



SW-0216G4

User' s Manual

Table of Contents

INTRODUCTION	1
CHAPTER 1 OPERATION OF WEB-BASED MANAGEMENT	2
CONNECTING NETWORK DEVICES	5
TWISTED-PAIR DEVICES	5
CHAPTER 2 SYSTEM	7
2-1 SYSTEM INFORMATION	7
2-1.1 Information	7
2-1.2 Configuration	10
2-2 TIME	11
2-2.1 Manual	11
2-2.2 NTP	13
2-3 ACCOUNT	14
2-3.1 Users	14
2-3.2 Privilege Level	16
2-4 IP	18
2-4.1 IPV4	18
2-5 SYSLOG	20
2-5.1 Configuration	20
2-5.2 Log	21
2-5.3 Detailed Log	22
2-6 SNMP	23
2-6.1 Configuration	23
2-6.2 Tarp	25
CHAPTER 3. CONFIGURATION	27
3-1 PORT	27
3-1.1 Configuration	27
3-1.2 Port Description	29
3-1.3 Traffic Overview	30
3-1.4 Detailed Statistics	31
3-1.5 Qos Statistics	33
3-1.6 SFP Information	34
3-1.7 EEE	36
3-2 AGGREGATION	38
3-2.1 Static Trunk	38
3-2.1.1 Static Trunk	38
3-2.2 LACP	40
3-2.2.1 Configuration	40
3-2.2.2 System Status	42
3-2.2.3 Port Status	43
3-2.2.4 Port Statistics	45
3-3 SPANNING TREE	46
3-3.1 Bridge Settings	46
3-3.2 MSTI Mapping	49
3-3.3 MSTI Priorities	51
3-3.4 CIST Ports	52
3-3.5 MSTI Ports	54
3-3.6 Bridge Status	56
3-3.7 Port Status	57
3-3.8 Port Statistics	58
3-4 IGMP SNOOPING	59
3-4.1 Basic Configuration	59
3-4.2 VLAN Configuration	62
3-4.3 Port Group Filtering	64
3-4.4 Status	66
3-4.5 Group Information	68
3-4.6 IPv4 SSM information	69
3-5 MVR	71
3-5.1 Configuration	71
3-5.2 Port Group Allow	73

3-5.3 Groups Information.....	74
3-5.4 Statistics	75
3-5.5 EEE.....	76
3-5.6 Port Statistics	78
3-6 VLAN	80
3-6.1 VLAN Membership	80
3-6.2 Ports.....	82
3-6.3 Switch Status.....	85
3-6.4 Port Status.....	87
3-6.5 Private VLANs	89
3-6.5.1 Private VLANs Membership.....	89
3-6.5.2 Port Isolation.....	90
3-6.6 MAC-based VLAN.....	91
3-6.6.1 Configuration	91
3-6.6.2 Status.....	93
3-6.7 Protocol -based VLAN	94
3-6.7.1 Protocol to Group.....	94
3-6.7.2 Group to VLAN	96
3-6.8 IEEE 802.1QinQ (double-tag) configuration.....	98
3-7 QoS.....	101
3-7.1 Port Classification.....	101
3-7.2 Port Scheduler.....	103
3-7.3 Port Shaping.....	106
3-7.4 QoS Control List Configuration.....	109
3-7.5 QCL Status	113
3-8 LOOP PROTECTION	115
3-8.1 Configuration.....	115
3-8.2 Status.....	117
3-9 MIRRORING	118
3-10 TRAP EVENT SEVERITY	120
CHAPTER 4. SECURITY	122
4-1 NAS	122
4-1.1 Configuration.....	122
4-1.2 Switch Status.....	126
4-1.3 Port Status.....	128
4-2 PORT SECURITY	131
4-2.1 Limit Control	131
4-2.2 Switch Status.....	134
4-2.3 Port Status.....	136
CHAPTER 5. MAINTENANCE	138
5-1 WARM START.....	138
5-2 FIRMWARE.....	139
5-2.1 Firmware Upgrade	139
5-2.2 Firmware Selection	140
5-3 SAVE / RESTORE	142
5-3.1 Factory Defaults.....	142
5-3.2 Save Start	143
5-3.3 Save User.....	144
5-3.4 Restore User.....	145
5-4 EXPORT / IMPORT.....	146
5-4.1 Export Config	146
5-4.2 Import Config	147
5-5 DIAGNOSTICS	148
5-5.1 Ping.....	148



NOTE: Emphasizes important information or calls your attention to related features or instructions.



WARNING: Alerts you to a potential hazard that could cause personal injury.



CAUTION: Alerts you to a potential hazard that could cause loss of data, or damage the system or equipment.

Overview

In this User Manual, it will not only tell you how to install and connect your network system but configure and monitor the SW-0216G4 through the web by (RJ-45) serial interface and Ethernet ports step-by-step. Many explanations in detail of hardware and software functions are shown as well as the examples of the operation for web-based interface.

The SW-0216G4, the next generation web smart switch, from Manufacture Corporation, provides a reliable infrastructure for your business network. This switch delivers more intelligent features you need to improve the availability of your critical business applications, protects your sensitive information, and optimize your network bandwidth to deliver information and applications more effectively. It provides the ideal combination of affordability and capabilities for entry level networking of small business or enterprise which demands IP Phone, IP Camera or Wireless applications, thus helps you create a more efficient, better-connected workforce.

SW-0216G4 Web smart Switches provide 18 ports in a single device; the specification is highlighted as follows.

- Web Smart features provide better manageability, security, QoS, and performance
- 802.3az Energy Efficient Ethernet standard
- Dual speed SFPs for FE or GbE fiber uplink
- s-Flow supports
- Easy-Port-Configuration for ease of setup in the IP Phone, IP Camera or Wireless environment

Overview of User Manual

- Chapter 1 "Operation of Web-based Management"
- Chapter 2 "System Information"
- Chapter 3 "Configuration"
- Chapter 4 "Security"
- Chapter 5 "Maintenance"

Initial Configuration

This chapter instructs you how to configure and manage the SW-0216G4 through the web user interface. With this facility, you can easily access and monitor through any one port of the switch all the status of the switch, including MIBs status, each port activity, Spanning tree status, port aggregation status, multicast traffic, VLAN and priority status, even illegal access record and so on.

The default values of the SW-0216G4 are listed in the table below:

IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.254
Username	admin
Password	

After the SW-0216G4 has been finished configuration the it interface, you can browse it. For instance, type <http://192.168.1.1> in the address row in a browser, it will show the following screen and ask you inputting username and password in order to login and access authentication.

The default username is **"admin"** and password is **empty**. For the first time to use, please enter the default username and password, and then click the **<Login>** button. The login process now is completed. In this login menu, you have to input the complete username and password respectively, the SW-0216G4 will not give you a shortcut to username automatically. This looks inconvenient, but safer.

In the SW-0216G4, it supports a simple user management function allowing only one administrator to configure the system at the same time. If there are two or more users using administrator's identity, it will allow the only one who logs in first to configure the system. The rest of users, even with administrator's identity, can only monitor the system. For those who have no administrator's identity, can only monitor the system. There are only a maximum of three users able to login simultaneously in the SW-0216G4.



NOTE:

When you login the Switch WEB to manager. You must first type the Username of the admin. Password was blank, so when you type after the end Username, please press enter. Management page to enter WEB.

When you login SW-0216G4 series switch Web UI management, you can use both ipv4 login to manage

To optimize the display effect, we recommend you use Microsoft IE 6.0 above, Netscape V7.1 above or FireFox V1.00 above and have the resolution 1024x768. The switch supported neutral web browser interface.



NOTE:

AS SW-0216G4 the function enable dhcp, so If you do not have DHCP server to provide ip addresses to the switch, the Switch **default ip 192.168.1.1**

Figure 1 The login page



NOTE: If you need to configuration the function or parameter then you can refer the detail in the User Manual. Or you could access to the Switch and click the "help" under the web GUI and the switch will pop-up the simple help content to teach you how to set the parameters.

SW-0216G4 web help function:

SW-0216G4

Auto-Logout 10 min Logout **Help**

System Configuration

Model Name	SW-0216G4
System Description	16-Port 10/100/1000BASE-T + 2-Port TP/ (100M/1G)SFP Web Smart Switch
Location	
Contact	
Device Name	SW-0216G4
System Date	2011-01-01 00:01:27
System Uptime	0d 00:01:27
BIOS Version	v1.00
Firmware Version	v2.46 2013-12-25
Hardware-Mechanical Version	v1.01-v1.01
Serial Number	980A00297AR
Host IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Gateway IP Address	192.168.1.254
Host MAC Address	00-22-cf-ed-52-ab
Console Baudrate	115200
RAM Size	64MB
Flash Size	16MB
Bridge FDB Size	8192 MAC Addresses
Transmit Queue	8 queues per port
Maximum Frame Size	9600

System Information Help - Windows Internet Ex...

http://192.168.20.22/help/help_sys.htm

System Information Help

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.

Chip ID

The Chip ID of this switch.

System Date

The current (GMT) system time and date. The system time

CONNECTING NETWORK DEVICES

The switch is designed to be connected to 10, 100 or 1000Mbps network cards in PCs and servers, as well as to other switches and hubs. It may also be connected to remote devices using optional SFP transceivers.

TWISTED-PAIR DEVICES

Each device requires an unshielded twisted-pair (UTP) cable with RJ-45 connectors at both ends. Use Category 5, 5e or 6 cable for 1000BASE-T connections, Category 5 or better for 100BASE-TX connections.

CABLING GUIDELINES

The RJ-45 ports on the switch support automatic MDI/MDI-X pinout configuration, so you can use standard straight-through twisted-pair cables to connect to any other network device (PCs, servers, switches, routers, or hubs).

See Appendix B for further information on cabling.

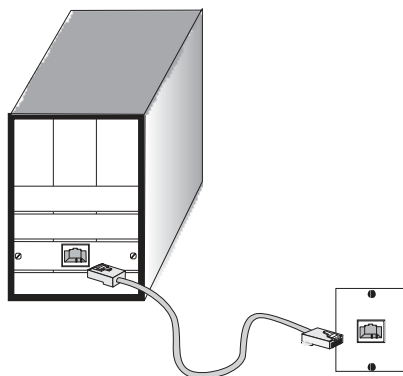


CAUTION: Do not plug a phone jack connector into an RJ-45 port. This will damage the switch. Use only twisted-pair cables with RJ-45 connectors that conform to FCC standards.

CONNECTING TO PCS, SERVERS, HUBS AND SWITCHES

Step1. Attach one end of a twisted-pair cable segment to the device's RJ-45 connector.

Figure 1: Making Twisted-Pair Connections



Step2. If the device is a network card and the switch is in the wiring closet, attach the other end of the cable segment to a modular wall outlet that is connected to the wiring closet. (See the section “Network Wiring Connections.”) Otherwise, attach the other end to an available port on the switch.

Make sure each twisted pair cable does not exceed 100 meters (328 ft) in length.



NOTE: Avoid using flow control on a port connected to a hub unless it is actually required to solve a problem. Otherwise back pressure jamming signals may degrade overall performance for the segment attached to the hub.

Step3. As each connection is made, the Link LED (on the switch) corresponding to each port will light green (1000 Mbps) or amber (100 Mbps) to indicate that the connection is valid.

NETWORK WIRING CONNECTIONS

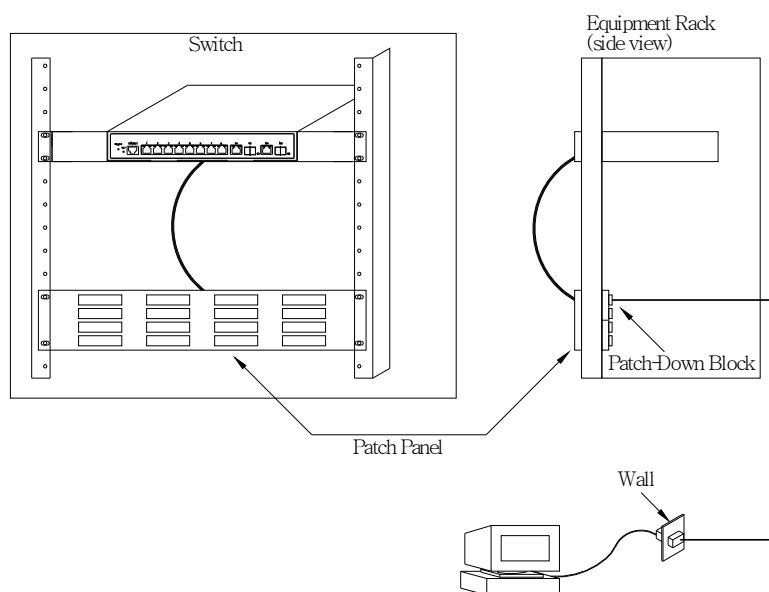
Today, the punch-down block is an integral part of many of the newer equipment racks. It is actually part of the patch panel. Instructions for making connections in the wiring closet with this type of equipment follows.

Step1. Attach one end of a patch cable to an available port on the switch, and the other end to the patch panel.

Step2. If not already in place, attach one end of a cable segment to the back of the patch panel where the punch-down block is located, and the other end to a modular wall outlet.

Step3. Label the cables to simplify future troubleshooting. See “Cable Labeling and Connection Records” on page 29

Figure 2: Network Wiring Connections



This chapter describes all of the basic configuration tasks which includes the System Information and any manage of the Switch (e.g. Time, Account, IP, Syslog and SNMP.)

2-1 System Information

After you login, the switch shows you the system information. This page is default and tells you the basic information of the system, including “Model Name”, “System Description”, “Contact”, “Device Name”, “System Up Time”, “BIOS Version”, “Firmware Version”, “Hardware-Mechanical Version”, “Serial Number”, “Host IP Address”, “Host Mac Address”, “Device Port”, “RAM Size”, “Flash Size” and. With this information, you will know the software version used, MAC address, serial number, how many ports good and so on. This is helpful while malfunctioning.

2-1.1 Information

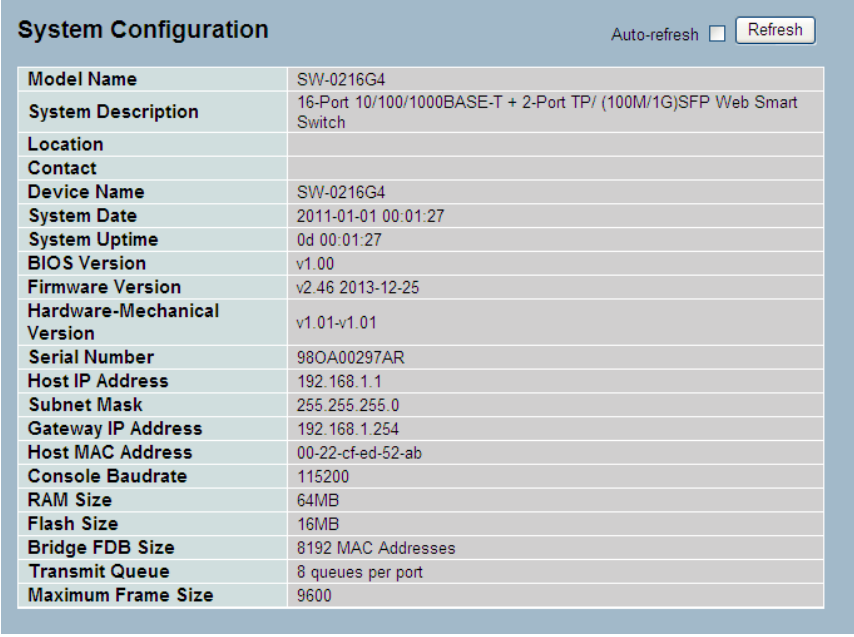
The switch system information is provided here.

Web interface

To configure System Information in the web interface:

1. Click SYSTEM, System, and Information.
2. Specify the contact information for the system administrator as well as the name and location of the switch. Also indicate the local time zone by configuring the appropriate offset.
3. Click Refresh

Figure 2-1.1: System Information



The screenshot shows a web interface titled "System Configuration" with an "Auto-refresh" checkbox and a "Refresh" button. Below the title is a table of system information.

Model Name	SW-0216G4
System Description	16-Port 10/100/1000BASE-T + 2-Port TP/ (100M/1G)SFP Web Smart Switch
Location	
Contact	
Device Name	SW-0216G4
System Date	2011-01-01 00:01:27
System Uptime	0d 00:01:27
BIOS Version	v1.00
Firmware Version	v2.46 2013-12-25
Hardware-Mechanical Version	v1.01-v1.01
Serial Number	980A00297AR
Host IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Gateway IP Address	192.168.1.254
Host MAC Address	00-22-cf-ed-52-ab
Console Baudrate	115200
RAM Size	64MB
Flash Size	16MB
Bridge FDB Size	8192 MAC Addresses
Transmit Queue	8 queues per port
Maximum Frame Size	9600

Parameter description:

- **Model name:**
The model name of this device.
- **System description:**
As it is, this tells what this device is. Here, it is “**20-Port 10/100/1000Base-T + 4 TP/(100/1G) SFP Combo + 2 (100/1G) SFP Web Smart Switch**”.
- **Location:**
Basically, it is the location where this switch is put. User-defined.
- **Contact:**
For easily managing and maintaining device, you may write down the contact person and phone here for getting help soon. You can configure this parameter through the device’s user interface or SNMP.
- **Device name:**
The name of the switch. User-defined.
- **System Date:**
Display the current system time and date. The field format is YYYY-MM-DD HH:MM:SS
- **System up time:**
The time accumulated since this switch is powered up. Its format is day, hour, minute, second.
- **BIOS version:**
The version of the BIOS in this switch.
- **Firmware version:**
The firmware version in this switch.
- **Hardware-Mechanical version:**
The version of Hardware and Mechanical. The figure before the hyphen is the version of electronic hardware; the one after the hyphen is the version of mechanical.
- **Serial number:**
The serial number is assigned by the Manufacture Corporation.
- **Host IP address:**
The IP address of the switch.
- **Subnet Mask:**
Displays the IP subnet mask assigned to the device.
- **Gateway IP Address:**
Displays the default gateway IP address assigned to the device.
- **Host MAC address:**
It is the Ethernet MAC address of the management agent in this switch.
- **Console Baudrate:**
Displays the baudrate of RS232(COM) port.
- **RAM size:**
The size of the RAM in this switch.
- **Flash size:**
The size of the flash memory in this switch.
- **Bridge FDB size :**
Displays the bridge forwarding database size of the device.

- **Transmit Queue :**
Displays the information about the transmit priority queue of switch.
- **Maximum Frame size :**
Displays the information about switch supported maximum frame size.

2-1.2 Configuration

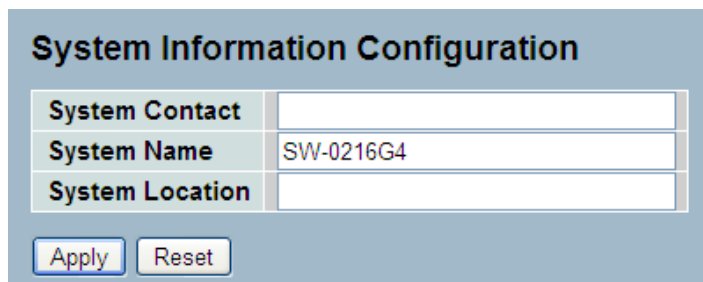
You can identify the system by configuring the contact information, name, and location of the switch.

Web interface

To configure System Information in the web interface:

1. Click System, System Information, Configuration.
2. Write System Contact , System Name, System Location information in this page.
3. Click Apply

Figure 2-1.2: System Information configuration



System Information Configuration	
System Contact	<input type="text"/>
System Name	<input type="text" value="SW-0216G4"/>
System Location	<input type="text"/>
<input type="button" value="Apply"/> <input type="button" value="Reset"/>	

Parameter description:

- **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 :**
An administratively assigned name for this managed node. By convention, this is the node's fully-qualified domain name. A domain name is a text string drawn from the alphabet (A-Za-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.

2-2 Time

This page configure the switch Time. Time configure is including Time Configuration and NTP Configuration

2-2.1 Manual

The switch provides manual and automatic ways to set the system time via NTP. Manual setting is simple and you just input "Year", "Month", "Day", "Hour", "Minute" and "Second" within the valid value range indicated in each item.

Web Interface

To configure Time in the web interface:

1. Click Time , Manual.
2. Specify the Time parameter in manual parameters.
3. Click Apply

Figure 2-2.1: The time configuration

Time Configuration	
Clock Source:	<input checked="" type="radio"/> Use Local Settings <input type="radio"/> Use NTP Server
Local Time:	2011-01-01 00:10:20 YYYY-MM-DD HH:MM:SS
Time Zone Offset:	0 min
Daylight Savings	<input type="checkbox"/> Enable
Time Set Offset:	60 min. (Range: 1 - 1440, Default: 60)
Daylight Savings Type:	<input checked="" type="radio"/> By dates <input type="radio"/> Recurring
From:	YYYY-MM-DD HH:MM
To:	YYYY-MM-DD HH:MM
From:	Day: Sun Week: First Month: Jan Time: 00:00 HH:MM
To:	Day: Sun Week: First Month: Jan Time: 00:00 HH:MM
Save Reset	

Parameter description:

- **Clock Source:**

There are two modes for configuring where the Clock Source is from. You can choose one of them to make time setting.

 1. Use Local Settings: In this mode Clock Source is from Local Time. Set the time manually.
 2. Use NTP Server: In this mode Clock Source is from NTP Server. The switch can link to Network Time Protocol server to obtain the correct time automatically when NTP server has been set.
- **Local Time:**

Show the current time of the system.
- **Time Zone Offset:**

Provide the timezone offset relative to UTC/GMT. The offset is given in minutes east of GMT. The valid range is from -720 to 720 minutes

- **Daylight Saving:**

Daylight saving is adopted in some countries. If set, it will adjust the time lag or in advance in unit of hours, according to the starting date and the ending date. For example, if you set the day light saving to be 1 hour. When the time passes over the starting time, the system time will be increased one hour after one minute at the time since it passed over. And when the time passes over the ending time, the system time will be decreased one hour after one minute at the time since it passed over.

The switch supports valid configurable day light saving time is $-5 \sim +5$ step one hour. The zero for this parameter means it need not have to adjust current time, equivalent to in-act daylight saving. You don't have to set the starting/ending date as well. If you set daylight saving to be non-zero, you have to set the starting/ending date as well; otherwise, the daylight saving function will not be activated.

- **Time Set Offset:**

Provide the Daylight saving time set offset. The offset is given in minutes east of GMT. The valid range is from 1 to 1440 minutes. default is 60 mins

- **Daylight Savings Type:**

Provide the Daylight savings type selection. You can select "By Dates" or "Recurring" two type for Daylight saving type.

- **From:**

To configure when Daylight saving start date and time, the format is "YYYY-MM-DD HH:MM".

- **To:**

To configure when Daylight saving end date and time, the format is "YYYY-MM-DD HH:MM".



NOTE: The under "from" and "to" was displayed what you set on the "From" and "To" field information.

2-2.2 NTP

NTP is Network Time Protocol and is used to sync the network time based Greenwich Mean Time (GMT). If use the NTP mode and select a built-in NTP time server or manually specify an user-defined NTP server as well as Time Zone, the switch will sync the time in a short after pressing <Apply> button. Though it synchronizes the time automatically, NTP does not update the time periodically without user's processing.

Time Zone is an offset time off GMT. You have to select the time zone first and then perform time sync via NTP because the switch will combine this time zone offset and updated NTP time to come out the local time, otherwise, you will not able to get the correct time. The switch supports configurable time zone from -12 to +13 step 1 hour.

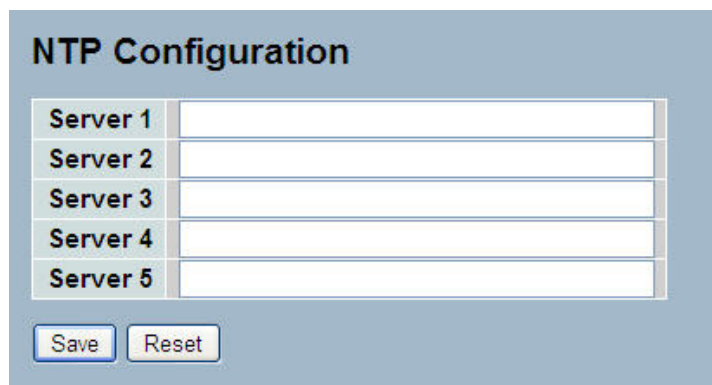
Default Time zone: +8 Hrs.

