NEXT-POE4008L2-130

8 Port 10/100/1000Mbps PoE and Gigabit combo SFPs/ RJ-45s Web managed Switch

User's Manual

CONTENTS

Revision History

Version	Date	Author	Changes from Previous Version
1.0	April 28, 2015	Mori/Jes	Released

Safety Warning

Purpose

This manual gives specific information on how to operate and use the management functions of this switch.

Audience

This manual is intended for use by network administrators who are responsible for operating and maintaining network equipments ; consequently, it assumes a basic network network knowledge of general switch functions, the Internet Protocol (IP), IEEE 802.3at/af Power over Ethernet Standard and Simple Network Management Protocol(SNMP).

FCC Warning

This device has been tested and found to comply with limits for a Class A digital device, pursuant to Part 15 of 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 and radiates radio frequency energy and, if not installed and used in accordance with the user's manual, it may cause interference in which case users will be required to correct interference at their own expenses.

CE Warning

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

Chapter 1 Introduction

This chapter provides an overview of this PoE Web Smart switch, and introduces the key features and supported specifications of this PoE Web Smart switches.

PRODUCT OVERVIEW

This PoE switch is a PoE L2+ Managed switch equiped with 8-ports 10/100/1000BaseT(X) plus 2-ports gigabit SFP open slots. It provides a broad range of features for Layer 2+ switching and fully 802.3at/af PoE/PoE+ functions.
It was designed for easy installation and high performance in an environment where the traffic is on the network and the number of users increases continuously. The smart and efficient power design can improve the power saving.

FEATURES

Features	Descriptions
Dual Images	Prevent any kind of upgrading process failure
IPv4	Supports IPv4 addressing, management and QoS
Log	Support local and remote syslog server with 3 levels(Info, Warning, Error)
Power Saving	ActiPHY, PerfectReach LED Power management Thermal Protection
Security	Private VLAN(Static) ACLs for filtering, policing, and port copy, including ACL wizards

	(continued)
Authentication	Telnet, Web - username/password Telnet - SSH SNMP v1/2c – Community strings SNMP version 3 – MD5 or SHA password Port-based 802.1X
Port Limiting	Input rate limiting per port(manual setting or ACL)
Port Configuration	Speed, Duplex mode, Flow control, MTU, Power saving mode
Port Mirroring	1 sessions, up to 10 source port to one analysis port per session
Port Trunking	IEEE 802.3ad Link Aggregation, static and LACP
Spanning Tree Algorithm	Supports standard STP, Rapid Spanning Tree Protocol (RSTP)
IEEE 802.1D Bridge	Supports dynamic data switching and addresses learning
Quality of Service	Traffic classes(1,2, or 4/8 active priorities) Storm control for UC, MC and BC
DHCP	Client
Configuration	Save and Restore configuration
Firmware	Upgrade & firmware image switch using Web & console port
CLI command	Support Cli command with console port (Baudrate:115200, DataBit:8, Parity: N,StopBit 1)

SPECIFICATIONS

Standard
IEEE 802.3at/af Power over Ethernet(PoE/PoE+)
IEEE 802.3ad Link Aggregation
IEEE 802.3x Flow Control
IEEE 802.1x Port-based Network Access Control
IEEE 802.1Q VLAN Tagging
IEEE 802.1d Spanning Tree Protocol
IEEE 802.1w Rapid Spanning Tree Protocol
8 integrated IEEE 802.3ab-compliant 10/100/1000BASE-T Ethernet
MIBs
RFC 1213 MIB II
RFC 3411 SNMP Management Frameworks
RFC 3621 LLEP-MED Power
RFC 3635 Ethernet-like MIB
RFC 4188 Bridge MIB
IEEE 802.1AB LLDP MIB

