XGS3600 Series

XGS3600-26F / XGS3600-28 / XGS3600-28F

GbE L2 Switch with 10G GbE uplink

Version 1.00
Edition 1, 03/2015

User's Guide

Default Login Details	
IP Address	http://192.168.0.1 (MGMT port) http://192.168.1.1 (In-band ports)
User Name	admin
Password	1234

IMPORTANT!

READ CAREFULLY BEFORE USE.

KEEP THIS GUIDE FOR FUTURE REFERENCE.

Screenshots and graphics in this book may differ slightly from your product due to differences in your product firmware or your computer operating system. Every effort has been made to ensure that the information in this manual is accurate.

Table of Contents

Overview

In this user's manual, it will not only tell you how to install and connect your network system but configure and monitor the XGS3600 Series through the built-in CLI and web by (RS-232) 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 and command-line interface (CLI).

The XGS3600 Series, the next generation L2+ Ethernet Fiber switches from Manufacture, is a 20-port GbE SFP, 4-port Combo GbE (RJ-45/SFP) and 4-port 10GbE (SFP+) L2+ Ethernet Switch portfolio of affordable fiber switches and a standard switch that meets all IEEE 802.3/u/x/z/ab/ae standards. The switch deliver more intelligent features you need to improve the availability of your critical business applications, protect 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 fiber networking includes ITU-T G.8032 Ethernet Ring Protection Switching for Ethernet switch management requirement. It is suitable for Ethernet switch applications. and helps you create a more efficient, better-connected workforce. Others it supports AC and DC Dual Power input (100~240VAC/-48VDC) for Power Redundancy requirement.

XGS3600 SERIES L2+ Ethernet Fiber Switches provide 26 ports in a single device; the specification is highlighted as follows.

- L2+ features provide better manageability, security, QoS, and performance.
- ITU-T G.8032 Ethernet Ring Protection Switching.
- Support 20 Port (100M/1G SFP) Fiber high-density for scalable connect requirement.
- Support 4-port Combo GbE RJ-45/(100M/1G SFP) for flexible connection requirement.
- Support 4-port 10GbE (1G/10G SFP+) for high speed backbone uplink requirement
- Support 1-port GbE RJ-45 for out-of-band management requirement.
- Support IPv4/IPv6 dual stack management
- Support SSH/SSL secured management
- Support SNMP v1/v2c/v3
- Support RMON groups 1,2,3,9
- Support sFlow
- Support IGMP v1/v2/v3 Snooping
- Support MLD v1/v2 Snooping
- Support RADIUS and TACACS+ authentication
- Support IP Source Guard
- Support DHCP Relay (Option 82)
- Support DHCP Snooping
- Support ACL and QCL for traffic filtering
- Support 802.1d(STP), 802.1w(RSTP) and 802.1s(MSTP)
- Support LACP and static link aggregation
- Support Q-in-Q double tag VLAN
- Support GVRP dynamic VLAN
- Support AC (100~240VAC) and DC (-48VDC) dual power input for power redundancy application

Overview of this user's manual

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

Chapter 1

Operation of Web-based Management

Initial Configuration

This chapter instructs you how to configure and manage the XGS3600 Series 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 XGS3600 Series 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	1234

After the XGS3600 Series 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 **1234**. 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 XGS3600 Series will not give you a shortcut to username automatically. This looks inconvenient, **but safer.**

In the XGS3600 Series, 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 logins 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 XGS3600 Series.

NOTE:
When you login XGS3600 Series switch Web UI management, you can use both ipv4 ipv6 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

Figure 1 The login page

Chapter 2 System Configuration
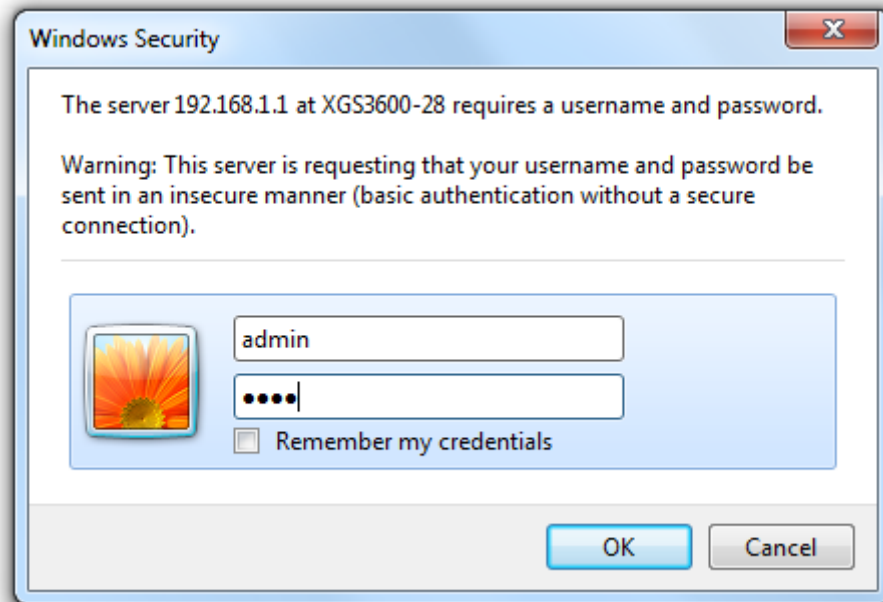
This chapter describes all of the basic configuration tasks which includes the System Information and any management of the Switch (e.g. Time, Account, IP, Syslog and SNMP.)

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

System Information

Model Name	XGS3600-28
System Description	24-port GbE L2 Switch with 10 GbE uplink
Location	
Contact	
Device Name	XGS3600-28
System Date	2011-01-01 00:17:07
System Uptime	0d 00:17:07
BIOS Version	v1.00
Firmware Version	V1.00(AAPA.2)C0
Hardware-Mechanical Version	v1.01-v1.01
Series Number	S132U37000017
Host IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Gateway IP Address	192.168.1.254
Host MAC Address	10-7b-ef-4c-5c-fc
Console Baudrate	115200
RAM Size	128MB
Flash Size	16MB
Bridge FDB Size	32768 MAC Addresses
Transmit Queue	8 queues per port
Maximum Frame Size	10056
Fan Speed	Fan1:7058(rpm) Fan2:6994(rpm) Fan3:7248(rpm)
Powers	AC Power On 12.0V ; DC Power Off 0.0V
Temperature 1	38(C) ; 100(F)
Temperature 2	35(C) ; 95(F)

Parameter description:

- **Model name:**

  The model name of this device.

- **System description:**

  As it is, this tells what this device is. Here, it is "**24-port GbE L2 Switch with 10 GbE uplink**".

- **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:**

  Show the system time of the switch. Its format: day of week, month, day, hours : minutes : seconds, year.

- **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.

- **Host IP address:**

  The IP address of the switch.

- **Host MAC address:**

  It is the Ethernet MAC address of the management agent in this switch.

- **Device Port:**

  Show all types and numbers of the port in the switch.

- **RAM size:**

  The size of the RAM in this switch.

- **Flash size:**

  The size of the flash memory in this switch.

- **Bridge FDB size :**

  To display the bridge FDB size information.

- **Transmit Queue :**

  To display the device's transmit hardware priority queue information.

- **Maximum Frame size :**

    To display the device's maximum frame size information.

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

Contact	
Device Name	
Location	

Apply   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.

2-1.3 CPU Load

This page displays the CPU load, using an SVG graph. The load is measured as averaged over the last 100ms, 1sec and 10 seconds intervals. The last 120 samples are graphed, and the last numbers are displayed as text as well. In order to display the SVG graph, your browser must support the SVG format. Consult the SVG Wiki for more information on browser support. Specifically, at the time of writing, Microsoft Internet Explorer will need to have a plugin installed to support SVG.

Web interface

To configure System Information in the web interface:

1. Click System, System Information, CPU Load .
2. Display the CPU Load on the screen
3. Click Auto-refresh .

Figure 2-1.3: CPU Load

Parameter description:

- **Auto-refresh**

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

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

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

Parameter description:

- **Clock Source:**

  To click what clock source for the XGS3600 Series. You can select "Use local Settings" or "Use NTP Server" for XGS3600 Series time clock source.

- **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 ~ +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	au.pool.ntp.org
Server 2	
Server 3	
Server 4	
Server 5	

[Apply] [Reset]

Parameter description:

- **Server 1 to 5 :**

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

- **Buttons**

  These buttons are displayed on the NTP page:

  Apply – Click to apply 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

Parameter description:

- **User Name :**

    The name identifying the user. This is also a link to Add/Edit User.

- **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.

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 Private VLANs QoS SMTP SNMP Security Spanning Tree System Trap Event VCL VLANs Voice VLAN Privilege Levels from 1 to 15 .

Web Interface

To configure Privilege Level in the web interface:

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

Figure2- 3.2: The Privilege Level configuration

Privilege Level Configuration

Group Name	Privilege Levels
Account	10
Aggregation	10
Diagnostics	10
EPS	10
ERPS	10
ETH LINK OAM	10
EVC	10
GARP	10
GVRP	10
IP	10
IPMC Snooping	10
LACP	10
LLDP	10
LLDP MED	10
Loop Protect	10
MAC Table	10
MEP	10
MRSTP	10
MVR	10
Maintenance	15
Mirroring	10
PTP	10
Ports	10
Private VLANs	10
QoS	10
SMTP	10
SNMP	10
Security	10
Spanning Tree	10
System	10
Trap Event	10
VCL	10
VLAN Translation	10
VLANs	10

Apply   Reset

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: System Information, Time, Syslog.

  Security: IP Source Guard, ARP Inspection, DHCP snooping, DHCP Relay, NAS, Authentication (AAA), Port Security, System Access Management, ACL, HTTPS, SSH and Auth Method.

  Account: Users, Privilege Level..

  Diagnostics: Ping, Ping6 and VeriPHY.

  Maintenance: System Reboot, System Restore Default, Configuration Save, Export/Import Configuration and Firmware upgrade.

- **Privilege Levels**

  Every group has an authorization Privilege level. 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, IPv6, which would have 128-bits Internet Protocol addresses. This number can be represented roughly by a three with thirty-nine zeroes after it. However, IPv4 is still the protocol of choice for most of the Internet.

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 a 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	☐	Renew
Inband IP Address	192.168.1.1	192.168.1.1
Inband IP Mask	255.255.255.0	255.255.255.0
Inband IP Gateway	192.168.1.254	192.168.1.254
Inband VLAN ID	1	1
Inband Default Gateway	☐	
Outband IP Address	192.168.0.1	192.168.0.1
Outband IP Mask	255.255.255.0	255.255.255.0
Outband IP Gateway	192.168.0.254	192.168.0.254
DNS Server	0.0.0.0	0.0.0.0

IP DNS Proxy Configuration

DNS Proxy ☐

Apply Reset

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 Gateway :**

  Provide the IP address of the gateway 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.

2-4.2 IPV6

This section describes how to configure the switch-managed IPv6 information. The Configured column is used to view or change the IPv6 configuration. And the Current column is used to show the active IPv6 configuration.

Configure the switch-managed IPv6 information on this page.

The Configured column is used to view or change the IPv6 configuration.

The Current column is used to show the active IPv6 configuration.

Web Interface

To configure Management IPv6 of the switch in the web interface:
1. Click System, IPv6 Configuration.
2. Specify the IPv6 settings, and enable Auto Configuration service if required.
3. Click Apply.

Figure2- 4.2: The IPv6 configuration

IPv6 Configuration

	Configured	Current
Auto Configuration	☐	Renew
Address	::192.168.1.1	::192.168.1.1 Link-Local Address: fe80::6082:cdb9:19ab:c0e2
Prefix	96	96
Gateway	::	::

Apply   Reset

Parameter description:

- **Auto Configuration :**

  Enable IPv6 auto-configuration by checking this box. If fails, the configured IPv6 address is zero. The router may delay responding to a router solicitation for a few seconds, the total time needed to complete auto-configuration can be significantly longer.

- **Address :**

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

- **Prefix :**

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

- **Gateway**

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

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 Apply.

Figure2- 5.1: The System Log configuration

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 :**

    Indicates the IPv4 host address of syslog server. 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:

  <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.

- **Syslog Type :**

  Every trap event in the system has its specific type for syslog. You can see the mapping in the Trap Event Severity page.

- **Active :**

  Individually enable or disable the sending of syslog message to the syslog server for a specific Syslog Type.

- **Facility :**

  Indicate the facility for sending syslog message for a specific Syslog Type. Only local_use_0 to local_use_7 can be assigned to one Syslog Type.

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

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

Detailed System Log Information

ID	1

Message

Level	Warning
Time	2011-01-01 00:00:08
Message	Switch just made a warm boot

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 System

This section describes how to configure SNMP System on the switch. This function is used to configure SNMP settings, community name, trap host and public traps as well as the throttle of SNMP. A SNMP manager must pass the authentication by identifying both community names, then it can access the MIB information of the target device. So, both parties must have the same community name. Once completing the setting, click <Apply> button, the setting takes effect.

Web Interface

To display the configure SNMP System in the web interface:
1. Click SNMP, System.
2. Evoke SNMP State to enable or disable the SNMP function .
3. Specify the Engine ID
4. Click Apply.

Figure2- 6.1: The SNMP System Configuration

SNMP System Configuration

SNMP State	⦿ Enable ◯ Disable
Engine ID	80001455030001c1000000

Apply

Parameter description:

These parameters are displayed on the SNMP System Configuration page:

● **SNMP State :**

The term SNMP here The term SNMP here is used for the activation or de-activation of SNMP.

Enable: Enable SNMP state operation.
Disable: Disable SNMP state operation.
Default: Enable.

● **Engine ID :**

SNMPv3 engine ID. syntax: 0-9,a-f,A-F, min 5 octet, max 32 octet, fifth octet can't input 00. IF change the Engine ID that will clear all original user.

2-6.2 Configuration

The function is used to configure SNMP Community and its mode. By enable or disable the function user can specify how to get or set the communities.

Web Interface

To display the setting SNMP Configuration in the web interface:
1. Click SNMP, Configuration.
2. Specify the SNMP Configuration' parameters.
3. Enable Set Community
4. Click Apply.

Figure2-6.2: The SNMPv2C Configuration

SNMP Configuration

Get Community	public	
Set Community	private	Enable ▼

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. 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.

- **Mode:**

  Indicates the Set Community mode operation. Possible modes are:

  Enabled: Enable Set Community.

  Disabled: Disable Set Community.

2-6.3 Communities

The function is used to configure SNMPv3 communities. The Community and UserName is unique. To create a new community account, please check <Add new community> button, and enter the account information then check <Apply>. Max Group Number : 4.

Web Interface

To display the configure SNMP Communities in the web interface:
1. Click SNMP, Communities.
2. Click Add new community.
3. Specify the SNMP communities parameters.
4. Click Apply.
5. If you want to modify or clear the setting then click Reset.

Figure2-6.3: The SNMPv1/v2 Communities Security Configuration

SNMPv1/v2 Communities to Security Configuration

Delete	Community	User Name	Source IP	Source Mask
Delete			0.0.0.0	0.0.0.0

Add new community   Apply

Parameter description:

- **Delete**

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

- **Community**

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

- **User Name:**

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

- **Source IP**

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

- **Source Mask**

  Indicates the SNMP access source address mask

2-6.4 Users

The function is used to configure SNMPv3 user. The Entry index key is UserName. To create a new UserName account, please check <Add new user> button, and enter the user information then check <Apply>. Max Group Number : 10.

Web Interface

To display how to add new user to the configure SNMP Users in the web interface:

1. Click SNMP, Users.
2. Click "Add new user"
3. Specify the Privilege parameter.
4. Click Apply.

Figure 2-6.4: The SNMP Users Configuration

SNMPv3 Users Configuration

Delete	User Name	Security Level	Authentication Protocol	Authentication Password	Privacy Protocol	Privacy Password
Delete		Auth, Priv ▼	MD5 ▼		DES ▼	

Add new user   Apply

Parameter description:

- **Delete**

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

- **User Name**

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

- **Security Level**

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

    NoAuth, NoPriv: No authentication and no privacy.

    Auth, NoPriv: Authentication and no privacy.

    Auth, Priv: Authentication and privacy.

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

- **Authentication Protocol**

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

    None: No authentication protocol.

    MD5: An optional flag to indicate that this user uses MD5 authentication protocol.

    SHA: An optional flag to indicate that this user uses SHA authentication protocol.

    The value of security level cannot be modified if entry already exists. That

means must first ensure that the value is set correctly.

- **Authentication Password**

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

- **Privacy Protocol**

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

  None: No privacy protocol.

  DES: An optional flag to indicate that this user uses DES authentication protocol.

- **Privacy Password**

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

2-6.5 Groups

The function is used to configure SNMPv3 group. The Entry index key are Security Model and Security Name. To create a new group account, please check <Add new group> button, and enter the group information then check <Apply>. Max Group Number : v1: 2, v2: 2, v3:10.

Web Interface

To display the configure SNMP Groups in the web interface:
1. Click SNMP, Groups.
2. Specify the Privilege parameter.
3. Click Apply.

Figure 2-6.5: The SNMP Groups Configuration

Parameter description:

- **Delete**

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

- **Security Model**

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

  v1: Reserved for SNMPv1.

  v2c: Reserved for SNMPv2c.

  usm: User-based Security Model (USM).

- **Security Name**

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

- **Group Name**

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

2-6.6 Views

The function is used to configure SNMPv3 view. The Entry index key are OID Subtree and View Name. To create a new view account, please check <Add new view> button, and enter the view information then check <Apply>. Max Group Number : 28.

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

Web Interface

1. Click SNMP, Views.
2. Click Add new View.
3. Specify the SNMP View parameters.
4. Click Apply.

Figure 2-6.6: The SNMP Views Configuration

SNMPv3 Views Configuration

Delete	View Name	View Type	OID Subtree
Delete		included ▼	

[Add new view] [Apply]

Parameter description:

● **Delete**

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

● **View Name**

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

● **View Type**

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

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

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

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

● **OID Subtree**

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

● **Apply**

To click the Apply icon to save the configuration to ROM.

2-6.7 Access

The function is used to configure SNMPv3 accesses. The Entry index key are Group Name, Security Model and Security level. To create a new access account, please check <Add new access> button, and enter the access information then check <Apply>. Max Group Number : 14

Web Interface

To display the configure SNMP Access in the web interface:
1. Click SNMP, Accesses.
2. Click Add new Access.
3. Specify the SNMP Access parameters.
4. Click Apply.
5. If you want to modify or clear the setting then click Reset.
.

Figure 2-6.7: The SNMP Accesses Configuration

Parameter description:

- **Delete**

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

- **Group Name**

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

- **Security Model**

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

  any: Any security model accepted(v1|v2c|usm).

  v1: Reserved for SNMPv1.

  v2c: Reserved for SNMPv2c.

  usm: User-based Security Model (USM).

- **Security Level**

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

  NoAuth, NoPriv: No authentication and no privacy.

  Auth, NoPriv: Authentication and no privacy.

  Auth, Priv: Authentication and privacy.

- **Read View Name**

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

- **Write View Name**

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

2-6.8 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

Trap Hosts 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								

Apply

Trap Host Configuration

Trap Version	v2c
Server IP	0.0.0.0
UDP Port	162
Community/Security Name	
Severity Level	Info
Security Level	NoAuth, NoPriv
Authentication Protocol	MD5
Authentication Password	
Privacy Protocol	DES
Privacy Password	

Apply Reset

Parameters description:

- **Delete:**

  Check <Delete> entry then check <Apply> button, the entry will be delete.

- **Trap Version:**

  Indicates the SNMP trap supported version. Possible versions are:

  SNMP v2c: Set SNMP trap supported version 2c.

  SNMP v3: Set SNMP trap supported version 3.

- **Server IP:**

This is the IP of the trap host.

- **UDP Port:**

  This is the receiving-port number of the trap host. Range: 1 - 65535.

- **Community / Security Name:**

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

- **Security Level:**

  The Severity Level: Emerg, Alert, Crit, Error, Warning, Notice, Info, Debug.

- **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:**

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

  MD5: An optional flag to indicate that this user uses MD5 authentication protocol.

  SHA: An optional flag to indicate that this user uses SHA authentication protocol.

- **Authentication Password:**

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

- **Privacy Protocol:**

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

  DES: An optional flag to indicate that this user uses DES authentication protocol.

- **Privacy Password:**

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

This chapter describes all of the basic network configuration tasks which include the Ports, Layer 2 network protocol (e.g. VLANs, QoS, IGMP and ACLs 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 sze ,
   Excessive Collision mode and Power Control.
3. Click Apply.

Figure 3-1.1: The Port Configuration

Port Configuration

Refresh

Port	Link	Speed		Maximum Frame Size	Excessive Collision Mode	Power Control
		Current	Configured			
*			<> ▼		<> ▼	<> ▼
1	🟢	1Gfdx	Auto ▼	10056	Discard ▼	Disabled ▼
2	🔴	Down	Auto ▼	10056	Discard ▼	Disabled ▼
3	🔴	Down	Auto ▼	10056	Discard ▼	Disabled ▼
4	🔴	Down	Auto ▼	10056	Discard ▼	Disabled ▼
5	🔴	Down	Auto ▼	10056	Discard ▼	Disabled ▼
6	🔴	Down	Auto ▼	10056	Discard ▼	Disabled ▼
7	🔴	Down	Auto ▼	10056	Discard ▼	Disabled ▼
8	🔴	Down	Auto ▼	10056	Discard ▼	Disabled ▼
9	🔴	Down	Auto ▼	10056	Discard ▼	Disabled ▼
10	🔴	Down	Auto ▼	10056	Discard ▼	Disabled ▼
11	🔴	Down	Auto ▼	10056	Discard ▼	Disabled ▼
12	🔴	Down	Auto ▼	10056	Discard ▼	Disabled ▼
13	🔴	Down	Auto ▼	10056	Discard ▼	Disabled ▼
14	🔴	Down	Auto ▼	10056	Discard ▼	Disabled ▼
15	🔴	Down	Auto ▼	10056	Discard ▼	Disabled ▼
16	🔴	Down	Auto ▼	10056	Discard ▼	Disabled ▼
17	🔴	Down	Auto ▼	10056	Discard ▼	Disabled ▼
18	🔴	Down	Auto ▼	10056	Discard ▼	Disabled ▼
19	🔴	Down	Auto ▼	10056	Discard ▼	Disabled ▼
20	🔴	Down	Auto ▼	10056	Discard ▼	Disabled ▼
21	🔴	Down	Auto ▼	10056	Discard ▼	Disabled ▼
22	🔴	Down	Auto ▼	10056	Discard ▼	Disabled ▼
23	🔴	Down	Auto ▼	10056	Discard ▼	Disabled ▼
24	🟢	100fdx	Auto ▼	10056	Discard ▼	Disabled ▼
25	🔴	Down	10Gbps FDX ▼	10056		
26	🔴	Down	10Gbps FDX ▼	10056		
27	🔴	Down	10Gbps FDX ▼	10056		
28	🔴	Down	10Gbps FDX ▼	10056		

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 :**

Provide the current link speed of the port.

- **Configured Link Speed :**

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

  Disabled - Disables the switch port operation.

  Auto - Cu port auto negotiating speed with the link partner and selects the highest speed that is compatible with the link partner.

  10Mbps HDX - Forces the cu port in 10Mbps half duplex mode.

  10Mbps FDX - Forces the cu port in 10Mbps full duplex mode.

  100Mbps HDX - Forces the cu port in 100Mbps half duplex mode.

  100Mbps FDX - Forces the cu port in 100Mbps full duplex mode.

  1Gbps FDX - Forces the cu port in 1Gbps full duplex mode.

  Auto_AMS - Automatically determines the speed of the SFP. Note: There is no standardized way to do SFP auto detect, so here it is done by reading the SFP rom. Due to the missing standardized way of doing SFP auto detect some SFPs might not be detectable. The port is set in AMS mode with SFP preferred. Cu port is set in Auto mode.

  100-FX - SFP port in 100-FX speed. Cu port disabled.

  100-FX_AMS - Port in AMS mode with SFP preferred. SFP port in 100-FX speed. Cu port in Auto mode.

  1000-X - SFP port in 1000-X speed. Cu port disabled.

  1000-X_AMS - Port in AMS mode with SFP preferred. SFP port in 1000-X speed. Cu port in Auto mode.

- **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 back of 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**

  Apply – Click to apply 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
the full name and version identification for the system's
hardware type, software version, and networking application.
3. Click Apply.

Figure 3-1.2: The Port Configuration

Port Description

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

Apply Reset

Parameter description:

- **Port :**

    This is the logical port number for this row.

- **Description :**

    Enter up to 47 characters to be descriptive name for identifies this port.

- **Buttons**

  Apply – Click to apply changes.

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

3-1.3 Port Telephone

This page displays current port telephone number.

Web Interface

To configure an Port Telephone in the web interface:
1. Click Configuration, Port, then Port telephone.
2. Specify the telephone number.
3. Click Apply.

Figure 3-1.3: The Port Telephone

Port Telephone

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

Apply   Reset

Parameter description:

- **Port :**

    This is the logical port number for this row.

- **Description :**

    Enter up to 32 characters to be telephone number for identifies this port.

- **Buttons**

    Apply – Click to apply changes.

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

3-1.4 Traffic Overview

The section describes to the Port statistics information and provides overview of general traffic statistics for all switch ports. The ports belong to the currently selected stack unit, as reflected by the page header

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 3-1.4: The Port Statistics Overview

Port Statistics Overview — Auto-refresh ☐ [Refresh] [Clear]

Port	Packets		Bytes		Errors		Drops		Filtered
	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received
1	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0	0
13	0	0	0	0	0	0	0	0	0
14	0	0	0	0	0	0	0	0	0
15	0	0	0	0	0	0	0	0	0
16	0	0	0	0	0	0	0	0	0
17	0	0	0	0	0	0	0	0	0
18	0	0	0	0	0	0	0	0	0
19	0	0	0	0	0	0	0	0	0
20	0	0	0	0	0	0	0	0	0
21	0	0	0	0	0	0	0	0	0
22	8023	4625	1935376	2762454	0	0	796	0	796
23	0	0	0	0	0	0	0	0	0
24	0	0	0	0	0	0	0	0	0
25	0	0	0	0	0	0	0	0	0
26	0	0	0	0	0	0	0	0	0
27	0	0	0	0	0	0	0	0	0
28	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.

3-1.5 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 selected port belongs to the currently selected stack unit, as reflected by the page header.

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

Web Interface

To Display per port's 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 statistics 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 3-1.5: The Port Detail Statistics Overview

Detailed Port Statistics Port 1 — Port 1 ▼ Auto-refresh ☐ [Refresh] [Clear]

Receive Total		Transmit Total	
Rx Packets	0	Tx Packets	0
Rx Octets	0	Tx Octets	0
Rx Unicast	0	Tx Unicast	0
Rx Multicast	0	Tx Multicast	0
Rx Broadcast	0	Tx Broadcast	0
Rx Pause	0	Tx Pause	0
Receive Size Counters		Transmit Size Counters	
Rx 64 Bytes	0	Tx 64 Bytes	0
Rx 65-127 Bytes	0	Tx 65-127 Bytes	0
Rx 128-255 Bytes	0	Tx 128-255 Bytes	0
Rx 256-511 Bytes	0	Tx 256-511 Bytes	0
Rx 512-1023 Bytes	0	Tx 512-1023 Bytes	0
Rx 1024-1526 Bytes	0	Tx 1024-1526 Bytes	0
Rx 1527- Bytes	0	Tx 1527- Bytes	0
Receive Queue Counters		Transmit Queue Counters	
Rx Q0	0	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	0
Receive Error Counters		Transmit Error Counters	
Rx Drops	0	Tx Drops	0
Rx CRC/Alignment	0	Tx Late/Exc. Coll.	0
Rx Undersize	0		
Rx Oversize	0		
Rx Fragments	0		
Rx Jabber	0		
Rx Filtered	0		

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.

3-1.6 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. The ports belong to the currently selected stack unit, as reflected by the page header.

Web Interface

To Display the Queuing 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 Queuing Counters or clear all information when you click " Clear".

Figure 3-1.6: The Queuing Counters Overview

Queuing Counters — Auto-refresh ☐ [Refresh] [Clear]

Port	Q0		Q1		Q2		Q3		Q4		Q5		Q6		Q7	
	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
13	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
14	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
15	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
17	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
18	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
19	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
20	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
21	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
22	7492	0	0	0	0	0	0	0	0	0	0	0	0	0	0	4792
23	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
24	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
25	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
26	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
27	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
28	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 :**

   There are 8 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 Queuing Counters automatically.

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

    You can click them for refresh the Queuing Counters or clear them by manual.

3-1.7 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 3-1.7: The SFP Information Overview

SFP Information for Port 1

Connector Type	none
Fiber Type	none
Tx Central Wavelength	none
Bit Rate	none
Vendor OUI	none
Vendor Name	none
Vendor P/N	none
Vendor Revision	none
Vendor Serial Number	none
Date Code	none
Temperature	none
Vcc	none
Mon1 (Bias)	none
Mon2 (TX PWR)	none
Mon3 (RX PWR)	none

Parameter description:

- **Connector Type**:

    Displays the external optical or electrical cable connector provided as the media interface.

- **Fiber Type:**

    Displays the fiber channel transmission media.

- **Tx Central Wavelength:**

    Display the fiber optical transmitting central wavelength, for instance, 850nm, 1310nm, 1550nm and so on.

- **Norminal Bit Rate:**

    Display the maximum baud rate of the fiber module supported, for instance, 10M, 100M, 1G and so on.

- **Vendor OUI:**

    Displays the vendor IEEE company ID.

- **Vendor Name:**

   Displays the vendor name.

- **Vendor P/N:**

   Displays the vendor part number or product name.

- **Vendor Rev (Revision):**

   Display the module revision.

- **Vendor SN (Serial Number):**

   Displays the vendor serial number for the transceiver.

- **Date Code:**

   Displays the vendor's manufacturing date code.

- **Temperature:**

   Displays the internally measured transceiver temperature. Temperature accuracy is vendor specific but must be better than 3 degrees Celsius over specified operating temperature and voltage.

- **Vcc:**

   Displays the internally measured transceiver supply voltage. Accuracy is vendor specific but must be better than 3 percent of the manufacturer's nominal value over specified operating temperature and voltage. Note that in some transceivers, transmitter supply voltage and receiver supply voltage are isolated. In that case, only one supply is monitored. Refer to the device specification for more detail.

- **Mon1(Bias) mA:**

   Displays the measured TX bias current in uA. Accuracy is vendor specific but must be better than 10 percent of the manufacturer's nominal value over specified operating temperature and voltage.

- **Mon2(TX PWR):**

   Displays the measured coupled TX output power in mW. Accuracy is vendor specific but must be better than 3dB over specified operating temperature and voltage. Data is assumed to be based on measurement of a laser monitor photodiode current. Data is not valid when the transmitter is disabled.

- **Mon3(RX PWR):**

   Displays the measured received optical power in mW. Absolute accuracy is dependent upon the exact optical wavelength. For the vendor specified wavelength, accuracy should be better than 3dB over specified temperature and voltage. This accuracy should be maintained for input power levels up to the lesser of maximum transmitted or maximum received optical power per the appropriate standard. It should be maintained down to the minimum transmitted power minus cable plant loss (insertion loss or passive loss) per the appropriate standard. Absolute accuracy beyond this minimum required received input optical power range is vendor specific.

3-2 ACL

The XGS3600 Series switch access control list (ACL) is probably the most commonly used object in the IOS. It is used for packet filtering but also for selecting types of traffic to be analyzed, forwarded, or influenced in some way. The ACLs are divided into EtherTypes. IPv4, ARP protocol, MAC and VLAN parameters etc. Here we will just go over the standard and extended access lists for TCP/IP. As you create ACEs for ingress classification, you can assign a policy for each port, the policy number is 1-8, however, each policy can be applied to any port. This makes it very easy to determine what type of ACL policy you will be working with.

3-2.1 Ports

The section describes how to configure the ACL parameters (ACE) of the each switch port. These parameters will affect frames received on a port unless the frame matches a specific ACE

Web Interface

To configure the ACL Ports Configuration in the web interface:

1. Click Configuration, ACL, then Ports
2. To scroll the specific parameter value to select the correct value for port
   ACL setting.
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.
5. After you configure complete then you could see the Counter of the port.
   then you could click refresh to update the counter or Clear the information.

Figure 3-2.1: The ACL Ports Configuration

ACL Ports Configuration

Port	Policy ID	Action	Rate Limiter ID	Port Redirect	Shutdown	State	Counter
*		<>	<>	<>	<>	<>	*
1	0	Permit	Disabled	Disabled	Disabled	Enabled	0
2	0	Permit	Disabled	Disabled	Disabled	Enabled	0
3	0	Permit	Disabled	Disabled	Disabled	Enabled	0
4	0	Permit	Disabled	Disabled	Disabled	Enabled	0
5	0	Permit	Disabled	Disabled	Disabled	Enabled	0
6	0	Permit	Disabled	Disabled	Disabled	Enabled	0
7	0	Permit	Disabled	Disabled	Disabled	Enabled	0
8	0	Permit	Disabled	Disabled	Disabled	Enabled	0
9	0	Permit	Disabled	Disabled	Disabled	Enabled	0
10	0	Permit	Disabled	Disabled	Disabled	Enabled	0
11	0	Permit	Disabled	Disabled	Disabled	Enabled	0
12	0	Permit	Disabled	Disabled	Disabled	Enabled	0
13	0	Permit	Disabled	Disabled	Disabled	Enabled	0
14	0	Permit	Disabled	Disabled	Disabled	Enabled	0
15	0	Permit	Disabled	Disabled	Disabled	Enabled	0
16	0	Permit	Disabled	Disabled	Disabled	Enabled	0
17	0	Permit	Disabled	Disabled	Disabled	Enabled	0
18	0	Permit	Disabled	Disabled	Disabled	Enabled	0
19	0	Permit	Disabled	Disabled	Disabled	Enabled	0
20	0	Permit	Disabled	Disabled	Disabled	Enabled	0
21	0	Permit	Disabled	Disabled	Disabled	Enabled	0
22	0	Permit	Disabled	Disabled	Disabled	Enabled	16818
23	0	Permit	Disabled	Disabled	Disabled	Enabled	0
24	0	Permit	Disabled	Disabled	Disabled	Enabled	0
25	0	Permit	Disabled	Disabled	Disabled	Enabled	0
26	0	Permit	Disabled	Disabled	Disabled	Enabled	0

Apply Reset

Parameter description:

- **Port :**

  The logical port for the settings contained in the same row.

- **Policy ID :**

  Select the policy to apply to this port. The allowed values are 1 through 8. The default value is 1.

- **Action :**

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

- **Rate Limiter ID :**

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

- **Port Redirect :**

  Select which port frames are redirected on. The allowed values are Disabled or a specific port number. The default value is "Disabled".

- **Shutdown :**

  Specify the port shut down operation of this port. The allowed values are:

Enabled: If a frame is received on the port, the port will be disabled.

Disabled: Port shut down is disabled.

The default value is "Disabled".

- **State :**

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

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

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

  The default value is "Enabled".

- **Counter :**

  Counts the number of frames that match this ACE.

- **Buttons**

  Apply – Click to apply changes.

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

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

  You can click them for refresh the ACL Port Configuration or clear them by manual.

3-2.2 Rate Limiters

The section describes how to configure the switch's ACL Rate Limiter parameters. The Rate Limiter Level from 1 to 12 that allow user to set rate limiter value and units with pps.

Web Interface

To configure ACL Rate Limiter in the web interface:
1. Click Configuration, ACL, then Rate Limiter
2. To specific the Rate field and the range from 0 to 131071.
3. To scroll the Unit with pps or kbps
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: The ACL Rate Limiter Configuration

Parameter description:

- **Rate Limiter ID :**

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

- **Rate**

  The allowed values are: 0-131071 in pps or 0, 100, 200, 300, …, 1000000 in kbps.

- **Buttons**

  Apply – Click to apply changes.

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

3-2.3 Access Control List

The section describes how to configure Access Control List rule. An Access Control List (ACL) is a sequential list of permit or deny conditions that apply to IP addresses, MAC addresses, or other more specific criteria. This switch tests ingress packets against the conditions in an ACL one by one. A packet will be accepted as soon as it matches a permit rule, or dropped as soon as it matches a deny rule. If no rules match, the frame is accepted. Other actions can also be invoked when a matching packet is found, including rate limiting, copying matching packets to another port or to the system log, or shutting down a port.

This page shows the Access Control List (ACL), which is made up of the ACEs defined on this switch. Each row describes the ACE that is defined. The maximum number of ACEs is 256 on each switch. Click on the lowest plus sign to add a new ACE to the list. The reserved ACEs used for internal protocol, cannot be edited or deleted, the order sequence cannot be changed an the priority is highest

Web Interface

To configure Access Control List in the web interface:
1. Click Configuration, ACL, then Configuration

2. Click the ⊕ button to add a new ACL, or use the other ACL modification buttons to specify the editing action (i.e., edit, delete, or moving the relative position of entry in the list)
3. To specific the parameter of the ACE
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.
6. When editing an entry on the ACE Configuration page, note that the Items displayed depend on various selections, such as Frame Type and IP Protocol Type. Specify the relevant criteria to be matched for this rule, and set the actions to take when a rule is matched (such as Rate Limiter, Port Copy, Logging, and Shutdown).

Figure 3-2.3: The Access Control List Configuration

Parameter description:

- **Name :**

    Indicates the name of the ACE. Maximum length of the ACE Name String is 32. All ASCII printable characters (except double quotation, less-than sign, greater-than sign) can be used to form the ACE Name.

- **Ingress Port :**

    Select the ingress port for which this ACE applies.

    All: The ACE applies to all port.

    Port n: The ACE applies to this port number, where n is the number of the switch port.

- **Policy Filter :**

    Specify the policy number filter for this ACE.

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

    Specific: If you want to filter a specific policy with this ACE, choose this value. Two field for entering an policy value and bitmask appears.

- **Policy Value :**

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

- **Policy Bitmask :**

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

- **Frame Type :**

    Select the frame type for this ACE. These frame types are mutually exclusive.

    Any: Any frame can match this ACE.

    Ethernet Type: Only Ethernet Type frames can match this ACE. The IEEE 802.3 describes the value of Length/Type Field specifications to be greater than or equal to 1536 decimal (equal to 0600 hexadecimal).

    ARP: Only ARP frames can match this ACE. Notice the ARP frames won't match the ACE with Ethernet type.

    IPv4: Only IPv4 frames can match this ACE. Notice the IPv4 frames won't match the ACE with Ethernet type.

- **Action :**

    Specify the action to take with a frame that hits this ACE.

    Permit: The frame that hits this ACE is granted permission for the ACE operation.

    Deny: The frame that hits this ACE is dropped.

- **Rate Limiter :**

    Specify the rate limiter in number of base units. The allowed range is 1 to 12. Disabled indicates that the rate limiter operation is disabled.

- **Port Redirect :**

    Frames that hit the ACE are redirected to the port number specified here. The allowed range is the same as the switch port number range. Disabled indicates that the port redirect operation is disabled.

- **Shutdown :**

Specify the port shut down operation of the ACE. The allowed values are:

Enabled: If a frame matches the ACE, the ingress port will be disabled.

Disabled: Port shut down is disabled for the ACE.

- **Counter :**

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

  Modification Buttons

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

  : Inserts a new ACE before the current row.

  : Edits the ACE row.

  : Moves the ACE up the list.

  : Moves the ACE down the list.

  : Deletes the ACE.

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

MAC Parameters

- **SMAC Filter**

  (Only displayed when the frame type is Ethernet Type or ARP.)
  Specify the source MAC filter for this ACE.
  Any: No SMAC filter is specified. (SMAC filter status is "don't-care".)
  Specific: If you want to filter a specific source MAC address with this ACE, choose this value. A field for entering an SMAC value appears.

- **SMAC Value**

  When "Specific" is selected for the SMAC filter, you can enter a specific source MAC address. The legal format is "xx-xx-xx-xx-xx-xx" or "xx.xx.xx.xx.xx.xx" or "xxxxxxxxxxxx" (x is a hexadecimal digit). A frame that hits this ACE matches this SMAC value.

- **DMAC Filter**

  Specify the destination MAC filter for this ACE.
  Any: No DMAC filter is specified. (DMAC filter status is "don't-care".)
  MC: Frame must be multicast.
  BC: Frame must be broadcast.
  UC: Frame must be unicast.
  Specific: If you want to filter a specific destination MAC address with this ACE, choose this value. A field for entering a DMAC value appears.