Web Interface

To configure Time in the web interface:

1. Click SYSTEM, NTP.
2. Specify the Time parameter in manual parameters.
3. Click Apply

Figure 2-2.2: The NTP configuration



NTP Configuration	
Server 1	<input type="text"/>
Server 2	<input type="text"/>
Server 3	<input type="text"/>
Server 4	<input type="text"/>
Server 5	<input type="text"/>

Parameter description:

- **Server 1 to 5 :**
Provide the NTP IPv4 address of this switch. For example, '192.1.2.34'.
- **Buttons**
These buttons are displayed on the NTP page:
Save – Click to save changes.
Reset - Click to undo any changes made locally and revert to previously saved values.

2-3 Account

In this function, only administrator can create, modify or delete the username and password. Administrator can modify other guest identities' password without confirming the password but it is necessary to modify the administrator-equivalent identity. Guest-equivalent identity can modify his password only. Please note that you must confirm administrator/guest identity in the field of Authorization in advance before configuring the username and password. Only one administrator is allowed to exist and unable to be deleted. In addition, up to 4 guest accounts can be created.

2-3.1 Users

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

Web Interface

To configure Account in the web interface:

1. Click SYSTEM, Account, Users.
2. Click Add new user
3. Specify the User Name parameter.
4. Click Apply

Figure2-3.1: The Users Account configuration

The screenshot shows two parts of the web interface. The top part, titled 'Users Configuration', contains a table with two columns: 'User Name' and 'Privilege Level'. The table has one row with 'admin' in the 'User Name' column and '15' in the 'Privilege Level' column. Below the table is a button labeled 'Add new user', which is highlighted with a red box and a red arrow pointing down to the 'Add User' form below. The 'Add User' form has a title 'Add User' and a section titled 'User Settings'. It contains four input fields: 'User Name', 'Password', 'Password (again)', and 'Privilege Level'. The 'Privilege Level' field is a dropdown menu currently set to '1'. At the bottom of the form are three buttons: 'Save', 'Reset', and 'Cancel'.

Parameter description:

- **User Name :**

The name identifying the user. This is also a link to [Add/Edit User](#).

A string identifying the user name that this entry should belong to. The allowed string length is 1 to 32. The valid user name is a combination of letters, numbers and underscores.

- **Password**

To type the password. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 32 to 126.

- **Password (again)**

To type the password again. You must type the same password again in the field.

- **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.



NOTE: You can add more user name up to 19 set in Users configuration. You can configure 20 set of user name totally including admin account.

2-3.2 Privilege Level

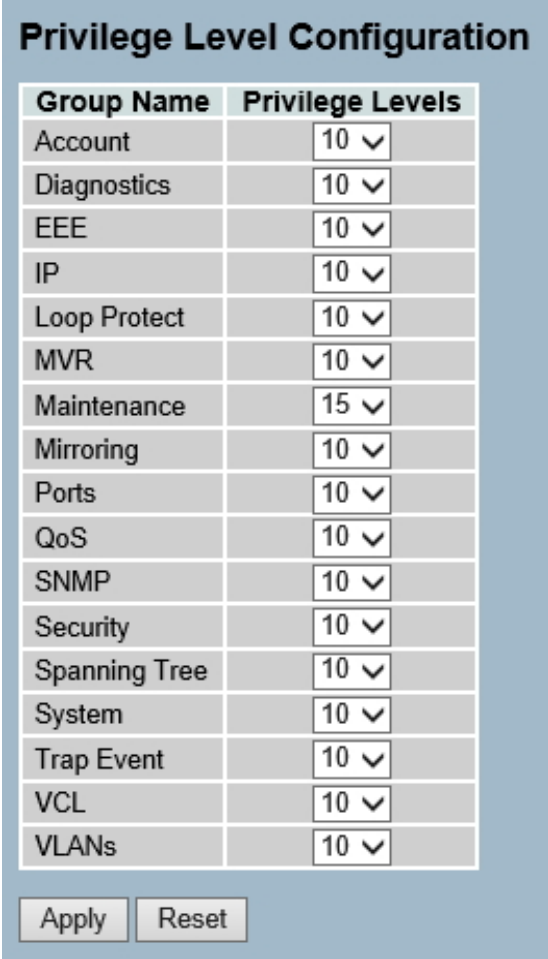
This page provides an overview of the privilege levels. The switch provides user set Account, Aggregation, Diagnostics, EEE, GARP, GVRP, IP, IPMC Snooping LACP LLDP LLDP MED MAC Table MRP MVR MVRP Maintenance Mirroring POE Ports Private VLANs QoS SMTP SNMP Security Spanning Tree System Trap Event VCL VLANs Voice VLAN Privilege Levels form 1 to 15 .

Web Interface

To configure Privilege Level in the web interface:

1. Click SYSTEM, Account, Privilege Level.
2. Specify the Privilege parameter.
3. Click Apply

Figure2- 3.2: The Privilege Level configuration



The screenshot shows a web interface titled "Privilege Level Configuration". It contains a table with two columns: "Group Name" and "Privilege Levels". The table lists 18 groups, each with a dropdown menu for selecting a privilege level. Below the table are two buttons: "Apply" and "Reset".

Group Name	Privilege Levels
Account	10
Diagnostics	10
EEE	10
IP	10
Loop Protect	10
MVR	10
Maintenance	15
Mirroring	10
Ports	10
QoS	10
SNMP	10
Security	10
Spanning Tree	10
System	10
Trap Event	10
VCL	10
VLANs	10

Parameter description:

- **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, Log.

Security: Authentication, Port (contains Dot1x port, MAC based and the MAC Address Limit)

IP: Everything except 'ping'.

Port: Everything except 'VeriPHY'.

Diagnostics: 'ping' and 'VeriPHY'.

Maintenance: System Reboot, System Restore Default, System Password, Configuration Save, Configuration Load and Firmware Load. Web- Users, Privilege Levels and everything in Maintenance.

- **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.

2-4 IP

IP is an acronym for Internet Protocol. 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.

2-4.1 IPV4

The IPv4 address for the switch could be obtained via DHCP Server for VLAN 1. To manually configure an address, you need to change the switch's default settings to values that are compatible with your network. You may also need to establish a default gateway between the switch and management stations that exist on another network segment.

Configure the switch-managed IP information on this page

The Configured column is used to view or change the IP configuration.

The Current column is used to show the active IP configuration.

Web Interface

To configure an IP address in the web interface:

1. Click System, IP Configuration.
2. Specify the IPv4 settings, and enable DNS proxy service if required.
3. Click Apply

Figure2- 4.1: The IP configuration

IP Configuration

	Configured	Current
DHCP Client	<input type="checkbox"/>	<input type="button" value="Renew"/>
IP Address	<input type="text" value="192.168.5.129"/>	192.168.5.129
IP Mask	<input type="text" value="255.255.255.0"/>	255.255.255.0
IP Gateway	<input type="text" value="0.0.0.0"/>	0.0.0.0
VLAN ID	<input type="text" value="1"/>	1
DNS Server	<input type="text" value="0.0.0.0"/>	0.0.0.0

IP DNS Proxy Configuration

DNS Proxy

Parameter description:

- **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 fails and the configured IP address is non-zero, DHCP will stop and the configured IP settings will be used. The DHCP client will announce the configured System Name as hostname to provide 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.

- **SNTP Server :**

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

- **DNS Server :**

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

- **VLAN ID :**

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

- **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.

2-5 Syslog

The Syslog is a standard for logging program messages . It allows separation of the software that generates messages from the system that stores them and the software that reports and analyzes them. It can be used as well a generalized informational, analysis and debugging messages. It is supported by a wide variety of devices and receivers across multiple platforms.

2-5.1 Configuration

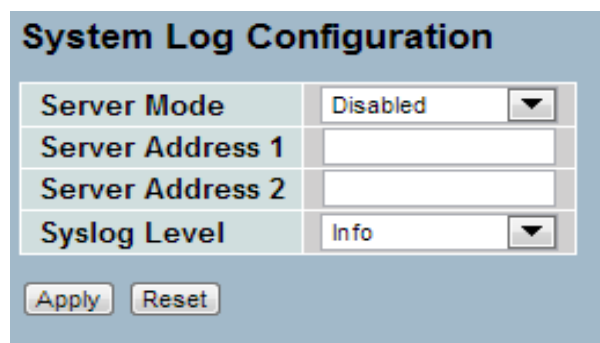
This section describes how to configure the system log and provide a wide variety of devices and receivers across multiple platforms.

Web Interface

To configure Syslog configuration in the web interface:

1. Click SYSTEM, Syslog.
2. Specify the syslog parameters includes IP Address of Syslog server and Port number.
3. Evoke the Sylog to enable it.
4. Click Save.

Figure2- 5.1: The System Log configuration



System Log Configuration	
Server Mode	Disabled
Server Address 1	
Server Address 2	
Syslog Level	Info
Apply Reset	

Parameter description:

- **Server Mode :**

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

Enabled: Enable server mode operation.

Disabled: Disable server mode operation.

- **Server Address 1 and 2 :**

Indicates the IPv4 host address of syslog server 1 and server 2 (For redundancy). If the switch provide DNS feature, it also can be a host name.

- **Syslog Level :**

Indicates what kind of message will send to syslog server. Possible modes are: Info: Send informations, warnings and errors. Warning: Send warnings and errors. Error: Send errors.

2-5.2 Log

This section describes that display the system log information of the switch

Web Interface

To display the log configuration in the web interface:

1. Click Syslog, Log.
2. Display the log information.

Figure2- 5.2: The System Log configuration

ID	Level	Time	Message
1	Info	-	Switch just made a cold boot.
2	Info	1970-01-01 00:00:05	Link up on port 1
3	Info	1970-01-01 00:26:08	Link down on port 1
4	Info	1970-01-01 00:55:53	Link up on port 1
5	Info	1970-01-01 01:47:14	Link down on port 1
6	Info	1970-01-01 01:48:36	Link up on port 1
7	Info	1970-01-01 02:20:04	Link down on port 1
8	Info	1970-01-01 18:55:49	Link up on port 1
9	Info	1970-01-01 19:58:11	Link down on port 1
10	Info	1970-01-01 19:58:45	Link up on port 1

Parameter description:

- **Auto-refresh**
To evoke the auto-refresh icon then the device will refresh the log automatically.
- **Level**
level of the system log entry. The following level types are supported:
Information level of the system log.
Warning: Warning level of the system log.
Error: Error level of the system log.All: All levels.
- **ID**
ID (≥ 1) of the system log entry.
- **Time**
It will display the log record by device time. The time of the system log entry.
- **Message**
It will display the log detail message. The message of the system log entry.
- **Upper right icon (Refresh, clear,....)**
You can click them for refresh the system log or clear them by manual, others for next/up page or entry.

2-5.3 Detailed Log

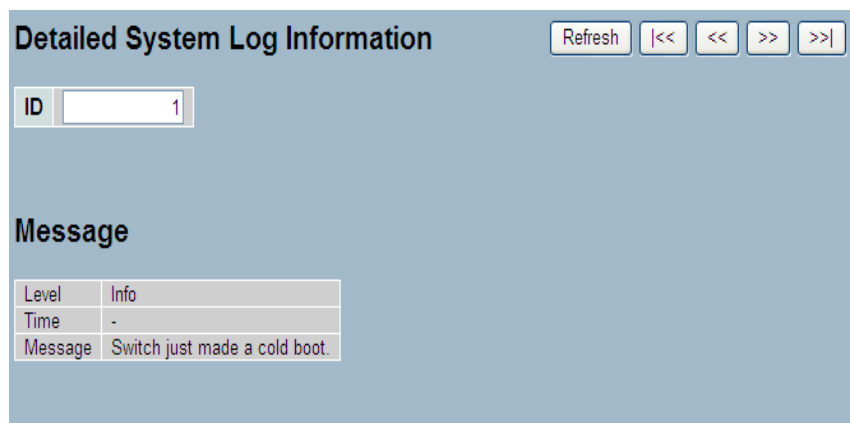
This section describes that display the detailed log information of the switch

Web Interface

To display the detailed log configuration in the web interface:

1. Click Syslog, Detailed Log.
2. Display the log information.

Figure2- 5.3: The Detailed System Log Information



Parameter description:

- **ID**
The ID (≥ 1) of the system log entry.
- **Message**
The detailed message of the system log entry.
- **Upper right icon (Refresh, clear,....)**
You can click them for refresh the system log or clear them by manual, others for next/up page or entry.

2-6 SNMP

Any Network Management System (NMS) running the Simple Network Management Protocol (SNMP) can manage the Managed devices equipped with SNMP agent, provided that the Management Information Base (MIB) is installed correctly on the managed devices. The SNMP is a protocol that is used to govern the transfer of information between SNMP manager and agent and traverses the Object Identity (OID) of the management Information Base (MIB), described in the form of SMI syntax. SNMP agent is running on the switch to response the request issued by SNMP manager.

Basically, it is passive except issuing the trap information. The switch supports a switch to turn on or off the SNMP agent. If you set the field SNMP “Enable”, SNMP agent will be started up. All supported MIB OIDs, including RMON MIB, can be accessed via SNMP manager. If the field SNMP is set “Disable”, SNMP agent will be de-activated, the related Community Name, Trap Host IP Address, Trap and all MIB counters will be ignored.

2-6.1 Configuration

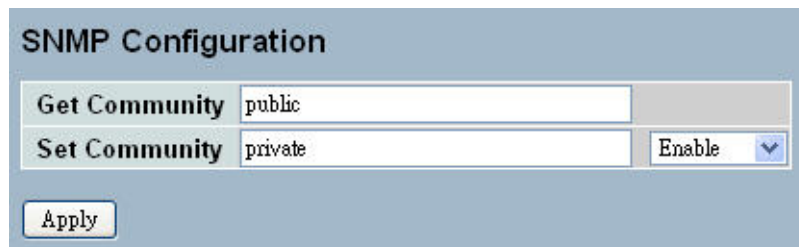
There are two communities by default. It is applicable to configure the Get Community and the Set Community for SNMPv1 and SNMPv2.

Web Interface

To configure SNMP Communities in the web interface:

1. Click SNMP, Configuration.
2. Specify the parameters of Get Community and Set Community.
3. Scroll to enable or disable the function of Set Community.
4. Click Apply.
5. If you want to modify or clear the setting then click Reset.

Figure2- 6.1: SNMP Configuration



SNMP Configuration	
Get Community	public
Set Community	private
	Enable
<input type="button" value="Apply"/>	

Parameter description:

- **Get 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.

- **Set 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.

- **Mode:**

Indicates the Set Community mode operation. Possible modes are:

Enabled: Enable Set Community.

Disabled: Disable Set Community.

2-6.2 Tarp

The function is used to configure SNMP trap. To create a new trap account, please check <No number> button, and enter the trap information then check <Apply>. Max Group Number : 6.

Web Interface

To configure SNMP Trap setting:

1. Click SNMP, Trap .
2. Display the SNMP Trap Hosts information table.
3. Choice a entry to display and modify the detail parameters or click delete button to delete the trap hosts entry.

Figure 2-6.8: The SNMP Trap Host Configuration

Delete	No	Version	Server IP	UDP Port	Community/Security Name	Severity Level	Security Level	Authentication Protocol	Privacy Protocol
	1								
	2								
	3								
	4								
	5								
	6								

Save

Trap Host Configuration

Trap Version	v2c
Server IP	0.0.0.0
UDP Port	162
Community	
Severity Level	Info

Apply Reset

Parameters description:

- **Delete:**
Check <Delete> entry then check <Save> button, the entry will be delete.
- **Trap Version:**
You may choose v1, v2c or v3 trap.
- **Server IP:**
To assign the SNMP Host IP address.
- **UDP Port:**
To assign Port number. Default: 162
- **Community / Security Name:**
The length of "Community / Security Name" string is restricted to 1-32.

- **Security Level:**

Indicates what kind of message will send to Security Level.
Possible modes are:
Info: Send informations, warnings and errors.
Warning: Send warnings and errors.
Error: Send errors.
- **Security Level:**

There are three kinds of choices.
NoAuth, NoPriv: No authentication and no privacy.
Auth, NoPriv: Authentication and no privacy.
Auth, Priv: Authentication and privacy.
- **Authentication Protocol:**

You can choose MD5 or SHA for authentication.
- **Authentication Password:**

The length of 'MD5 Authentication Password' is restricted to 8 – 32.
The length of 'SHA Authentication Password' is restricted to 8 – 40.
- **Privacy Protocol:**

You can set DES encryption for UserName.
- **Privacy Password:**

The length of ' Privacy Password ' is restricted to 8 – 32.

This chapter describes all of the basic network configuration tasks which includes the Ports, Layer 2 network protocol (e.g. VLANs, QoS and IGMP etc.) and any setting of the Switch.

3-1 Port

The section describes to configure the Port detail parameters of the switch. Others you could using the Port configure to enable or disable the Port of the switch. Monitor the ports content or status in the function.

3-1.1 Configuration

This chapter describes how to view the current port configuration and how to configure ports to non-default settings, including

Linkup/Linkdown

Speed (Current and configured)

Flow Control (Current Rx, Current Tx and Configured)

Maximum Frame Size

Excessive Collision Mode

Power Control.

Web Interface

To configure an Current Port Configuration in the web interface:

1. Click Configuration, Port, then Configuration
2. Specify the Speed Configured, Flow Control , Maximum Frame size , Excessive Collision mode and Power Control.
3. Click Save.

Figure 3-1.1: The Port Configuration

Port Configuration									
Port	Link	Current	Speed	Flow Control			Maximum Frame Size	Excessive Collision Mode	Power Control
			Configured	Current Rx	Current Tx	Configured			
*			<>					<>	<>
1	100fdx	Auto	Auto	×	×		9600	Discard	Disabled
2	Down	Auto	Auto	×	×		9600	Discard	Disabled
3	Down	Auto	Auto	×	×		9600	Discard	Disabled
4	Down	Auto	Auto	×	×		9600	Discard	Disabled
5	Down	Auto	Auto	×	×		9600	Discard	Disabled
6	Down	Auto	Auto	×	×		9600	Discard	Disabled
7	Down	Auto	Auto	×	×		9600	Discard	Disabled
8	Down	Auto	Auto	×	×		9600	Discard	Disabled
9	Down	Auto	Auto	×	×		9600	Discard	Disabled
10	Down	Auto	Auto	×	×		9600	Discard	Disabled
11	Down	Auto	Auto	×	×		9600	Discard	Disabled
12	Down	Auto	Auto	×	×		9600	Discard	Disabled
13	1Gfdx	Auto	Auto	×	×		9600	Discard	Disabled
14	Down	Auto	Auto	×	×		9600	Discard	Disabled
15	Down	Auto	Auto	×	×		9600	Discard	Disabled
16	Down	Auto	Auto	×	×		9600	Discard	Disabled
17	Down	Auto	Auto				9600		
18	Down	Auto	Auto				9600		

Apply Reset

Parameter description:

- **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 :**

Provides the current link speed of the port.
- **Configured Link Speed :**

Select any available link speed for the given switch port.
Auto Speed selects the highest speed that is compatible with a link partner.
Disabled disables the switch port operation.
- **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.
- **Upper right icon (Refresh)**

You can click them for refresh the Port link Status by manual

3-1.2 Port Description

The section describes to configure the Port's alias or any descriptions for the Port Identity. It provides user to write down an alphanumeric string describing the full name and version identification for the system's hardware type, software version, and networking application

Web Interface

To configure an Port Description in the web interface:

1. Click Configuration, Port, then Port Description
2. Specify the detail Port alias or description an alphanumeric string describing the full name and version identification for the system's hardware type, software version, and networking application.
3. Click Save.

Figure 3-1.2: The Port Configuration

Port	Description
1	
2	
3	
4	
5	
6	
7	
8	
9	
10	
11	
12	
13	
14	
15	
16	
17	
18	

Apply Reset

Parameter description:

- **Port :**
This is the logical port number for this row.
- **Description :**
Description of device ports can not include " # % & ' + \.
- **Buttons**
Apply – Click to save changes.
Reset- Click to undo any changes made locally and revert to previously saved values.

3-1.3 Traffic Overview

The section describes to the Port statistics information and provides overview of general traffic statistics for all switch ports.

Web Interface

To Display the Port Statistics Overview in the web interface:

1. Click Configuration, Port, then Traffic Overview
2. If you want to auto-refresh then you need to evoke the “Auto-refresh” .
3. Click “ Refresh“ to refresh the port statistics or clear all information when you click “ Clear”.

Figure 3-1.3: The Port Statistics Overview

Port Statistics Overview										
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	2265	560	432634	267133	0	0	0	0	1581	
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	

Parameter description:

- **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
- **Auto-refresh :**
To evoke the auto-refresh icon then the device will refresh the information automatically.
- **Upper right icon (Refresh, Clear):**
You can click them for refresh the Port Statistics information by manual. Others click Clear to clean up all Port Statistics.

3-1.4 Detailed Statistics

The section describes how to provide detailed traffic statistics for a specific switch port. Use the port select box to select which switch port details to display.

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

Web Interface

To Display the per Port Port detailed Statistics Overview in the web interface:

1. Click Configuration, Port, then Detailed Port Statistics
2. Scroll the Port Index to select which port you want to show the detailed Port statistic overview” .
3. If you want to auto-refresh the information then you need to evoke the “Auto-refresh”.
4. Click “ Refresh” to refresh the port detailed statistics or clear all information when you click “ Clear”.

Figure 3-1.4: The Port Detail Statistics Overview

Receive Total		Transmit Total	
Rx Packets	7637	Tx Packets	10688
Rx Octets	1518566	Tx Octets	3337459
Rx Unicast	7183	Tx Unicast	4974
Rx Multicast	29	Tx Multicast	5714
Rx Broadcast	425	Tx Broadcast	0
Rx Pause	0	Tx Pause	0
Receive Size Counters		Transmit Size Counters	
Rx 64 Bytes	4761	Tx 64 Bytes	72
Rx 65-127 Bytes	200	Tx 65-127 Bytes	5380
Rx 128-255 Bytes	86	Tx 128-255 Bytes	2866
Rx 256-511 Bytes	2588	Tx 256-511 Bytes	97
Rx 512-1023 Bytes	2	Tx 512-1023 Bytes	2139
Rx 1024-1526 Bytes	0	Tx 1024-1526 Bytes	134
Rx 1527- Bytes	0	Tx 1527- Bytes	0
Receive Queue Counters		Transmit Queue Counters	
Rx Q0	7637	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	10688

Parameter description:

- **Auto-refresh:**
To evoke the auto-refresh to refresh the Port Statistics information automatically.
- **Upper left scroll bar:**
To scroll which port to display the Port statistics with “Port-0”, “Port-1...”

Receive Total and Transmit Total

- **Rx and Tx Packets :**
The number of received and transmitted (good and bad) packets.
- **Rx and Tx Octets :**
The number of received and transmitted (good and bad) bytes. Includes FCS, but excludes framing bits.
- **Rx and Tx Unicast**
The number of received and transmitted (good and bad) unicast packets.

- **Rx and Tx Multicast :**

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

- **Rx and Tx Broadcast :**

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

- **Rx and Tx Pause :**

A count of the MAC Control frames received or transmitted on this port that have an opcode indicating a PAUSE operation.

Receive and Transmit Size Counters

The number of received and transmitted (good and bad) packets split into categories based on their respective frame sizes.

Receive and Transmit Queue Counters

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

Receive Error Counters

- **Rx Drops :**

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

- **Rx CRC/Alignment :**

The number of frames received with CRC or alignment errors.

- **Rx Undersize :**

The number of short 1 frames received with valid CRC.

- **Rx Oversize :**

The number of long 2 frames received with valid CRC.

- **Rx Fragments :**

The number of short 1 frames received with invalid CRC.

- **Rx Jabber :**

The number of long 2 frames received with invalid CRC.

- **Rx Filtered :**

The number of received frames filtered by the forwarding process.

Short frames are frames that are smaller than 64 bytes.

Long frames are frames that are longer than the configured maximum frame length for this port.

Transmit Error Counters

- **Tx Drops :**

The number of frames dropped due to output buffer congestion.

- **Tx Late/Exc. Coll. :**

The number of frames dropped due to excessive or late collisions.

- **Auto-refresh:**

To evoke the auto-refresh to refresh the Queuing Counters automatically.

- **Upper right icon (Refresh, clear)**

You can click them for refresh the Port Detail Statistics or clear them by manual.

3-1.5 Qos Statistics

The section describes that switch could display the QoS detailed Queuing counters for a specific switch port. for the different queues for all switch ports.

Web Interface

To Display the Queueing Counters in the web interface:

1. Click Configuration, Port, then QoS Statistics
2. If you want to auto-refresh the information then you need to evoke the "Auto-refresh".
3. Click " Refresh" to refresh the Queueing Counters or clear all information when you click " Clear".

