read more about Guest VLANs here.

Buttons

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

3.2.3.2.4. Security - Network - NAS - Port

NAS Statistics for Switch 1 Port 1 Port 1 ▾ Auto-refresh ☐ Refresh

Port State

Admin State	Force Authorized
Port State	Globally Disabled

This page provides detailed NAS statistics for a specific switch port running EAPOL-based IEEE 802.1X authentication. For MAC-based ports, it shows selected backend server (RADIUS Authentication Server) statistics only.

Use the port select box to select which port details to be displayed. The selected port belongs to the currently selected stack unit as reflected by the table header.

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 Class

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. Read more about RADIUS-assigned VLANs here.

If the port is moved to the Guest VLAN, "(Guest)" is appended to the VLAN ID. Read more about Guest VLANs here.

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

		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**	dot1xAuthEapLengthErrorFramesRx	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

These backend (RADIUS) frame counters are available for the following administrative states:

- Port-based 802.1X

- Single 802.1X

- Multi 802.1X

- MAC-based Auth.

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.

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.
Version	dot1xAuthLastEapolFrameVersion	**802.1X-based**: 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

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. To populate the table, select one of the attached MAC Addresses from the table below.

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. As long as 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).

Buttons

- **Auto-refresh:** Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
- **Refresh:** Click to refresh the page immediately.
- **Clear:** This button is available in the following modes:
  - ➢ Force Authorized
  - ➢ Force Unauthorized
  - ➢ Port-based 802.1X
  - ➢ Single 802.1X
- **Clear:** Click to clear the counters for the selected port.
- **Clear All:** This button is available in the following modes:
  - ➢ Multi 802.1X
  - ➢ MAC-based Auth.X
- **Clear This:** Click to clear both the port counters and all of the attached client's counters. The "Last Client" will not be cleared, however. This button is available in the following modes:
  - ➢ Multi 802.1X
  - ➢ MAC-based Auth.X

3.2.3.2.5. Security - Network - ACL Status

ACL Status for Switch 1					Combined	Auto-refresh ☐	Refresh			
User	Ingress Port	Frame Type	Action	Rate Limiter	Port Redirect	CPU	CPU Once	Counter	Conflict
No entries									

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 512 on each switch.

User

Indicates the ACL user.

Ingress Port

Indicates the ingress port of the ACE. Possible values are:

- **All:** The ACE will match all ingress port.
- **Port:** The ACE will match a specific ingress port.

Frame Type

Indicates the frame type of the ACE. Possible values are:

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

Action

Indicates the forwarding action of the ACE.

- **Permit:** Frames matching the ACE may be forwarded and learned.
- **Deny:** Frames matching the ACE are dropped.

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.

CPU Once

Forward first packet that matched the specific ACE to CPU.

Counter

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

Conflict

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

Buttons

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

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

3.2.3.2.6. Security - Network - DHCP - Snooping Statistics

This page provides statistics for DHCP snooping. The statistics doesn't count the DHCP packets for system DHCP client or DHCP relay mode is enabled.

Receive and Transmit Packets

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 Lease 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.

Buttons

The port select box determines which port is affected by clicking the buttons.

- **Auto-refresh:** Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
- **Refresh:** Click to refresh the page.
- **Clear:** Clears the counters for the selected port.

3.2.3.2.7. Security - Network - DHCP - Relay Statistics

DHCP Relay Statistics   Auto-refresh ☐ Refresh | Clear

Server Statistics

Transmit to Server	Transmit Error	Receive from Server	Receive Missing Agent Option	Receive Missing Circuit ID	Receive Missing Remote ID	Receive Bad Circuit ID	Receive Bad Remote ID
0	0	0	0	0	0	0	0

Client Statistics

Transmit to Client	Transmit Error	Receive from Client	Receive Agent Option	Replace Agent Option	Keep Agent Option	Drop Agent Option
0	0	0	0	0	0	0

This page provides statistics for DHCP relay.

Server Statistics

Transmit to Server

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

Transmit Error

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

Receive from Server

The number of packets received from server.

Receive Missing Agent Option

The number of packets received without agent information options.

Receive Missing Circuit ID

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

Receive Missing Remote ID

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

Receive Bad Circuit ID

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

Receive Bad Remote ID

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

Client Statistics

Transmit to Client

The number of relayed packets from server to client.

Transmit Error

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

Receive from Client

The number of received packets from server.

Receive Agent Option

The number of received packets with relay agent information option.

Replace Agent Option

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

Keep Agent Option

The number of packets whose relay agent information was retained.

Drop Agent Option

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

Buttons

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

- **Refresh:** Click to refresh the page.

- **Clear:** Clear all statistics.

3.2.3.2.8. Security - Network - ARP Inspection

Entries in the Dynamic ARP Inspection Table are shown on this page. The Dynamic ARP Inspection Table contains up to 1024 entries, and is sorted first by port, then by VLAN ID, then by MAC address, and then by IP address.

Navigating the ARP Inspection Table

Each page shows up to 99 entries from the Dynamic ARP Inspection 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 Dynamic ARP Inspection Table.

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

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

ARP Inspection Table Columns

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.

Buttons

- **Auto-refresh:** Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
- **Refresh:** Refreshes the displayed table starting from the input fields.
- **Clear:** Flushes all dynamic entries.
- **|<<:** Updates the table starting from the first entry in the Dynamic ARP Inspection Table.
- **>>:** Updates the table, starting with the entry after the last entry currently displayed.

3.2.3.2.9. 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.

Navigating the IP Source Guard Table

Each page shows up to 99 entries from the Dynamic IP Source Guard 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 Dynamic IP Source Guard Table.

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

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

IP Source Guard Table Columns

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.

Buttons

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

- **Refresh:** Refreshes the displayed table starting from the input fields.

- **Clear:** Flushes all dynamic entries.

- **|<<:** Updates the table starting from the first entry in the Dynamic IP Source Guard Table.

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

3.2.3.3. Security - Network

3.2.3.3.1. Security - AAA - RADIUS Overview

RADIUS Authentication Server Status Overview Auto-refresh ☐ [Refresh]

#	IP Address	Status
1	0.0.0.0:1812	Disabled
2	0.0.0.0:1812	Disabled
3	0.0.0.0:1812	Disabled
4	0.0.0.0:1812	Disabled
5	0.0.0.0:1812	Disabled

RADIUS Accounting Server Status Overview

#	IP Address	Status
1	0.0.0.0:1813	Disabled
2	0.0.0.0:1813	Disabled
3	0.0.0.0:1813	Disabled
4	0.0.0.0:1813	Disabled
5	0.0.0.0:1813	Disabled

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

RADIUS Authentication Servers

#

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

IP Address

The IP address and UDP port number (in <IP Address>:<UDP Port> notation) of this server.

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.

RADIUS Accounting Servers

#

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

IP Address

The IP address and UDP port number (in <IP Address>:<UDP Port> notation) of this server.

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 accounting attempts.
- **Dead (X seconds left):** Accounting attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.

Buttons

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

3.2.3.3.2. Security - AAA - RADIUS Details

RADIUS Authentication Statistics for Server #1 | Server #1 ∨ | Auto-refresh ☐ | Refresh | Clear |

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			0.0.0.0:1812
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			0.0.0.0:1813
State			Disabled
Round-Trip Time			0 ms

This page provides detailed statistics for a particular RADIUS server.

RADIUS Authentication Statistics

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

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

Packet Counters

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

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.

Other Info

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

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: `Disabled` : The selected 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.
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 Statistics

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

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

Packet Counters

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

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	radiusAcctClientExtBadAuthenticators	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.

Other Info

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

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: `Disabled` : The selected 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 accounting attempts. `Dead (X seconds left)` : Accounting attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.
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.

Buttons

The server select box determines which server is affected by clicking the buttons.

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

- **Refresh:** Click to refresh the page immediately.

- **Clear:** Clears the counters for the selected server. The "Pending Requests" counter will not be cleared by this operation.

3.2.3.4. Security - Switch - RMON

3.2.3.4.1. Security - Switch - RMON - Statistics

RMON Statistics Status Overview for Switch 1

Auto-refresh ☐ | Refresh | |<< | >>

Start from Control Index 0 with 20 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																		

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

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

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

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.

Broad-cast

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

Multi-cast

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).

Under-size

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

Over-size

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

Frag.

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

Jabb.

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

Coll.

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

64

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

65~127

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

128~255

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

256~511

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

512~1023

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

1024~1588

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

Buttons

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

- **Refresh:** Click to refresh the page immediately.

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

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

3.2.3.4.2. Security - Switch - RMON - History

History Index	Sample Index	Sample Start	Drop	Octets	Pkts	Broad-cast	Multi-cast	CRC Errors	Under-size	Over-size	Frag.	Jabb.	Coll.	Utilization

RMON History Overview for Switch 1 — Auto-refresh ☐ Refresh |<< >>

Start from Control Index 0 and Sample Index 0 with 20 entries per page.

No more entries

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.

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

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

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.

Buttons

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

3.2.3.4.3. Security - Switch - RMON - Alarm

RMON Alarm Overview for Switch 1

Auto-refresh ☐ | Refresh | |<< | >>

Start from Control Index 0 with 20 entries per page.

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

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.

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

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

ID

Indicates the index of Alarm control entry.

Interval

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

Variable

Indicates the particular variable to be sampled

Sample Type

The method of sampling the selected variable and calculating the value to be compared against the thresholds.

Value

The value of the statistic during the last sampling period.

Startup Alarm

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

Rising Threshold

Rising threshold value.

Rising Index

Rising event index.

Falling Threshold

Falling threshold value.

Falling Index

Falling event index.

Buttons

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

- **Refresh:** Click to refresh the page immediately.

- **|<<:** Updates the table starting from the first entry in the Alarm Table, i.e. the entry with the lowest ID.

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

3.2.3.4.4. Security - Switch - RMON - Events

RMON Event Overview for Switch 1   Auto-refresh ☐ Refresh |<< >>

Start from Control Index 0   and Sample Index 0   with 20   entries per page.

Event Index	LogIndex	LogTime	LogDescription
No more entries			

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 table.

The "Start from Event Index and Log Index" allows the user to select the starting point in the Event table. Clicking the Refresh button will update the displayed table starting from that or the next closest Event table match.

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

Event Index

Indicates the index of the event entry.

Log Index

Indicates the index of the log entry.

LogTIme

Indicates Event log time

LogDescription

Indicates the Event description.

Buttons

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

3.2.4. Monitor - LACP

3.2.4.1. LACP - System Status

RMON Event Overview for Switch 1   Auto-refresh ☐ Refresh |<< >>

Start from Control Index 0   and Sample Index 0   with 20   entries per page.

Event Index	LogIndex	LogTime	LogDescription
No more entries			

This page provides a status overview for all LACP instances.

Aggr ID

The Aggregation ID associated with this aggregation instance. For LLAG the id is shown as 'isid:aggr-id' and for GLAGs as 'aggr-id'

Partner System ID

The system ID (MAC address) of the aggregation partner.

Partner Key

The Key that the partner has assigned to this aggregation ID.

Last changed

The time since this aggregation changed.

Local Ports

Shows which ports are a part of this aggregation for this switch/stack. The format is: "Switch ID:Port".

Buttons

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

3.2.4.2. LACP - Port Status

This page provides a status overview for LACP status for all ports.

Port

The switch port number.

LACP

'Yes' means that LACP is enabled and the port link is up. 'No' means that LACP is not enabled or that the port link is down. 'Backup' means that the port could not join the aggregation group but will join if other port leaves. Meanwhile it's LACP status is disabled.

Key

The key assigned to this port. Only ports with the same key can aggregate together.

Aggr ID

The Aggregation ID assigned to this aggregation group. IDs 1 and 2 are GLAGs while IDs 3-14 are LLAGs.

Partner System ID

The partner's System ID (MAC address).

Partner Port

The partner's port number connected to this port.

Partner Prio

The partner's port priority.

Buttons

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

3.2.4.3. LACP - Port Statistics

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

Port

The switch port number.

LACP Received

Shows how many LACP frames have been received at each port.

LACP Transmitted

Shows how many LACP frames have been sent from each port.

Discarded

Shows how many unknown or illegal LACP frames have been discarded at each port.

Buttons

- **Auto-refresh:** Automatic refresh occurs every 3 seconds.
- **Refresh:** Click to refresh the page immediately.
- **Clear:** Clears the counters for all ports.

3.2.5. Monitor - Loop Protection

Loop Protection Status for Switch 1   Auto-refresh ☐ Refresh

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

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

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.

Buttons

- **Refresh:** Click to refresh the page immediately.
- **Auto-refresh:** Check this box to enable an automatic refresh of the page at regular intervals.

3.2.6. Monitor - Spanning Tree

3.2.6.1. Spanning Tree - Bridge Status

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

The displayed table contains a row for each STP bridge instance, where the column displays the following information:

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.

Buttons

- **Refresh:** Click to refresh the page immediately.
- **Auto-refresh:** Check this box to enable an automatic refresh of the page at regular intervals.

3.2.6.2. Spanning Tree - Port Status

STP Statistics for Switch 1 Auto-refresh ☐ Refresh Clear

Port	Transmitted				Received				Discarded	
	MSTP	RSTP	STP	TCN	MSTP	RSTP	STP	TCN	Unknown	Illegal
1:23	5	0	0	0	1	1877	0	0	0	0

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

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.

Buttons

- **Refresh:** Click to refresh the page immediately.
- **Clear:** Click to reset the counters.
- **Auto-refresh:** Check this box to enable an automatic refresh of the page at regular intervals.

3.2.6.3. Spanning Tree - Port Statistics

STP Statistics for Switch 1	Auto-refresh ☐ Refresh Clear

Port	Transmitted				Received				Discarded	
	MSTP	RSTP	STP	TCN	MSTP	RSTP	STP	TCN	Unknown	Illegal
1:23	5	0	0	0	1	1994	0	0	0	0

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

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.

Buttons

- **Refresh:** Click to refresh the page immediately.
- **Clear:** Click to reset the counters.
- **Auto-refresh:** Check this box to enable an automatic refresh of the page at regular intervals.

3.2.7. Monitor - MVR

3.2.7.1. MVR - Statistics

MVR Statistics for Switch 1

Auto-refresh ☐ Refresh Clear

VLAN ID	IGMP/MLD Queries Received	IGMP/MLD Queries Transmitted	IGMPv1 Joins Received	IGMPv2/MLDv1 Reports Received	IGMPv3/MLDv2 Reports Received	IGMPv2/MLDv1 Leaves Received
1	0 / 0	0 / 0	0	0 / 0	0 / 0	0 / 0

This page provides MVR Statistics information.

The statistics is related to the currently selecting stack unit, as reflected by the page header.

VLAN ID

The Multicast VLAN ID.

IGMP/MLD Queries Received

The number of Received Queries for IGMP and MLD, respectively.

IGMP/MLD Queries Transmitted

The number of Transmitted Queries for IGMP and MLD, respectively.

IGMPv1 Joins Received

The number of Received IGMPv1 Join's.

IGMPv2/MLDv1 Report's Received

The number of Received IGMPv2 Join's and MLDv1 Report's, respectively.

IGMPv3/MLDv2 Report's Received

The number of Received IGMPv1 Join's and MLDv2 Report's, respectively.

IGMPv2/MLDv1 Leave's Received

The number of Received IGMPv2 Leave's and MLDv1 Done's, respectively.

Buttons

- **Auto-refresh:** Check this box to enable an automatic refresh of the page at regular intervals.
- **Refresh:** Click to refresh the page immediately.
- **Clear:** Clears all Statistics counters.

3.2.7.2. MVR - MVR Channel Groups

Entries in the MVR Channels (Groups) Information Table are shown on this page. The MVR Channels (Groups) Information Table is sorted first by VLAN ID, and then by group.

Navigating the MVR Channels (Groups) Information Table

Each page shows up to 99 entries from the MVR Group table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the MVR Channels (Groups) Information Table. The "Start from VLAN", and "Group Address" input fields allow the user to select the starting point in the MVR Channels (Groups) Information Table. Clicking the Refresh button will update the displayed table starting from that or the closest next MVR Channels (Groups) Information Table match. In addition, the two input fields will - upon a Refresh button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

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

MVR Channels (Groups) Information Table Columns

VLAN ID

VLAN ID of the group.

Groups

Group ID of the group displayed.

Port Members

Ports under this group.

Buttons

- **Auto-refresh:** Automatic refresh occurs every 3 seconds.
- **Refresh:** Refreshes the displayed table starting from the input fields.
- **|<<:** Updates the table starting from the first entry in the MVR Channels (Groups) Information Table.
- **>>:** Updates the table, starting with the entry after the last entry currently displayed.

3.2.7.3. MVR - MVR SFM Information

MVR SFM Information for Switch 1   Auto-refresh ☐   Refresh |<<   >>

Start from VLAN 1   and Group Address ::   with 20   entries per page.

VLAN ID	Group	Port	Mode	Source Address	Type	Hardware Filter/Switch
No more entries						

Entries in the MVR SFM Information Table are shown on this page. The MVR SFM (Source-Filtered Multicast) Information Table also contains the SSM (Source-Specific Multicast) information. This table is sorted first by VLAN ID, then by group, and then by Port. Different source addresses belong to the same group are treated as single entry.

Navigating the MVR SFM Information Table

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

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

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

MVR SFM Information Table Columns

VLAN ID

VLAN ID of the group.

Group

Group address of the group displayed.

Port

Switch port number.

Mode

Indicates the filtering mode maintained per (VLAN ID, port number, Group Address) basis. It can be either Include or Exclude.

Source Address

IP Address of the source. Currently, system limits the total number of IP source addresses for filtering to be 128. When there is no any source filtering address, the text "None" is shown in the Source Address field.

Type

Indicates the Type. It can be either Allow or Deny.

Hardware Filter/Switch

Indicates whether data plane destined to the specific group address from the source IPv4/IPv6 address could be handled by chip or not.

Buttons

- **Auto-refresh:** Automatic refresh occurs every 3 seconds.
- **Refresh:** Refreshes the displayed table starting from the input fields.
- **|<<:** Updates the table starting from the first entry in the MVR SFM Information Table.
- **>>:** Updates the table, starting with the entry after the last entry currently displayed

3.2.8. Monitor - IPMC

3.2.8.1. IPMC - IGMP Snooping

3.2.8.1.1. IPMC - IGMP Snooping - Status

IGMP Snooping Status for Switch 1   Auto-refresh ☐ Refresh Clear

Statistics

VLAN ID	Querier Version	Host Version	Querier Status	Queries Transmitted	Queries Received	V1 Reports Received	V2 Reports Received	V3 Reports Received	V2 Leaves Received

Router Port

Port	Status
1	-
2	-
3	-

This page provides IGMP Snooping status.

The status related to the currently selected stack unit, as reflected by the page header.

VLAN ID

The VLAN ID of the entry.

Querier Version

Working Querier Version currently.

Host Version

Working Host Version currently.

Querier Status

Shows the Querier status is "ACTIVE" or "IDLE".

"DISABLE" denotes the specific interface is administratively disabled.

Queries Transmitted

The number of Transmitted Queries.

Queries Received

The number of Received Queries.

V1 Reports Received

The number of Received V1 Reports.