- **DMAC Value**

  When "Specific" is selected for the DMAC filter, you can enter a specific destination MAC address. The legal format is "xx-xx-xx-xx-xx-xx" or "xx.xx.xx.xx.xx.xx" or "xxxxxxxxxxxx" (x is a hexadecimal digit). A frame that hits this ACE matches this DMAC value.

VLAN Parameters

- **VLAN ID Filter**

  Specify the VLAN ID filter for this ACE.
  Any: No VLAN ID filter is specified. (VLAN ID filter status is "don't-care".)
  Specific: If you want to filter a specific VLAN ID with this ACE, choose this

value. A field for entering a VLAN ID number appears.

- **VLAN ID**

  When "Specific" is selected for the VLAN ID filter, you can enter a specific VLAN ID number. The allowed range is 1 to 4094. A frame that hits this ACE matches this VLAN ID value.

- **Tag Priority**

  Specify the tag priority for this ACE. A frame that hits this ACE matches this tag priority. The allowed number range is 0 to 7. The value Any means that no tag priority is specified (tag priority is "don't-care".)

MAC Parameters

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

- **ARP/RARP**

  Specify the available ARP/RARP opcode (OP) flag for this ACE.

  Any: No ARP/RARP OP flag is specified. (OP is "don't-care".)

  ARP: Frame must have ARP/RARP opcode set to ARP.

  RARP: Frame must have ARP/RARP opcode set to RARP.

  Other: Frame has unknown ARP/RARP Opcode flag.

- **Request/Reply**

  Specify the available ARP/RARP opcode (OP) flag for this ACE.

  Any: No ARP/RARP OP flag is specified. (OP is "don't-care".)

  Request: Frame must have ARP Request or RARP Request OP flag set.

  Reply: Frame must have ARP Reply or RARP Reply OP flag.

- **Sender IP Filter**

  Specify the sender IP filter for this ACE.

  Any: No sender IP filter is specified. (Sender IP filter is "don't-care".)

  Host: Sender IP filter is set to Host. Specify the sender IP address in the SIP Address field that appears.

  Network: Sender IP filter is set to Network. Specify the sender IP address and sender IP mask in the SIP Address and SIP Mask fields that appear.

- **Sender IP Address**

  When "Host" or "Network" is selected for the sender IP filter, you can enter a specific sender IP address in dotted decimal notation.

- **Sender IP Mask**

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

- **Target IP Filter**

  Specify the target IP filter for this specific ACE.

  Any: No target IP filter is specified. (Target IP filter is "don't-care".)

  Host: Target IP filter is set to Host. Specify the target IP address in the Target IP Address field that appears.

  Network: Target IP filter is set to Network. Specify the target IP address and target IP mask in the Target IP Address and Target IP Mask fields that appear.

- **Target IP Address**

  When "Host" or "Network" is selected for the target IP filter, you can enter a

specific target IP address in dotted decimal notation.

- **Target IP Mask**

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

- **ARP SMAC Match**

  Specify whether frames can hit the action according to their sender hardware address field (SHA) settings.

  0: ARP frames where SHA is not equal to the SMAC address.

  1: ARP frames where SHA is equal to the SMAC address.

  Any: Any value is allowed ("don't-care").

- **RARP DMAC Match**

  Specify whether frames can hit the action according to their target hardware address field (THA) settings.

  0: RARP frames where THA is not equal to the DMAC address.

  1: RARP frames where THA is equal to the DMAC address.

  Any: Any value is allowed ("don't-care").

- **IP/Ethernet Length**

  Specify whether frames can hit the action according to their ARP/RARP hardware address length (HLN) and protocol address length (PLN) settings.

  0: ARP/RARP frames where the HLN is not equal to Ethernet (0x06) or the (PLN) is not equal to IPv4 (0x04).

  1: ARP/RARP frames where the HLN is equal to Ethernet (0x06) and the (PLN) is equal to IPv4 (0x04).

  Any: Any value is allowed ("don't-care").

- **IP**

  Specify whether frames can hit the action according to their ARP/RARP hardware address space (HRD) settings.

  0: ARP/RARP frames where the HLD is not equal to Ethernet (1).

  1: ARP/RARP frames where the HLD is equal to Ethernet (1).

  Any: Any value is allowed ("don't-care").

- **Ethernet**

  Specify whether frames can hit the action according to their ARP/RARP protocol address space (PRO) settings.

  0: ARP/RARP frames where the PRO is not equal to IP (0x800).

  1: ARP/RARP frames where the PRO is equal to IP (0x800).

  Any: Any value is allowed ("don't-care").

IP Parameters

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

- **IP Protocol Filter**

  Specify the IP protocol filter for this ACE.

  Any: No IP protocol filter is specified ("don't-care").

  Specific: If you want to filter a specific IP protocol filter with this ACE, choose this value. A field for entering an IP protocol filter appears.

ICMP: Select ICMP to filter IPv4 ICMP protocol frames. Extra fields for defining ICMP parameters will appear. These fields are explained later in this help file.

UDP: Select UDP to filter IPv4 UDP protocol frames. Extra fields for defining UDP parameters will appear. These fields are explained later in this help file.

TCP: Select TCP to filter IPv4 TCP protocol frames. Extra fields for defining TCP parameters will appear. These fields are explained later in this help file.

- **IP Protocol Value**

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

- **IP TTL**

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

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

  non-zero: IPv4 frames with a Time-to-Live field greater than zero must be able to match this entry.

  Any: Any value is allowed ("don't-care").

- **IP Fragment**

  Specify the fragment offset settings for this ACE. This involves the settings for the More Fragments (MF) bit and the Fragment Offset (FRAG OFFSET) field for an IPv4 frame.

  No: IPv4 frames where the MF bit is set or the FRAG OFFSET field is greater than zero must not be able to match this entry.

  Yes: IPv4 frames where the MF bit is set or the FRAG OFFSET field is greater than zero must be able to match this entry.

  Any: Any value is allowed ("don't-care").

- **IP Option**

  Specify the options flag setting for this ACE.

  No: IPv4 frames where the options flag is set must not be able to match this entry.

  Yes: IPv4 frames where the options flag is set must be able to match this entry.

  Any: Any value is allowed ("don't-care").

- **SIP Filter**

  Specify the source IP filter for this ACE.

  Any: No source IP filter is specified. (Source IP filter is "don't-care".)

  Host: Source IP filter is set to Host. Specify the source IP address in the SIP Address field that appears.

  Network: Source IP filter is set to Network. Specify the source IP address and source IP mask in the SIP Address and SIP Mask fields that appear.

- **SIP Address**

  When "Host" or "Network" is selected for the source IP filter, you can enter a specific SIP address in dotted decimal notation.

- **SIP Mask**

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

- **DIP Filter**

Specify the destination IP filter for this ACE.

Any: No destination IP filter is specified. (Destination IP filter is "don't-care".)

Host: Destination IP filter is set to Host. Specify the destination IP address in the DIP Address field that appears.

Network: Destination IP filter is set to Network. Specify the destination IP address and destination IP mask in the DIP Address and DIP Mask fields that appear.

- **DIP Address**

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

- **DIP Mask**

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

ICMP Parameters

- **ICMP Type Filter**

  Specify the ICMP filter for this ACE.

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

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

- **ICMP Type Value**

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

- **ICMP Code Filter**

  Specify the ICMP code filter for this ACE.

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

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

- **ICMP Code Value**

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

TCP/UDP Parameters

- **TCP/UDP Source Filter**

  Specify the TCP/UDP source filter for this ACE.

  Any: No TCP/UDP source filter is specified (TCP/UDP source filter status is "don't-care").

  Specific: If you want to filter a specific TCP/UDP source filter with this ACE, you can enter a specific TCP/UDP source value. A field for entering a TCP/UDP source value appears.

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

- **TCP/UDP Source No.**

  When "Specific" is selected for the TCP/UDP source filter, you can enter a

specific TCP/UDP source value. The allowed range is 0 to 65535. A frame that hits this ACE matches this TCP/UDP source value.

- **TCP/UDP Source Range**

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

- **TCP/UDP Destination Filter**

  Specify the TCP/UDP destination filter for this ACE.

  Any: No TCP/UDP destination filter is specified (TCP/UDP destination filter status is "don't-care").

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

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

- **TCP/UDP Destination Number**

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

- **TCP/UDP Destination Range**

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

- **TCP FIN**

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

  0: TCP frames where the FIN field is set must not be able to match this entry.

  1: TCP frames where the FIN field is set must be able to match this entry.

  Any: Any value is allowed ("don't-care"). TCP SYN

- **TCP SYN**

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

  0: TCP frames where the SYN field is set must not be able to match this entry.

  1: TCP frames where the SYN field is set must be able to match this entry.

  Any: Any value is allowed ("don't-care").

- **TCP RST**

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

  0: TCP frames where the RST field is set must not be able to match this entry.

  1: TCP frames where the RST field is set must be able to match this entry.

  Any: Any value is allowed ("don't-care").

- **TCP PSH**

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

  0: TCP frames where the PSH field is set must not be able to match this entry.

  1: TCP frames where the PSH field is set must be able to match this entry.

  Any: Any value is allowed ("don't-care").

- **TCP ACK**

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

  0: TCP frames where the ACK field is set must not be able to match this entry.

  1: TCP frames where the ACK field is set must be able to match this entry.

  Any: Any value is allowed ("don't-care").

- **TCP URG**

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

  0: TCP frames where the URG field is set must not be able to match this entry.

  1: TCP frames where the URG field is set must be able to match this entry.

  Any: Any value is allowed ("don't-care").

TCP/UDP Parameters

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

- **EtherType Filter**

  Specify the Ethernet type filter for this ACE.

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

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

- **Ethernet Type Value**

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

- **Buttons**

  Apply – Click to apply changes.

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

- **Auto-refresh:**

  To evoke the auto-refresh to refresh the information automatically.

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

  You can click them for refresh the ACL configuration or clear them by manual. Others remove all to clean up all ACL configurations on the table.

3-2.4 ACL Status

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

Web Interface

To display the ACL status in the web interface:
1. Click Configuration, ACL, then ACL status
2. If you want to auto-refresh the information then you need to evoke the "Auto-refresh".
3. Click " Refresh" to refresh the ACL Status

Figure 3-2.4: The ACL Status

ACL Status

User	Name	Ingress Port	Frame Type	Action	Rate Limiter	Port Redirect	CPU	CPU Once	Counter	Conflict
IP Management		All	IPv4/UDP 68 DHCP Server	Permit	Disabled	Disabled	Yes	No	0	No
IP Management		All	ARP	Permit	undefined	Disabled	Yes	No	5	No
Reserved		All	EType	Permit	undefined	Disabled	No	No	0	No
Reserved		All	EType	Permit	undefined	Disabled	No	No	0	No

Parameter description:

- **User :**

  Indicates the ACL user.

- **Name :**

  The name of the ACE.

- **Ingress Port :**

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

  All: The ACE will match all ingress port.

  Port: The ACE will match a specific ingress port.

- **Frame Type :**

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

  Any: The ACE will match any frame type.

  EType: The ACE will match Ethernet Type frames. Note that an Ethernet Type based ACE will not get matched by IP and ARP frames.

  ARP: The ACE will match ARP/RARP frames.

  IPv4: The ACE will match all IPv4 frames.

  IPv4/ICMP: The ACE will match IPv4 frames with ICMP protocol.

  IPv4/UDP: The ACE will match IPv4 frames with UDP protocol.

  IPv4/TCP: The ACE will match IPv4 frames with TCP protocol.

  IPv4/Other: The ACE will match IPv4 frames, which are not ICMP/UDP/TCP.
  IPv6: The ACE will match all IPv6 standard frames.

- **Action :**

  Indicates the forwarding action of the ACE.

Permit: Frames matching the ACE may be forwarded and learned.

Deny: Frames matching the ACE are dropped.

- **Rate Limiter :**

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

- **Port Redirect:**

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

- **CPU :**

  Forward packet that matched the specific ACE to CPU.

- **CPU Once :**

  Forward first packet that matched the specific ACE to CPU.

- **Counter :**

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

- **Conflict :**

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

- **Auto-refresh:**

  To evoke the auto-refresh to refresh the information automatically.

- **Upper right icon (Refresh)**

  You can click them for refresh the ACL status information by manual.

3-3 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.

3-3.1 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.

3-3.1.1 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 3-3.1.1: The Aggregation Mode Configuration

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.

3-3.2 Aggregation View

This page provides a status overview for Aggregation View status for all ports.

Web Interface

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

1. Click Configuration, Static Trunk, and Aggregation View.
2. If you want to auto-refresh the information then you need to evoke the "Auto-refresh".
3. Click " Refresh" to refresh the Aggregation view.

Figure 3-3.2: The Aggregation View

Parameter description:

Hash Code Contributors

- **Group ID :**

  Indicates the group ID for the settings contained in the same row. Only one group ID is valid per port.

- **Name :**

  Link aggregation Group Name for its related Group ID.

- **Type :**

  This Group is Static aggregation or None (---).

- **Configured Ports :**

  Ports configured in this static trunk group.

- **Aggregated Ports :**

  The active ports in this static trunk group.

- **Inactive Ports :**

  The inactive ports in this static trunk group. Ports that is not aggregated may be due to link-down, management disabled, speed/duplex mismatched.

3-3.3 Port View

This page provides a status overview in a per-port based view. The re-enable checkbox can be used to re-enable speed/duplex mismatched ports that are disabled by static aggregation.

Web Interface

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

1. Click Configuration, Static Trunk, and Aggregation View.
2. If you want to auto-refresh the information then you need to evoke the "Auto-refresh".
3. Click " Refresh" to refresh the Aggregation view.

Figure 3-3.3: The Port View

Port View

Port	Group ID	Name	Inactive Reason	Re-Enable
1	1	LLAG1	Link Down	☐
2	1	LLAG1	Link Down	☐
3	1	LLAG1	Link Down	☐
4			Link Down	☐
21			Link Down	☐
22				☐
23			Link Down	☐
24			Link Down	☐
25			Link Down	☐
26			Link Down	☐
27			Link Down	☐
28			Link Down	☐

Apply

Parameter description:

Hash Code Contributors

● **Port :**

The port number

● **Group ID :**

The Static trunk group ID. Only one group ID is valid per port.

● **Name :**

Link aggregation Group Name for its related Group ID.

● **Inactive Reason :**

Indicates why a static group port member is not activated. Possible values may include : Linkdown, ACL, Loop(Loop Protection), ErrDis(Error Disable), StaticTrunk(Aggregation Disable). Ports not configured in any static group or active member ports will be blank on this field.

● **Re-Enable :**

The re-enable checkbox can be used to re-enable speed/duplex mismatched ports that are disabled by static aggregation. Static aggregation will automatically disable half-duplex ports. If speed mismatch exists in a static group, only ports with the highest speed remain enabled. Once a port is disabled by static aggregation, Re-Enable is the only way to activate it.

3-3.4 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.

3-3.4.1 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 3-3.4.1: The LACP Port Configuration

LACP Port Configuration

Port	LACP Enabled	Key		Role	
*	☐	<> ▼		<> ▼	
1	☐	Auto ▼		Active ▼	
2	☐	Auto ▼		Active ▼	
3	☐	Auto ▼		Active ▼	
4	☐	Auto ▼		Active ▼	
5	☐	Auto ▼		Active ▼	
6	☐	Auto ▼		Active ▼	
7	☐	Auto ▼		Active ▼	
8	☐	Auto ▼		Active ▼	
9	☐	Auto ▼		Active ▼	
10	☐	Auto ▼		Active ▼	
11	☐	Auto ▼		Active ▼	
12	☐	Auto ▼		Active ▼	
13	☐	Auto ▼		Active ▼	
14	☐	Auto ▼		Active ▼	
15	☐	Auto ▼		Active ▼	
16	☐	Auto ▼		Active ▼	
17	☐	Auto ▼		Active ▼	
18	☐	Auto ▼		Active ▼	
19	☐	Auto ▼		Active ▼	
20	☐	Auto ▼		Active ▼	
21	☐	Auto ▼		Active ▼	
22	☐	Auto ▼		Active ▼	
23	☐	Auto ▼		Active ▼	
24	☐	Auto ▼		Active ▼	
25	☐	Auto ▼		Active ▼	
26	☐	Auto ▼		Active ▼	
27	☐	Auto ▼		Active ▼	
28	☐	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 per stack.

- **Key :**

  The Key value incurred by the port, range 1-65535 . The Auto setting will set the key as appropriate by the physical link speed, 10Mb = 1, 100Mb = 2, 1Gb = 3. Using the Specific setting, a user-defined value can be entered. Ports with

the same Key value can participate in the same aggregation group, while ports with different keys cannot.

- **Role :**

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

- **Buttons**

  Apply – Click to apply changes.

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

3-3.4.2 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 3-3.4.2: The LACP System Status

LACP System Status

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

Auto-refresh ☐ Refresh

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/stack. 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.

3-3.4.3 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 3-3.4.3: The LACP Status

LACP Status   Auto-refresh ☐ [Refresh]

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	-	-	-	-
19	No	-	-	-	-
20	No	-	-	-	-
21	No	-	-	-	-
22	No	-	-	-	-
23	No	-	-	-	-
24	No	-	-	-	-
25	No	-	-	-	-
26	No	-	-	-	-
27	No	-	-	-	-
28	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.

3-3.4.4 Port Statistics
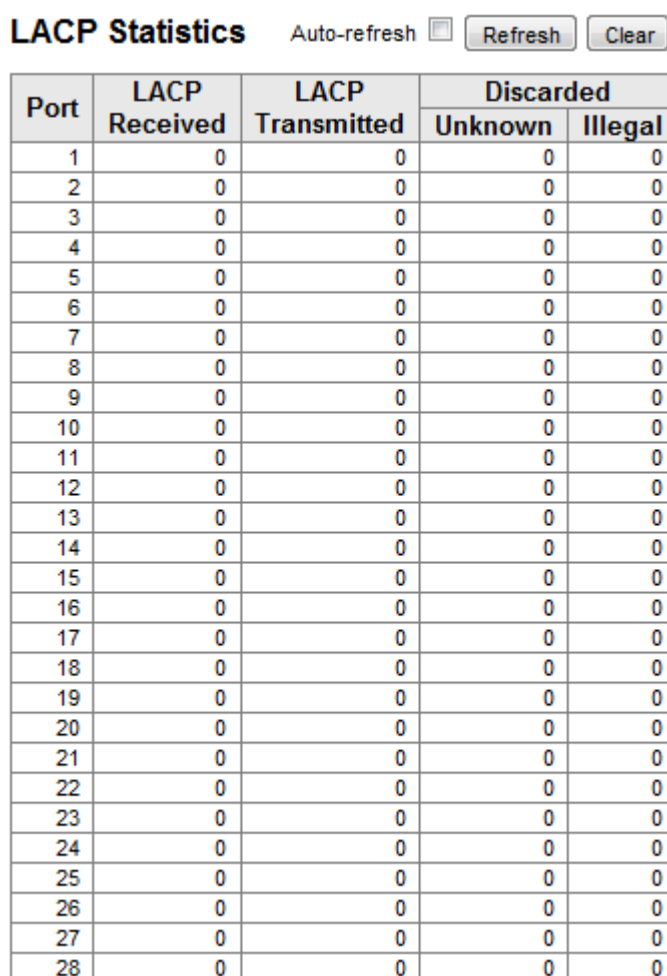
This section describes that when you complete to set LACP function on the switch then it provides a Port Statistics overview for all LACP instances

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 3-3.4.4: 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
19	0	0	0	0
20	0	0	0	0
21	0	0	0	0
22	0	0	0	0
23	0	0	0	0
24	0	0	0	0
25	0	0	0	0
26	0	0	0	0
27	0	0	0	0
28	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.

3-4 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.
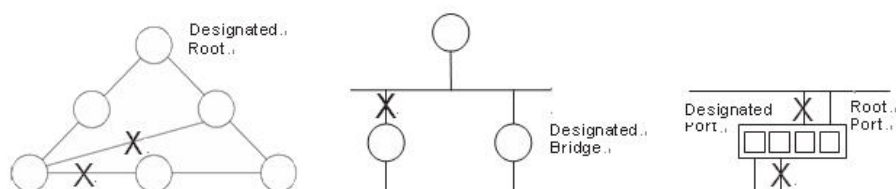
Once a stable network topology has been established, all bridges listen for Hello BPDUs (Bridge Protocol Data Units) transmitted from the Root Bridge. If a bridge does not get a Hello BPDU after a predefined interval (Maximum Age), the bridge assumes that the link to the Root Bridge is down. This bridge will then initiate negotiations with other bridges to reconfigure the network to reestablish a valid network topology.

3-4.1 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 Stack.

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 3-4.1: The STP Bridge Configuration

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 <= (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 apply changes.

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

3-4.2 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 3-4.2: The MSTI Configuration

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 mapped to it.)

- **Buttons**

  Apply – Click to apply changes.

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

3-4.3 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 3-4.3: The MSTI Configuration

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 apply changes.

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

3-4.4 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 scroll 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 3-4.4: 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	Restricted TCN	BPDU Guard	Point-to-point
-	☐	Auto	128	Non-Edge	☑	☐	☐	☐	Forced True

CIST Normal Port Configuration

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

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

3-4.5 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. The aggregation settings are stack global.

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 3-4.5: The MSTI Port Configuration
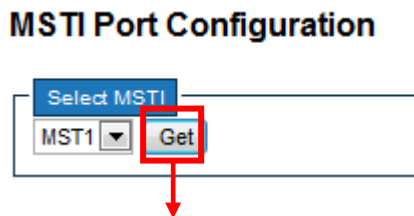
MST1 MSTI Port Configuration

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 ▼
19	Auto ▼		128 ▼
20	Auto ▼		128 ▼
21	Auto ▼		128 ▼
22	Auto ▼		128 ▼
23	Auto ▼		128 ▼
24	Auto ▼		128 ▼
25	Auto ▼		128 ▼
26	Auto ▼		128 ▼
27	Auto ▼		128 ▼
28	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 apply changes.

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

3-4.6 Bridge Status

After you complete the MSTI Port configuration, you could 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 3-4.6: The STP Bridges status

STP Bridges   Auto-refresh ☐ [Refresh]

| MSTI | Bridge ID | Root | | | Topology Flag | Topology Change Last |
		ID	Port	Cost		
CIST	80:00-00:01:C1:00:00:00	80:00-00:01:C1:00:00:00	-	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.

3-4.7 Port Status

After you complete the STP configuration, you could 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 3-4.7: The STP Port status

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	-
19	Non-STP	Forwarding	-
20	Non-STP	Forwarding	-
21	Non-STP	Forwarding	-
22	Non-STP	Forwarding	-
23	Non-STP	Forwarding	-
24	Non-STP	Forwarding	-
25	Non-STP	Forwarding	-
26	Non-STP	Forwarding	-
27	Non-STP	Forwarding	-
28	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.

3-4.8 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 3-4.8: 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.

3-5 MRSTP

The MRSTP (Multiple Rapid Spanning Tree Protocol) is not standard Spanning tree protocol. It means the switch supports the MRSTP then it exist several spanning trees at the same time and these spanning trees won't affect to each other.

A switch supports MRSTP and accepts two or more RSTP in signal equipment. These two RSTP group have different ports to join them and between different Hello Time, Max Age, Forwarding Delay. The MRSTP configuration method was the same as RSTP, but it needs to set for several times. Otherwise each MRSTP could be set for differential parameters.

3-5.1 Instance

The section describes switch to provide an MRSTP instance table which include information (Instance, State, Version, Priority, Hello time, Max-age and Forwarding delay) of all MRSTP instances provisioned in the particular MRSTP region which the bridge belongs to. Through this table, additional MRSTP configuration data can be applied and MRSTP status can be retrieved.

Web Interface

To configure the MRSTP Instance parameters in the web interface:

1. Click Configuration, MRSTP, Instance
2. Scroll to select enable or disable which Global configuration
3. Evoke which state and instance you will set on the switch..
4. Scroll to set includes Version, Hello-time, Max-age and Forwarding Del parameter.
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 3-5.1: The MRSTP Instance Configuration.

MRSTP Instance Configuration

Global State | Disabled

Instance	State	Version	Priority	Hello-Time	Max-age	FW-Delay
*	☐	<>	<>	<>	<>	<>
1	☐	RSTP	32768	2	20	15
2	☐	RSTP	32768	2	20	15
3	☐	RSTP	32768	2	20	15
4	☐	RSTP	32768	2	20	15
5	☐	RSTP	32768	2	20	15
6	☐	RSTP	32768	2	20	15
7	☐	RSTP	32768	2	20	15
8	☐	RSTP	32768	2	20	15
9	☐	RSTP	32768	2	20	15
10	☐	RSTP	32768	2	20	15
11	☐	RSTP	32768	2	20	15
12	☐	RSTP	32768	2	20	15

Save | Reset

Parameter description:

● **Global State:**

Scroll to select "Enabled" or "disabled" the Global MRSTP state on the switch.

● **Instance :**

Every MRSTP instance need to have a unique instance ID.

● **State :**

Controls whether an MRSTP instance is enabled or not. To really enable an MRSTP instance, the MRSTP Global State must also be enabled.

- **Version :**

  The STP protocol version setting. Valid values are STP and RSTP.

- **Priority :**

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

- **Hello-time :**

  Available value range: 1 / 2

  In contrast with RSTP, Hello Time in MRSTP that needs per port setting for the CIST.

- **Max-age :**

  Available value range: 6-40sec. The same definition was as in the RSTP protocol.

- **FW Delay (Forwarding delay) :**

  Available value range: 4-30sec. The same definition was as in the RSTP protocol.

- **Buttons**

  Apply – Click to apply changes.

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

3-5.2 Port Configuration

The chapter describes MRSTP port configuration after you configure the MRSTP instance then you can assign the port to join what instance and set the parameters for MRSTP implementation.

Web Interface

To configure the MRSTP Port configuration in the web interface:

1. Click Configuration, MRSTP, Port Configuration
2. Scroll to select what instance you want to assign to the Port.
3. Scroll to select includes Path Cost, Priority, Admin Edge and Admin P2P parameters.
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 3-5.2: The MRSTP Port Configuration.

MRSTP Port Configuration

Port	Instance	Path Cost		Priority	Admin Edge	Admin P2P	Migrate Check
*	<>	<>		<>	<>	<>	☐
1	None	Auto		128	Edge	Auto	☐
2	None	Auto		128	Edge	Auto	☐
3	None	Auto		128	Edge	Auto	☐
4	None	Auto		128	Edge	Auto	☐
5	None	Auto		128	Edge	Auto	☐
6	None	Auto		128	Edge	Auto	☐
7	None	Auto		128	Edge	Auto	☐
8	None	Auto		128	Edge	Auto	☐
9	None	Auto		128	Edge	Auto	☐
10	None	Auto		128	Edge	Auto	☐
11	None	Auto		128	Edge	Auto	☐
12	None	Auto		128	Edge	Auto	☐
13	None	Auto		128	Edge	Auto	☐
14	None	Auto		128	Edge	Auto	☐
15	None	Auto		128	Edge	Auto	☐
16	None	Auto		128	Edge	Auto	☐
17	None	Auto		128	Edge	Auto	☐
18	None	Auto		128	Edge	Auto	☐
19	None	Auto		128	Edge	Auto	☐
20	None	Auto		128	Edge	Auto	☐
21	None	Auto		128	Edge	Auto	☐
22	None	Auto		128	Edge	Auto	☐
23	None	Auto		128	Edge	Auto	☐
24	None	Auto		128	Edge	Auto	☐
25	None	Auto		128	Edge	Auto	☐
26	None	Auto		128	Edge	Auto	☐
27	None	Auto		128	Edge	Auto	☐
28	None	Auto		128	Edge	Auto	☐

Apply Reset

Parameter description:

● **Port:**

The switch port number of the MRSTP port.

- **Instance :**

    Controls a switch port whether to participate in an MRSTP Bridge Instance or not.

- **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 path cost. (See above)..

- **Admin Edge :**

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

- **Admin P2P :**

    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.

- **Migrate Check :**

    It forces the port sending out an RSTP BPDU instead of a legacy STP BPDU at next transmission. The benefit of this operation is to make the port quickly get back to act as an RSTP port .

- **Buttons**

    Apply – Click to apply changes.

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

3-5.3 Port Status

The section describes switch to provide an MRSTP Port status table. You will see the MRSTP configuration result and get each port join the MRSTP group and its statistics

Web Interface

To view the MRSTP Port status in the web interface:

1. Click Configuration, MRSTP, Port Status
2. Evoke "Auto-refresh" then the switch will update the table automatically.
4. Click the Refresh then it will update the table manually.

Figure 3-5.3: The MRSTP Port Status.

MRSTP Port Status   Auto-refresh ☐ [Refresh]

Port	Instance	State	Role	PathCost	PathCost Config.	Priority	Admin Edge	Admin P2P
1	None	NON-MRSTP	none	0	0	128	Edge	Auto
2	None	NON-MRSTP	none	0	0	128	Edge	Auto
3	None	NON-MRSTP	none	0	0	128	Edge	Auto
4	None	NON-MRSTP	none	0	0	128	Edge	Auto
5	None	NON-MRSTP	none	0	0	128	Edge	Auto
6	None	NON-MRSTP	none	0	0	128	Edge	Auto
7	None	NON-MRSTP	none	0	0	128	Edge	Auto
8	None	NON-MRSTP	none	0	0	128	Edge	Auto
9	None	NON-MRSTP	none	0	0	128	Edge	Auto
10	None	NON-MRSTP	none	0	0	128	Edge	Auto
11	None	NON-MRSTP	none	0	0	128	Edge	Auto
12	None	NON-MRSTP	none	0	0	128	Edge	Auto
13	None	NON-MRSTP	none	0	0	128	Edge	Auto
14	None	NON-MRSTP	none	0	0	128	Edge	Auto
15	None	NON-MRSTP	none	0	0	128	Edge	Auto
16	None	NON-MRSTP	none	0	0	128	Edge	Auto
17	None	NON-MRSTP	none	0	0	128	Edge	Auto
18	None	NON-MRSTP	none	0	0	128	Edge	Auto
19	None	NON-MRSTP	none	0	0	128	Edge	Auto
20	None	NON-MRSTP	none	0	0	128	Edge	Auto
21	None	NON-MRSTP	none	0	0	128	Edge	Auto
22	None	NON-MRSTP	none	0	0	128	Edge	Auto
23	None	NON-MRSTP	none	0	0	128	Edge	Auto
24	None	NON-MRSTP	none	0	0	128	Edge	Auto
25	None	NON-MRSTP	none	0	0	128	Edge	Auto
26	None	NON-MRSTP	none	0	0	128	Edge	Auto
27	None	NON-MRSTP	none	0	0	128	Edge	Auto
28	None	NON-MRSTP	none	0	0	128	Edge	Auto

Parameter description:

- **Port：**

  The physical port index, available value is 1 to 24.

- **Instance :**

  Every MRSTP instance need to have a unique instance ID

- **Status :**

  To display the port join MRSTP status.

- **Role :**

  If "Yes" causes the Port not to be selected as Root Port for the CIST or any MSTI, even it has the best spanning tree priority vector. Such a Port will be selected as an Alternate Port after the Root Port has been selected. This parameter is "None" by default. If set, it can cause lack of spanning tree connectivity. It is set by a network administrator to prevent bridges external to a core region of the network influencing the spanning tree active topology, possibly because those bridges are not under the full control of the

administrator.

- **Path Cost :**

    To display the port path cost. If path cost is show zero, the STP will get the recommended value resulted from auto-negotiation of the link accordingly and display this value in the field of Path Cost Status. Otherwise, it may show the value that the administrator set up in Configured Path Cost and Path Cost Status.

- **Priority :**

    To display the port priority. Priority here means Port Priority. Port Priority and Port Number are mixed to form the Port ID. Port IDs are often compared in order to determine which port of a bridge would become the Root Port. The range is 0 – 240.

- **Admin Edge :**

    To display the port admin edge status. If you don't set any value then it will show default value is Edge.

- **Admin P2P :**

    To display the port admin P2P status. If you don't set any value then it will show default value is Auto.

- **Auto-refresh:**

    To evoke the auto-refresh to refresh the information automatically.

- **Upper right icon (Refresh)**

    You can click them for refresh the MRSTP port status information by manual.

3-6 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 cannot 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.

3-6.1 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 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 3-5.1: The IGMP Snooping Configuration.

IGMP Snooping Configuration

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

Port Related Configuration

Port	Router Port	Fast Leave	Throttling
*	☐	☐	<>
1	☐	☐	unlimited
2	☐	☐	unlimited
3	☐	☐	unlimited
4	☐	☐	unlimited
5	☐	☐	unlimited
6	☐	☐	unlimited
7	☐	☐	unlimited
8	☐	☐	unlimited
9	☐	☐	unlimited
10	☐	☐	unlimited
11	☐	☐	unlimited
12	☐	☐	unlimited
13	☐	☐	unlimited
14	☐	☐	unlimited
15	☐	☐	unlimited
16	☐	☐	unlimited
17	☐	☐	unlimited
18	☐	☐	unlimited
19	☐	☐	unlimited
20	☐	☐	unlimited
21	☐	☐	unlimited
22	☐	☐	unlimited
23	☐	☐	unlimited
24	☐	☐	unlimited
25	☐	☐	unlimited
26	☐	☐	unlimited
27	☐	☐	unlimited
28	☐	☐	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**

    Apply – Click to apply changes.

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

3-5.2 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 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 3-5.2: The IGMP Snooping VLAN Configuration.

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 :**

  Apply – Click to apply 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.

3-5.3 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 3-5.3: The IGMP Snooping Port Group Filtering Configuration.

Parameter description:

● **Delete :**

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

● **Port :**

  The logical port for the settings..

● **Filtering Groups :**

  The IP Multicast Group that will be filtered.

● **Buttons:**

  Apply – Click to apply changes.

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

3-5.4 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 3-5.4: The IGMP Snooping Status.

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".

"DISABLE" denotes the specific interface is administratively disabled.

- **Queries Transmitted :**

    The number of Transmitted Queries.

- **Queries Received :**

    The number of Received Queries.

- **V1 Reports Received :**

    The number of Received V1 Reports.

- **V2 Reports Received :**

    The number of Received V2 Reports.

- **V3 Reports Received :**

    The number of Received V3 Reports.

- **V2 Leaves Received :**

    The number of Received V2 Leaves.

Router Port Contributors

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

Static denotes the specific port is configured to be a router port.

Dynamic denotes the specific port is learnt to be a router port.

Both denote the specific port is configured or learnt to be a router port.

- **Port :**

    Switch port number.

- **Status :**

    Indicate whether specific port is a router port or not.

- **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.

3-5.5 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 3-5.5: 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..

3-5.6 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 3-6.6: The IGMPv3 IPv4 SSM Information.

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..

3-6 MLD Snooping

Curiously enough, a network node that acts as a source of IPv6 multicast traffic is only an indirect participant in MLD snooping—it just provides multicast traffic, and MLD doesn't interact with it. (Note, however, that in an application like desktop conferencing a network node may act as both a source and an MLD host; but MLD interacts with that node only in its role as an MLD host.)

A source node creates multicast traffic by sending packets to a multicast address. In IPv6, addresses with the first eight bits set (that is, "FF" as the first two characters of the address) are multicast addresses, and any node that listens to such an address will receive the traffic sent to that address. Application software running on the source and destination systems cooperates to determine what multicast address to use. (Note that this is a function of the application software, not of MLD.)

When MLD snooping is enabled on a VLAN, the switch acts to minimize unnecessary multicast traffic. If the switch receives multicast traffic destined for a given multicast address, it forwards that traffic only to ports on the VLAN that have MLD hosts for that address. It drops that traffic for ports on the VLAN that have no MLD hosts
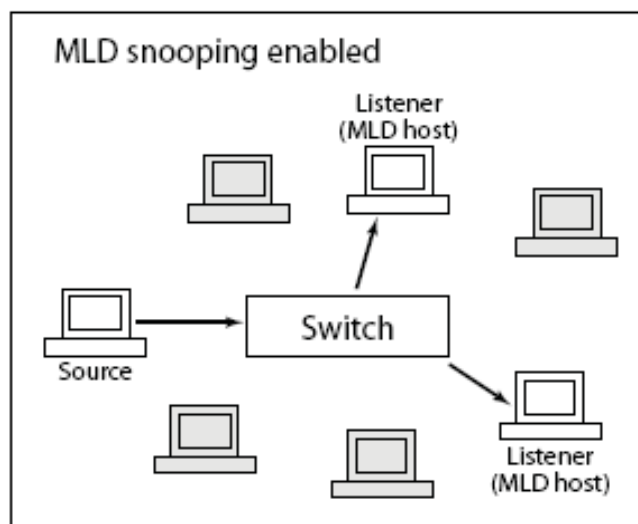
3-6.1 Basic Configuration

The section will let you understand how to configure the MLD Snooping basic configuration and the parameters.

Web Interface

To configure the MLD Snooping Configuration in the web interface:

1. Click Configuration, MLD Snooping, Basic Configuration
2. Evoke to enable or disable the Global configuration parameters
   Evoke the port to join Router port and Fast Leave.
3. Scroll to select the Throtting mode with unlimited or 1 to 10
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 3-6.1: The MLD Snooping Basic Configuration.

MLD Snooping Configuration

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

Port Related Configuration

Port	Router Port	Fast Leave	Throttling
*	☐	☐	<>
1	☐	☐	unlimited
2	☐	☐	unlimited
3	☐	☐	unlimited
4	☐	☐	unlimited
5	☐	☐	unlimited
6	☐	☐	unlimited
7	☐	☐	unlimited
8	☐	☐	unlimited
9	☐	☐	unlimited
10	☐	☐	unlimited
11	☐	☐	unlimited
12	☐	☐	unlimited
13	☐	☐	unlimited
14	☐	☐	unlimited
15	☐	☐	unlimited
16	☐	☐	unlimited
17	☐	☐	unlimited
18	☐	☐	unlimited
19	☐	☐	unlimited
20	☐	☐	unlimited
21	☐	☐	unlimited
22	☐	☐	unlimited
23	☐	☐	unlimited
24	☐	☐	unlimited
25	☐	☐	unlimited
26	☐	☐	unlimited
27	☐	☐	unlimited
28	☐	☐	unlimited

Apply   Reset

Parameter description:

- **Snooping Enabled :**

  Enable the Global MLD Snooping.

- **Unregistered IPMCv6 Flooding enabled :**

  Enable unregistered IPMCv6 traffic flooding. Please note that disabling unregistered IPMCv6 traffic flooding may lead to failure of Neighbor Discovery.

- **MLD SSM Range :**

  SSM (Source-Specific Multicast) Range allows the SSM-aware hosts and routers run the SSM service model for the groups in the address (Using IPv6 Address) range.

- **Proxy Enabled :**

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

- **Port:**

  The Port index what you enable or disable the MLD Snooping function.

- **Fast Leave :**

  To evoke to enable the fast leave on the port.

- **Router Port :**

  Specify which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or MLD querier. If an aggregation member port is selected as a router port, the whole aggregation will act as a router port.

- **Throttling :**

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

- **Buttons:**

  Apply – Click to apply changes.

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

3-6.2 VLAN Configuration

When MLD snooping is enabled on a VLAN, the switch acts to minimize unnecessary multicast traffic. If the switch receives multicast traffic destined for a given multicast address, it forwards that traffic only to ports on the VLAN that have MLD hosts for that address. It drops that traffic for ports on the VLAN that have no MLD hosts

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

Web Interface

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

1. Click Configuration, MLD Snooping, VLAN Configuration
2. Specify the VLAN ID with entries per page.
3. Click " Refresh" to refresh an entry of the MLD Snooping VLAN Configuration Information.
4. Click "<< or >> " to move to previous or next entry.

Figure 3-6.2: The MLD Snooping VLAN Configuration.

Parameter description:

- **VLAN ID :**

  The VLAN ID of the entry.

- **Snooping Enabled :**

  Enable the per-VLAN MLD Snooping. Only up to 32 VLANs can be selected.

- **MLD Querier :**

  A router sends MLD Query messages onto a particular link. This Router is called the Querier.. Enable the MLD Querier in the VLAN.

- **Compatibility :**

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

- **Rv :**

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

- **QI :**

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

- **QRI :**

  Query Response Interval. The Maximum Response Delay used to calculate the Maximum

Response Code inserted into the periodic General Queries. The allowed range is 0 to 31744 in tenths of seconds; default query response interval is 100 in tenths of seconds (10 seconds). .

- **LLQI (LMQI for IGMP) :**

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

- **URI :**

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

- **Upper right icon (Refresh, <<, >>)**
  You can click them for refresh the IGMP Group Status by manual, others for next/up page or entry..

- **Buttons:**

  Apply – Click to apply changes.