Figure 3-1.5: The Queueing Counters Overview

Queueing Counters																
Port	Q0		Q1		Q2		Q3		Q4		Q5		Q6		Q7	
	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
5	2541	0	0	0	0	0	0	0	0	0	0	0	0	0	0	613
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

Parameter description:

- **Port :**
The logical port for the settings contained in the same row.
- **Qn :**
Qn is the Queue number, QoS queues per port. Q0 is the lowest priority queue.
- **Rx/Tx :**
The number of received and transmitted packets per queue.
- **Auto-refresh:**
To evoke the auto-refresh to refresh the Queueing Counters automatically.
- **Upper right icon (Refresh, clear)**
You can click them for refresh the Queueing Counters or clear them by manual.

3-1.6 SFP Information

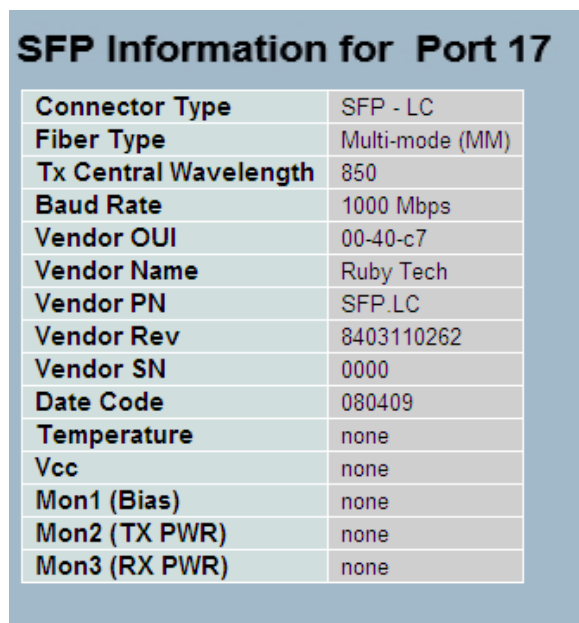
The section describes that switch could display the SFP module detail information which you connect it to the switch. The information includes: Connector type, Fiber type, wavelength, baud rate and Vendor OUI etc.

Web Interface

To Display the SFP information in the web interface:

1. Click Configuration, Port, then SFP Information
2. To display the SFP Information.

Figure 3-1.6: The SFP Information Overview



SFP Information for Port 17	
Connector Type	SFP - LC
Fiber Type	Multi-mode (MM)
Tx Central Wavelength	850
Baud Rate	1000 Mbps
Vendor OUI	00-40-c7
Vendor Name	Ruby Tech
Vendor PN	SFP.LC
Vendor Rev	8403110262
Vendor SN	0000
Date Code	080409
Temperature	none
Vcc	none
Mon1 (Bias)	none
Mon2 (TX PWR)	none
Mon3 (RX PWR)	none

Parameter description:

- **Connector Type:**
Display the connector type, for instance, UTP, SC, ST, LC and so on.
- **Fiber Type:**
Display the fiber mode, for instance, Multi-Mode, Single-Mode.
- **Tx Central Wavelength:**
Display the fiber optical transmitting central wavelength, for instance, 850nm, 1310nm, 1550nm and so on.
- **Baud Rate:**
Display the maximum baud rate of the fiber module supported, for instance, 10M, 100M, 1G and so on.
- **Vendor OUI :**
Display the manufacturer's OUI code which is assigned by IEEE.
- **Vendor Name:**
Display the company name of the module manufacturer.

- **Vendor P/N:**
Display the product name of the naming by module manufacturer.
- **Vendor Rev (Revision):**
Display the module revision.
- **Vendor SN (Serial Number):**
Show the serial number assigned by the manufacturer.
- **Date Code:**
Show the date this SFP module was made.
- **Temperature:**
Show the current temperature of SFP module.
- **Vcc:**
Show the working DC voltage of SFP module.
- **Mon1(Bias) mA:**
Show the Bias current of SFP module.
- **Mon2(TX PWR):**
Show the transmit power of SFP module.
- **Mon3(RX PWR):**
Show the receiver power of SFP module.

3-1.7 EEE

The section which allows the user to inspect and configure the current EEE port settings.

EEE is a power saving option that reduces the power usage when there is very low traffic utilization (or no traffic).

EEE works 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 information about the devices wakeup time using the LLDP protocol.

For maximizing the power saving, the circuit isn't started at once transmit data are ready for a port, but is instead queued until 3000 bytes of data are ready to be transmitted. For not introducing a large delay in case that data less then 3000 bytes shall be transmitted, data are always transmitted after 48 us, giving a maximum latency of 48 us + the wakeup time.

If desired it is possible to minimize the latency for specific frames, by mapping the frames to a specific queue (done with QOS), and then mark the queue as an urgent queue. When an urgent queue gets data to be transmitted, the circuits will be powered up at once and the latency will be reduced to the wakeup time.

Web Interface

To configure the EEE Configuration in the web interface:

1. Click Configuration, Port, then EEE
2. To evoke which port wants to enable the EEE function. To evoke which
3. EEE Urgent Queues level and the range from 1 to 8. the queue will Postpone the transmission until 3000 bytes are ready to be transmitted.
4. Click the Apply to save the setting
5. If you want to cancel the setting then you need to click the reset button. It will revert to previously saved values.

Figure 3-1.7: The EEE Configuration

The screenshot shows the 'EEE Configuration' web interface. It features a table with columns for 'Port', 'EEE Enabled', and 'EEE Urgent Queues' (1-8). Each cell contains a checkbox. Below the table are 'Apply' and 'Reset' buttons.

Port	EEE Enabled	EEE Urgent Queues							
		1	2	3	4	5	6	7	8
*	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
7	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
11	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
13	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
14	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
15	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
16	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Apply Reset

Parameter description:

- **EEE Port Configuration:**

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

- **Port :**

The switch port number of the logical EEE port.

- **EEE Enabled :**

Controls whether EEE is enabled for this switch port.

- **EEE Urgent Queues :**

Queues set will activate transmission of frames as soon as any data is available. Otherwise the queue will postpone the transmission until 3000 bytes are ready to be transmitted.

- **Buttons**

Save – Click to save changes.

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

3-2 Aggregation

The Aggregation is used to configure the settings of Link Aggregation. You can bundle more than one port with the same speed, full duplex and the same MAC to be a single logical port, thus the logical port aggregates the bandwidth of these ports. This means you can apply your current Ethernet equipment's to build the bandwidth aggregation. For example, if there are three Fast Ethernet ports aggregated in a logical port, then this logical port has bandwidth three times as high as a single Fast Ethernet port has.

3-2.1 Static Trunk

The Aggregation Configuration is used to configure the settings of Link Aggregation. You can bundle more than one port with the same speed, full duplex and the same MAC to be a single logical port, thus the logical port aggregates the bandwidth of these ports. This means you can apply your current Ethernet equipment's to build the bandwidth aggregation.

3-2.1.1 Static Trunk

Ports using Static Trunk as their trunk method can choose their unique Static GroupID to form a logic "trunked port". The benefit of using Static Trunk method is that a port can immediately become a member of a trunk group without any handshaking with its peer port. This is also a disadvantage because the peer ports of your static trunk group may not know that they should be aggregate together to form a "logic trunked port". Using Static Trunk on both end of a link is strongly recommended. Please also note that low speed links will stay in "not ready" state when using static trunk to aggregate with high speed links.

Web Interface

To configure the Trunk Aggregation Hash mode and Aggregation Group in the web interface:

1. Click Configuration, Static Trunk, and then Aggregation Mode Configuration.
2. Evoke to enable or disable the aggregation mode function.
Evoke Aggregation Group ID and Port members
3. Click the apply to save the setting
4. If you want to cancel the setting then you need to click the reset button. It will revert to previously saved values.

Figure 3-2.1.1: The Aggregation Mode Configuration

Aggregation Mode Configuration

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

Aggregation Group Configuration

Group ID	Port Members																	
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Normal	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
1	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
2	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
3	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
4	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
5	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
6	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
7	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
8	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
9	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Apply
Reset

Parameter description:

Hash Code Contributors

● **Source MAC Address :**

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

● **Destination MAC Address :**

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

● **IP Address :**

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

● **TCP/UDP Port Number :**

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

Aggregation Group Configuration

● **Group ID :**

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

● **Port Members :**

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

● **Buttons**

Apply – Click to apply changes.

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

3-2.2 LACP

Ports using Link Aggregation Control Protocol (according to IEEE 802.3ad specification) as their trunking method can choose their unique LACP GroupID to form a logic “trunked port”. The benefit of using LACP is that a port makes an agreement with its peer port before it becomes a ready member of a “trunk group” (also called aggregator). LACP is safer than the other trunking method - static trunk.

3-2.2.1 Configuration

This page allows the user to inspect the current LACP port configurations, and possibly change them as well. An LACP trunk group with more than one ready member-ports is a “real trunked” group. An LACP trunk group with only one or less than one ready member-ports is not a “real trunked” group.

Web Interface

To configure the Trunk Aggregation LACP parameters in the web interface:

1. Click Configuration, LACP, Configuration
2. Evoke to enable or disable the LACP on the port of the switch.
Scroll the Key parameter with Auto or Specific Default is Auto.
3. Scroll the Role with Active or Passive. Default is Active
4. Click the apply to save the setting
5. If you want to cancel the setting then you need to click the reset button.
It will revert to previously saved values

Figure 3-2.2.1: The LACP Port Configuration

Port	LACP Enabled	Key	Role
*	<input type="checkbox"/>	<> ▾	<> ▾
1	<input type="checkbox"/>	Auto ▾	Active ▾
2	<input type="checkbox"/>	Auto ▾	Active ▾
3	<input type="checkbox"/>	Auto ▾	Active ▾
4	<input type="checkbox"/>	Auto ▾	Active ▾
5	<input type="checkbox"/>	Auto ▾	Active ▾
6	<input type="checkbox"/>	Auto ▾	Active ▾
7	<input type="checkbox"/>	Auto ▾	Active ▾
8	<input type="checkbox"/>	Auto ▾	Active ▾
9	<input type="checkbox"/>	Auto ▾	Active ▾
10	<input type="checkbox"/>	Auto ▾	Active ▾
11	<input type="checkbox"/>	Auto ▾	Active ▾
12	<input type="checkbox"/>	Auto ▾	Active ▾
13	<input type="checkbox"/>	Auto ▾	Active ▾
14	<input type="checkbox"/>	Auto ▾	Active ▾
15	<input type="checkbox"/>	Auto ▾	Active ▾
16	<input type="checkbox"/>	Auto ▾	Active ▾
17	<input type="checkbox"/>	Auto ▾	Active ▾
18	<input type="checkbox"/>	Auto ▾	Active ▾

Apply Reset

Parameter description:

- **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.

- **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).

- **Buttons**
Apply – Click to apply changes.
Reset- Click to undo any changes made locally and revert to previously saved values.

3-2.2.2 System Status

This section describes that when you complete to set LACP function on the switch then it provides a status overview for all LACP instances

Web Interface

To display the LACP System status in the web interface:

1. Click Configuration, LACP, System Status
2. If you want to auto-refresh the information then you need to evoke the "Auto-refresh".
3. Click "Refresh" to refresh the LACP System Status.

Figure 3-2.2.2: The LACP System Status



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

Parameter description:

- **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. The format is: "Switch ID:Port".
- **Auto-refresh:**
To evoke the auto-refresh to refresh the information automatically.
- **Upper right icon (Refresh)**
You can click them for refresh the LACP System status information by manual.

3-2.2.3 Port Status

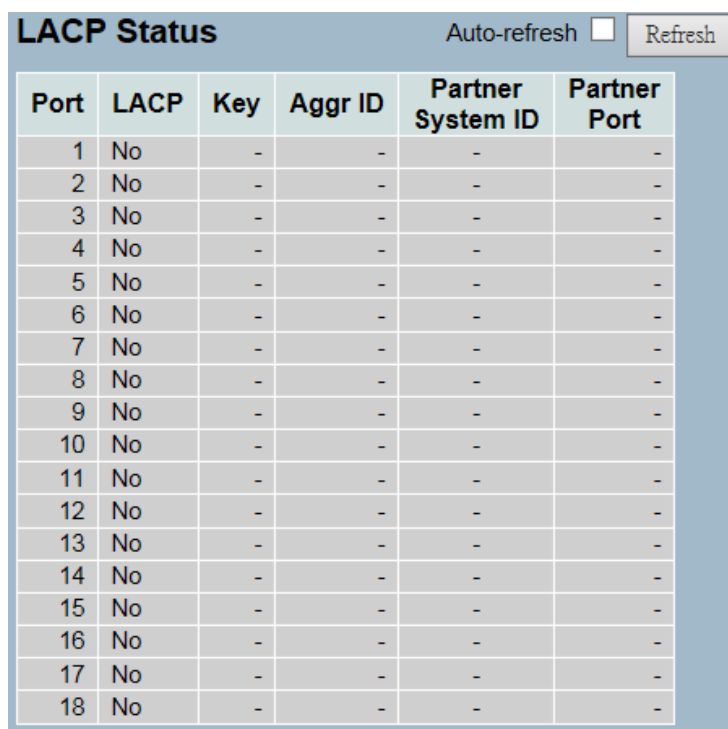
This section describes that when you complete to set LACP function on the switch then it provides a Port Status overview for all LACP instances

Web Interface

To display the LACP Port status in the web interface:

1. Click Configuration, LACP, Port Status
2. If you want to auto-refresh the information then you need to evoke the "Auto-refresh".
3. Click "Refresh" to refresh the LACP Port Status.

Figure 3-2.2.3: The LACP Status



Port	LACP	Key	Aggr ID	Partner System ID	Partner Port
1	No	-	-	-	-
2	No	-	-	-	-
3	No	-	-	-	-
4	No	-	-	-	-
5	No	-	-	-	-
6	No	-	-	-	-
7	No	-	-	-	-
8	No	-	-	-	-
9	No	-	-	-	-
10	No	-	-	-	-
11	No	-	-	-	-
12	No	-	-	-	-
13	No	-	-	-	-
14	No	-	-	-	-
15	No	-	-	-	-
16	No	-	-	-	-
17	No	-	-	-	-
18	No	-	-	-	-

Parameter description:

- **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.

- **Auto-refresh:**
To evoke the auto-refresh to refresh the information automatically.
- **Upper right icon (Refresh) :**
You can click them for refresh the LACP port status information by manual.

3-2.2.4 Port Statistics

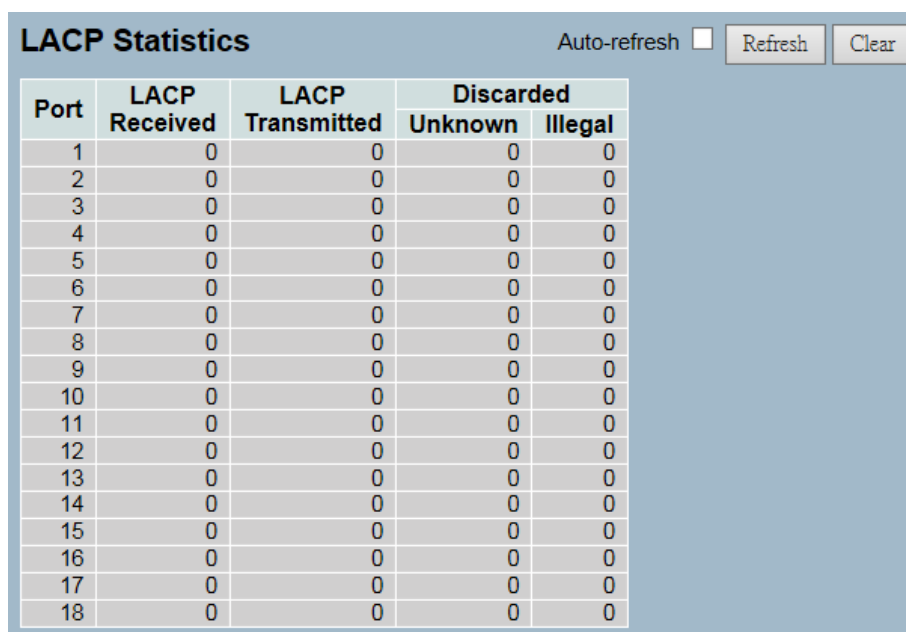
This section describes that when you complete to set LACP function on the switch then it provides a Port Statistics overview for all LACP instances

Web Interface

To display the LACP Port status in the web interface:

1. Click Configuration, LACP, Port Statistics
2. If you want to auto-refresh the information then you need to evoke the “Auto refresh”.
3. Click “ Refresh“ to refresh the LACP Statistics.

Figure 3-2.2.4: The LACP Statistics



Port	LACP Received	LACP Transmitted	Discarded	
			Unknown	Illegal
1	0	0	0	0
2	0	0	0	0
3	0	0	0	0
4	0	0	0	0
5	0	0	0	0
6	0	0	0	0
7	0	0	0	0
8	0	0	0	0
9	0	0	0	0
10	0	0	0	0
11	0	0	0	0
12	0	0	0	0
13	0	0	0	0
14	0	0	0	0
15	0	0	0	0
16	0	0	0	0
17	0	0	0	0
18	0	0	0	0

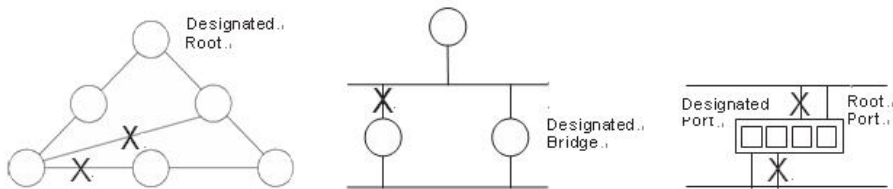
Parameter description:

- **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.
- **Auto-refresh:**
To evoke the auto-refresh to refresh the information automatically.
- **Upper right icon (Refresh, Clear)**
You can click them for refresh the LACP port statistics information or clear by manual.

3-3 Spanning Tree

The Spanning Tree Protocol (STP) can be used to detect and disable network loops, and to provide backup links between switches, bridges or routers. This allows the switch to interact with other bridging devices (that is, an STP-compliant switch, bridge or router) in your network to ensure that only one route exists between any two stations on the network, and provide backup links which automatically take over when a primary link goes down.

STP - STP uses a distributed algorithm to select a bridging device (STP-compliant switch, bridge or router) that serves as the root of the spanning tree network. It selects a root port on each bridging device (except for the root device) which incurs the lowest path cost when forwarding a packet from that device to the root device. Then it selects a designated bridging device from each LAN which incurs the lowest path cost when forwarding a packet from that LAN to the root device. All ports connected to designated bridging devices are assigned as designated ports. After determining the lowest cost spanning tree, it enables all root ports and designated ports, and disables all other ports. Network packets are therefore only forwarded between root ports and designated ports, eliminating any possible network loops.



Once a stable network topology has been established, all bridges listen for Hello BPDUs (Bridge Protocol Data Units) transmitted from the Root Bridge. If a bridge does not get a Hello BPDU after a predefined interval (Maximum Age), the bridge assumes that the link to the Root Bridge is down. This bridge will then initiate negotiations with other bridges to reconfigure the network to reestablish a valid network topology.

3-3.1 Bridge Settings

The section describes that how to configure the Spanning Tree Bridge and STP System settings. It allows you to configure STP System settings are used by all STP Bridge instance in the Switch.

Web Interface

To configure the Spanning Tree Bridge Settings parameters in the web interface:

1. Click Configuration, Spanning Tree, Bridge Settings
2. Scroll to select the parameters and write down available value of parameters in blank field in Basic Settings
3. Evoke to enable or disable the parameters and write down available value of parameters in blank field in Advanced settings
4. Click the Apply to save the setting
- 5 . If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values

Figure 3-3.1: The STP Bridge Configuration

The screenshot shows the 'STP Bridge Configuration' window. It is divided into two sections: 'Basic Settings' and 'Advanced Settings'. The 'Basic Settings' section contains a table with the following parameters and values:

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

The 'Advanced Settings' section contains a table with the following parameters and values:

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

At the bottom of the window, there are two buttons: 'Apply' and 'Reset'.

Parameter description:

Basic Settings

- **Protocol Version :**
The 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 $\leq (\text{FwdDelay}-1)*2$.
- **Maximum Hop Count :**
This defines the initial value of remaining Hops for MSTI information generated at the boundary of an MSTI region. It defines how many bridges a root bridge can distribute its BPDU information to. Valid values are in the range 6 to 40 hops.
- **Transmit Hold Count :**
The number of 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**

Apply – Click to save changes.

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

3-3.2 MSTI Mapping

When you implement an Spanning Tree protocol on the switch that the bridge instance. The CIST is not available for explicit mapping, as it will receive the VLANs not explicitly mapped. Due to the reason that you need to set the list of VLANs mapped to the MSTI. The VLANs 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.)

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

Web Interface

To configure the Spanning Tree MSTI Mapping parameters in the web interface:

1. Click Configuration, Spanning Tree, MSTI Mapping
2. Specify the configuration identification parameters in the field
Specify the VLANs Mapped blank field.
3. Click the Apply to save the setting
4. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values

Figure 3-3.2: The MSTI Configuration

MSTI Configuration

Add VLANs separated by spaces or comma.

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

Configuration Identification

Configuration Name	00-40-c7-55-55-55
Configuration Revision	0

MSTI Mapping

MSTI	VLANs Mapped
MSTI1	
MSTI2	
MSTI3	
MSTI4	
MSTI5	
MSTI6	
MSTI7	

Apply Reset

Parameter description:

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 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

- **Buttons**

Save – Click to save changes.

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

3-3.3 MSTI Priorities

When you implement an Spanning Tree protocol on the switch that the bridge instance. The CIST is the default instance which is always active. For 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

The section describes it allows the user to inspect the current STP MSTI bridge instance priority configurations, and possibly change them as well.

Web Interface

To configure the Spanning Tree MSTI Priorities parameters in the web interface:

1. Click Configuration, Spanning Tree, MSTI Priorities
2. Scroll the Priority maximum is 240. Default is 128.
3. Click the Apply to save the setting
4. If you want to cancel the setting then you need to click the Reset button.
It will revert to previously saved values

Figure 3-3.3: The MSTI Configuration

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

Parameter description:

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

3-3.4 CIST Ports

When you implement an Spanning Tree protocol on the switch that the bridge instance. You need to configure the CIST Ports. The section describes it allows the user to inspect the to inspect the current STP CIST port configurations, and possibly change them as well.

Web Interface

To configure the Spanning Tree CIST Ports parameters in the web interface:

1. Click Configuration, Spanning Tree, CIST Ports
2. Scroll and evoke to set all parameters of CIST Aggregated Port Configuration.
3. Evoke to enable or disable the STP, then scoll and evoke to set all parameters of the CIST normal Port configuration.
4. Click the Apply to save the setting
5. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values

Figure 3-3.4: The STP CIST Port Configuration

STP CIST Port Configuration										
CIST Aggregated Port Configuration										
Port	STP Enabled	Path Cost	Priority	Admin Edge	Auto Edge	Restricted Role	TCN	BPDU Guard	Point-to-point	
-	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Forced True	
CIST Normal Port Configuration										
Port	STP Enabled	Path Cost	Priority	Admin Edge	Auto Edge	Restricted Role	TCN	BPDU Guard	Point-to-point	
*	<input type="checkbox"/>	<>	<>	<>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<>	
1	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto	
2	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto	
3	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto	
4	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto	
5	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto	
6	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto	
7	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto	
8	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto	
9	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto	
10	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto	
11	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto	
12	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto	
13	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto	
14	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto	
15	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto	
16	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto	
17	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto	
18	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto	

Apply Reset

Parameter description:

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

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

Apply – Click to save changes.
Reset- Click to undo any changes made locally and revert to previously saved values.

3-3.5 MSTI Ports

The section describes it 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. It contains MSTI port settings for physical and aggregated ports.

Web Interface

To configure the Spanning Tree MSTI Port Configuration parameters in the web interface:

1. Click Configuration, Spanning Tree, MSTI Ports
2. Scroll to select the MST1 or other MSTI Port
3. Click Get to set the detail parameters of the MSTI Ports.
4. Scroll to set all parameters of the MSTI Port configuration.
5. Click the Apply to save the setting
6. If you want to cancel the setting then you need to click the Reset button.
It will revert to previously saved values

Figure 3-3.5: The MSTI Port Configuration

MSTI Port Configuration

Select MSTI Port: MST1 Get

MST1 MSTI Port Configuration

MSTI Aggregated Ports Configuration

Port	Path Cost	Priority
-	Auto	128

MSTI Normal Ports Configuration

Port	Path Cost	Priority
*	<>	<>
1	Auto	128
2	Auto	128
3	Auto	128
4	Auto	128
5	Auto	128
6	Auto	128
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

Apply Reset

Parameter description:

- **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**

Apply – Click to save changes.