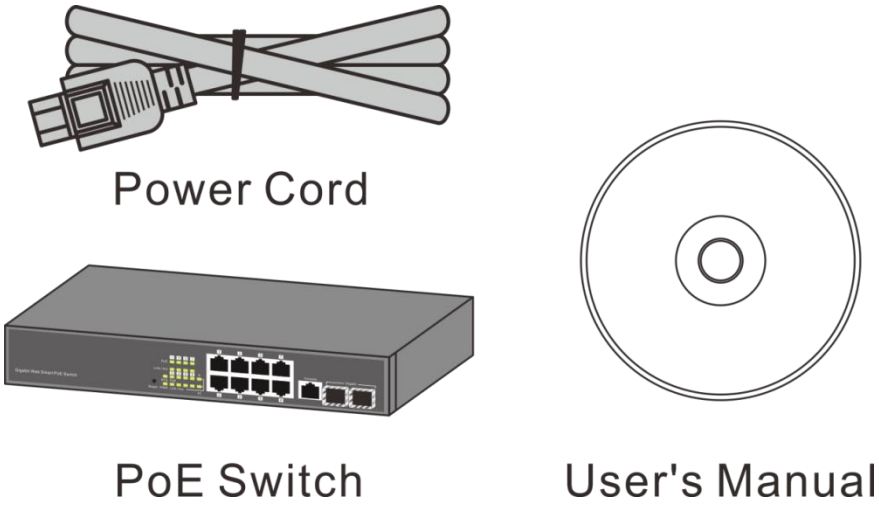
PERFORMANCES

Information
MAC Address : 8K , 4K VLAN support
Packet Memory : 4 Megabits of Integrated shared memory
Jambo Frame : 9.6K
Transmission Method : Store and Forward

PACKING

Before you start to install this switch, please verify your package that contains the following items:

- One PoE 8+2-port Gigabit Ethernet Switch
- One Power Cord
- One User’s Manual (CD disk)



Note: If any of these items is found missing or damaged, please contact your local supplier for replacement.

Chapter 2 Hardware Descriptions

This chapter primarily presents hardware of the PoE switch,
physical dimenstions and functional overview would be described.

DIMENSION AND WEIGHT

263 x 160 x 44 mm (H x W x D) / 1.5kg

FRONT PANEL

The Front Panel of the PoE L2+ managed switch consists of 8-port gigabit ethernet port and 2-port gigabit SFP open slot. The LED indicators are also located on the Front Panel.

LED INDICATORS

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

LED	Status	Description
Power	Orange	System on
	Nil	System off
PoE	Orange	Port is linked to Power Device
	Nil	No Power Device is connected
Link/ACT	Green and Flashing	Link and Data Activating
	Nil	Port is disable or disconnected

REAR PANEL

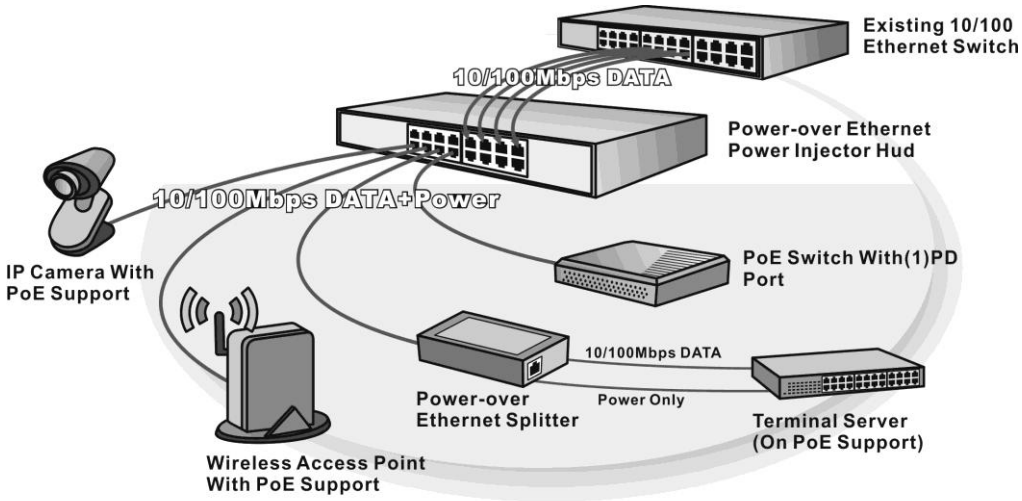
The 3-pronged power plug is placed at the rear panel of the PoE Web Smart Switch right side show as below:

HARDWARE INSTALLATION

Installing Equipment

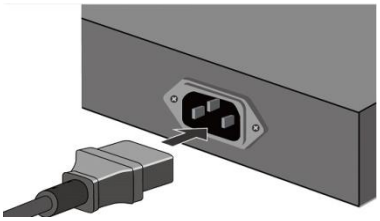
You can mount the this device into a standard 19-inch equipment rack. You can center- or front-mount the device in a rack. Optional rack-mounting brackets are supplied with the device.