V2 Reports Received

The number of Received V2 Reports.

V3 Reports Received

The number of Received V3 Reports.

V2 Leaves Received

The number of Received V2 Leaves.

Router Port

Display which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or IGMP querier.

Static denotes the specific port is configured to be a router port.

Dynamic denotes the specific port is learnt to be a router port.

Both denote the specific port is configured or learnt to be a router port.

Port

Switch port number.

Status

Indicate whether specific port is a router port or not.

Buttons

- **Auto-refresh:** Automatic refresh occurs every 3 seconds.
- **Refresh:** Click to refresh the page immediately.
- **Clear:** Clears all Statistics counters.

3.2.8.1.2. IPMC - IGMP Snooping - Groups Information

IGMP Snooping Group Information for Switch 1 Auto-refresh ☐ | Refresh | |<< | >>

Start from VLAN 1 and group address 224.0.0.0 with 20 entries per page.

VLAN ID	Groups	Port Members 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28
No more entries		

Entries in the IGMP Group Table are shown on this page. The IGMP Group Table is sorted first by VLAN ID, and then by group.

Navigating the IGMP Group Table

Each page shows up to 99 entries from the IGMP Group table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the IGMP Group Table. The "Start from VLAN", and "group" input fields allow the user to select the starting point in the IGMP Group Table. Clicking the Refresh button will update the displayed table starting from that or the closest next IGMP Group Table match. In addition, the two input fields will - upon a Refresh button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

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

IGMP Group Table Columns

VLAN ID

VLAN ID of the group.

Groups

Group address of the group displayed.

Port Members

Ports under this group.

Buttons

- **Auto-refresh:** Automatic refresh occurs every 3 seconds.
- **Refresh:** Refreshes the displayed table starting from the input fields.
- **|<<:** Updates the table, starting with the first entry in the IGMP Group Table.
- **>>:** Updates the table, starting with the entry after the last entry currently displayed.

3.2.8.1.3. IPMC - IGMP Snooping - IPv4 SFM Information

Entries in the IGMP SFM Information Table are shown on this page. The IGMP SFM (Source-Filtered Multicast) Information Table also contains the SSM (Source-Specific Multicast) information. This table is sorted first by VLAN ID, then by group, and then by Port. Different source addresses belong to the same group are treated as single entry.

Navigating the IGMP SFM Information Table

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

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

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

IGMP SFM Information Table Columns

VLAN ID

VLAN ID of the group.

Group

Group address of the group displayed.

Port

Switch port number.

Mode

Indicates the filtering mode maintained per (VLAN ID, port number, Group Address) basis. It can be either Include or Exclude.

Source Address

IP Address of the source. Currently, system limits the total number of IP source addresses for

filtering to be 128.

Type

Indicates the Type. It can be either Allow or Deny.

Hardware Filter/Switch

Indicates whether data plane destined to the specific group address from the source IPv4 address could be handled by chip or not.

Buttons

- **Auto-refresh:** Automatic refresh occurs every 3 seconds.
- **Refresh:** Refreshes the displayed table starting from the input fields.
- **|<<:** Updates the table starting from the first entry in the IGMP SFM Information Table
- **>>:** Updates the table, starting with the entry after the last entry currently displayed.

3.2.8.2. IPMC - MLD Snooping

3.2.8.2.1. IPMC - MLD Snooping - Status

MLD Snooping Status for Switch 1

Auto-refresh ☐ Refresh Clear

Statistics

VLAN ID	Querier Version	Host Version	Querier Status	Queries Transmitted	Queries Received	V1 Reports Received	V2 Reports Received	V1 Leaves Received

Router Port

Port	Status
1	-
2	-

This page provides MLD Snooping status.

The status related to the currently selected stack unit, as reflected by the page header.

VLAN ID

The VLAN ID of the entry.

Querier Version

Working Querier Version currently.

Host Version

Working Host Version currently.

Querier Status

Shows the Querier status is "ACTIVE" or "IDLE".

"DISABLE" denotes the specific interface is administratively disabled.

Queries Transmitted

The number of Transmitted Queries.

Queries Received

The number of Received Queries.

V1 Reports Received

The number of Received V1 Reports.

V2 Reports Received

The number of Received V2 Reports.

V1 Leaves Received

The number of Received V1 Leaves.

Router Port

Display which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or IGMP querier.

Static denotes the specific port is configured to be a router port.

Dynamic denotes the specific port is learnt to be a router port.

Both denote the specific port is configured or learnt to be a router port.

Port

Switch port number.

Status

Indicate whether specific port is a router port or not.

Buttons

- **Auto-refresh:** Automatic refresh occurs every 3 seconds.
- **Refresh:** Click to refresh the page immediately.
- **Clear:** Clears all Statistics counters.

3.2.8.2.2. IPMC - MLD Snooping - Groups Information

MLD Snooping Group Information for Switch 1   Auto-refresh ☐ | Refresh | |<< | >>

Start from VLAN 1   and group address ff00::   with 20   entries per page.

VLAN ID	Groups	Port Members
		1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28
No more entries		

Entries in the MLD Group Table are shown on this page. The MLD Group Table is sorted first by VLAN ID, and then by group.

Navigating the MLD Group Table

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

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

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

MLD Group Table Columns

VLAN ID

VLAN ID of the group.

Groups

Group address of the group displayed.

Port Members

Ports under this group.

Buttons

- **Auto-refresh:** Automatic refresh occurs every 3 seconds.
- **Refresh:** Refreshes the displayed table starting from the input fields.
- **|<<:** Updates the table, starting with the first entry in the MLD Group Table.
- **>>:** Updates the table, starting with the entry after the last entry currently displayed.

3.2.8.2.3. IPMC - MLD Snooping - IPv6 Group Information

Entries in the MLD SFM Information Table are shown on this page. The MLD SFM (Source-Filtered Multicast) Information Table also contains the SSM (Source-Specific Multicast) information. This table is sorted first by VLAN ID, then by group, and then by Port. Different source addresses belong to the same group are treated as single entry.

Navigating the MLD SFM Information Table

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

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

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

MLD SFM Information Table Columns

VLAN ID
VLAN ID of the group.

Group
Group address of the group displayed.

Port
Switch port number.

Mode
Indicates the filtering mode maintained per (VLAN ID, port number, Group Address) basis. It can be either Include or Exclude.

Source Address

IP Address of the source. Currently, system limits the total number of IP source addresses for filtering to be 128.

Type

Indicates the Type. It can be either Allow or Deny.

Hardware Filter/Switch

Indicates whether data plane destined to the specific group address from the source IPv6 address could be handled by chip or not.

Buttons

- **Auto-refresh:** Automatic refresh occurs every 3 seconds.
- **Refresh:** Refreshes the displayed table starting from the input fields.
- **|<<:** Updates the table starting from the first entry in the MLD SFM Information Table.
- **>>:** Updates the table, starting with the entry after the last entry currently displayed.

3.2.9. Monitor - LLDP

3.2.9.1. LLDP - Neighbours

LLDP Remote Device Summary						Auto-refresh ☐ Refresh
Local Port	**Chassis ID**	**Port ID**	**Port Description**	**System Name**	**System Capabilities**	**Management Address**
Port 23	00-01-C1-00-00-00	4	Port #4		Bridge(+)	192.168.2.253 (IPv4)
Port 23	00-03-CE-46-7C-0B	4	Port #4		Bridge(+)	192.168.20.254 (IPv4)
Port 23	D4-6A-91-36-10-34	7	Port #7		Bridge(+)	192.168.2.230 (IPv4)
Port 23	00-03-CE-24-51-88	8	Port #8		Bridge(+)	192.168.2.4 (IPv4)

This page provides a status overview for all LLDP neighbours. The displayed table contains a row for each port on which an LLDP neighbour is detected. The columns hold the following information:

Local Port

The port on which the LLDP frame was received.

Chassis ID

The Chassis ID is the identification of the neighbour's LLDP frames.

Port ID

The Port ID is the identification of the neighbour port.

Port Description

Port Description is the port description advertised by the neighbour unit.

System Name

System Name is the name advertised by the neighbour unit.

System Capabilities

System Capabilities describes the neighbour unit's capabilities. The possible capabilities are:

1. Other

2. Repeater

3. Bridge

4. WLAN Access Point

5. Router

6. Telephone

7. DOCSIS cable device

8. Station only

9. Reserved

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 neighbour unit's address that is used for higher layer entities to assist

discovery by the network management. This could for instance hold the neighbour's IP address.

Buttons

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

  3 seconds.

- **Refresh:** Click to refresh the page.

3.2.9.2. LLDP - LLDP-MED Neighbours

LLDP-MED Neighbour Information for Switch 1 Auto-refresh ☐ Refresh

Local Port
No LLDP-MED neighbour information found

This page provides a status overview of all LLDP-MED neighbours. The displayed table contains a row for each port on which an LLDP neighbour is detected. This function applies to VoIP devices which support LLDP-MED. The columns hold the following information:

Port

The port 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:

1. LAN Switch/Router
2. IEEE 802.1 Bridge
3. IEEE 802.3 Repeater (included for historical reasons)
4. IEEE 802.11 Wireless Access Point
5. 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 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 of 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 of 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 neighbour unit's LLDP-MED capabilities. The possible capabilities are:

1. LLDP-MED capabilities
2. Network Policy
3. Location Identification
4. Extended Power via MDI - PSE

5. Extended Power via MDI - PD

6. Inventory

7. 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 possible application types are shown below.

1. 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.

2. Voice Signaling - for use in network topologies that require a different policy for the voice Signaling than for the voice media.

3. 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.

4. Guest Voice Signaling - for use in network topologies that require a different policy for the guest voice Signaling than for the guest voice media.

5. Softphone Voice - for use by softphone applications on typical data centric devices, such as PCs or laptops.

6. Video Conferencing - for use by dedicated Video Conferencing equipment and other similar appliances supporting real-time interactive video/audio services.

7. 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.

8. 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

- **Unknown:** The network policy for the specified application type is currently unknown.
- **Defined:** The network policy is defined.

TAG

TAG is indicative of whether the specified application type is using a tagged or an untagged VLAN. 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 port 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 port 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, the 802.3 PMD operating mode will be determined the operational MAU type field value rather than by auto-negotiation.

Auto-negotiation Capabilities

Auto-negotiation Capabilities shows the link partners MAC/PHY capabilities.

Buttons

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

3.2.9.3. LLDP - PoE

LLDP Neighbour Power Over Ethernet Information for Switch 1 Auto-refresh ☐ Refresh

Local Port	Power Type	Power Source	Power Priority	Maximum Power
23	PSE Device	Primary Power Supply	Low	0 [W]
23	PSE Device	Primary Power Supply	Low	0 [W]
23	PSE Device	Primary Power Supply	Low	0 [W]
23	PSE Device	Primary Power Supply	Low	0 [W]

This page provides a status overview for all LLDP PoE neighbours. The displayed table contains a row for each port on which an LLDP PoE neighbour is detected. The columns hold the following information:

Local Port

The port 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 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 port that is sourcing the power. There are three levels of power priority. The three levels are: Critical, High and Low.

If the power priority is unknown it is indicated as "Unknown"

Maximum Power

The Maximum Power Value contains a numerical value that indicates the maximum power in watts required by a PD device from a PSE device, or the minimum power a PSE device is capable of sourcing over a maximum length cable based on its current configuration.

The maximum allowed value is 102.3 W. If the device indicates value higher than 102.3 W, it is represented as "reserved"

Buttons

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

3.2.9.4. LLDP - EEE

LLDP Neighbors EEE Information for Switch 1   Auto-refresh ☐ Refresh

Local Port	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					

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, 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 ", as a way to agree upon the minimum wakeup time they need.

This page provides an overview of EEE information exchanged by LLDP.

LLDP Neighbors EEE Information

The displayed table contains a row for each port. The columns hold the following information:

Local Port

The port on 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.

Rx Tw

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 Receive Tw

The link partner's fallback receive Tw.

A receiving link partner may inform the transmitter of an alternate desired Tw_sys_tx. Since a receiving link partner is likely to 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 whether or not 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 via 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 via 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.

Buttons

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

3.2.9.5. LLDP - Port Statistics

LLDP Global Counters for Switch 1

Auto-refresh ☐ Refresh   Clear

Global Counters	
Neighbour entries were last changed	2015-03-19T13:14:29+08:00 (10105 secs. ago)
Total Neighbours Entries Added	4
Total Neighbours Entries Deleted	0
Total Neighbours Entries Dropped	0
Total Neighbours Entries Aged Out	0

LLDP Statistics Local Counters for Switch 1

Local Port	Tx Frames	Rx Frames	Rx Errors	Frames Discarded	TLVs Discarded	TLVs Unrecognized	Org. Discarded	Age-Outs
1	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0

This page provides an overview of all LLDP traffic.

Two types of counters are shown. Global counters are counters that refer to the whole stack, while local counters refer to per port counters for the currently selected switch.

Global Counters

Neighbour 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 Neighbours Entries Added

Shows the number of new entries added since switch reboot.

Total Neighbours Entries Deleted

Shows the number of new entries deleted since switch reboot.

Total Neighbours Entries Dropped

Shows the number of LLDP frames dropped due to the entry table being full.

Total Neighbours Entries Aged Out

Shows the number of entries deleted due to Time-To-Live expiring.

Local Counters

The displayed table contains a row for each port. The columns hold the following information:

Local Port

The port on which LLDP frames are received or transmitted.

Tx Frames

The number of LLDP frames transmitted on the port.

Rx Frames

The number of LLDP frames received on the port.

Rx Errors

The number of received LLDP frames containing some kind of error.

Frames Discarded

If an LLDP frame is received on a port, and the switch's internal table has run full, the LLDP frame is counted and discarded. This situation is known as "Too Many Neighbours" 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 port's link is down, an LLDP shutdown frame is received, or when the entry ages out.

TLVs Discarded

Each LLDP frame can contain multiple pieces of information, known as TLVs (TLV is short for "Type Length Value"). If a TLV is malformed, it is counted and discarded.

TLVs Unrecognized

The number of well-formed TLVs, but with an unknown type value.

Org. Discarded

The number of organizationally received TLVs.

Age-Outs

Each LLDP frame contains information about how long time the LLDP information is valid (age-out time). If no new LLDP frame is received within the age out time, the LLDP information is removed, and the Age-Out counter is incremented.

Buttons

- **Auto-refresh:** Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
- **Refresh:** Click to refresh the page.
- **Clear:** Clears the local counters. All counters (including global counters) are cleared upon reboot.

3.2.10. Monitor - PoE

Power Over Ethernet Status for Switch 1   Auto-refresh ☐ Refresh

Local Port	PD class	Power Requested	Power Allocated	Power Used	Current Used	Priority	Port Status
1	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
2	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
3	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
4	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
5	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
6	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
7	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
8	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
9	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
10	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
11	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
12	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
13	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
14	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
15	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
16	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
17	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
18	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
19	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
20	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
21	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
22	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
23	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
24	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
Total		0 [W]	0 [W]	0 [W]	0 [mA]		

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

Local Port

This is the logical port number for this row.

PD Class

Each PD is classified according to a class that defines the maximum power the PD will use. The PD

Class shows the PDs class.

Five Classes are defined:

- Class 0: Max. power 15.4 W
- Class 1: Max. power 4.0 W
- Class 2: Max. power 7.0 W
- Class 3: Max. power 15.4 W
- Class 4: Max. power 30.0 W

Power Requested

The Power Requested shows the requested amount of power the PD wants to be reserved.

Power Allocated

The Power Allocated shows the amount of power the switch has allocated for the PD.

Power Used

The Power Used shows how much power the PD currently is using.

Current Used

The Power Used shows how much current the PD currently is using.

Priority

The Priority shows the port's priority configured by the user.

Port Status

The Port Status shows the port's status. The status can be one of the following values:

- PoE not available - No PoE chip found - PoE not supported for the port.
- PoE turned OFF - PoE disabled : PoE is disabled by user.
- PoE turned OFF - Power budget exceeded - The total requested or used power by the PDs exceeds the maximum power the Power Supply can deliver, and port(s) with the lowest priority is/are powered down.
- No PD detected - No PD detected for the port.
- PoE turned OFF - PD overload - The PD has requested or used more power than the port can deliver, and is powered down.
- PoE turned OFF - PD is off.
- Invalid PD - PD detected, but is not working correctly.

Buttons

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

3.2.11. 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.

Navigating the MAC Table

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

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

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

MAC Table Columns

Switch (stack only)

The stack unit where the entry is learned.

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.

Buttons

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

3.2.12. Monitor - VLANs

3.2.12.1. VLANs - VLAN Membership

VLAN Membership Status for Combined users for Switch 1 [∨] Auto-refresh ☐ [Refresh]

Start from VLAN [NaN] with [NaN] entries per page. [|<<] [>>]

	Port Members
VLAN ID	1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26

This page provides an overview of membership status of VLAN 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 will show a combination of the administrator and internal software modules configuration, and basically reflects what is actually 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, the following image will be displayed: ✔
- If a port is in the forbidden port list, the following image will be displayed: ✕
- If a port is in the forbidden port list and at the same time attempted included in the VLAN, the following image will be displayed ✕. The port will not be a member of the VLAN in this case.

Navigating the VLAN Membership Status page

Each page shows up to 99 entries from the VLAN table (default being 20), selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the VLAN Table. The first displayed will be the one with the lowest VLAN ID found in the VLAN Table.

The "VLAN" input field allows the user to select the starting point in the VLAN Table. Clicking the "Refresh" button will update the displayed table starting from that or the closest next VLAN Table match.

The ">>" button will use the last entry of the currently displayed VLAN entry as a basis for the next lookup. When the end is reached, the text "No data exists for the selected user" is shown in the table. Use the "|<<" button to start over.

Buttons

- Combined ⌄ : Select VLAN Users from this drop down list.

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

- **Refresh:** Click to refresh the page immediately.

3.2.12.2. VLANs - VLAN Ports

VLAN Port Status for Static user for Switch 1 [Static ▾] Auto-refresh ☐ [Refresh]

Port	PVID	Port Type	Ingress Filtering	Frame Type	Tx Tag	UVID	Conflicts
1	1	UnAware	Disabled	All	Untag_this	1	No
2	1	UnAware	Disabled	All	Untag_this	1	No
3	1	UnAware	Disabled	All	Untag_this	1	No
4	1	UnAware	Disabled	All	Untag_this	1	No
5	1	UnAware	Disabled	All	Untag_this	1	No
6	1	UnAware	Disabled	All	Untag_this	1	No
7	1	UnAware	Disabled	All	Untag_this	1	No
8	1	UnAware	Disabled	All	Untag_this	1	No
9	1	UnAware	Disabled	All	Untag_this	1	No
10	1	UnAware	Disabled	All	Untag_this	1	No
11	1	UnAware	Disabled	All	Untag_this	1	No
12	1	UnAware	Disabled	All	Untag_this	1	No
13	1	UnAware	Disabled	All	Untag_this	1	No
14	1	UnAware	Disabled	All	Untag_this	1	No
15	1	UnAware	Disabled	All	Untag_this	1	No
16	1	UnAware	Disabled	All	Untag_this	1	No
17	1	UnAware	Disabled	All	Untag_this	1	No
18	1	UnAware	Disabled	All	Untag_this	1	No
19	1	UnAware	Disabled	All	Untag_this	1	No
20	1	UnAware	Disabled	All	Untag_this	1	No
21	1	UnAware	Disabled	All	Untag_this	1	No
22	1	UnAware	Disabled	All	Untag_this	1	No
23	1	UnAware	Disabled	All	Untag_this	1	No
24	1	UnAware	Disabled	All	Untag_this	1	No
25	1	UnAware	Disabled	All	Untag_this	1	No
26	1	UnAware	Disabled	All	Untag_this	1	No

This page provides VLAN Port Status.