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

3-3.6 Bridge Status

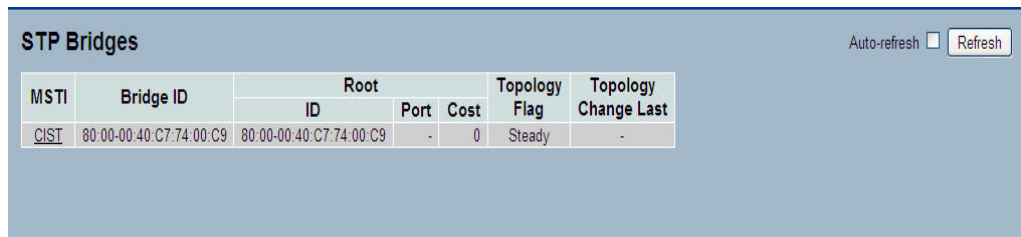
After you complete the MSTI Port configuration the you could to ask the switch display the Bridge Status. The Section provides a status overview of all STP bridge instances. The displayed table contains a row for each STP bridge instance, where the column displays the following information:

Web Interface

To display the STP Bridges status in the web interface:

1. Click Configuration, Spanning Tree, STP Bridges
2. If you want to auto-refresh the information then you need to evoke the "Auto-refresh".
3. Click " Refresh" to refresh the STP Bridges.

Figure 3-3.6: The STP Bridges status



MSTI	Bridge ID	Root			Topology Flag	Topology Change Last
		ID	Port	Cost		
CIST	80:00:00:40:C7:74:00:C9	80:00:00:40:C7:74:00:C9	-	0	Steady	-

Parameter description:

- **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.
- **Auto-refresh:**
To evoke the auto-refresh to refresh the information automatically.
- **Upper right icon (Refresh)**
You can click them for refresh the STP Bridges status information by manual.

3-3.7 Port Status

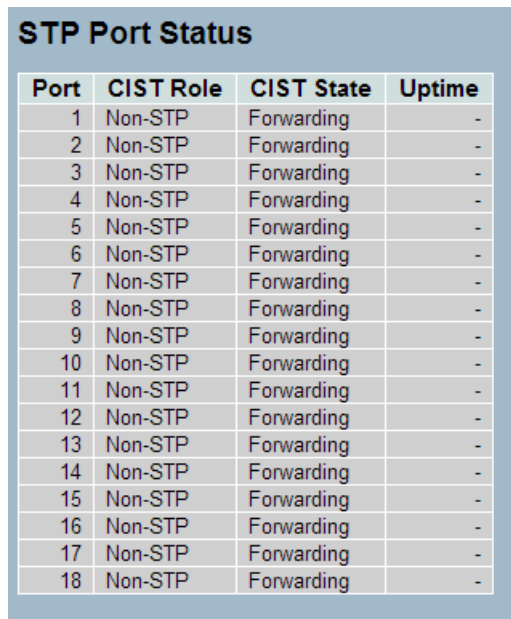
After you complete the STP configuration the you could to ask the switch display the STP Port Status. The Section provides you to ask switch to display the STP CIST port status for physical ports of the currently selected switch.:

Web Interface

To display the STP Port status in the web interface:

1. Click Configuration, Spanning Tree, STP Port Status
2. If you want to auto-refresh the information then you need to evoke the "Auto-refresh".
3. Click " Refresh" to refresh the STP Bridges.

Figure 3-3.7: The STP Port status



Port	CIST Role	CIST State	Uptime
1	Non-STP	Forwarding	-
2	Non-STP	Forwarding	-
3	Non-STP	Forwarding	-
4	Non-STP	Forwarding	-
5	Non-STP	Forwarding	-
6	Non-STP	Forwarding	-
7	Non-STP	Forwarding	-
8	Non-STP	Forwarding	-
9	Non-STP	Forwarding	-
10	Non-STP	Forwarding	-
11	Non-STP	Forwarding	-
12	Non-STP	Forwarding	-
13	Non-STP	Forwarding	-
14	Non-STP	Forwarding	-
15	Non-STP	Forwarding	-
16	Non-STP	Forwarding	-
17	Non-STP	Forwarding	-
18	Non-STP	Forwarding	-

Parameter description:

- **Port :**
The switch port number of the logical STP port.
- **CIST Role :**
The current STP port role of the CIST port. The port role can be one of the following values: AlternatePort, Backup Port, RootPort, DesignatedPort Disabled.
- **CIST State :**
The current STP port state of the CIST port. The port state can be one of the following values: Blocking Learning Forwarding.
- **Uptime**
The time since the bridge port was last initialized.
- **Auto-refresh:**
To evoke the auto-refresh to refresh the information automatically.
- **Upper right icon (Refresh)**
You can click them for refresh the STP Port status information by manual.

3-3.8 Port Statistics

After you complete the STP configuration then you could to let the switch display the STP Statistics. The Section provides you to ask switch to display the STP Statistics detail counters of bridge ports in the currently selected switch.

Web Interface

To display the STP Port status in the web interface:

1. Click Configuration, Spanning Tree, Port Statistics
2. If you want to auto-refresh the information then you need to evoke the "Auto-refresh".
3. Click " Refresh" to refresh the STP Bridges.

Figure 3-3.8: The STP Statistics

Port	Transmitted				Received				Discarded	
	MSTP	RSTP	STP	TCN	MSTP	RSTP	STP	TCN	Unknown	Illegal
No ports enabled										

Parameter description:

- **Port :**
The switch port number of the logical STP port.
- **MSTP :**
The number of MSTP Configuration BPDU's received/transmitted on the port.
- **RSTP :**
The number of RSTP Configuration 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.
- **Auto-refresh:**
To evoke the auto-refresh to refresh the information automatically.
- **Upper right icon (Refresh, Clear)**
You can click them for refresh the STP Statistics information or clear by manual.

3-4 IGMP Snooping

The function, is used to establish the multicast groups to forward the multicast packet to the member ports, and, in nature, avoids wasting the bandwidth while IP multicast packets are running over the network. This is because a switch that does not support IGMP or IGMP Snooping can not tell the multicast packet from the broadcast packet, so it can only treat them all as the broadcast packet. Without IGMP Snooping, the multicast packet forwarding function is plain and nothing is different from broadcast packet.

A switch supported IGMP Snooping with the functions of query, report and leave, a type of packet exchanged between IP Multicast Router/Switch and IP Multicast Host, can update the information of the Multicast table when a member (port) joins or leaves an IP Multicast Destination Address. With this function, once a switch receives an IP multicast packet, it will forward the packet to the members who joined in a specified IP multicast group before.

The packets will be discarded by the IGMP Snooping if the user transmits multicast packets to the multicast group that had not been built up in advance. IGMP mode enables the switch to issue IGMP function that you enable IGMP proxy or snooping on the switch, which connects to a router closer to the root of the tree. This interface is the upstream interface. The router on the upstream interface should be running IGMP.

3-4.1 Basic Configuration

The section describes how to set the basic IGMP snooping on the switch, which connects to a router closer to the root of the tree. This interface is the upstream interface. The router on the upstream interface should be running IGMP.

Web Interface

To configure the IGMP Snooping parameters in the web interface:

1. Click Configuration, IGMP Snooping, Basic Configuration
2. Evoke to select enable or disable which Global configuration
3. Evoke which port wants to become a Router Port or enable/ disable the Fast Leave function..
4. Scroll to set the Throtting parameter.
5. Click the save to save the setting
6. If you want to cancel the setting then you need to click the Reset button.
It will revert to previously saved values

Figure 3-4.1: The IGMP Snooping Configuration.

IGMP Snooping Configuration

Global Configuration	
Snooping Enabled	<input type="checkbox"/>
Unregistered IPMCv4 Flooding Enabled	<input type="checkbox"/>
IGMP SSM Range	232.0.0.0 / 8
Proxy Enabled	<input type="checkbox"/>

Port Related Configuration

Port	Router Port	Fast Leave	Throttling
*	<input type="checkbox"/>	<input type="checkbox"/>	<> ▼
1	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▼
2	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▼
3	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▼
4	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▼
5	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▼
6	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▼
7	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▼
8	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▼
9	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▼
10	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▼
11	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▼
12	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▼
13	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▼
14	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▼
15	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▼
16	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▼
17	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▼
18	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▼

Apply Reset

Parameter description:

- **Snooping Enabled:**
Enable the Global IGMP Snooping.
- **Unregistered IPMCv4 Flooding enabled :**
Enable unregistered IPMCv4 traffic flooding.
- **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.
Format: (IP address/ sub mask)
- **Proxy Enabled :**
Enable IGMP Proxy. This feature can be used to avoid forwarding unnecessary join and leave messages to the router side.
- **Port :**
It shows the physical Port index of switch.

- **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.

3-4.2 VLAN Configuration

The section describes the VLAN configuration setting process integrated with IGMP Snooping function. For Each setting 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 button will update the displayed table starting from that or the next closest VLAN Table match.

Web Interface

To configure the IGMP Snooping VLAN Configuration in the web interface:

1. Click Configuration, IGMP Snooping, VLAN Configuration
2. Evoke to select enable or disable Snooping , IGMP Querier
Specify the parameters in the blank field.
3. Click the refresh to update the data or click << or >> to display previous entry or next entry.
4. Click the save to save the setting
5. If you want to cancel the setting then you need to click the Reset button.
It will revert to previously saved values

Figure 3-4.2: The IGMP Snooping VLAN Configuration.

IGMP Snooping VLAN Configuration

Start from VLAN 1 with 20 entries per page.

VLAN ID	Snooping Enabled	IGMP Querier	Compatibility	RV	QI (sec)	QRI (0.1 sec)	LLQI (0.1 sec)	URI (sec)
1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	-	-	-	-	-	-
2	<input type="checkbox"/>	<input checked="" type="checkbox"/>	-	-	-	-	-	-
3	<input type="checkbox"/>	<input checked="" type="checkbox"/>	-	-	-	-	-	-
4	<input type="checkbox"/>	<input checked="" type="checkbox"/>	-	-	-	-	-	-
5	<input type="checkbox"/>	<input checked="" type="checkbox"/>	-	-	-	-	-	-
6	<input type="checkbox"/>	<input checked="" type="checkbox"/>	-	-	-	-	-	-
7	<input type="checkbox"/>	<input checked="" type="checkbox"/>	-	-	-	-	-	-
8	<input type="checkbox"/>	<input checked="" type="checkbox"/>	-	-	-	-	-	-
9	<input type="checkbox"/>	<input checked="" type="checkbox"/>	-	-	-	-	-	-

Apply Reset Refresh << >>

Parameter description:

- **VLAN ID :**
It displays the VLAN ID of the entry.
- **Snooping Enabled :**
Enable the per-VLAN IGMP Snooping. Only up to 32 VLANs can be selected. .
- **IGMP Querier :**
A router sends IGMP Query messages onto a particular link. This Router is called the 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 Max Response Time used to calculate the Max Resp 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 :**
 - Save** – Click to save changes.
 - Reset-** Click to undo any changes made locally and revert to previously saved values.
- **Upper right icon (Refresh, |<<, >>) :**
You can click them Refreshes the displayed table starting from the "VLAN" input fields. Or click "|<<" to update the table starting from the first entry in the VLAN table, i.e. the entry with the lowest VLAN ID. Others click ">>" to update the table, starting with the entry after the last entry currently displayed.

3-4.3 Port Group Filtering

The section describes how to set the IGMP Port Group Filtering? With the IGMP filtering feature, an user can exert this type of control. In some network Application environments, as like the metropolitan or multiple-dwelling unit (MDU) installations, an user might want to control the multicast groups to which a user on a switch port can belong. It allows the user to control the distribution of multicast services, such as IP/TV, based on some type of subscription or service plan.

With this feature, you can filter multicast joins on a per-port basis by configuring IP multicast profiles and associating them with individual switch ports. An IGMP profile can contain one or more multicast groups and specifies whether access to the group is permitted or denied. If an IGMP profile denying access to a multicast group is applied to a switch port, the IGMP join report requesting the stream of IP multicast traffic is dropped, and the port is not allowed to receive IP multicast traffic from that group. If the filtering action permits access to the multicast group, the IGMP report from the port is forwarded for normal processing.

IGMP filtering controls only IGMP membership join reports and has no relationship to the function that directs the forwarding of IP multicast traffic.

Web Interface

To configure the IGMP Snooping Port Group Configuration in the web interface:

1. Click Configuration, IGMP Snooping, Port Group Filtering
2. Click Add new Filtering Group
3. Scroll the Port to enable the Port Group Filtering.
Specify the Filtering Groups in the blank field.
4. Click the Apply to save the setting
5. If you want to cancel the setting then you need to click the Reset button.
It will revert to previously saved values

Figure 3-4.3: The IGMP Snooping Port Group Filtering Configuration.

Delete	Port	Filtering Groups
<input type="checkbox"/>	3	224.1.1.10
<input type="checkbox"/>	5	224.1.1.12

Delete	1	
--------	---	--

Parameter description:

- **Delete :**
Check to delete the entry. It will be deleted during the next save.
- **Port :**
To evoke the port enable the IGMP Snooping Port Group Filtering function.
- **Filtering Groups :**
The IP Multicast Group that will be filtered.
- **Buttons:**
Apply – Click to save changes.
Reset- Click to undo any changes made locally and revert to previously saved values.

3-4.4 Status

After you complete the IGMP Snooping configuration, then you could to let the switch display the IGMP Snooping Status. The Section provides you to let switch to display the IGMP Snooping detail status.

Web Interface

To display the IGMP Snooping status in the web interface:

1. Click Configuration, IGMP Snooping, Status
2. If you want to auto-refresh the information then you need to evoke the "Auto-refresh".
3. Click " Refresh" to refresh the IGMP Snooping Status.
4. Click " Clear" to clear the IGMP Snooping Status.

Figure 3-4.4: The IGMP Snooping Status.

IGMP Snooping Status											
									Auto-refresh <input type="checkbox"/>	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		
1	v3	v3	ACTIVE	0	0	0	0	0	0		

Router Port	
Port	Status
1	-
2	-
3	-
4	-
5	-
6	-
7	-
8	-
9	-
10	-
11	-
12	-
13	-
14	-
15	-
16	-
17	-
18	-

Parameter description:

- **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".

- **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.
- **Auto-refresh**
To evoke the auto-refresh icon then the device will refresh the log automatically.
- **Upper right icon (Refresh, clear)**
You can click them for refresh the Status or clear them by manual.

3-4.5 Group Information

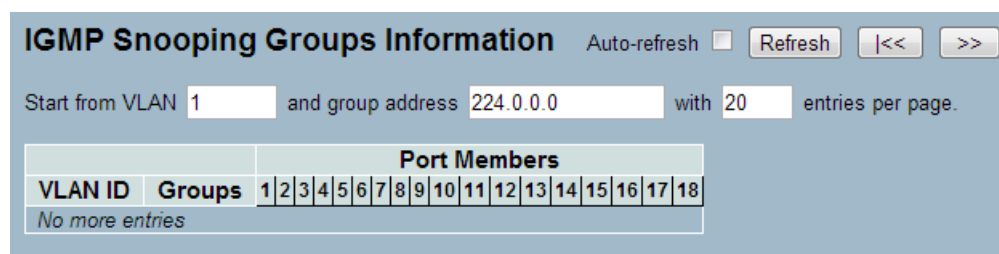
After you complete to set the IGMP Snooping function then you could let the switch to display the IGMP Snooping Group Information. Entries in the IGMP Group Table are shown on this page. The IGMP Group Table is sorted first by VLAN ID, and then by group. The will use the last entry of the currently displayed 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.

Web Interface

To display the IGMP Snooping Group Information in the web interface:

1. Click Configuration, IGMP Snooping, Group Information
2. If you want to auto-refresh the information then you need to evoke the "Auto-refresh".
3. Click " Refresh" to refresh a entry of the IGMP Snooping Groups Information.
4. Click "<< or >> " to move to previous or next entry.

Figure 3-4.5: The IGMP Snooping Groups Information.



Parameter description:

Navigating 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. 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.

IGMP Group Table Columns

- **VLAN ID :**
VLAN ID of the group.
- **Groups :**
Group address of the group displayed.
- **Port Members :**
Ports under this group.
- **Auto-refresh**
To evoke the auto-refresh icon then the device will refresh the log automatically.
- **Upper right icon (Refresh, <<, >>)**
You can click them for refresh the IGMP Group Status by manual, others for next/up page or entry..

3-4.6 IPv4 SSM information

Source Specific Multicast (SSM) is a datagram delivery model that best supports one-to-many applications, also known as broadcast applications. SSM is a core network technology of IP multicast targeted for audio and video broadcast application environments.

For the SSM delivery mode, an IP multicast receiver host must use IGMP Version 3 (IGMPv3) to subscribe to channel (S, G). By subscribing to this channel, the receiver host is indicating that it wants to receive IP multicast traffic sent by source host S to group G. The network will deliver IP multicast packets from source host S to group G to all hosts in the network that have subscribed to the channel (S, G).

SSM does not require group address allocation within the network, only within each source host. Different applications running on the same source host must use different SSM groups. Different applications running on different source hosts can arbitrarily reuse SSM group addresses without causing any excess traffic on the network.

Addresses in the range 232.0.0.0/8 (232.0.0.0 to 232.255.255.255) are reserved for SSM by IANA. In the switch, you can configure SSM for arbitrary IP multicast addresses also.

Web Interface

To display the IGMPv3 IPv4 SSM Information in the web interface:

1. Click Configuration, IGMP Snooping, IPv4 SSM Information
2. If you want to auto-refresh the information then you need to evoke the "Auto-refresh".
3. Click "Refresh" to refresh a entry of the IGMPv3 IPv4 SSM Information.
4. Click "<< or >>" to move to previous or next entry.

Figure 3-4.6: The IGMPv3 IPv4 SSM Information.

IGMPv3 Information Auto-refresh Refresh |<< >>

Start from VLAN and Group with entries per page.

VLAN ID	Group	Port No.	Mode	Source Address	Type
No more entries					

Parameter description:

Navigating the IGMPv3 Information Table

Each page shows up to 99 entries from the IGMPv3 SSM (Source Specific Multicast) 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 IGMPv3 Information Table.

The "Start from VLAN", and "group" input fields allow the user to select the starting point in the IGMPv3 Information Table. Clicking the button will update the displayed table starting from that or the closest next IGMPv3 Information Table match. In addition, the two input fields will - upon a button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

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.

IGMPv3 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.
- **Auto-refresh**
To evoke the auto-refresh icon then the device will refresh the log automatically.
- **Upper right icon (Refresh, <<, >>)**
You can click them for refresh the IGMP Group Status by manual, others for next/up page or entry..

3-5 MVR

The MVR feature enables multicast traffic forwarding on the Multicast VLAN. In a multicast television application, a PC or a television with 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 join message to Switch A to join the appropriate multicast. Uplink ports that send and receive multicast data to and from the multicast VLAN are called MVR source ports.

3-5.1 Configuration

The section describes user could set the MVR basic Configuration and some parameters in the switch

Web Interface

To configure the MLD Snooping Port Group Configuration in the web interface:

1. Click Configuration, MVR, Configuration
2. Scroll the MVR mode to enable or disable and Scroll to set all parameters.
3. Click the Apply to save the setting
4. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values

Figure 3-5.1: The MVR Configuration

MVR Configuration

MVR Mode: Disabled
VLAN ID: 100

Port Configuration

Port	Mode	Type	Immediate Leave
*	<>	<>	<>
1	Disabled	Receiver	Disabled
2	Disabled	Receiver	Disabled
3	Disabled	Receiver	Disabled
4	Disabled	Receiver	Disabled
5	Disabled	Receiver	Disabled
6	Disabled	Receiver	Disabled
7	Disabled	Receiver	Disabled
8	Disabled	Receiver	Disabled
9	Disabled	Receiver	Disabled
10	Disabled	Receiver	Disabled
11	Disabled	Receiver	Disabled
12	Disabled	Receiver	Disabled
13	Disabled	Receiver	Disabled
14	Disabled	Receiver	Disabled
15	Disabled	Receiver	Disabled
16	Disabled	Receiver	Disabled
17	Disabled	Receiver	Disabled
18	Disabled	Receiver	Disabled

Apply Reset

Parameter description:

- **MVR Mode :**
Enable/Disable the Global MVR.
- **VLAN ID :**
Specify the Multicast VLAN ID.
- **Mode :**
Enable MVR on the port.
- **Type :**
Specify the MVR port type on the port.
- **Immediate Leave :**
Enable the fast leave on the port.
- **Buttons:**
Apply – Click to save changes.
Reset- Click to undo any changes made locally and revert to previously saved values.

3-5.2 Port Group Allow

The section describes user could add the MVR Groups Allow entries on the switch. The IP Multicast Group which been added into the table will be allowed to get through to the logical port. .

Web Interface

1. Click Configuration, MVR, Port Group Allow
2. To Click the "Add New Allow Group"
3. To choice which logical port you do want to set and enter the IP address from "Start Address" to "End Address".
4. Click "Apply" to Save the Port Allow Group.

Figure 3-5.2: The Port Group Allow

Delete	Port	Start Address	End Address
Delete	1 ▼	192.168.1.55	192.168.1.68
Delete	1 ▼		

Add new Allow Group

Apply Reset

Parameter description:

- **Delete**
Check to delete the entry. It will be deleted during the next apply.
- **Port**
The logical port for the settings.
- **Allow Groups**
The IP Multicast Group that will be allowed.
- **Adding New Allow Group**
Click " Add New Allow Group" to add a new entry to the Group Allow table. Specify the Port, and Allow Group of the new entry. Click "Apply".
- **Buttons**
Apply: Click to apply changes.
Reset: Click to undo any changes made locally and revert to previously saved values.

3-5.3 Groups Information

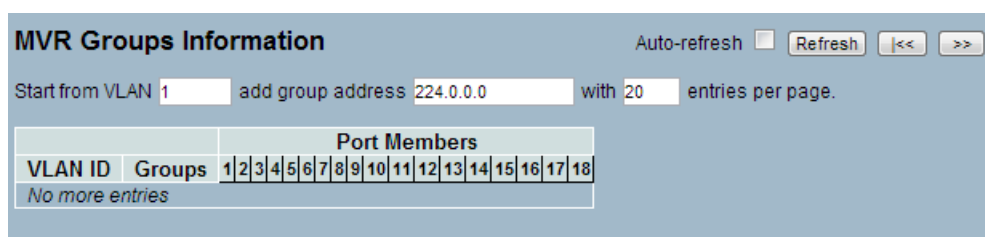
The section describes user could display the MVR Groups detail information on the switch. Entries in the MVR Group Table are shown on this page. The MVR Group Table is sorted first by VLAN ID, and then by group

Web Interface

To display the MVR Groups Information in the web interface:

1. Click Configuration, MVR, Groups Information
2. If you want to auto-refresh the information then you need to evoke the “Auto-refresh”.
3. To Click the “ Refresh” to refresh a entry of the MVR Groups Information.
4. Click “<< or >> “ to move to previous or next entry.

Figure 3-5.3: The MVR Groups Information



Parameter description:

MVR Group Table Columns

- **VLAN ID :**
VLAN ID of the group.
- **Groups :**
Group ID of the group displayed.
- **Port Members :**
Ports under this group.
- **Auto-refresh :**
To evoke the auto-refresh icon then the device will refresh the information automatically.
- **Upper right icon (Refresh, <<, >>):**
You can click them for refresh the MVR Group information by manual, others for next/up page or entry..

3-5.4 Statistics

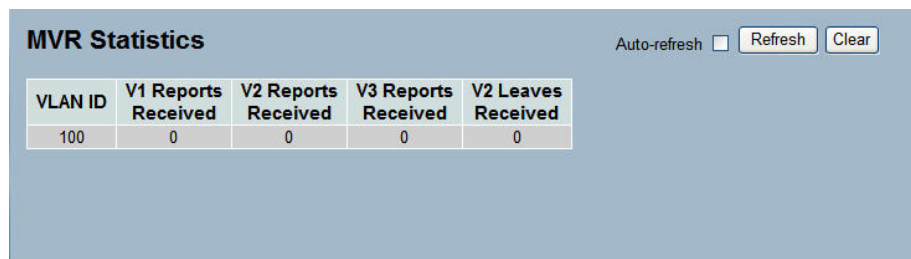
The section describes the switch will display the MVR detail Statistics after you had configured MVR on the switch. It provides the detail MVR Statistics Information

Web Interface

To display the MVR Statistics Information in the web interface:

1. Click Configuration, MVR, Statistics
2. If you want to auto-refresh the information then you need to evoke the “Auto-refresh”.
3. To Click the “ Refresh “ to refresh a entry of the MVR Statistics Information.
4. Click “<< or >> “ to move to previous or next entry.