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

3-6.3 Port Group Filtering

The section describes that you could to set the Port Group Filtering in the MLD Snooping function. On the UI that you could add new filtering group and safety policy.

Web Interface

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

1. Click Configuration, MLD Snooping, Port Group Filtering Configuration
2. Click the Add new Filtering Group
3. Specify the Filtering Groups with entries per page.
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 3-6.3: The MLD Snooping Port Group Filtering Configuration

Parameter description:

- **Delete :**

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

- **Port :**

  The logical port for the settings. You can evoke to enable the port to join filtering Group

- **Filtering Groups**

  The IP Multicast Group that will be filtered.

- **Buttons:**

  Apply – Click to apply changes.

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

3-6.4 Status

The section describes when you complete the MLD Snooping and how to display the MLD Snooping Status and detail information. It will help you to find out the detail information of MLD Snooping status.

Web Interface

To display the MLD Snooping Status in the web interface:

1. Click Configuration, MLD Snooping, Status
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 MLD Snooping Status Information.
4. Click " Clear" to clear the MLD Snooping Status..

Figure 3-6.4: The MLD Snooping Status

Parameter description:

- **VLAN ID :**

    The VLAN ID of the entry.

- **Querier Version :**

    Working Querier Version currently.

- **Host Version :**

  Working Host Version currently.

- **Querier Status :**

  Show 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.

- **V1 Leaves Received :**

  The number of Received V1 Leaves.

- **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..

3-6.5 Group Information

The section describes user could set the MLD Snooping Groups Information. The "Start from VLAN", and "group" input fields allow the user to select the starting point in the MLD Group Table

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

Web Interface

To display the MLD Snooping Group information in the web interface:

1. Click Configuration, MLD 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 MLD Snooping Group Information.
4. Click " Clear" to clear the MLD Snooping Groups information..

Figure 3-6.5: The MLD Snooping Groups Information

Parameter description:

Navigating the MLD Group Table

Each page shows up to 99 entries from the MLD Group table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the MLD Group Table.The "Start from VLAN", and "group" input fields allow the user to select the starting point in the MLD Group Table. Clicking the button will update the displayed table starting from that or the next closest.

MLD Group 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 as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the button to start over.

MLD Snooping Information 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..

3-6.6 IPv6 SSM Information

The section describes the user to configure the Entries in the MLDv2 Information Table are shown on this page. The MLDv2 Information Table is sorted first by VLAN ID, then by group, and then by Port No. Different source addresses belong to the same group are treated as single entry.

Each page shows up to 64 entries from the MLDv2 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 MLDv2 Information Table. The "Start from VLAN", and "group" input fields allow the user to select the starting point in the MLDv2 Information Table.

Web Interface

To display the MLDv2 IPv6 SSM Information in the web interface:

1. Click Configuration, MLD Snooping, IPv6 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 MLDv2 IPv6 SSM Information.
4. Click "<< or >> " to move to previous or next entry.

Figure 3-6.6: The IPv6 SSM Information

Parameter description:

MLDv2 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.

3-7 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.

3-7.1 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 3-7.1: 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
19	Disabled	Receiver	Disabled
20	Disabled	Receiver	Disabled
21	Disabled	Receiver	Disabled
22	Disabled	Receiver	Disabled
23	Disabled	Receiver	Disabled
24	Disabled	Receiver	Disabled
25	Disabled	Receiver	Disabled
26	Disabled	Receiver	Disabled
27	Disabled	Receiver	Disabled
28	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 apply changes.

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

3-7.2 Port Group Allow

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 Allow in the web interface:

1. Click Configuration, MVR, Port Group Allow
2. Click the "Add new Allow Group" and specify the Start Address and End Address
3. Click the "Delete "to delete an entry of the MVR Groups.
4. Click "Apply " to save configuration.

Figure 3-7.2: The MVR Groups Information

MVR Port Group Allow Configuration

Delete	Port	Start Address	End Address
Delete	1 ▼		
Delete	1 ▼		
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.

3-7.3 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 3-7.2: 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.

3-7.4 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 3-7.4: The MVR Statistics Information

MVR Statistics

Auto-refresh ☐ [Refresh] [Clear]

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.

3-8 LLDP

The switch supports the LLDP. For current information on your switch model, The Link Layer Discovery Protocol (LLDP) provides a standards-based method for enabling switches to advertise themselves to adjacent devices and to learn about adjacent LLDP devices. The Link Layer Discovery Protocol (LLDP) is a vendor-neutral Link Layer protocol in the Internet Protocol Suite used by network devices for advertising their identity, capabilities, and neighbors on a IEEE 802 local area network, principally wired Ethernet. The protocol is formally referred to by the IEEE as Station and Media Access Control Connectivity Discovery specified in standards document IEEE 802.1AB.

3-8.1 LLDP Configuration

You can per port to do the LLDP configuration and the detail parameters, the settings will take effect immediately. This page allows the user to inspect and configure the current LLDP port settings.

Web Interface

To configure LLDP:

1. Click LLDP configuration
2. Modify LLDP timing parameters
3. Set the required mode for transmitting or receiving LLDP messages
4. Specify the information to include in the TLV field of advertised messages
5. Click Apply

Figure 3-8.1: The LLDP Configuration

LLDP Configuration

LLDP Parameters

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

Port	Mode	CDP aware	Port Descr	Sys Name	Sys Descr	Sys Capa	Mgmt Addr
*	<>	☐	☐	☐	☐	☐	☐
1	Disabled	☐	☑	☑	☑	☑	☑
2	Disabled	☐	☑	☑	☑	☑	☑
3	Disabled	☐	☑	☑	☑	☑	☑
4	Disabled	☐	☑	☑	☑	☑	☑
5	Disabled	☐	☑	☑	☑	☑	☑
6	Disabled	☐	☑	☑	☑	☑	☑
7	Disabled	☐	☑	☑	☑	☑	☑
8	Disabled	☐	☑	☑	☑	☑	☑
9	Disabled	☐	☑	☑	☑	☑	☑
10	Disabled	☐	☑	☑	☑	☑	☑
11	Disabled	☐	☑	☑	☑	☑	☑
12	Disabled	☐	☑	☑	☑	☑	☑
13	Disabled	☐	☑	☑	☑	☑	☑
14	Disabled	☐	☑	☑	☑	☑	☑
15	Disabled	☐	☑	☑	☑	☑	☑
16	Disabled	☐	☑	☑	☑	☑	☑
17	Disabled	☐	☑	☑	☑	☑	☑
18	Disabled	☐	☑	☑	☑	☑	☑
19	Disabled	☐	☑	☑	☑	☑	☑
20	Disabled	☐	☑	☑	☑	☑	☑
21	Disabled	☐	☑	☑	☑	☑	☑
22	Disabled	☐	☑	☑	☑	☑	☑
23	Disabled	☐	☑	☑	☑	☑	☑
24	Disabled	☐	☑	☑	☑	☑	☑
25	Disabled	☐	☑	☑	☑	☑	☑
26	Disabled	☐	☑	☑	☑	☑	☑
27	Disabled	☐	☑	☑	☑	☑	☑
28	Disabled	☐	☑	☑	☑	☑	☑

Apply   Reset

Parameter description:

LLDP Parameters

- **Tx Interval :**

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

- **Tx Hold :**

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

- **Tx Delay :**

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

- **Tx Reinit :**

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

LLDP Port Configuration

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

- **Port :**

  The switch port number of the logical LLDP port.

- **Mode :**

  Select LLDP mode.

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

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

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

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

- **CDP Aware :**

  Select CDP awareness.

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

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

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

  CDP TLV "Address" is mapped to the LLDP "Management Address" field. The CDP

address TLV can contain multiple addresses, but only the first address is shown in the LLDP neighbors' table.

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

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

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

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

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

- **Port Descr :**

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

- **Sys Name :**

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

- **Sys Descr :**

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

- **Sys Capa :**

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

- **Mgmt Addr :**

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

- **Buttons:**

    Apply – Click to apply changes.

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

3-8.2 LLDP Neighbours

This page provides a status overview for all LLDP neighbours. The displayed table contains a row for each port on which an LLDP neighbour is detected. The columns hold the following information:

Web Interface

To show LLDP neighbours:
1. Click LLDP Neighbours
2. Click Refresh for manual update web screen
3. Click Auto-refresh for auto-update web screen

Figure 3-8.2: The LLDP Neighbours information

NOTE: If none of the devices in your network support LLDP then the table will show "No LLDP neighbour information found".

Parameter description:

- **Local Port :**

  The port on which the LLDP frame was received.

- **Chassis ID :**

  The Chassis ID is the identification of the neighbour's LLDP frames.

- **Remote Port ID :**

  The Remote Port ID is the identification of the neighbour port.

- **System Name :**

  System Name is the name advertised by the neighbour unit.

- **Port Description :**

  Port Description is the port description advertised by the neighbour unit.

- **System Capabilities :**

  System Capabilities describes the neighbour unit's capabilities. The possible capabilities are:

  1. Other

  2. Repeater

  3. Bridge

  4. WLAN Access Point

  5. Router

  6. Telephone

  7. DOCSIS cable device

  8. Station only

9. Reserved

When a capability is enabled, the capability is followed by (+). If the capability is disabled, the capability is followed by (-).

- **System Description :**

  System Description is the port description advertised by the neighbour unit.

- **Management Address :**

  Management Address is the neighbour unit's address that is used for higher layer entities to assist discovery by the network management. This could for instance hold the neighbour's IP address.

- **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 LLDP Neighbours information by manual.

3-8.3 LLDP-MED Configuration

Media Endpoint Discovery is an enhancement of LLDP, known as LLDP-MED, that provides the following facilities:

Auto-discovery of LAN policies (such as VLAN, Layer 2 Priority and Differentiated services (Diffserv) settings) enabling plug and play networking.

Device location discovery to allow creation of location databases and, in the case of Voice over Internet Protocol (VoIP), Enhanced 911 services.

Inventory management, allowing network administrators to track their network devices, and determine their characteristics (manufacturer, software and hardware versions, serial or asset number).

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

Web Interface

To configure LLDP-MED:
1. Click LLDP-MED Configuration
2. Modify Fast start repeat count parameter, default is 4
3. Modify Coordinates Location psrameters
4. Fill Civic Address Location parameters
5. Add new policy
6. Click Apply, will show following Policy Port Configuration
7. Select Policy ID for each port
8. Click Apply

Figure 3-8.3: The LLDP-MED Configuration

LLDPMED Configuration

Fast Start Repeat Count

Fast start repeat count	4

Coordinates Location

Latitude	0 degrees	North	Longitude	0 degrees	East	Altitude	0	Meters	Map Datum

Civic Address Location

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

Emergency Call Service

Emergency Call Service	

Policies

Add new policy

Policy Port Configuration

Apply	Reset

Policies

Delete	Policy ID	Application Type	Tag	VLAN ID	L2 Priority	DSCP
Delete	0	Voice	Tagged	1	0	0
Delete	1	Voice	Tagged	1	0	0

Add new policy

Parameter description:

Fast start repeat count

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

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

Because there is a risk of an LLDP frame being lost during transmission between neighbours, it is recommended to repeat the fast start transmission multiple times to increase the possibility of the neighbours receiving the LLDP frame. With Fast start repeat count it is possible to specify the number of times the fast start transmission would be repeated. The recommended value is 4 times, given that 4 LLDP frames with a 1 second interval will be transmitted, when an LLDP frame with new information is received.

It should be noted that LLDP-MED and the LLDP-MED Fast Start mechanism is only intended to run on links between LLDP-MED Network Connectivity Devices and Endpoint Devices, and as such does not apply to links between LAN infrastructure elements, including Network Connectivity Devices, or other types of links.

Coordinates Location

● **Latitude :**

Latitude SHOULD be normalized to within 0-90 degrees with a maximum of 4 digits.

It is possible to specify the direction to either North of the equator or South of the equator.

● **Longitude :**

Longitude SHOULD be normalized to within 0-180 degrees with a maximum of 4 digits.

It is possible to specify the direction to either East of the prime meridian or West of the prime meridian.

● **Altitude :**

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

It is possible to select between two altitude types (floors or meters).

Meters: Representing meters of Altitude defined by the vertical datum specified.

Floors: Representing altitude in a form more relevant in buildings which have different floor-to-floor dimensions. An altitude = 0.0 is meaningful even outside a building, and represents ground level at the given latitude and longitude. Inside a building, 0.0 represents the floor level associated with ground level at the main entrance.

● **Map Datum :**

The Map Datum is used for the coordinates given in these options:

WGS84: (Geographical 3D) - World Geodesic System 1984, CRS Code 4327, Prime Meridian Name: Greenwich.

NAD83/NAVD88: North American Datum 1983, CRS Code 4269, Prime Meridian Name: Greenwich; The associated vertical datum is the North American Vertical Datum of 1988 (NAVD88). This datum pair is to be used when referencing locations on land, not near tidal water (which would use Datum = NAD83/MLLW).

NAD83/MLLW: North American Datum 1983, CRS Code 4269, Prime Meridian Name: Greenwich; The associated vertical datum is Mean Lower Low Water (MLLW). This datum pair is to be used when referencing locations on water/sea/ocean.

Civic Address Location

IETF Geopriv Civic Address based Location Configuration Information (Civic Address LCI).

- **Country code :**

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

- **State :**

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

- **County :**

  County, parish, gun (Japan), district.

- **City :**

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

- **City district :**

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

- **Block (Neighbourhood) :**

  Neighbourhood, block.

- **Street :**

  Street - Example: Poppelvej.

- **Leading street direction :**

  Leading street direction - Example: N.

- **Trailing street suffix :**

  Trailing street suffix - Example: SW.

- **Street suffix :**

  Street suffix - Example: Ave, Platz.

- **House no. :**

  House number - Example: 21.

- **House no. suffix :**

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

- **Landmark :**

  Landmark or vanity address - Example: Columbia University.

- **Additional location info :**

  Additional location info - Example: South Wing.

- **Name :**

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

- **Zip code :**

Postal/zip code - Example: 2791.

- **Building :**

  Building (structure) - Example: Low Library.

- **Apartment :**

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

- **Floor :**

  Floor - Example: 4.

- **Room no. :**

  Room number - Example: 450F.

- **Place type :**

  Place type - Example: Office.

- **Postal community name :**

  Postal community name - Example: Leonia.

- **P.O. Box :**

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

- **Additional code :**

  Additional code - Example: 1320300003.

- **Emergency Call Service:**

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

- **Emergency Call Service :**

  Emergency Call Service ELIN identifier data format is defined to carry the ELIN identifier as used during emergency call setup to a traditional CAMA or ISDN trunk-based PSAP. This format consists of a numerical digit string, corresponding to the ELIN to be used for emergency calling.

Policies

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

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

The network policy attributes advertised are:

1. Layer 2 VLAN ID (IEEE 802.1Q-2003)

2. Layer 2 priority value (IEEE 802.1D-2004)

3. Layer 3 Diffserv code point (DSCP) value (IETF RFC 2474)

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

1. Voice

2. Guest Voice

3. Softphone Voice

4. Video Conferencing

5. Streaming Video

6. Control / Signalling (conditionally support a separate network policy for the media types above)

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

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

- **Delete :**

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

- **Policy ID :**

  ID for the policy. This is auto generated and shall be used when selecting the polices that shall be mapped to the specific ports.

- **Application Type :**

  Intended use of the application types:

  1. Voice - for use by dedicated IP Telephony handsets and other similar appliances supporting interactive voice services. These devices are typically deployed on a separate VLAN for ease of deployment and enhanced security by isolation from data applications.

  2. Voice Signalling (conditional) - for use in network topologies that require a different policy for the voice signalling than for the voice media. This application type should not be advertised if all the same network policies apply as those advertised in the Voice application policy.

  3. Guest Voice - support a separate 'limited feature-set' voice service for guest users and visitors with their own IP Telephony handsets and other similar appliances supporting interactive voice services.

  4. Guest Voice Signalling (conditional) - for use in network topologies that require a different policy for the guest voice signalling than for the guest voice media. This application type should not be advertised if all the same network policies apply as those advertised in the Guest Voice application policy.

  5. Softphone Voice - for use by softphone applications on typical data centric devices, such as PCs or laptops. This class of endpoints frequently does not support multiple VLANs, if at all, and are typically configured to use an 'untagged' VLAN or a single 'tagged' data specific VLAN. When a network policy is defined for use with an 'untagged' VLAN (see Tagged flag below), then the L2 priority field is ignored and only the DSCP value has relevance.

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

  7. Streaming Video - for use by broadcast or multicast based video content distribution and other similar applications supporting streaming video services that require specific network policy treatment. Video applications relying on TCP with buffering would not be an intended use of this application type.

  8. Video Signalling (conditional) - for use in network topologies that require a separate policy for the video signalling than for the video media. This application type should not be advertised if all the same network policies apply as those advertised in the Video Conferencing application policy.

- **Tag :**

  Tag indicating whether the specified application type is using a 'tagged' or an 'untagged' VLAN.

  Untagged indicates that the device is using an untagged frame format and as such does not include a tag header as defined by IEEE 802.1Q-2003. In this case, both the VLAN ID and the Layer 2 priority fields are ignored and only the DSCP value has relevance.

Tagged indicates that the device is using the IEEE 802.1Q tagged frame format, and that both the VLAN ID and the Layer 2 priority values are being used, as well as the DSCP value. The tagged format includes an additional field, known as the tag header. The tagged frame format also includes priority tagged frames as defined by IEEE 802.1Q-2003.

- **VLAN ID :**

  VLAN identifier (VID) for the port as defined in IEEE 802.1Q-2003.

- **L2 Priority :**

  L2 Priority is the Layer 2 priority to be used for the specified application type. L2 Priority may specify one of eight priority levels (0 through 7), as defined by IEEE 802.1D-2004. A value of 0 represents use of the default priority as defined in IEEE 802.1D-2004.

- **DSCP :**

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

- **Adding a new policy :**

  Click to add a new policy. Specify the Application type, Tag, VLAN ID, L2 Priority and DSCP for the new policy. Click "Apply".

- **Port Policies Configuration :**

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

- **Port :**

  The port number to which the configuration applies.

- **Policy Id :**

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

- **Buttons:**

  Apply – Click to apply changes.

  Reset- Click to undo any changes made locally and revert to previously saved values.
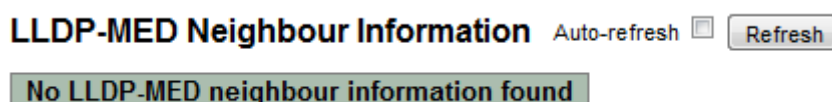
3-8.4 LLDP-MED Neighbours

This page provides a status overview of all LLDP-MED neighbours. The displayed table contains a row for each port on which an LLDP neighbour is detected. This function applies to VoIP devices which support LLDP-MED. The columns hold the following information:

Web Interface

To show LLDP-MED neighbours:

1.Click LLDP-MED Neighbours

2. Click Refresh for manual update web screen

3.Click Auto-refresh for auto-update web screen

Figure 3-9.4: The LLDP-MED Neighbours information

LLDP-MED Neighbour Information Auto-refresh ☐ [Refresh]

No LLDP-MED neighbour information found

ⓘ **NOTE:** If none of the devices in your network support LLDP-MED then the table will show "No LLDP-MED neighbour information found".

Parameter description:

● **Port :**

The port on which the LLDP frame was received.

● **Device Type :**

LLDP-MED Devices are comprised of two primary Device Types: Network Connectivity Devices and Endpoint Devices.

LLDP-MED Network Connectivity Device Definition

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

1. LAN Switch/Router

2. IEEE 802.1 Bridge

3. IEEE 802.3 Repeater (included for historical reasons)

4. IEEE 802.11 Wireless Access Point

5. Any device that supports the IEEE 802.1AB and MED extensions defined by TIA-1057 and can relay IEEE 802 frames via any method.

■ **LLDP-MED Endpoint Device Definition :**

LLDP-MED Endpoint Devices, as defined in TIA-1057, are located at the IEEE 802 LAN network edge, and participate in IP communication service using the LLDP-MED framework.

Within the LLDP-MED Endpoint Device category, the LLDP-MED scheme is broken into further Endpoint Device Classes, as defined in the following.

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

compliance as a Communication Device (Class III) will also support all aspects of TIA-1057 applicable to both Media Endpoints (Class II) and Generic Endpoints (Class I).

■ **LLDP-MED Generic Endpoint (Class I) :**

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

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

■ **LLDP-MED Media Endpoint (Class II) :**

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

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

■ **LLDP-MED Communication Endpoint (Class III) :**

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

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

● **LLDP-MED Capabilities :**

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

1. LLDP-MED capabilities

2. Network Policy

3. Location Identification

4. Extended Power via MDI - PSE

5. Extended Power via MDI - PD

6. Inventory

7. Reserved

● **Application Type :**

Application Type indicating the primary function of the application(s) defined for this network policy, advertised by an Endpoint or Network Connectivity Device. The possible application types are shown below.

1. Voice - for use by dedicated IP Telephony handsets and other similar appliances supporting interactive voice services. These devices are typically deployed on a separate VLAN for ease of deployment and enhanced security by isolation from data applications.

2. Voice Signalling - for use in network topologies that require a different policy for the voice signalling than for the voice media.

3. Guest Voice - to support a separate limited feature-set voice service for guest users and visitors with their own IP Telephony handsets and other similar appliances supporting interactive voice services.

4. Guest Voice Signalling - for use in network topologies that require a different policy for the guest voice signalling than for the guest voice media.

5. Softphone Voice - for use by softphone applications on typical data centric devices, such as PCs or laptops.

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

7. Streaming Video - for use by broadcast or multicast based video content distribution and other similar applications supporting streaming video services that require specific network policy treatment. Video applications relying on TCP with buffering would not be an intended use of this application type.

8. Video Signalling - for use in network topologies that require a separate policy for the video signalling than for the video media.

- **Policy :**

    Policy indicates that an Endpoint Device wants to explicitly advertise that the policy is required by the device. Can be either Defined or Unknown

    Unknown: The network policy for the specified application type is currently unknown.

    Defined: The network policy is defined.

- **TAG :**

    TAG is indicative of whether the specified application type is using a tagged or an untagged VLAN. Can be Tagged or Untagged.

    Untagged: The device is using an untagged frame format and as such does not include a tag header as defined by IEEE 802.1Q-2003.

    Tagged: The device is using the IEEE 802.1Q tagged frame format.

- **VLAN ID :**

    VLAN ID is the VLAN identifier (VID) for the port as defined in IEEE 802.1Q-2003. A value of 1 through 4094 is used to define a valid VLAN ID. A value of 0 (Priority Tagged) is used if the device is using priority tagged frames as defined by IEEE 802.1Q-2003, meaning that only the IEEE 802.1D priority level is significant and the default PVID of the ingress port is used instead.

- **Priority :**

    Priority is the Layer 2 priority to be used for the specified application type.One of the eight priority levels (0 through 7).

- **DSCP :**

    DSCP is the DSCP value to be used to provide Diffserv node behavior for the specified application type as defined in IETF RFC 2474. Contain one of 64 code point values (0 through 63).

3-8.5 Port Statistics

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

Web Interface

To show LLDP Statistics:
1. Click LLDP, then click Port Statistics to show LLDP counters
2. Click Refresh for manual update web screen
3. Click Auto-refresh for auto-update web screen
4. Click Clear to clear all counters

Figure 3-8.5: The LLDP Port Statistics information

Auto-refresh ☐ [Refresh] [Clear]

Global Counters	
Neighbour entries were last changed	2011-01-01 00:00:00 (9753 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
19	0	0	0	0	0	0	0
20	0	0	0	0	0	0	0
21	0	0	0	0	0	0	0
22	0	0	0	0	0	0	0
23	0	0	0	0	0	0	0
24	0	0	0	0	0	0	0
25	0	0	0	0	0	0	0
26	0	0	0	0	0	0	0
27	0	0	0	0	0	0	0
28	0	0	0	0	0	0	0

Parameter description:

Global Counters

● **Neighbour entries were last changed at :**

It also shows the time when the last entry was last deleted or added. It also shows the time elapsed since the last change was detected.

● **Total Neighbours Entries Added :**

Shows the number of new entries added since switch reboot.

● **Total Neighbours Entries Deleted :**

Shows the number of new entries deleted since switch reboot.

● **Total Neighbours Entries Dropped :**

Shows the number of LLDP frames dropped due to the entry table being full.

● **Total Neighbours Entries Aged Out :**

Shows the number of entries deleted due to Time-To-Live expiring.

Local Counters

The displayed table contains a row for each port. The columns hold the following information:

● **Local Port :**

The port on which LLDP frames are received or transmitted.

● **Tx Frames :**

The number of LLDP frames transmitted on the port.

● **Rx Frames :**

The number of LLDP frames received on the port.

● **Rx Errors :**

The number of received LLDP frames containing some kind of error.

● **Frames Discarded :**

If an LLDP frame is received on a port, and the switch's internal table has run full, the LLDP frame is counted and discarded. This situation is known as "Too Many Neighbours" in the LLDP standard. LLDP frames require a new entry in the table when the Chassis ID or Remote Port ID is not already contained within the table. Entries are removed from the table when a given port's link is down, an LLDP shutdown frame is received, or when the entry ages out.

● **TLVs Discarded :**

Each LLDP frame can contain multiple pieces of information, known as TLVs (TLV is short for "Type Length Value"). If a TLV is malformed, it is counted and discarded.

● **TLVs Unrecognized :**

The number of well-formed TLVs, but with an unknown type value.

● **Org. Discarded :**

The number of organizationally received TLVs.

● **Age-Outs :**

Each LLDP frame contains information about how long 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.

● **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 LLDP Port Statistics information by manual. Or press clear to clean up the entries.

3- 9 Filtering Data Base

Filtering Data Base Configuration gathers many functions, including MAC Table Information, Static MAC Learning, which cannot be categorized to some function type.

MAC table

Switching of frames is based upon the DMAC address contained in the frame. The switch builds up a table that maps MAC addresses to switch ports for knowing which ports the frames should go to (based upon the DMAC address in the frame). This table contains both static and dynamic entries. The static entries are configured by the network administrator if the administrator wants to do a fixed mapping between the DMAC address and switch ports. The frames also contain a MAC address (SMAC address), which shows the MAC address of the equipment sending the frame. The SMAC address is used by the switch to automatically update the MAC table with these dynamic MAC addresses. Dynamic entries are removed from the MAC table if no frame with the corresponding SMAC address has been seen after a configurable age time

3- 9.1 Configuration

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

Web Interface

To configure MAC Address Table in the web interface:
Aging Configuration
1. Click configuration .
2. Specify the Disable Automatic Aging and Aging Time.
3. Click Apply.
MAC Table Learning
1. Click configuration .
2. Specify the Port Members(Auto,Disable,Secure).
3. Click Apply.
Static MAC Table Configuration
1. Click configuration and Add new Static entry .
2. Specify the VLAN IP and Mac address ,Port Members.
3. Click Apply.

Figure 3- 9.1: The MAC Address Table Configuration

Static MAC Table Configuration

			Port Members																												
Delete	VLAN ID	MAC Address	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
Delete	1	00-00-00-00-00-00	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

Parameter description:

- **Aging Configuration :**

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

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

  The allowed range is 10 to 1000000 seconds.

  Disable the automatic aging of dynamic entries by checking ☑   Disable automatic aging.

MAC Table Learning

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

- **Auto :**

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

- **Disable :**

  No learning is done.

- **Secure :**

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

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

Static MAC Table Configuration

The static entries in the MAC table are shown in this table. The static MAC table can contain 64 entries. The maximum of 64 entries is for the whole stack, and not per switch.

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

- **Delete :**

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

- **VLAN ID :**

  The VLAN ID of the entry.

- **MAC Address :**

  The MAC address of the entry.

- **Port Members :**

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

- **Adding a New Static Entry :**

  Click to add a new entry to the static MAC table. Specify the VLAN ID, MAC address, and port members for 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- 9.2 Dynamic MAC Table

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

Web Interface

To Display MAC Address Table in the web interface:
1. Click Dynamic MAC Table .
2. Specify the VLAN and MAC Address.
3. Display MAC Address Table.

Figure 3- 9.2: The Dynamic MAC Address Table information

Parameter description:

MAC Table Columns

Switch (stack only) The stack unit where the entry is learned.

- **Type :**

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

- **VLAN :**

    The VLAN ID of the entry.

- **MAC address :**

    The MAC address of the entry.

- **Port Members :**

    The ports that are members of the entry.

- **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 MAC address entries by manual.or press clear to clean up the MAC table. Others press << or >> to upper or down page of the table.

3-10 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 using the Management VLAN window. Only one management VLAN can be active at a time.

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

3-10.1 VLAN Membership

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

Web Interface

To configure VLAN membership configuration in the web interface:
1. Click VLAN membership Configuration.
2. Specify Management VLAN ID. 0~ 4094
3. Click Apply.

Figure 3-10.1: The VLAN Membership Configuration

Parameter description:

- **Delete :**

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

- **VLAN ID :**

    Indicates the ID of this particular VLAN.

- **VLAN Name :**

    Indicates the name of the VLAN. Maximum length of the VLAN Name String is 32. All ASCII printable characters (except double quotation,less-than sign,greater-than sign) can be used to form the VLAN Name.

- **Port Members :**

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

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

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

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

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

- **Adding a New VLAN :**

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

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

  A VLAN without any port members on any stack unit will be deleted when you click "Apply".

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

- **Buttons:**

  Apply – Click to apply 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 VLAN entries by manual. Or press clear to clean up the VLAN table. Others press |<< or >> to upper or down page of the table.

3-10.2 Ports

The function in VLAN Tag Rule Setting, user can input VID number to each port. The range of VID number is from 1 to 4094. User also can choose ingress filtering rules to each port. There are two ingress filtering rules which can be applied to the switch. The Ingress Filtering Rule 1 is "forward only packets with VID matching this port's configured VID". The Ingress Filtering Rule 2 is "drop untagged frame". You can also select the Role of each port as Access, Trunk, or Hybrid.

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 Apply.

Figure 3-10.2: The VLAN Port Configuration

Ethertype for Custom S-ports 0x 88A8

VLAN Port Configuration

Port	Port Type	Ingress Filtering	Frame Type	Egress Rule	PVID
*	<>	☐	<>	<>	
1	Unaware	☐	All	Hybrid	1
2	Unaware	☐	All	Hybrid	1
3	Unaware	☐	All	Hybrid	1
4	Unaware	☐	All	Hybrid	1
5	Unaware	☐	All	Hybrid	1
6	Unaware	☐	All	Hybrid	1
7	Unaware	☐	All	Hybrid	1
8	Unaware	☐	All	Hybrid	1
9	Unaware	☐	All	Hybrid	1
10	Unaware	☐	All	Hybrid	1
11	Unaware	☐	All	Hybrid	1
12	Unaware	☐	All	Hybrid	1
13	Unaware	☐	All	Hybrid	1
14	Unaware	☐	All	Hybrid	1
15	Unaware	☐	All	Hybrid	1
16	Unaware	☐	All	Hybrid	1
17	Unaware	☐	All	Hybrid	1
18	Unaware	☐	All	Hybrid	1
19	Unaware	☐	All	Hybrid	1
20	Unaware	☐	All	Hybrid	1
21	Unaware	☐	All	Hybrid	1
22	Unaware	☐	All	Hybrid	1
23	Unaware	☐	All	Hybrid	1
24	Unaware	☐	All	Hybrid	1
25	Unaware	☐	All	Hybrid	1
26	Unaware	☐	All	Hybrid	1
27	Unaware	☐	All	Hybrid	1
28	Unaware	☐	All	Hybrid	1

Apply   Reset

Parameter description:

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

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

- **Port :**

  This is the logical port number of this row.

- **Port Type :**

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

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

Port Type	Ingress Action	Egress Action
Unaware	When the port received untagged frames, the frame is tagged with the PVID and forwarded. When the port received tagged frames : No matter what the TPID value is, one outer tag (PVID) will be added and the frame will be forwarded.	The TPID of the frame transmitted through the Unaware port will be set to 0x8100. The final status of the frame after egressing are also effected by Egress Rule.
	packet Tag VID=5 TPID=any / packet → Unaware → Tag VID=(PVID) TPID=8100 → Tag VID=(PVID) TPID=8100 / packet → Tag VID=(PVID) TPID=8100 / Tag VID=5 TPID=any / packet	
C-port	When the port received untagged frames, the frame is tagged with the PVID and forwarded. When the port received tagged frames : 1. if the TPID of the tagged frame is 0x8100, it is forwarded. 2. if a tagged frame contains the TPID of any value except 0x8100, 0x88a8 and Ethertype, it is forwarded and also tagged with PVID. 3. if the TPID of the tagged frame is 0x88A8 or Ethertype, it will be discarded.	The TPID of the frame transmitted through the C-port will be set to 0x8100.

	packet	Tag VID=(PVID) TPID=8100 packet
C-port		
Tag VID=8 TPID=8100 packet	→	Tag VID=8 TPID=8100 packet
Tag VID=8 TPID =X , X is not 8100 or 88a8 or Ethertype packet	→	Tag VID=(PVID) TPID=8100 Tag VID=8 TPID=X packet
Tag VID=8 TPID=88a8 or Ethertype packet		TPID=88a8 or Ethertype , packet will be discarded

S-port	When the port received untagged frames, the frame is tagged with the PVID and forwarded. When the port received tagged frames: 1. If the TPID of the tagged frame is 0x8100, it is discarded. Otherwise, the frame is forwarded. 2. This mode will not add a tag.	The TPID of the frame transmitted through the S-port will be set to 0x88A8.

	packet	Tag VID=(PVID) TPID=88a8 packet
S-port		
Tag VID=10 TPID=8100 packet	→	TPID=8100 packet will be discarded
Tag VID=10 TPID=Y, Y is not 8100 packet		Tag VID=10 TPID=88a8 packet

S-custom-port	When the port received untagged frames, the frame is tagged with the PVID and forwarded. When the port received tagged frames : 1. If the TPID of the tagged frame is either 0x88a8 or **Ethertype for Custom S-ports**, the frame is forwarded. Otherwise, the frame is discarded. 2. This mode will not add a tag.	The TPID of the frame transmitted through the 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.**

packet

Tag
VID=(PVID)
TPID=Ethertype for
Customer S-ports

packet

Tag
VID=5
TPID=Z, Z is not either
88a8 or Ethertype for
Custom S-ports

packet

S-
custom-
port

TPID=Z, Z is not either
88a8 or Ethertype for
Custom S-ports packet will
be discarded

Tag
VID=5
TPID=either 88a8 or
Ethertype for Custom S-
ports

packet

Tag
VID=5
TPID=Ethertype for
Custom S-ports

packet
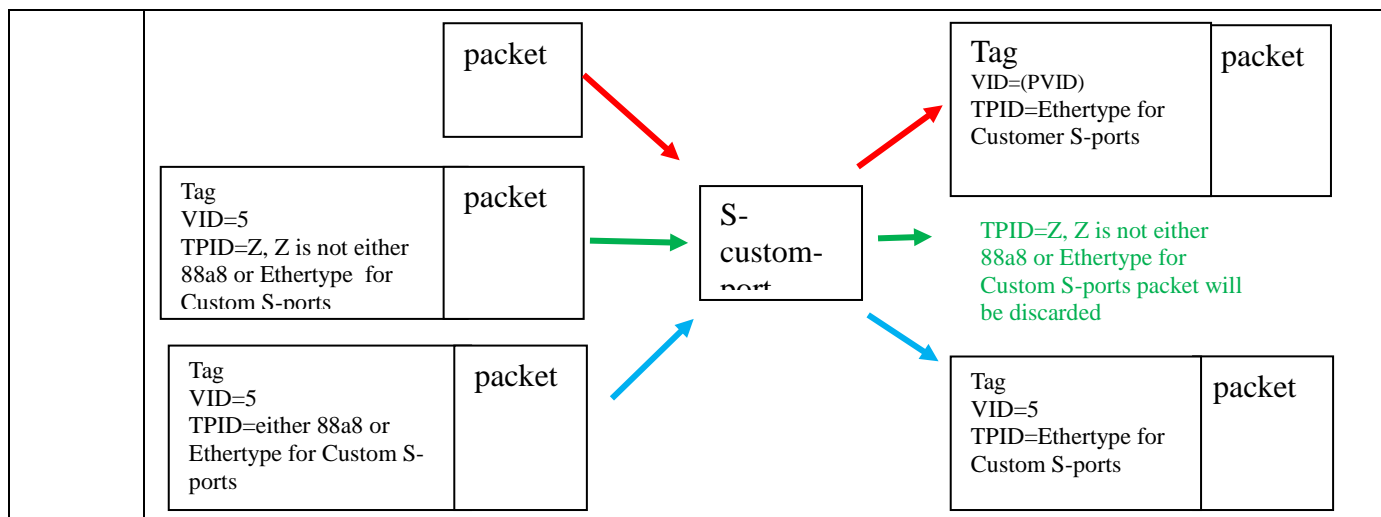
- **Ingress Filtering :**

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

- **Frame Type :**

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

- **Egress Rule :**

  Configures the Port Egress Rule. The allowed values are Hybric, Trunk or Access. This parameter affects VLAN egress processing.

  If Trunk is selected, a VLAN tag with the classified VLAN ID is inserted in frames transmitted on the port. This mode is normally used for ports connected to VLAN aware switches.

  If Hybrid (the default value) is selected, if the classified VLAN ID of a frame transmitted on the port is different from the Port VLAN ID, a VLAN tag with the classified VLAN ID is inserted in the frame.

  If Access is selected, untag all frames transmitted on the port.

- **Port VLAN ID :**

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

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

- **Buttons:**

  Apply – Click to apply changes.

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

3-10.3 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 n the web interface:
1. Click VLAN membership.
2. Specify the static NAS MVRP MVP Voice VLAN MSTP GVRP Combined.
3. Display membership information.

Figure 3-10.3: The VLAN Membership Status for Static user

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:

CLI/Web/SNMP : These are referred to as static.

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

MVR : MVR is used to eliminate the need to duplicate multicast traffic for subscribers in each VLAN. Multicast traffic for all channels is sent only on a single (multicast) VLAN.

MSTP : The 802.1s Multiple Spanning Tree protocol (MSTP) uses VLANs to create multiple spanning trees in a network, which significantly improves network resource utilization while maintaining a loop-free environment.

● **Port Members**

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

If a port is included in a VLAN, an image port will be displayed.

If a port is included in a Forbidden port list, an image forbid will be displayed.

If a port is included in a Forbidden port list and dynamic VLAN user register VLAN on same Forbidden port, then conflict port will be displayed as .

● **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.

3-10.4 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 n 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 3-10.4: The VLAN Port Status for Static user

Port	PVID	Port Type	Ingress Filtering	Frame Type		UVID	Conflicts
					Static		
1	1	UnAware	Disabled	All	NAS	1	No
2	1	UnAware	Disabled	All	GVRP	1	No
3	1	UnAware	Disabled	All	MVR	1	No
4	1	UnAware	Disabled	All	MSTP	1	No
5	1	UnAware	Disabled	All	ERPS	1	No
6	1	UnAware	Disabled	All	MEP	1	No
7	1	UnAware	Disabled	All	EVC	1	No
8	1	UnAware	Disabled	All	VCL Combined	1	No
9	1	UnAware	Disabled	All	Untag_this	1	No
10	1	UnAware	Disabled	All	Untag_this	1	No
11	1	UnAware	Disabled	All	Untag_this	1	No
12	1	UnAware	Disabled	All	Untag_this	1	No
13	1	UnAware	Disabled	All	Untag_this	1	No
14	1	UnAware	Disabled	All	Untag_this	1	No
15	1	UnAware	Disabled	All	Untag_this	1	No
16	1	UnAware	Disabled	All	Untag_this	1	No
17	1	UnAware	Disabled	All	Untag_this	1	No
18	1	UnAware	Disabled	All	Untag_this	1	No
19	1	UnAware	Disabled	All	Untag_this	1	No
20	1	UnAware	Disabled	All	Untag_this	1	No
21	1	UnAware	Disabled	All	Untag_this	1	No
22	1	UnAware	Disabled	All	Untag_this	1	No
23	1	UnAware	Disabled	All	Untag_this	1	No
24	1	UnAware	Disabled	All	Untag_this	1	No
25	1	UnAware	Disabled	All	Untag_this	1	No
26	1	UnAware	Disabled	All	Untag_this	1	No
27	1	UnAware	Disabled	All	Untag_this	1	No
28	1	UnAware	Disabled	All	Untag_this	1	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 4094 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.

3-10.5 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.