The ports belong to the currently selected stack unit, as reflected by the page header.

VLAN USER

VLAN User module uses services of the VLAN management functionality to configure VLAN memberships and VLAN port configuration such as PVID, UVID. Currently we support following VLAN User types:

- CLI/Web/SNMP: These are referred to as static.
- NAS: NAS provides port-based authentication, which involves communications between a Supplicant, Authenticator, and an Authentication Server.
- Voice VLAN: Voice VLAN is a VLAN configured specially for voice traffic typically originating from IP phones.
- MVR: MVR is used to eliminate the need to duplicate multicast traffic for subscribers in each VLAN. Multicast traffic for all channels is sent only on a single (multicast) VLAN.
- MSTP: The 802.1s Multiple Spanning Tree protocol (MSTP) uses VLANs to create multiple spanning trees in a network, which significantly improves network resource utilization while maintaining a loop-free environment.

Port

The logical port for the settings contained in the same row.

PVID

Shows the VLAN identifier for that port. The allowed values are 1 through 4095. The default value is 1.

Port Type

Shows the Port Type. Port type can be any of Unaware, C-port, S-port, Custom S-port.

If Port Type is Unaware, all frames are classified to the Port VLAN ID and tags are not removed.

C-port is Customer Port. S-port is Service port. Custom S-port is S-port with Custom TPID.

Ingress Filtering

Shows the ingress filtering on a port. This parameter affects VLAN ingress processing. If ingress filtering is enabled and the ingress port is not a member of the classified VLAN, the frame is discarded.

Frame Type

Shows whether the port accepts all frames or only tagged frames. This parameter affects VLAN ingress processing. If the port only accepts tagged frames, untagged frames received on that port are discarded.

Tx Tag

Shows egress filtering frame status whether tagged or untagged.

UVID

Shows UVID (untagged VLAN ID). Port's UVID determines the packet's behaviour at the egress side.

Conflicts

Shows status of Conflicts whether exists or not. When a Volatile VLAN User requests to set VLAN membership or VLAN port configuration, the following conflicts can occur:

- Functional Conflicts between features.
- Conflicts due to hardware limitation.
- Direct conflict between user modules.

Buttons

- Static ⌄ : Select VLAN Users from this drop down list.

- **Auto-refresh:** Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
- **Refresh:** Click to refresh the page immediately.
- **>>:** Updates the table, starting with the entry after the last entry currently displayed.

3.2.13. Monitor - VCL

3.2.13.1. VCL - MAC-based VLAN

This page shows MAC-based VLAN entries configured by various MAC-based VLAN users. Currently we support following VLAN User types:

- CLI/Web/SNMP: These are referred to as static.
- NAS: NAS provides port-based authentication, which involves communications between a Supplicant, Authenticator, and an Authentication Server.

MAC Address

Indicates the MAC address.

VLAN ID

Indicates the VLAN ID.

Port Members

Port members of the MAC-based VLAN entry.

Buttons

- **Refresh:** Refreshes the displayed table.
- **Auto-refresh:** Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds (only present if stacking is enabled).

3.2.14. Monitor - sFlow

This page shows receiver and per-port sFlow statistics.

Receiver Statistics

Owner

This field shows the current owner of the sFlow configuration. It assumes one of three 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.

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.

Rx and Tx Flow Samples

The number of flow samples sent to the sFlow receiver originating from this port. Here, flow samples are divided into Rx and Tx flow samples, where Rx flow samples contains the number of packets that were sampled upon reception (ingress) on the port and Tx flow samples contains the number of packets that were sampled upon transmission (egress) on the port.

Counter Samples

The total number of counter samples sent to the sFlow receiver originating from this port.

Buttons

- **Auto-refresh:** Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds (only present if stacking is enabled).
- **Refresh:** Click to refresh the page.
- **Clear Receiver:** Clears the sFlow receiver counters.
- **Clear Port:** Clears the per-port counters.

3.3. Web Management - Diagnostics

This section of the management web page provides you tools for diagnosing your network.

3.3.1. Diagnostics - Ping

ICMP Ping

IP Address	0.0.0.0
Ping Length	56
Ping Count	5
Ping Interval	1

Start

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

After you press the "Start" button, ICMP packets are transmitted, and the sequence number and round trip time are displayed upon reception of a reply. The amount of data received inside of an IP packet of type ICMP ECHO_REPLY will always be 8 bytes more than the requested data space(the ICMP header). The page refreshes automatically until responses to all packets are received, or until a timeout occurs.

PING server 10.10.132.20, 56 bytes of data.

64 bytes from 10.10.132.20: icmp_seq=0, time=0ms

64 bytes from 10.10.132.20: icmp_seq=1, time=0ms

64 bytes from 10.10.132.20: icmp_seq=2, time=0ms

64 bytes from 10.10.132.20: icmp_seq=3, time=0ms

64 bytes from 10.10.132.20: icmp_seq=4, time=0ms

Sent 5 packets, received 5 OK, 0 bad

You can configure the following properties of the issued ICMP packets:

IP Address
The destination IP Address.

Ping Length
The payload size of the ICMP packet. Values range from 2 bytes to 1452 bytes.

Ping Count
The count of the ICMP packet. Values range from 1 time to 60 times.

Ping Interval
The interval of the ICMP packet. Values range from 0 second to 30 seconds.

Buttons

- **Start:** Click to start transmitting ICMP packets.
- **New Ping:** Click to re-start diagnostics with PING.

3.3.2. Diagnostics - Ping6

ICMPv6 Ping

IP Address	0:0:0:0:0:0:0:0
Ping Length	56
Ping Count	5
Ping Interval	1

Start

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

After you press the "Start" button, ICMPv6 packets are transmitted, and the sequence number and round trip time are displayed upon reception of a reply. The page refreshes automatically until responses to all packets are received, or until a timeout occurs.

PING6 server ::10.10.132.20, 56 bytes of data.

64 bytes from ::10.10.132.20: icmp_seq=0, time=0ms

64 bytes from ::10.10.132.20: icmp_seq=1, time=0ms

64 bytes from ::10.10.132.20: icmp_seq=2, time=0ms

64 bytes from ::10.10.132.20: icmp_seq=3, time=0ms

64 bytes from ::10.10.132.20: icmp_seq=4, time=0ms

Sent 5 packets, received 5 OK, 0 bad

You can configure the following properties of the issued ICMP packets:

IP Address

The destination IP Address.

Ping Length

The payload size of the ICMP packet. Values range from 2 bytes to 1452 bytes.

Ping Count

The count of the ICMP packet. Values range from 1 time to 60 times.

Ping Interval

The interval of the ICMP packet. Values range from 0 second to 30 seconds.

Buttons

- **Start:** Click to start transmitting ICMP packets.
- **New Ping:** Click to re-start diagnostics with PING.

3.3.3. Diagnostics - VeriPHY

VeriPHY Cable Diagnostics for Switch 1

Port [All ∨]

[Start]

	Cable Status							
Port	Pair A	Length A	Pair B	Length B	Pair C	Length C	Pair D	Length D
1	--	--	--	--	--	--	--	--
2	--	--	--	--	--	--	--	--
3	--	--	--	--	--	--	--	--
4	--	--	--	--	--	--	--	--
5	--	--	--	--	--	--	--	--

This page is used for running the VeriPHY Cable Diagnostics for 10/100 and 1G copper ports.

Press the "Start" button to run the diagnostics. This will take approximately 5 seconds. If all ports are selected, this can take approximately 15 seconds. When completed, the page refreshes automatically, and you can view the cable diagnostics results in the cable status table. Note that VeriPHY is only accurate for cables of length 7 - 140 meters.

10 and 100 Mbps ports will be linked down while running VeriPHY. Therefore, running VeriPHY on a 10 or 100 Mbps management port will cause the switch to stop responding until VeriPHY is complete.

The ports belong to the currently selected stack unit, as reflected by the page header.

Port

The port where you are requesting VeriPHY Cable Diagnostics.

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 3 meters

3.4. Web Management - Maintenance

Here you can make system maintenance such rebooting the PoE switch, reset all settings (except Switch's IP address) back to default value, updating switch firmware, or upload/download all system settings.

3.4.1. Maintenance - Restart Device
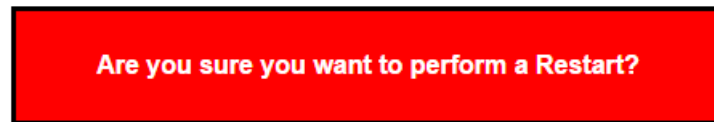
You can restart the stack on this page. After restart, the stack will boot normally.

Buttons

- **Yes:** Click to restart device.
- **No:** Click to return to the Port State page without restarting.

3.4.2. Maintenance - Factory Defaults

Factory Defaults

Are you sure you want to reset the configuration to Factory Defaults?

Yes   No

You can reset the configuration of the stack on this page. Only the IP configuration is retained.

The new configuration is available immediately, which means that no restart is necessary.

Buttons

- **Yes:** Click to reset the configuration to Factory Defaults.
- **No:** Click to return to the Port State page without resetting the configuration.

Note: Restoring factory default can also be performed by making a physical loopback between port 1 and port 2 within the first minute from switch reboot. In the first minute after boot, 'loopback' packets will be transmitted at port 1. If a 'loopback' packet is received at port 2 the switch will do a restore to default

3.4.3. Maintenance - Software Upload

Configuration Upload

Choose File | No file chosen   Upload

You can update the switch's firmware here.

Buttons

- **Choose File:** Click this button to choose the firmware file.

- **Update:** Click this button to start upload the firmware.

Firmware update in progress

> The uploaded firmware image is being transferred to flash.
> The system will restart after the update.
> Until then, do not reset or power off the device!

Waiting, please stand by...

The system will inform you when the new firmware is uploaded to the switch. After updating the firmware, the switch will reboot.

Warning: The management web page will stop functioning during the firmware updating process. Do not restart or power off the device at this time or the switch may malfunction.

3.4.3. Maintenance - Configuration

3.4.3.1. Configuration - Save

Configuration Save

Save Configuration
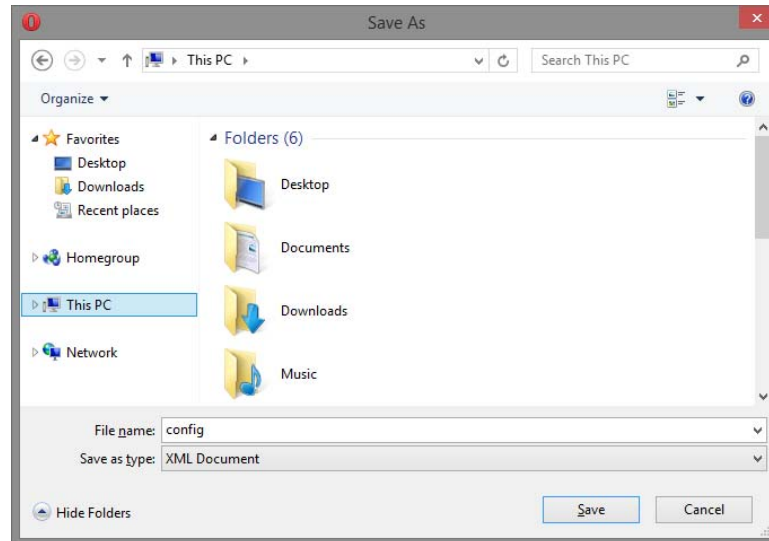
You can save all the current setting values as a file in XML format.

Buttons

- **Save Configuration:** Click to save the configuration file.

3.4.3.2. Configuration - Load

Configuration Upload

Choose File | No file chosen   Upload
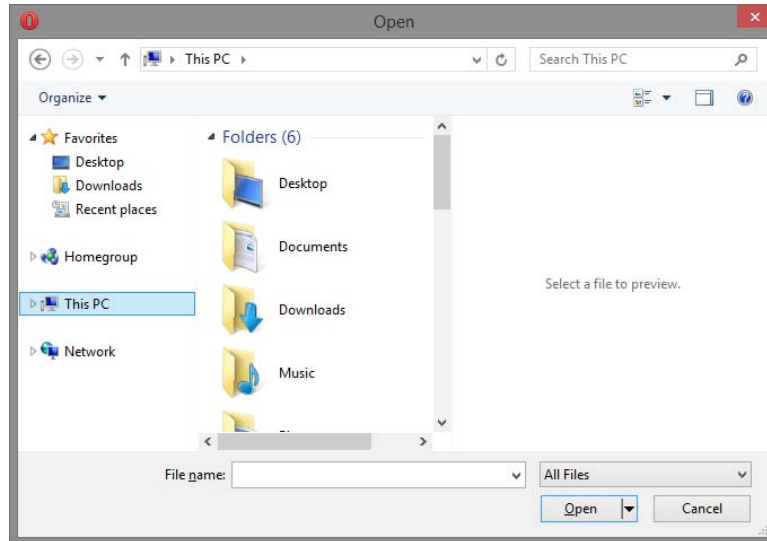
Buttons

- **Choose File:** Click this button to choose the configuration file that you've saved. .
- **Upload:** Click to upload the configuration file.

Chapter 4:

CLI Management

In CLI Management:

As mentioned in *Chapter 2.1. Preparation for Serial Console* and *Chapter 2.3. Preparation for Telnet/SSH Interface*, This switch provides a CLI (Command Line Interface) management interface. You can make all settings and monitor system status with this management CLI.

You can access the CLI via serial console, telnet, or SSH. All the commands for these three different connection types are the same and can be related. Please see the follow section for detailed descriptions about the commands.

4.1. CLI Management - Overview

The CLI (Command Line Interface) is a user interface that's embedded in the switch. You can view system information, status, and configure the switch via command inputting.

```
Password:
Login in progress...
Welcome to Vitesse Command Line Interface (v1.0).
Type 'help' or '?' to get help.

>
```

As shown in the figure above, a command prompt ">" will available, prompting you to input the command.

You can input part of the command here as well. For example, instead of "port configuration", you can input "por co" instead.

The following section will listing all the commands available in the switch.

4.2. CLI Management - System

Feature	Command Line
System Information	
System Group	Enter the System Configuration Group to do further configuration. >system Type 'up' to move up one level or '/' to go to root level System>
System Contact	**Syntax:** System Name [<name>] **Parameters:** <name>: System name string. (1-255) **Example:** Contact Name = Orwell System>contact Orwell
System Name	**Syntax:** System Name [<name>] **Parameters:** <name>: System name string. (1-255) **Example:** Contact Name = switch System>name switch switch:/> *(After given system name, the prompt character will be changed automatically.)*
System Location	**Syntax:** System Location [<location>] **Parameters:** <location>: System location string. (1-255) **Example:** Location Name switch:/System>loca fll_01
Time Zone Offset	**Syntax:** System Time zone [<offset>] **Parameters:**

	<offset>: Time zone offset in minutes (-720 to 720) relative to UTC **Example:** Time Zone = 100 switch:/System>time 100
IP Configuration	
IP Group	Enter the IP Configuration Group switch:/>ip Type 'up' to move up one level or '/' to go to root level switch:/IP>
DHCP Client	**Syntax:** IP DHCP [enable|disable] switch:/IP>dhcp en
IP Setting (Address, Mask, Gateway, Managed VID)	**Syntax:** IP Setup [<ip_addr>] [<ip_mask>] [<ip_router>] [<vid>] **Example:** IP=192.168.2.2, Mask=255.255.255.0, Gateway: 192.168.2.254, VID=1 switch:/IP>setup 192.168.2.2 255.255.255.0 192.168.2.254 1

NTP	Enable NTP Mode by below command:
	 switch:/IP>ntp mode en
	 Type the NTP Server address settings by below command:
	   Syntax:
	   IP NTP Server Add <server_index> <ip_addr_string>
	   IP NTP Server Ipv6 Add <server_index> <server_ipv6>
	   IP NTP Server Delete <server_index>
	   Example:
	   switch:/IP>ntp ser add 1 192.168.100.1
	   switch:/IP>ntp ser add 2 168.95.1.1
	 Check the NTP Server settings by below command:
	   switch:/IP>ntp conf
	   IP NTP Configuration:
	   =====================
	   NTP Mode : Enabled
	   Idx Server IP host address (a.b.c.d) or a host name string
	   --- --
	   1 192.168.100.1

	2 168.95.1.1	
	3	
	4	
	5	
DNS Server	**Syntax:**	
	IP DNS [<ip_addr>]	
	Parameters:	
	<ip_addr>: IP address (a.b.c.d), default: Show IP address	
	Example:	
	switch:/IP>dns 168.95.1.1	
DNS Proxy	**Syntax:** IP DNS_Proxy [enable|disable]	
	switch:/IP>dns_proxy en	
IPv6 Configuration		
IPv6 Commands	**Syntax:**	
	IP IPv6 AUTOCONFIG [enable|disable]	
	IP IPv6 Setup [<ipv6_addr>] [<ipv6_prefix>] [<ipv6_router>]	
	IP IPv6 State <ipv6_addr> [enable|disable]	
	IP IPv6 Ping6 <ipv6_addr> [(Length <ping_length>)] [(Count <ping_count>)] [(Interval <ping_interval>)]	
Auto Configuration	**Syntax:**	
	IP IPv6 AUTOCONFIG [enable|disable]	
	Example:	
	switch:/IP>ipv6 auto en	
IPv6 Address Setting (Address, Prefix, Router)	**Syntax:**	
	IP IPv6 Setup [<ipv6_addr>] [<ipv6_prefix>] [<ipv6_router>]	
	Example:	
	switch:/IP>ipv6 setup 2001:DB8::250:8bff:fee8:f800 48 2001:DB8::250:8bff:fee8:f8ff	
IPv6 Ping Test	**Syntax:**	
	IP IPv6 Ping6 <ipv6_addr> [(Length <ping_length>)] [(Count <ping_count>)] [(Interval <ping_interval>)]	
	Example:	
	switch:/IP>ipv6 ping6 2001:DB8::250:8bff:fee8:f800	
NTP		
NTP Mode	Enable NTP Mode by below command:	
	switch:/IP>ntp mode en	