Figure 3-5.4: The MVR Statistics Information



VLAN ID	V1 Reports Received	V2 Reports Received	V3 Reports Received	V2 Leaves Received
100	0	0	0	0

Parameter description:

- **VLAN ID :**
The Multicast VLAN ID.
- **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.
- **Auto-refresh :**
To evoke the auto-refresh icon then the device will refresh the information automatically.
- **Upper right icon (Refresh, <<, >>):**
You can click them for refresh the MVR Group information by manual, others for next/up page or entry.

3-5.5 EEE

By using EEE power savings can be achieved at the expense of traffic latency. This latency occurs due to that the circuits EEE turn off to save power, 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.

Web Interface

To display the MVR Statistics Information in the web interface:

1. Click Configuration, MVR, EEE

Figure 3-5.4: The EEE

Local Port	Tx Tw	Rx Tw	Fallback Receive Tw	Echo Tx Tw	Echo Rx Tw	Resolved Tx Tw	Resolved Rx Tw	EEE activated
No LLDP EEE information found								

Parameter description:

- **Local Port :**
The port on which LLDP frames are received or transmitted.
- **Tx Tw :**
The link partner's maximum time that transmit path can holdoff sending data after deassertion of LPI.
- **Rx Tw:**
The link partner's time that receiver would like the transmitter to holdoff 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 activated :**
Show if the switch and the link partner have agreed upon which wakeup times to use.
Red - Switch and link partner have not agreed upon wakeup time.
Green - Switch and link partner have agreed upon wakeup time.

3-5.6 Port Statistics

This page provides an overview of all LLDP traffic.

Two types of counters are shown. Global counters are counters that refer to the whole switch, while local counters refer to per port counters for the currently selected switch.

Web Interface

To display the MVR Statistics Information in the web interface:

1. Click Configuration, MVR, Port Statistics

Figure 3-5.6: The Port statistics

Global Counters	
Neighbour entries were last changed	2011-01-01 00:00:00 (183 sec. ago)
Total Neighbours Entries Added	0
Total Neighbours Entries Deleted	0
Total Neighbours Entries Dropped	0
Total Neighbours Entries Aged Out	0

LLDP Statistics							
Local Counters							
Local Port	Tx Frames	Rx Frames	Rx Errors	Frames Discarded	TLVs Discarded	TLVs Unrecognized	Age-Outs
1	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0
13	0	0	0	0	0	0	0
14	0	0	0	0	0	0	0
15	0	0	0	0	0	0	0
16	0	0	0	0	0	0	0
17	0	0	0	0	0	0	0
18	0	0	0	0	0	0	0

Parameter description:

Global Counter

- **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.

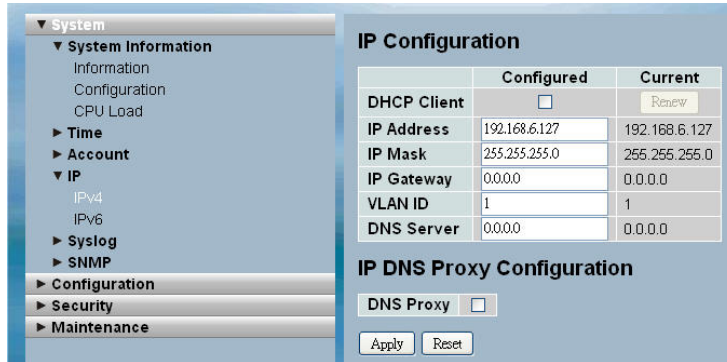
Local Counter

- **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.
- **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.

3-6 VLAN

To assign a specific VLAN for management purpose. The management VLAN is used to establish an IP connection to the switch from a workstation connected to a port in the VLAN. This connection supports a VSM, SNMP, and Telnet session. By default, the active management VLAN is VLAN 1, but you can designate any VLAN as the management VLAN by configuring System->IP->IPv4->VLAN ID. Only one management VLAN can be active at a time.

Figure 3-5.1.1: IP Configuration for management VLAN



When you specify a new management VLAN, your HTTP connection to the old management VLAN is lost. For this reason, you should have a connection between your management station and a port in the new management VLAN or connect to the new management VLAN through a multi-VLAN route.

3-6.1 VLAN Membership

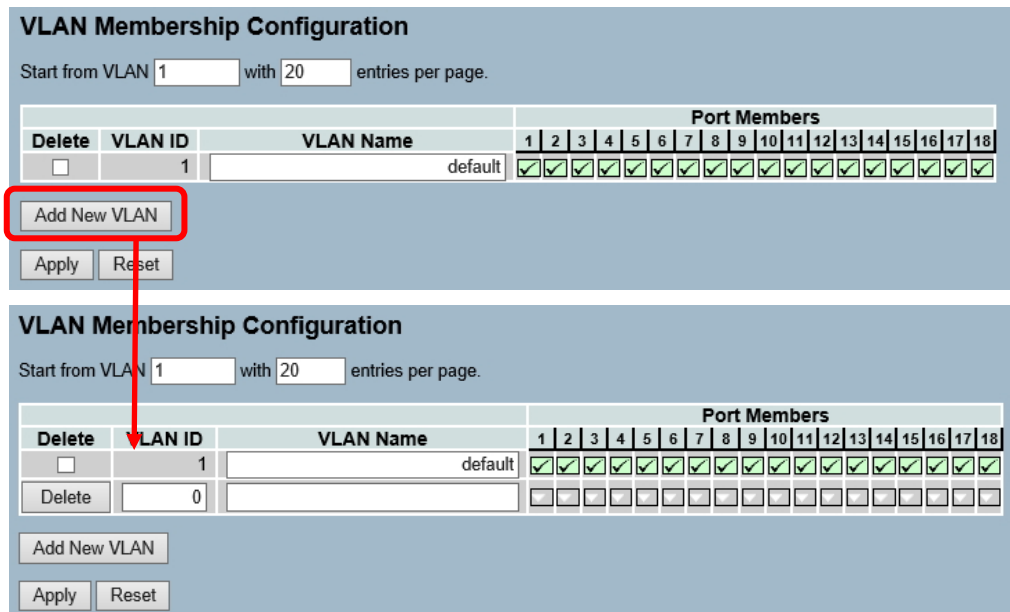
The VLAN membership configuration for the selected switch can be monitored and modified here. Up to 4094 VLANs are supported. This page allows for adding and deleting VLANs as well as adding and deleting port members of each VLAN.

Web Interface

To configure VLAN membership configuration in the web interface:

1. Click VLAN membership Configuration.
2. Specify Management VLAN ID from 1~ 4094.
3. Click Save.

Figure 3-6.1.2: The VLAN Membership Configuration



Parameter description:

- **Delete :**

To delete a VLAN entry, check this box and the entry will be deleted on the selected switch.

Warning: the default VLAN 1 can be deleted. But if deleting the default VLAN 1, the connection to the switch would be lost and some errors would occur.
- **VLAN ID :**

Indicates the ID of every single VLAN. Legal values for a VLAN ID are 1 to 4094.
- **VLAN Name :**

Indicates the name of VLAN. VLAN Name can contain alphabets, numbers, and mix of alphabets and numbers, but exclude special characters. VLAN Name can leave blanks. The length of VLAN name supports up to 32 characters. VLAN name can be edited for the existing VLAN entries.
- **Port Members :**

A row of check boxes for each port displays port members of each VLAN. To include a port in a VLAN, tick the box. To remove or exclude the port from the VLAN, make sure the box is unchecked.
- **Adding a New VLAN :**

Click to add a new VLAN group. An empty row, no port is member and all boxes are unchecked, is added to the table to configure.

A VLAN without any port members cannot be set up.
- **Buttons:**

Apply – Click to save changes.

Reset- Click to undo any change which is made before pressing Apply button. Go back to the previous group configuration.
- **Upper right icon (Refresh, |<<, >>):**

You can click them to refresh the VLAN entries manually. Press |<< or >> to previous or next page of the table.

3-6.2 Ports

User can configure all parameter to each port in VLAN Port Setting. These parameter involved two parts, Ingress rule and Egress rule. The function of Port Type, Ingress Filtering, Frame Type, and PVID affect Ingress process. Furthermore, Port Type, Egress Rule, and PVID affect Egress process.

Web Interface

To configure VLAN Port configuration in the web interface:

1. Click VLAN Port Configuration.
2. Specify the VLAN Port Configuration parameters.
3. Click Save.

Figure 3-6.2: The VLAN Port Configuration

Ethertype for Custom S-ports 0x88A8

VLAN Port Configuration

Port	Port Type	Ingress Filtering	Frame Type	Egress Rule	PVID
*	<>	<input type="checkbox"/>	<>	<>	
1	Unaware	<input type="checkbox"/>	All	Hybrid	1
2	Unaware	<input type="checkbox"/>	All	Hybrid	1
3	Unaware	<input type="checkbox"/>	All	Hybrid	2
4	Unaware	<input type="checkbox"/>	All	Hybrid	2
5	Unaware	<input type="checkbox"/>	All	Hybrid	3
6	Unaware	<input type="checkbox"/>	All	Hybrid	3
7	Unaware	<input type="checkbox"/>	All	Hybrid	4
8	Unaware	<input type="checkbox"/>	All	Hybrid	4
9	Unaware	<input type="checkbox"/>	All	Hybrid	5
10	Unaware	<input type="checkbox"/>	All	Hybrid	5
11	Unaware	<input type="checkbox"/>	All	Hybrid	6
12	Unaware	<input type="checkbox"/>	All	Hybrid	6
13	Unaware	<input type="checkbox"/>	All	Hybrid	7
14	Unaware	<input type="checkbox"/>	All	Hybrid	7
15	Unaware	<input type="checkbox"/>	All	Hybrid	8
16	Unaware	<input type="checkbox"/>	All	Hybrid	8
17	Unaware	<input type="checkbox"/>	All	Hybrid	9
18	Unaware	<input type="checkbox"/>	All	Hybrid	9

Apply Reset

Parameter description:

- **Ethertype for Custom S-ports :**

This field specifies the ether type used for Custom S-ports while s-custom-port enabled. This is a global setting for all the Custom S-ports. Custom Ether type enables the user to change the Ether type value on a port to any value in order to support network devices which do not use the standard 0x8100 Ether type field value on 802.1Q-tagged or 802.1p-tagged frames.

- **Port :**

Indicate the port number of each port.

- **Port Type :**

Port can be one of the following types: Unaware, C-port, S-port, and S-custom-port.

	Ingress action	Egress action
Unaware	<p>When the port received untagged frames, an untagged frame obtain a tag (based on PVID) and is forwarded.</p> <p>When the port received tagged frames : No matter which is TPID value, it will add one outer tag that is PVID , and is forwarded.</p>	<p>The TPID of frame transmitted by Unaware port will be set to 0x8100. The final status of the frame after egressing are also effected by Egress Rule.</p>
C-port	<p>When the port received untagged frames, an untagged frame obtain a tag (based on PVID) and is forwarded.</p> <p>When the port received tagged frames : 1. if an tagged frame with TPID=0x8100, it is forwarded. (not add tag) 2. if an tagged frame with TPID is not 0x8100, and not 0x88a8 , and not Ethertype , it is forwarded.(will add one outer tag that is PVID) 3. if the TPID of tagged frame is 0x88A8 or Ethertype, it will be discarded.</p>	<p>The TPID of frame transmitted by C-port will be set to 0x8100.</p>
S-port	<p>When the port received untagged frames, an untagged frame obtain a tag (based on PVID) and is forwarded.</p> <p>When the port received tagged frames: 1. Only the TPID of tagged frame is 0x8100, it will be discarded, others TPID will be forwarded. 2. This mode will not add tag.</p>	<p>The TPID of frame transmitted by S-port will be set to 0x88A8.</p>
S-custom-port	<p>When the port received untagged frames, an untagged frame obtain a tag (based on PVID) and is forwarded.</p> <p>When the port received tagged frames : 1. Only the TPID of tagged frame is either 0x88a8 or Ethertype for Customer S-ports will be forwarded, others will be discarded. 2. This mode will not add tag.</p>	<p>The TPID of frame transmitted by S-custom-port will be set to an self-customized value, which can be set by the user using the column of Ethertype for Custom S-ports.</p>

- **Ingress Filtering :**

Enable ingress filtering on a port by ticking the box. If ingress filtering is enabled and the ingress port is not a member of the classified VLAN group of the frame, the frame is discarded (Do not forward).

If ingress filtering is disabled and the ingress port is not a member of the classified VLAN group of the frame, however, the frame is still forwarded.

By default, ingress filtering is disabled (untick).

- **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.

- **Egress Rule :**

Determines what device the port connect to. If the port connect to VLAN-unaware devices, such as terminal/work station, Access link should be used. If the port connect to VLAN-aware devices, for example, switch connect to switch, Trunk link should be used. Hybrid link is used for more flexible application.

Hybrid : If the tag of tagged frame is as the same as PVID, the tag of the frame will be removed. The frame become an untagged frame and transmitted.

Any other tagged frame whose tag value is different from PVID are transmitted directly.

Trunk : all tagged frames with any tag value are transmitted.

Access : The tag of any tagged frame will be removed to become an untagged frame. These untagged frames will be transmitted.

- **PVID :**

Configures the Port VLAN identifier. The allowed values are 1 through 4094. The default value is 1.

When the port received a untagged frame, the port will give a tag to it based on the value of PVID, and the frame become tagged frame.



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

3-6.3 Switch Status

The function Switch Status gathers the information of all VLAN status and reports it by the order of Static NAS MVRP MVP Voice VLAN MSTP GVRP Combined.

Web Interface

To Display VLAN membership status in the web interface:

1. Click VLAN membership.
2. Specify the Static NAS MVRP MVP Voice VLAN MSTP GVRP Combined.
3. Display membership information.

Figure 3-6.3: The VLAN Membership Status for Static user

VLAN ID	Port Members																	
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
2	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
7	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Parameter description:

VLAN USER (You can scroll to select one kind VLAN user as below:)

VLAN User module uses services of the VLAN management functionality to configure VLAN memberships and VLAN port configurations such as PVID and UVID. Currently we support the following VLAN user types:

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.

MVRP : Multiple VLAN Registration Protocol (MVRP) allows dynamic registration and deregistration of VLANs on ports on a VLAN bridged network.

GVRP : GARP VLAN Registration Protocol (GVRP) allows dynamic registration and deregistration of VLANs on ports on a VLAN bridged network.

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.

- **VLAN ID** :

Indicates the ID of this particular VLAN.

- **VLAN Membership** :

The VLAN Membership Status Page shall show the current VLAN port members for all VLANs configured by a selected VLAN User (selection shall be allowed by a Combo Box). When ALL VLAN Users are selected, it shall show this information for all the VLAN Users, and this is by default. VLAN membership allows the frames classified to the VLAN ID to be forwarded on the respective VLAN member ports.

- **Auto-refresh :**
To evoke the auto-refresh icon then the device will refresh the information automatically.
- **Upper right icon (Refresh):**
You can click them for refresh the VLAN entries by manual.

3-6.4 Port Status

The function Port Status gathers the information of all VLAN status and reports it by the order of Static NAS MVRP MVP Voice VLAN MSTP GVRP Combined.

Web Interface

To Display VLAN Port Status in the web interface:

1. Click VLAN Port Status.
2. Specify the Static NAS MVRP MVP Voice VLAN MSTP GVRP Combined.
3. Display Port Status information.

Figure 3-6.4: The VLAN Port Status for Static user

Port	PVID	Port Type	Ingress Filtering	Frame Type	Tx Tag	VID	Conflicts
1	1	UnAware	Disabled	All	Static	1	No
2	1	UnAware	Disabled	All	NAS	1	No
3	2	UnAware	Disabled	All	GVRP	2	No
4	2	UnAware	Disabled	All	MVR	2	No
5	3	UnAware	Disabled	All	Voice VLAN	3	No
6	3	UnAware	Disabled	All	MSTP	3	No
7	4	UnAware	Disabled	All	VCL	4	No
8	4	UnAware	Disabled	All	Untag_this	4	No
9	5	UnAware	Disabled	All	Untag_this	5	No
10	5	UnAware	Disabled	All	Untag_this	5	No
11	6	UnAware	Disabled	All	Untag_this	6	No
12	6	UnAware	Disabled	All	Untag_this	6	No
13	7	UnAware	Disabled	All	Untag_this	7	No
14	7	UnAware	Disabled	All	Untag_this	7	No
15	8	UnAware	Disabled	All	Untag_this	8	No
16	8	UnAware	Disabled	All	Untag_this	8	No
17	9	UnAware	Disabled	All	Untag_this	9	No
18	9	UnAware	Disabled	All	Untag_this	9	No

Parameter description:

- **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.

- **Auto-refresh :**
To evoke the auto-refresh icon then the device will refresh the information automatically.

- **Upper right icon (Refresh):**
You can click them for refresh the VLAN Port Status information by manual.

3-6.5 Private VLANs

In a private VLAN, communication between ports in that private VLAN is not permitted. A VLAN can be configured as a private VLAN.

3-6.5.1 Private VLANs Membership

The Private VLAN membership configurations for the switch can be monitored and modified here. Private VLANs can be added or deleted here. Port members of each Private VLAN can be added or removed here. Private VLANs are based on the source port mask, and there are no connections to VLANs. This means that VLAN IDs and Private VLAN IDs can be identical. A port must be a member of both a VLAN and a Private VLAN to be able to forward packets. By default, all ports are VLAN unaware and members of VLAN 1 and Private VLAN 1. A VLAN unaware port can only be a member of one VLAN, but it can be a member of multiple Private VLANs.

Web Interface

To configure Private VLAN configuration in the web interface:

1. Click add new Private VLAN configuration
2. Specify the Private VLAN ID and Port Members
3. Click Apply.

Figure 3-6.5.1: The Private VLAN Membership Configuration

Delete	PVLAN ID	Port Members																	
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
<input type="checkbox"/>	1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Add New Private VLAN

Apply Reset

Parameter description:

- **Delete :**
To delete a private VLAN entry, check this box. The entry will be deleted during the next save.
- **Private VLAN ID :**
Indicates the ID of this particular private VLAN.
- **Port Members :**
A row of check boxes for each port is displayed for each private VLAN ID. To include a port in a Private VLAN, check the box. To remove or exclude the port from the Private VLAN, make sure the box is unchecked. By default, no ports are members, and all boxes are unchecked.
- **Adding a New Private VLAN :**
Click to add a new private VLAN ID. An empty row is added to the table, and the private VLAN can be configured as needed.
- **Buttons:**
Apply – Click to save changes.
Reset- Click to undo any changes made locally and revert to previously saved values.

3-6.5.2 Port Isolation

Port Isolation provides for an apparatus and method to isolate ports on layer 2 switches on the same VLAN to restrict traffic flow. The apparatus comprises a switch having said plurality of ports, each port configured as a protected port or a non-protected port. An address table memory stores an address table having a destination address and port number pair. A forwarding map generator generates a forwarding map which is responsive to a destination address of a data packet. The method for isolating ports on a layer 2 switch comprises configuring each of the ports on the layer 2 switch as a protected port or a non-protected port. A destination address on an data packet is matched with a physical address on said layer 2 switch and a forwarding map is generated for the data packet based upon the destination address on the data packet. The data packet is then sent to the plurality of ports pursuant to the forwarding map generated based upon whether the ingress port was configured as a protected or non-protected port.

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 and Private VLAN.

Web Interface

To configure Port Isolation configuration in the web interface:

1. Click VLAN, Port Isolation.
2. Evoke which port want to enable Port Isolation
3. Click Apply.

Figure 3-6.5.2: The Port Isolation Configuration

Port Isolation Configuration																	
Port Number																	
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Apply Reset

Parameter description:

- **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:**

Apply – Click to save changes.

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

3-6.6 MAC-based VLAN

MAC address-based VLAN decides the VLAN for forwarding an untagged frame based on the source MAC address of the frame.

A most common way of grouping VLAN members is by port, hence the name port-based VLAN. Typically, the device adds the same VLAN tag to untagged packets that are received through the same port. Later on, these packets can be forwarded in the same VLAN. Port-based VLAN is easy to configure, and applies to networks where the locations of terminal devices are relatively fixed. As mobile office and wireless network access gain more popularity, the ports that terminal devices use to access the networks are very often non-fixed. A device may access a network through Port A this time, but through Port B the next time. If Port A and Port B belong to different VLANs, the device will be assigned to a different VLAN the next time it accesses the network. As a result, it will not be able to use the resources in the old VLAN. On the other hand, if Port A and Port B belong to the same VLAN, after terminal devices access the network through Port B, they will have access to the same resources as those accessing the network through Port A do, which brings security issues. To provide user access and ensure data security in the meantime, the MAC-based VLAN technology is developed.

MAC-based VLANs group VLAN members by MAC address. With MAC-based VLAN configured, the device adds a VLAN tag to an untagged frame according to its source MAC address. MAC-based VLANs are mostly used in conjunction with security technologies such as 802.1X to provide secure, flexible network access for terminal devices.

3-6.6.1 Configuration

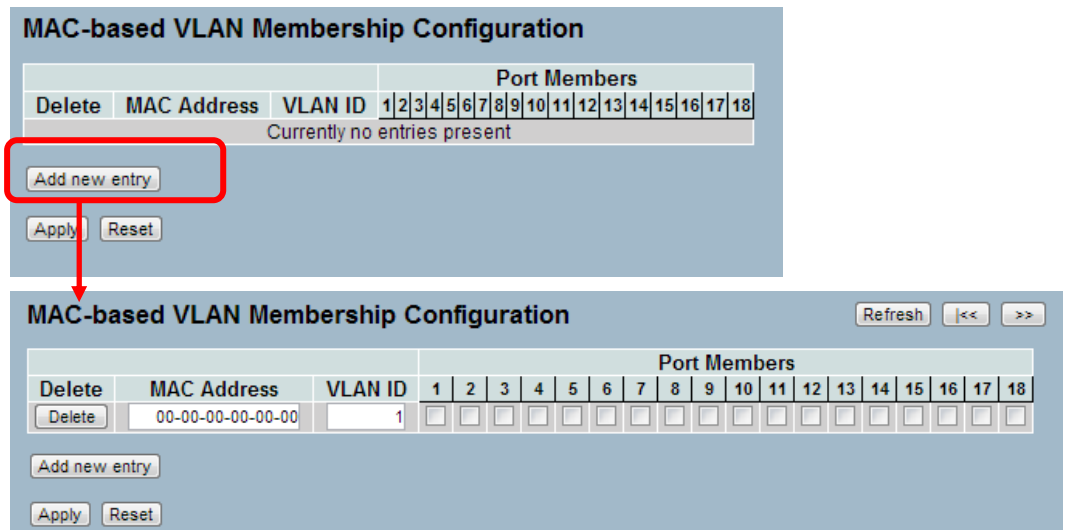
The MAC-based VLAN entries can be configured here. This page allows for adding and deleting MAC-based VLAN entries and assigning the entries to different ports. This page shows only static entries.

Web Interface

To configure MAC address-based VLAN configuration in the web interface:

1. Click MAC address-based VLAN configuration and add new entry.
2. Specify the MAC address and VLAN ID.
3. Click Apply.

Figure 3-6.6.1: The MAC-based VLAN Membership Configuration



Parameter description:

- **Delete :**
To delete a MAC-based VLAN entry, check this box and press save. The entry will be deleted on the selected switch.
- **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 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 switch unit when you click on "Save". A MAC-based VLAN without any port members on any unit will be deleted when you click "Save".
The button can be used to undo the addition of new MAC-based VLANs.
- **Buttons:**
 - Apply** – Click to save changes.
 - Reset-** Click to undo any changes made locally and revert to previously saved values.

3-6.6.2 Status

This section shows MAC-based VLAN entries configured by various MAC-based VLAN users. Currently we support following VLAN User types:

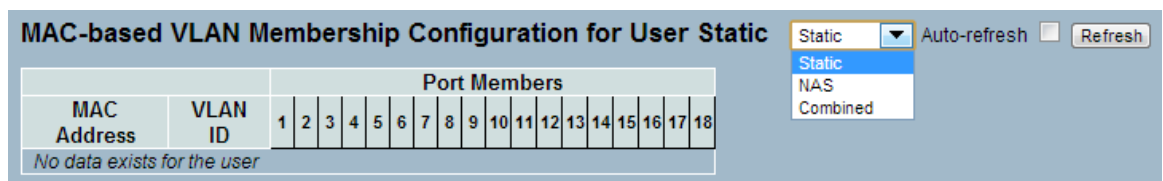
NAS : NAS provides port-based authentication, which involves communications between a Supplicant, Authenticator, and an Authentication Server.