3-10.5.1 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 3-10.5.1: The Private VLAN Membership Configuration

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 "Add New Private VLAN" to add a new private VLAN ID. An empty row is added to the table, and the private VLAN can be configured as needed. The allowed range for a private VLAN ID is the same as the switch port number range. Any values outside this range are not accepted, and a warning message appears. Click "OK" to discard the incorrect entry, or click "Cancel" to return to the editing and make a correction.

The Private VLAN is enabled when you click "Apply".

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

● **Buttons:**

Apply – Click to apply changes.

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

3-10.5.2 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 3-10.5.2: The Port Isolation Configuration

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 apply changes.

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

3-10.6 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.

3-10.6.1 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 add new entry.
2. Specify the MAC address and VLAN ID.
3. Click Apply.

Figure 3-10.6.1: 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 in the stack.

● **MAC Address :**

Indicates the MAC address.

● **VLAN ID :**

Indicates the VLAN ID.

- **Port Members :**

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

- **Adding a New MAC-based VLAN**

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

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

  The "Delete" button can be used to undo the addition of new MAC-based VLANs.

- **Buttons:**

  Apply – Click to apply changes.

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

3-10.6.2 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 Staic NAS Combined.
3. Display MAC-based information.

Figure 3-10.6.2: The MAC-based VLAN Membership Status for User Static

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.

3-10.7 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.

3-10.7.1 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 stack switch unit switch.

Web Interface

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

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

Figure 3-10.7.1: The Protocol to Group Mapping 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 apply.

- **Frame Type :**

    Frame Type can have one of the following values:

    1. **Ethernet**
    2. **LLC**
    3. **SNAP**

- **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).

- **Adding a New Group to VLAN mapping entry :**

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

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

- **Buttons:**

  Apply – Click to apply 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.

3-10.7.2 Group to VLAN

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

Web Interface

To Display Group Name to VLAN mapping table configured in the web interface:
1. Click Group Name VLAN configuration add new entry.
2. Specify the Group Name and VLAN ID.
3. Click Apply.

Figure 3-12.7.2: The Group Name of VLAN Mapping Table

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 apply

- **Group Name :**

    A valid Group Name is a string of almost 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 1-4094.

- **Port Members :**

    A row of check boxes for each port is displayed for each Group Name to VLAN ID mapping. To include a port in a mapping, check the box. To remove or exclude the port from the mapping, make sure the box is unchecked. By default, no ports are members, and all boxes are unchecked.

- **Adding a New Group to VLAN mapping entry :**

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

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

- **Buttons:**

    Apply – Click to apply 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.

3-11 VLAN Translation

VLAN Translation allows traffic from one VLAN to be transported across a different VLAN. Packet VLAN IDs from the original VLAN are changed at the ingress port of the translating VLAN. When the packets reach the egress point on the translating VLAN, the VLAN ID is translated back to the original ID.

This feature is useful for service providers who must carry traffic from different customers across their network while preserving the VLAN ID and priority information.

3-11.1 Port to Group Mapping

This page allows you to map set of Port members to a Group ID for all switch ports.

Web Interface

To Display Port to Group mapping table configured in the web interface:
1.Click Configuration, VLAN Translation and Port to Group mapping
2.To click the icon to change import group ID to new group ID.
3.Click Apply.

Figure3-11.1: The port to group mapping table

Parameter description:

These parameters are displayed on the SNMP System Configuration page:

- **Group ID :**

  A valid Group ID is an integer value from first to last port. A set of VLAN Translations are mapped to a group Id. This way a port is mapped to a list of VLAN Translations easily by mapping it to a group. Number of groups in this switch is equal to the number of ports present in this switch. A port can be mapped to any of the groups. Multiple ports can also be mapped to a group with same group Id.
  Note: By default, each port is mapped to a group with a group Id equal to the port number. For example, port 1 is mapped to the group with ID=1.

- **Port Member :**

  A row of radio buttons, one radio button for each port is displayed for each Group ID. To include a port in a Group, click the radio button. A port must belong to atleast one group.

- **Adding a New Port to Group mapping entry :**

  Click "Add New Entry" to add a new entry in Port to Group Mapping Table. An empty row is added to the table with the Group ID and array of radio buttons, one radio button for each port(click corresponding radio button to make port to be member of a particular Group). Legal values for a VLAN ID are **1** through **4095**.

  The Delete button can be used to undo the addition of new entry.

- **Buttons :**

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

Refresh: Click to refresh the page immediately.

Apply: Click to apply changes.

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

3-11.2 VID Translation Mapping

This session allows you to map VLAN ID to other VLAN ID for a particular Group ID Globally.

Web Interface

To Display Port to Group mapping table configured in the web interface:
1.Click Configuration, VLAN Translation and VID Translation
2.To click "Add New Entry" and specify Group ID, VLAN ID and Translated to VID.
3.Click Apply.

Figure3-11.2: The VLAN translation table

VLAN Translation Table   Auto-refresh ☐   [Refresh]

Delete	Group ID	VLAN ID	Translated to VID
	No VLAN Translation entry found		

[Add New Entry]

[Apply] [Reset]

Parameter description:

These parameters are displayed on the SNMP System Configuration page:

● **Delete :**

  To delete a VLAN Translation Group database entry, check this box. The entry will be deleted on the switch during the next Apply.

● **Group ID :**

  A valid Group ID is an integer value from 1 to 28. A set of VLAN Translations are mapped to a group Id. This way a port is mapped to a list of VLAN Translations easily by mapping it to a group. Number of groups in a switch is equal to the number of ports present in this switch. A port can be mapped to any of the groups. Multiple ports can also be mapped to a group with same group Id.
  Note: By default, each port is mapped to a group with a group Id equal to the port number. For example, port 1 is mapped to the group with ID=1.

● **VLAN ID :**

  Indicates the ID to which Group ID will be mapped. A valid VLAN ID ranges from 1-4094.

● **Translated to VLAN ID :**

  Indicates the VID to which VLAN ID of ingress frames will be changed, if VID in incoming frames if same as configured in VLAN ID field preceded by this field on member ports of a particular group to which this entry belongs.

● **Adding a New Port to Group mapping entry :**

  Click "Add New Entry" to add a new entry in VLAN Translation table. An empty row is added to the table, the Group ID, VLAN ID and Translated to VID fields can be configured as needed. Legal values for a VLAN ID are **1** through **4094**.

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

● **Buttons :**

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

  Refresh: Click to refresh the page immediately.

  Apply: Click to apply changes.

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

3-12 GARP

The Generic Attribute Registration Protocol (GARP) provides a generic framework whereby devices in a bridged LAN, e.g. end stations and switches, can register and de-register attribute values, such as VLAN Identifiers, with each other. In doing so, the attributes are propagated to devices in the bridged LAN, and these devices form a ¡°reachability¡± tree that is a subset of an active topology. GARP defines the architecture, rules of operation, state machines and variables for the registration and de-registration of attribute values.

A GARP participation in a switch or an end station consists of a GARP application component, and a GARP Information Declaration (GID) component associated with each port or the switch. The propagation of information between GARP participants for the same application in a bridge is carried out by the GARP Information Propagation (GIP) component. Protocol exchanges take place between GARP participants by means of LLC Type 1 services, using the group MAC address and PDU format defined for the GARP application concerned.

3-12.1 Configuration

This page allows you to configure the basic GARP Configuration settings for all switch ports. The settings relate to the currently selected stack unit, as reflected by the page header.

Web Interface

To configure GARP Port Configuration in the web interface:
1. Click GARP configure.
2. Specify GARP Configuration Parameters.
3. Click Apply.

Figure 3-12.1: The GARP Port Configuration

GARP Port Configuration

Auto-refresh ☐ Refresh

Port	Timer Values			Application	Attribute Type	GARP Applicant
	Join Timer	Leave Timer	Leave All Timer			
1	200	600	10000	GVRP ▼	VLAN ▼	normal-participant ▼
2	200	600	10000	GVRP ▼	VLAN ▼	normal-participant ▼
3	200	600	10000	GVRP ▼	VLAN ▼	normal-participant ▼
4	200	600	10000	GVRP ▼	VLAN ▼	normal-participant ▼
5	200	600	10000	GVRP ▼	VLAN ▼	normal-participant ▼
6	200	600	10000	GVRP ▼	VLAN ▼	normal-participant ▼
7	200	600	10000	GVRP ▼	VLAN ▼	normal-participant ▼
8	200	600	10000	GVRP ▼	VLAN ▼	normal-participant ▼
9	200	600	10000	GVRP ▼	VLAN ▼	normal-participant ▼
10	200	600	10000	GVRP ▼	VLAN ▼	normal-participant ▼
11	200	600	10000	GVRP ▼	VLAN ▼	normal-participant ▼
12	200	600	10000	GVRP ▼	VLAN ▼	normal-participant ▼
13	200	600	10000	GVRP ▼	VLAN ▼	normal-participant ▼
14	200	600	10000	GVRP ▼	VLAN ▼	normal-participant ▼
15	200	600	10000	GVRP ▼	VLAN ▼	normal-participant ▼
16	200	600	10000	GVRP ▼	VLAN ▼	normal-participant ▼
17	200	600	10000	GVRP ▼	VLAN ▼	normal-participant ▼
18	200	600	10000	GVRP ▼	VLAN ▼	normal-participant ▼
19	200	600	10000	GVRP ▼	VLAN ▼	normal-participant ▼
20	200	600	10000	GVRP ▼	VLAN ▼	normal-participant ▼
21	200	600	10000	GVRP ▼	VLAN ▼	normal-participant ▼
22	200	600	10000	GVRP ▼	VLAN ▼	normal-participant ▼
23	200	600	10000	GVRP ▼	VLAN ▼	normal-participant ▼
24	200	600	10000	GVRP ▼	VLAN ▼	normal-participant ▼
25	200	600	10000	GVRP ▼	VLAN ▼	normal-participant ▼
26	200	600	10000	GVRP ▼	VLAN ▼	normal-participant ▼
27	200	600	10000	GVRP ▼	VLAN ▼	normal-participant ▼
28	200	600	10000	GVRP ▼	VLAN ▼	normal-participant ▼

Apply Reset

Parameter description:

- **Port** :

  The Port column shows the list of ports for which you can configure GARP settings. There are 4 types configuration settings which can be configured on per port bases.

  - Timer Values
  - Application
  - Attribute Type
  - GARP Applicant

- **Timer Values** :

  To set the GARP join timer, leave timer and .leave all timers, units is Micro-second.

  Three different timers can be configured on this page:

  Join Timer :The default value for Join timer is 200ms.
  Leave Timer : The range of values for Leave Time is 600-1000ms. The default value for Leave Timer is 600ms.
  Leave All Timer : The default value for Leave All Timer is 10000ms

- **Application** :

  Currently only supported application is GVRP.

- **Attribute Type** :

  Currently only supported Attribute Type is VLAN.

- **GARP Applicant**

  This configuration is used to configure the Applicant state machine behavior for GARP on a particular port locally.

- **normal-participant:** In this mode the Applicant state machine will operate normally in GARP protocol exchanges.
- **non-participant:** In this mode the Applicant state machine will not participate in the protocol operation.

The default configuration is normal participant.

- **Buttons:**

  Save – Click to apply changes.

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

3-12.2 Statistics

The section describes to port statistics of GARP for all switch ports. The port statistics relate to the currently selected stack unit, as reflected by the page header.

Web Interface

To display GARP Port statistics in the web interface:
1. Click GARP statistics.
2. Scroll which port you want to display the GARP Counter information..
3. Click Refresh to modify the GARP statistics information.

Figure 3-12.2: The GARP Port Statistics

GARP Port Statistics

Port	Peer MAC	Failed Count
1	--	--
2	--	--
3	--	--
4	--	--
5	--	--
6	--	--
7	--	--
8	--	--
9	--	--
10	--	--
11	--	--
12	--	--
13	--	--
14	--	--
15	--	--
16	--	--
17	--	--
18	--	--
19	--	--
20	--	--
21	--	--
22	--	--
23	--	--
24	--	--
25	--	--
26	--	--
27	--	--
28	--	--

Parameter description:

- **Port :**

  The Port column shows the list of all ports for which per port GARP statistics are shown.

- **Peer MAC :**

  Peer MAC is MAC address of the neighbour Switch from with GARP frame is received.

- **Failed Count :**

GARP fail to register count.

- **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 GARP Port Statistics information by manual.

3-13 GVRP

GVRP is an application based on Generic Attribute Registration Protocol (GARP), mainly used to automatically and dynamically maintain the group membership information of the VLANs. The GVRP offers the function providing the VLAN registration service through a GARP application. It makes use of GARP Information Declaration (GID) to maintain the ports associated with their attribute database and GARP Information Propagation (GIP) to communicate among switches and end stations. With GID information and GIP, GVRP state machine maintain the contents of Dynamic VLAN Registration Entries for each VLAN and propagate these information to other GVRP-aware devices to setup and update their knowledge database, the set of VLANs associated with currently active members, and through which ports these members can be reached.

3-13.1 Configuration

This page allows you to configure the basic GVRP Configuration settings for all switch ports. The settings relate to the currently selected stack unit, as reflected by the page header.

Web Interface

To configure GVRP Port Configuration in the web interface:
1. Click GVRP configure.
2. Specify GVRP Configuration Parameters..
3. Click Apply.

Figure 3-13.1: The GVRP Global Configuration

Global Configuration

GVRP Mode Disable ▾

Port Configuration

Port	GVRP Mode	GVRP rrole
1	Disable ▾	Disable ▾
2	Disable ▾	Disable ▾
3	Disable ▾	Disable ▾
4	Disable ▾	Disable ▾
5	Disable ▾	Disable ▾
6	Disable ▾	Disable ▾
7	Disable ▾	Disable ▾
8	Disable ▾	Disable ▾
9	Disable ▾	Disable ▾
10	Disable ▾	Disable ▾
11	Disable ▾	Disable ▾
12	Disable ▾	Disable ▾
13	Disable ▾	Disable ▾
14	Disable ▾	Disable ▾
15	Disable ▾	Disable ▾
16	Disable ▾	Disable ▾
17	Disable ▾	Disable ▾
18	Disable ▾	Disable ▾
19	Disable ▾	Disable ▾
20	Disable ▾	Disable ▾
21	Disable ▾	Disable ▾
22	Disable ▾	Disable ▾
23	Disable ▾	Disable ▾
24	Disable ▾	Disable ▾
25	Disable ▾	Disable ▾
26	Disable ▾	Disable ▾
27	Disable ▾	Disable ▾
28	Disable ▾	Disable ▾

Apply   Reset

Parameter description:

- **GVRP Mode :**

  GVRP Mode is a global setting, to enable the GVRP globally select 'Enable' from menu and to disable GVRP globally select 'Disable'. In stacking, this configuration command sends message to all the slaves connected in stack.

  Default value of Global GVRP Mode is 'Disable'

- **Port :**

  The Port column shows the list of ports for which you can configure per port GVRP settings. There are two configuration settings which can be configured on per port bases.

  - GVRP Mode:
  - GVRP rrole:

1. GVRP Mode

This configuration is to enable/disable GVRP Mode on perticular port locally.

- **Disable:** Select to Disable GVRP mode on this port.
- **Enable:** Select to Enable GVRP mode on this port.

The default value of configuration is disable.

2. GVRP rrole

This configuration is used to configure restricted role on an interface.

- **Disable:** Select to Disable GVRP rrole on this port.
- **Enable:** Select to Enable GVRP rrole on this port.

The default configuration is disable.

- **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 GVRP Global configuration information by manual.

- **Buttons:**

  Apply – Click to apply changes.

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

3-13.2 Statistics

The section describes to shows the basic GVRP Port statistics for all switch ports. The statistics relate to the currently selected stack unit, as reflected by the page header.

Web Interface

To display GVRP Port statistics in the web interface:

1. Click GVRP statistics.
2. Scroll which port you want to display the GVRP Counter information.
3. Click Refresh to modify the GVRP statistics information.

Figure 3-13.2: The GVRP Port Statistics

GVRP Port Statistics

Port	Join Tx Count	Leave Tx Count
1	0	0
2	0	0
3	0	0
4	0	0
5	0	0
6	0	0
7	0	0
8	0	0
9	0	0
10	0	0
11	0	0
12	0	0
13	0	0
14	0	0
15	0	0
16	0	0
17	0	0
18	0	0
19	0	0
20	0	0
21	0	0
22	0	0
23	0	0
24	0	0
25	0	0
26	0	0
27	0	0
28	0	0

Parameter description:

- **Port :**

   The Port coulmn shows the list of ports for which you can see port counters and statistics.

- **Join Tx Count :**

   Explain Join tx Count here...

- **Leave Tx Count :**

Explain Leave Tx Count 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 GVRP Port Statistics information by manual.

3-14 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.

3-14.1 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 stack 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 3-14.1: The QoS Configuration

QoS Ingress Port Classification

Port	QoS class	DP level	PCP	DEI	Tag Class.	DSCP Based
*	<> ▼	<> ▼	<> ▼	<> ▼		☐
1	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	☐
2	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	☐
3	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	☐
4	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	☐
5	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	☐
6	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	☐
7	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	☐
8	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	☐
9	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	☐
10	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	☐
11	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	☐
12	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	☐
13	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	☐
14	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	☐
15	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	☐
16	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	☐
17	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	☐
18	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	☐
19	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	☐
20	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	☐
21	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	☐
22	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	☐
23	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	☐
24	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	☐
25	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	☐
26	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	☐
27	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	☐
28	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	☐

[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.

  > **NOTE:** If the QoS class has been dynamically changed, then the actual QoS class is shown in parentheses after the configured QoS class.

- **DP level :**

  Controls the default Drop Precedence 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 apply changes.

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

3-14.2 Port Policing

This section provides an overview of QoS Ingress Port Policers for all switch ports The Port Policing is useful in constraining traffic flows and marking frames above specific rates. Policing is primarily useful for data flows and voice or video flows because voice and video usually maintains a steady rate of traffic

Web Interface

To display the QoS Port Schedulers in the web interface:

1. Click Configuration, QoS, Port Policing

2. Evoke which port need to enable the QoS Ingress Port Policers and type the Rate limit condition.

3. Scroll to select the Rate limit Unit with kbps, Mbps, fps and kfps.

4. Click Apply to save the configuration.

Figure 3-14.2: The QoS Ingress Port Policers Configuration

QoS Ingress Port Policers

Port	Mode	Rate	Unit
*	☐		◇
1	☐	500	kbps
2	☐	500	kbps
3	☐	500	kbps
26	☐	500	kbps
27	☐	500	kbps
28	☐	500	kbps

Apply   Reset

Parameter description:

- **Port :**

  The port number for which the configuration below applies.

- **Mode :**

  Controls whether the policer is enabled on this switch port.

- **Rate :**

  Controls the rate for the policer. The default value is 500. This value is restricted to 100-1000000 when the "Unit" is "kbps" or "fps", and it is restricted to 1-10000 when the "Unit" is "Mbps" or "kfps".

- **Unit :**

  Controls the unit of measure for the policer rate as kbps, Mbps, fps or kfps . The default value is "kbps".

- **Buttons:**

  Apply – Click to apply changes.

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

3-14.3 Queue Policers

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

Web Interface

To display the QoS Port Schedulers in the web interface:

1. Click Configuration, QoS, Queue Policing

2. Evoke which queue need to enable the QoS Ingress Queue Policers.

3. Scroll to select the Rate limit Unit with kbps, Mbps, fps and kfps.

4. Click Apply to save the configuration.

Figure 3-16.3: The QoS Ingress Port Policers Configuration

QoS Ingress Queue Policers

Port	Queue 0 Enable	Queue 1 Enable	Queue 2 Enable	Queue 3 Enable	Queue 4 Enable	Queue 5 Enable	Queue 6 Enable	Queue 7 Enable
*	☐	☐	☐	☐	☐	☐	☐	☐
1	☐	☐	☐	☐	☐	☐	☐	☐
2	☐	☐	☐	☐	☐	☐	☐	☐
3	☐	☐	☐	☐	☐	☐	☐	☐
4	☐	☐	☐	☐	☐	☐	☐	☐
5	☐	☐	☐	☐	☐	☐	☐	☐
6	☐	☐	☐	☐	☐	☐	☐	☐
7	☐	☐	☐	☐	☐	☐	☐	☐
8	☐	☐	☐	☐	☐	☐	☐	☐
9	☐	☐	☐	☐	☐	☐	☐	☐
10	☐	☐	☐	☐	☐	☐	☐	☐
11	☐	☐	☐	☐	☐	☐	☐	☐
12	☐	☐	☐	☐	☐	☐	☐	☐
13	☐	☐	☐	☐	☐	☐	☐	☐
14	☐	☐	☐	☐	☐	☐	☐	☐
15	☐	☐	☐	☐	☐	☐	☐	☐
16	☐	☐	☐	☐	☐	☐	☐	☐
17	☐	☐	☐	☐	☐	☐	☐	☐
18	☐	☐	☐	☐	☐	☐	☐	☐
19	☐	☐	☐	☐	☐	☐	☐	☐
20	☐	☐	☐	☐	☐	☐	☐	☐
21	☐	☐	☐	☐	☐	☐	☐	☐
22	☐	☐	☐	☐	☐	☐	☐	☐
23	☐	☐	☐	☐	☐	☐	☐	☐
24	☐	☐	☐	☐	☐	☐	☐	☐
25	☐	☐	☐	☐	☐	☐	☐	☐
26	☐	☐	☐	☐	☐	☐	☐	☐
27	☐	☐	☐	☐	☐	☐	☐	☐
28	☐	☐	☐	☐	☐	☐	☐	☐

Apply   Reset

Parameter description:

● **Port :**

The port number for which the configuration below applies.

● **Enabled :**

Controls whether the queue policer is enabled on this switch port.

- **Rate :**

  Controls the rate for the queue policer. The default value is 500. This value is restricted to 100-1000000 when the "Unit" is "kbps", and it is restricted to 1-10000 when the "Unit" is "Mbps".

  This field is only shown if at least one of the queue policers are enabled.

- **Unit :**

  Controls the unit of measure for the queue policer rate as kbps or Mbps. The default value is "kbps".

  This field is only shown if at least one of the queue policers is enabled.

- **Buttons:**

  Apply – Click to apply changes.

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

3-14.4 Port Scheduler

This section provides an overview of QoS Egress Port Schedulers for all switch ports. and the ports belong to the currently selected stack 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 3-14.4: The QoS Egress Port Schedules

QoS Egress Port Schedulers

Click the Port index to set the QoS Egress Port Schedulers

Port	Mode	Q0	Q1	Q2			
1	Strict Priority	-	-	-			
2	Strict Priority	-	-	-	-	-	-
3	Strict Priority	-	-	-	-	-	-
4	Strict Priority	-	-	-	-	-	-
5	Strict Priority	-	-	-	-	-	-
6	Strict Priority	-	-	-	-	-	-
7	Strict Priority	-	-	-	-	-	-
8	Strict Priority	-	-	-	-	-	-
9	Strict Priority	-	-	-	-	-	-
10	Strict Priority	-	-	-	-	-	-
11	Strict Priority	-	-	-	-	-	-
12	Strict Priority	-	-	-	-	-	-
13	Strict Priority	-	-	-	-	-	-
14	Strict Priority	-	-	-	-	-	-
15	Strict Priority	-	-	-	-	-	-
16	Strict Priority	-	-	-	-	-	-
17	Strict Priority	-	-	-	-	-	-
18	Strict Priority	-	-	-	-	-	-
19	Strict Priority	-	-	-	-	-	-
20	Strict Priority	-	-	-	-	-	-
21	Strict Priority	-	-	-	-	-	-
22	Strict Priority	-	-	-	-	-	-
23	Strict Priority	-	-	-	-	-	-
24	Strict Priority	-	-	-	-	-	-
25	Strict Priority	-	-	-	-	-	-
26	Strict Priority	-	-	-	-	-	-
27	Strict Priority	-	-	-	-	-	-
28	Strict Priority	-	-	-	-	-	-

QoS Egress Port Scheduler and Shapers Port 1

Port 1 ▼

Scheduler Mode	Strict Priority ▼

Queue Shaper			
Enable	Rate	Unit	Excess

Port Shaper		
Enable	Rate	Unit

Q0 — S
☐ 500 kbps ▼ ☐

Q1 — S
☐ 500 kbps ▼ ☐

Q2 — S
☐ 500 kbps ▼ ☐

Q3 — S
☐ 500 kbps ▼ ☐

Q4 — S
☐ 500 kbps ▼ ☐

Q5 — S
☐ 500 kbps ▼ ☐

Q6 — S
☐ 500 kbps ▼ ☐

Q7 — S
☐ 500 kbps ▼ ☐

STRICT

S
☐ 500 kbps ▼

Apply   Reset   Cancel

QoS Egress Port Scheduler and Shapers Port 1

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 500. This value is restricted to 100-1000000 when the "Unit" is "kbps", and it is restricted to 1-10000 when the "Unit" is "Mbps".

- **Queue Shaper Unit :**

  Controls the unit of measure for the queue shaper rate as "kbps" or "Mbps". The default

value is "kbps".

- **Queue Shaper Excess :**

  Controls whether the queue is allowed to use excess bandwidth.

- **Queue Scheduler Weight :**

  Controls the weight for this queue. The default value is "17". This value is restricted to 1-100. This parameter is only shown if "Scheduler Mode" is set to "Weighted".

- **Queue Scheduler Percent :**

  Shows the weight in percent for this queue. This parameter is only shown if "Scheduler Mode" is set to "Weighted"

- **Port Shaper Enable :**

  Controls whether the port shaper is enabled for this switch port.

- **Port Shaper Rate :**

  Controls the rate for the port shaper. The default value is 500. This value is restricted to 100-1000000 when the "Unit" is "kbps", and it is restricted to 1-10000 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 apply changes.

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

3-14.5 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 stack 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 3-14.5: The QoS Egress Port Shapers

QoS Egress Port Shapers

Click the Port index to set the QoS Egress Port Shapers

Port	Shapers								Port
---	Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7	
1	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
10	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
11	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
12	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
13	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
14	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
15	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
16	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
17	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
18	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
19	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
20	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
21	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
22	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
23	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
24	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
25	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
26	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
27	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
28	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled

QoS Egress Port Scheduler and Shapers Port 1

Port 1 ▾

Scheduler Mode | Strict Priority ▾

Queue Shaper			
Enable	**Rate**	**Unit**	**Excess**

Q0 (S) ☐ 500 kbps ▾ ☐

Q1 (S) ☐ 500 kbps ▾ ☐

Q2 (S) ☐ 500 kbps ▾ ☐

Q3 (S) ☐ 500 kbps ▾ ☐

Q4 (S) ☐ 500 kbps ▾ ☐

Q5 (S) ☐ 500 kbps ▾ ☐

Q6 (S) ☐ 500 kbps ▾ ☐

Q7 (S) ☐ 500 kbps ▾ ☐

STRICT

Port Shaper		
Enable	**Rate**	**Unit**
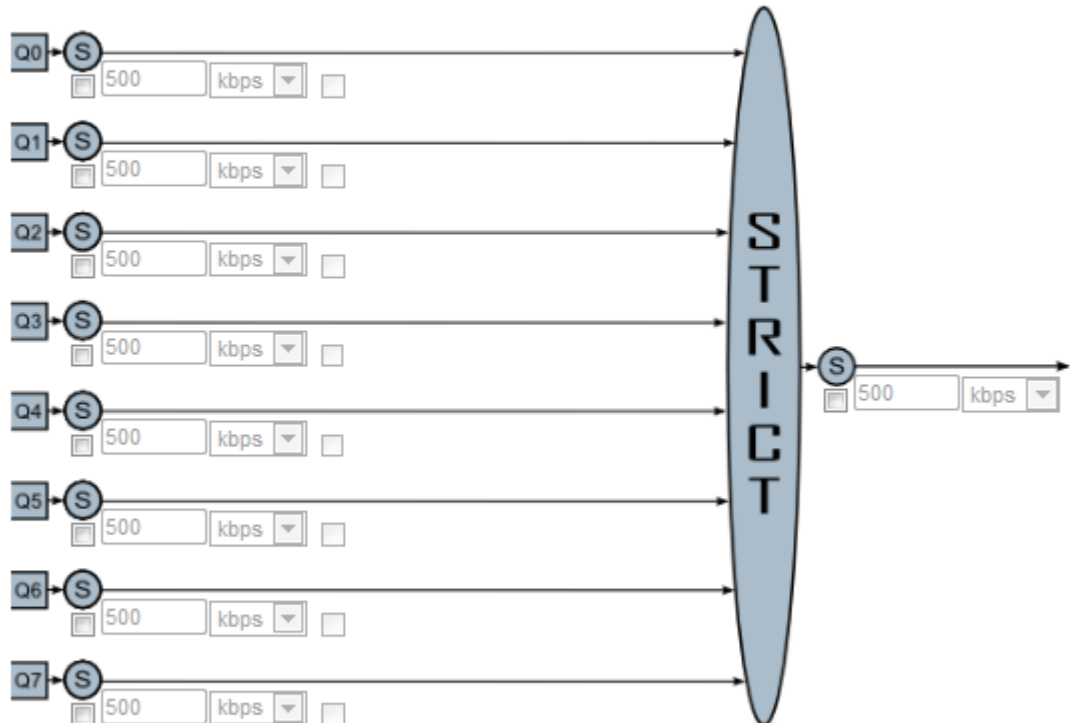
(S) ☐ 500 kbps ▾

[Apply] [Reset] [Cancel]

QoS Egress Port Scheduler and Shapers Port 1   Port 1 ▼

Scheduler Mode Weighted ▼

| Queue Shaper | | | | Queue Scheduler | | Port Shaper | | |
| Enable | Rate | Unit | Excess | Weight | Percent | Enable | Rate | Unit |

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

Q0 — (S) — 500 kbps ▼ □   17   17%
Q1 — (S) — 500 kbps ▼ □   17   17%
Q2 — (S) — 500 kbps ▼ □   17   17%
Q3 — (S) — 500 kbps ▼ □   17   17%
Q4 — (S) — 500 kbps ▼ □   17   17%
Q5 — (S) — 500 kbps ▼ □   17   17%
Q6 — (S) — 500 kbps ▼ □
Q7 — (S) — 500 kbps ▼ □

D W R R   S T R I C T

(S) □ 500 kbps ▼

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 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 500. This value is restricted to 100-1000000 when the "Unit" is "kbps", and it is restricted to 1-10000 when the "Unit" is "Mbps".

- **Queue Shaper Unit :**

  Controls the unit of measure for the queue shaper rate as "kbps" or "Mbps". The default value is "kbps".

- **Queue Shaper Excess :**

Controls whether the queue is allowed to use excess bandwidth.

- **Queue Scheduler Weight :**

  Controls the weight for this queue. The default value is "17". This value is restricted to 1-100. This parameter is only shown if "Scheduler Mode" is set to "Weighted".

- **Queue Scheduler Percent :**

  Shows the weight in percent for this queue. This parameter is only shown if "Scheduler Mode" is set to "Weighted"

- **Port Shaper Enable :**

  Controls whether the port shaper is enabled for this switch port.

- **Port Shaper Rate :**

  Controls the rate for the port shaper. The default value is 500. This value is restricted to 100-1000000 when the "Unit" is "kbps", and it is restricted to 1-10000 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 apply changes.

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

3-14.6 Port Tag Remarking

The Section provides user to get an overview of QoS Egress Port Tag Remarking for all switch ports. Others the ports belong to the currently selected stack unit, as reflected by the page header. .

Web Interface

To display the QoS Port Tag Remarking in the web interface:

1. Click Configuration, QoS, Port Tag Remarking

Figure 3-14.6: The Port Tag Remarking

Parameter description:

- **Port :**

  The logical port for the settings contained in the same row. Click on the port number in order to configure tag remarking.

- **Mode :**

Shows the tag remarking mode for this port.

Classified: Use classified PCP/DEI values.

Default: Use default PCP/DEI values.

Mapped: Use mapped versions of QoS class and DP level.

- **Tag Remarking Mode :**

  To scroll to select the tag remarking mode for this port.

  Classified: Use classified PCP/DEI values.

  Default: Use default PCP/DEI values.

  Mapped: Use mapped versions of QoS class and DP level.

- **PCP/DEI Configuration :**

  Controls the default PCP and DEI values used when the mode is set to Default.

- **DP level Configuration :**

  Controls the Drop Precedence level translation table when the mode is set to Mapped.

  The purpose of this table is to reduce the 2 bit classified DP level to a 1 bit DP level used in the (QoS class, DP level) to (PCP, DEI) mapping process.

- **(QoS class, DP level) to (PCP, DEI) Mapping :**

  Controls the mapping of the classified (QoS class, DP level) to (PCP, DEI) values when the mode is set to Mapped.

- **Buttons:**

  Apply – Click to apply changes.

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

  Cancel – Click to cancel the changes.

3-14.7 Port DSCP

The section will teach user to set the QoS Port DSCP configuration that was allowed you to configure the basic QoS Port DSCP Configuration settings for all switch ports. Others the settings relate to the currently selected stack unit, as reflected by the page header.

Web Interface

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

1. Click Configuration, QoS, Port DSCP
2. Evoke to enable or disable the Ingress Translate and Scroll the Classify Parameter configuration
3. Scroll to select Egress Rewrite parameters
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 3-14.7: The QoS Port DSCP Configuration

QoS Port DSCP Configuration

Port	Ingress		Egress
	Translate	Classify	Rewrite
*	☐	<> ▼	<> ▼
1	☐	Disable ▼	Disable ▼
2	☐	Disable ▼	Disable ▼
3	☐	Disable ▼	Disable ▼
4	☐	Disable ▼	Disable ▼
5	☐	Disable ▼	Disable ▼
6	☐	Disable ▼	Disable ▼
7	☐	Disable ▼	Disable ▼
8	☐	Disable ▼	Disable ▼
9	☐	Disable ▼	Disable ▼
10	☐	Disable ▼	Disable ▼
11	☐	Disable ▼	Disable ▼
12	☐	Disable ▼	Disable ▼
13	☐	Disable ▼	Disable ▼
14	☐	Disable ▼	Disable ▼
15	☐	Disable ▼	Disable ▼
16	☐	Disable ▼	Disable ▼
17	☐	Disable ▼	Disable ▼
18	☐	Disable ▼	Disable ▼
19	☐	Disable ▼	Disable ▼
20	☐	Disable ▼	Disable ▼
21	☐	Disable ▼	Disable ▼
22	☐	Disable ▼	Disable ▼
23	☐	Disable ▼	Disable ▼
24	☐	Disable ▼	Disable ▼
25	☐	Disable ▼	Disable ▼
26	☐	Disable ▼	Disable ▼
27	☐	Disable ▼	Disable ▼
28	☐	Disable ▼	Disable ▼

[Apply] [Reset]

Parameter description:

- **Port :**

   The Port column shows the list of ports for which you can configure DSCP ingress and egress settings.

- **Ingress :**

   In Ingress settings you can change ingress translation and classification settings for individual ports.

   There are two configuration parameters available in Ingress:

   1. **Translate :** To Enable the Ingress Translation click the checkbox

   2. **Classify:** Classification for a port have 4 different values

   - Disable: No Ingress DSCP Classification.

- DSCP=0: Classify if incoming (or translated if enabled) DSCP is 0.
- Selected: Classify only selected DSCP for which classification is enabled as specified in DSCP Translation window for the specific DSCP.
- All: Classify all DSCP.

- **Egress :**

  Port Egress Rewriting can be one of below parameters

  - Disable: No Egress rewrite.
  - Enable: Rewrite enable without remapped.
  - Remap: DSCP from analyzer is remapped and frame is remarked with remapped DSCP value.

- **Buttons:**

  Apply – Click to apply changes.

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

3-14.8 DSCP-Based QoS

The section will teach user to configure the DSCP-Based QoS mode that This page allows you to configure the basic QoS DSCP based QoS Ingress Classification settings for all switches.

Web Interface

To configure the DSCP –Based QoS Ingress Classification parameters in the web interface:

1. Click Configuration, QoS, DSCP-Based QoS
2. Evoke to enable or disable the DSCP for Trust
3. Scroll to select QoS Class and DPL parameters
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 3-14.8: The DSCP-Based QoS Ingress Classification Configuration

Parameter description:

- **DSCP :**

  Maximum number of support ed DSCP values are 64.

- **Trust :**

  Controls whether a specific DSCP value is trusted. Only frames with trusted DSCP values are mapped to a specific QoS class and Drop Precedence Level. Frames with untrusted DSCP values are treated as a non-IP frame.

- **QoS Class :**

    QoS Class value can be any of (0-7)

- **DPL :**

    Drop Precedence Level (0-3)

- **Buttons:**

    Apply – Click to apply changes.

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

3-14.9 DSCP Translation

The section describes the switch allows you to configure the basic QoS DSCP Translation settings for all switches. DSCP translation can be done in Ingress or Egress.

Web Interface

To configure the DSCP Translation parameters in the web interface:

1. Click Configuration, QoS, DSCP Translation
2. Scroll to set the Ingress Translate and Egress Remap DP0 and Remap DP1 Parameters
3. Evoke to enable or disable Classify
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 3-14.9: The DSCP Translation Configuration

DSCP Translation

DSCP	Ingress Translate	Ingress Classify	Egress Remap
*	<>	☐	<>
0 (BE)	0 (BE)	☐	0 (BE)
1	1	☐	1
2	2	☐	2
3	3	☐	3
4	4	☐	4
5	5	☐	5
6	6	☐	6
7	7	☐	7
8 (CS1)	8 (CS1)	☐	8 (CS1)
9	9	☐	9
10 (AF11)	10 (AF11)	☐	10 (AF11)
11	11	☐	11
12 (AF12)	12 (AF12)	☐	12 (AF12)
13	13	☐	13
14 (AF13)	14 (AF13)	☐	14 (AF13)
51	51	☐	51
52	52	☐	52
53	53	☐	53
54	54	☐	54
55	55	☐	55
56 (CS7)	56 (CS7)	☐	56 (CS7)
57	57	☐	57
58	58	☐	58
59	59	☐	59
60	60	☐	60
61	61	☐	61
62	62	☐	62
63	63	☐	63

Apply Reset

Parameter description:

- **DSCP :**

    Maximum number of supported DSCP values is 64 and valid DSCP value ranges from 0 to 63.

- **Ingress :**

    Ingress side DSCP can be first translated to new DSCP before using the DSCP for QoS class and DPL map.

    There are two configuration parameters for DSCP Translation –

    1. **Translate :** DSCP at Ingress side can be translated to any of (0-63) DSCP values.

    2. **Classify :** Click to enable Classification at Ingress side.

- **Egress :**

    There are following configurable parameters for Egress side –

    1. **Remap DP0 :** Select the DSCP value from select menu to which you want to remap. DSCP value ranges from 0 to 63

    2. **Remap DP1 :** Select the DSCP value from select menu to which you want to remap. DSCP value ranges from 0 to 63.

    There is following configurable parameter for Egress side -

    - **Remap:** Select the DSCP value from select menu to which you want to remap. DSCP value ranges from 0 to 63.

- **Buttons:**

    Apply – Click to apply changes.

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

3-14.10 DSCP Classification

The section describes to teach user to configure and allows you to map DSCP value to a QoS Class and DPL value. Others the settings relate to the currently selected stack unit, as reflected by the page header.

Web Interface

To configure the DSCP Classification parameters in the web interface:
1. Click Configuration, QoS, DSCP Translation
2. Scroll to set the DSCP 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 3-14.10: The DSCP Classification Configuration

DSCP Classification

QoS Class	DSCP
*	<>
0	0 (BE)
1	0 (BE)
2	0 (BE)
3	0 (BE)
4	0 (BE)
5	0 (BE)
6	0 (BE)
7	0 (BE)

Apply Reset

Parameter description:

- **QoS Class :**

  Available QoS Class value ranges from 0 to 7. QoS Class (0-7) can be mapped to followed parameters.

- **DSCP :**

  Select DSCP value (0-63) from DSCP menu to map DSCP to corresponding QoS Class

  and DPL value

- **Buttons:**

  Apply – Click to apply changes.

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

3-14.11 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 Contol 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 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 3-14.11: 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 1-4095 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: 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.

- **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.

- **Port Members :**

  Check the checkbox button in case you what 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 Configuration :**

    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 changes.

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

3-14.12 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 an entry of the MVR Statistics
   information.

Figure 3-14.12: The QoS Control List Status

User	QCE#	Frame Type	Port	Action			Conflict
				Class	DPL	DSCP	
No entries							

Parameter description:

● **User :**

Indicates the QCL user.

● **QCE#**

Indicates the index of QCE.

● **Frame Type :**

Indicates the type of frame to look for incomming 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.

● **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 QCE status. It may happen that resources required to add a QCE may not 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 resource required by the QCE and pressing 'Refresh' button.