NTP Server Address Setting	**Syntax:** Type the NTP Server address settings by below command: IP NTP Server Add <server_index> <ip_addr_string> IP NTP Server Ipv6 Add <server_index> <server_ipv6> IP NTP Server Delete <server_index> **Example:** switch:/IP>ntp ser add 1 192.168.100.1 switch:/IP>ntp ser add 2 168.95.1.1
NTP Setting Status	Check the NTP Server settings by below command: switch:/IP>ntp conf IP NTP Configuration: ===================== NTP Mode : Enabled Idx Server IP host address (a.b.c.d) or a host name string --- --- 1 192.168.100.1 2 168.95.1.1 3 4 5
System Log	
Server Mode	**Syntax:** System Log Server Mode [enable|disable] **Example:** switch:/System>log server mode en
Server Address	**Syntax:** System Log Server Address [<ip_addr_string>] **Example:** switch:/System>log server add 192.168.2.100
Syslog Level	**Syntax:** System Log Level [info|warning|error] **Information:** switch:/System>log level inf **Warning:**

	switch:/System>log level war
	Error:
	switch:/System>log level err
Clear Syslog	**Syntax:**
	System Log Clear [all|info|warning|error]
	switch:/System>log clear all
System Log Configuration	switch:/System>log conf
	System Log Configuration:
	========================
	System Log Server Mode : Enabled
	System Log Server Address : 192.168.2.100
	System Log Level : Error

4.3. CLI Management - Port

Feature	Command Line
Port Configuration	
Port Group	switch:/>port Type 'up' to move up one level or '/' to go to root level switch:/Port>
Link State	**Syntax:** Port State [<port_list>] [enable|disable] **Example:** Enable/Disable Port 1 State. After port 1 disabled, the port can't access the switch. Port>state 1 en Port>state 1 dis
Link Speed and Duplex	**Syntax:** Port Mode [<port_list>] [auto|10hdx|10fdx|100hdx|100fdx|1000fdx|sfp_auto_ams|1000x_ams|100fx_ams|1000x|100fx] **Example:** Port>mode 2 1000fdx (Configure port 2 to 1000 Full Duplex) Port>mode 1-4 1000fdx (Configure port 1-4 to 1000 Full Duplex)
Flow Control	**Syntax:** Port Flow Control [<port_list>] [enable|disable] **Example:** Port>flow cont 1 en (Enable Flow Control on Port 1) Port>flow cont 1 dis (Disable Flow Control on Port 2)
Maximum Frame Size	**Syntax:** Port MaxFrame [<port_list>] [<max_frame>] **Example:** Set port 1-24's maximum frame size to 9K jumbo frame

	Port>maxf 1-24 9600
Port Status	
Port Status	Port>conf 1-2 Port Configuration: ================== Port State Mode Flow Control MaxFrame Power Excessive Link ---- ------- ---------- ------------ -------- -------- --------- ---- 1 Enabled Auto Disabled 9600 Disabled Discard Down 2 Enabled Auto Disabled 9600 Disabled Discard 1Gfdx ....
Port Mode	Port>mode 2 Port Mode Link ---- ---------- ---- 2 Auto 1Gfdx
Port Status - All Information	switch:/Port>config Port Configuration: ================== Port State Mode Flow Control MaxFrame Power Excessive Link ---- ------- ---------- ------------ -------- -------- --------- ---- 1 Enabled Auto Disabled 9600 Disabled Discard Down 2 Enabled Auto Disabled 9600 Disabled Discard 1Gfdx 3 Enabled Auto Disabled 9600 Disabled Discard Down ....
Status of Link UP ports	switch:/Port>conf all up Port Configuration: ================== Port State Mode Flow Control MaxFrame Power Excessive Link

	---- -------- ----------- ------------ -------- -------- --------- ----
	2 Enabled Auto Disabled 9600 Disabled Discard 1Gfdx
Port Statistic	switch:/Port>statistic 1
	Port 1 Statistics:
	Rx Packets: 0 Tx Packets: 0
	Rx Octets: 0 Tx Octets: 0
	Rx Unicast: 0 Tx Unicast: 0
	....

4.4. CLI Management - MAC

Feature	Command Line
MAC Address Table Configuration	
Aging Time Configuration	**Syntax:** MAC Agetime [<age_time>] **Parameters:** <age_time>: MAC address age time (0,10-1000000) 0=disable **Example:** MAC>age 100　　(change aging time to 100 seconds, the aging time range is 10-1000000) MAC>age 0　　(0 = Disable Aging time)
MAC Learning Configuration	**Syntax:** MAC Learning [<port_list>] [auto|disable|secure] **Example:** MAC>lear 1-8 sec MAC>lear 9-12 dis MAC>learn 1-12 auto
Static MAC Table	**Syntax:** MAC Add <mac_addr> <port_list> [<vid>] **Example:** MAC>add 0b16212c3742 1-5 1 (This type will be changed to hexadecimal automatically.) MAC>add 0b-16-21-2c-37-42 1-10 1 (This type is hexadecimal, it will not be changed.) **Result:** Non-volatile static: VID MAC Address Ports --- ---------------- ----- 1 00-10-15-02-25-2a 1-5 1 0b-16-21-2c-37-42 1-10

4.5. CLI Management - VLAN

Feature	Command Line
VLAN Configuration	
VLAN Membership	**Syntax:** VLAN Add <vid>|<name> [<ports_list>] VLAN Name Add <name> <vid> **Example:** VLAN>add 3 5-8 (Add port 5-8 to VLAN 3) VLAN>name add vlan3 3 (vlan3 is the name of VLAN 3)
Port Configuration	**Syntax:** VLAN FrameType [<port_list>] [all|tagged|untagged] VLAN IngressFilter [<port_list>] [enable|disable] VLAN tx_tag [<port_list>] [untag_pvid|untag_all|tag_all] VLAN PortType [<port_list>] [unaware|c-port|s-port|s-custom-port] **Example:** VLAN>framety 1-3 all VLAN>ingr 1-3 en VLAN>tx_t 1-3 untag_pvid VLAN>portty 1-3 un

4.6. CLI Management - PVLAN (Private VLAN)

Feature	Command Line
PVLAN Configuration	
PVLAN Configuration	**Syntax:** PVLAN Configuration [<port_list>] PVLAN Add <pvlan_id> [<port_list>] PVLAN Delete <pvlan_id> PVLAN Lookup [<pvlan_id>] PVLAN Isolate [<port_list>] [enable|disable] **Example:** PVLAN>add 10 9-12 PVLAN>add 10 1-2 PVLAN>add 20 1-2 PVLAN>add 20 13-18 PVLAN>iso 9-18 en (Enable Isolated Ports) **Result:** PVLAN ID Ports -------- ----- 1 1-8,17-26 10 1,2 20 13-18

4.7. CLI Management - Security

Feature	Command Line
Security-Switch Configuration	
Security -Switch Group	>securi swi Type 'up' to move up one level or '/' to go to root level Security/Switch>? Command Groups: --------------- Security Switch Users : User management Security Switch Privilege: Privilege level Security Switch Auth : Authentication Security Switch SSH : Secure Shell Security Switch HTTPS : Hypertext Transfer Protocol over Secure Socket Layer Security Switch Access : Access management Security Switch SNMP : Simple Network Management Protocol Security Switch RMON : Remote Network Monitoring
User Configuration	Security/Switch>user ? Available Commands: Security Switch Users Configuration Security Switch Users Add <user_name> <password> <privilege_level> Security Switch Users Delete <user_name>
Add New User	**Syntax:** Security Switch Users Add <user_name> <password> <privilege_level> **Example:** Add New User Name, Password with highest privilege, Name: Orwell, Password: possword, Privilege: 15 Security/Switch>users add Orwell password 15
Delete the User	**Syntax:**

	Security Switch Users Delete <user_name> **Example:** Delete the User, Orwell from User Name database Security/Switch>users del Orwell
User Name Database	Security/Switch>users conf Users Configuration: ==================== User Name Privilege Level ------------------------------- --------------- admin 15 Orwell 15
Privilege Level	**Syntax:** Security Switch Privilege Level Group <group_name> [<cro>] [<crw>] [<sro>] [<srw>] (cro=Configuration Read-Only, crw=Configuration/Excute Read/Write, sro=Status/Statistics Read-Only, srw=Status/Statistics Read/Write) **Example:** Set Privilege level of VLAN Group Security/Switch/Privilege>level group VLANs 10 10 10 10 (cro=10, crw=10, sro=10, srw=10)
Privilege Level Configuration Table	Security/Switch>pri level conf Privilege Level Configuration: ============================= Privilege Current Level: 15 Group Name Privilege Level CRO CRW SRO SRW

	--------------------------------- --- --- --- --- Aggregation 5 10 5 10 Debug 15 15 15 15 Diagnostics 5 10 5 10
Authentication Method	**Syntax:** Security Switch Auth Method [console|telnet|ssh|web] [none|local|radius|tacacs+] [enable|disable] **Example:** Configure Telnet Authentication method to Radius Enable Security/Switch>auth method telnet radius en
Authentication Configuration	Security/Switch>auth conf Auth Configuration: =================== Client Authentication Method Local Authentication Fallback ------- --------------------- ----------------------------- console local Disabled telnet local Disabled ssh local Disabled web local Disabled
SSH	**Syntax:** Security Switch SSH Mode [enable|disable] **Example:** Security/Switch>ssh mode en Security/Switch>ssh mode dis
HTTPS	**Syntax:** Security Switch HTTPS Mode [enable|disable] Security/Switch>https mode en Security/Switch>https mode dis Security Switch HTTPS Redirect [enable|disable]

	Security/Switch>https mode en (Must enabled HTTPS) Security/Switch>https redi en **Result:** Security/Switch>https conf HTTPS Configuration: ==================== HTTPS Mode : Enabled HTTPS Redirect Mode : Enabled
Access Management	**Syntax:** Security Switch Access Add <access_id> <start_ip_addr> <end_ip_addr> [web] [snmp] [telnet] **Example:** Limit the IP range from the 192.168.2.1 to 192.168.2.10 can access the web UI. Security/Switch>access add 1 192.168.2.1 192.168.2.10 web
SNMP System Configuration (Mode, Version, Read /Write Community)	**Syntax:** Security Switch SNMP Mode [enable|disable] Security Switch SNMP Version [1|2c|3] Security Switch SNMP Read Community [<community>] Security Switch SNMP Write Community [<community>] **Example:** Security/Switch>snmp mode en Security/Switch>snmp ver 2c Security/Switch/SNMP>read com abc Security/Switch/SNMP>write com orwell **Result:**

	SNMP Configuration: =================== SNMP Mode : Enabled SNMP Version : 2c Read Community : abc Write Community : orwell
SNMP Community	**Syntax:** Security Switch SNMP Community Add <community> [<ip_addr>] [<ip_mask>] Security Switch SNMP Community Delete <index> Security Switch SNMP Community Lookup [<index>] **Example:** Security/Switch>snmp commu add abc Security/Switch>snmp commu add test 192.168.2.100 255.255.255.0
SNMP Trap Server Setting	Enter the SNMP Trap Configuration Group Security/Switch/SNMP>trap Type 'up' to move up one level or '/' to go to root level Security/Switch/SNMP/Trap> **Syntax:** Security Switch SNMP Trap Mode [enable|disable] Security Switch SNMP Trap Version [1|2c|3] Security Switch SNMP Trap Community [<community>] Security Switch SNMP Trap Destination [<ip_addr_string>] Security Switch SNMP Trap IPv6 Destination [<ipv6_addr>] **Example:** Security/Switch/SNMP/Trap>mode ena Security/Switch/SNMP/Trap>version 2c Security/Switch/SNMP/Trap>community public

	Security/Switch/SNMP/Trap>destination 192.168.2.100 **Result:** Trap Mode : Enabled Trap Version : 2c Trap Community : public Trap Destination : 192.168.2.100 Trap IPv6 Destination : ::
SNMP Trap Event Setting	**Syntax:** Security Switch SNMP Trap Authentication Failure [enable|disable] Security Switch SNMP Trap Link-up [enable|disable] Security Switch SNMP Trap Inform Mode [enable|disable] Security Switch SNMP Trap Inform Timeout [<timeout>] Security Switch SNMP Trap Inform Retry Times [<retries>] **Example:** Security/Switch/SNMP>trap auth fai en Security/Switch/SNMP>trap link-up en Security/Switch/SNMP>trap info mode en Security/Switch/SNMP>trap info time 5 Security/Switch/SNMP>trap info ret times 5 **Result:** Trap Authentication Failure : Enabled Trap Link-up and Link-down : Enabled Trap Inform Mode : Enabled Trap Inform Timeout (seconds) : 5 Trap Inform Retry Times : 5
SNMPv3 User	**Syntax:** Security Switch SNMP User Add <engineid> <user_name> [MD5|SHA] [<auth_password>] [DES] [<priv_password>] **Example:** Security/Switch/SNMP>user add 800007e5017f000001 orwell

	Security/Switch/SNMP>user add 800007e5017f000001 andy md5 andy123 **Result:** SNMPv3 Users Table: Idx Engine ID User Name Level Auth Priv --- --------- ----------------------------- -------------- ---- ---- 1 Local default_user NoAuth, NoPriv None 2 Local orwell NoAuth, NoPriv None 3 Local andy Auth, NoPriv MD5 None Number of entries: 3
RMON	In Security/Switch Group, the system supports 4 types RMON groups, please follow the RMON Syntax to add the entries. **Syntax:** Security/Switch>rmon ? **Statistics:** Security Switch RMON Statistics Add <stats_id> <data_source> Security Switch RMON Statistics Delete <stats_id> Security Switch RMON Statistics Lookup [<stats_id>] **Histroy:** Security Switch RMON History Add <history_id> <data_source> [<interval>] [<buckets>] Security Switch RMON History Delete <history_id> Security Switch RMON History Lookup [<history_id>] **Alarm:** Security Switch RMON Alarm Add <alarm_id> <interval> <alarm_vairable> [absolute|delta] <rising_threshold> <rising_event_index> <falling_threshold> <falling_event_index> [rising|falling|both] Security Switch RMON Alarm Delete <alarm_id> Security Switch RMON Alarm Lookup [<alarm_id>]

	Event: Security Switch RMON Event Add <event_id> [none|log|trap|log_trap] [<community>] [<description>] Security Switch RMON Event Delete <event_id> Security Switch RMON Event Lookup [<event_id>]
Security-Network Configuration	
Limit Control	
Limit Control - System Configuration	**Syntax:** Security Network Limit Configuration [<port_list>] Security Network Limit Mode [enable|disable] Security Network Limit Aging [enable|disable] Security Network Limit Agetime [<age_time>] **Example:** Security/Network>limit mode enable Security/Network>limit agin enable Security/Network>limit agetim 1000 **Result:** Port Security Limit Control Configuration: == Mode : Enabled Aging : Disabled Age Period: 3600
Limit Control - Port Configuration	**Syntax:** Security Network Limit Port [<port_list>] [enable|disable] Security Network Limit [<port_list>] [<limit>] Security Network Limit Action [<port_list>] [none|trap|shut|trap_shut] Security Network Limit Reopen [<port_list>] **Example:** Security/Network>limit port 1 enabl

	Security/Network>limit 1 5
	Security/Network>limit action 1 trap

Network Access Server Configuration (also known as IEEE 802.1X)	
NAS System Configuration	**Syntax:** **Mode:** Security Network NAS Mode [enable|disable] Security Network NAS Re-authentication [enable|disable] **Time Settings** Security Network NAS ReauthPeriod [<reauth_period>] Security Network NAS EapolTimeout [<eapol_timeout>] Security Network NAS Agetime [<age_time>] Security Network NAS Holdtime [<hold_time>] **Radius-Assigned** Security Network NAS RADIUS_QoS [global|<port_list>] [enable|disable] Security Network NAS RADIUS_VLAN [global|<port_list>] [enable|disable] **Guest VLAN** Security Network NAS Guest_VLAN [global|<port_list>] [enable|disable] [<vid>] [<reauth_max>] [<allow_if_eapol_seen>] **Example:** Guest_VLAN Global Enabled, Guest VLAN ID=100, Max. Re-Authentication Count = 10, Allow Guest VLAN if EAPOL See = Enable Security/Network>nas gues glob en 100 10 en
NAS Port Configuration	**Syntax**: Security Network NAS State [<port_list>] [auto|authorized|unauthorized|single|multi|macbased] auto= Port-based 802.1X authorized = Force Authorized unauthorized = Force Unauthorized

	single = Single 802.1X multi= Multi 802.1X macbased = MAC_Based Authentication **Example:** Security/Network>nas state 2 auto
ACL (Access Control List)	
ACL Port Configuration	**Syntax**: Security Network ACL Action [<port_list>] [permit|deny] [<rate_limiter>] [<port_redirect>] [<mirror>] [<logging>] [<shutdown>] **Parameters:** <port_list> : Port list or 'all', default: All ports permit : Permit forwarding (default) deny : Deny forwarding <rate_limiter> : Rate limiter number (1-15) or 'disable' <port_redirect>: Port list for copy of frames or 'disable' <mirror> : Mirror of frames: enable|disable <logging> : System logging of frames: log|log_disable <shutdown> : Shut down ingress port: shut|shut_disable **Example:** Security/Network/ACL>Action 1 permit 10 dis en log shut **Result:** ACL Configuration: ================== Port Policy Action Rate L. Port C. Mirror Logging Shutdown Counter ---- ------ ------ ------- ------- -------- -------- -------- ------- 1 0 Permit 10 Disabled Enabled Enabled Enabled 0
Rate Limiter	**Syntax**: Security Network ACL Rate [<rate_limiter_list>] [<rate_unit>] [<rate>]

	Parameters: <rate_limiter_list>: Rate limiter list (1-16), default: All rate limiters <rate_unit> : IP flags: pps|kbps, default: pss <rate>: Rate in pps (0-100) or kbps (0, 100, 2*100, 3*100, ..., 1000000) **Example: Rate Limiter ID=10, Rate = 300kbps** Security/Network/ACL>rate 10 kbps 300 **Result:** Rate Limiter Rate ----------- ---- .... 9 1 PPS 10 300 KBPS ....
ACL Policy	**Syntax:** Security Network ACL Policy [<port_list>] [<policy>] **Example:** Security/Network/ACL>policy 1 2
Access Control List	**Syntax:** Security Network ACL Add [<ace_id>] [<ace_id_next>] [(port <port_list>)] [(policy <policy> <policy_bitmask>)] [<tagged>] [<vid>] [<tag_prio>] [<dmac_type>] [(etype [<etype>] [<smac>] [<dmac>]) | (arp [<sip>] [<dip>] [<smac>] [<arp_opcode>] [<arp_flags>]) | (ip [<sip>] [<dip>] [<protocol>] [<ip_flags>]) | (icmp [<sip>] [<dip>] [<icmp_type>] [<icmp_code>] [<ip_flags>]) | (udp [<sip>] [<dip>] [<sport>] [<dport>] [<ip_flags>]) | (tcp [<sip>] [<dip>] [<sport>] [<dport>] [<ip_flags>] [<tcp_flags>])] [permit|deny] [<rate_limiter>] [<port_redirect>] [<mirror>] [<logging>][<shutdown>]

Parameters:

<ace_id>   : ACE ID (1-256), default: Next available ID

<ace_id_next>   : Next ACE ID (1-256), default: Add ACE last

port   : Port ACE keyword

<port_list>   : Port list or 'all', default: All ports

policy   : Policy ACE keyword

<policy>   : Policy number (0-255)

<policy_bitmask>: Policy number bitmask (0x0-0xFF)