Web Interface

To Display MAC-based VLAN configured in the web interface:

1. Click MAC-based VLAN Status.
2. Specify the Static NAS Combined.
3. Display MAC-based information.

Figure 3-6.6.2: The MAC-based VLAN Membership Status for User Static



MAC Address	VLAN ID	Port Members																	
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
No data exists for the user																			

Parameter description:

- **MAC Address :**
Indicates the MAC address.
- **VLAN ID :**
Indicates the VLAN ID.
- **Port Members :**
Port members of the MAC-based VLAN entry.
- **Auto-refresh :**
To evoke the auto-refresh icon then the device will refresh the information automatically.
- **Upper right icon (Refresh):**
You can click them for refresh the MAC-based VLAN Membership information by manual.

3-6.7 Protocol -based VLAN

This section describe Protocol -based VLAN, The Switch support Protocol include Ethernet LLC SNAP Protocol, LLC

The Logical Link Control (LLC) data communication protocol layer is the upper sub-layer of the Data Link Layer (which is itself layer 2, just above the Physical Layer) in the seven-layer OSI reference model. It provides multiplexing mechanisms that make it possible for several network protocols (IP, IPX, Decnet and Appletalk) to coexist within a multipoint network and to be transported over the same network media, and can also provide flow control and automatic repeat request (ARQ) error management mechanisms.

SNAP

The Subnetwork Access Protocol (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 spaces. It is used with IEEE 802.3, IEEE 802.4, IEEE 802.5, IEEE 802.11 and other IEEE 802 physical network layers, as well as with non-IEEE 802 physical network layers such as FDDI that use 802.2 LLC.

3-6.7.1 Protocol to Group

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 switch.

Web Interface

To configure Protocol -based VLAN configuration in the web interface:

1. Click Protocol -based VLAN configuration and add new entry.
2. Specify the Ethernet LLC SNAP Protocol and Group Name.
3. Click Apply.

Figure 3-6.7.1: The Protocol to Group Mapping Table

The screenshot shows two states of the 'Protocol to Group Mapping Table' web interface. The top state shows a table with columns 'Delete', 'Frame Type', 'Value', and 'Group Name', and a message 'No Group entry found!'. A red box highlights the 'Add new entry' button, with a red arrow pointing down to the bottom state. The bottom state shows the same table with a single entry: 'Delete' (checkbox), 'Frame Type' (dropdown menu set to 'Ethernet'), 'Value' (text field containing 'Etype: 0x0800'), and 'Group Name' (empty text field). The 'Add new entry' button is still present below the table.

Parameter description:

- **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 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 button can be used to undo the addition of new entry.

- **Buttons:**

Save – Click to save changes.

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

- **Upper right icon (Refresh):**

You can click them for refresh the Protocol Group Mapping information by manual.

3-6.7.2 Group to VLAN

This section allows you to map a already configured Group Name to a VLAN for the selected switch.

Web Interface

To Display Group Name to VLAN mapping table configured in the web interface:

1. Click Group Name VLAN configuration and add new entry.
2. Specify the Group Name and VLAN ID.
3. Click Save.

Figure 3-6.7.2: The Group Name of VLAN Mapping Table

Group Name to VLAN mapping Table

			Port Members																	
Delete	Group Name	VLAN ID	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
No Group entries																				

Group Name to VLAN mapping Table Auto-refresh

			Port Members																	
Delete	Group Name	VLAN ID	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
<input type="button" value="Delete"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Parameter description:

- **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 of at 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 perused 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 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 button can be used to undo the addition of new entry.
- **Buttons:**
 - Save** – Click to save changes.
 - Reset**- Click to undo any changes made locally and revert to previously saved values.
- **Auto-refresh :**
To evoke the auto-refresh icon then the device will refresh the information automatically.
- **Upper right icon (Refresh):**
You can click them for refresh the Protocol Group Mapping information by manual.

3-6.8 IEEE 802.1QinQ (double-tag) configuration

Service providers can use Q-in-Q to transparently pass Layer 2 VLAN traffic from a customer site, through the service provider network, to another customer site without removing or changing the customer VLAN tags

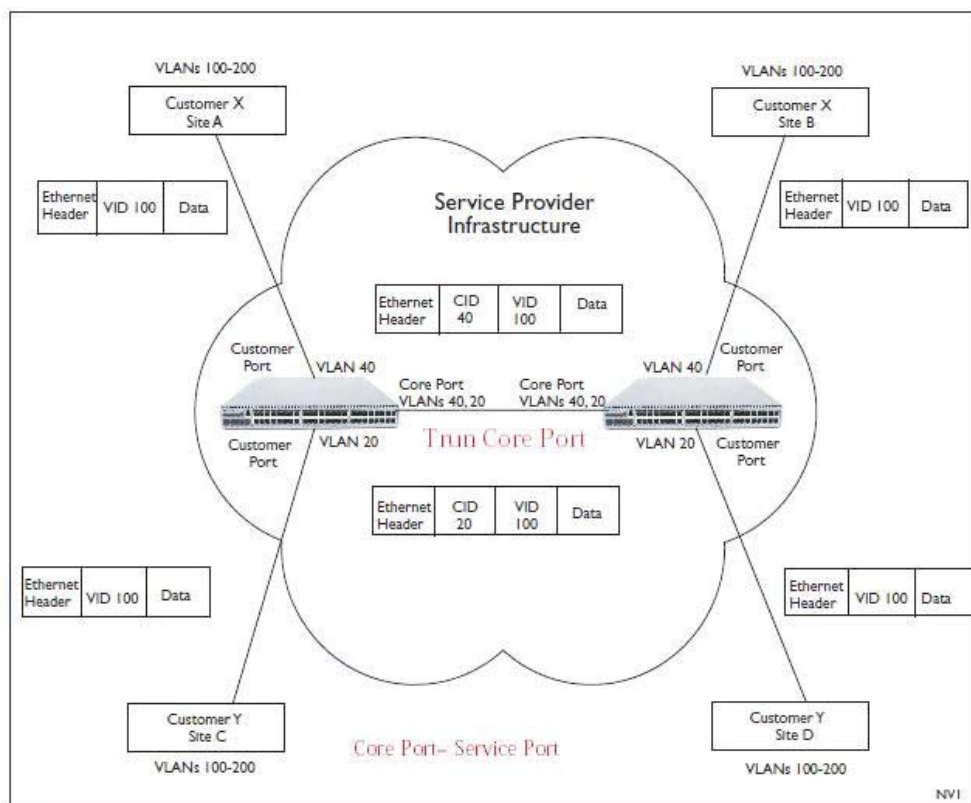
The double Q-in-Q tags can indicate different information, the inner tag indicates the user, the outer tag indicates carrier provider, the Q-in-Q packet with two tags can traverse the carrier's network and the inner tag is transmitted transparently.

Scenario :

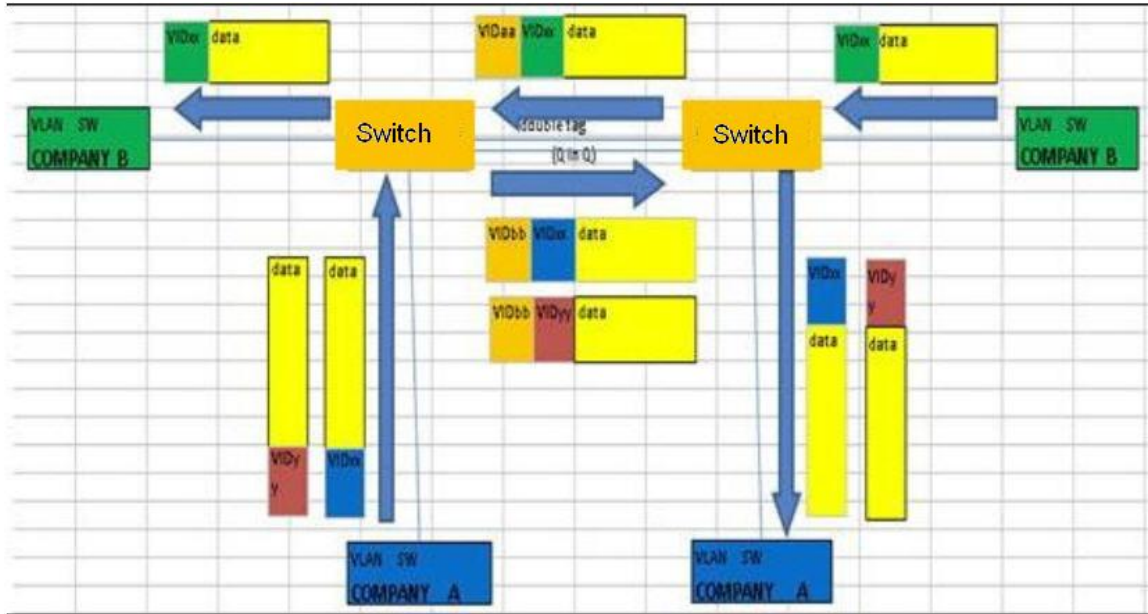
Switch will be used for Leased Line Service.

They are already using Tag VLAN (802.1q), so they would like to add another Tag without changing existing VLAN.

Typical Application :



An abstract illustration to above application :



Configure Steps :

Step 1: Create VLAN 20 and VLAN 40

Configure Port 3 .Port 4 and Port 8 are belong to VLAN 20
 Configure Port 1 .Port 2 and Port 8 are belong to VLAN 40
 Port 8 is uplink port .

The above setting is configured at SW1(Left side) and SW2(Right side).

VLAN Membership Configuration Refresh << >>

Start from VLAN with entries per page.

Delete	VLAN ID	VLAN Name	Port Members																	
			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
<input type="checkbox"/>	1	default	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	20	v20	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	40	v40	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Step 2 : Configure PVID

Port1 and Port2 are PVID=40 and their port role are VLAN access mode .
 Port3 and Port4 are PVID=20 and their port role are VLAN access mode .
 The port role of Port 8 is VLAN trunk mode.

Step 3 : Configure Port Type to “Unaware“ at Port1 ~ Port 4.

Step 4 : Configure Port Type to “S-Port“ at Port 8.

(The uplink port, port 8, can be set as C-Port or S-Port. The uplink port on the both switches must be set the same Type. We set S-Port to S-Port as example.)

Q in Q belong to the tag-based mode, however, it would treat all frames as the untagged ones, which means that tag with PVID will be added into all packets. Then,

these packets will be forwarded as Tag-based VLAN. So, the incoming packets with tag will become the double-tag ones.

Ethertype for Custom S-ports 0x

VLAN Port Configuration

Port	Port Type	Ingress Filtering	Frame Type	Egress Rule	PVID
*	<input type="text" value="⊞"/>	<input type="checkbox"/>	<input type="text" value="⊞"/>	<input type="text" value="⊞"/>	
1	Unaware	<input type="checkbox"/>	All	Access	1
2	Unaware	<input type="checkbox"/>	All	Access	1
3	Unaware	<input type="checkbox"/>	All	Access	1
4	Unaware	<input type="checkbox"/>	All	Access	1
5	Unaware	<input type="checkbox"/>	All	Hybrid	1
6	Unaware	<input type="checkbox"/>	All	Hybrid	1
7	Unaware	<input type="checkbox"/>	All	Hybrid	1
8	Unaware	<input type="checkbox"/>	All	Trunk	1
9	Unaware	<input type="checkbox"/>	All	Hybrid	1
10	Unaware	<input type="checkbox"/>	All	Hybrid	1

3-7 QoS

The switch support four QoS queues per port with strict or weighted fair queuing scheduling. It supports QoS Control Lists (QCL) for advance programmable QoS classification, based on IEEE 802.1p, Ethertype, VID, IPv4/IPv6 DSCP and UDP/TCP ports and ranges.

High flexibility in the classification of incoming frames to a QoS class. The QoS classification looks for information up to Layer 4, including IPv4 and IPv6 DSCP, IPv4 TCP/UDP port numbers, and user priority of tagged frames. This QoS classification mechanism is implemented in a QoS control list (QCL). The QoS class assigned to a frame 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.

The switch support advanced memory control mechanisms providing excellent performance of all QoS classes under any traffic scenario, including jumbo frame. A super priority queue with dedicated memory and strict highest priority in the arbitration. The ingress super priority queue allows traffic recognized as CPU traffic to be received and queued for transmission to the CPU even when all the QoS class queues are congested.

3-7.1 Port Classification

The section allows you to configure the basic QoS Ingress Classification settings for all switch ports. and the settings relate to the currently selected unit, as reflected by the page header.

Web Interface

To configure the QoS Port Classification parameters in the web interface:

1. Click Configuration, QoS, Port Classification
2. Scroll to select QoS class, DP Level, PCP and DEI parameters
3. Click the Apply to save the setting
4. If you want to cancel the setting then you need to click the Reset button.
It will revert to previously saved values

Figure 3-7.1: The QoS Configuration

QoS Ingress Port Classification						
Port	QoS class	DP level	PCP	DEI	Tag Class.	DSCP Based
*	<> v	<> v	<> v	<> v		<input type="checkbox"/>
1	0 v	0 v	0 v	0 v	Disabled	<input type="checkbox"/>
2	0 v	0 v	0 v	0 v	Disabled	<input type="checkbox"/>
3	0 v	0 v	0 v	0 v	Disabled	<input type="checkbox"/>
4	0 v	0 v	0 v	0 v	Disabled	<input type="checkbox"/>
5	0 v	0 v	0 v	0 v	Disabled	<input type="checkbox"/>
6	0 v	0 v	0 v	0 v	Disabled	<input type="checkbox"/>
7	0 v	0 v	0 v	0 v	Disabled	<input type="checkbox"/>
8	0 v	0 v	0 v	0 v	Disabled	<input type="checkbox"/>
9	0 v	0 v	0 v	0 v	Disabled	<input type="checkbox"/>
10	0 v	0 v	0 v	0 v	Disabled	<input type="checkbox"/>
11	0 v	0 v	0 v	0 v	Disabled	<input type="checkbox"/>
12	0 v	0 v	0 v	0 v	Disabled	<input type="checkbox"/>
13	0 v	0 v	0 v	0 v	Disabled	<input type="checkbox"/>
14	0 v	0 v	0 v	0 v	Disabled	<input type="checkbox"/>
15	0 v	0 v	0 v	0 v	Disabled	<input type="checkbox"/>
16	0 v	0 v	0 v	0 v	Disabled	<input type="checkbox"/>
17	0 v	0 v	0 v	0 v	Disabled	<input type="checkbox"/>
18	0 v	0 v	0 v	0 v	Disabled	<input type="checkbox"/>

Apply Reset

Parameter description:

- **Port :**
The port number for which the configuration below applies.
- **QoS class :**
Controls the default QoS class, i.e., the QoS class for frames not classified in any other way. There is a one to one mapping between QoS class, queue and priority. A QoS class of 0 (zero) has the lowest priority.
- **DP level :**
Controls the default DP level, i.e., the DP level for frames not classified in any other way.
- **PCP :**
Controls the default PCP for untagged frames.
- **DEI :**
Controls the default DEI for untagged frames.
- **Tag Class. :**
Shows the classification mode for tagged frames on this port.
Disabled: Use default QoS class and DP level for tagged frames.
Enabled: Use mapped versions of PCP and DEI for tagged frames.
Click on the mode in order to configure the mode and/or mapping.
- **DSCP Based :**
Click to Enable DSCP Based QoS Ingress Port Classification.
- **Buttons:**
Apply – Click to save changes.
Reset- Click to undo any changes made locally and revert to previously saved values.



NOTE: DP 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.

PCP : PCP is an acronym for Priority Code Point. It is a 3-bit field storing the priority level for the 802.1Q frame.

DEI : DEI is an acronym for Drop Eligible Indicator. It is a 1-bit field in the VLAN tag.

Actual PCP is Pri column in Vlan tag packet , DEI is cfi column

PCP value from 0~7 , it can be used for priority definition .
DEI value is 0 or 1 , it is settable , map to DP value is 0 or 1. When ingress Qos class value is the same , then through DP level value to define the priority , DP value larger will be dropped first.

ex: From Port 1 input 1G Pkts , Egress Port 7 Rate be set with 500M . Port 1 Pkts will includes two kinds packet:

a. PCP & DEI = 0 0 , via configured map to Qos class & DP level = 1 , 0

b. PCP & DEI = 0 1 , via configured map to Qos class & DP level = 1 , 1

Result will find (a) Packet all past, and (b) packets all drop

3-7.2 Port Scheduler

This section provides an overview of QoS Egress Port Schedulers for all switch ports. and the ports belong to the currently selected unit, as reflected by the page header.

Web Interface

To display the QoS Port Schedulers in the web interface:

1. Click Configuration, QoS, Port Schedulers
2. Display the QoS Egress Port Schedulers

Figure 3-7.2: The QoS Egress Port Schedules

The figure illustrates the configuration of QoS Egress Port Schedulers. It is divided into two main sections:

Top Section: QoS Egress Port Schedulers Table

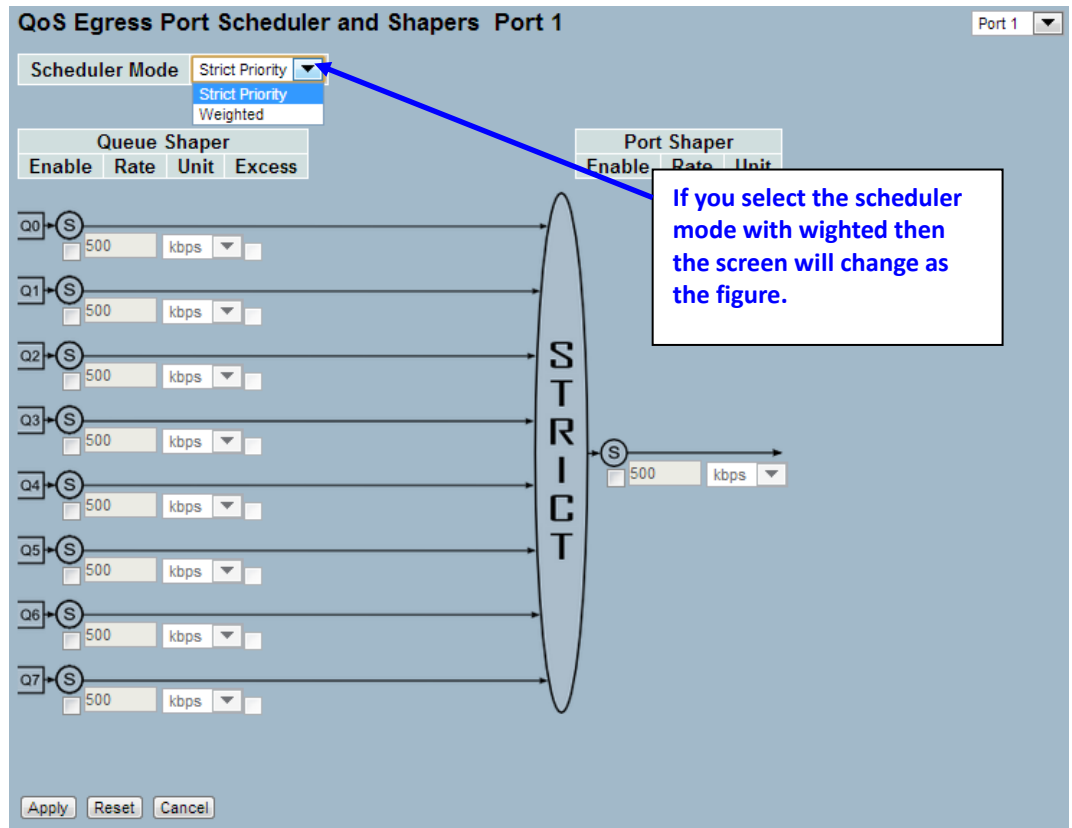
Port	Mode	Weight			
		Q0	Q1	Q2	Q3
1	Strict Priority	-	-	-	-
2	Strict Priority	-	-	-	-
3	Strict Priority	-	-	-	-
4	Strict Priority	-	-	-	-
5	Strict Priority	-	-	-	-
6	Strict Priority	-	-	-	-
7	Strict Priority	-	-	-	-
8	Strict Priority	-	-	-	-
9	Strict Priority	-	-	-	-
10	Strict Priority	-	-	-	-
11	Strict Priority	-	-	-	-
12	Strict Priority	-	-	-	-
13	Strict Priority	-	-	-	-
14	Strict Priority	-	-	-	-
15	Strict Priority	-	-	-	-
16	Strict Priority	-	-	-	-
17	Strict Priority	-	-	-	-
18	Strict Priority	-	-	-	-

A red box highlights the 'Port' column, and a red arrow points from the '1' in the first row to the detailed configuration view below. A blue callout box with an arrow pointing to the 'Port' column contains the text: "Click the Port index to set the QoS Egress Port Schedulers".

Bottom Section: QoS Egress Port Scheduler and Shapers Port 1

This section shows the configuration for Port 1. The Scheduler Mode is set to "Strict Priority". The Port Shaper is also configured with a rate of 500 kbps. The Queue Shaper section shows 8 queues (Q0-Q7) with a rate of 500 kbps each. The output is labeled "STRICT".

Buttons: Apply, Reset, Cancel



Parameter description:

- **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.
- **Weight (Qn) :**
Shows the weight for this queue and port.
- **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 ?. This value is restricted to ?-1000000 when the "Unit" is "kbps", and it is restricted to 1-? 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 ?. This value is restricted to ?-1000000 when the "Unit" is "kbps", and it is restricted to 1-? 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:**
 - Apply** – Click to save changes.
 - Reset**- Click to undo any changes made locally and revert to previously saved values.

3-7.3 Port Shaping

This section provides an overview of QoS Egress Port Shaping for all switch ports. Others the user could get all detail information of the ports belong to the currently selected unit, as reflected by the page header.

Web Interface

To display the QoS Port Shapers in the web interface:

1. Click Configuration, QoS, Port Shapers
2. Display the QoS Egress Port Shapers

Figure 3-7.3: The QoS Egress Port Shapers

The screenshot displays the 'QoS Egress Port Shapers' configuration page. At the top, a table lists ports 1 through 8, with columns for Q0, Q1, Q2, and Q3. All entries are 'disabled'. A red box highlights port 2, and a red arrow points from it to the detailed configuration view below. A blue callout box points to the 'Port' column header with the text 'Click the Port index to set the QoS Egress Port Shapers'.

Port	Q0	Q1	Q2	Q3
1	disabled	disabled	disabled	disabled
2	disabled	disabled	disabled	disabled
3	disabled	disabled	disabled	disabled
4	disabled	disabled	disabled	disabled
5	disabled	disabled	disabled	disabled
6	disabled	disabled	disabled	disabled
7	disabled	disabled	disabled	disabled
8	disabled	disabled	disabled	disabled

QoS Egress Port Scheduler and Shapers Port 1

Scheduler Mode: **Strict Priority** (Selected)
Strict Priority
Weighted

Queue Shaper				Port Shaper		
Enable	Rate	Unit	Excess	Enable	Rate	Unit
<input type="checkbox"/>	500	kbps	<input type="text"/>	<input type="checkbox"/>	500	kbps
<input type="checkbox"/>	500	kbps	<input type="text"/>	<input type="checkbox"/>	500	kbps
<input type="checkbox"/>	500	kbps	<input type="text"/>	<input type="checkbox"/>	500	kbps
<input type="checkbox"/>	500	kbps	<input type="text"/>	<input type="checkbox"/>	500	kbps
<input type="checkbox"/>	500	kbps	<input type="text"/>	<input type="checkbox"/>	500	kbps
<input type="checkbox"/>	500	kbps	<input type="text"/>	<input type="checkbox"/>	500	kbps
<input type="checkbox"/>	500	kbps	<input type="text"/>	<input type="checkbox"/>	500	kbps

Buttons: Apply, Reset, Cancel

QoS Egress Port Scheduler and Shapers Port 1 Port 1 ▼

Scheduler Mode: Strict Priority ▼
Strict Priority
Weighted

Queue Shaper				Port Shaper		
Enable	Rate	Unit	Excess	Enable	Rate	Unit
<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	<input type="checkbox"/>		
<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	<input type="checkbox"/>		
<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	<input type="checkbox"/>		
<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	<input type="checkbox"/>		
<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	<input type="checkbox"/>		
<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	<input type="checkbox"/>		
<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	<input type="checkbox"/>		
<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	<input type="checkbox"/>		

S
T
R
I
C
T

500 kbps ▼

Apply Reset Cancel

If you select the scheduler mode with wighted then the screen will change as the figure.