- **Auto-refresh :**

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

- **Resolve Conflict :**

  Click it to resolve the conflict issue.

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

  You can click them for refresh the QCL information by manual.

3-14.13 Storm Control

The section allows user to configure the Storm control for the switch. There is a unicast storm rate control, multicast storm rate control, and a broadcast storm rate control. These only affect flooded frames, i.e. frames with a (VLAN ID, DMAC) pair not present on the MAC Address table. The configuration indicates the permitted packet rate for unicast, multicast or broadcast traffic across the switch

Web Interface

To configure the Storm Control Configuration parameters in the web interface:

1. Click Configuration, QoS, Storm Control Configuration
2. Evoke to select the frame type to enable storm control
3. Scroll to set the Rate Parameters
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 3-14.13: The Storm Control Configuration

QoS Port Storm Control

Port	Unicast Frames			Broadcast Frames			Unknown Frames		
	Enabled	Rate	Unit	Enabled	Rate	Unit	Enabled	Rate	Unit
*	☐		<> ▼	☐		<> ▼	☐		<> ▼
1	☐	500	kbps ▼	☐	500	kbps ▼	☐	500	kbps ▼
2	☐	500	kbps ▼	☐	500	kbps ▼	☐	500	kbps ▼
3	☐	500	kbps ▼	☐	500	kbps ▼	☐	500	kbps ▼
4	☐	500	kbps ▼	☐	500	kbps ▼	☐	500	kbps ▼
5	☐	500	kbps ▼	☐	500	kbps ▼	☐	500	kbps ▼
6	☐	500	kbps ▼	☐	500	kbps ▼	☐	500	kbps ▼
7	☐	500	kbps ▼	☐	500	kbps ▼	☐	500	kbps ▼
8	☐	500	kbps ▼	☐	500	kbps ▼	☐	500	kbps ▼
9	☐	500	kbps ▼	☐	500	kbps ▼	☐	500	kbps ▼
10	☐	500	kbps ▼	☐	500	kbps ▼	☐	500	kbps ▼
11	☐	500	kbps ▼	☐	500	kbps ▼	☐	500	kbps ▼
12	☐	500	kbps ▼	☐	500	kbps ▼	☐	500	kbps ▼
13	☐	500	kbps ▼	☐	500	kbps ▼	☐	500	kbps ▼
14	☐	500	kbps ▼	☐	500	kbps ▼	☐	500	kbps ▼
15	☐	500	kbps ▼	☐	500	kbps ▼	☐	500	kbps ▼
16	☐	500	kbps ▼	☐	500	kbps ▼	☐	500	kbps ▼
17	☐	500	kbps ▼	☐	500	kbps ▼	☐	500	kbps ▼
18	☐	500	kbps ▼	☐	500	kbps ▼	☐	500	kbps ▼
19	☐	500	kbps ▼	☐	500	kbps ▼	☐	500	kbps ▼
20	☐	500	kbps ▼	☐	500	kbps ▼	☐	500	kbps ▼
21	☐	500	kbps ▼	☐	500	kbps ▼	☐	500	kbps ▼
22	☐	500	kbps ▼	☐	500	kbps ▼	☐	500	kbps ▼
23	☐	500	kbps ▼	☐	500	kbps ▼	☐	500	kbps ▼
24	☐	500	kbps ▼	☐	500	kbps ▼	☐	500	kbps ▼
25	☐	500	kbps ▼	☐	500	kbps ▼	☐	500	kbps ▼
26	☐	500	kbps ▼	☐	500	kbps ▼	☐	500	kbps ▼
27	☐	500	kbps ▼	☐	500	kbps ▼	☐	500	kbps ▼
28	☐	500	kbps ▼	☐	500	kbps ▼	☐	500	kbps ▼

[Apply] [Reset]

Parameter description:

● **Port :**

The port number for which the configuration below applies.

- **Enable :**

  Controls whether the storm control is enabled on this switch port.

- **Rate :**

  Controls the rate for the storm control. The default value is 500. This value is restricted to 100-1000000 when the "Unit" is "kbps" or "fps", and it is restricted to 1-10000 when the "Unit" is "Mbps" or "kfps".

- **Unit :**

  Controls the unit of measure for the storm control rate as kbps, Mbps, fps or kfps . The default value is "kbps".

- **Buttons:**

  Apply – Click to apply changes.

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

3-14.14 WRED

This page allows you to configure the Random Early Detection (RED) settings for queue 0 to 5. RED cannot be applied to queue 6 and 7.

Through different RED configuration for the queues (QoS classes) it is possible to obtain Weighted Random Early Detection (WRED) operation between queues.

The settings are global for all ports in the switch.

RED Drop Probability Function

The following illustration shows the drop probability function with associated parameters.
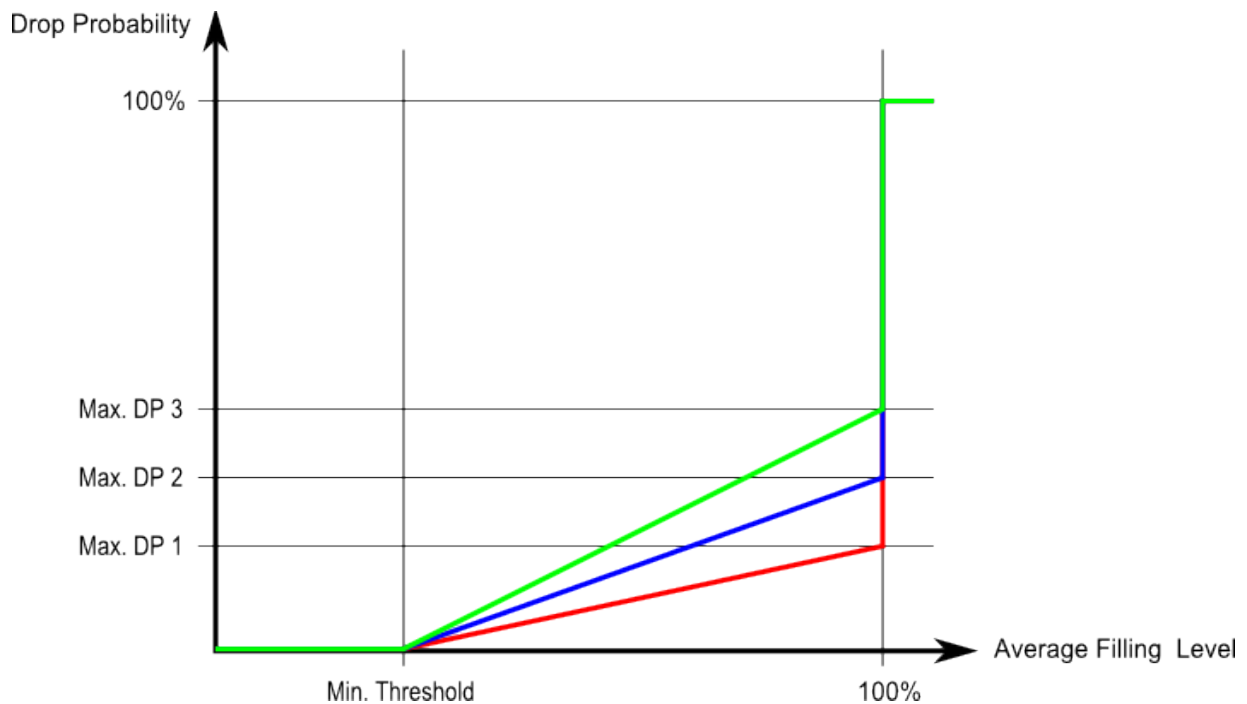
Max. DP 1-3 is the drop probability when the average queue filling level is 100%. Frames marked with Drop Precedence Level 0 are never dropped. Min. Threshold is the average queue filling level where the queues randomly start dropping frames. The drop probability for frames marked with Drop Precedence Level n increases linearly from zero (at Min. Threshold average queue filling level) to Max. DP n (at 100% average queue filling level).

Web Interface

To configure the Weighted Random Early Detection Configuration parameters in the web interface:

1. Click Configuration, QoS, WRED Configuration
2. Evoke to enable WRED
3. Specify Min. Threshold, Max. DP 1, Max. DP 2, Max. DP 3
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 3-14.14: The WRED Configuration

Weighted Random Early Detection Configuration

Queue	Enable	Min. Threshold	Max. DP 1	Max. DP 2	Max. DP 3
0	☐	0	1	5	10
1	☐	0	1	5	10
2	☐	0	1	5	10
3	☐	0	1	5	10
4	☐	0	1	5	10
5	☐	0	1	5	10

[Apply] [Reset]

Parameter description:

- **Queue**

  The queue number (QoS class) for which the configuration below applies.

- **Enable**

  Controls whether RED is enabled for this queue.

- **Min. Threshold**

  Controls the lower RED threshold. If the average queue filling level is below this threshold, the drop probability is zero. This value is restricted to 0-100.

- **Max. DP 1**

  Controls the drop probability for frames marked with Drop Precedence Level 1 when the average queue filling level is 100%. This value is restricted to 0-100.

- **Max. DP 2**

  Controls the drop probability for frames marked with Drop Precedence Level 2 when the average queue filling level is 100%. This value is restricted to 0-100.

- **Max. DP 3**

  Controls the drop probability for frames marked with Drop Precedence Level 3 when the average queue filling level is 100%. This value is restricted to 0-100.

- **Buttons**

  Apply: Click to apply changes.

  Reset: Click to undo any changes made locally and revert

3-15 EVC

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

3-15.1 Configuration

The section describes how to set EVC Control List Configuration.

Web Interface

To configure the EVC parameters in the web interface:
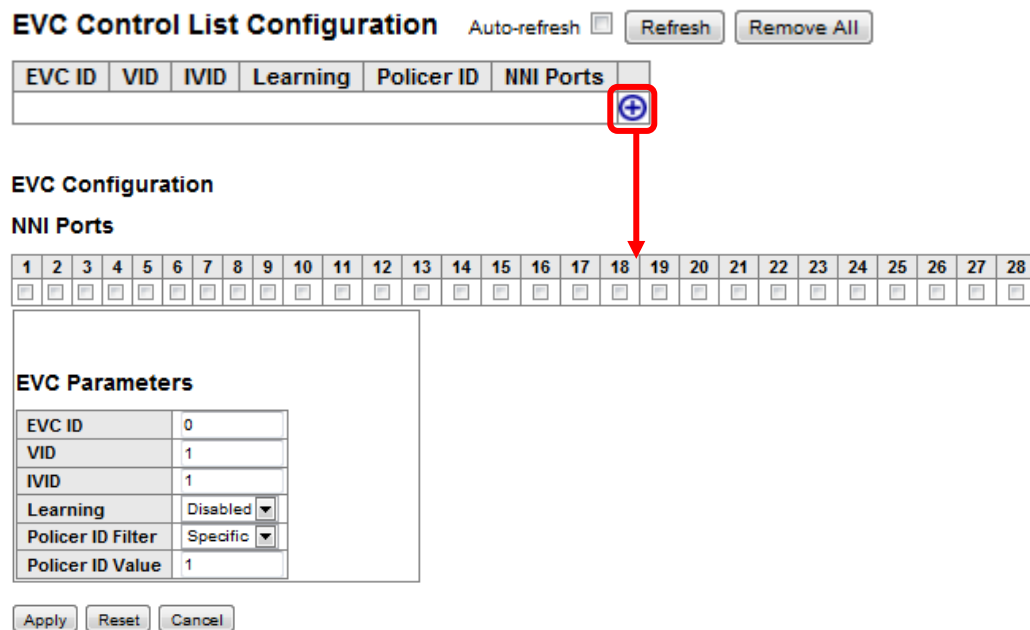
1. Click Configuration, EVC, Configuration

2. Click ⊕ button to add a new EVC, or use the other EVC
3. Choice which NNI ports would you like to set the parameters
4. If you want to cancel the setting then you need to click the Reset button.
   It will revert to previously saved values or click Apply to save changes.

Figure 3-15.1: The EVC Configuration.

Parameter description:

- **EVC ID**

  The EVC ID identifies the EVC. The range is from 1 through 128.

- **VID**

  The VLAN ID in the PB network. It may be inserted in a C-tag, S-tag or S-custom tag depending on the NNI port VLAN configuration. The range is from 1 through 4094.

- **IVID**

  The Internal/classified VLAN ID in the PB network. The range is from 1 through 4094.

- **Learning**

  The learning mode for the EVC controls whether source MAC addresses are learned for

frames matching the EVC. Learning may be disabled if the EVC only includes two UNI/NNI ports. The possible values are:

Enabled: Learning is enabled (MAC addresses are learned).
Disabled: Learning is disabled (MAC addresses are not learned).

- **Policer ID**

  The ingress bandwidth profile mode for the EVC. The possible values are:
  Specific: The range is from 1 through 128.
  Discard: All received frames are discarded for the EVC.
  None: None bandwidth profile for the EVC.

- **NNI Ports**

  The list of Network to Network Interfaces for the EVC.

- **Modification Buttons**

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

  : Edits the EVC row.
  : Deletes the EVC.
  : Adds new EVC.

- **Buttons**

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

  Refresh: Click to refresh the page.

  Remove All: Click to remove all EVCs.

3-15.2 Ports

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

Web Interface

To configure the DSCP Classification parameters in the web interface:
1. Click Configuration, EVC, Ports
2. Scroll to set the DEI Mode 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 3-15.2: The EVC Ports

Parameter description:

- **Port :**

  The logical port for the settings contained in the same row.

- **DEI Mode :**

  The DEI mode for an NNI port determines whether frames transmitted on the port will have the DEI field in the outer tag marked based on the colour of the frame. The allowed values are:

  Coloured: The DEI is 1 for yellow frames and 0 for green frames.

  Fixed: The DEI value is determined by ECE rules.

- **Buttons:**

  Apply – Click to apply changes.

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

3-15.3 Bandwidth Profile

This page displays current EVC ingress bandwidth profile configurations. These policers may be used to limit the traffic received on UNI ports. The settings can also be configured here.

Web Interface

To configure GARP Port Configuration in the web interface:
1. Click configure, EVC, Bandwidth Profile.
2. Scroll to set the State and Policer Mode 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 3-15.3: The Bandwidth Profile

Bandwidth Profiles Configuration

Start from Policer ID |1| with |20| entries per page.

Policer ID	State	Policer Mode	CIR (kbps)	CBS (bytes)	EIR (kbps)	EBS (bytes)
*	◇	◇				
1	Disabled	Blind	0	0	0	0
2	Disabled	Blind	0	0	0	0
3	Disabled	Blind	0	0	0	0
4	Disabled	Blind	0	0	0	0
5	Disabled	Blind	0	0	0	0
6	Disabled	Blind	0	0	0	0
7	Disabled	Blind	0	0	0	0
8	Disabled	Blind	0	0	0	0
9	Disabled	Blind	0	0	0	0
10	Disabled	Blind	0	0	0	0
11	Disabled	Blind	0	0	0	0
12	Disabled	Blind	0	0	0	0
13	Disabled	Blind	0	0	0	0
14	Disabled	Blind	0	0	0	0
15	Disabled	Blind	0	0	0	0
16	Disabled	Blind	0	0	0	0
17	Disabled	Blind	0	0	0	0
18	Disabled	Blind	0	0	0	0
19	Disabled	Blind	0	0	0	0
20	Disabled	Blind	0	0	0	0

Apply   Reset

Parameter description:

- **Start Policer ID :**

  The start Policer ID for displaying the table entries. The allowed range is from 1 through 128.

- **Number of Entries :**

  The number of entries per page. The allowed range is from 2 through 128.

- **Policer ID :**

  The Policer ID is used to identify one of the 128 policers.

- **State :**

The administrative state of the bandwidth profile. The allowed values are:

Enabled: The bandwidth profile enabled.

Disabled: The bandwidth profile is disabled.

- **Policer Mode**

    The colour mode of the bandwidth profile. The allowed values are:

    Coupled: Colour-aware mode with coupling enabled.

    Aware: Colour-aware mode with coupling disabled.

    Blind: Colour-blind mode.

- **CIR**

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

- **CBS**

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

- **EIR**

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

- **EBS**

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

- **Buttons:**

    Apply – Click to apply changes.

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

3-15.4 ECE

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

Web Interface

To configure the ECE Control List parameters in the web interface:
1. Click Configuration, EVC, EVE
2. Click the ⊕ to add a new ECE Control List
3. Scroll all parameters and evoke the Port Member to join the ECE ID rules
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
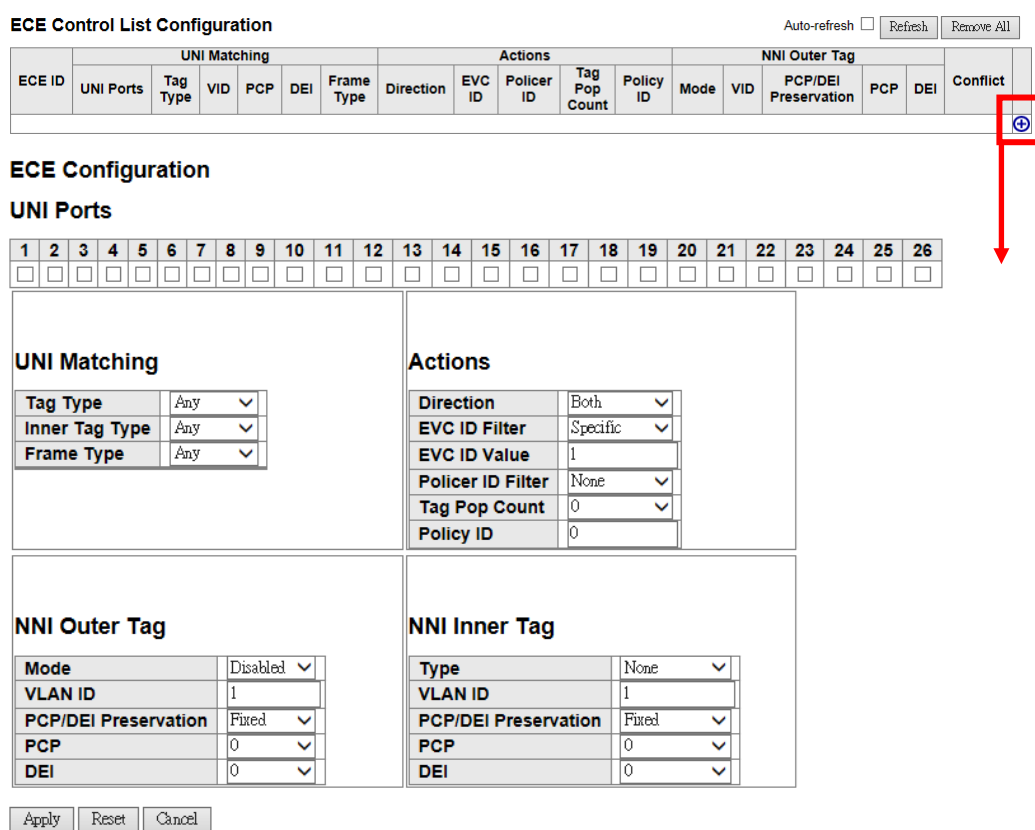
Figure 3-15.4: The ECE Control List Configuration

Parameter description:

ECE Control List Configuration

- **ECE ID:**

  The ECE ID identifies the ECE. Unique ECE IDs are automatically assigned to ECEs added. The possible range is from 1 through 128.

UNI Matching

- **UNI Ports :**

  The list of User Network Interfaces for the ECE.

- **Tag Type :**

  The tag type for the ECE. The possible values are:

Tagged: The ECE will match tagged frames only.

Untagged: The ECE will match untagged frames only.

Any: The ECE will match both tagged and untagged frames.

- **VID :**

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

  Specific: The range is from 1 through 4094.

  Any: The ECE will match any VLAN ID.

- **PCP:**

  The PCP value for the ECE. It only significant if tag type 'Tagged' is selected. The possible values are:

  Specific: The ECE will match a specific PCP in the range 0 through 7.

  Range: The ECE will match PCP values in the selected range 0-1, 2-3, 4-5, 6-7, 0-3 or 4-7.

  Any: The ECE will match any PCP value.

- **VID :**

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

  Specific: The range is from 1 through 4094.

  Any: The ECE will match any VLAN ID.

- **PCP :**

  The PCP value for the ECE. It only significant if tag type 'Tagged' is selected. The possible values are:

  Specific: The ECE will match a specific PCP in the range 0 through 7.

  Range: The ECE will match PCP values in the selected range 0-1, 2-3, 4-5, 6-7, 0-3 or 4-7.

  Any: The ECE will match any PCP value.

- **DEI :**

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

- **Frame Type :**

  The frame type for the ECE. The possible values are:

  Any: The ECE will match any frame type.

  IPv4: The ECE will match IPv4 frames only.

  IPv6: The ECE will match IPv6 frames only.

Actions

- **Direction :**

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

  Both: Bidirectional.

  UNI-to-NNI: Unidirectional from UNI to NNI.

  NNI-to-UNI: Unidirectional from NNI to UNI.

- **EVC ID :**

  The EVC ID for the ECE. The ECE is only active when mapping to an existing EVC. Possible values are:

Specific: The range is from 1 through 128.

None: The ECE does not map to an EVC.

- **Policer ID :**

  The ingress bandwidth profile mode for the ECE. The possible values are:

  Specific: The range is from 1 through 128.

  Discard: All received frames are discarded for the ECE.

  None: All received frames are forwarded for the ECE. Tag Pop Count

- **Tag Pop Count :**

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

- **Policy ID :**

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

NNI Outer Tag

- **Outer Tag Mode :**

  The outer tag for nni-to-uni direction for the ECE. The possible values are:

  Enable: Enable outer tag for nni-to-uni direction for the ECE.

  Disable: Disable outer tag for nni-to-uni direction for the ECE.

- **Outer Tag VID :**

  The EVC outer tag VID for UNI ports. The range is from 0 through 4094.

- **Outer Tag PCP/DEI Preservation :**

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

  Preserved: The outer tag PCP and DEI are preserved.

  Disable: The outer tag PCP and DEI are fixed.

- **Outer Tag PCP :**

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

- **Outer Tag DEI :**

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

- **Conflict :**

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

- **Modification Buttons :**

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

  : Inserts a new ECE before the current row.

  : Edits the ECE.

  : Moves the ECE up the list.

  : Moves the ECE down the list.

  : Deletes the ECE.

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

ECE Control List Configuration

UNI Ports

The list of User Network Interfaces for the ECE.

UNI Matching

● **Tag Type :**

The tag type for mataching the ECE. The possible values are:

Any: The ECE will match both tagged and untagged frames.

Untagged: The ECE will match untagged frames only.

Tagged: The ECE will match tagged frames only.

● **VLAN ID Filter :**

The VLAN ID filter for matching the ECE. It only significant if tag type 'Tagged' is selected. The possible values are:
Any: No VLAN ID filter is specified. (VLAN ID filter status is "don't-care".)
Specific: If you want to filter a specific VLAN ID value with this ECE, choose this value. A field for entering a specific value appears.
Range: If you want to filter a specific VLAN ID range filter with this ECE, choose this value. A field for entering a range appears.

● **VLAN ID Value :**

When "Specific" is selected for the VLAN ID filter, you can enter a specific value. The allowed value is from 0 through 4094.

● **VLAN ID Range :**

When "Range" is selected for the VLAN ID filter, you can enter a specific range. The allowed range is from 0 through 4094.

● **PCP :**

The PCP value for mataching the ECE. It only significant if tag type 'Tagged' is selected. The possible values are:

Any: The ECE will match any PCP value.

Specific: The ECE will match a specific PCP in the range 0 through 7.

Range: The ECE will match PCP values in the selected range 0-1, 2-3, 4-5, 6-7, 0-3 or 4-7.

● **DEI :**

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

● **Inner Tag Type :**

The inner tag type for mataching the ECE. The possible values are:

Any: The ECE will match both tagged and untagged frames.

Untagged: The ECE will match untagged frames only.

Tagged: The ECE will match tagged frames only.

● **Inner VLAN ID Filter :**

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

Any: No inner VLAN ID filter is specified. (Inner VLAN ID filter status is "don't-care".)

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

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

● **Inner VLAN ID Value :**

When "Specific" is selected for the VLAN ID filter, you can enter a specific value. The allowed value is from 0 through 4094.

- **Inner VLAN ID Range :**

  When "Range" is selected for the VLAN ID filter, you can enter a specific range. The allowed range is from 0 through 4094.

- **Inner Tag PCP :**

  The inner PCP value for mataching the ECE. It only significant if inner tag type 'Tagged' is selected. The possible values are:

  Any: The ECE will match any PCP value.

  Range: The ECE will match PCP values in the selected range 0-1, 2-3, 4-5, 6-7, 0-3 or 4-7.

  Specific: The ECE will match a specific PCP in the range 0 through 7.

- **Inner Tag DEI :**

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

- **Frame Type :**

  The frame type for the ECE. The possible values are:

  Any: The ECE will match any frame type.

  IPv4: The ECE will match IPv4 frames only.

  IPv6: The ECE will match IPv6 frames only.

- **DSCP Filter :**

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

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

  Specific: If you want to filter a specific DSCP value with this ECE, choose this value. A field for entering a specific value appears.

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

- **DSCP Value :**

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

- **DSCP Range :**

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

Actions

- **Direction :**

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

  Both: Bidirectional.

  UNI-to-NNI: Unidirectional from UNI to NNI.

  NNI-to-UNI: Unidirectional from NNI to UNI.

- **EVC ID Filter :**

  The EVC ID for the ECE. The ECE is only active when mapping to an existing EVC. The possible values are:

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

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

- **EVC ID Value :**

When "Specific" is selected for the VLAN ID filter, you can enter a specific value. The allowed value is from 1 through 128.

- **Policer ID Filter :**

    The policer ID filter for matching the ECE. The possible values are:

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

    Discard: All received frames are discarded for the ECE.

    None: All received frames are forwarded for the ECE.

    None: The bandwidth profile for the specified EVC ID is used.

- **Policer ID Value :**

    When "Specific" is selected for the policer ID filter, you can enter a specific value. The value is from 1 through 128.

- **Tag Pop Count :**

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

- **Policy ID :**

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

NNI Outer Tag

- **Outer Tag Mode :**

    The outer tag for nni-to-uni direction for the ECE. The possible values are:

    Enable: Enable outer tag for nni-to-uni direction for the ECE.

    Disable: Disable outer tag for nni-to-uni direction for the ECE.

- **Outer Tag VID :**

    The EVC outer tag VID for UNI ports. The allowed value is from 0 through 4094.

- **Outer Tag PCP/DEI Preservation :**

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

    Preserved: The outer tag PCP and DEI is preserved.

    Fixed: The outer tag PCP and DEI is fixed.

- **Outer Tag PCP :**

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

- **Outer Tag DEI :**

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

NNI Inner Tag

- **Inner Tag Type :**

    The inner type for the ECE determines whether an inner tag is inserted in frames forwarded to NNI ports. The possible values are:

    None: An inner tag is not inserted.

    C-tag: An inner C-tag is inserted.

    S-tag: An inner S-tag is inserted.

    S-custom-tag: An inner tag is inserted and the tag type is determined by the VLAN port configuration of the NNI.

- **Inner Tag VLAN ID :**

The inner tag VLAN ID for the ECE. The allowed range is from 0 through 4094.

- **Inner Tag PCP/DEI Preservation :**

    The inner tag PCP and DEI preservation for the ECE. The possible values are:

    Preserved: The inner tag PCP and DEI is preserved.

    Fixed: The inner tag PCP and DEI is fixed.

- **Inner Tag PCP :**

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

- **Inner Tag DEI:**

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

- **Buttons:**

    Apply – Click to apply changes.

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

3-15.5 EVC Statistics

This page provides NNI port traffic statistics for the selected EVC. It also shows counters for UNI ports of ECEs mapping to the EVC..

Web Interface

To configure the EVC Statistics parameters in the web interface:

1. Click Configuration, EVC, Statistics
2. Choose which unit of data Frames/ Bytes/ Both you want to check
3. If you want to update the most new information, please select "Auto-refresh"

Figure 3-15.5: The EVC Statistics

Parameter description:

- **Clear**

  This box is used to mark a port for clearance in next Clear operation.

- **Port**

  The UNI/NNI port for the EVC.

- **Rx Green**

  The number of green received.

- **Tx Green**

  The number of green transmitted.

- **Rx Yellow**

  The number of yellow received.

- **Tx Yellow**

  The number of yellow transmitted.

- **Rx Red**

  The number of red received.

- **Rx Discarded**

  The number of discarded in the ingress queue system.

- **Tx Discarded**

  The number of discarded in the egress queue system.

3-15.6 EVE Statistics

This page provides UNI port traffic statistics for available ECE. It also shows counters for NNI ports of the EVC to which the ECE is mapped.

Web Interface

To configure the EVC Statistics parameters in the web interface:

1. Click Configuration, EVE, Statistics
2. Choose which unit of data Frames/ Bytes/ Both e you want to check
3. If you want to update the most new information, please select "Auto-refresh"

Figure 3-15.5: The EVC Statistics

Clear	Port	Green Frames		Yellow Frames		Red Frames	Discarded Frames	
		Rx	Tx	Rx	Tx	Rx	Rx	Tx

Parameter description:

- **Clear**

  This box is used to mark a port for clearance in next Clear operation.

- **Port**

  The UNI/NNI port for the EVC.

- **Rx Green**

  The number of green received.

- **Tx Green**

  The number of green transmitted.

- **Rx Yellow**

  The number of yellow received.

- **Tx Yellow**

  The number of yellow transmitted.

- **Rx Red**

  The number of red received.

- **Rx Discarded**

  The number of discarded in the ingress queue system.

- **Tx Discarded**

  The number of discarded in the egress queue system.

3-16 Loop Protection

The loop detection is used to detect the presence of traffic. When switch receives packet's (looping detection frame) MAC address the same as oneself from port, show Loop Protection happens. The port will be locked when it received the looping detection 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.

3-16.1 Configuration

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

Web Interface

To configure the Loop protection parameters in the web interface:

1. Click Configuration, Loop Protection, Configuration.
2. Scroll all parameters and evoke the Enable
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 3-16.1: The Configuration

Parameter description:

General Settings

- **Enable Loop Protection**

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

- **Transmission Time**

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

- **Shutdown Time**

  The period (in seconds) for which a port will be kept disabled in the event of a loop is detected (and the port action shuts down the port). Valid values are 0 to 604800 seconds (7 days). A value of zero will keep a port disabled (until next device restart).

Port Configuration

- **Port**

  The switch port number of the port.

- **Enable**

  Controls whether loop protection is enabled on this switch port.

- **Action**

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

- **Tx Mode**

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

- **Buttons:**

  Apply – Click to apply changes.

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

3-16.2 Status

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

Web Interface

To configure the EVC Statistics parameters in the web interface:

1. Click Configuration, Loop Protection, Status
2. If you want to update the most new information, please select "Auto-refresh"

Figure 3-16.2: The Status

Loop Protection Status

Auto-refresh ☐ Refresh

Port	Action	Transmit	Loops	Status	Loop	Time of Last Loop
1	Shutdown	Enabled	0	Down	-	-
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	Down	-	-
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	-	-
19	Shutdown	Enabled	0	Down	-	-
20	Shutdown	Enabled	0	Down	-	-
21	Shutdown	Enabled	0	Down	-	-
22	Shutdown	Enabled	0	Up	-	-
23	Shutdown	Enabled	0	Down	-	-
24	Shutdown	Enabled	0	Down	-	-
25	Shutdown	Enabled	0	Down	-	-
26	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.

- **Loops**

   The number of loops detected on this port.

3-17 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 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 3-17: The Mirror Configuration

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 apply changes.

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

3-18 Trap Event Severity

The function is used to set an 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 3-18: The Trap Event Severity Configuration

Parameter description:

- **Group Name :**

  The name identifying the severity group.

- **Syslog Type :**

  Every group has its own specific type for syslog. The sending of syslog messages and syslog facility can be individually controlled according to Syslog Type in System Log Configuration page.

- **Severity Level :**

  Every group has an severity level. 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 apply changes.

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

3-19 SMTP Configuration

The function is used to set an Alarm trap when the switch alarm then you could set the SMTP server to send you the alarm mail.

Web Interface

To configure the SMTP Configuration in the web interface:

1. Click Configuration, SMTP Configuration
2. Scroll to select the Severity Level
3. Specify the parameters in each 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 3-19: The SMTP Configuration

Parameter description:

These parameters are displayed on the SMTP Configuration page:

- **Mail Server :**

  The IP address or hostname of the mail server. IP address is expressed in dotted decimal notation. This will be the device that sends out the mail for you

- **Username :**

  Specify the username on the mail server.

- **Password :**

  Specify the password on the mail server.

- **Severity :**

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

  <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.

- **Sender :**

  To set the mail sender name.

- **Return-Path :**

  Specify the sender email address of the alarm mail. This address will be the "from" address on the email message.

- **Email Address 1-6 :**

  Specify the email address of the receiver.

- **Buttons:**

  Apply – Click to apply changes.

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

3-20 802.3ah OAM

For Carrier Ethernet application that customer need to reduce operating cost and increase the remote maintain availability. The advent of Ethernet as a metropolitan and wide-area networking technology has accelerated the need for a new set of OAM protocols. Service provider networks are large and complex with a wide user base, and they often involve different operators that must work together to provide end-to-end services to enterprise customers. While enterprise end-customer demands continue to increase, so do the requirements for service provider Ethernet networks, particularly in the areas of availability and mean time to repair (MTTR). Ethernet OAM addresses these challenges and more, thereby directly impacting the competitiveness of the service provider. Ethernet has been used as a LAN technology for many years, and enterprises have managed these networks effectively, Ethernet OAM is a broad topic, but this paper will focus on three main areas of Ethernet OAM that are most in need by service providers and are rapidly evolving in the standards bodies: Service Layer OAM (IEEE 802.1ag Connectivity Fault Management), Link Layer OAM (IEEE 802.3ah OAM), and Ethernet Local Management Interface (MEF-16 E-LMI). Each of these different OAM protocols has unique objectives and is complementary to the others. IEEE 802.1ag Connectivity Fault Management provides "service" management.

3-20.1 Port Config

This chapter allows the user to inspect the current Link OAM port configurations, and change them as well. It will help user to understand the Port configuration parameter what you need to set when you enable IEEE802.3ah OAM function on the switch.

Web Interface

To configure the 802.3ah OAM in the web interface:

1. Click Configuration, 802.3ah OAM then Port config.
2. Evoke which Port wants to enable OAM function.
3. Scroll to select OAM mode with Passive or Active.
4. Evoke which port wants to support Loopback, Link monitor, MIB Retrieval or Loopback operation.
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- 20.1: The Link OAM Port Configuration

Link OAM Port Configuration

Port	OAM Enabled	OAM Mode	Loopback Support	Link Monitor Support	MIB Retrieval Support	Loopback Operation
1	☐	Passive ▾	☐	☑	☐	☐
2	☐	Passive ▾	☐	☑	☐	☐
3	☐	Passive ▾	☐	☑	☐	☐
4	☐	Passive ▾	☐	☑	☐	☐
5	☐	Passive ▾	☐	☑	☐	☐
6	☐	Passive ▾	☐	☑	☐	☐
7	☐	Passive ▾	☐	☑	☐	☐
8	☐	Passive ▾	☐	☑	☐	☐
9	☐	Passive ▾	☐	☑	☐	☐
10	☐	Passive ▾	☐	☑	☐	☐
11	☐	Passive ▾	☐	☑	☐	☐
12	☐	Passive ▾	☐	☑	☐	☐
13	☐	Passive ▾	☐	☑	☐	☐
14	☐	Passive ▾	☐	☑	☐	☐
15	☐	Passive ▾	☐	☑	☐	☐
16	☐	Passive ▾	☐	☑	☐	☐
17	☐	Passive ▾	☐	☑	☐	☐
18	☐	Passive ▾	☐	☑	☐	☐
19	☐	Passive ▾	☐	☑	☐	☐
20	☐	Passive ▾	☐	☑	☐	☐
21	☐	Passive ▾	☐	☑	☐	☐
22	☐	Passive ▾	☐	☑	☐	☐
23	☐	Passive ▾	☐	☑	☐	☐
24	☐	Passive ▾	☐	☑	☐	☐
25	☐	Passive ▾	☐	☑	☐	☐
26	☐	Passive ▾	☐	☑	☐	☐
27	☐	Passive ▾	☐	☑	☐	☐
28	☐	Passive ▾	☐	☑	☐	☐
29	☐	Passive ▾	☐	☑	☐	☐

[Save] [Reset]

Parameter description:

- **Port Members :**

  The switch port number.

- **OAM Enabled :**

  Controls whether Link OAM is enabled on this switch port. Enabling Link OAM provides the network operators the ability to monitor the health of the network and quickly determine the location of failing links or fault conditions.

- **OAM Mode :**

  To scroll to select OAM mode with Passive or Active. It supports you to configure the OAM Mode as Active or Passive. The default mode is Passive.

  Passive:

  DTE's configured in Passive mode do not initiate the Discovery process. Passive DTE's react to the initiation of the Discovery process by the remote DTE. This eliminates the possibility of passive to passive links. Passive DTE's shall not send Variable Request or Loopback Control OAMPDUs.

  Active:

  DTE's configured in Active mode initiate the exchange of Information OAMPDUs as defined by the Discovery process. Once the Discovery process completes, Active DTE's are permitted to send any OAMPDU while connected to a remote OAM peer entity in Active mode. Active DTE's operate in a limited respect if the remote OAM entity is operating in Passive mode. Active devices should not respond to OAM remote loopback commands and variable requests from a Passive peer.

- **Loopback support :**

  To evoke to enable the Loopback support. Link OAM remote loopback can be used for fault localization and link performance testing. Enabling the loopback support will allow the DTE to execute the remote loopback command that helps in the fault detection..

- **Link Monitor support :**

  Controls whether the Link Monitor support is enabled for the switch port that you need to evoke which port you wants to enable the function. On enabling the Link Monitor support, the DTE supports event notification that permits the inclusion of diagnostic information. .

- **MIB Retrieval Support :**

  To evoke which port you want to enable the MIB Retrieval support function. On enabling the MIB retrieval support, the DTE supports polling of various Link OAM based MIB variables' contents. .

- **Loopback Operation :**

  To evoke to enable or disable the Loopback Operation function on the Port. If the Loopback support is enabled, enabling this field will start a loopback operation for the port.

- **Buttons:**

  Apply – Click to apply changes.

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

3-20.2 Event Config

This chapter allows the user to inspect the current Link OAM Event configurations, and change them as well. It allows you to set what kind event to trigger 802.3ah OAM monitor and management function.

Web Interface

To configure the Link event configuration in the web interface:

1. Click Configuration, 802.3ah OAM then Event config.
2. Evoke auto-refresh to update the Link Event data.
3. Set all parameters on Link event 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 3-20.2: The Link Event Configuration

Link Event Configuration for Port 1

Port 1 ⌄ Auto-refresh ☐ | Refresh | Clear

Event Name	Error Window	Error Threshold
Error Frame Event	1	0
Symbol Period Error Event	1	0
Seconds Summary Event	60	1

Apply | Reset

Parameter description:

- **Port :**

  The switch port number.

- **Event Name :**

  Name of the Link Event which is being configured.

- **Error Window :**

  Represents the window period in the order of 1 sec for the observation of various link events.

- **Error Threshold :**

  Represents the threshold value for the window period for the appropriate Link event so as to notify the peer of this error.

- **Error Frame Event :**

  The Errored Frame Event counts the number of errored frames detected during the specified period. The period is specified by a time interval (Window in order of 1 sec). This event is generated if the errored frame count is equal to or greater than the specified threshold for that period (Period Threshold). Errored frames are frames that had transmission errors as detected at the Media Access Control sublayer. Error Window for 'Error Frame Event' must be an integer value between 1-60 and its default value is '1'. Whereas Error Threshold must be between 0-0xffffffff and its default value is '0'.

- **Symbol Period Error Event :**

  The Errored Symbol Period Event counts the number of symbol errors that occurred during the specified period. The period is specified by the number of symbols that can be received in a time interval on the underlying physical layer. This event is generated if the symbol error count is equal to or greater than the specified threshold for that period. Error Window for 'Symbol Period Error Event' must be an integer value between 1-60 and its default value is '1'. Whereas Error Threshold must be between 0-0xffffffff and its default value is '0'.

- **Seconds Summary Event :**

  The Errored Frame Seconds Summary Event TLV counts the number of errored frame seconds that occurred during the specified period. The period is specified by a time interval. This event is generated if the number of errored frame seconds is equal to or greater than the specified threshold for that period. An errored frame second is a one second interval wherein at least one frame error was detected. Errored frames are frames that had transmission errors as detected at the Media Access Control sublayer. Error Window for 'Seconds Summary Event' must be an integer value between 10-900 and its default value is '60'. Whereas Error Threshold must be between 0-0xffff and its default value is '1'.