<tagged>   : Tagged of frames: any|enable|disable

<vid>   : VLAN ID (1-4095) or 'any'

<tag_prio>   : VLAN tag priority (0-7) or 'any'

<dmac_type>   : DMAC type: any|unicast|multicast|broadcast

etype   : Ethernet Type keyword

<etype>   : Ethernet Type: 0x600 - 0xFFFF or 'any' but excluding 0x800(IPv4) 0x806(ARP) and 0x86DD(IPv6)

<smac>   : Source MAC address ('xx-xx-xx-xx-xx-xx' or 'xx.xx.xx.xx.xx.xx' or 'xxxxxxxxxxxx', x is a hexadecimal digit) or 'any'

<dmac>   : Destination MAC address ('xx-xx-xx-xx-xx-xx' or 'xx.xx.xx.xx.xx.xx' or 'xxxxxxxxxxxx', x is a hexadecimal digit) or 'any'

arp   : ARP keyword

<sip>   : Source IP address (a.b.c.d/n) or 'any'

<dip>   : Destination IP address (a.b.c.d/n) or 'any'

<arp_opcode>   : ARP operation code: any|arp|rarp|other

<arp_flags>   : ARP flags: request|smac|tmac|len|ip|ether [0|1|any]

ip   : IP keyword

<protocol>   : IP protocol number (0-255) or 'any'

<ip_flags>   : IP flags: ttl|options|fragment [0|1|any]

icmp   : ICMP keyword

<icmp_type>   : ICMP type number (0-255) or 'any'

<icmp_code>   : ICMP code number (0-255) or 'any'

udp   : UDP keyword

<sport>   : Source UDP/TCP port range (0-65535) or 'any'

<dport>   : Destination UDP/TCP port range (0-65535) or 'any'

	tcp : TCP keyword
	<tcp_flags> : TCP flags: fin|syn|rst|psh|ack|urg [0|1|any]
	permit : Permit forwarding (default)
	deny : Deny forwarding
	<rate_limiter> : Rate limiter number (1-15) or 'disable'
	<port_redirect> : Port list for copy of frames or 'disable'
	<mirror> : Mirror of frames: enable|disable
	<logging> : System logging of frames: log|log_disable
	<shutdown> : Shut down ingress port: shut|shut_disable
	Example:
	Add one ACE:
	Security/Network/ACL>add 2 port 6-10 policy 3 8 ip
	ACE ID 2 added last
	Edit one ACE:
	Security/Network/ACL>add 1 port 1-5 policy 2 8 any
	ACE ID 1 modified last
	Result:
	ID Type Port Policy Frame Action Rate L. Port C. Mirror Counter
	-- ------- -------- -------- ----- ------ -------- -------- -------- -------
	1 User 1-5 2 /0x8 Any Permit Disabled Disabled Disabled 0
	2 User 6-10 3 /0x8 IP Permit Disabled Disabled Disabled 0
DHCP	
DHCP Snooping	**Syntax:**
	Security Network DHCP Snooping Mode [enable|disable]
	Security Network DHCP Snooping Port Mode [<port_list>]
	[trusted|untrusted]
	Security Network DHCP Snooping Statistics [<port_list>] [clear]
	Example:
	Security/Network>dhcp snooping mode en
	Security/Network>dhcp snooping port mode 1 tru (Port 1)
	Security/Network>dhcp snooping port mode 1-10 tru (Port 1-10)

DHCP Relay	**Syntax:** Security Network DHCP Relay Mode [enable|disable] Security Network DHCP Relay Server [<ip_addr>] Security Network DHCP Relay Information Mode [enable|disable] Security Network DHCP Relay Information Policy [replace|keep|drop] **Example:** Security/Network>dhcp relay server 192.168.2.100 Security/Network>dhcp relay mode en (Assign one Server IP before enable the Relay mode) Security/Network>dhcp rel info mode en Security/Network>dhcp rel info policy keep
IP Source Guard	
IP Source Guard Configuration	**Syntax:** Security Network IP Source Guard Configuration Security Network IP Source Guard Mode [enable|disable] Security Network IP Source Guard Port Mode [<port_list>] [enable|disable] Security Network IP Source Guard limit [<port_list>] [<dynamic_entry_limit>|unlimited] Security Network IP Source Guard Entry [<port_list>] add|delete <vid> <allowed_ip> <allowed_mac> Security Network IP Source Guard Status [<port_list>] Security Network IP Source Guard Translation **Example:** Security/Network>ip source guard mode en Security/Network>ip source guard port mode 1-10 en (Port 1-10) Security/Network>ip source guard limit 1-10 2 (limit 2 MAC Address)
IP Source Guard Static	**Syntax:**

Table	Security Network IP Source Guard Entry [<port_list>] add|delete <vid> <allowed_ip> <allowed_mac>
	Example:
	Security/Network>ip source guard entry 5 add 2 192.168.2.101 001122334455
	Result:
	IP Source Guard Entry Table:
	Type Port VLAN IP Address MAC Address
	------- ---- ---- -------------- -----------------
	Static 1 1 192.168.2.10 11-22-33-44-55-66
	Static 5 2 192.168.2.101 00-0b-16-21-2c-37
ARP Inspection	
ARP Inspection	**Syntax:**
	Security Network ARP Inspection Configuration
	Security Network ARP Inspection Mode [enable|disable]
	Security Network ARP Inspection Port Mode [<port_list>] [enable|disable]
	Security Network ARP Inspection Entry [<port_list>] add|delete <vid> <allowed_mac> <allowed_ip>
	Security Network ARP Inspection Status [<port_list>]
	Security Network ARP Inspection Translation
	Example:
	Security/Network>arp inspection mode en
	Security/Network>arp inspection port mode 1-10 en
	Security/Network>arp inspection entry 1 add 10 112233445566 192.168.2.10
	Security/Network>arp inspection status
	ARP Inspection Entry Table:

	Type Port VLAN MAC Address IP Address ------- ---- ---- ----------------- ------------- Static 1 10 0b-16-21-2c-37-42 192.168.2.10
Security-AAA Configuration	
Common Server Configuration	**Syntax:** Security AAA Timeout [<timeout>] Security AAA Deadtime [<dead_time>]
RADIUS Authentication Server	**Syntax:** Security AAA RADIUS [<server_index>] [enable|disable] [<ip_addr_string>] [<secret>] [<server_port>] **Example:** Security>aaa radi 1 en 192.168.2.200 password 1812
RADIUS Accounting Server	**Syntax:** Security AAA ACCT_RADIUS [<server_index>] [enable|disable] [<ip_addr_string>] [<secret>] [<server_port>] **Example:** Security>aaa ACCT_radi 1 en 192.168.2.200 password 1813
TACACS+ Authentication Server	**Syntax:** Security AAA TACACS+ [<server_index>] [enable|disable] [<ip_addr_string>] [<secret>] [<server_port>] **Example:** Security>aaa tacacs+ 1 en 192.168.2.200 password 49
AAA Configuration	Security>aaa con AAA Configuration: ================== Server Timeout : 15 seconds Server Dead Time : 300 seconds

```
RADIUS Authentication Server Configuration:

==========================================

Server   Mode      IP Address      Secret                          Port

------   --------  --------------  ----------------------------    -----

1        Enabled   192.168.2.200   ********                        1812

2        Disabled                                                  1812

3        Disabled                                                  1812

4        Disabled                                                  1812

5        Disabled                                                  1812


RADIUS Accounting Server Configuration:

=======================================

Server   Mode      IP Address      Secret                          Port

------   --------  --------------  ----------------------------    -----

1        Enabled   192.168.2.200   ********                        1813

2        Disabled                                                  1813

3        Disabled                                                  1813

4        Disabled                                                  1813

5        Disabled                                                  1813


TACACS+ Authentication Server Configuration:

===========================================

Server   Mode      IP Address      Secret                          Port

------   --------  --------------  ----------------------------    -----

1        Enabled   192.168.2.200   ********                        49

2        Disabled                                                  49

3        Disabled                                                  49

4        Disabled                                                  49

5        Disabled                                                  49

Security>
```

4.8. CLI Management - STP

Feature	Command Line
Bridge Configuration	
Protocol Version	**Syntax:** STP Version [<stp_version>] **Parameters:** \<stp_version>: mstp|rstp|stp **Example:** STP>ver rstp
Bridge Priority	**Syntax**: STP Msti Priority [<msti>] [<priority>] **Example**: STP>msti pri MSTI# Bridge Priority ----- -------------- CIST 32768 STP>msti pri 4096 (The available priority parameter includes: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440)
Forward Delay	**Syntax**: STP FwdDelay [<delay>] (Valid values are in the range 4 to 30 seconds)
Max. Age	**Syntax**: STP MaxAge [<max_age>] (Valid values are in the range 6 to 40 seconds, *and* MaxAge must be <= (FwdDelay-1)*2.)
Maximum Hop Count	**Syntax**: STP MaxHops [<maxhops>]

	(Valid values are in the range 6 to 40 hops)
Transmit Hold Count	**Syntax**: STP Txhold [<holdcount>] (Valid values are in the range 1 to 10 BPDU's per second.)
Advanced Setting	**Syntax**: STP bpduFilter [enable|disable] STP bpduGuard [enable|disable] STP recovery [<timeout>] (After recovery timeout time is set, the recovery is enabled automatically.)
MSTI Mapping	
MSTI/VLAN Mapping	**Syntax:** STP Msti Add <msti> <vid-range> **Example:** STP>mst add 1 100 Add VLAN 100 to MSTI1 STP>mst map MSTI VLANs mapped to MSTI ---- ------------------- MSTI1 100 MSTI2 No VLANs mapped MSTI3 No VLANs mapped MSTI4 No VLANs mapped MSTI5 No VLANs mapped MSTI6 No VLANs mapped MSTI7 No VLANs mapped
Port Setting	
STP Port Mode	**Syntax:** STP Port Mode [<port_list>] [enable|disable] STP Port Edge [<port_list>] [enable|disable] STP Port AutoEdge [<port_list>] [enable|disable] STP Port P2P [<port_list>] [enable|disable|auto] STP Port RestrictedRole [<port_list>] [enable|disable]

	STP Port RestrictedTcn [<port_list>] [enable|disable]
	STP Port bpduGuard [<port_list>] [enable|disable]
	STP Port Statistics [<port_list>] [clear]
	Example:
	STP>port mode 1-24 dis (Disable STP on port 1-24)
	STP>port edge 1-24 en (Enable Edge port on port 1-24)
	STP>port autoedge 1-24 en (Enable Auto Edge on P1-24)
	STP>port p2p 1-24 en (Enable P2P mode on P1-24)
	STP>port p2p 1-24 auto (Enable Automatic P2P detection)
	STP>port bpdu 1-24 en (Enable BPDUGuard on P1-24)
Port Path Cost	**Syntax:**
	STP Msti Port Cost [<msti>] [<port_list>] [<path_cost>]
	Parameters:
	<msti> : STP bridge instance no (0-7, CIST=0, MSTI1=1, ...)
	<port_list>: Port list or 'all'. Port zero means aggregations.
	<path_cost>: STP port path cost (1-200000000) or 'auto'
	Example: Configure CIST 0 Port Path Cost
	STP>msti port cost 0 all auto (Path cost = auto)
	STP>msti port cost 0 all 100000 (Path cost = 100000)
Port Priority	**Syntax:**
	STP Msti Port Priority [<msti>] [<port_list>] [<priority>]
	Parameters:
	<msti> : STP bridge instance no (0-7, CIST=0, MSTI1=1, ...)
	<port_list>: Port list or 'all'. Port zero means aggregations.
	<priority> : STP port priority (0/16/32/48/.../224/240)
	Example: Configure CIST 0 Port Priority
	STP Msti Port Priority [<msti>] [<port_list>] [<priority>]
	STP>msti port priority 0 5 240 (Port 5 Priority = 240)
	STP>msti port priority 0 all 128 (All Ports' priority = 128)

	Example: Configure MSTI 1 Port Priority
	STP>msti port priority 1 5 240 (MSTI1 port 5 priority=240)

4.9. CLI Management - Aggr

Feature	Command Line
Static Aggregation Configuration	
Aggregation Group Configuration	**Syntax:** Aggr Add <port_list> [<aggr_id>] **Example:** Add port 5-8 to Group 1 >aggr add 5-8 1 >aggr del 1 (Delete the group 1)
Hash Code Contributors	**Syntax:** Aggr Mode [smac|dmac|ip|port] [enable|disable] smac = Source MAC Address dmac = Destination MAC Address ip = IP Address port = TCP/UDP Port Number **Example:** Only the Source MAC Hash is enabled. The rest mode are disabled. >agg mode smac en >agg mode dmac dis >agg mode ip dis >agg mode port dis
LACP	
LACP Port Configuration	**Syntax:** LACP Configuration [<port_list>] LACP Mode [<port_list>] [enable|disable] LACP Key [<port_list>] [<key>] LACP Role [<port_list>] [active|passive] LACP Status [<port_list>] LACP Statistics [<port_list>] [clear]

Example: Configure port 5-8 to a LACP group

>lacp mode 5-8 en   (Mode = Enable)

>lacp key 5-8 100   (Key = 100)

>lacp role 5-8 act   (Role = Enable)

4.10. CLI Management - LACP

Feature	Command Line
LACP Functions	
Configuration	**Description:** Show LACP configuration. **Syntax:** LACP Configuration [<port_list>] **Parameters:** <port_list>: Port list or 'all', default: All ports
Mode	**Description:** Set or show LACP mode. **Syntax:** LACP Mode [<port_list>] [enable|disable] **Parameters:** <port_list>: Port list or 'all', default: All ports enable : Enable LACP protocol disable: Disable LACP protocol (default: Show LACP mode)
Key	**Description:** Set or show the LACP key. **Syntax:** LACP Key [<port_list>] [<key>] **Parameters:** <port_list>: Port list or 'all', default: All ports <key> : LACP key (1-65535) or 'auto'
Prio	**Description:** Set or show the LACP prio. **Syntax:**

	LACP Prio [<port_list>] [<prio>]
	Parameters:
	<port_list>: Port list or 'all', default: All ports
	<prio> : LACP Prio (0-65535)
System Prio	**Description:**
	Set or show the LACP System prio.
	Syntax:
	LACP System Prio [<sysprio>]
	Parameters:
	<sysprio>: LACP System Prio (0-65535)
Role	**Description:**
	Set or show the LACP role.
	Syntax:
	LACP Role [<port_list>] [active|passive]
	Parameters:
	<port_list>: Port list or 'all', default: All ports
	active : Initiate LACP negotiation
	passive: Listen for LACP packets
	(default: Show LACP role)
Status	**Description:**
	Show LACP Status.
	Syntax:
	LACP Status [<port_list>]
	Parameters:
	<port_list>: Port list or 'all', default: All ports
Statistics	**Description:**
	Show LACP Statistics.
	Syntax:
	LACP Statistics [<port_list>] [clear]

	Parameters: <port_list>: Port list or 'all', default: All ports clear : Clear LACP statistics
Timeout	**Description:** Set or show the LACP timeout. **Syntax:** LACP Timeout [<port_list>] [fast|slow] **Parameters:** <port_list>: Port list or 'all', default: All ports fast : Fast PDU transmissions (fast timeout) slow : Slow PDU transmissions (slow timeout) (default: Show LACP timeout)

4.11. CLI Management - LLDP

Feature	Command Line
LLDP Parameters	
LLDP Timers	**Syntax:** LLDP Interval [<interval>] LLDP Hold [<hold>] LLDP Delay [<delay>] LLDP Reinit [<reinit>] **Example:** LLDP>interval 30 LLDP>hold 4 LLDP>delay 2 LLDP>reini 2
LLDP Mode	**Syntax:** LLDP Mode [<port_list>] [enable|disable|rx|tx] (rx=RX Only, tx=TX Only) **Example:** Enable LLDP on Ports LLDP>mode 1-10 en (Port 1-10 are enabled) LLDP>mode 1-26 en (Port 1-26 are enabled)
CDP aware	**Syntax:** LLDP cdp_aware [<port_list>] [enable|disable] **Example:** Enable CDP on Port 1-5 LLDP>cdp_a 1-5 en (CDP on Port 1-5 are enabled)
LLDP Optional_TLV Parameters	**Syntax:** LLDP optional_TLV [<port_list>] [port_descr|sys_name|sys_descr|sys_capa|mgmt_addr] [enable|disable] **Example:** LLDP>option 1-3 port en LLDP>option 1-3 sys_name en LLDP>option 1-3 sys_desc en LLDP>option 1-3 sys_capa en

	LLDP>option 1-3 mgmt_add en

4.12. CLI Management - LLDPMED

Feature	Command Line
LLDPMED Parameters	
Configuration	**Description:** Show LLDP-MED configuration. **Syntax:** LLDPMED Configuration [<port_list>] **Parameters:** <port_list>: Port list or 'all', default: All ports LLDPMED>config ? **Description:** Show LLDP-MED configuration. **Syntax:** LLDPMED Configuration [<port_list>] **Parameters:** <port_list>: Port list or 'all', default: All ports
Civic	**Description:** Set or show LLDP-MED Civic Address Location. **Syntax:** LLDPMED Civic [country|state|county|city|district|block|street|leading_street_direction|trailing_street_suffix|str_suf|house_no|house_no_suffix|landmark|additio nal_info|name|zip_code|building|apartment|floor|room_number|place_type|postal_co m_name|p_o_box|additional_code] [<civic_value>] **Parameters:** country: Country

	state: National subdivisions (state, caton, region, province, prefecture)
	county: County, parish,gun (JP), district(IN)
	city: City, townchip, shi (JP)
	district: City division,borough, city, district, ward,chou (JP)
	block: Neighborhood, block
	street: Street
	leading_street_direction : Leading street direction
	trailing_street_suffix: Trailing street suffix
	str_suf: Street Suffix
	house_no: House Number
	house_no_suffix: House number suffix
	landmark: Landmark or vanity address
	additional_info: Additional location informationname: Name(residence and office occupant)
	zip_code: Postal/zip code
	building: Building (structure)
	apartment: Unit (apartment, suite)
	floor: Floor
	room_number: Room number
	place_type: Placetype
	postal_com_name: Postal community name
	p_o_box: Post office box (P.O. Box)
	additional_code: Additional code
	(default: Show Civic Address Location configuration)
	<civic_value>: lldpmed The value for the Civic Address Location entry.
ecs	**Description:** Set or show LLDP-MED Emergency Call Service. **Syntax:** LLDPMED ecs [<ecs_value>] **Parameters:** <ecs_value>: lldpmed The value for the Emergency Call Service

Policy	
Delete	**Description:** Delete the selected policy. **Syntax:** LLDPMED policy delete <policy_list> **Parameters:** <policy_list>: List of policies to delete
Add	**Description:** Adds a policy to the list of polices. **Syntax:** LLDPMED policy add <policy_type> [tagged|untagged] [<vlan_id>] [<l2_priority>] [<dscp>] **Parameters:** <policy_type>: The policy_type parameter takes the following values: **voice:** 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:** Voice Signaling (conditional) for use in network topologies that require a different policy for the voice signaling than for the voice media. **guest_voice:** 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:** 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.

softphone_voice: 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.

video_conferencing: Video Conferencing for use by dedicated Video Conferencing equipment and other similar appliances supporting real-time interactive video/audio services.

streaming_video: 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: Video Signaling (conditional) for use in network topologies that require a separate policy for the video signaling than for the video media.

tagged: The device is using tagged framesunragged: The device is using untagged frames

<vlan_id>: VLAN id
<l2_priority>: This field may specify one of eight priority levels (0 through 7), as defined by IEEE 802.1D-2004 [3].
<dscp>: This field shall contain the DSCP value to be used to provide Diffserv node behavior for the specified application type as defined in IETF RFC 2474 [5]. This 6 bit field may contain one of 64 code point values (0 through 63). A value of 0 represents use of the default DSCP value as defined in RFC 2475.