Connecting Networking



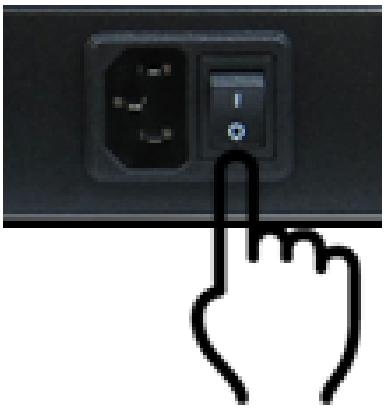
Connecting Power

The AC power cord shipped with the device connects the device to earth ground when plugged into an AC grounding-type power outlet. The device must be connected to earth ground during normal operation. To connect power to the device, plug one end of the AC power cord into the AC power appliance inlet on the back panel of the device. Plug the other end into an AC power source.



Power ON/OFF Device

To power on this device, press the AC power switch on the rear panel to the on position. The POWER LED lights during startup and remains on steadily when the device is operating normally. To power off this device, press the power switch to the OFF position.



Chapter 3 Web Management

This chapter provides the entire L2+ managed switch features, along with a detailed description of how to configure each feature via web interface.

Initial Switch Configuration

This part guides you to configure and manage this switch through the web interface. With this facility, you can easily configure and monitor through any one port of this switch.

Start up by the following steps:

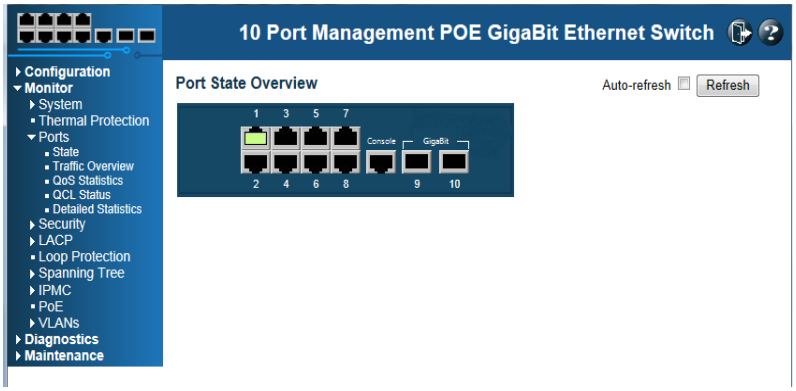
1. Place the switch close to your PC/NB that you intend to use for configuration. It will help you to check the status of the switch by LED in front panel while working on your PC/NB.
2. Connect the Ethernet port of your PC/NB to any port on the front panel of the switch. Turn the switch on and make sure the connectivity by checking LED in the front panel of the switch.
3. Configure your PC's IP address the same subnet with the switch's.
   The following table describes the default necessary login Information:
   Login Information

IP Address	192.168.2.1
IP Mask	255.255.255.0
IP Router	0.0.0.0
Username	admin
Password	

4. Open the web browser, and go to 192.168.2.1Site then the login windows will pop out. Key in the username "admin" and leave password blank then clicks OK.

Figure 3-1.

5. **After you login successfully, you will see the home page is displayed as shown below. The home page display the Menu Bar on the left side of the screen and show the front panel port states on the right side.**



Before you start to configure, we strongly recommended you to change the password. To change the password, click Security and then Switch. Fill old and new password in Password tab.

WEB Interface

Configuration Option Configurable parameters have seveal forms : text field, drop-down list, radio button and checkbox. Once you change the parameters, please make sure to click Save button to apply

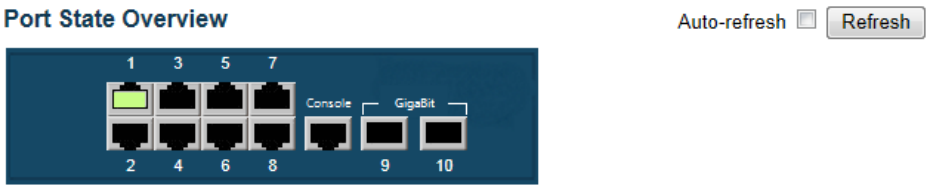
The following table provides the description of each button:

Configuration buttons

Button	Description
Save	Set specific value into the Switch
Reset	Restore the parameters to previous saving value
	Show the help information for selected page
	Logout the management web interface of the switch

Front Panel

The default page after you login successfully is port states' page. The port 1 to port 8 are gigabit Ethernet port and port 9 and 10 are SFP slot. When the port image is green, it means this port is connected. Auto-refresh mode is disable by default setting. It will update the current port state by 5 seconds if you check it. Or you can click Refresh button to update the states manually. Click the each port image will open detailed statstics of selected port.



MENU TREE

There is a Menu Tree in the left side of Web management system with 4 categories: Configuration, Monitor, Diagnostic and Maintenance. The follow table has a breifly description of each tab.