- **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 refresh and clear information by manual.

- **Buttons:**

  Apply – Click to apply changes.

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

3-20.3 Port Status

This chapter introduce you when you configure the IEEE802.3ah OAM then the switch will display the Port Status in this page. It provides Link OAM configuration operational status. The displayed field shows the active configuration status for the selected port.

Web Interface

To display the Port Status in the web interface:

1. Click Configuration, 802.3ah OAM then Port status.
2. Scroll to select which port you want to monitor the Link OAM Status.
3. Evoke auto-refresh to update the detailed Link OAM Status data.
4. Click the Refresh to update the Port Status.

.

Figure 3-20.3: The Link OAM Port status

Detailed Link OAM Status for Port 1   Port 1 ▾ Auto-refresh ☐ [Refresh]

PDU Permission	Receive only	
Discovery State	Fault state	
Remote MAC Address	------	

Local		Remote	
Mode	Passive	Mode	------
Unidirectional Operation Support	Disabled	Unidirectional Operation Support	------
Remote Loopback Support	Disabled	Remote Loopback Support	------
Link Monitoring Support	Enabled	Link Monitoring Support	------
MIB Retrieval Support	Disabled	MIB Retrieval Support	------
MTU Size	1500	MTU Size	------
Multiplexer State	Forwarding	Multiplexer State	------
Parser State	Forwarding	Parser State	------
Organizational Unique Identification	00-40-c7	Organizational Unique Identification	------
PDU Revision	0	PDU Revision	------

Parameter description:

● **PDU Permission :**

This field is available only for the Local DTE. It displays the current permission rules set for the local DTE. Possible values are "Link fault", "Receive only", "Information exchange only", "ANY".

● **Discovery State :**

The field will display the current state of the discovery process. The possible states are includes **Fault state**, **Active state**, **Passive state**, **SEND_LOCAL_REMOTE_STATE**, **SEND_LOCAL_REMOTE_ OK_STATE, SEND_ANY_STATE**.

● **Remote MAC Address :**

The field will show which device join the OAM and its MAC address.

● **Mode :**

The field will show the Mode in which the Link OAM is operating, Active or Passive.

● **Unidirectional Operation Support :**

The field will show the status of this configuration is retrieved from the PHY. This feature is not available to be configured by the user.

● **Remote Loopback Support :**

If status is enabled, DTE is capable of OAM remote loopback mode. The field will show enabled.

- **Link Monitoring Support :**

  If status is enabled, DTE supports interpreting Link Events. The field will show enabled.

- **MIB Retrieval Support :**

  If status ie enabled DTE supports sending Variable Response OAMPDUs.. The field will show enabled.

- **MTU Size :**

  It represents the largest OAMPDU, in octets, supported by the DTE. This value is compared to the remotes Maximum PDU Size and the smaller of the two is used.

- **Multiplexer State :**

  When in forwarding state, the Device is forwarding non-OAMPDUs to the lower sublayer. Incase of discarding, the device discards all the non-OAMPDU's.

- **Parser State :**

  When in forwarding state, Device is forwarding non-OAMPDUs to higher sublayer. When in loopback, Device is looping back non-OAMPDUs to the lower sublayer. When in discarding state, Device is discarding non-OAMPDUs.

- **Organizational Unique Identification :**

  24-bit Organizationally Unique Identifier of the vendor.

- **PDU Revision :**

  It indicates the current revision of the Information TLV. The value of this field shall start at zero and be incremented each time something in the Information TLV changes. Upon reception of an Information TLV from a peer, an OAM client may use this field to decide if it needs to be processed (an Information TLV that is identical to the previous Information TLV doesn't need to be parsed as nothing in it has changed).

- . **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 refresh information by manual.

3-20.4 Link Events

This chapter introduces the user to inspect the current Link OAM Link Event configurations, and change them as well. The Link OAM Link Event status relate to the currently selected stack unit, as reflected by the page header. The left pane displays the Event status for the Local OAM unit while the right pane displays the status for the Peer for the respective port.

Web Interface

To display the Link Events in the web interface:

1. Click Configuration, 802.3ah OAM then Link Events.
2. Scroll to select which port you want to monitor the Link Events.
3. Evoke auto-refresh to update the detailed Link Events data.
4. Click the Refresh to update the Link Events.

.

Figure 3-20.4: The detailed Link OAM Port status

Parameter description:

- **Port :**

  You can scroll to select which port you want to monitor detailed Link OAM events. It shows the switch port number.

- **Frame Error Event Timestamp :**

  The field shows this two-octet field indicates the time reference when the event was generated, in terms of 100 ms intervals.

- **Frame Error Event Window :**

  The field shows this two-octet field indicates the duration of the period in terms of 100 ms intervals. 1) The default value is one second. 2) The lower bound is one second. 3) The upper bound is one minute.

- **Frame Error Event threshold :**

  The field shows this four-octet field indicates the number of detected errored frames in the period is required to be equal to or greater than in order for the event to be generated. 1) The default value is one frame error. 2) The lower bound is zero frame errors. 3) The upper bound is unspecified.

- **Frame Errors :**

  The field shows this four-octet field indicates the number of detected errored frames in the period.

- **Total Frame Errors :**

  The field shows this eight-octet field indicates the sum of errored frames that have been detected since the OAM sub-layer was reset.

- **Total Frame Error Events :**

  The field shows this four-octet field indicates the number of Errored Frame Event TLVs that have been generated since the OAM sub-layer was reset.

- **Frame Period Error Event Timestamp :**

  The field shows this two-octet field indicates the time reference when the event was generated, in terms of 100 ms intervals.

- **Frame Period Error Event Window :**

  The field shows this four-octet field indicates the duration of period in terms of frames.

- **Frame Period Error Event Threshold :**

  The field shows this four-octet field indicates the number of errored frames in the period is required to be equal to or greater than in order for the event to be generated.

- **Frame Period Errors :**

  The field shows this four-octet field indicates the number of frame errors in the period.

- **Total Frame Period Errors :**

  The field shows this eight-octet field indicates the sum of frame errors that have been detected since the OAM sub-layer was reset.

- **Total Frame Period Error Events :**

  The field shows this four-octet field indicates the number of Errored Frame Period Event TLVs that have been generated since the OAM sub-layer was reset.

- **Symbol Period Error Event Timestamp :**

  The field shows this two-octet field indicates the time reference when the event was generated, in terms of 100 ms intervals.

- **Symbol Period Error Event Window :**

  The field shows this eight-octet field indicates the number of symbols in the period.

- **Symbol Period Error Event Threshold :**

  The field shows this eight-octet field indicates the number of errored symbols in the period is required to be equal to or greater than in order for the event to be generated.

- **Symbol Period Errors :**

  The field shows this eight-octet field indicates the number of symbol errors in the period.

- **Symbol frame Period Errors :**

  The field shows this eight-octet field indicates the sum of symbol errors since the OAM sub-layer was reset

- **Event Seconds Summary Time Stamp :**

  The field shows this two-octet field indicates the time reference when the event was generated, in terms of 100 ms intervals, encoded as a 16-bit unsigned integer.

- **Event Seconds Summary Window :**

  The field shows this two-octet field indicates the duration of the period in terms of 100 ms intervals, encoded as a 16-bit unsigned integer.

- **Event Seconds Summary Threshold :**

  The field shows this two-octet field indicates the number of errored frame seconds in the period is required to be equal to or greater than in order for the event to be generated, encoded as a 16-bit unsigned integer.

.

- **Event Seconds Summary Events :**

  The field shows this two-octet field indicates the number of errored frame seconds in the period, encoded as a 16-bit unsigned integer.

- **Event Seconds Summary Error Total :**

  The field shows this four-octet field indicates the sum of errored frame seconds that have been detected since the OAM sub-layer was reset.

- **Event Seconds Summary Event Total :**

  The field shows This four-octet field indicates the number of Errored Frame Seconds Summary Event TLVs that have been generated since the OAM sub-layer was reset, encoded as a 32bit unsigned integer..

- **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 refresh or clear information by manual.

3-20.5 Statistics

This chapter introduces how to provide detailed OAM traffic statistics for a specific switch port. Use the port select box to select which switch port details to display. The displayed counters represent the total number of OAM frames received and transmitted for the selected port. Discontinuities of these counters can occur at re-initialization of the management system.

Web Interface

To display the Statistics in the web interface:

1. Click Configuration, 802.3ah OAM then Statistics.
2. Scroll to select which port you want to monitor the Statistics.
3. Evoke auto-refresh to update the detailed Link Events data.
4. Click the Refresh to update the Link OAM Port statistics.

.

Figure 3-20.5: The detailed Link OAM Port Statistics

Detailed Link OAM Statistics for Port 1   Port 1 ⌄ Auto-refresh ☐ Refresh Clear

Receive Total		Transmit Total	
Rx OAM Information PDU's	0	Tx OAM Information PDU's	0
Rx Unique Error Event Notification	0	Tx Unique Error Event Notification	0
Rx Duplicate Error Event Notification	0	Tx Duplicate Error Event Notification	0
Rx Loopback Control	0	Tx Loopback Control	0
Rx Variable Request	0	Tx Variable Request	0
Rx Variable Response	0	Tx Variable Response	0
Rx Org Specific PDU's	0	Tx Org Specific PDU's	0
Rx Unsupported Codes	0	Tx Unsupported Codes	0
Rx Link Fault PDU's	0	Tx Link Fault PDU's	0
Rx Dying Gasp	0	Tx Dying Gasp	0
Rx Critical Event PDU's	0	Tx Critical Event PDU's	0

Parameter description:

- **Port :**

  You can scroll to select which port you want to monitor detailed Link OAM events. It shows the switch port number.

- **Rx and Tx OAM Information PDU's :**

  The number of received and transmitted OAM Information PDU's.Discontinuities of this counter can occur at re-initialization of the management system.

- **Rx and Tx Unique Error Event Notification :**

  A count of the number of unique Event OAMPDUs received and transmitted on this interface. Event Notifications may be sent in duplicate to increase the probability of successfully being received, given the possibility that a frame may be lost in transit. Duplicate Event Notification transmissions are counted by Duplicate Event Notification counters for Tx and Rx respectively. A unique Event Notification OAMPDU is indicated as an Event Notification OAMPDU with a Sequence Number field that is distinct from the previously transmitted Event Notification OAMPDU Sequence Number.

- **Rx and Tx Duplicate Error Event Notification :**

  A count of the number of duplicate Event OAMPDUs received and transmitted on this interface. Event Notification OAMPDUs may be sent in duplicate to increase the probability of successfully being received, given the possibility that a frame may be lost in transit. A duplicate Event Notification OAMPDU is indicated as an Event Notification OAMPDU with a Sequence Number field that is identical to the previously transmitted Event Notification OAMPDU Sequence Number.

- **Rx and Tx Loopback Control :**

  A count of the number of Loopback Control OAMPDUs received and transmitted on this interface.

- **Rx and Tx Variable Request :**

  A count of the number of Variable Request OAMPDUs received and transmitted on this interface.

- **Rx and Tx Variable Response :**

  A count of the number of Variable Response OAMPDUs received and transmitted on this interface.

- **Rx and Tx Org Specific PDU's :**

  A count of the number of Organization Specific OAMPDUs transmitted on this interface.

- **Rx and Tx Unsupported Codes :**

  A count of the number of OAMPDUs transmitted on this interface with an unsupported op-code.

- **Rx and Tx Link fault PDU's :**

  A count of the number of Link fault PDU's received and transmitted on this interface.

- **Rx and Tx Dying Gasp :**

  A count of the number of Dying Gasp events received and transmitted on this interface.

- **Rx and Tx Critical Event PDU's :**

  A count of the number of Critical event PDU's received and transmitted on this interface.

- **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 refresh or clear information by manual.

3-21 Ethernet OAM

The chapter describes the Ethernet OAM configuration. Before you configure the Ethernet OAM then you need to understand what MEP (Maintenance Entity Point) is first. The MEP means the Points at the edge of the domain, define the boundary for the domain. A MEP sends and receives CFM frames through the relay function, drops all CFM frames of its level or lower that come from the wire side.

Web Interface

To configure the Ethernet OAM in the web interface:

1. Click Configuration, Ethernet OAM
2. Click Add new MEP then you can create new MEP on the switch.
3. Assign each parameter to add new MEP.
4. If you want to cancel the setting then you need to click the Reset button.
   It will revert to previously saved values
5. Click Refresh then switch will update the MEP table by manually.

Figure 3-21: The Maintenance Entity Point Configuration.

Parameter description:

- **Delete:**

  This box is used to mark a MEP for deletion in next Save operation.

- **Instance :**

  The ID of the MEP. Click on the ID of a MEP to enter the configuration page.

- **Domain:**

  Port: This is a MEP in the Port Domain. 'Flow Instance' is a Port.

  Evc: This is a MEP in the EVC Domain. 'Flow Instance' is a EVC

- **Mode :**

  In the field you can scroll to select "Mep" or " Mip".

  MEP: This is a Maintenance Entity End Point.

  MIP: This is a Maintenance Entity Intermediate Point.

- **Direction :**

You can scroll to select the direction with "Ingress" or "Egress".

Ingress: This is a Ingress (down) MEP - monitoring ingress traffic on 'Residence Port'.

Egress: This is a Egress (up) MEP - monitoring egress traffic on 'Residence Port'.

- **Residence Port :**

  The port where MEP is monitoring - see 'Direction'. You need to assign a port to monitor the MEP status.

- **Level :**

  The MEG level of this MEP. Shared MEGs are the case where there is no encapsulation of the ETH frames differently between subscriber's frames and SP's frames. Hence they share the pool of MEG levels, where the customer can use 5 through 7 and the SP and operate use the rest. If there is a different encapsulation, then each can use all 8 levels, hence they are independent.

- **Flow instance :**

  The MEP is related to this flow - See 'Domain'. MEP monitors the flow by sending periodic CCMs for that flow.

- **Tagged VID :**

  Port MEP: An outer C/S-tag (depending on VLAN Port Type) is added with this VID.

  Entering '0' means no TAG added.

- **This MAC :**

  The field will display the MEP device MAC address. Switch will detect the MEP device MAC address. The MAC of this MEP - can be used by other MEP when unicast is selected (Info only).

- **Alarm :**

  The field will display the MEP alarm data. There is an active alarm on the MEP. .

- **Buttons:**

  Add new MEP - Click to add a new MEP entry.

  Apply – Click to apply 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 refresh information by manual.

3-22 EPS

The chapter describes the Ethernet Protection Switching (EPS). The switch supports the Ethernet (Linear) Protection Switch instances are configured here.

Web Interface

To configure the EPS in the web interface:

1. Click Configuration, EPS
2. Click Add new EPS then you can create new EPS entry on the switch.
3. Assign each parameter to add new EPS.
4. If you want to cancel the setting then you need to click the Reset button.
   It will revert to previously saved values
5. Click Refresh then switch will update the EPS table by manually.

Figure 3-22: The EPS Configuration.

Parameter description:

- **Delete:**

  This box is used to mark a EPS for deletion in next Save operation.

- **EPS ID:**

  The ID of the EPS. Click on the ID of an EPS to enter the configuration page.

- **Domain:**

  You can scroll to select the domain with "Port", " Esp" . "Evc" and "Mpls"

  Port: This will create an EPS in the Port Domain. 'W/P Flow' is a Port.

  Esp: Future use **(needs to upgrade FW then will support it)**

  Evc: This will create an EPS in the EVC Domain. 'W/P Flow' is an EVC.

  Mpls: Future use **(needs to upgrade FW then will support it)**

- **Architecture:**

  The field you can scroll to select architecture of EPS as"1+1" or "1:1".

  1+1 : This will create a 1+1 EPS.

XGS3600 Series User's Guide

252

1:1 : This will create a 1:1 EPS.

- **W flow:**

  The field you need to assign the working flow for the EPS. - See 'Domain'.

- **P flow:**

  The field you need to assign the Protecting flow for the EPS. - See 'Domain'.

- **W SF MEP:**

  The field you need to assign the working Signal Fail reporting MEP.

- **P SF MEP:**

  The field you need to assign the protecting Signal Fail reporting MEP.

- **APS MEP:**

  The field you need to assign the APS PDU handling MEP.

- **Alarm:**

  There is an active alarm on the EPS. When you complete the setting then switch will show the alarm status.

- **Buttons:**

  Add new EPS - Click to add a new EPS entry.

  Apply – Click to apply 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 refresh information by manual.

3-23 ERPS

The chapter describes the Ethernet Ring Protection Switching (ERPS). It is an effort at ITU-T under G.8032 Recommendation to provide sub-50ms protection and recovery switching for Ethernet traffic in a ring topology and at the same time ensuring that there are no loops formed at the Ethernet layer. The switch supports the Ethernet Ring Protection Switch instances are configured here.

Web Interface

To configure the ERPS in the web interface:

1. Click Configuration, ERPS
2. Click Add new ERPS then you can create new ERPS entry on the switch.
3. Assign each parameter to add new ERPS.
4. If you want to cancel the setting then you need to click the Reset button.
   It will revert to previously saved values
5. Click Refresh then switch will update the ERPS table by manually.

Figure 3-23: The ERPS Configuration.

Parameter description:

- **Delete:**

    This box is used to mark an ERPS for deletion in next Save operation.

- **ERPS ID (Protection group ID) :**

    The ID of the created Protection group. Click on the ID of an Protection group to enter the configuration page. .

- **Port 0 (E Port):**

    This will create an East port of the switch in the ring.

- **Port 1 (W Port):**

    This will create a West port of the switch in the Ring. As interconnected sub-ring will have only one ring port, "W port" is configured as "0" for interconnected sub-ring. "0" in this field indicates that no west port is associated with this instance.

- **Port 0 SF MEP (E SF MEP):**

    The field you need to assign the East Signal Fail reporting MEP.

- **Port 1 SF MEP (W SF MEP):**

The West Signal Fail reporting MEP. As only one SF MEP is associated with interconnected sub-ring without virtual channel, it is configured as "0" for such ring instances. "0" in this field indicates that no west SF MEP is associated with this instance.

- **Port 0 APS MEP (E APS MEP):**

  The field you need to assign the East APS PDU handling MEP.

- **Port 1 APS MEP (W APS MEP):**

  The West APS PDU handling MEP. As only one APS MEP is associated with interconnected sub-ring without virtual channel, it is configured as "0" for such ring instances. "0" in this field indicates that no west APS MEP is associated with this instance.

- **Ring Type:**

  To scroll to select the type of Protection ring. It can be either **major ring** or **sub-ring**. .

- **Interconnected Node:**

  Interconnected Node indicates that the ring instance is interconnected. Click on the checkbox to configure this. "Yes" indicates it is an interconnected node for this instance. "No" indicates that the configured instance is not interconnected.

- **Virtual Channel:**

  Sub-rings can either have virtual channel or not on the interconnected node. This is configured using "Virtual Channel" checkbox. "Yes" indicates it is a sub-ring with virtual channel. "No" indicates, sub-ring doesn't have virtual channel.

- **Major Ring ID:**

  Major ring group ID for the interconnected sub-ring. It is used to send topology change updates on major ring. If ring is major, this value is same as the protection group ID of this ring.

- **Alarm:**

  There is an active alarm on the ERPS. When you complete the setting then switch will show the alarm status.

- **Buttons:**

  Add new ERPS - Click to add a new ERPS entry.

  Apply – Click to apply 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 refresh information by manual.

Security

This chapter describes all of the switch security configuration tasks to enhance the security of local network including IP Source Guard, ARP Inspection, DHCP Snooping, AAA, and etc..

4-1 IP Source Guard

IP Source Guard is a secure feature used to restrict IP traffic on DHCP snooping untrusted ports by filtering traffic based on the DHCP Snooping Table or manually configured IP Source Bindings. It helps prevent IP spoofing attacks when a host tries to spoof and use the IP address of another host.

The section describes to configure the IP Source Guard detail parameters of the switch. You could use the IP Source Guard configure to enable or disable with the Port of the switch.

4-1.1 Configuration

This section describes how to configure IP Source Guard setting including：
Mode (Enabled and Disabled)
Maximum Dynamic Clients (0, 1, 2, Unlimited)

Web Interface

To configure an IP Source Guard Configuration in the web interface:
1. Select "Enabled" in the Mode of IP Source Guard Configuration.
2. Select "Enabled" of the specific port in the Mode of Port Mode Configuration.
3. Select Maximum Dynamic Clients (0, 1, 2, Unlimited) of the specific port in the Mode of Port Mode Configuration.
4. Click Apply.

Figure 4-1.1: The IP Source Guard Configuration

IP Source Guard Configuration

Mode [Disabled ▼]

[Translate dynamic to static]

Port Mode Configuration

Port	Mode	Max Dynamic Clients
*	<> ▼	<> ▼
1	Disabled ▼	Unlimited ▼
2	Disabled ▼	Unlimited ▼
3	Disabled ▼	Unlimited ▼
4	Disabled ▼	Unlimited ▼
5	Disabled ▼	Unlimited ▼
6	Disabled ▼	Unlimited ▼
7	Disabled ▼	Unlimited ▼
8	Disabled ▼	Unlimited ▼
9	Disabled ▼	Unlimited ▼
10	Disabled ▼	Unlimited ▼
11	Disabled ▼	Unlimited ▼
12	Disabled ▼	Unlimited ▼
13	Disabled ▼	Unlimited ▼
14	Disabled ▼	Unlimited ▼
15	Disabled ▼	Unlimited ▼
16	Disabled ▼	Unlimited ▼
17	Disabled ▼	Unlimited ▼
18	Disabled ▼	Unlimited ▼
19	Disabled ▼	Unlimited ▼
20	Disabled ▼	Unlimited ▼
21	Disabled ▼	Unlimited ▼
22	Disabled ▼	Unlimited ▼
23	Disabled ▼	Unlimited ▼
24	Disabled ▼	Unlimited ▼
25	Disabled ▼	Unlimited ▼
26	Disabled ▼	Unlimited ▼
27	Disabled ▼	Unlimited ▼
28	Disabled ▼	Unlimited ▼

[Apply] [Reset]

Parameter description:

- **Mode of IP Source Guard Configuration :**

  Enable the Global IP Source Guard or disable the Global IP Source Guard. All configured ACEs will be lost when the mode is enabled.

- **Port Mode Configuration :**

  Specify IP Source Guard is enabled on which ports. Only when both Global Mode and Port Mode on a given port are enabled, IP Source Guard is enabled on this given port.

- **Max Dynamic Clients :**

Specify the maximum number of dynamic clients that can be learned on given port. This value can be 0, 1, 2 or unlimited. If the port mode is enabled and the value of max dynamic client is equal to 0, it means only allow the IP packets forwarding that are matched in static entries on the specific port.

- **Buttons:**

    Apply – Click to apply changes.

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

4-1.2 Static Table

The section describes to configure the Static IP Source Guard Table parameters of the switch. You could use the Static IP Source Guard Table configure to manage the entries.

Web Interface

To configure a Static IP Source Guard Table Configuration in the web interface:
1. Click "Add new entry".
2. Specify the Port, VLAN ID, IP Address, and MAC address in the entry.
3. Click Apply.

Figure 4-1.2: The Static IP Source Guard Table

Static IP Source Guard Table

Delete	Port	VLAN ID	IP Address	IP Mask
Delete	1 ▼			

Add new entry

Apply   Reset

Parameter description:

- **Delete :**

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

- **Port :**

  The logical port for the settings.

- **VLAN ID :**

  The VLAN ID for the settings.

- **IP Address :**

  Allowed Source IP address.

- **IP Mask :**

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

- **Adding new entry :**

  Click "Adding new entry" to add a new entry to the Static IP Source Guard table. Specify the Port, VLAN ID, IP address, and IP Mask for 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.

4-1.3 Dynamic Table

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

Each page shows up to 99 entries from the Dynamic IP Source Guard table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the Dynamic IP Source Guard Table. The "Start from port address", "VLAN" and "IP address" input fields allow the user to select the starting point in the Dynamic IP Source Guard Table. Clicking the "Refresh" button will update the displayed table starting from that or the closest next Dynamic IP Source Guard Table match. In addition, the two input fields will - upon a "Refresh" button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address. The ">>" will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the "|<<" button to start over.

Web Interface

To configure a Dynamic IP Source Guard Table Configuration in the web interface:
1. Specify the Start from port, VLAN ID, IP Address, and entire per page.
2. Checked "Auto-refresh".

Figure 4-1.3: The Dynamic Table

Parameter description:

- **Port :**

    Switch Port Number for which the entries are displayed.

- **VLAN ID :**

    VLAN-ID in which the IP traffic is permitted.

- **IP Address :**

    User IP address of the entry.

- **MAC Address :**

    Source MAC address.

- **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 Dynamic IP Source Guard Table by manual, others for next/up page or entry.

4-2 ARP Inspection

The section describes to configure the ARP Inspection parameters of the switch. You could use the ARP Inspection configure to manage the ARP table.

4-2.1 Configuration

This section describes how to configure ARP Inspection setting including：
Mode (Enabled and Disabled)
Port (Enabled and Disabled)

Web Interface

To configure an ARP Inspection Configuration in the web interface:
1. Select "Enabled" in the Mode of ARP Inspection Configuration.
2. Select "Enabled" of the specific port in the Mode of Port Mode Configuration.
3. Click Apply.

Figure 4-2.1: The ARP Inspection Configuration

ARP Inspection Configuration

Mode	Disabled ∨

| Translate dynamic to static |

Port Mode Configuration

Port	Mode
*	◇ ∨
1	Disabled ∨
2	Disabled ∨
26	Disabled ∨
27	Disabled ∨
28	Disabled ∨

| Apply | Reset |

Parameter description:

- **Mode of ARP Inspection Configuration :**

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

- **Port Mode Configuration :**

  Specify ARP Inspection is enabled on which ports. Only when both Global Mode and Port Mode on a given port are enabled, ARP Inspection is enabled on this given port.

- **Buttons:**

  Apply – Click to apply changes.

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

  Translate dynamic to static-: Click to translate all dynamic entries to static entries.

4-2.2 Static Table

The section describes to configure the Static ARP Inspection Table parameters of the switch. You could use the Static ARP Inspection Table configure to manage the ARP entries.

Web Interface

To configure a Static ARP Inspection Table Configuration in the web interface:
1. Click "Add new entry".
2. Specify the Port, VLAN ID, IP Address, and MAC address in the entry.
3. Click Apply.

Figure 4-2.2: The Static ARP Inspection Table

Parameter description:

- **Delete :**

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

- **Port :**

  The logical port for the settings.

- **VLAN ID :**

  The VLAN ID for the settings.

- **MAC Address :**

  Allowed Source MAC address in ARP request packets.

- **IP Address :**

  Allowed Source IP address in ARP request packets.

- **Adding new entry :**

  Click "Adding new entry" to add a new entry to the Static ARP Inspection table. Specify the Port, VLAN ID, MAC address, and IP address for 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.

4-2.3 Dynamic Table

The section describes to configure the Dynamic ARP Inspection Table parameters of the switch. The Dynamic ARP Inspection Table contains up to 1024 entries, and is sorted first by port, then by VLAN ID, then by MAC address, and then by IP address.

Web Interface

To configure a Dynamic ARP Inspection Table Configuration in the web interface:
1. Specify the Start from port, VLAN ID, MAC Address, IP Address, and entire per page.
2. Checked "Auto-refresh".

.

Figure 4-2.3: The Dynamic ARP Inspection Table

Parameter description:

- **Port :**

  Switch Port Number for which the entries are displayed.

- **VLAN ID :**

  VLAN-ID in which the ARP traffic is permitted.

- **MAC Address :**

  User MAC address of the entry.

- **IP Address :**

  User IP address of the entry.

- **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 Dynamic ARP Inspection Table by manual, others for next/up page or entry

4-3 DHCP Snooping

The section describes to configure the DHCP Snooping parameters of the switch. The DHCP Snooping can prevent attackers from adding their own DHCP servers to the network.

4-3.1 Configuration

This section describes how to configure DHCP Snooping setting including：
Snooping Mode (Enabled and Disabled)
Port Mode Configuration (Trusted, Untrusted)

Web Interface

To configure a DHCP Snooping in the web interface:

1. Select "Enabled" in the Mode of DHCP Snooping Configuration.
2. Select "Trusted" of the specific port in the Mode of Port Mode Configuration.
3. Click Apply.

Figure 4-3.1: The DHCP Snooping Configuration

Parameter description:

- **Snooping Mode：**

   Indicate the DHCP snooping mode operation. Possible modes are:

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

   Disabled: Disable DHCP snooping mode operation.

- **Port Mode：**

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

   Trusted: Configures the port as trusted source of the DHCP messages.

Untrusted: Configure the port as untrusted source of the DHCP messages.

- **Buttons:**

  Apply – Click to apply changes.

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

4-3.2 Statistics

The section describes to show the DHCP Snooping Statistics information of the switch. The statistics show only packet counters when DHCP snooping mode is enabled and relay mode is disabled. And it doesn't count the DHCP packets for DHCP client.

Web Interface

To configure a DHCP Snooping Statistics Configuration in the web interface:
1. Specify the Port which you want to monitor.
2. Check "Auto-refresh".

Figure 4-3.2: The DHCP Snooping Port Statistics

Parameter description:

- **Rx and Tx Discover :**

  The number of discover (option 53 with value 1) packets received and transmitted.

- **Rx and Tx Offer :**

  The number of offer (option 53 with value 2) packets received and transmitted.

- **Rx and Tx Request :**

  The number of request (option 53 with value 3) packets received and transmitted.

- **Rx and Tx Decline :**

  The number of decline (option 53 with value 4) packets received and transmitted.

- **Rx and Tx ACK :**

  The number of ACK (option 53 with value 5) packets received and transmitted.

- **Rx and Tx NAK :**

  The number of NAK (option 53 with value 6) packets received and transmitted.

- **Rx and Tx Release :**

  The number of release (option 53 with value 7) packets received and transmitted.

- **Rx and Tx Inform :**

The number of inform (option 53 with value 8) packets received and transmitted.

- **Rx and Tx Lease Query :**

  The number of lease query (option 53 with value 10) packets received and transmitted.

- **Rx and Tx Lease Unassigned :**

  The number of lease unassigned (option 53 with value 11) packets received and transmitted.

- **Rx and Tx Lease Unknown :**

  The number of lease unknown (option 53 with value 12) packets received and transmitted.

- **Rx and Tx Lease Active :**

  The number of lease active (option 53 with value 13) packets received and transmitted.

- **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 DHCP Snooping Port Statistics by manual, others for clear to clean up the entries.

4-4 DHCP Relay

The section describes how to forward DHCP requests to another specific DHCP servers via DHCP relay. The DHCP servers may be on another network.

4-4.1 Configuration

Configure DHCP Relay on this page.

Web Interface

To configure a DHCP Relay in the web interface:
1. Select "Enabled" in the Relay Mode of DHCP Relay Configuration.
2. Specify Relay Server IP address.
3. Select "Enabled" in the Relay Information Mode of DHCP Relay Configuration.
4. Specify Relay (Replace, Keep and Drop) in the Relay Information Mode of DHCP Relay Configuration.
5. Click Apply.

Figure 4-4.1: The DHCP Relay Statistics

Parameter description:

- **Relay Active :**

    Indicate the DHCP relay mode operation. Possible modes are:

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

    Disabled: Disable DHCP relay mode operation.

- **Remote DHCP Server :**

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

- **VLAN ID :**

    Enter the source VLAN ID for which the DHCP Relay settings apply. Enter 0 if you want to configure the default settings for all VLAN.

- **Option82 Profile :**

DHCP Option82 Profile.

- **Buttons:**

  Apply – Click to apply changes.

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

4-4.2 Profile

Configure DHCP Option82 Profile on this page.

Web Interface

To configure a DHCP Relay in the web interface:
1. Click Configuration, DHCP Relay, Profile
2. Scroll to select the Vendor-specific Information Policy and Option Mode
3. Specify Profile Name, Info
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 4-4.2: The DHCP Relay Statistics

Parameter description:

- **Profile Name :**

    DHCP Option82 Profile. 0 - 23 characters normal ASCII Types.

- **Vendor-specific Information Policy :**

    Indicate the DHCP relay information option policy. When DHCP Relay Agent Information mode operation is enabled, if agent receives a DHCP message that already contains relay agent information it will enforce the policy. And it only works under DHCP if Relay Agent Information operation mode is enabled. Possible policies are:

    Replace: Replace the original relay information when a DHCP message that already contains it is received.

    Keep: Keep the original relay information when a DHCP message that already contains it is received.

    Drop: Drop the packet when a DHCP message that already contains relay information is received.

- **Option Mode :**

    Option82 sub-option. Possible option mode are:

    Private: [0x01][len][slot][port][vid-2 bytes][string 0-23 char]. [0x02][len][Clent MAC-6 bytes]

    Option82: [0x01][len][0-23 char][delimiter][eth][delimiter][slot][delimiter][port][delimiter][vlan]. [0x02][len -Max :63][Port desc 47][delimiter][Port Tel 32 char]

- **Info (Circuit ID) :**

    0 - 23 characters normal ASCII Types.

- **Hostname :**

  Option Mode must be Option82.

  Possible modes are:

  Enabled: Add Hostname Information, if Hostname is not configured, add IP Information.

  Disabled: Add Info(Circuit ID) Information.

- **Slot-ID :**

  Option Mode must be Option82.

  Possible modes are:

  Enabled: Add Slot Information, Slot ID can select 0 or 1, Default:1.

  Disabled: Remove Slot Information.

- **Port Number :**

  Option Mode must be Option82.

  Possible modes are:

  Enabled: Add Port Number Information.

  Disabled: Remove Port Number Information.

- **VLAN :**

  Option Mode must be Option82.

  Possible modes are:

  Enabled: Add VLAN Information.

  Disabled: Remove VLAN Information.

- **Delimiter :**

  Option Mode must be Option82. Possible Delimiter are:

  #

  ;

  .

  ,

  /

  space

- **Index :**

  This field displays the index number of the entry.

- **Buttons:**

  Apply – Click to apply changes.

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

4-4.3 Statistics

The section describes to show the DHCP Relay Statistics information of the switch. The statistics show both of Server and Client packet counters when DHCP Relay mode is enabled.

Web Interface

To configure a DHCP Snooping Statistics Configuration in the web interface:
1. Checked "Auto-refresh".

Figure 4-4.3: The DHCP Relay Statistics

Parameter description:

- **Transmit to Server :**

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

- **Transmit Error :**

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

- **Receive from Server :**

  The number of packets received from server.

- **Receive Missing Agent Option :**

  The number of packets received without agent information options.

- **Receive Missing Circuit ID :**

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

- **Receive Missing Remote ID :**

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

- **Receive Bad Circuit ID :**

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

- **Receive Bad Remote ID :**

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

Client Statistics

- **Transmit to Client :**

  The number of relayed packets from server to client.

- **Transmit Error :**

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

- **Receive from Client :**

    The number of received packets from server.

- **Receive Agent Option :**

    The number of received packets with relay agent information option.

- **Replace Agent Option :**

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

- **Keep Agent Option :**

    The number of packets whose relay agent information was retained.

- **Drop Agent Option :**

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

- **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 DHCP Relay Statistics by manual, others for clear to clean up the entries.

4-5 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.

4-5.1 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 Netwrok Access Server in the web interface:
1. Select "Enabled" in the Mode of Netwrok 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 Peroid (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 Apply.

Figure 4-5.1: The Network Access Server Configuration

Network Access Server Configuration

System Configuration

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

Port Configuration

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

[Apply] [Reset]

Parameter description:

- **Mode :**

  Indicate if NAS is globally enabled or disabled on the switch stack. 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 :**

  Determine 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 :**

Determine 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.

- **RADIUS-Assigned QoS Enabled :**

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

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

- **RADIUS-Assigned VLAN Enabled :**

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

  The "RADIUS-Assigned VLAN Enabled" checkbox provides a quick way to globally enable/disable RADIUS-server assigned VLAN functionality. When checked, the individual

ports' ditto setting determine whether RADIUS-assigned VLAN is enabled on that port. When unchecked, RADIUS-server assigned VLAN is disabled on all ports.

- **Guest VLAN Enabled :**

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

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

- **Guest VLAN ID :**

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

  Valid values are in the range [1; 4094].

- **Max. Reauth. Count :**

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

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

- **Allow Guest VLAN if EAPOL Seen :**

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

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

- **Port Configuration :**

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

- **Port :**

  The port number for which the configuration below applies.

- **Admin State :**

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

- **Force Authorized :**

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

- **Force Unauthorized :**

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

- **Port-based 802.1X :**

  In the 802.1X-world, the user is called the supplicant, the switch is the authenticator, and the RADIUS server is the authentication server. The authenticator acts as the man-in-the-middle, forwarding requests and responses between the supplicant and the authentication server. Frames sent between the supplicant and the switch is special 802.1X frames, known as EAPOL (EAP Over LANs) frames. EAPOL frames encapsulate EAP PDUs (RFC3748). Frames sent between the switch and the RADIUS server is RADIUS packets. RADIUS packets also encapsulate EAP PDUs together with other attributes like the switch's IP address, name, and the supplicant's port number on the switch. EAP is very

flexible, in that it allows for different authentication methods, like MD5-Challenge, PEAP, and TLS. The important thing is that the authenticator (the switch) doesn't need to know which authentication method the supplicant and the authentication server are using, or how many information exchange frames are needed for a particular method. The switch simply encapsulates the EAP part of the frame into the relevant type (EAPOL or RADIUS) and forwards it.

When authentication is complete, the RADIUS server sends a special packet containing a success or failure indication. Besides forwarding this decision to the supplicant, the switch uses it to open up or block traffic on the switch port connected to the supplicant

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

- **Single 802.1X :**

  In port-based 802.1X authentication, once a supplicant is successfully authenticated on a port, the whole port is opened for network traffic. This allows other clients connected to the port (for instance through a hub) to piggy-back on the successfully authenticated client and get network access even though they really aren't authenticated. To overcome this security breach, use the Single 802.1X variant. Single 802.1X is really not an IEEE standard, but features many of the same characteristics as does port-based 802.1X. In Single 802.1X, at most one supplicant can get authenticated on the port at a time. Normal EAPOL frames are used in the communication between the supplicant and the switch. If more than one supplicant is connected to a port, the one that comes first when the port's link comes up will be the first one considered. If that supplicant doesn't provide valid credentials within a certain amount of time, another supplicant will get a chance. Once a supplicant is successfully authenticated, only that supplicant will be allowed access. This is the most secure of all the supported modes. In this mode, the Port Security module is used to secure a supplicant's MAC address once successfully authenticated.

- **Multi 802.1X :**

  In port-based 802.1X authentication, once a supplicant is successfully authenticated on a port, the whole port is opened for network traffic. This allows other clients connected to the port (for instance through a hub) to piggy-back on the successfully authenticated client and get network access even though they really aren't authenticated. To overcome this security breach, use the Multi 802.1X variant.

  Multi 802.1X is really not an IEEE standard, but features many of the same characteristics as does port-based 802.1X. Multi 802.1X is - like Single 802.1X - not an IEEE standard, but a variant that features many of the same characteristics. In Multi 802.1X, one or more supplicants can get authenticated on the same port at the same time. Each supplicant is authenticated individually and secured in the MAC table using the Port Security module.

  In Multi 802.1X it is not possible to use the multicast BPDU MAC address as destination MAC address for EAPOL frames sent from the switch towards the supplicant, since that would cause all supplicants attached to the port to reply to requests sent from the switch.

Instead, the switch uses the supplicant's MAC address, which is obtained from the first EAPOL Start or EAPOL Response Identity frame sent by the supplicant. An exception to this is when no supplicants are attached. In this case, the switch sends EAPOL Request Identity frames using the BPDU multicast MAC address as destination - to wake up any supplicants that might be on the port.

The maximum number of supplicants that can be attached to a port can be limited using the Port Security Limit Control functionality.

- **MAC-based Auth.:**

  Unlike port-based 802.1X, MAC-based authentication is not a standard, but merely a best-practices method adopted by the industry. In MAC-based authentication, users are called clients, and the switch acts as the supplicant on behalf of clients. The initial frame (any kind of frame) sent by a client is snooped by the switch, which in turn uses the client's MAC address as both username and password in the subsequent EAP exchange with the RADIUS server. The 6-byte MAC address is converted to a string on the following form "xx-xx-xx-xx-xx-xx", that is, a dash (-) is used as separator between the lower-cased hexadecimal digits. The switch only supports the MD5-Challenge authentication method, so the RADIUS server must be configured accordingly.