Parameter description:

- **Port :**
The logical port for the settings contained in the same row. Click on the port number in order to configure the shapers.
- **Shapers (Qn) :**
Shows "disabled" or actual queue shaper rate - e.g. "800 Mbps".
- **Shapers (Port) :**
Shows "disabled" or actual port shaper rate - e.g. "800 Mbps".
- **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 ?. This value is restricted to ?-1000000 when the "Unit" is "kbps", and it is restricted to 1-? 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 ?. This value is restricted to ?-1000000 when the "Unit" is "kbps", and it is restricted to 1-? 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:**
Apply – Click to save changes.
Reset- Click to undo any changes made locally and revert to previously saved values.

3-7.4 QoS Control List Configuration

The section shows the QoS Control List(QCL), which is made up of the QCEs. Each row describes a QCE that is defined. The maximum number of QCEs is 256 on each switch. Click on the lowest plus sign to add a new QCE to the list.

Web Interface

To configure the QoS Control List parameters in the web interface:


1. Click Configuration, QoS, QoS Control List
2. Click the  to add a new QoS Control List
3. Scroll all parameters and evoke the Port Member to join the QCE rules
4. Click the save to save the setting
5. If you want to cancel the setting then you need to click the Reset button.
It will revert to previously saved values

Figure 3-7.4: The QoS Control List Configuration

Parameter description:

- **QCE# :**
Indicates the index of QCE.
- **Port :**
Indicates the list of ports configured with the QCE.
- **Frame Type :**
Indicates the type of frame to look for incoming frames. Possible frame types are:
Any: The QCE will match all frame type.
Ethernet: Only Ethernet frames (with Ether Type 0x600-0xFFFF) are allowed.
LLC: Only (LLC) frames are allowed.
SNAP: Only (SNAP) frames are allowed

IPv4: The QCE will match only IPV4 frames.

IPv6: The QCE will match only IPV6 frames.

- **SMAC :**

Displays the OUI field of Source MAC address, i.e. first three octet (byte) of MAC address.

- **DMAC :**

Specify the type of Destination MAC addresses for incoming frame. Possible values are:

Any: All types of Destination MAC addresses are allowed.

Unicast: Only Unicast MAC addresses are allowed.

Multicast: Only Multicast MAC addresses are allowed.

Broadcast: Only Broadcast MAC addresses are allowed.

The default value is 'Any'.

- **VID :**

Indicates (VLAN ID), either a specific VID or range of VIDs. VID can be in the range 1-4094 or 'Any'.

- **PCP :**

Priority Code Point: Valid value PCP are specific(0, 1, 2, 3, 4, 5, 6, 7) or range(0-1, 2-3, 4-5, 6-7, 0-3, 4-7) or 'Any'.

- **DEI :**

Drop Eligible Indicator: Valid value of DEI can be any of values between 0, 1 or 'Any'.

- **Action :**

Indicates the classification action taken on ingress frame if parameters configured are matched with the frame's content.

There are three action fields: Class, DPL and DSCP.

Class: Classified QoS Class; if a frame matches the QCE it will be put in the queue.

DPL: Classified Drop Precedence Level; if a frame matches the QCE then DP level will set to value displayed under DPL column.

DSCP: Classified DSCP value; If a frame matches the QCE then DSCP will be classified with the value displayed under DSCP column.

- **Modification Buttons :**

You can modify each QCE (QoS Control Entry) in the table using the following buttons:



: Inserts a new QCE before the current row.



: Edits the QCE.



: Moves the QCE up the list.



: Moves the QCE down the list.



: Deletes the QCE.



: The lowest plus sign adds a new entry at the bottom of the QCE listings.

Parameter description:

- **Port Members :**

Check the checkbox button in case you want to make any port member of the QCL entry. By default all ports will be checked

- **Key Parameters :**

Key configuration are described as below:

Tag: Value of Tag field can be 'Any', 'Untag' or 'Tag'

VID: Valid value of VLAN ID can be any value in the range 1-4095 or 'Any'; user can enter either a specific value or a range of VIDs

PCP: Priority Code Point: Valid value PCP are specific(0, 1, 2, 3, 4, 5, 6, 7) or range(0-1, 2-3, 4-5, 6-7, 0-3, 4-7) or 'Any'

DEI: Drop Eligible Indicator: Valid value of DEI can be any of values between 0, 1 or 'Any'

SMAC: Source MAC address: 24 MS bits (OUI) or 'Any'

DMAC Type: Destination MAC type: possible values are unicast(UC), multicast(MC), broadcast(BC) or 'Any'

Frame Type: Frame Type can have any of the following values

1. Any
2. Ethernet
3. LLC
4. SNAP
5. IPv4
6. IPv6



NOTE: All frame types are explained below:

1. Any : Allow all types of frames.

2. Ethernet : Ethernet Type Valid ethernet type can have value within 0x600-0xFFFF or 'Any', default value is 'Any'.

3. LLC: SSAP Address: Valid SSAP(Source Service Access Point) can vary from 0x00 to 0xFF or 'Any', the default value is 'Any'

DSAP Address: Valid DSAP(Destination Service Access Point) can vary from 0x00 to 0xFF or 'Any', the default value is 'Any'

Control: Address Valid Control Address can vary from 0x00 to 0xFF or 'Any', the default value is 'Any'

4. SNAP : PID: Valid PID(a.k.a ethernet type) can have value within 0x00-0xFFFF or 'Any', default value is 'Any'

5. IPv4 : Protocol: IP protocol number: (0-255, TCP or UDP) or 'Any'.

Source IP: Specific Source IP address in value/mask format or 'Any'. IP and Mask are in the format x.y.z.w where x, y, z, and w are decimal numbers between 0 and 255. When Mask is converted to a 32-bit binary string and read from left to right, all bits following the first zero must also be zero.

DSCP: Diffserv Code Point value(DSCP): It can be specific value, range of value or 'Any'. DSCP values are in the range 0-63 including BE, CS1-CS7, EF or AF11-AF43

IP Fragment: IPv4 frame fragmented option: yes|no|any

Sport: Source TCP/UDP port: (0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP

Dport: Destination TCP/UDP port: (0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP

6. IPv6 : Protocol: IP protocol number: (0-255, TCP or UDP) or 'Any'

Source IP: IPv6 source address: (a.b.c.d) or 'Any', 32 LS bits

DSCP: Diffserv Code Point value(DSCP): It can be specific value, range of value or 'Any'. DSCP values are in the range 0-63 including BE, CS1-CS7, EF or AF11-AF43

Sport: Source TCP/UDP port: (0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP

Dport: Destination TCP/UDP port: (0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP

- **Action Parameters :**

Class: QoS Class: "class (0-7)", default- basic classification

DP: Valid DP Level can be (0-3)", default- basic classification

DSCP: Valid dscp value can be (0-63, BE, CS1-CS7, EF or AF11-AF43)

- **Buttons:**

Apply– Click to apply the configuration and move to main QCL page.

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

Cancel–Return to the previous page without saving the configuration change.

3-7.5 QCL Status

The section will let you know how to configure and shows the QCL status by different QCL users. Each row describes the QCE that is defined. It is a conflict if a specific QCE is not applied to the hardware due to hardware limitations. The maximum number of QCEs is 256 on each switch.

Web Interface

To display the QoS Control List Status in the web interface:

1. Click Configuration, QoS , QCL Status
2. If you want to auto-refresh the information then you need to evoke the "Auto-refresh".
3. Scroll to select the combined, static, Voice VLAN and conflict.
4. To Click the " Refresh" to refresh a entry of the MVR Statistics Information.

Figure 3-7.5: The QoS Control List Status

User	QCE#	Frame Type	Port	Action			Conflict
				Class	DP	DSCP	
Static	2	Any	2-4,7,8,10A-10B	Class 2	Default	Default	No
Static	1	Any	5-10B	Class 0	Default	Default	No

Parameter description:

- **User :**
Indicates the QCL user.
- **QCE#**
Indicates the index of QCE.
- **Frame Type :**
Indicates the type of frame to look for incoming frames. Possible frame types are:
 - Any:** The QCE will match all frame type.
 - Ethernet:** Only Ethernet frames (with Ether Type 0x600-0xFFFF) are allowed.
 - LLC:** Only (LLC) frames are allowed
 - LLC:** Only (SNAP) frames are allowed.
 - IPv4:** The QCE will match only IPV4 frames.
 - IPv6:** The QCE will match only IPV6 frames.
- **Port :**
Indicates the list of ports configured with the QCE.

- **Action :**

Indicates the classification action taken on ingress frame if parameters configured are matched with the frame's content.

There are three action fields: Class, DPL and DSCP.

Class: Classified QoS Class; if a frame matches the QCE it will be put in the queue.

DPL: Drop Precedence Level; if a frame matches the QCE then DP level will set to value displayed under DPL column.

DSCP: If a frame matches the QCE then DSCP will be classified with the value displayed under DSCP column.

- **Conflict :**

Displays Conflict status of QCL entries. As H/W resources are shared by multiple applications. It may happen that resources required to add a QCE may not be available, in that case it shows conflict status as 'Yes', otherwise it is always 'No'. Please note that conflict can be resolved by releasing the H/W resources required to add QCL entry on pressing 'Resolve Conflict' button.

- **Buttons:**



– Select the QCL status from this drop down list.

Auto-refresh- Click to undo any changes made locally and revert to previously saved values.

Resolve Conflict– Click to release the resources required to add QCL entry, incase conflict status for any QCL entry is 'yes'.

Refresh– You can click them to refresh the QCL information by manual; any changes made locally will be undone.

3-8 Loop Protection

The loop protection is used to detect the presence of traffic. When switch receives packet's (looping protection frame) MAC address the same as oneself from port, Loop Protection happens. The port will be locked when it received the looping protection frames. If you want to resume the locked port, please find out the looping path and take off the looping path, then select the resume the locked port and click on "Resume" to turn on the locked ports.

3-8.1 Configuration

The section describes how to set Loop Protection.

Web Interface

To configure the Loop Protection parameters in the web interface:

1. Click Configuration, Loop Protection, Configuration
2. Evoke to select enable or disable the port loop Protection
5. Click the save to save the setting
6. If you want to cancel the setting then you need to click the Reset button.
It will revert to previously saved values

Figure 3-8.1: The Loop Protection Configuration.

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

Port Configuration			
Port	Enable	Action	Tx Mode
*	<input type="checkbox"/>	<>	<>
1	<input checked="" type="checkbox"/>	Shutdown Port	Enable
2	<input checked="" type="checkbox"/>	Shutdown Port	Enable
3	<input checked="" type="checkbox"/>	Shutdown Port	Enable
4	<input checked="" type="checkbox"/>	Shutdown Port	Enable
5	<input checked="" type="checkbox"/>	Shutdown Port	Enable
6	<input checked="" type="checkbox"/>	Shutdown Port	Enable
7	<input checked="" type="checkbox"/>	Shutdown Port	Enable
8	<input checked="" type="checkbox"/>	Shutdown Port	Enable
9	<input checked="" type="checkbox"/>	Shutdown Port	Enable
10	<input checked="" type="checkbox"/>	Shutdown Port	Enable
11	<input checked="" type="checkbox"/>	Shutdown Port	Enable
12	<input checked="" type="checkbox"/>	Shutdown Port	Enable
13	<input checked="" type="checkbox"/>	Shutdown Port	Enable
14	<input checked="" type="checkbox"/>	Shutdown Port	Enable
15	<input checked="" type="checkbox"/>	Shutdown Port	Enable
16	<input checked="" type="checkbox"/>	Shutdown Port	Enable
17	<input checked="" type="checkbox"/>	Shutdown Port	Enable
18	<input checked="" type="checkbox"/>	Shutdown Port	Enable

Apply Reset

Parameter description:

- **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 is to shut 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 No:**
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:**
 - Apply** – Click to save changes.
 - Reset-** Click to undo any changes made locally and revert to previously saved values.

3-8.2 Status

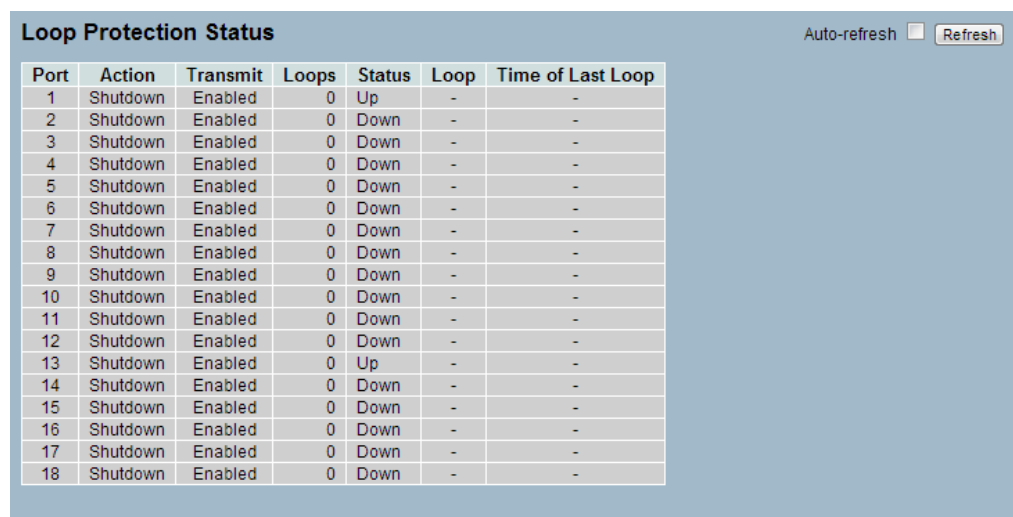
The section describes how to display the Loop Protection status what you set on the switch and the Loop protection status.

Web Interface

To display the Loop protection parameters in the web interface:

1. Click Configuration, Loop protection, Status
2. Evoke to select enable or disable the auto-refresh.
3. Click the refresh to clear or update the record of Loop protection.

Figure 3-8.2: The Loop Protection Status.



Port	Action	Transmit	Loops	Status	Loop	Time of Last Loop
1	Shutdown	Enabled	0	Up	-	-
2	Shutdown	Enabled	0	Down	-	-
3	Shutdown	Enabled	0	Down	-	-
4	Shutdown	Enabled	0	Down	-	-
5	Shutdown	Enabled	0	Down	-	-
6	Shutdown	Enabled	0	Down	-	-
7	Shutdown	Enabled	0	Down	-	-
8	Shutdown	Enabled	0	Down	-	-
9	Shutdown	Enabled	0	Down	-	-
10	Shutdown	Enabled	0	Down	-	-
11	Shutdown	Enabled	0	Down	-	-
12	Shutdown	Enabled	0	Down	-	-
13	Shutdown	Enabled	0	Up	-	-
14	Shutdown	Enabled	0	Down	-	-
15	Shutdown	Enabled	0	Down	-	-
16	Shutdown	Enabled	0	Down	-	-
17	Shutdown	Enabled	0	Down	-	-
18	Shutdown	Enabled	0	Down	-	-

Parameter description:

- **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.

3-9 Mirroring

You can mirror traffic from any source port to a target port for real-time analysis. You can then attach a logic analyzer or RMON probe to the target port and study the traffic crossing the source port in a completely unobtrusive manner.

Mirror Configuration is to monitor the traffic of the network. For example, we assume that Port A and Port B are Monitoring Port and Monitored Port respectively, thus, the traffic received by Port B will be copied to Port A for monitoring.

Web Interface

To configure the Mirror in the web interface:

1. Click Configuration, Mirroring
2. Scroll to select Port to mirror on which port
3. Scroll to disabled, enable, TX Only and RX Only to set the Port mirror mode
4. Click the save to save the setting
5. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values

Figure 3-9.1: The Mirror Configuration

Mirror Configuration

Port to mirror to: Disabled

Port	Mode
*	<>
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

Apply Reset

Parameter description:

- **Port to mirror on :**

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.

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 Tx frames on the mirror port. Because of this, mode for the selected mirror port is limited to Disabled or Rx only.

- **Buttons:**

Apply – Click to save changes.

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

3-10 Trap Event Severity

The function, is used to set a Alarm trap and get the Event log. The Trap Events Configuration function is used to enable the switch to send out the trap information while pre-defined trap events occurred.

Web Interface

To configure the Trap Event Severity Configuration in the web interface:

1. Click Configuration, Trap Event Severity Configuration
2. Scroll to select the Group name and Severity Level
3. Click the Apply to save the setting
4. If you want to cancel the setting then you need to click the Reset button.
It will revert to previously saved values

Figure 3-10.1: The Trap Event Severity Configuration

Group Name	Severity Level
Auth Failed	Warning
Cold Start	Warning
Config Info	Info
Firmware Upgrade	Info
Link Status	Warning
Login	Info
Logout	Info
Loop Protect	Info
Mgmt IP Change	Info
Module Change	Notice
NAS	Info
Password Change	Info
Port Security	Info
VLAN	Info
Warm Start	Warning

Apply Reset

Parameter description:

- **Group Name :**
The name identifying the severity group.
- **Severity Level :**
Scroll to select a severity level on each group. The following level types are supported:
 - <0> Emergency: System is unusable.
 - <1> Alert: Action must be taken immediately.
 - <2> Critical: Critical conditions.
 - <3> Error: Error conditions.

<4> **Warning:** Warning conditions.

<5> **Notice:** Normal but significant conditions.

<6> **Information:** Information messages.

<7> **Debug:** Debug-level messages.

- **Buttons:**

Apply – Click to save changes.

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

This chapter describes all of the switch security configuration tasks to enhance the security of local network including NAS, Port Security.

4-1 NAS

The section describes to configure the NAS parameters of the switch. The NAS server can be employed to connect users to a variety of resources including Internet access, conference calls, printing documents on shared printers, or by simply logging on to the Internet.

4-1.1 Configuration

This section describes how to configure NAS setting of IEEE 802.1X, MAC-based authentication system, and port settings. The NAS configuration consists of two sections, a system- and a port-wide.

Web Interface

To configure a System Configuration of Network Access Server in the web interface:

1. Select "Enabled" in the Mode of Network Access Server Configuration.
2. Checked Reauthentication Enabled.
3. Set Reauthentication Period (Default is 3600 seconds).
4. Set EAPOL Timeout (Default is 30 seconds).
5. Set Aging Period (Default is 300 seconds).
6. Set Hold Time (Default is 10 seconds).
7. Checked RADIUS-Assigned QoS Enabled.
8. Checked RADIUS-Assigned VLAN Enabled.
9. Checked Guest VLAN Enabled.
10. Specify Guest VLAN ID.
11. Specify Max. Reauth. Count.
12. Checked Allow Guest VLAN if EAPOL Seen.
13. Click Save.

Figure 4-1.1: The Network Access Server Configuration

Network Access Server Configuration		
System Configuration		
Mode	Disabled <input type="button" value="v"/>	
Reauthentication Enabled	<input type="checkbox"/>	
Reauthentication Period	3600	seconds
EAPOL Timeout	30	seconds
Aging Period	300	seconds
Hold Time	10	seconds

Port Configuration

Port	Admin State	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

Apply Reset

Parameter description:

- **Mode :**
Indicates if NAS is globally enabled or disabled on the switch. If globally disabled, all ports are allowed forwarding of frames.
- **Reauthentication Enabled :**
If checked, successfully authenticated supplicants/clients are reauthenticated after the interval specified by the Reauthentication Period. Reauthentication for 802.1X-enabled ports can be used to detect if a new device is plugged into a switch port or if a supplicant is no longer attached.

For MAC-based ports, reauthentication is only useful if the RADIUS server configuration has changed. It does not involve communication between the switch and the client, and therefore doesn't imply that a client is still present on a port (see Aging Period below).
- **Reauthentication Period :**
Determines the period, in seconds, after which a connected client must be reauthenticated. This is only active if the Reauthentication Enabled checkbox is checked. Valid values are in the range 1 to 3600 seconds.
- **EAPOL Timeout :**
Determines the time for retransmission of Request Identity EAPOL frames.
Valid values are in the range 1 to 255 seconds. This has no effect for MAC-based ports.
- **Aging Period :**
This setting applies to the following modes, i.e. modes using the Port Security functionality to secure MAC addresses:

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

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

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

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

- **Hold Time :**

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

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

If a client is denied access - either because the RADIUS server denies the client access or because the RADIUS server request times out (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 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.

- **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:

- **Port State :**

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

Globally Disabled: NAS is globally disabled.

Link Down: NAS is globally enabled, but there is no link on the port.

Authorized: The port is in Force Authorized or a single-supplicant mode and the supplicant is authorized.

Unauthorized: The port is in Force Unauthorized or a single-supplicant mode and the supplicant is not successfully authorized by the RADIUS server.

X Auth/Y Unauth: The port is in a multi-supplicant mode. Currently X clients are authorized and Y are unauthorized.

- **Restart :**

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

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

Reauthenticate: Schedules a reauthentication whenever the quiet-period of the port runs out (EAPOL-based authentication). For MAC-based authentication,

reauthentication will be attempted immediately.

The button only has effect for successfully authenticated clients on the port and will not cause the clients to get temporarily unauthorized.

Reinitialize: Forces a reinitialization of the clients on the port and thereby a reauthentication immediately. The clients will transfer to the unauthorized state while the reauthentication is in progress.

- **Buttons:**

- Save** – Click to save changes.

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

- **Upper right icon (Refresh):**

- You can click them for refresh the NAS Configuration by manual.

4-1.2 Switch Status

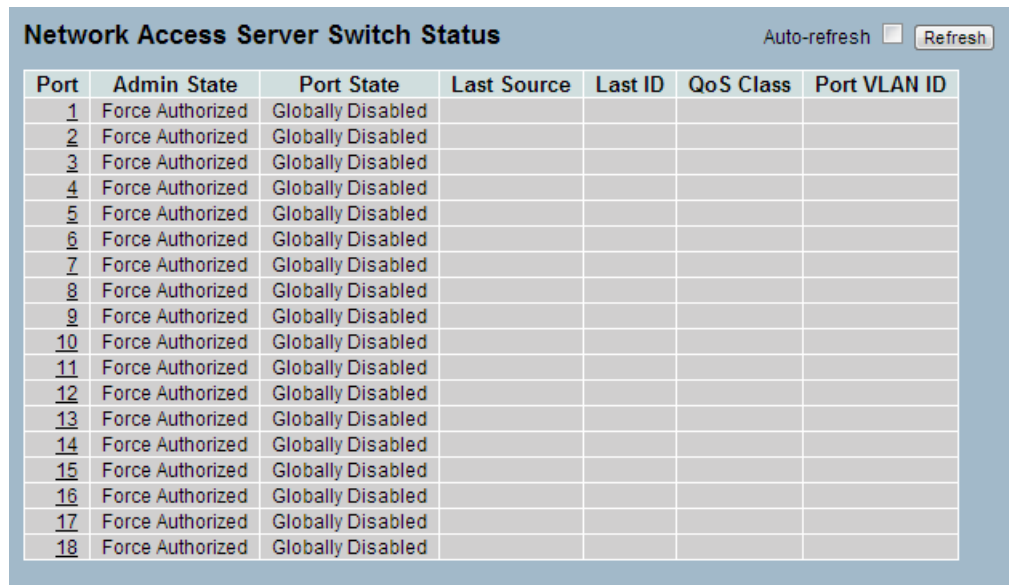
The section describes to show the each port NAS status information of the switch. The status includes Admin State Port State, Last Source, Last ID, QoS Class, and Port VLAN ID.

Web Interface

To configure a NAS Switch Status Configuration in the web interface:

1. Checked "Auto-refresh".

Figure 4-1.2: The Network Access Server Switch Status



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

Parameter description:

- **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.

- **Auto-refresh :**

To evoke the auto-refresh icon then the device will refresh the information automatically.

- **Upper right icon (Refresh):**

You can click them for refresh the NAS Switch Status by manual.

4-1.3 Port Status

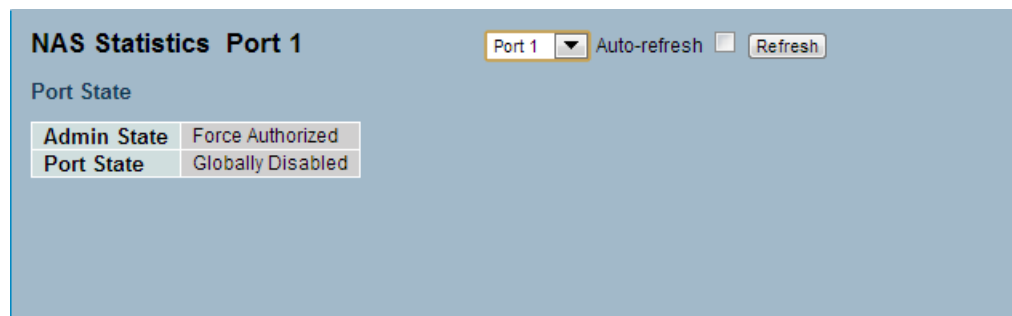
The section describes to provides detailed NAS statistics for a specific switch port running EAPOL-based IEEE 802.1X authentication.