MENU TREE

Menu	Descriptions
▶**Configuration**	
▶System	
■Information	Configures system contact, name, location and timezone offset
■IP & Time	Configures IPv4 (Statics IP Address, DHCP client), VLAN ID and SNTP settings
■Log	Configures Remote system log Server which 3 levels(Infor, Warning, Error)
▶Power Reductinon	
■LED	Reduces LED intensity during specified hours and configure link change at error settings
■Thermal Protection	Configures temperature 4 priority levels and each value. Port will shut-down if the temperature exceeded the assigned value.
■Ports	Configures ports' connection settings
▶Secuirty	
▶Switch	
■Password	Change the new password
■Auth Method	Configures authentication method for console and web access via local database and RADIUS

Table. MENU TREE (Continue)

Menu	Descriptions
▶SNMP	
■System	Configures read-only and R/W community strings for SNMP v1/v2c, engine ID for SNMP v3, and trap parameters
■ Communities	Configures community strings
■Users	Configures SNMP v3 users on this switch
■Groups	Configures SNMP v3 groups
■Views	Configures SNMP v3 views
■Access	Assigns security model, Security level, and R/W views to SNMP groups
▶Network	
■ACL	Access Control Lists
■AAA	Configures RADIUS authentication server.(Max 5 Server supported)
▶Port Trunking	
■Static	Speifies ports to group into static trunks
■LACP	Allows ports to join trunk dynamically
■Loop Protection	Configure ports to shutdown if the ports are in loop
▶Spanning Tree	
■Bridge Setting	1. Configures global bridge setting for STP and RSTP 2. Configures edge port setting for BPDU filtering, BPDU guard and port error recovery

MENU TREE (Continue)

Menu	Descriptions
■Bridge Ports	Configure CIST port, priority and path cost
▶IPMC	
▶IGMP Snooping	
■Basic Configuration	Configures global and related port setting
■VLAN Configuration	Configures IGMP snooping per VLAN group
■PoE	Configures total power supply and each PoE port type(PoE/PoE++/disabled)
▶VLANs	
■VLAN Membership	Configures VLAN groups
■Ports	Specifies default PVID and VLAN atrributes
▶Private VLANs	
■PVLAN Membership	Configures PVLAN groups
■Port isolation	Configures Port isolation
▶QoS	
■Port Classification	Configures QoS Ingress Classification Settings for all ports
■Port Policing	Configures QoS ingress Port policers to constrain traffic flows and mark frames by specific rate
■QoS Control List	Configures QoS Control Entry based on parameters such as VLAN ID, UDP/TCP port, IPv4 DSCP or Tag Priority
■Storn Control	Set limitation for broadcast, unicast and multicast traffic

MENU TREE (Continue)

Menu	Descriptions
■Mirroring	Set source and destination port for mirroring
▶**Monitor**	
▶System	
■Information	Displays system contact, name, location, switch's MAC address, system time, firmware version
■CPU load	Displays CPU load by realtime SVG graph
■Log	Displays logged message with selected level (Info, Warning, Error, All)
■Detailed Log	Displays fully logged message
■Thermal Protection	Shows the current port temperature and status
▶Ports	
■State	Displays a graphic image of the front panel to indicate current port states
■Traffic Overview	Shows the basic port statistics
■QoS Statistics	Shows the count of incoming and outgoing egress queues
■QCL Status	Shows the QoS Control Lists status
■Detailed Statistics	Shows the detailed port statistics
▶Security	
▶Network	
■ACL Status	Shows the ACL status by different ACL users

MENU TREE (Continue)

Menu	Descriptions
▶AAA	
■RADIUS Overview	Displays the status of associated authentication RADIUS servers
■RADIUS Details	Displays the traffic and status of each associated RADIUS server
▶LACP	
■System Status	Displays each local port's LACP information included Aggr ID, Partner system ID and Parter key
■Port Status	Displays each local port's Key, Aggr ID, Partner system ID and Parnter port
■Port Statistics	Displays statistics for LACP protocol message
■Loop Protection	Display loop status for each port
▶Spanning Tree	
■Bridge Status	Displays STP detailed bridge status, CIST Ports and Aggregations state
■Port Status	Displays CIST role, State and uptime for each port
■Port Statistics	Displays statistics for RSTP, STP and TCN packets
▶IPMC	
▶IGMP Snooping	
■Status	Displays statistics related to IGMP packets passed upstream to the IGMP Querier or downstream to multicast clients

MENU TREE (Continue)