4.13. CLI Management - EEE

Feature	Command Line
EEE Configuration	
EEE Port Configuration	**Syntax**: EEE Mode [<port_list>] [enable|disable] **Parameters**: <port_list>: Port list or 'all', default: All ports enable : Enable EEE disable: Disable EEE **Example**: Enable Port 1-5 EEE>mode 1-5 en
Urgent Queue of Port	**Syntax**: EEE Urgent_queues [<port_list>] [<queue_list>] **Parameters**: <port_list> : Port list or 'all', default: All ports <queue_list>: List of queues to configure as urgent queues (1-8 or none) **Example**: Enable Urgent_Queue on Port 1-5 EEE>urge 1-5 2

4.14. CLI Management - POE

Feature	Command Line
PoE Configuration	
PoE Configuration	**Syntax**: PoE Mgmt_mode [class_con|class_res|al_con|al_res|lldp_res|lldp_con] **Parameters:** class_con : Class + Actual Consumption class_res : Class + Reserved Power al_con　　　 : Allocation + Actual Consumption al_res　　　 : Allocation + Reserved Power lldp_con　 : LLDP-MED + Actual Consumption lldp_res　 : LLDP-MED + Reserved Power **Example:** PoE>mgmt class_con
PoE Power Supply Configuration (Warning: The default value is for reference only. If the value is not comfort to your product specification, please give the correct value before you start using PoE function.)	**Syntax**: PoE Maximum_Power [<port_list>] [<port_power>] **Parameters:** <port_list> : Port list or 'all', default: All ports <port_power>: PoE maximum power for the port (0-15.4 Watt for PoE mode, 0-30.0 Watt for PoE+ mode) **Example:** PoE>max 1-24 10　　 (Max. power of Port 1-24 to 10Watt) PoE>max 1-24 15.4　 (Max. power of Port 1-24 to 15.4 Watt)
PoE Port Configuration	**Syntax:** PoE Mode [<port_list>] [disabled|poe|poe+] **Parameters:** <port_list>: Port list or 'all', default: All ports disables　　　 : Disable PoE
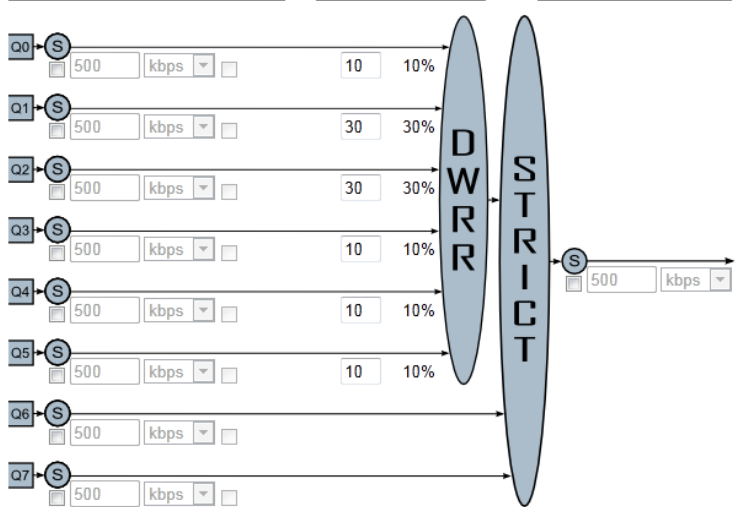
	poe: Enables PoE IEEE 802.3af (Class 4 limited to 15.4W) poe+: Enables PoE+ IEEE 802.3at (Class 4 limited to 30W) (default: Show PoE's mode) **Example:** Set Port 1-24 ro PoE+ mode PoE>mode 1-24 poe+
PoE Status	**Primary Power Supply** PoE>prim Primary Power Supply --------------------- 200 [W] **Port Status** PoE>sta Port PD Class Port Status Power Used [W] Current Used [mA] ---- -------- ------------------------------------- ------------- ------- --------- 1 - No PD detected 0.0 0 2 - No PD detected 0.0 0

4.15. CLI Management - QoS

Feature	Command Line
QoS Configuration	
Port Classification	**Syntax:** QoS Port Classification Class [<port_list>] [<class>] QoS Port Classification DPL [<port_list>] [<dpl>] QoS Port Classification PCP [<port_list>] [<pcp>] QoS Port Classification DEI [<port_list>] [<dei>] QoS Port Classification Tag [<port_list>] [enable|disable] QoS Port Classification Map [<port_list>] [<pcp_list>] [<dei_list>] [<class>] [<dpl>] QoS Port Classification DSCP [<port_list>] [enable|disable] **Range of the Value:** <class>: QoS class (0-7) <dpl>: Drop Precedence Level (0-1) <pcp>: Priority Code Point (0-7) <dei>: Drop Eligible Indicator (0-1) **Example:** QoS/Port/Classification>clas 1-2 7 QoS/Port/Classification>dpl 1-2 1 QoS/Port/Classification>pcp 1-2 7 QoS/Port/Classification>dei 1-2 1 QoS/Port/Classification>tag 1-2 en QoS/Port/Classification>dscp 1-2 en
QoS Ingress Port Tag Classification	**Syntax:** QoS Port Classification Map [<port_list>] [<pcp_list>] [<dei_list>] [<class>] [<dpl>]
Port Policing	**Syntax:** QoS Port Policer Mode [<port_list>] [enable|disable] QoS Port Policer Rate [<port_list>] [<rate>] QoS Port Policer Unit [<port_list>] [kbps|fps] QoS Port Policer FlowControl [<port_list>] [enable|disable]

	\<rate\>: Rate in kbps or fps (100-3300000) **Example:** QoS/Port/Policer>mode 1-2 en QoS/Port/Policer>rate 1-2 300 QoS/Port/Policer>unit 1-2 kbps QoS/Port/Policer>flow 1-2 en
Port Scheduler	**Syntax:** Syntax: QoS Port Scheduler Mode [\<port_list\>] [strict|weighted] **Example:** QoS/Port/Scheduler>mode 1-2 stric (Strict Priority) QoS/Port/Scheduler>mode 1-2 wei (Weighted) **QoS Egress Port Scheduler and Shapers** QoS/Port/Scheduler>wei 1-2 1 30 (Port 1-2, Q1=30) QoS/Port/Scheduler>wei 1-2 2 30 (Port 1-2, Q2=30)
Port Shaping	**Syntax:** **Port Shaper:** QoS Port Shaper Mode [\<port_list\>] [enable|disable] QoS Port Shaper Rate [\<port_list\>] [\<bit_rate\>]

	Queue Shaper: QoS Port QueueShaper Mode [<port_list>] [<queue_list>] [enable|disable] QoS Port QueueShaper Rate [<port_list>] [<queue_list>] [<bit_rate>] QoS Port QueueShaper Excess [<port_list>] [<queue_list>] [enable|disable] **Parameters:** <port_list>: Port list or 'all', default: All ports <bit_rate> : Rate in kilo bits per second (100-3300000) **Example:** QoS/Port/Shaper>rate 1-2 1000 QoS/Port/QueueShaper>mode 1-2 all en (Queue Shaper) QoS/Port/QueueShaper>rate 1-2 all 600 (Queue Shaper)
DSCP Configuration	**Syntax:** QoS Port DSCP Translation [<port_list>] [enable|disable] QoS Port DSCP Classification [<port_list>] [none|zero|selected|all] QoS Port DSCP EgressRemark [<port_list>] [disable|enable|remap_dp_unaware|remap_dp_aware] Note*: DSCP is an advanced QoS setting, please follow the DSCP table of upper access/core switch to configure the table. The table of the whole network must be unified.*
Storm Configuration	
Strom Control	**Syntax:** QoS Storm Unicast [enable|disable] [<packet_rate>] QoS Storm Multicast [enable|disable] [<packet_rate>] QoS Storm Broadcast [enable|disable] [<packet_rate>] <packet_rate>: Rate in fps (1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1k, 2k, 4k, 8k, 16k, 32k, 64k, 128k, 256k, 512k, 1024k, 2048k, 4096k, 8192k, 16384k, 32768k) **Example:** QoS/Storm>unic en 32768k

	QoS/Storm>multi en 4096k
	QoS/Storm>broad en 4k

4.16. CLI Management - Mirror

Feature	Command Line
Mirroring Configuration	
Mirror Configuration	**Syntax:** Mirror Port [<port>|disable] Mirror Mode [<port_cpu_list>] [enable|disable|rx|tx] **Example:** Mirror>port 5 Mirror>mode 6-8 en **Result:** Mirror Configuration: ===================== Mirror Port: 5 Port Mode ---- -------- 1 Disabled 2 Disabled 3 Disabled 4 Disabled 5 Disabled 6 Enabled 7 Enabled 8 Enabled

4.17. CLI Management - Config

Feature	Command Line
Config	
Save	**Description:** Save configuration to TFTP server. **Syntax:** Config Save <ip_server> <file_name> **Parameters:** <ip_server>: TFTP server IPv4 address (a.b.c.d) <file_name>: Configuration file name
Load	**Description:** Load configuration from TFTP server. **Syntax:** Config Load <ip_server> <file_name> [check] **Parameters:** <ip_server>: TFTP server IPv4 address (a.b.c.d) <file_name>: Configuration file name **check:** Check configuration file only, default: Check and apply file

4.18. CLI Management - Firmware

Feature	Command Line
Firmware	
Load	**Description:** Load new firmware from TFTP server. **Syntax:** Firmware Load <ip_addr_string> <file_name> **Parameters:** <ip_addr_string>: IP host address (a.b.c.d) or a host name string <file_name>: Firmware file name
IPv6 Load	**Description:** Load new firmware from IPv6 TFTP server. **Syntax:** Firmware IPv6 Load <ipv6_server> <file_name> **Parameters:** <ipv6_server>: TFTP server IPv6 address <file_name>: Firmware file name
Information	**Description:** Display information about active and alternate firmware images. **Syntax:** Firmware Information

4.19. CLI Management - UPnP

Feature	Command Line
UPnP Configuration	
UPnp Configuration	**Syntax:** UPnP Configuration UPnP Mode [enable|disable] UPnP TTL [<ttl>] UPnP AdvertisingDuration [<duration>] **Example:** UPnP>mode en UPnP>ttl 5 (Default=4) UPnP>adver 200 (Default=100) **Result:** UPnP Configuration: ================== UPnP Mode : Enabled UPnP TTL : 5 UPnP Advertising Duration : 200

4.20. CLI Management - MVR

Feature	Command Line
MVR Configuration	
MVR Mode	**Syntax**: MVR Mode [enable|disable]
MVR - VLAN Interface Setting	**Syntax:** MVR VLAN Setup [<mvid>] [add|del|upd] [(Name <mvr_name>)] **Example:** MVR VLAN 2, MVR Name = Source2 MVR>vlan setup 2 add Name Source2
MVR - Port Role	**Syntax:** MVR VLAN Port [<vid>|<mvr_name>] [<port_list>] [source|receiver|inactive] **Example:** Port 2 = Source Port, Port 6-7 = Receiver Port MVR>vlan port 2 2 source MVR>vlan port 2 6-7 rec
Immediately Leave	**Syntax:** MVR Immediate Leave [<port_list>] [enable|disable] **Example:** MVR>immedi leave 1-10 en
MVR Configuration	MVR>conf　　(View the settings of above configuration) MVR Configuration: ================== MVR Mode: Enabled MVR Interface Setting VID　Name　　　　　　　　　　　　Mode　　　Tagging　Priority　LLQI ----　--------------------------------　----------　--------　--------　----- 2　　Source2　　　　　　　　Dynamic　　Tagged　0　　　　5 [Port Setting of Source2(VID-2)] Source Port　: 2 Receiver Port: 6,7 Inactive Port: 1,3-5,8-26 [Channel Setting of Source2(VID-2)] <Empty Channel Table>

	MVR Immediate Leave Setting
	Port Immediate Leave
	---- ---------------
	1 Enabled
	2 Enabled
	3 Enabled
	4 Enabled
	5 Enabled
	6 Enabled
	7 Enabled
	8 Enabled
	9 Enabled
	10 Enabled
	11 Disabled
	12 Disabled

4.21. CLI Management - Voice VLAN

Feature	Command Line
Voice VLAN Configuration	
Voice VLAN Configuration	**Syntax:** Voice VLAN Mode [enable|disable] Voice VLAN ID [<vid>] Voice VLAN Agetime [<age_time>] Voice VLAN Traffic Class [<class>] **Example:** Voice>vlan mode en Voice>vlan id 100 Voice>vlan age 86400 Voice>vlan traff class 7 **Result:** Voice VLAN Configuration: ========================= Voice VLAN Mode : Enabled Voice VLAN VLAN ID : 100 Voice VLAN Age Time(seconds) : 86400 Voice VLAN Traffic Class : 7
Port Configuration	**Syntax:** Voice VLAN Port Mode [<port_list>] [disable|auto|force] Voice VLAN Security [<port_list>] [enable|disable] Voice VLAN Discovery Protocol [<port_list>] [oui|lldp|both] **Example:** Voice/VLAN>port mode 1-4 auto Voice/VLAN>security 1-4 en Voice/VLAN>disco pro 1-4 both **Result:** Voice VLAN Port Configuration: ============================== Port Mode Security Discovery Protocol ---- -------- -------- ------------------

	1	Auto	Enabled	Both
	2	Auto	Enabled	Both
	3	Auto	Enabled	Both
	4	Auto	Enabled	Both
OUI Configuration	**Syntax:** Voice VLAN OUI Add <oui_addr> [<description>] Voice VLAN OUI Delete <oui_addr> Voice VLAN OUI Clear Voice VLAN OUI Lookup [<oui_addr>] **Example:** Voice/VLAN>oui add 00-12-08 hello **Result:** Voice/VLAN>oui lookup Voice VLAN OUI Table: ===================== Telephony OUI Description ------------- ----------- 00-01-E3 Siemens AG phones 00-03-6B Cisco phones 00-0F-E2 H3C phones 00-60-B9 Philips and NEC AG phones 00-D0-1E Pingtel phones 00-E0-75 Polycom phones 00-E0-BB 3Com phones 00-12-77 e10 00-12-08 hello

4.22. CLI Management - Loop Protect

Feature	Command Line
General Settings	
Enable Loop Protection	**Syntax:** Loop Protect Mode [enable|disable] Loop Protect Transmit [<transmit-time>] Loop Protect Shutdown [<shutdown-time>] **Example:** >loop protect mode en
Transmission Time	>loop protect trans 10 (10 seconds)
Shutdown Time	>loop protect shut 200 (200 seconds)
Port Configuration	
Loop Protection - Port Configuration	**Syntax:** Loop Protect Port Mode [<port_list>] [enable|disable] Loop Protect Port Action [<port_list>] [shutdown|shut_log|log] Loop Protect Port Transmit [<port_list>] [enable|disable] **Example:** Loop/Protect>port mode 1 en Loop/Protect>port action 1 shut_log (Shutdown Port and Log) Loop/Protect>port transmit 1 en

4.23. CLI Management - IPMC

Feature	Command Line
IGMP Snooping Configuration	
IGMP Snooping Enable	**Syntax:** IPMC Mode [mld|igmp] [enable|disable] **Example:** IPMC>mode igmp en
Unregistered IPMCv4 Flooding Enabled	**Syntax:** IPMC Flooding [mld|igmp] [enable|disable] **Example:** IPMC>flood igmp en
IGMP SSM Range (Source-Specific Multicast)	**Syntax:** IPMC SSM [mld|igmp] [(Range <prefix> <mask_len>)] **Example:** IPMC>ssm igmp range 239.0.0.0 8 (Range from 239.0.0.0, mask length=8)
Leave Proxy Enable	**Syntax**: IPMC Leave Proxy [mld|igmp] [enable|disable] **Example:** IPMC>leave proxy igmp en (Enable) IPMC>leave proxy igmp dis (Disable)
Proxy Enable	**Syntax**: IPMC Proxy [mld|igmp] [enable|disable] **Example:** IPMC>proxy igmp en (Enable) IPMC>proxy igmp dis (Disable)
Port Related **Configuration** (Router Port, Fast Leave, Throttling)	**Syntax:** IPMC Router [mld|igmp] [<port_list>] [enable|disable] IPMC Fastleave [mld|igmp] [<port_list>] [enable|disable] IPMC Throttling [mld|igmp] [<port_list>] [limit_group_number] **Example:** IPMC>router igmp 25-26 en (Port 25-26 are router ports) IPMC>Fast igmp 1-24 en (Enable IGMP Fast Leave on P1-24) IPMC>thro igmp 1-2 5 (Throtting of Port 1, 2 is 5 groups.)
VLAN Configuration	**Syntax:** IPMC State [mld|igmp] [<vid>] [enable|disable]

	IPMC Querier [mld|igmp] [<vid>] [enable|disable] IPMC Compatibility [mld|igmp] [<vid>] [auto|v1|v2|v3] IPMC Parameter RV [mld|igmp] [<vid>] [ipmc_param_rv] IPMC Parameter QI [mld|igmp] [<vid>] [ipmc_param_qi] IPMC Parameter QRI [mld|igmp] [<vid>] [ipmc_param_qri] IPMC Parameter LLQI [mld|igmp] [<vid>] [ipmc_param_llqi] IPMC Parameter URI [mld|igmp] [<vid>] [ipmc_param_uri] **Example:** IPMC>state igmp 2 en (Enable IGMP Snooping on VLAN 2) IPMC>quer igmp 2 en (Enable IGMP Querier on VLAN 2) IPMC>compa igmp 2 v2 (Enable IGMPv2 on VLAN 2)
MLD Snooping	
MLD Snooping	Note: The MLD Snooping is applied to IPv6 Multicast. The commands are the same as above IGMP Snooping (IPv4) Commands. Just chooses mld instead of igmp when seeing [mld|igmp] in the syntax. The IP Address should be IPv6 format for sure.