  When authentication is complete, the RADIUS server sends a success or failure indication, which in turn causes the switch to open up or block traffic for that particular client, using the Port Security module. Only then will frames from the client be forwarded on the switch. There are no EAPOL frames involved in this authentication, and therefore, MAC-based Authentication has nothing to do with the 802.1X standard.

  The advantage of MAC-based authentication over port-based 802.1X is that several clients can be connected to the same port (e.g. through a 3rd party switch or a hub) and still require individual authentication, and that the clients don't need special supplicant software to authenticate. The advantage of MAC-based authentication over 802.1X-based authentication is that the clients don't need special supplicant software to authenticate. The disadvantage is that MAC addresses can be spoofed by malicious users - equipment whose MAC address is a valid RADIUS user can be used by anyone. Also, only the MD5-Challenge method is supported. The maximum number of clients that can be attached to a port can be limited using the Port Security Limit Control functionality.

- **RADIUS-Assigned QoS Enabled :**

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

  This option is only available for single-client modes, i.e.

  - **Port-based 802.1X**

  - **Single 802.1X**

  RADIUS attributes used in identifying a QoS Class:

  Refer to the written documentation for a description of the RADIUS attributes needed in order to successfully identify a QoS Class. The User-Priority-Table attribute defined in RFC4675 forms the basis for identifying the QoS Class in an Access-Accept packet.

  Only the first occurrence of the attribute in the packet will be considered, and to be valid, it must follow this rule:

  - All 8 octets in the attribute's value must be identical and consist of ASCII characters in the range '0' - '3', which translates into the desired QoS Class in the range [0; 3].

- **RADIUS-Assigned VLAN Enabled :**

  When RADIUS-Assigned VLAN is both globally enabled and enabled (checked) for a given port, the switch reacts to VLAN ID information carried in the RADIUS Access-Accept packet transmitted by the RADIUS server when a supplicant is successfully authenticated.

If present and valid, the port's Port VLAN ID will be changed to this VLAN ID, the port will be set to be a member of that VLAN ID, and the port will be forced into VLAN unaware mode. Once assigned, all traffic arriving on the port will be classified and switched on the RADIUS-assigned VLAN ID.

If (re-)authentication fails or the RADIUS Access-Accept packet no longer carries a VLAN ID or it's invalid, or the supplicant is otherwise no longer present on the port, the port's VLAN ID is immediately reverted to the original VLAN ID (which may be changed by the administrator in the meanwhile without affecting the RADIUS-assigned).

This option is only available for single-client modes, i.e.

• **Port-based 802.1X**

• **Single 802.1X**

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

RADIUS attributes used in identifying a VLAN ID:

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

 • The Tunnel-Medium-Type, Tunnel-Type, and Tunnel-Private-Group-ID attributes must all be present at least once in the Access-Accept packet.

 • The switch looks for the first set of these attributes that have the same Tag value and fulfil the following requirements (if Tag == 0 is used, the Tunnel-Private-Group-ID does not need to include a Tag):

   - Value of Tunnel-Medium-Type must be set to "IEEE-802" (ordinal 6).

   - Value of Tunnel-Type must be set to "VLAN" (ordinal 13).

   - Value of Tunnel-Private-Group-ID must be a string of ASCII chars in the range '0' - '9', which is interpreted as a decimal string representing the VLAN ID. Leading '0's are discarded. The final value must be in the range [1; 4095].

● **Guest VLAN Enabled :**

When Guest VLAN is both globally enabled and enabled (checked) for a given port, the switch considers moving the port into the Guest VLAN according to the rules outlined below.

This option is only available for EAPOL-based modes, i.e.:

• **Port-based 802.1X**

• **Single 802.1X**

• **Multi 802.1X**

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

Guest VLAN Operation:

When a Guest VLAN enabled port's link comes up, the switch starts transmitting EAPOL Request Identity frames. If the number of transmissions of such frames exceeds Max. Reauth. Count and no EAPOL frames have been received in the meanwhile; the switch considers entering the Guest VLAN. The interval between transmission of EAPOL Request Identity frames is configured with EAPOL Timeout. If Allow Guest VLAN if EAPOL Seen is enabled, the port will now be placed in the Guest VLAN. If disabled, the switch will first check its history to see if an EAPOL frame has previously been received on the port (this history is cleared if the port link goes down or the port's Admin State is changed), and if not, the port will be placed in the Guest VLAN. Otherwise it will not move to the Guest VLAN, but continue transmitting EAPOL Request Identity frames at the rate given by EAPOL Timeout.

Once in the Guest VLAN, the port is considered authenticated, and all attached clients on the port are allowed access on this VLAN. The switch will not transmit an EAPOL Success

frame when entering the Guest VLAN.

While in the Guest VLAN, the switch monitors the link for EAPOL frames, and if one such frame is received, the switch immediately takes the port out of the Guest VLAN and starts authenticating the supplicant according to the port mode. If an EAPOL frame is received, the port will never be able to go back into the Guest VLAN if the "Allow Guest VLAN if EAPOL Seen" is disabled.

- **Port State :**

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

  Globally Disabled: NAS is globally disabled.

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

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

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

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

- **Restart :**

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

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

  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:**

  Apply – Click to apply 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.

4-5.2 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 4-5.2: The Network Access Server Switch Status

Network Access Server Switch Status

Port	Admin State	Port State	Last Source	Last ID	QoS Class	Port VLAN ID
1	Force Authorized	Globally Disabled				
2	Force Authorized	Globally Disabled				
3	Force Authorized	Globally Disabled				
4	Force Authorized	Globally Disabled				
5	Force Authorized	Globally Disabled				
6	Force Authorized	Globally Disabled				
7	Force Authorized	Globally Disabled				
8	Force Authorized	Globally Disabled				
9	Force Authorized	Globally Disabled				
10	Force Authorized	Globally Disabled				
11	Force Authorized	Globally Disabled				
12	Force Authorized	Globally Disabled				
13	Force Authorized	Globally Disabled				
14	Force Authorized	Globally Disabled				
15	Force Authorized	Globally Disabled				
16	Force Authorized	Globally Disabled				
17	Force Authorized	Globally Disabled				
18	Force Authorized	Globally Disabled				
19	Force Authorized	Globally Disabled				
20	Force Authorized	Globally Disabled				
21	Force Authorized	Globally Disabled				
22	Force Authorized	Globally Disabled				
23	Force Authorized	Globally Disabled				
24	Force Authorized	Globally Disabled				
25	Force Authorized	Globally Disabled				
26	Force Authorized	Globally Disabled				
27	Force Authorized	Globally Disabled				
28	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.

4-5.3 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-refresh".

Figure 4-5.3: 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.

4-6 AAA

This section shows you to use an AAA (Authentication, Authorization, Accounting) server to provide access control to your network. The AAA server can be a TACACS+ or RADIUS server to create and manage objects that contain settings for using AAA servers.

4-6.1 Configuration

This section describes how to configure AAA setting of TACACS+ or RADIUS server.

Web Interface

To configure a Common Configuration of AAA in the web interface:
1. Set Timeout (Default is 15 seconds).
2. Set Dead Time (Default is 300 seconds).

To configure a TACACS+ Authorization and Accounting Configuration of AAA in the web interface:
1. Select "Enabled" in the Authorization.
2. Select "Enabled" in the Failback to Local Authorization.
3. Select "Enabled" in the Account.

To configure a RADIUS Authentication Server Configuration of AAA in the web interface:
. Check "Enabled".
2. Specify IP address or Hostname for Radius Server.
3. Specify Authentication Port for Radius Server (Default is 1812).
4. Specify the Secret with Radius Server.

To configure a RADIUS Accounting Server Configuration of AAA in the web interface:
1. Check "Enabled".
2. Specify IP address or Hostname for Radius Server.
3. Specify Accounting Port for Radius Server (Default is 1813).
4. Specify the Secret with Radius Server.

To configure a TACACS+ Authentication Server Configuration of AAA in the web interface:
1. Check "Enabled".
2. Specify IP address or Hostname for TACACS+ Server.
3. Specify Authentication Port for TACACS+ Server (Default is 49).
4. Specify the Secret with TACACS+ Server.

Figure 4-6.1.1: The Common Server Configuration

Authentication Server Configuration

Common Server Configuration

Timeout	15	seconds
Dead Time	300	seconds

TACACS+ Authorization and Accounting Configuration

Authorization	Disabled ▼
Fallback to Local Authorization	Disabled ▼
Accounting	Disabled ▼

RADIUS Authentication Server Configuration

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

RADIUS Accounting Server Configuration

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

TACACS+ Authentication Server Configuration

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

[Apply] [Reset]

Parameter description:

● **Timeout :**

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

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

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

● **Dead Time :**

The Dead Time, which can be set to a number between 0 and 3600 seconds, is the period during which the switch will not send new requests to a server that has failed to respond to a previous request. This will stop the switch from continually trying to contact a server that

it has already determined as dead.

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

RADIUS Authentication Server Configuration

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

- **# :**

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

- **Enabled :**

  Enable the RADIUS Authentication Server by checking this box.

- **IP Address/Hostname :**

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

- **Port :**

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

- **Secret :**

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

RADIUS Accounting Server Configuration

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

- **# :**

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

- **Enabled :**

  Enable the RADIUS Accounting Server by checking this box.

- **IP Address/Hostname :**

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

- **Port :**

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

- **Secret :**

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

TACACS+ Authentication Server Configuration

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

- **# :**

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

- **Enabled :**

  Enable the TACACS+ Authentication Server by checking this box.

- **IP Address/Hostname :**

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

- **Port :**

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

- **Secret :**

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

- **Buttons:**

  Apply – Click to apply changes.

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

4-6.2 Radius Overview

This section shows you an overview of the RADIUS Authentication and Accounting servers status to ensure the function is workable.

Web Interface

To configure a RADIUS Overview Configuration in the web interface:

1. Checked "Auto-refresh".

Figure 4-6.2: The RADIUS Authentication Server Status Overview

Parameter description:

- **# :**

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

- **IP Address :**

    The IP address and UDP port number (in <IP Address>:<UDP Port> notation) of this server.

- **State :**

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

    Disabled: The server is disabled.

    Not Ready: The server is enabled, but IP communication is not yet up and running.

    Ready: The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept access attempts.

    Dead (X seconds left): Access attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.

RADIUS Accounting Servers

- **# :**

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

- **IP Address :**

The IP address and UDP port number (in <IP Address>:<UDP Port> notation) of this server.

- **State** :

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

  Disabled: The server is disabled.

  Not Ready: The server is enabled, but IP communication is not yet up and running.

  Ready: The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept accounting attempts.

  Dead (X seconds left): Accounting attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.

- **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 RADIUS Status by manual.

4-6.3 Radius Details

This section shows you an detailed statistics of the RADIUS Authentication and Accounting servers. The statistics map closely to those specified in RFC4668 - RADIUS Authentication Client MIB.

Web Interface

To configure a RADIUS Details Configuration in the web interface:
1. Specify Port which want to check.
2. Checked "Auto-refresh".

Figure 4-6.3: The RADIUS Authentication Statistics Server

RADIUS Authentication Statistic Server #1 ▼ Auto-refresh ☐ [Refresh] [Clear]

Receive Packets		Transmit Packets	
Access Accepts	0	Access Requests	0
Access Rejects	0	Access Retransmissions	0
Access Challenges	0	Pending Requests	0
Malformed Access Responses	0	Timeouts	0
Bad Authenticators	0		
Unknown Types	0		
Packets Dropped	0		
Other Info			
IP Address			0.0.0.0:1812
State			Disabled
Round-Trip Time			0 ms

RADIUS Accounting Statistics for Server #1

Receive Packets		Transmit Packets	
Responses	0	Requests	0
Malformed Responses	0	Retransmissions	0
Bad Authenticators	0	Pending Requests	0
Unknown Types	0	Timeouts	0
Packets Dropped	0		
Other Info			
IP Address			0.0.0.0:1813
State			Disabled
Round-Trip Time			0 ms

Parameter description:

● **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 RADIUS Statistics information by manual. Others you can click the clear to clean up all entries.

4-7 Port Security

This section shows you 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.

4-7.1 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 Action (Trap, Shutdown, Trap & Shutdown)
4. Click Apply.

Figure 4-7.1: The Port Security Limit Control Configuration

Port Security Limit Control Configuration

System Configuration

Mode	Disabled ▼
Aging Enabled	☐
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
19	Disabled ▼	4	None ▼	Disabled	Reopen
20	Disabled ▼	4	None ▼	Disabled	Reopen
21	Disabled ▼	4	None ▼	Disabled	Reopen
22	Disabled ▼	4	None ▼	Disabled	Reopen
23	Disabled ▼	4	None ▼	Disabled	Reopen
24	Disabled ▼	4	None ▼	Disabled	Reopen
25	Disabled ▼	4	None ▼	Disabled	Reopen
26	Disabled ▼	4	None ▼	Disabled	Reopen
27	Disabled ▼	4	None ▼	Disabled	Reopen
28	Disabled ▼	4	None ▼	Disabled	Reopen

[Apply] [Reset]

Parameter description:

System Configuration

- **Mode :**

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

- **Aging Enabled :**

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

- **Aging Period :**

  If Aging Enabled is checked, then the aging period is controlled with this input. If other modules are using the underlying port security for securing MAC addresses, they may

have other requirements to the aging period. The underlying port security will use the shorter requested aging period of all modules that use the functionality.

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

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

Port Configuration

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

- **Port :**

  The port number to which the configuration below applies.

- **Mode :**

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

- **Limit :**

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

  The stackswitch 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.

  Block: If Limit + 1 MAC addresses is seen on the port, block the whole 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 blocked. 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 & Block: If Limit + 1 MAC addresses is seen on the port, both the "Trap" and the "Block" 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.

Blocked: Indicates that the port is blocked by the Limit Control module. This state can only be shown if Action is set to Block or Trap & Block.

- **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:**

  Apply – Click to apply changes.

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

4-7.2 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-refresh"

Figure 4-7.2: 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

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	-	-
19	---	Disabled	-	-
20	---	Disabled	-	-
21	---	Disabled	-	-
22	---	Disabled	-	-
23	---	Disabled	-	-
24	---	Disabled	-	-
25	---	Disabled	-	-
26	---	Disabled	-	-
27	---	Disabled	-	-
28	---	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 in the stack 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.

  Blocked: 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 (-).

- **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.

4-7.3 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-refresh".

Figure 4-7.3: The Port Security Port Status

Port Security Port Status Port 1   Port 1 ▾ Auto-refresh ☐ [Refresh]

Total Secured Mac entries: 0

Index	MAC Address	VLAN ID	State	Time of Addition	Age/Hold
No MAC addresses attached					

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.

4-8 Access Management

This section shows you to configure access management table of the Switch including HTTP/HTTPS, SNMP, and TELNET/SSH. You can manage the Switch over an Ethernet LAN, or over the Internet.

4-8.1 Configuration

This section shows you how to configure access management table of the Switch. The maximum entry number is 16. If the application's type match any one of the access management entries, it will allow access to the switch.

Web Interface

To configure a Access Management Configuration in the web interface:
1. Select "Enabled" in the Mode of Access Management Configuration.
2. Click "Add new entry".
3. Specify the Start IP Address, End IP Address.
4. Checked Access Management method (HTTP/HTTPS, SNMP, and TELNET/SSH) in the entry.
5. Click Apply.

Figure 4-8.1: The Access Management Configuration

Access Management Configuration

Mode	Disabled ▼

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

Add new entry

Apply   Reset

Parameter description:

● **Mode :**

Indicates the access management mode operation. Possible modes are:

Enabled: Enable access management mode operation.

Disabled: Disable access management mode operation.

● **Delete :**

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

● **Start IP address :**

Indicates the start IP address for the access management entry.

● **End IP address :**

Indicates the end IP address for the access management entry.

● **HTTP/HTTPS :**

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

● **SNMP :**

Indicates that the host can access the switch from SNMP interface if the host IP address

matches the IP address range provided in the entry.

- **TELNET/SSH :**

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

- **Buttons:**

    Apply – Click to apply changes.

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

4-8.2 Statistics

This section shows you a detailed statistics of the Access Management including HTTP, HTTPS, SSH. TELNET, and SSH.

Web Interface

To configure an Assess Management Statistics in the web interface:

1. Checked "Auto-refresh".

Figure 4-8.2: The Access Management Statistics

Access Management Statistics

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

Parameter description:

● **Interface :**

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

● **Received Packets :**

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

● **Allowed Packets :**

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

● **Discarded Packets. :**

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

● **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 Access Management Statistics information by manual. Others you can click the clear button to clean up all entries.

4-9 SSH
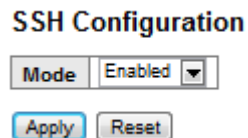
This section shows you to use SSH (Secure SHell) to securely access the Switch. SSH is a secure communication protocol that combines authentication and data encryption to provide secure encrypted communication.

Web Interface

To configure a SSH Configuration in the web interface:
1. Select "Enabled" in the Mode of SSH Configuration.
2. Click Apply.

Figure 4-9.1: The SSH Configuration

SSH Configuration

| Mode | Enabled ▼ |

Apply   Reset

Parameter description:

- **Mode :**

  Indicates the SSH mode operation. Possible modes are:

  Enabled: Enable SSH mode operation.

  Disabled: Disable SSH mode operation.

- **Buttons:**

  Apply – Click to apply changes.

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

4-10 HTTPs

This section shows you how to use HTTPS to securely access the Switch. HTTPS is a secure communication protocol that combines authentication and data encryption to provide secure encrypted communication via the browser.

Web Interface

To configure a HTTPS Configuration in the web interface:
1. Select "Enabled" in the Mode of HTTPS Configuration.
2.   Select "Enabled" in the Automatic Redirect of HTTPS Configuration.
3.   Click Apply.

Figure 4-10.1: The HTTPS Configuration

HTTPS Configuration

Mode	Enabled ▾
Automatic Redirect	Disabled ▾

[Apply] [Reset]

Parameter description:

- **Mode :**

    Indicates the HTTPS mode operation. Possible modes are:

    Enabled: Enable HTTPS mode operation.

    Disabled: Disable HTTPS mode operation.

- **Automatic Redirect :**

    Indicates the HTTPS redirect mode operation. Automatically redirect web browser to HTTPS when HTTPS mode is enabled. Possible modes are:

    Enabled: Enable HTTPS redirect mode operation.

    Disabled: Disable HTTPS redirect mode operation.

4-11 Auth Method

This page shows how to configure a user with authenticated when he logs into the switch stack via one of the management client interfaces.

Web Interface

To configure a Authentication Method Configuration in the web interface:
1. Specify the Client (console, telent, ssh, web) which you want to monitor.
2. Specify the Authentication Method (none,local, radius, tacacs+)
3. Checked Fallback.
4. Click Apply.

Figure 4-11.1: The HTTPS Configuration

Parameter description:

- **Client :**

  The management client for which the configuration below applies.

- **Authentication Method :**

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

  - none : authentication is disabled and login is not possible.
  - local : use the local user database on the switch stack for authentication.
  - radius : use a remote RADIUS server for authentication.
  - tacacs+ : use a remote TACACS+ server for authentication.

- **Fallback :**

  Enable fallback to local authentication by checking this box.

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

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

- **Buttons:**

  Apply – Click to apply changes.

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

4-12 PPPoE IA

Configure PPPoE IA on this page.

Web Interface

To configure a DHCP Relay in the web interface:
1. Click Security, PPPoE IA
2. Scroll to select the Vendor-specific Information Policy and Option Mode
3. Specify VLAN ID, Info
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 4-4.2: The DHCP Relay Statistics

PPPoE Intermediate Agent

Enable Agent	☐
VLAN ID	
Vendor-specific Information Policy	Keep ▾
Option Mode	Private ▾
Info(Circuit ID)	
TR-101 Option	☐ Hostname ☐ Slot-ID 1 ▾ ☐ Port Number ☐ VLAN
TR-101 Delimiter	/ ▾

Apply   Cancel

Note: The agent with VLAN ID 0 is the default agent

Index	VLAN ID	Enable	Policy Mode	Option Mode	Info(Circuit ID)	Select
1	0	Disable	Keep	Private		☐

Enable   Disable   Delete   Select   All   None

Parameter description:

- **Enable Agent :**

  Indicates the PPPoE IA Agent mode operation. Possible modes are:

  Enabled: Enable PPPoE IA Agent mode operation. When PPPoE IA Agent mode operation is enabled, add a vendor-specific tag to PADI and PADR packets from PPPoE clients int the specified VLAN.

  Disabled: Disable PPPoE IA Agent mode operation.

- **VLAN ID :**

  Enter the source VLAN ID for which the PPPoE IA settings apply. Enter 0 if you want to configure the default settings for all VLAN.

- **Vendor-specific Information Policy :**

  Indicates the Vendor-specific information option policy. When PPPoE Enable Agent mode operation is enabled, if agent receives a PPPoE message that already contains Vendor-specific information it will enforce the policy. And it only works under PPPoE if Enable Agent mode is enabled. Possible policies are:

  Replace: Replace the original Vendor-specific information when a PPPoE message that already contains it is received.

  Keep: Keep the original Vendor-specific information when a PPPoE message that already contains it is received.

  Drop: Drop the packet when a PPPoE message that already contains Vendor-specific information is received.

- **Option Mode :**

  PPPoE IA sub-option. Possible option mode are:

  Private: [0x01][len][slot][port][vid-2 bytes][string 0-23 char]. [0x02][len][Clent MAC-6 bytes]

  TR-101: [0x01][len][0-23 char][delimiter][eth][delimiter][slot][delimiter][port][delimiter][vlan]. [0x02][len -Max :63][Port desc 47][delimiter][Port Tel 32 char]

- **Info (Circuit ID) :**

  Enter any extra information the switch adds to PADI and PADR packets in the specified VLAN. 0 - 23 characters normal ASCII Types.

- **Hostname :**

  Option Mode must is TR-101.

  Possible modes are:

  Enabled: Add Hostname Information, if Hostname is not configured, add IP Information.

  Disabled: Add Info(Circuit ID) Information.

- **Slot-ID :**

  Option Mode must is TR-101.

  Possible modes are:

  Enabled: Add Slot Information, Slot ID can select 0 or 1, Default:1.

  Disabled: Remove Slot Information.

- **Port Number :**

  Option Mode must is TR-101.

  Possible modes are:

  Enabled: Add Port Number Information.

  Disabled: Remove Port Number Information.

- **VLAN :**

  Option Mode must is TR-101.

  Possible modes are:

  Enabled: Add VLAN Information.

  Disabled: Remove VLAN Information.

- **Delimiter :**

  Option Mode must is TR-101. Possible Delimiter are:

  #

  ;

  .

  ,

  /

  space

- **Index :**

  This field displays the index number of the entry.

- **Buttons:**

  Apply – Click to apply changes.

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

4-13 Error Disable

4-13.1 CPU Protection

Configure CPU Protection on this page.

Web Interface

To configure an CPU Protection in the web interface:
1. Click Security, Error Disable, CPU Protection
2. Scroll to select the Reason
3. Specify Rate Limit
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 4-13.1: The CPU Protection

Parameter description:

- **Reason :**

    Select the type of control packet you want to configure here. Possible modes are:

    ARP

    BPDU

    IGMP

- **Port :**

    This field displays the port number.

- **Rate Limit(pkt/s) :**

    Enter a number from 0 to 256 to specify how many control packets this port can receive or transmit per second. 0 means no rate limit.

- **Buttons:**

    Apply – Click to apply changes.

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

4-13.2 Errdisable Detect

Configure Errdisable Detect on this page.

Web Interface

To configure an Errdisable Detect in the web interface:
1. Click Security, Error Disable, Errdisable Detect
2. Scroll to select the Mode and active
3. Click the Apply to save the setting

Figure 4-13.2: The CPU Protection

Errdisable Detect

Cause	Active	Mode
*	☐	◇ ⌄
ARP	☐	Inactive-port ⌄
BPDU	☐	Inactive-port ⌄
IGMP	☐	Inactive-port ⌄

[Apply] [Cancel]

Parameter description:

- **Cause :**

  This field displays the types of control packet that may cause CPU overload.

- **Active :**

  Select this option to have the Switch detect if the configured rate limit for a specific control packet is exceeded and take the action selected below.

- **Mode :**

  Select the action that the Switch takes when the number of control packets exceed the rate limit on a port, set in the CPU protection screen. Possible modes are:

  inactive-port: The Switch disables the port on which the control packets are received.

  inactive-reason: The Switch bypasses the processing of the specified control packets (such as ARP or IGMP packets), or drops all the specified control packets (such as BPDU) on the port.

  rate-limitation: The Switch drops the additional control packets the port has to handle in every one second.

- **Buttons:**

  Apply – Click to apply changes.

  Cancel- Click Cancel to begin configuring the fields afresh.

4-13.3 Errdisable Recovery

Configure Errdisable Recovery on this page.

Web Interface

To configure an Errdisable Detect in the web interface:
1. Click Security, Error Disable, Errdisable Recovery
2. Select the Timer status.
3. Specify Interval
4. Click the Apply to save the setting

Figure 4-13.2: The CPU Protection

Errdisable Recovery

Reason	Timer Status	Interval
*	☐	
ARP	☐	300
BPDU	☐	300
IGMP	☐	300

Apply Cancel

Parameter description:

● **Active :**

Select this option to turn on the error-disable recovery function on the Switch.

● **Reason :**

This field displays the supported features that allow the Switch to shut down a port or discard packets on a port according to the feature requirements and what action you configure.

● **Time Status :**

Select this option to alllow the Switch to wait for the specified time interval to activate a port or allow specific packets on a port, after the error was gone. Deselect this option to turn off this rule.

● **Interval :**

Enter the number of seconds (from 30 to 2592000) for the time interval.

● **Buttons:**

Apply – Click to apply changes.

Cancel- Click Cancel to begin configuring the fields afresh.

4-8.2 Errdisable Status

This page displays the Errdisable status

Web Interface

To configure an Errdisable Status in the web interface:

1. Checked "Auto-refresh".

Figure 4-8.2: The Errdisable Status

Errdisable Status

Port	Protecting Status
1	
2	
3	
4	
5	
6	
7	
8	
9	
10	
11	
12	
13	
14	
15	
16	
17	
18	
19	
20	
21	
22	
23	
24	
25	
26	

Parameter description:

● **Port :**

This field displays the port number.

● **Protecting Status :**

Protecting Status.

● **Auto-refresh :**

Check this box to enable an automatic refresh of the page at regular intervals.

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

5-1 Restart Device

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. Chick Restart Device.
2.   Click Yes.

Figure 5-1.1: The Restart Device

Restart Device

Are you sure you want to perform a Restart?

Yes   No
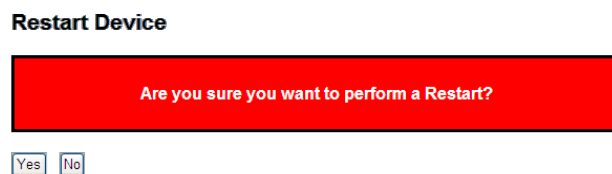
Parameter description:

- **Restart Device :**

    You can restart the stack switch on this page. After restart, the stack 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. Chick Browser to select firmware in you device.

2. Click Upload.

Figure 5-2.1: The Firmware update

Firmware Update
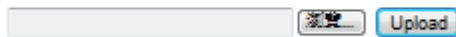
[_____] [瀏覽_] [Upload]

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:** Uploading software will update all managed switches in the stack to the location of a software image. 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 in the stack restart.

> **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. Chick Activate Alternate Image.

2. Click yes to complete firmware selection..

Figure 5-2.2: The Firmware Selection

Software Image Selection

Active Image	
Image	managed
Version	V1.00(AAPA.2)C0
Date	2014-12-25T11:49:39+08:00

Alternate Image	
Image	managed.bk
Version	V1.00(AAFM.0)C0
Date	2013-08-27T16:11:03+08:00

Activate Alternate Image Cancel

Message from webpage

? Are you sure you want to activate the alternate software image?
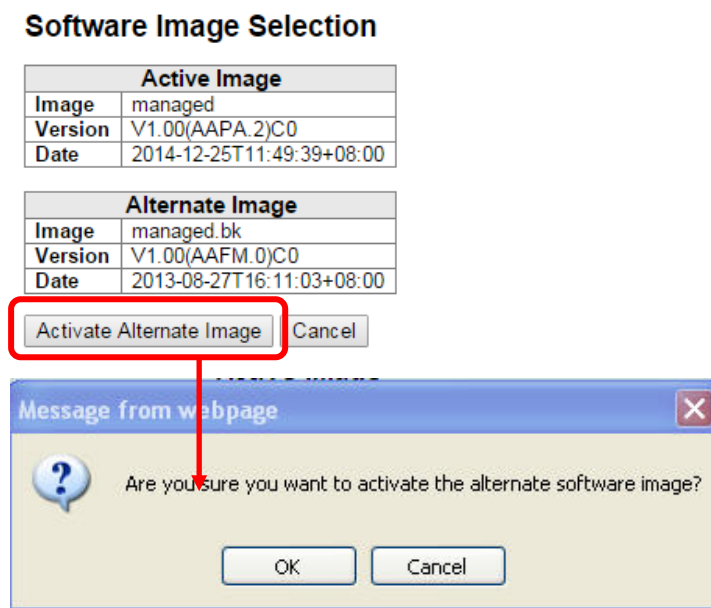
OK   Cancel

Parameter description:

● **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.

● **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.

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. Chick Factory Defaults.

2. Click Yes.

Figure 5-3.1: The Factory Defaults

Factory Defaults

Are you sure you want to reset the configuration to
Factory Defaults?

Yes   No

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.

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. Chick Save Start.
2. Click Yes.

Figure 5-3.2: The Save Start configuration

Save as Start Configuration

Are you sure to save the current setting as
Start Configuration?

Save

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. Chick Save User.
2. Click Yes.

Figure 5-3.3: The Save as Backup Configuration

Save as Backup Configuration
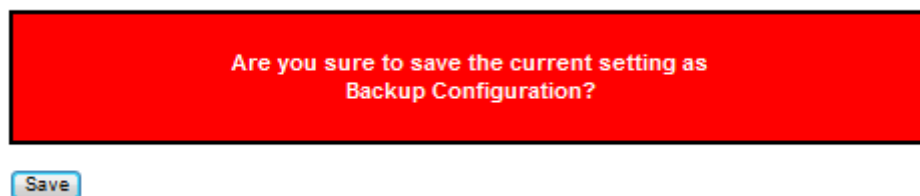
Are you sure to save the current setting as
Backup Configuration?

Save

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 user's 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. Chick Restore User.
2. Click Yes.

Figure 5-3.4: The Restore the Backup Configuration

Restore Backup Configuration

Are you sure to restore the Backup Configuration?

Save

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. Chick Save configuration.

2. Save the file in your device.

Figure 5-4.1: The Restore the Backup Configuration
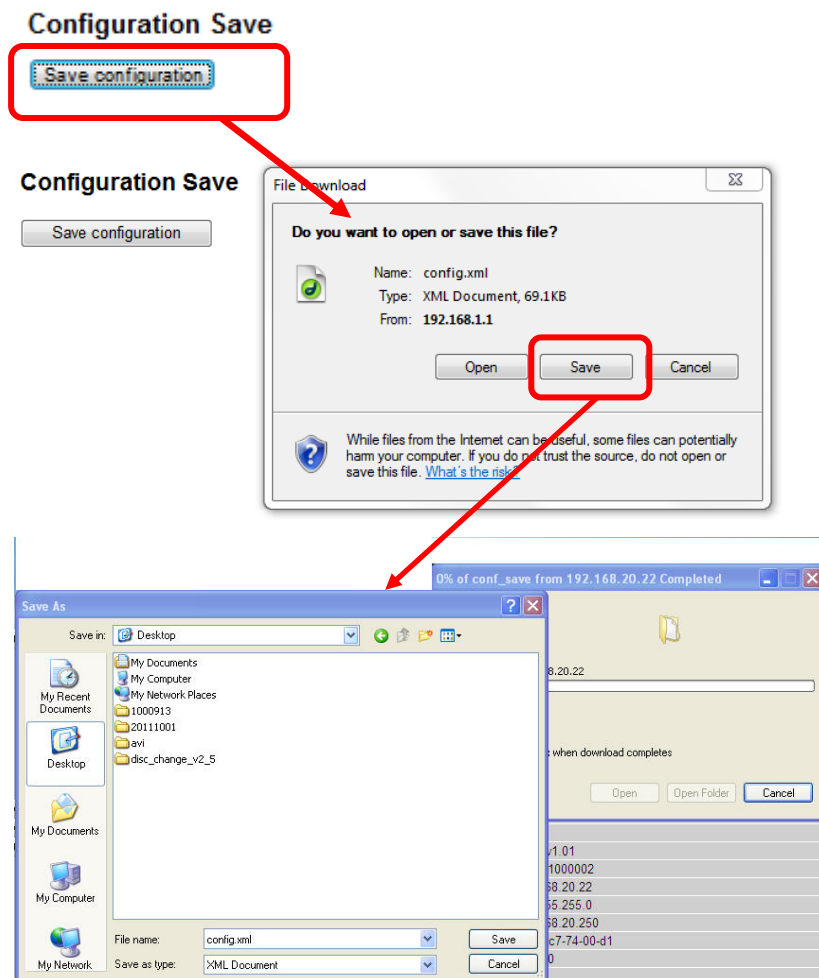
Parameter description:

> **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. Chick Browser to select the config file in you device.
2. Click Upload.

Figure 5-4.2: The Import Config
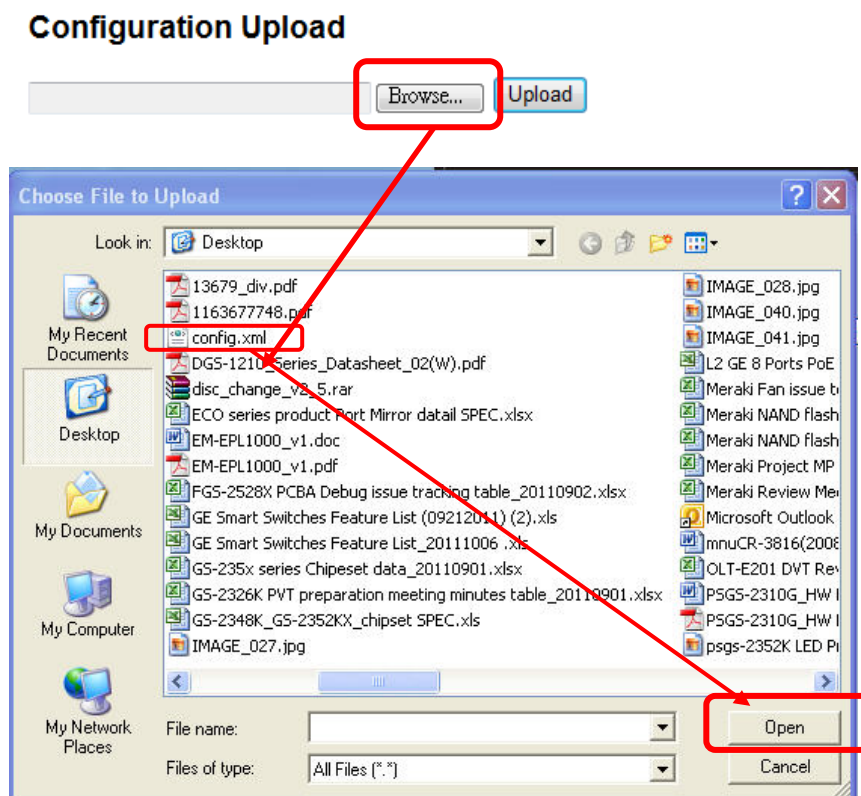
Parameter description:

- ● **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

Parameter description:

- **IP Address :**

    The destination IP Address.

- **Ping Length:**

    The payload size of the ICMP packet. Values range from 2 bytes to 1452 bytes.

- **Ping Count:**

    The count of the ICMP packet. Values range from 1 time to 60 times.

- **Ping Interval:**

    The interval of the ICMP packet. Values range from 0 second to 30 seconds.

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

5-5.2 Ping6

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

Web Interface

To configure an ICMPv6 PING Configuration in the web interface:
1.Specify ICMPv6 PING IP Address.
2.Specify ICMPv6 PING Size.
3.Click Start.

Figure 5-5.2: The ICMPv6 Ping

Parameter description:

- **IP Address :**

    The destination IP Address.

- **Ping Length :**

    The payload size of the ICMP packet. Values range from 2 bytes to 1452 bytes.

- **Ping Count :**

    The count of the ICMP packet. Values range from 1 time to 60 times.

- **Ping Interval:**

    The interval of the ICMP packet. Values range from 0 second to 30 seconds.

After you press , 5 ICMPv6 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.

PING 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

You can configure the following properties of the issued ICMP packets:

5-5.3 VeriPHY

This section is used for running the VeriPHY Cable Diagnostics. Press to run the diagnostics. This will take approximately 5 seconds. If all ports are selected, this can take approximately 15 seconds. When completed, the page refreshes automatically, and you can view the cable diagnostics results in the cable status table. Note that VeriPHY is only accurate for cables of length 7 -140 meters.10 and 100 Mbps ports will be linked down while running VeriPHY. Therefore, running VeriPHY on a 10 or 100 Mbps management port will cause the switch to stop responding until VeriPHY is complete.

Web Interface

To configure a VeriPHY Cable Diagnostics Configuration in the web interface:
1. Specify Port which want to check.
2. Click Start.

Figure 5-5.3: The VeriPHY

VeriPHY Cable Diagnostics

Port [All ▼]

[Start]

Cable Status							
Port	Pair A	Length A	Pair B	Length B	Pair C	Length C	Pair D	Length D
21	--	--	--	--	--	--	--	--
22	--	--	--	--	--	--	--	--
23	--	--	--	--	--	--	--	--
24	--	--	--	--	--	--	--	--

Parameter description:

● **Port :**

The port where you are requesting VeriPHY Cable Diagnostics.

● **Cable Status :**

Port: Port number.

Pair: The status of the cable pair.

Length: The length (in meters) of the cable pair.

A. Glossary of Web-based Management

A

ACE

ACE is an acronym for Access Control Entry. It describes access permission associated with a particular ACE ID.

There are three ACE frame types (Ethernet Type, ARP, and IPv4) and two ACE actions (permit and deny). The ACE also contains many detailed, different parameter options that are available for individual application.

ACL

ACL is an acronym for Access Control List. It is the list table of ACEs, containing access control entries that specify individual users or groups permitted or denied to specific traffic objects, such as a process or a program.
Each accessible traffic object contains an identifier to its ACL. The privileges determine whether there are specific traffic object access rights.
ACL implementations can be quite complex, for example, when the ACEs are prioritized for the various situation. In networking, the ACL refers to a list of service ports or network services that are available on a host or server, each with a list of hosts or servers permitted or denied to use the service. ACL can generally be configured to control inbound traffic, and in this context, they are similar to firewalls.

There are 3 web-pages associated with the manual ACL configuration:

ACL|Access Control List: The web page shows the ACEs in a prioritized way, highest (top) to lowest (bottom). Default the table is empty. An ingress frame will only get a hit on one ACE even though there are more matching ACEs. The first matching ACE will take action (permit/deny) on that frame and a counter associated with that ACE is incremented. An ACE can be associated with a Policy, 1 ingress port, or any ingress port (the whole switch). If an ACE Policy is created then that Policy can be associated with a group of ports under the "Ports" web-page. There are number of parameters that can be configured with an ACE. Read the Web page help text to get further information for each of them. The maximum number of ACEs is 64.
ACL|Ports: The ACL Ports configuration is used to assign a Policy ID to an ingress port. This is useful to group ports to obey the same traffic rules. Traffic Policy is created under the "Access Control List" - page. You can you also set up specific traffic properties (Action / Rate Limiter / Port copy, etc) for each ingress port. They will though only apply if the frame gets past the ACE matching without getting matched. In that case a counter associated with that port is incremented. See the Web page help text for each specific port property.
ACL|Rate Limiters: Under this page you can configure the rate limiters. There can be 15 different rate limiters, each ranging from 1-1024K packets per seconds. Under "Ports" and "Access Control List" web-pages you can assign a Rate Limiter ID to the ACE(s) or ingress port(s).

AES

AES is an acronym for Advanced Encryption Standard. The encryption key protocol is applied in 802.1i standard to improve WLAN security. It is an encryption standard by the U.S. government, which will replace DES and 3DES. AES has a fixed block size of 128 bits and a key size of 128, 192, or 256 bits.

APS

APS is an acronym for Automatic Protection Switching. This protocol is used to secure that switching is done bidirectional in the two ends of a protection group, as defined in G.8031.