Web Interface

To configure a NAS Port Status Configuration in the web interface:

1. Specify Port which want to check.
2. Checked "Auto-reflash".

Figure 4-1.3: The NAS Statistics



Parameter description:

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

- **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.

- **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.

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).
- **Auto-refresh :**
To evoke the auto-refresh icon then the device will refresh the information automatically.
- **Upper right icon (Refresh, Clear):**
You can click them for refresh the NAS Statistics by manual. Others you can click clear to clean up all entries.

4-2 Port Security

This section shows you to to configure the Port Security settings of the Switch. You can use the Port Security feature to restrict input to an interface by limiting and identifying MAC addresses.

4-2.1 Limit Control

This section shows you to to configure the Port Security settings of the Switch. You can use the Port Security feature to restrict input to an interface by limiting and identifying MAC addresses.

Web Interface

To configure a System Configuration of Limit Control in the web interface:

1. Select "Enabled" in the Mode of System Configuration.
2. Checked Aging Enabled.
3. Set Aging Period (Default is 3600 seconds).

To configure a Port Configuration of Limit Control in the web interface:

1. Select "Enabled" in the Mode of Port Configuration.
2. Specify the maximum number of MAC addresses in the Limit of Port Configuration.
3. Set Ation (Trap, Shutdown, Trap & Shutdown)
4. Click Save.

Figure 4-2.1: The Port Security Limit Control Configuration

Port Security Limit Control Configuration Refresh

System Configuration

Mode	Disabled
Aging Enabled	<input type="checkbox"/>
Aging Period	3600 seconds

Port Configuration

Port	Mode	Limit	Action	State	Re-open
*	<>		<>		
1	Disabled	4	None	Disabled	Reopen
2	Disabled	4	None	Disabled	Reopen
3	Disabled	4	None	Disabled	Reopen
4	Disabled	4	None	Disabled	Reopen
5	Disabled	4	None	Disabled	Reopen
6	Disabled	4	None	Disabled	Reopen
7	Disabled	4	None	Disabled	Reopen
8	Disabled	4	None	Disabled	Reopen
9	Disabled	4	None	Disabled	Reopen
10	Disabled	4	None	Disabled	Reopen
11	Disabled	4	None	Disabled	Reopen
12	Disabled	4	None	Disabled	Reopen
13	Disabled	4	None	Disabled	Reopen
14	Disabled	4	None	Disabled	Reopen
15	Disabled	4	None	Disabled	Reopen
16	Disabled	4	None	Disabled	Reopen
17	Disabled	4	None	Disabled	Reopen
18	Disabled	4	None	Disabled	Reopen

Apply Reset

Parameter description:

System Configuration

- **Mode :**

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

- **Aging Enabled :**

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

- **Aging Period :**

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

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

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

Port Configuration

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

- **Action :**

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

None: Do not allow more than Limit MAC addresses on the port, but take no further action.

Trap: If Limit + 1 MAC addresses is seen on the port, send an SNMP trap. If Aging is disabled, only one SNMP trap will be sent, but with Aging enabled, new SNMP traps will be sent everytime the limit gets exceeded.

Shutdown: If Limit + 1 MAC addresses is seen on the port, shut down the port. This implies that all secured MAC addresses will be removed from the port, and no new address will be learned. Even if the link is physically disconnected and reconnected on the port (by disconnecting the cable), the port will remain shut down. There are three ways to re-open the port:

- 1) Boot the switch,
- 2) Disable and re-enable Limit Control on the port or the switch,
- 3) Click the Reopen button.

Trap & Shutdown: If Limit + 1 MAC addresses is seen on the port, both the "Trap" and the "Shutdown" actions described above will be taken.

- **State :**

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

Disabled: Limit Control is either globally disabled or disabled on the port.

Ready: The limit is not yet reached. This can be shown for all actions.

Limit Reached: Indicates that the limit is reached on this port. This state can only be shown if Action is set to None or Trap.

Shutdown: Indicates that the port is shut down by the Limit Control module. This state can only be shown if Action is set to Shut down or Trap & Shutdown.

- **Re-open Button :**

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



NOTE: That clicking the reopen button causes the page to be refreshed, so non-committed changes will be lost

- **Upper right icon (Refresh):**

You can click them for refresh the Port Security information by manual.

- **Buttons:**

Save – Click to save changes.

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

4-2.2 Switch Status

This section 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.

Web Interface

To configure a Port Security Switch Status Configuration in the web interface:

1. Checked "Auto-reflash"

Figure 4-2.2: The Port Security Switch Status

Port Security Switch Status					
User Module Legend					
User Module Name	Abbr				
Limit Control	L				
802.1X	8				
DHCP Snooping	D				
Voice VLAN	V				
Port Status					
Port	Users	State	MAC Count		
			Current	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	-	-	

Parameter description:

- **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 and a number of columns, which are:
- **Port :**

The port number for which the status applies. Click the port number to see the status for this particular port.
- **Users :**

Each of the user modules has a column that shows whether that module has enabled Port Security or not. 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 (-).

Indicates the number of currently learned MAC addresses (forwarding as well as blocked) on the port. If no user modules are enabled on the port, a dash (-) will be shown.
- **Auto-refresh :**

To evoke the auto-refresh icon then the device will refresh the information automatically.
- **Upper right icon (Refresh):**

You can click them for refresh the Port Security Switch Status information by manual.

4-2.3 Port Status

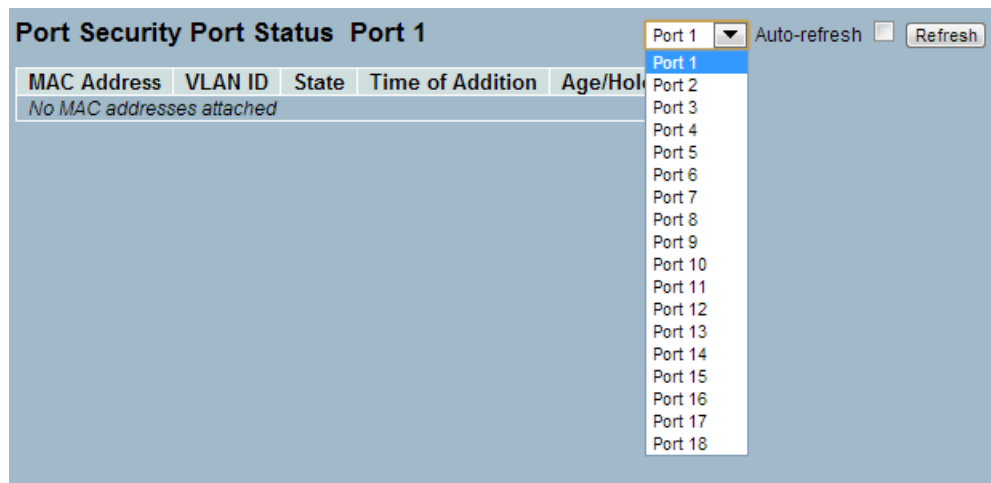
This section shows the MAC addresses secured by the Port Security module. Port Security is a module with no direct configuration. Configuration comes indirectly from other modules - the user modules. When a user module has enabled port security on a port, the port is set-up for software-based learning. 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.

Web Interface

To configure a Port Security Switch Status Configuration in the web interface:

1. Specify the Port which you want to monitor
2. Checked "Auto-reflash".

Figure 4-2.3: The Port Security Port Status



Parameter description:

- **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.

- **Auto-refresh :**
To evoke the auto-refresh icon then the device will refresh the information automatically.
- **Upper right icon (Refresh):**
You can click them for refresh the Port Security Port Status information by manual.

This chapter describes all of the switch Maintenance configuration tasks to enhance the performance of local network including Restart Device, Firmware upgrade, Save/Restore, Import/Export, and Diagnostics.

5-1 Warm Start

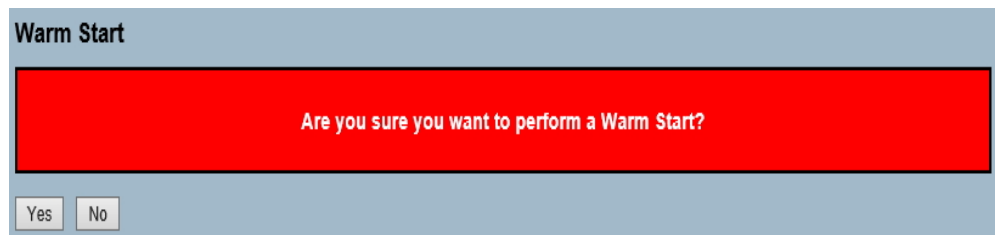
This section describes how to restart switch for any maintenance needs. Any configuration files or scripts that you saved in the switch should still be available afterwards.

Web Interface

To configure a Restart Device Configuration in the web interface:

1. Click Restart Device.
2. Click Yes.

Figure 5-1.1: The Warm Start



Parameter description:

- **Restart Device :**
You can restart the switch on this page. After restart, the switch will boot normally.
- **Buttons:**
Yes – Click to "Yes" then the device will restart.
No- Click to undo any restart action.

5-2 Firmware

This section describes how to upgrade Firmware. The Switch can be enhanced with more value-added functions by installing firmware upgrades.

5-2.1 Firmware Upgrade

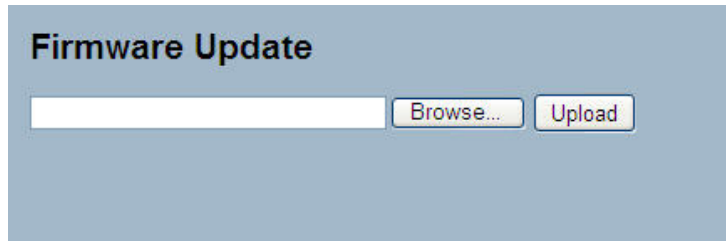
This page facilitates an update of the firmware controlling the Switch.

Web Interface

To configure a Firmware Upgrade Configuration in the web interface:

1. Click Browser to select firmware in you device.
2. Click Upload.

Figure 5-2.1: The Firmware update



Parameter description:

- **Browse :**
Click the “Browse...” button to search the Firmware URL and filename.
- **Upload:**
Click the “Upload” button then the switch will start to upload the firmware from firmware stored location PC or Server.



NOTE: This page facilitates an update of the firmware controlling the switch. Uploading software will update all managed switches to the location of a software image and click. After the software image is uploaded, a page announces that the firmware update is initiated. After about a minute, the firmware is updated and all managed switches restart. the switch restarts.



WARNING: While the firmware is being updated, Web access appears to be defunct. The front LED flashes Green/Off with a frequency of 10 Hz while the firmware update is in progress. Do not restart or power off the device at this time or the switch may fail to function afterwards.

5-2.2 Firmware Selection

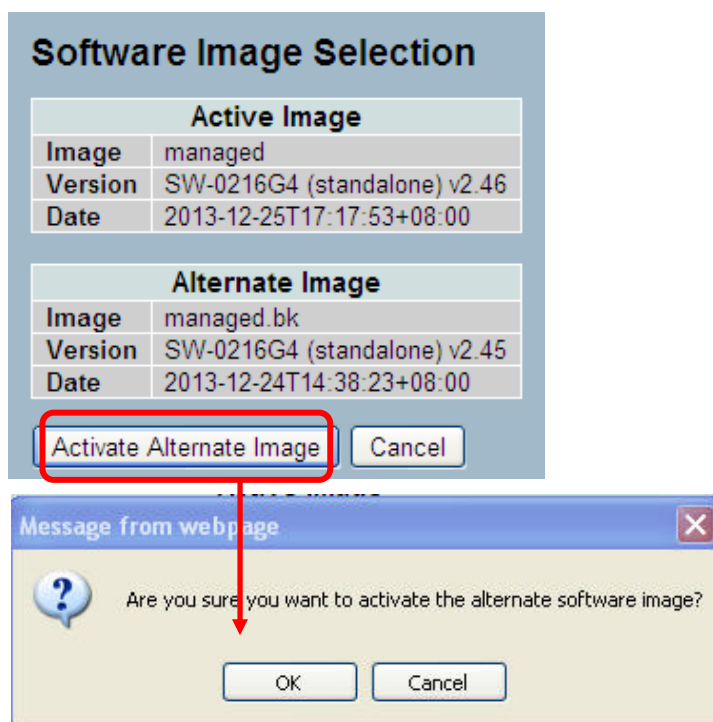
Due to the switch supports Dual image for firmware redundancy purpose. You can select what firmware image for your device start firmware or operating firmware. This page provides information about the active and alternate (backup) firmware images in the device, and allows you to revert to the alternate image.

Web Interface

To configure a Firmware Selection in the web interface:

1. Click Activate Alternate Image.
2. Click yes to complete firmware selection..

Figure 5-2.2: The Firmware Selection



Parameter description:

- **Image :**
The flash index name of the firmware image. The name of primary (preferred) image is `image`, the alternate image is named `image.bk`.
- **Version :**
The version of the firmware image.
- **Date :**
The date where the firmware was produced.
- **Buttons:**
Activate Alternate Image – Click to use the alternate image. This button may be disabled depending on system state.
Cancel - Cancel activating the backup image. Navigates away from this page.



NOTE:

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

5-3 Save / Restore

This section describes how to save and restore the Switch configuration including reset to Factory Defaults, Save Start, Save Users, Restore Users for any maintenance needs.

5-3.1 Factory Defaults

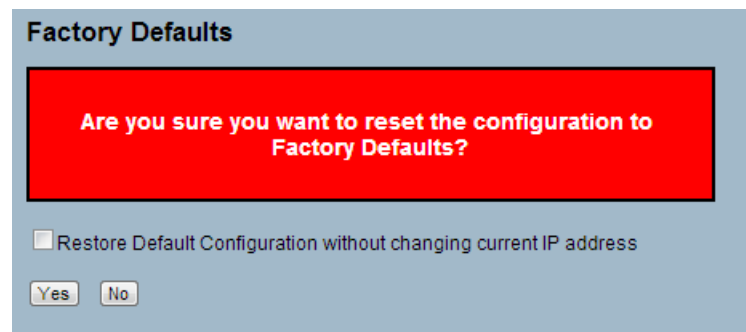
This section describes how to reset the Switch configuration to Factory Defaults. Any configuration files or scripts will recover to factory default values.

Web Interface

To configure a Factory Defaults Configuration in the web interface:

1. Click Factory Defaults.
2. Click Yes.

Figure 5-3.1: The Factory Defaults



Parameter description:

- **Buttons:**

Yes – Click to "Yes" button to reset the configuration to Factory Defaults..

No- Click to to return to the Port State page without resetting the configuration.



NOTE:

1. Restoring factory default can also be performed by push the reset button more than 10 seconds.
-

5-3.2 Save Start

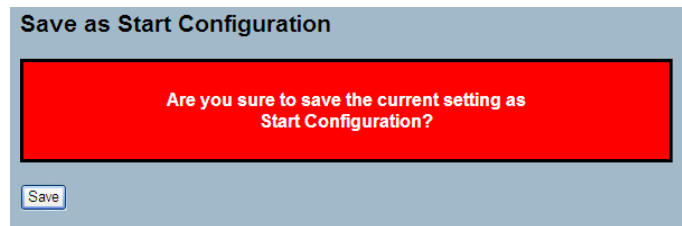
This section describes how to save the Switch Start configuration. Any current configuration files will be saved as XML format.

Web Interface

To configure a Save Start Configuration in the web interface:

1. Click Save Start.
2. Click Yes.

Figure 5-3.2: The Save Start configuration



Parameter description:

- **Buttons:**

Save – Click the “Save” button to save current setting as Start Configuration.

5-3.3 Save User

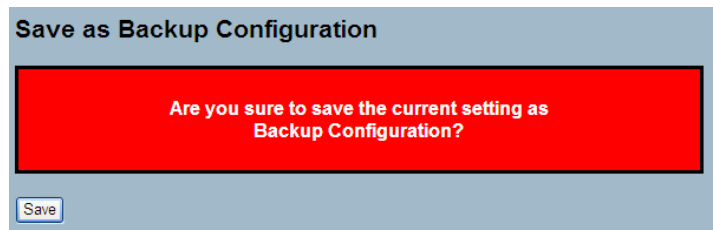
This section describes how to save users information. Any current configuration files will be saved as XML format.

Web Interface

To configure a Save User Configuration in the web interface:

1. Click Save User.
2. Click Yes.

Figure 5-3.3: The Save as Backup Configuration



Parameter description:

- **Buttons:**

Save – Click the "Save" button to save current setting as Backup Configuration.

5-3.4 Restore User

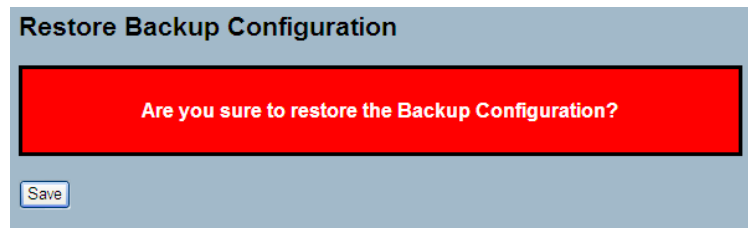
This section describes how to restore users information back to the switch. Any current configuration files will be restored via XML format.

Web Interface

To configure a Restore User Configuration in the web interface:

1. Click Restore User.
2. Click Yes.

Figure 5-3.4: The Restore the Backup Configuration



Parameter description:

- **Buttons:**

Save – Click the "Save" button to restore the Backup Configuration to the switch.

5-4 Export / Import

This section describes how to export and import the Switch configuration. Any current configuration files will be exported as XML format.

5-4.1 Export Config

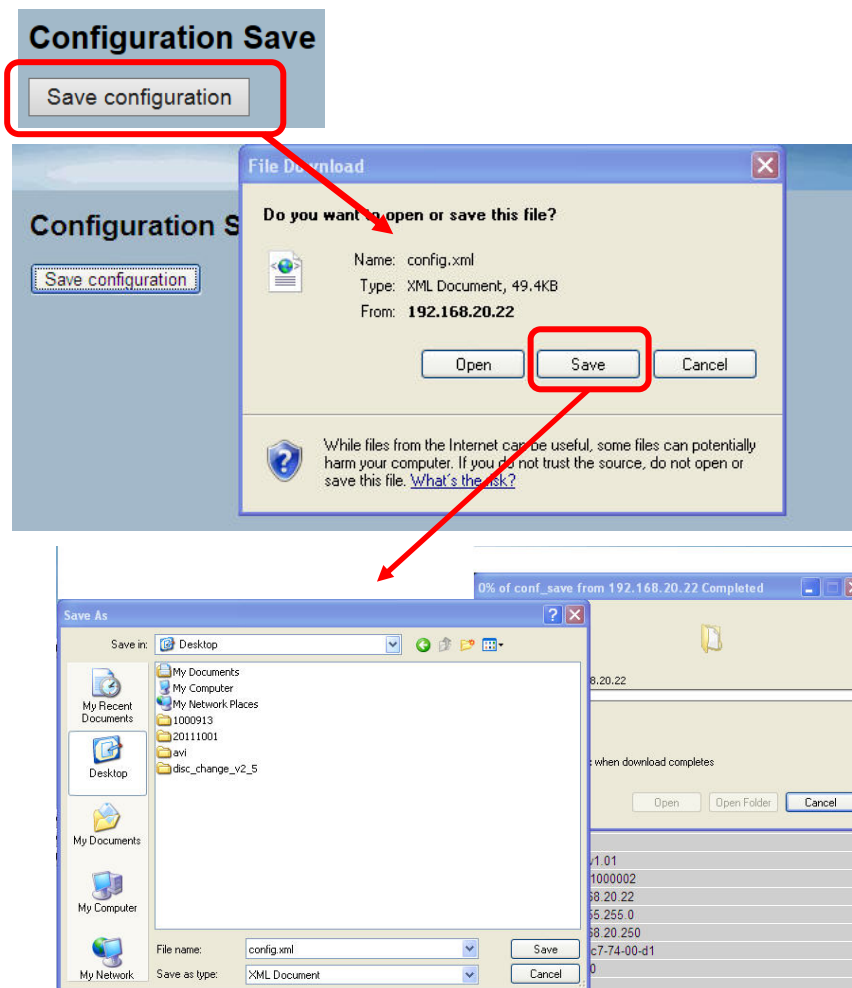
This section describes to export the Switch Configuration for maintenance needs. Any current configuration files will be exported as XML format.

Web Interface

To configure an Export Config Configuration in the web interface:

1. Click Save configuration.
2. Save the file in your device.

Figure 5-4.1: The Restore the Backup Configuration



Parameter description:

Save – Click the “Save” button to store the Configuration to the PC or Server.

5-4.2 Import Config

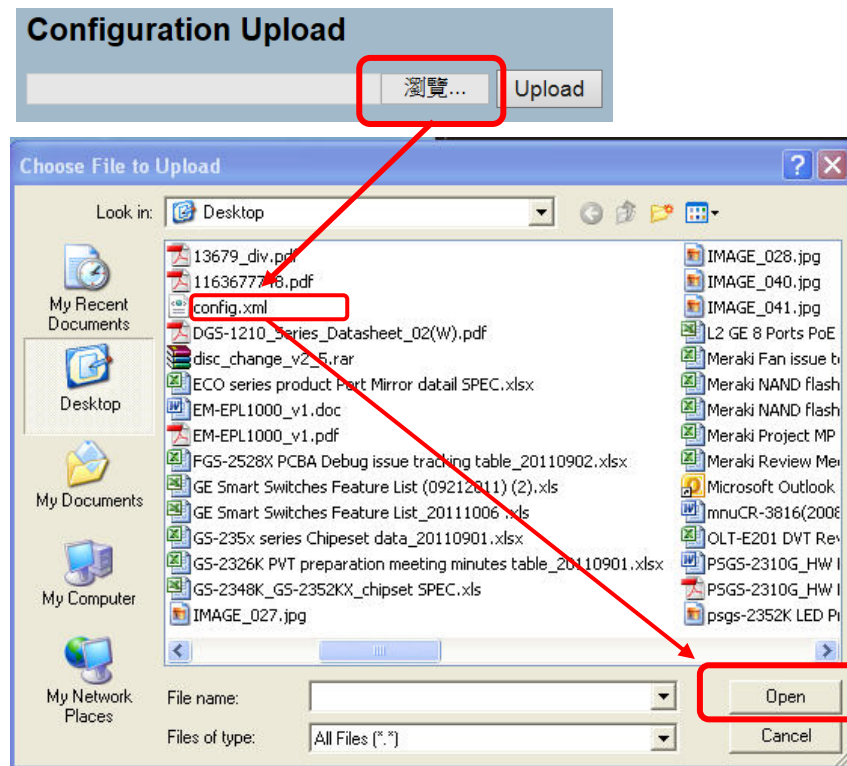
This section describes to export the Switch Configuration for maintenance needs. Any current configuration files will be exported as XML format.

Web Interface

To configure an Import Config Configuration in the web interface:

1. Click Browser to select the config file in you device.
2. Click Upload.

Figure 5-4.2: The Import Config



Parameter description:

- **Browse :**
Click the "Browse..." button to search the Configuration URL and filename.
- **Upload:**
Click the "Upload" button then the switch will start to upload the configuration from configuration stored location PC or Server.

5-5 Diagnostics

This section provides a set of basic system diagnosis. It let users know that whether the system is health or needs to be fixed. The basic system check includes ICMP Ping, ICMPv6, and VeriPHY Cable Diagnostics.

5-5.1 Ping

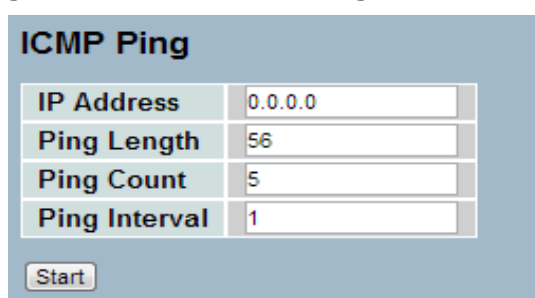
This section allows you to issue ICMP PING packets to troubleshoot Ipv4 connectivity issues.

Web Interface

To configure an ICMP PING Configuration in the web interface:

- 1.Specify ICMP PING IP Address.
- 2.Specify ICMP PING Size.
- 3.Click Start.

Figure 5-5.1: The ICMP Ping



ICMP Ping	
IP Address	0.0.0.0
Ping Length	56
Ping Count	5
Ping Interval	1

Start

Parameter description:

- **IP Address :**
The destination IP Address you want to ping it.
- **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.

After you press , 5 ICMP packets are transmitted, and the sequence number and roundtrip 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
```

```
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
```