4.24. CLI Management - sFlow

Feature	Command Line
sFlow Configuration	
Receiver Configuration	**Syntax:** sFlow Receiver [release] [<timeout>] [<ip_addr_host>] [<udp_port>] [<datagram_size>] **Example:** sFlow>receiver 10 192.168.2.100 6343 1400 **Result:** Receiver Configuration: ======================= Owner : <none> Receiver : 192.168.2.100 UDP Port : 6343 Max. Datagram: 1400 bytes Time left : 0 seconds
Receiver Release	sFlow>receiver
Port Configuration	**Syntax:** sFlow Receiver [release] [<timeout>] [<ip_addr_host>] [<udp_port>] [<datagram_size>] sFlow FlowSampler [<port_list>] [<sampling_rate>] [<max_hdr_size>] sFlow CounterPoller [<port_list>] [<interval>] sFlow Statistics Receiver [clear] sFlow Statistics Samplers [<port_list>] [clear] **Example:** sFlow>flow 1-2 10 128 (Enable FlowSample on port 1-2, rate=10, max. size=128) sFlow>coun 1-2 5 (Enable CounterPoller of port 1-2, and set interval to 5)

```
sFlow>statistic sample 1-2


Per-Port Statistics:

====================

Port    Rx Flow Samples    Tx Flow Samples    Counter Samples

----    --------------     --------------     --------------

  1              0                 0                  0

  2              0                 0                  0
```

4.25. CLI Management - VCL

Feature	Command Line
MAC-based VLAN Configuration	
MAC-based VLAN Configuration	**Syntax:** VCL Macvlan Add <mac_addr> <vid> [<port_list>] **Example:** VCL/Macvlan>add 001122334455 10 1-4 **Result:** VCL/Macvlan>conf MAC Address VID Ports ---------------- ---- ----- 00-0b-16-21-2c-37 10 1-4
Protocol-based VLAN Configuration	
Protocol to Group	**Syntax:** VCL ProtoVlan Protocol Add Eth2 <ether_type>|arp|ip|ipx|at <group_id> **Example:** VCL/ProtoVlan>protocol add Eth2 0x0808 E4
Group to VLAN	**Syntax:** VCL ProtoVlan Vlan Add [<port_list>] <group_id> <vid> **Example:** VCL/ProtoVlan>vlan add 1-8 E4 10
Protocol VLAN Configuration	**Result:** VCL/ProtoVlan>conf Protocol Type Protocol (Value) Group ID ------------- ----------------------- -------- EthernetII ETYPE:0x808 E4 LLC_Other DSAP:0xff; SSAP:0xff L3 LLC_SNAP OUI-00:e0:2b; PID:0x1 S2 EthernetII ETYPE:0x800 E1

	Group ID VID Ports --------------- ---- ----- E4 10 1-8 E1 10 5-8
IP Subnet-based VLAN Configuration	
IP Subnet-based VLAN Configuration	**Syntax:** VCL IPVlan Add [<vce_id>] <ip_addr_mask> <vid> [<port_list>] **Parameters:** <vce_id> : Unique VCE ID for each VCL entry <ip_addr_mask>: Source IP address and mask (Format: a.b.c.d/n). <vid> : VLAN ID (1-4095) <port_list> : Port list or 'all', default: All ports **Example:** VCL/IPVlan>add 1 192.168.10.0/24 10 1-10 **Result:** VCE ID IP Address Mask Length VID Ports ------ --------------- ----------- ---- ----- 1 192.168.10.0 24 10 1-10

Appendix A: Product Safety

This appendix describes safety issues regarding to this product. To use this product safely, it is highly recommended to read this appendix before installing and using this product.

Failure to follow these precautions and warnings might cause product malfunction, electrical shock, or even fire. If this product is working abnormally (e.g. generating smoke), please stop using this product and contact your distributor or retailer immediately.

DO NOT install this product under conditions listed below:

- DO NOT install this product in an environment with conditions exceeding its specified operating environment.
- DO NOT install this product in an environment that is subjected to direct sunlight or near any heating equipment.
- DO NOT install this product in an environment with extreme temperature changes. Extreme temperature changes, even within the product's operating temperature range, may cause malfunctions.
- DO NOT install this product in a location near any sources of water or liquid.
- DO NOT stack this product with other network devices directly on top of one another. Stacking network devices directly without applying a mounting rack will cause this product to overheat.
- DO NOT install this product on an unstable surface. Doing so might cause this product to fall, resulting malfunction.

Product Maintenance Guide:

- DO NOT disassemble this product. Doing so might cause malfunction and void your product's warranty.
- It is recommended to keep your product clear of dust. To remove dust from your product, please use a dry brush and brush it off gently.
- When not using this product, please store it in an environment with low humidity, cool temperature, and free of dust. Failure to do so might cause malfunction.
- Before powering up this product, please make sure that the electric power source meets this product's requirement. DO NOT use other power adapters if this product comes with its own power adapter in the package.

Appendix B: IP Configuration for Your PC

This appendix describes how to set the IP address of your PC so you can connect to product configuration webpage. The configuration webpage allows you to set system variables or monitor system status.

The following section will guide you to set the IP address properly in a Microsoft Windows 8 environment. Setting IP address in other Microsoft operating system (such as Windows Vista or Windows 7) is quite the same and can be related.

1. Open **Network and Sharing Center** in **Control Panel**, and click on **Change adapter settings** as shown in the figure down below.
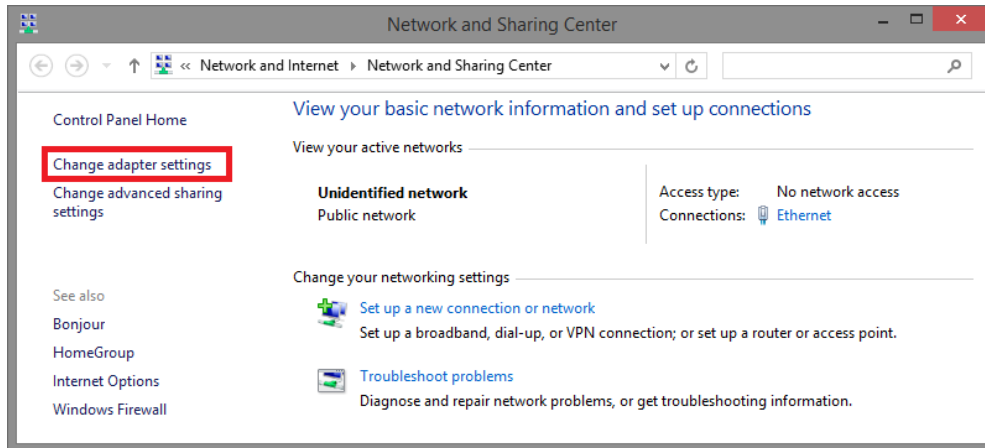
2. A **Network Connections** window will pop up, **showing** all the network connections available on your PC. Please double-click on the network connection you are using to connect the

3. An **Ethernet Status** window will pop up. Please click on the **Properties** button as shown in the figure down below.
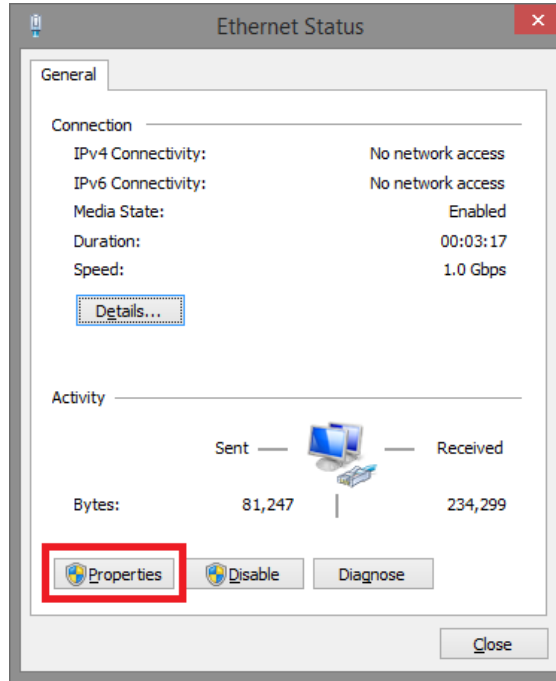
4. An **Ethernet Properties** window will pop up. Please double click on the **Internet Protocol Version 4 (TCP/IPv4)**.
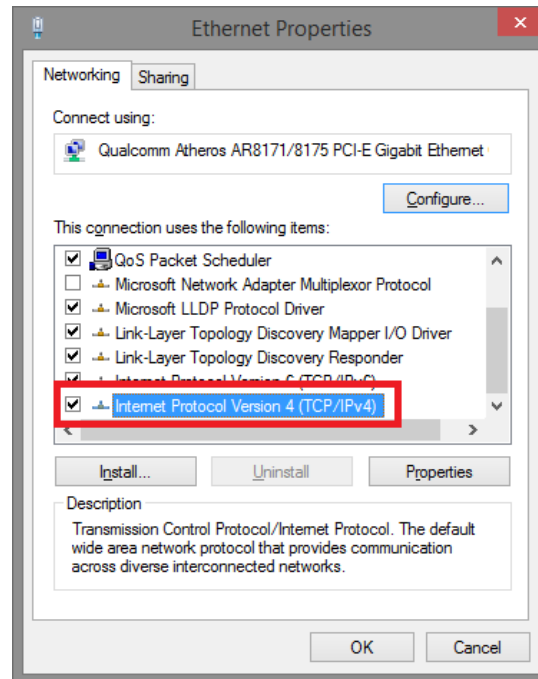
5.   An **Internet Protocol Version 4 (TCP/IPv4) Properties** window will pop up. Please set your PC's IP address and subnet mask as shown in the figure down below.

By default, your product's IP address should be **192.168.2.1**.You can set any IP address as long as it's not the same with your product's IP address and is in the same network segment with your product's IP address.

Press **OK** to apply the TCP/IPv4 settings you just made. Now you can connect to your product using a web browser (i.e. Internet Explorer, Chrome, or Firefox).

Appendix B:
IP Configuration for Your PC
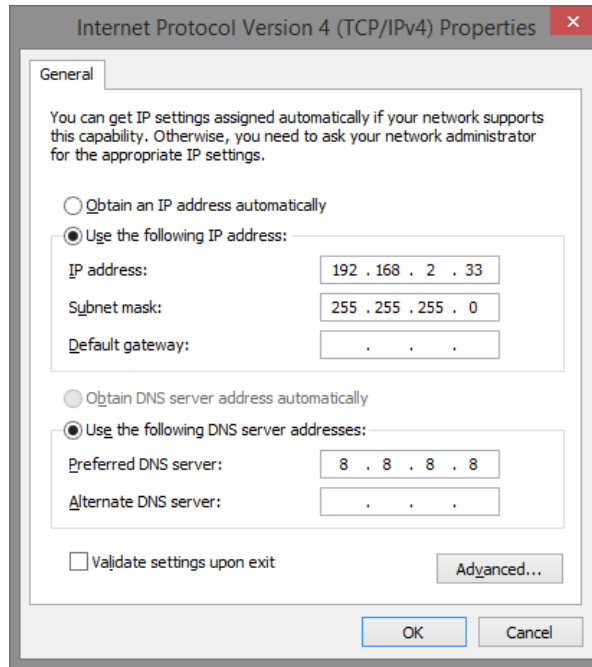
Appendix C: Glossary

This appendix contains the terms and glossaries that are used in this user manual.

A

ACE

ACE is an acronym for **A**ccess **C**ontrol **E**ntry. It describes access permission associated with a particular ACE ID.

There are three ACE frame types (Ethernet Type, ARP, and IPv4) and two ACE actions (permit and deny). The ACE also contains many detailed, different parameter options that are available for individual application.

ACL

ACL is an acronym for **A**ccess **C**ontrol **L**ist. It is the list table of ACEs, containing access control entries that specify individual users or groups permitted or denied to specific traffic objects, such as a process or a program.

Each accessible traffic object contains an identifier to its ACL. The privileges determine whether there are specific traffic object access rights.

ACL implementations can be quite complex, for example, when the ACEs are prioritized for the various situation. In networking, the ACL refers to a list of service ports or network services that are available on a host or server, each with a list of hosts or servers permitted or denied to use the service. ACL can generally be configured to control inbound traffic, and in this context, they are similar to firewalls.

There are 3 web-pages associated with the manual ACL configuration:

ACL|Access Control List: The web page shows the ACEs in a prioritized way, highest (top) to lowest (bottom). Default the table is empty. An ingress frame will only get a hit on one ACE even though there are more matching ACEs. The first matching ACE will take action (permit/deny) on that frame and a counter associated with that ACE is incremented. An ACE can be associated with a Policy, 1 ingress port, or any ingress port (the whole switch). If an ACE Policy is created then that Policy can be associated with a group of ports under the "Ports" web-page. There are number of parameters that can be configured with an ACE. Read the Web page help text to get further information for each of them. The maximum number of ACEs is 64.

ACL|Ports: The ACL Ports configuration is used to assign a Policy ID to an ingress port. This is useful to group ports to obey the same traffic rules. Traffic Policy is created under the "Access Control List" - page. You can you also set up specific traffic properties (Action / Rate Limiter / Port copy, etc) for each ingress port. They will though only apply if the frame gets past the ACE matching without getting matched. In that case a counter associated with that port is incremented. See the Web page help text for each specific port property.

ACL|Rate Limiters: Under this page you can configure the rate limiters. There can be 15 different rate limiters, each ranging from 1-1024K packets per seconds. Under "Ports" and "Access Control List" web-pages you can assign a Rate Limiter ID to the ACE(s) or ingress port(s).

Aggregation

Using multiple ports in parallel to increase the link speed beyond the limits of a port and to increase the redundancy for higher availability.

ARP

ARP is an acronym for **A**ddress **R**esolution **P**rotocol. It is a protocol that used to convert an IP address into a physical address, such as an Ethernet address. ARP allows a host to communicate with other hosts when only the Internet address of its neighbors is known. Before using IP, the host sends a broadcast ARP request containing the Internet address of the desired destination system.

ARP Inspection

ARP Inspection is a secure feature. Several types of attacks can be launched against a host or devices connected to Layer 2 networks by "poisoning" the ARP caches. This feature is used to block such attacks. Only valid ARP requests and responses can go through the switch device.

Auto-Negotiation

Auto-negotiation is the process where two different devices establish the mode of operation and the speed settings that can be shared by those devices for a link.

C

CDP

CDP is an acronym for **C**isco **D**iscovery **P**rotocol.

D

DEI

DEI is an acronym for **D**rop **E**ligible **I**ndicator. It is a 1-bit field in the VLAN tag.

DES

DES is an acronym for **D**ata **E**ncryption **S**tandard. It provides a complete description of a mathematical algorithm for encrypting (enciphering) and decrypting (deciphering) binary coded information.

Encrypting data converts it to an unintelligible form called cipher. Decrypting cipher converts the data back to its original form called plaintext. The algorithm described in this standard specifies both enciphering and deciphering operations which are based on a binary number called a key.

DHCP

DHCP is an acronym for **D**ynamic **H**ost **C**onfiguration **P**rotocol. It is a protocol used for assigning dynamic IP addresses to devices on a network.

DHCP used by networked computers (clients) to obtain IP addresses and other parameters such as the default gateway, subnet mask, and IP addresses of DNS servers from a DHCP server.

The DHCP server ensures that all IP addresses are unique, for example, no IP address is assigned to a second client while the first client's assignment is valid (its lease has not expired). Therefore, IP address pool management is done by the server and not by a human network administrator.

Dynamic addressing simplifies network administration because the software keeps track of IP addresses rather than requiring an administrator to manage the task. This means that a new computer can be added to a network without the hassle of manually assigning it a unique IP address.

DHCP Relay

DHCP Relay is used to forward and to transfer DHCP messages between the clients and the server when they are not on the same subnet domain.

The DHCP option 82 enables a DHCP relay agent to insert specific information into a DHCP request packets when forwarding client DHCP packets to a DHCP server and remove the specific information from a DHCP reply packets when forwarding server DHCP packets to a DHCP client. The DHCP server can use this information to implement IP address or other assignment policies. Specifically the option works by setting two sub-options: Circuit ID (option 1) and Remote ID (option2). The Circuit ID sub-option is supposed to include information specific to which circuit the request came in on. The Remote ID sub-option was designed to carry information relating to the remote host end of the circuit.

The definition of Circuit ID in the switch is 4 bytes in length and the format is "vlan_id" "module_id" "port_no". The parameter of "vlan_id" is the first two bytes represent the VLAN ID. The parameter of "module_id" is the third byte for the module ID (in standalone switch it always equal 0, in stackable switch it means switch ID). The parameter of "port_no" is the fourth byte and it means the port number.

The Remote ID is 6 bytes in length, and the value is equal the DHCP relay agents MAC address.

DHCP Snooping

DHCP Snooping is used to block intruder on the untrusted ports of the switch device when it tries to intervene by injecting a bogus DHCP reply packet to a legitimate conversation between the DHCP client and server.

DNS

DNS is an acronym for **D**omain **N**ame **S**ystem. It stores and associates many types of information with domain names. Most importantly, DNS translates human-friendly domain names and computer hostnames into computer-friendly IP addresses. For example, the domain name www.example.com might translate to 192.168.0.1.

Dotted Decimal Notation

Dotted Decimal Notation refers to a method of writing IP addresses using decimal numbers and dots as separators between octets.

An IPv4 dotted decimal address has the form x.y.z.w, where x, y, z, and w are decimal numbers between 0 and 255.

Drop Precedence Level

Every incoming frame is classified to a Drop Precedence Level (DP level), which is used throughout the device for providing congestion control guarantees to the frame according to what was configured for that specific DP level. A DP level of 0 (zero) corresponds to 'Committed' (Green) frames and a DP level of 1 or higher corresponds to 'Discard Eligible' (Yellow) frames.

DSCP

DSCP is an acronym for **D**ifferentiated **S**ervices **C**ode **P**oint. It is a field in the header of IP packets for packet classification purposes.

E

EEE

EEE is an abbreviation for Energy Efficient Ethernet defined in IEEE 802.3az.

EPS

EPS is an abbreviation for Ethernet Protection Switching defined in ITU/T G.8031.

Ethernet Type

Ethernet Type, or EtherType, is a field in the Ethernet MAC header, defined by the Ethernet networking standard. It is used to indicate which protocol is being transported in an Ethernet frame.

F

Fast Leave

Multicast snooping Fast Leave processing allows the switch to remove an interface from the forwarding-table entry without first sending out group specific queries to the interface. The VLAN interface is pruned from the multicast tree for the multicast group specified in the original leave message. Fast-leave processing ensures optimal bandwidth management for all hosts on a switched network, even when multiple multicast groups are in use simultaneously. This processing applies to IGMP and MLD.

H

HTTP

HTTP is an acronym for **H**ypertext **T**ransfer **P**rotocol. It is a protocol that used to transfer or convey information on the World Wide Web (WWW).

HTTP defines how messages are formatted and transmitted, and what actions Web servers and browsers should take in response to various commands. For example, when you enter a URL in your browser, this actually sends an HTTP command to the Web server directing it to fetch and transmit the requested Web page. The other main standard that controls how the World Wide Web works is HTML, which covers how Web pages are formatted and displayed.

Any Web server machine contains, in addition to the Web page files it can serve, an HTTP daemon, a program that is designed to wait for HTTP requests and handle them when they arrive. The Web browser is an HTTP client, sending requests to server machines. An HTTP client initiates a request by establishing a Transmission Control Protocol (TCP) connection to a particular port on a remote host (port 80 by default). An HTTP server listening on that port waits for the client to send a request message.

HTTPS

HTTPS is an acronym for **H**ypertext **T**ransfer **P**rotocol over **S**ecure Socket Layer. It is used to indicate a secure HTTP connection.