Aggregation

Using multiple ports in parallel to increase the link speed beyond the limits of a port and to increase the redundancy for higher availability.

(Also Port Aggregation, Link Aggregation).

ARP

ARP is an acronym for Address Resolution Protocol. It is a protocol that used to convert an IP address into a physical address, such as an Ethernet address. ARP allows a host to communicate with other hosts when only the Internet address of its neighbors is known. Before using IP, the host sends a broadcast ARP request containing the Internet address of the desired destination system.

ARP Inspection

ARP Inspection is a secure feature. Several types of attacks can be launched against a host or devices connected to Layer 2 networks by "poisoning" the ARP caches. This feature is used to block such attacks. Only valid ARP requests and responses can go through the switch device.

Auto-Negotiation

Auto-negotiation is the process where two different devices establish the mode of operation and the speed settings that can be shared by those devices for a link.

C

CC

CC is an acronym for Continuity Check. It is a MEP functionality that is able to detect loss of continuity in a network by transmitting CCM frames to a peer MEP.

CCM

CCM is an acronym for Continuity Check Message. It is a OAM frame transmitted from a MEP to it's peer MEP and used to implement CC functionality.

CDP

CDP is an acronym for Cisco Discovery Protocol.

D

DEI

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

DES

DES is an acronym for Data Encryption Standard. It provides a complete description of a mathematical algorithm for encrypting (enciphering) and decrypting (deciphering) binary coded information.

Encrypting data converts it to an unintelligible form called cipher. Decrypting cipher converts the data back to its original form called plaintext. The algorithm described in this standard specifies both enciphering and deciphering operations which are based on a binary number called a key.

DHCP

DHCP is an acronym for Dynamic Host Configuration Protocol. It is a protocol used for assigning dynamic IP addresses to devices on a network.

DHCP used by networked computers (clients) to obtain IP addresses and other parameters such as the default gateway, subnet mask, and IP addresses of DNS servers from a DHCP server.

The DHCP server ensures that all IP addresses are unique, for example, no IP address is assigned to a second client while the first client's assignment is valid (its lease has not expired). Therefore, IP address pool management is done by the server and not by a human network administrator.

Dynamic addressing simplifies network administration because the software keeps track of IP addresses rather than requiring an administrator to manage the task. This means that a new computer can be added to a network without the hassle of manually assigning it a unique IP address.

DHCP Relay

DHCP Relay is used to forward and to transfer DHCP messages between the clients and the server when they are not on the same subnet domain.

The DHCP option 82 enables a DHCP relay agent to insert specific information into a DHCP request packets when forwarding client DHCP packets to a DHCP server and remove the specific information from a DHCP reply packets when forwarding server DHCP packets to a DHCP client. The DHCP server can use this information to implement IP address or other assignment policies. Specifically the option works by setting two sub-options: Circuit ID (option 1) and Remote ID (option2). The Circuit ID sub-option is supposed to include information specific to which circuit the request came in on. The

Remote ID sub-option was designed to carry information relating to the remote host end of the circuit.

The definition of Circuit ID in the switch is 4 bytes in length and the format is "vlan_id" "module_id" "port_no". The parameter of "vlan_id" is the first two bytes represent the VLAN ID. The parameter of "module_id" is the third byte for the module ID (in standalone switch it always equal 0, in stackable switch it means switch ID). The parameter of "port_no" is the fourth byte and it means the port number.
The Remote ID is 6 bytes in length, and the value is equal the DHCP relay agents MAC address.

DHCP Snooping

DHCP Snooping is used to block intruder on the untrusted ports of the switch device when it tries to intervene by injecting a bogus DHCP reply packet to a legitimate conversation between the DHCP client and server.

DNS

DNS is an acronym for Domain Name System. It stores and associates many types of information with domain names. Most importantly, DNS translates human-friendly domain names and computer hostnames into computer-friendly IP addresses. For example, the domain name www.example.com might translate to 192.168.0.1.

DoS

DoS is an acronym for Denial of Service. In a denial-of-service (DoS) attack, an attacker attempts to prevent legitimate users from accessing information or services. By targeting at network sites or network connection, an attacker may be able to prevent network users from accessing email, web sites, online accounts (banking, etc.), or other services that rely on the affected computer.

Dotted Decimal Notation

Dotted Decimal Notation refers to a method of writing IP addresses using decimal numbers and dots as separators between octets.
An IPv4 dotted decimal address has the form x.y.z.w, where x, y, z, and w are decimal numbers between 0 and 255.

DSCP

DSCP is an acronym for Differentiated Services Code Point. It is a field in the header of IP packets for packet classification purposes.

E

EEE

EEE is an abbreviation for Energy Efficient Ethernet defined in IEEE 802.3az.

EPS

EPS is an abbreviation for Ethernet Protection Switching defined in ITU/T G.8031.

Ethernet Type

Ethernet Type, or EtherType, is a field in the Ethernet MAC header, defined by the Ethernet networking standard. It is used to indicate which protocol is being transported in an Ethernet frame.

F

FTP

FTP is an acronym for File Transfer Protocol. It is a transfer protocol that uses the Transmission Control Protocol (TCP) and provides file writing and reading. It also provides directory service and security features.

Fast Leave

Multicast snooping Fast Leave processing allows the switch to remove an interface from the forwarding-table entry without first sending out group specific queries to the interface. The VLAN interface is pruned from the multicast tree for the multicast group specified in the original leave message. Fast-leave processing ensures optimal bandwidth management for all hosts on a switched network, even when multiple multicast groups are in use simultaneously. This processing applies to IGMP and MLD.

H

HTTP

HTTP is an acronym for Hypertext Transfer Protocol. It is a protocol that used to transfer or convey information on the World Wide Web (WWW).

HTTP defines how messages are formatted and transmitted, and what actions Web servers and browsers should take in response to various commands. For example, when you enter a URL in your browser, this actually sends an HTTP command to the Web server directing it to fetch and transmit the requested Web page. The other main standard that controls how the World Wide Web works is HTML, which covers how Web pages are formatted and displayed.

Any Web server machine contains, in addition to the Web page files it can serve, an HTTP daemon, a program that is designed to wait for HTTP requests and handle them when they arrive. The Web browser is an HTTP client, sending requests to server machines. An HTTP client initiates a request by establishing a Transmission Control Protocol (TCP) connection to a particular port on a remote host (port 80 by default). An HTTP server listening on that port waits for the client to send a request message.

HTTPS

HTTPS is an acronym for Hypertext Transfer Protocol over Secure Socket Layer. It is used to indicate a secure HTTP connection.

HTTPS provide authentication and encrypted communication and is widely used on the World Wide Web for security-sensitive communication such as payment transactions and corporate logons.

HTTPS is really just the use of Netscape's Secure Socket Layer (SSL) as a sublayer under its regular HTTP application layering. (HTTPS uses port 443 instead of HTTP port 80 in its interactions with the lower layer, TCP/IP.) SSL uses a 40-bit key size for the RC4 stream encryption algorithm, which is considered an adequate degree of encryption for commercial exchange.

I

ICMP

ICMP is an acronym for Internet Control Message Protocol. It is a protocol that generated the error response, diagnostic or routing purposes. ICMP messages generally contain information about routing difficulties or simple exchanges such as time-stamp or echo transactions. For example, the PING command uses ICMP to test an Internet connection.

IEEE 802.1X

IEEE 802.1X is an IEEE standard for port-based Network Access Control. It provides authentication to devices attached to a LAN port, establishing a point-to-point connection or preventing access from that port if authentication fails. With 802.1X, access to all switch ports can be centrally controlled from a server, which means that authorized users can use the same credentials for authentication from any point within the network.

IGMP

IGMP is an acronym for Internet Group Management Protocol. It is a communications protocol used to manage the membership of Internet Protocol multicast groups. IGMP is used by IP hosts and adjacent multicast routers to establish multicast group memberships. It is an integral part of the IP multicast specification, like ICMP for unicast connections. IGMP can be used for online video and gaming, and allows more efficient use of resources when supporting these uses.

IGMP Querier

A router sends IGMP Query messages onto a particular link. This router is called the Querier.

IMAP

IMAP is an acronym for Internet Message Access Protocol. It is a protocol for email clients to retrieve email messages from a mail server.

IMAP is the protocol that IMAP clients use to communicate with the servers, and SMTP is the protocol used to transport mail to an IMAP server.

The current version of the Internet Message Access Protocol is IMAP4. It is similar to Post Office Protocol version 3 (POP3), but offers additional and more complex features. For example, the IMAP4 protocol leaves your email messages on the server rather than downloading them to your computer. If you wish to remove your messages from the server, you must use your mail client to generate local folders, copy messages to your local hard drive, and then delete and expunge the messages from the server.

IP

IP is an acronym for 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, IPv6, which would have 128-bits Internet Protocol addresses. This number can be represented roughly by a three with thirty-nine zeroes after it. However, IPv4 is still the protocol of choice for most of the Internet.

IPMC

IPMC is an acronym for IP MultiCast.

IP Source Guard

IP Source Guard is a secure feature used to restrict IP traffic on DHCP snooping untrusted ports by filtering traffic based on the DHCP Snooping Table or manually configured IP Source Bindings. It helps prevent IP spoofing attacks when a host tries to spoof and use the IP address of another host.

L

LACP

LACP is an IEEE 802.3ad standard protocol. The Link Aggregation Control Protocol, allows bundling several physical ports together to form a single logical port.

LLC

The IEEE 802.2 Logical Link Control (LLC) protocol provides a link mechanism for upper layer protocols. It is the upper sub-layer of the Data Link Layer and provides multiplexing mechanisms that make it possible for several network protocols (IP, IPX) to coexist within a multipoint network. LLC header consists of 1 byte DSAP (Destination Service Access Point), 1 byte SSAP (Source Service Access Point), 1 or 2 bytes Control field followed by LLC information.

LLDP

LLDP is an IEEE 802.1ab standard protocol.

The Link Layer Discovery Protocol(LLDP) specified in this standard allows stations attached to an IEEE 802 LAN to advertise, to other stations attached to the same IEEE 802 LAN, the major capabilities provided by the system incorporating that station, the management address or addresses of the entity or entities that provide management of those capabilities, and the identification of the stations point of attachment to the IEEE 802 LAN required by those management entity or entities. The information distributed via this protocol is stored by its recipients in a standard Management Information Base (MIB), making it possible for the information to be accessed by a Network Management System (NMS) using a management protocol such as the Simple Network Management Protocol (SNMP).

LLDP-MED

LLDP-MED is an extendsion of IEEE 802.1ab and is defined by the telecommunication industry association (TIA-1057).

LOC

LOC is an acronym for Loss Of Connectivity and is detected by a MEP and is indicating lost connectivity in the network. Can be used as a switch criteria by EPS

M

MAC Table

Switching of frames is based upon the DMAC address contained in the frame. The switch builds up a table that maps MAC addresses to switch ports for knowing which ports the frames should go to (based upon the DMAC address in the frame). This table contains both static and dynamic entries. The static entries are configured by the network administrator if the administrator wants to do a fixed mapping between the DMAC address and switch ports.

The frames also contain a MAC address (SMAC address), which shows the MAC address of the equipment sending the frame. The SMAC address is used by the switch to automatically update the MAC table with these dynamic MAC addresses. Dynamic entries are removed from the MAC table if no frame with the corresponding SMAC address have been seen after a configurable age time.

MEP

MEP is an acronym for Maintenance Entity Endpoint and is an endpoint in a Maintenance

Entity Group (ITU-T Y.1731).

MD5

MD5 is an acronym for Message-Digest algorithm 5. MD5 is a message digest algorithm, used cryptographic hash function with a 128-bit hash value. It was designed by Ron Rivest in 1991. MD5 is officially defined in RFC 1321 - The MD5 Message-Digest Algorithm.

Mirroring

For debugging network problems or monitoring network traffic, the switch system can be configured to mirror frames from multiple ports to a mirror port. (In this context, mirroring a frame is the same as copying the frame.)

Both incoming (source) and outgoing (destination) frames can be mirrored to the mirror port.

MLD

MLD is an acronym for Multicast Listener Discovery for IPv6. MLD is used by IPv6 routers to discover multicast listeners on a directly attached link, much as IGMP is used in IPv4. The protocol is embedded in ICMPv6 instead of using a separate protocol.

MVR

Multicast VLAN Registration (MVR) is a protocol for Layer 2 (IP)-networks that enables multicast-traffic from a source VLAN to be shared with subscriber-VLANs.

The main reason for using MVR is to save bandwidth by preventing duplicate multicast streams being sent in the core network, instead the stream(s) are received on the MVR-VLAN and forwarded to the VLANs where hosts have requested it/them(Wikipedia).

N

NAS

NAS is an acronym for Network Access Server. The NAS is meant to act as a gateway to guard access to a protected source. A client connects to the NAS, and the NAS connects to another resource asking whether the client's supplied credentials are valid. Based on the answer, the NAS then allows or disallows access to the protected resource. An example of a NAS implementation is IEEE 802.1X.

NetBIOS

NetBIOS is an acronym for Network Basic Input/Output System. It is a program that allows applications on separate computers to communicate within a Local Area Network (LAN), and it is not supported on a Wide Area Network (WAN).

The NetBIOS giving each computer in the network both a NetBIOS name and an IP address corresponding to a different host name, provides the session and transport services described in the Open Systems Interconnection (OSI) model.

NFS

NFS is an acronym for Network File System. It allows hosts to mount partitions on a remote system and use them as though they are local file systems.

NFS allows the system administrator to store resources in a central location on the network, providing authorized users continuous access to them, which means NFS supports sharing of files, printers, and other resources as persistent storage over a computer network.

NTP

NTP is an acronym for Network Time Protocol, a network protocol for synchronizing the clocks of computer systems. NTP uses UDP (datagrams) as transport layer.

O

OAM

OAM is an acronym for Operation Administration and Maintenance.

It is a protocol described in ITU-T Y.1731 used to implement carrier ethernet functionality. MEP functionality like CC and RDI is based on this

Optional TLVs.

A LLDP frame contains multiple TLVs
For some TLVs it is configurable if the switch shall include the TLV in the LLDP frame. These TLVs are known as optional TLVs. If an optional TLVs is disabled the corresponding information is not included in the LLDP frame.

OUI

OUI is the organizationally unique identifier. An OUI address is a globally unique identifier

assigned to a vendor by IEEE. You can determine which vendor a device belongs to according to the OUI address which forms the first 24 bits of a MAC address.

P

PCP

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

PD

PD is an acronym for Powered Device. In a PoE> system the power is delivered from a PSE (power sourcing equipment) to a remote device. The remote device is called a PD.

PHY

PHY is an abbreviation for Physical Interface Transceiver and is the device that implement the Ethernet physical layer (IEEE-802.3).

PING

ping is a program that sends a series of packets over a network or the Internet to a specific computer in order to generate a response from that computer. The other computer responds with an acknowledgment that it received the packets. Ping was created to verify whether a specific computer on a network or the Internet exists and is connected.

ping uses Internet Control Message Protocol (ICMP) packets. The PING Request is the packet from the origin computer, and the PING Reply is the packet response from the target.

Policer

A policer can limit the bandwidth of received frames. It is located in front of the ingress queue.

POP3

POP3 is an acronym for Post Office Protocol version 3. It is a protocol for email clients to retrieve email messages from a mail server.

POP3 is designed to delete mail on the server as soon as the user has downloaded it. However, some implementations allow users or an administrator to specify that mail be saved for some period of time. POP can be thought of as a "store-and-forward" service.

An alternative protocol is Internet Message Access Protocol (IMAP). IMAP provides the user with more capabilities for retaining e-mail on the server and for organizing it in folders on the server. IMAP can be thought of as a remote file server.

POP and IMAP deal with the receiving of e-mail and are not to be confused with the Simple Mail Transfer Protocol (SMTP). You send e-mail with SMTP, and a mail handler receives it on your recipient's behalf. Then the mail is read using POP or IMAP. IMAP4 and POP3 are the two most prevalent Internet standard protocols for e-mail retrieval. Virtually all modern e-mail clients and servers support both.

Private VLAN

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

Q

QCE

QCE is an acronym for QoS Control Entry. It describes QoS class associated with a particular QCE ID.

There are six QCE frame types: Ethernet Type, VLAN, UDP/TCP Port, DSCP, TOS, and Tag Priority. Frames can be classified by one of 4 different QoS classes: "Low", "Normal", "Medium", and "High" for individual application.

QCL

QCL is an acronym for QoS Control List. It is the list table of QCEs, containing QoS control entries that classify to a specific QoS class on specific traffic objects.

Each accessible traffic object contains an identifier to its QCL. The privileges determine specific traffic object to specific QoS class.

QL

QL In SyncE this is the Quality Level of a given clock source. This is received on a port in a SSM indicating the quality of the clock received in the port.

QoS

QoS is an acronym for Quality of Service. It is a method to guarantee a bandwidth relationship between individual applications or protocols.

A communications network transports a multitude of applications and data, including high-quality video and delay-sensitive data such as real-time voice. Networks must provide secure, predictable, measurable, and sometimes guaranteed services.

Achieving the required QoS becomes the secret to a successful end-to-end business solution. Therefore, QoS is the set of techniques to manage network resources.

R

RARP

RARP is an acronym for Reverse Address Resolution Protocol. It is a protocol that is used to obtain an IP address for a given hardware address, such as an Ethernet address. RARP is the complement of ARP.

RADIUS

RADIUS is an acronym for Remote Authentication Dial In User Service. It is a networking protocol that provides centralized access, authorization and accounting management for people or computers to connect and use a network service.

RDI

RDI is an acronym for Remote Defect Indication. It is a OAM functionallity that is used by a MEP to indicate defect detected to the remote peer MEP

RSTP

In 1998, the IEEE with document 802.1w introduced an evolution of STP: the Rapid Spanning Tree Protocol, which provides for faster spanning tree convergence after a topology change. Standard IEEE 802.1D-2004 now incorporates RSTP and obsoletes STP, while at the same time being backwards-compatible with STP.

S

SHA

SHA is an acronym for Secure Hash Algorithm. It designed by the National Security Agency (NSA) and published by the NIST as a U.S. Federal Information Processing Standard. Hash algorithms compute a fixed-length digital representation (known as a message digest) of an input data sequence (the message) of any length.

Shaper

A shaper can limit the bandwidth of transmitted frames. It is located after the ingress queues.

SMTP

SMTP is an acronym for Simple Mail Transfer Protocol. It is a text-based protocol that uses the Transmission Control Protocol (TCP) and provides a mail service modeled on the FTP file transfer service. SMTP transfers mail messages between systems and notifications regarding incoming mail.

SNAP

The 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.

SNMP

SNMP is an acronym for Simple Network Management Protocol. It is part of the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol for network management. SNMP allow diverse network objects to participate in a network management architecture. It enables network management systems to learn network problems by receiving traps or change notices from network devices implementing SNMP.

SNTP

SNTP is an acronym for Simple Network Time Protocol, a network protocol for synchronizing the clocks of computer systems. SNTP uses UDP (datagrams) as transport layer.

SPROUT

Stack Protocol using ROUting Technology. An advanced protocol for almost instantaneous discovery of topology changes within a stack as well as election of a master switch. SPROUT also calculates parameters for setting up each switch to perform shortest path forwarding within the stack.

SSID

Service Set Identifier is a name used to identify the particular 802.11 wireless LANs to which a user wants to attach. A client device will receive broadcast messages from all access points within range advertising their SSIDs, and can choose one to connect to based on pre-configuration, or by displaying a list of SSIDs in range and asking the user to select one (wikipedia).

SSH

SSH is an acronym for Secure SHell. It is a network protocol that allows data to be exchanged using a secure channel between two networked devices. The encryption used by SSH provides confidentiality and integrity of data over an insecure network. The goal of SSH was to replace the earlier rlogin, TELNET and rsh protocols, which did not provide strong authentication or guarantee confidentiality (Wikipedia).

SSM

SSM In SyncE this is an abbreviation for Synchronization Status Message and is containing a QL indication.

STP

Spanning Tree Protocol is an OSI layer-2 protocol which ensures a loop free topology for any bridged LAN. The original STP protocol is now obsolete by RSTP.

Switch ID

Switch IDs (1-16) are used to uniquely identify the switches within a stack. The Switch ID of each switch is shown on the display on the front of the switch and is used widely in the web pages as well as in the CLI commands.

SyncE

SyncE Is an abbreviation for Synchronous Ethernet. This functionality is used to make a network 'clock frequency' synchronized. Not to be confused with real time clock synchronized (IEEE 1588).

T

TACACS+

TACACS+ is an acronym for Terminal Acess Controller Access Control System Plus. It is a networking protocol which provides access control for routers, network access servers and other networked computing devices via one or more centralized servers. TACACS+ provides separate authentication, authorization and accounting services.

Tag Priority

Tag Priority is a 3-bit field storing the priority level for the 802.1Q frame.

TCP

TCP is an acronym for Transmission Control Protocol. It is a communications protocol that uses the Internet Protocol (IP) to exchange the messages between computers.

The TCP protocol guarantees reliable and in-order delivery of data from sender to receiver and distinguishes data for multiple connections by concurrent applications (for example, Web server and e-mail server) running on the same host.

The applications on networked hosts can use TCP to create connections to one another. It is known as a connection-oriented protocol, which means that a connection is established and maintained until such time as the message or messages to be exchanged by the application programs at each end have been exchanged. TCP is responsible for ensuring that a message is divided into the packets that IP manages and for reassembling the packets back into the complete message at the other end.

Common network applications that use TCP include the World Wide Web (WWW), e-mail, and File Transfer Protocol (FTP).

TELNET

TELNET is an acronym for TELetype NETwork. It is a terminal emulation protocol that uses the Transmission Control Protocol (TCP) and provides a virtual connection between TELNET server and TELNET client.

TELNET enables the client to control the server and communicate with other servers on the network. To start a Telnet session, the client user must log in to a server by entering a valid username and password. Then, the client user can enter commands through the Telnet program just as if they were entering commands directly on the server console.

TFTP

TFTP is an acronym for Trivial File Transfer Protocol. It is transfer protocol that uses the

User Datagram Protocol (UDP) and provides file writing and reading, but it does not provide directory service and security features.

U

UDP

UDP is an acronym for User Datagram Protocol. It is a communications protocol that uses the Internet Protocol (IP) to exchange the messages between computers.

UDP is an alternative to the Transmission Control Protocol (TCP) that uses the Internet Protocol (IP). Unlike TCP, UDP does not provide the service of dividing a message into packet datagrams, and UDP doesn't provide reassembling and sequencing of the packets. This means that the application program that uses UDP must be able to make sure that the entire message has arrived and is in the right order. Network applications that want to save processing time because they have very small data units to exchange may prefer UDP to TCP.

UDP provides two services not provided by the IP layer. It provides port numbers to help distinguish different user requests and, optionally, a checksum capability to verify that the data arrived intact.

Common network applications that use UDP include the Domain Name System (DNS), streaming media applications such as IPTV, Voice over IP (VoIP), and Trivial File Transfer Protocol (TFTP).

User Priority

User Priority is a 3-bit field storing the priority level for the 802.1Q frame. It is also known as PCP.

V

VLAN

Virtual LAN. A method to restrict communication between switch ports. VLANs can be used for the following applications:

VLAN unaware switching: This is the default configuration. All ports are VLAN unaware with Port VLAN ID 1 and members of VLAN 1. This means that MAC addresses are learned in VLAN 1, and the switch does not remove or insert VLAN tags.

VLAN aware switching: This is based on the IEEE 802.1Q standard. All ports are VLAN aware. Ports connected to VLAN aware switches are members of multiple VLANs and transmit tagged frames. Other ports are members of one VLAN, set up with this Port VLAN ID, and transmit untagged frames.

Provider switching: This is also known as Q-in-Q switching. Ports connected to subscribers are VLAN unaware, members of one VLAN, and set up with this unique Port VLAN ID. Ports connected to the service provider are VLAN aware, members of multiple VLANs, and set up to tag all frames. Untagged frames received on a subscriber port are forwarded to the provider port with a single VLAN tag. Tagged frames received on a subscriber port are forwarded to the provider port with a double VLAN tag.

VLAN ID

VLAN ID is a 12-bit field specifying the VLAN to which the frame belongs.

Voice VLAN

Voice VLAN is VLAN configured specially for voice traffic. By adding the ports with voice devices attached to voice VLAN, we can perform QoS-related configuration for voice data, ensuring the transmission priority of voice traffic and voice quality.

Legal Information

Copyright

Copyright © 2015 by ZyXEL Communications Corporation.

The contents of this publication may not be reproduced in any part or as a whole, transcribed, stored in a retrieval system, translated into any language, or transmitted in any form or by any means, electronic, mechanical, magnetic, optical, chemical, photocopying, manual, or otherwise, without the prior written permission of ZyXEL Communications Corporation.

Published by ZyXEL Communications Corporation. All rights reserved.

Disclaimer

ZyXEL does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. ZyXEL further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

Regulatory Notice and Statement

United States of America

Federal Communications Commission (FCC) EMC Statement

• This device complies with Part 15 of FCC rules. Operation is subject to the following two conditions:

(1) This device may not cause harmful interference.

(2) This device must accept any interference received, including interference that may cause undesired operations.

• Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

• This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules.

These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

Canada

The following information applies if you use the product within Canada area

Industry Canada ICES statement

CAN ICES-3 (A)/NMB-3(A)

European Union

The following information applies if you use the product within the European Union.

CE EMC statement

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

List of National Codes

Country	ISO 3166 2 letter code	Country	ISO 3166 2 letter code
Austria	AT	Liechtenstein	LI
Belgium	BE	Lithuania	LT
Bulgaria	BG	Luxembourg	LU
Croatia	HR	Malta	MT
Cyprus	CY	Netherlands	NL
Czech Republic	CZ	Norway	NO
Denmark	DK	Poland	PL
Estonia	EE	Portugal	PT
Finland	FI	Romania	RO
France	FR	Serbia	RS
Germany	DE	Slovakia	SK
Greece	GR	Slovenia	SI
Hungary	HU	Spain	ES
Iceland	IS	Switzerland	CH
Ireland	IE	Sweden	SE
Italy	IT	Turkey	TR
Latvia	LV	United Kingdom	GB

Notices
CLASS 1 LASER PRODUCT
APPAREIL À LASER DE CLASS 1
PRODUCT COMPLIES WITH 21 CFR 1040.10 AND 1040.11.
PRODUIT CONFORME SELON 21 CFR 1040.10 ET 1040.11.

Safety Warnings
・ Do NOT use this product near water, for example, in a wet basement or near a swimming pool.
・ Do NOT expose your device to dampness, dust or corrosive liquids.
・ Do NOT store things on the device.
・ Do NOT install, use, or service this device during a thunderstorm. There is a remote risk of electric shock from lightning.
・ Do not obstruct the device ventillation slots as insufficient airflow may harm your device.
・ Connect ONLY suitable accessories to the device.
・ Do NOT open the device or unit. Opening or removing covers can expose you to dangerous high voltage points or other risks. ONLY
qualified service personnel should service or disassemble this device. Please contact your vendor for further information.
・ Make sure to connect the cables to the correct ports.
・ Place connecting cables carefully so that no one will step on them or stumble over them.
・ Always disconnect all cables from this device before servicing or disassembling.
・ Use ONLY an appropriate power adaptor or cord for your device. Connect it to the right supply voltage (for example, 110V AC in North
America or 230V AC in Europe).
・ Use ONLY power wires of the appropriate wire gauge for your device. Connect it to a power supply of the correct voltage.
・ Do NOT allow anything to rest on the power adaptor or cord and do NOT place the product where anyone can walk on the power adaptor or cord.
・ Do NOT use the device if the power adaptor or cord is damaged as it might cause electrocution.
・ If the power adaptor or cord is damaged, remove it from the device and the power source.
・ Do NOT attempt to repair the power adaptor or cord. Contact your local vendor to order a new one.
・ Fuse Warning! Replace a fuse only with a fuse of the same type and rating.
・ The POE (Power over Ethernet) devices that supply or receive power and their connected Ethernet cables must all be completely indoors.

Environment Statement

WEEE Directive

Your product is marked with this symbol, which is known as the WEEE mark. WEEE stands for Waste Electronics and Electrical Equipment. It means that used electrical and electronic products should not be mixed with general waste. Used electrical and electronic equipment should be treated separately.

"INFORMAZIONI AGLI UTENTI"
Ai sensi della Direttiva 2012/19/UE del Parlamento europeo e del Consiglio, del 4 luglio 2012, sui rifiuti di apparecchiature elettriche ed elettroniche (RAEE)
Il simbolo del cassonetto barrato riportato sull'apparecchiatura o sulla sua confezione indica che il prodotto alla fine della propria vita utile deve essere raccolto separatamente dagli altri rifiuti.
La raccolta differenziata della presente apparecchiatura giunta a fine vita è organizzata e gestita dal produttore. L'utente che vorrà disfarsi della presente apparecchiatura dovrà quindi contattare il produttore e seguire il sistema che questo ha adottato per consentire la raccolta separata dell'apparecchiatura giunta a fine vita. L'adeguata raccolta differenziata per l'avvio successivo dell'apparecchiatura dismessa al riciclaggio, al trattamento e allo smaltimento ambientalmente compatibile contribuisce ad evitare possibili effetti negativi sull'ambiente e sulla salute e favorisce il reimpiego e/o riciclo
dei materiali di cui è composta l'apparecchiatura.
Lo smaltimento abusivo del prodotto da parte del detentore comporta l'applicazione delle sanzioni amministrative previste dalla normativa vigente."

Environmental Product Declaration

Български (Bulgarian)

Екологична продуктова декларация

RoHS	Директива 2011/65/EC
WEEE	Директива 2012/19/EC
PPW	Директива 94/62/EO
REACH	РЕГЛАМЕНТ (EO) № 1907/2006

Име/титла: Richard Hsu / Quality Management Division Senior Manager
Лодпис: Дата (дд/мм/гггг): 01/10/2014

Ceština (Czech)

Environmentální prohlášení o produktu

RoHS	Směrnice 2011/65/EU
WEEE	Směrnice 2012/19/EU
PPW	Směrnice 94/62/ES
REACH	Nařízení (ES) č. 1907/2006

Jméno/Podpis: Richard Hsu / Quality Management Division Senior Manager
Datum (dd/mm/rrrr): 01/10/2014

Dansk (Danish)

Miljøvaredeklaration

RoHS	Direktiv 2011/65/EU
WEEE	Direktiv 2012/19/EU
PPW	Direktiv 94/62/EF
REACH	Forordning (EF) nr. 1907/2006

Navn/Underskrift: Richard Hsu / Quality Management Division Senior Manager
Dato (dd/mm/áááá): 01/10/2014

Deutsch (German)

Produkt-Umweltdeklaration

RoHS	Richtlinie 2011/65/EU
WEEE	Richtlinie 2012/19/EU
PPW	Richtlinie 94/62/EG
REACH	VERORDNUNG (EG) Nr.1907/2006

Name/Unterschrift: Richard Hsu / Quality Management Division Senior Manager
Datum (jjj/mm/tt): 2014/10/01

Eesti keel (Estonian)

Toote keskkonnadeklaratsiooni

RoHS	Direktiiv 2011/65/EL
WEEE	Direktiiv 2012/19/EL
PPW	Direktiiv 94/62/EÜ
REACH	MÄÄRUS (EÜ) nr 1907/2006

Nimi/pealkiri/Allkiri: Richard Hsu / Quality Management Division Senior Manager
Kuupäev (pp/kk/aaaa): 01/10/2014

English

Environmental product declaration

RoHS	Directive 2011/65/EU
WEEE	Directive 2012/19/EU
PPW	Directive 94/62/EC
REACH	Regulation (EC) No 1907/2006

Name/title/Signature: Richard Hsu / Quality Management Division Senior Manager
Date (dd/mm/yyyy): 01/10/2014

Español (Spanish)

Declaraciones Ambientales de Producto

RoHS	Directiva 2011/65/UE
WEEE	Directiva 2012/19/UE
PPW	Directiva 94/62/CE
REACH	REGLAMENTO (CE) nº 1907/2006

Nombre/título/Firma: Richard Hsu / Quality Management Division Senior Manager
Fecha (aaaa/mm/dd): 2014/10/01

Français (French)

Profil environnemental de produit

RoHS	Directive 2011/65/UE
WEEE	Directive 2012/19/UE
PPW	Directive 94/62/CE
REACH	RÈGLEMENT (CE) N° 1907/2006

Nom/titre/Signature: Richard Hsu / Quality Management Division Senior Manager
Date (aaaa/mm/jj): 2014/10/01

Hrvatski (Croatian)

Deklaraciju o zbrinjavanju proizvoda

RoHS	Direktiva 2011/65/EU
WEEE	Direktiva 2012/19/EU
PPW	Direktiva 94/62/EZ
REACH	Uredbe (EZ) br. 1907/2006

Ime/naslov/Potpis: Richard Hsu / Quality Management Division Senior Manager
Datum (dd/mm/yyyy): 01/10/2014

Italiano (Italian)

Dichiarazione ambientale di prodotto

RoHS	Direttiva 2011/65/UE
WEEE	Direttiva 2012/19/UE
PPW	Direttiva 94/62/CE
REACH	REGOLAMENTO (CE) n. 1907/2006

Nome/titolo/Firma: Richard Hsu / Quality Management Division Senior Manager
Data (aaaa/mm/gg): 2014/10/01

Latviešu valoda(Latvian)

Produkta vides ietekmējuma deklarācija

RoHS	Direktīva 2011/65/ES
WEEE	Direktīva 2012/19/ES
PPW	Direktīva 94/62/EB
REACH	Regula (EK) Nr. 1907/2006

Nosaukum s/ tituls/Paraksts: Richard Hsu / Quality Management Division Senior Manager
Datums(dd/mm/gggg): 01/10/2014

Lietuvių kalba (Lithuanian)

Aplinkosauginę gaminio deklaraciją

RoHS	Direktyva 2011/65/ES
WEEE	Direktyva 2012/19/ES
PPW	Direktyva 94/62/EB
REACH	REGLAMENTAS (EB) Nr. 1907/2006

Vardas/titulas/Parašas: Richard Hsu / Quality Management Division Senior Manager
Data (dd/mm/mmmm): 01/10/2014

Magyar (Hungarian)

Környezetvédelmi terméknyilatkozatot

RoHS	2011/65/EU Irányelve
WEEE	2012/19/EU Irányelve
PPW	94/62/EK Irányelve
REACH	1907/2006/EK Rendelete

Név/cím/Aláírás: Richard Hsu / Quality Management Division Senior Manager
Dátum (éééé/hh/nn): 2014/10/01

Malti (Maltese)

Dikjarazzjoni Ambjentali dwar il-Prodott

RoHS	Direttiva 2011/65/UE
WEEE	Direttiva 2012/19/EU
PPW	Direttiva 94/62/KE
REACH	REGOLAMENT (KE) NRU 1907/2006

Isem/titolu/Firma: Richard Hsu / Quality Management Division Senior Manager
Data (ssss/xx/jj): 2014/10/01

Nederlands (Dutch)

Milieuproductverklaring

RoHS	Richtlijn 2011/65/EU
WEEE	Richtlijn 2012/19/EU
PPW	Richtlijn 94/62/EG
REACH	Verordening (EG) nr. 1907/2006

Naam/titel/Handtekening: Richard Hsu / Quality Management Division Senior Manager
Datum (dd/mm/jaar): 01/10/2014

Polski (Polish)

Deklarację środowiskową produktu

RoHS	Dyrektywa 2011/65/UE
WEEE	Dyrektywa 2012/19/UE
PPW	Dyrektywa 94/62/WE
REACH	Rozporządzenie (WE) nr 1907/2006

Nazwisko/tytuł/Podpis: Richard Hsu / Quality Management Division Senior Manager
Data (rrrr/mm/dd): 2014/10/01

Português (Portuguese)

Declaração ambiental do produto

RoHS	Directiva 2011/65/UE
WEEE	Directiva 2012/19/UE
PPW	Directiva 94/62/CE
REACH	Regulamento (CE) n.º 1907/2006

Nome/título/Assinatura: Richard Hsu / Quality Management Division Senior Manager
Data (dd/mm/aaaa): 01/10/2014

Română (Romanian)

Declaraţie de mediu privind produsele

RoHS	Directiva 2011/65/UE
WEEE	Directiva 2012/19/UE
PPW	Directiva 94/62/CE
REACH	REGULAMENTUL (CE) NR.907/2006

Numele/titlu/Semnătura: Richard Hsu / Quality Management Division Senior Manager
Data (zz/ll/aaaa): 01/10/2014

Slovenčina (Slovak)

Vyhlásenie o environmentálnom výrobku

RoHS	Smernica 2011/65/EU
WEEE	Smernica 2012/19/EU
PPW	Smernica 94/62/ES
REACH	Nariadenie (ES) č. 1907/2006

Meno/titul/Podpis: Richard Hsu / Quality Management Division Senior Manager
Dátum (dd/mm/rrrr): 01/10/2014

Slovenščina (Slovene)

Okoljsko deklaracijo izdelka

RoHS	Direktiva 2011/65/EU
WEEE	Direktiva 2012/19/EU
PPW	Direktiva 94/62/ES
REACH	Uredba (ES) št. 1907/2006

Ime/naziv/Podpis: Richard Hsu / Quality Management Division Senior Manager
Datum (dd/mm/llll): 01/10/2014

Suomi (Finnish)

Standardiin perustuva ympäristötuoteseloste

RoHS	Direktiivi 2011/65/EU
WEEE	Direktiivi 2012/19/EU
PPW	Direktiivi 94/62/EY
REACH	ASETUS (EY) N:o 1907/2006

Nimi/otsikko/Allekirjoitus: Richard Hsu / Quality Management Division Senior Manager
Päivämäärä (pp/kk/vvvv): 01/10/2014

Svenska (Swedish)

Miljöproduktdeklaration

RoHS	Direktiv 2011/65/EU
WEEE	Direktiv 2012/19/EU
PPW	Direktiv 94/62/EG
REACH	Förordning (EG) nr 1907/2006

Namn/titel/Namnteckning: Richard Hsu / Quality Management Division Senior Manager
Datum (dd/mm/åååå): 01/10/2014

Ελληνικά (Greek)

Περιβαλλοντική δήλωση προϊόντος

RoHS	Οδηγία 2011/65/EE
WEEE	Οδηγία 2012/19/EE
PPW	Οδηγία 94/62/EK
REACH	Κανονισμος (EK) αριθ. 1907/2006

Όνομα/ίτλος/Υπογραφή: Richard Hsu / Quality Management Division Senior Manager
Ημερομηνία (ηη/μμ/εεεε): 01/10/2014

Norsk (Norwegian)

Miljødeklarasjon

RoHS	Direktiv 2011/65/EU
WEEE	Direktiv 2012/19/EU
PPW	Direktiv 94/62/EF
REACH	Forordning (EF) nr. 1907/2006

Navn/tittel/Signatur: Richard Hsu / Quality Management Division Senior Manager
Dato (dd/mm/åååå): 01/10/2014

Taiwanese BSMI (Bureau of Standards, Metrology and Inspection) A Warning:

警告使用者
這是甲類的資訊產品，在居住的環境使用時，
可能造成射頻干擾，在這種情況下，
使用者會被要求採取某些適當的對策.

Viewing Certifications
Go to http://www.zyxel.com to view this product's documentation and certifications.

ZyXEL Limited Warranty
ZyXEL warrants to the original end user (purchaser) that this product is free from any defects in material or workmanship for a specific period (the Warranty Period) from the date of purchase. The Warranty Period varies by region. Check with your vendor and/or the authorized ZyXEL local distributor for details about the Warranty Period of this product. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, ZyXEL will, at its discretion, repair or replace the defective products or components without charge for either parts or labor, and to whatever extent it shall deem necessary to restore the product or components to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal or higher value, and will be solely at the discretion of ZyXEL. This warranty shall not apply if the product has been modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

Note
Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose. ZyXEL shall in no event be held liable for indirect or consequential damages of any kind to the purchaser.
To obtain the services of this warranty, contact your vendor. You may also refer to the warranty policy for the region in which you bought the device at http://www.zyxel.com/web/support_warranty_info.php.

Registration
Register your product online to receive e-mail notices of firmware upgrades and information at www.zyxel.com for global products, or at www.us.zyxel.com for North American products.

Trademarks
Other trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

Open Source Licenses
This product contains in part some free software distributed under GPL license terms and/or GPL like licenses. Open source licenses are provided with the firmware package. You can download the latest firmware at www.zyxel.com. To obtain the source code covered under those Licenses, please contact support@zyxel.com.tw to get it.