HTTPS provide authentication and encrypted communication and is widely used on the World Wide Web for security-sensitive communication such as payment transactions and corporate logons.

HTTPS is really just the use of Netscape's Secure Socket Layer (SSL) as a sublayer under its regular HTTP application layering. (HTTPS uses port 443 instead of HTTP port 80 in its interactions with the lower layer, TCP/IP.) SSL uses a 40-bit key size for the RC4 stream encryption algorithm, which is considered an adequate degree of encryption for commercial exchange.

I

ICMP

ICMP is an acronym for **I**nternet **C**ontrol **M**essage **P**rotocol. It is a protocol that generated the error response, diagnostic or routing purposes. ICMP messages generally contain information about routing difficulties or simple exchanges such as time-stamp or echo transactions. For example, the PING command uses ICMP to test an Internet connection.

IEEE 802.1X

IEEE 802.1X is an IEEE standard for port-based Network Access Control. It provides authentication to devices attached to a LAN port, establishing a point-to-point connection or preventing access from that port if authentication fails. With 802.1X, access to all switch ports can be centrally controlled from a server, which means that authorized users can use the same credentials for authentication from any point within the network.

IGMP

IGMP is an acronym for **I**nternet **G**roup **M**anagement **P**rotocol. It is a communications protocol used to manage the membership of Internet Protocol multicast groups. IGMP is used by IP hosts and adjacent multicast routers to establish multicast group memberships. It is an integral part of the IP multicast specification, like ICMP for unicast connections. IGMP can be used for online video and gaming, and allows more efficient use of resources when supporting these uses.

IGMP Querier

A router sends IGMP Query messages onto a particular link. This router is called the Querier.

IMAP

IMAP is an acronym for **I**nternet **M**essage **A**ccess **P**rotocol. It is a protocol for email clients to retrieve email messages from a mail server.

IMAP is the protocol that IMAP clients use to communicate with the servers, and SMTP is the protocol used to transport mail to an IMAP server.

The current version of the Internet Message Access Protocol is IMAP4. It is similar to Post Office Protocol version 3 (POP3), but offers additional and more complex features. For example, the IMAP4 protocol leaves your email messages on the server rather than downloading them to your computer. If you wish to remove your messages from the server, you must use your mail client to generate local folders, copy messages to your local hard drive, and then delete and expunge the messages from the server.

IP

IP is an acronym for **I**nternet **P**rotocol. It is a protocol used for communicating data across an internet network.

IP is a "best effort" system, which means that no packet of information sent over is assured to reach its destination in the same condition it was sent. Each device connected to a Local Area Network (LAN) or Wide Area Network (WAN) is given an Internet Protocol address, and this IP address is used to identify the device uniquely among all other devices connected to the extended network.

The current version of the Internet protocol is IPv4, which has 32-bits Internet Protocol addresses allowing for in excess of four billion unique addresses. This number is reduced drastically by the practice of webmasters taking addresses in large blocks, the bulk of which remain unused. There is a rather substantial movement to adopt a new version of the Internet Protocol, IPv6, which would have 128-bits Internet Protocol addresses. This number can be represented roughly by a three with thirty-nine zeroes after it. However, IPv4 is still the protocol of choice for most of the Internet.

IPMC

IPMC is an acronym for **IP M**ulti**C**ast.

IPMC supports IPv4 and IPv6 multicasting. IPMCv4 denotes multicast for IPv4. IPMCv6 denotes multicast for IPv6.

IP Source Guard

IP Source Guard is a secure feature used to restrict IP traffic on DHCP snooping untrusted ports by filtering traffic based on the DHCP Snooping Table or manually configured IP Source Bindings. It helps prevent IP spoofing attacks when a host tries to spoof and use the IP address of another host.

L

LACP

LACP is an IEEE 802.3ad standard protocol. The **L**ink **A**ggregation **C**ontrol **P**rotocol, allows bundling several physical ports together to form a single logical port.

LLC

The IEEE 802.2 **L**ogical **L**ink **C**ontrol (LLC) protocol provides a link mechanism for upper layer protocols. It is the upper sub-layer of the Data Link Layer and provides multiplexing mechanisms that make it possible for several network protocols (IP, IPX) to coexist within a multipoint network. LLC header consists of 1 byte DSAP (Destination Service Access Point), 1 byte SSAP (Source Service Access Point), 1 or 2 bytes Control field followed by LLC information.

LLDP

LLDP is an IEEE 802.1ab standard protocol.

The **L**ink **L**ayer **D**iscovery **P**rotocol (LLDP) specified in this standard allows stations attached to an IEEE 802 LAN to advertise, to other stations attached to the same IEEE 802 LAN, the major capabilities provided by the system incorporating that station, the management address or addresses of the entity or entities that provide management of those capabilities, and the identification of the stations point of attachment to the IEEE 802 LAN required by those management entity or entities. The information distributed via this protocol is stored by its recipients in a standard Management Information Base (MIB), making it possible for the information to be accessed by a Network Management System (NMS) using a management protocol such as the Simple Network Management Protocol (SNMP).

LLDP-MED

LLDP-MED is an extension of IEEE 802.1ab and is defined by the telecommunication industry association (TIA-1057).

LLQI

LLQI (Last Listener Query Interval) is the maximum response time used to calculate the Maximum Response Code inserted into Specific Queries. It is used to detect the departure of the last listener for a multicast address or source. In IGMP, this term is called LMQI (Last Member Query Interval).

LOC

LOC is an acronym for <u>L</u>oss <u>O</u>f <u>C</u>onnectivity and is detected by a MEP and is indicating lost connectivity in the network. Can be used as a switch criteria by EPS

M

MAC Table

Switching of frames is based upon the DMAC address contained in the frame. The switch builds up a table that maps MAC addresses to switch ports for knowing which ports the frames should go to (based upon the DMAC address in the frame). This table contains both static and dynamic entries. The static entries are configured by the network administrator if the administrator wants to do a fixed mapping between the DMAC address and switch ports.

The frames also contain a MAC address (SMAC address), which shows the MAC address of the equipment sending the frame. The SMAC address is used by the switch to automatically update the MAC table with these dynamic MAC addresses. Dynamic entries are removed from the MAC table if no frame with the corresponding SMAC address has been seen after a configurable age time.

Mirroring

For debugging network problems or monitoring network traffic, the switch system can be configured to mirror frames from multiple ports to a mirror port. (In this context, mirroring a frame is the same as copying the frame.)

Both incoming (source) and outgoing (destination) frames can be mirrored to the mirror port.

MLD

MLD is an acronym for <u>M</u>ulticast <u>L</u>istener <u>D</u>iscovery for IPv6. MLD is used by IPv6 routers to discover multicast listeners on a directly attached link, much as IGMP is used in IPv4. The protocol is embedded in ICMPv6 instead of using a separate protocol.

MSTP

In 2002, the IEEE introduced an evolution of RSTP: the <u>M</u>ultiple <u>S</u>panning <u>T</u>ree <u>P</u>rotocol. The MSTP protocol provides for multiple spanning tree instances, while ensuring RSTP and STP compatibility. The standard was originally defined by IEEE 802.1s, but was later incorporated in IEEE 802.1D-2005.

MVR

Multicast VLAN Registration (MVR) is a protocol for Layer 2 (IP)-networks that enables multicast-traffic from a source VLAN to be shared with subscriber-VLANs.

The main reason for using MVR is to save bandwidth by preventing duplicate multicast streams being sent in the core network, instead the stream(s) are received on the MVR-VLAN and forwarded to the VLANs where hosts have requested it/them (Wikipedia).

N

NTP

NTP is an acronym for **N**etwork **T**ime **P**rotocol, a network protocol for synchronizing the clocks of computer systems. NTP uses UDP (datagrams) as transport layer.

O

Optional TLVs.

A LLDP frame contains multiple TLVs

For some TLVs it is configurable if the switch shall include the TLV in the LLDP frame. These TLVs are known as optional TLVs. If an optional TLVs is disabled the corresponding information is not included in the LLDP frame.

OUI

OUI is the organizationally unique identifier. An OUI address is a globally unique identifier assigned to a vendor by IEEE. You can determine which vendor a device belongs to according to the OUI address which forms the first 24 bits of a MAC address.

P

PCP

PCP is an acronym for **P**riority **C**ode **P**oint. It is a 3-bit field storing the priority level for the 802.1Q frame. It is also known as User Priority.

PD

PD is an acronym for **P**owered **D**evice. In a PoE system the power is delivered from a PSE (power sourcing equipment) to a remote device. The remote device is called a PD.

PHY

PHY is an abbreviation for Physical Interface Transceiver and is the device that implement the Ethernet physical layer (IEEE-802.3).

PING

Ping is a program that sends a series of packets over a network or the Internet to a specific computer in order to generate a response from that computer. The other computer responds with an acknowledgment that it received the packets. Ping was created to verify whether a specific computer on a network or the Internet exists and is connected.

Ping uses Internet Control Message Protocol (ICMP) packets. The PING Request is the packet from the origin computer, and the PING Reply is the packet response from the target.

PoE

PoE is an acronym for **P**ower **O**ver **E**thernet.

Power Over Ethernet is used to transmit electrical power, to remote devices over standard Ethernet cable. It could for example be used for powering IP telephones, wireless LAN access points and other equipment, where it would be difficult or expensive to connect the equipment to main power supply.

Policer

A policer can limit the bandwidth of received frames. It is located in front of the ingress queue.

Private VLAN

In a private VLAN, PVLANs provide layer 2 isolation between ports within the same broadcast domain. Isolated ports configured as part of PVLAN cannot communicate with each other. Member ports of a PVLAN can communicate with each other.

PTP

PTP is an acronym for **P**recision **T**ime **P**rotocol, a network protocol for synchronizing the clocks of computer systems.

Q

QCE

QCE is an acronym for **Q**oS **C**ontrol **E**ntry. It describes QoS class associated with a particular QCE ID.

There are six QCE frame types: Ethernet Type, VLAN, UDP/TCP Port, DSCP, TOS, and Tag Priority. Frames can be classified by one of 4 different QoS classes: "Low", "Normal", "Medium", and "High" for individual application.

QCL

QCL is an acronym for **Q**oS **C**ontrol **L**ist. It is the list table of QCEs, containing QoS control entries that classify to a specific QoS class on specific traffic objects.

Each accessible traffic object contains an identifier to its QCL. The privileges determine specific traffic object to specific QoS class.

QL

QL In SyncE this is the Quality Level of a given clock source. This is received on a port in a SSM indicating the quality of the clock received in the port.

QoS

QoS is an acronym for **Q**uality **o**f **S**ervice. It is a method to guarantee a bandwidth relationship between individual applications or protocols.

A communications network transports a multitude of applications and data, including high-quality video and delay-sensitive data such as real-time voice. Networks must provide secure, predictable, measurable, and sometimes guaranteed services.

Achieving the required QoS becomes the secret to a successful end-to-end business solution. Therefore, QoS is the set of techniques to manage network resources.

QoS class

Every incoming frame is classified to a QoS class, which is used throughout the device for providing queuing, scheduling and congestion control guarantees to the frame according to what was configured for that specific QoS class. There is a one to one mapping between QoS class, queue and priority. A QoS class of 0 (zero) has the lowest priority.

R

RARP

RARP is an acronym for **R**everse **A**ddress **R**esolution **P**rotocol. It is a protocol that is used to obtain an IP address for a given hardware address, such as an Ethernet address. RARP is the complement of ARP.

RADIUS

RADIUS is an acronym for **R**emote **A**uthentication **D**ial **I**n **U**ser **S**ervice. It is a networking protocol that provides centralized access, authorization and accounting management for people or computers to connect and use a network service.

RSTP

In 1998, the IEEE with document 802.1w introduced an evolution of STP:

the **R**apid **S**panning **T**ree **P**rotocol, which provides for faster spanning tree convergence after a topology change. Standard IEEE 802.1D-2004 now incorporates RSTP and obsoletes STP, while at the same time being backwards-compatible with STP.

S

sFlow

sFlow is an industry standard technology for monitoring switched networks through random sampling of packets on switch ports and time-based sampling of port counters. The sampled packets and counters (referred to as flow samples and counter samples, respectively) are sent as sFlow UDP datagrams to a central network traffic monitoring server. This central server is called an sFlow receiver or sFlow collector.

Shaper

A shaper can limit the bandwidth of transmitted frames. It is located after the ingress queues.

SMTP

SMTP is an acronym for **S**imple **M**ail **T**ransfer **P**rotocol. It is a text-based protocol that uses the Transmission Control Protocol (TCP) and provides a mail service modeled on the FTP file transfer service. SMTP transfers mail messages between systems and notifications regarding incoming mail.

SNAP

The **S**ub **N**etwork **A**ccess **P**rotocol (SNAP) is a mechanism for multiplexing, on networks using IEEE 802.2 LLC, more protocols than can be distinguished by the 8-bit 802.2 Service Access Point (SAP) fields. SNAP supports identifying protocols by Ethernet type field values; it also supports vendor-private protocol identifier.

SNMP

SNMP is an acronym for **S**imple **N**etwork **M**anagement **P**rotocol. It is part of the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol for network management. SNMP allow diverse network objects to participate in a network management architecture. It enables network management systems to learn network problems by receiving traps or change notices from network devices implementing SNMP.

SNTP

SNTP is an acronym for **S**imple **N**etwork **T**ime **P**rotocol, a network protocol for synchronizing the clocks of computer systems. SNTP uses UDP (datagrams) as transport layer.

SSH

SSH is an acronym for **S**ecure **SH**ell. It is a network protocol that allows data to be exchanged using a secure channel between two networked devices. The encryption used by SSH provides confidentiality and integrity of data over an insecure network. The goal of SSH was to replace the earlier rlogin, TELNET and rsh protocols, which did not provide strong authentication or guarantee confidentiality.

SSM

SSM In SyncE this is an abbreviation for Synchronization Status Message and is containing a QL indication.

STP

Spanning **T**ree **P**rotocol is an OSI layer-2 protocol which ensures a loop free topology for any bridged LAN. The original STP protocol is now obsolete by RSTP.

SyncE

SyncE Is an abbreviation for Synchronous Ethernet. This functionality is used to make a network 'clock frequency' synchronized. Not to be confused with real time clock synchronized (IEEE 1588).

T

TACACS+

TACACS+ is an acronym for **T**erminal **A**cess **C**ontroller **A**ccess **C**ontrol **S**ystem **P**lus. It is a networking protocol which provides access control for routers, network access servers and other networked computing devices via one or more centralized servers. TACACS+ provides separate authentication, authorization and accounting services.

Tag Priority

Tag Priority is a 3-bit field storing the priority level for the 802.1Q frame.

TCP

TCP is an acronym for **T**ransmission **C**ontrol **P**rotocol. It is a communications protocol that uses the Internet Protocol (IP) to exchange the messages between computers.

The TCP protocol guarantees reliable and in-order delivery of data from sender to receiver and distinguishes data for multiple connections by concurrent applications (for example, Web server and e-mail server) running on the same host.

The applications on networked hosts can use TCP to create connections to one another. It is known as a connection-oriented protocol, which means that a connection is established and maintained until such time as the message or messages to be exchanged by the application programs at each end have been exchanged. TCP is responsible for ensuring that a message is divided into the packets

that IP manages and for reassembling the packets back into the complete message at the other end.

Common network applications that use TCP include the World Wide Web (WWW), e-mail, and File Transfer Protocol (FTP).

TELNET

TELNET is an acronym for **TEL**etype **NET**work. It is a terminal emulation protocol that uses the Transmission Control Protocol (TCP) and provides a virtual connection between TELNET server and TELNET client.

TELNET enables the client to control the server and communicate with other servers on the network. To start a Telnet session, the client user must log in to a server by entering a valid username and password. Then, the client user can enter commands through the Telnet program just as if they were entering commands directly on the server console.

TFTP

TFTP is an acronym for **T**rivial **F**ile **T**ransfer **P**rotocol. It is transfer protocol that uses the User Datagram Protocol (UDP) and provides file writing and reading, but it does not provide directory service and security features.

ToS

ToS is an acronym for **T**ype **o**f **S**ervice. It is implemented as the IPv4 ToS priority control. It is fully decoded to determine the priority from the 6-bit ToS field in the IP header. The most significant 6 bits of the ToS field are fully decoded into 64 possibilities, and the singular code that results is compared against the corresponding bit in the IPv4 ToS priority control bit (0~63).

TLV

TLV is an acronym for **T**ype **L**ength **V**alue. A LLDP frame can contain multiple pieces of information. Each of these pieces of information is known as TLV.

U

UDP

UDP is an acronym for **U**ser **D**atagram **P**rotocol. It is a communications protocol that uses the Internet Protocol (IP) to exchange the messages between computers.

UDP is an alternative to the Transmission Control Protocol (TCP) that uses the Internet Protocol (IP). Unlike TCP, UDP does not provide the service of dividing a message into packet datagrams, and UDP doesn't provide reassembling and sequencing of the packets. This means that the application program that uses UDP must be able to make sure that the entire message has arrived and is in the right order. Network applications that want to save processing time because they have very small

data units to exchange may prefer UDP to TCP.

UDP provides two services not provided by the IP layer. It provides port numbers to help distinguish different user requests and, optionally, a checksum capability to verify that the data arrived intact.

Common network applications that use UDP include the Domain Name System (DNS), streaming media applications such as IPTV, Voice over IP (VoIP), and Trivial File Transfer Protocol (TFTP).

UPnP

UPnP is an acronym for **U**niversal **P**lug and **P**lay. The goals of UPnP are to allow devices to connect seamlessly and to simplify the implementation of networks in the home (data sharing, communications, and entertainment) and in corporate environments for simplified installation of computer components

User Priority

User Priority is a 3-bit field storing the priority level for the 802.1Q frame. It is also known as PCP.

V

VLAN

Virtual LAN. A method to restrict communication between switch ports. VLANs can be used for the following applications:

VLAN unaware switching: This is the default configuration. All ports are VLAN unaware with Port VLAN ID 1 and members of VLAN 1. This means that MAC addresses are learned in VLAN 1, and the switch does not remove or insert VLAN tags.

VLAN aware switching: This is based on the IEEE 802.1Q standard. All ports are VLAN aware. Ports connected to VLAN aware switches are members of multiple VLANs and transmit tagged frames. Other ports are members of one VLAN, set up with this Port VLAN ID, and transmit untagged frames.

Provider switching: This is also known as Q-in-Q switching. Ports connected to subscribers are VLAN unaware, members of one VLAN, and set up with this unique Port VLAN ID. Ports connected to the service provider are VLAN aware, members of multiple VLANs, and set up to tag all frames. Untagged frames received on a subscriber port are forwarded to the provider port with a single VLAN tag. Tagged frames received on a subscriber port are forwarded to the provider port with a double VLAN tag.

VLAN ID

VLAN ID is a 12-bit field specifying the VLAN to which the frame belongs.

Voice VLAN

Appendix C:
Glossary

Voice VLAN is VLAN configured specially for voice traffic. By adding the ports with voice devices attached to voice VLAN, we can perform QoS-related configuration for voice data, ensuring the transmission priority of voice traffic and voice quality.