Menu	Descriptions
■Groups Information	Displays IGMP snooping groups information
■PoE	Displays total power consumption, PD class and power usage for each associated port
▶VLANs	
■VLAN Membership	Show the port members for specific VLAN ID
■VLAN Port	Shows the VLAN Port Status for Static user
▶**Diagnostics**	
■Ping	Tests specific IP Address by using ping function
▶**Maintenance**	
■Restart Device	Restarts the device
■Factory Defaults	Restores all settings to manufactory default
▶Software	
■Upload	Updates firmware of this switch through Web UI
■Image Select	Selects a rescovery firmware to boot up the device
▶Configuration	
■Save	Saves configuration to your local management PC
■Upload	Restores the previous configuration from a file

System Information

Using System Information page to set System Contact, Name, Location, Timezone offset

LOCATION：

▼ Configuration

▼ System

- Information

PARAMETERS：

Items	Description
System Contact	Administrator is responsible for this device (Maximum Length：255 characters)
System Name	Name of this device (Maximum Length：255 characters)
System Location	Sets the location of this device (Maximum Length：255 characters)
System Timezone offset (minutes)	Sets the timezone as an offset from Greenwich Mean Time(GMT), negative vale is meaning before GMT, postive value is meaning of after GMT (Range： -720~720)

Note the unit of system timezone is minute

WEB Interface

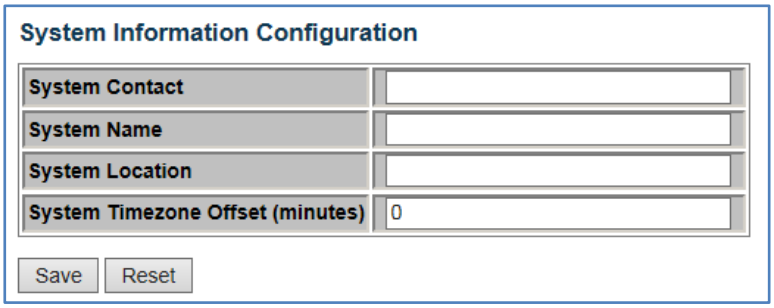
To configure System Information

A. Click *Configuration/System/Information*

B. Specify the System contact, Name, Location and

Timezone.

C. Click Save to apply the setting or Reset to restore the previous setting



IP & Time

Using IP & Time page to Configure Static IP Address or DHCP client, and SNTP server

LOCATION：

▼ Configuration

▼ System

■ IP & Time

PARAMETERS：

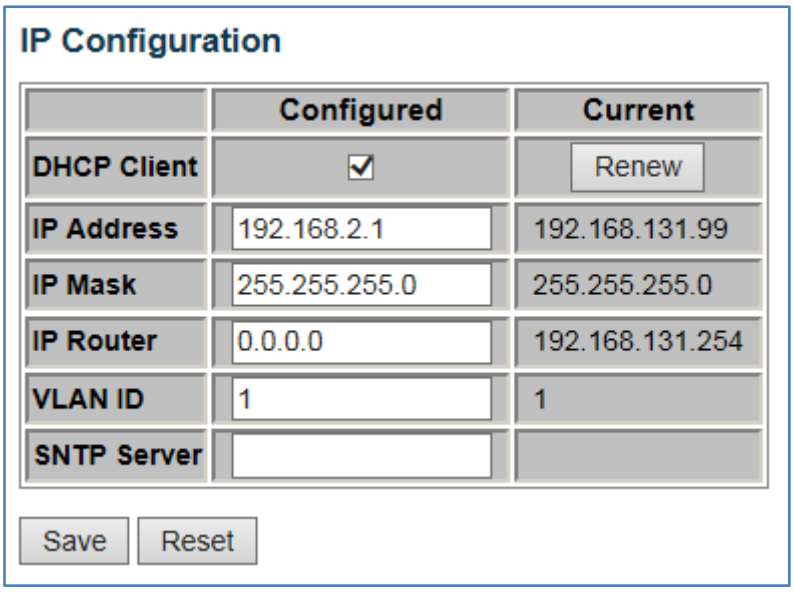
Items	Description
DHCP Client	Sets the checkbox in configured column to enable DHCP client or uncheck for static IP Address
IP Address	Address of the VLAN specified in the VLAN ID field. It should match with your management PC/NB's setting. (Default IP：192.168.2.1)
IP Mask	This mask identifies the host address bits

	used for routing to specific subnet.
IP Router	IP address of the gateway
VLAN ID	Default VLAN ID = 1, it needs to match your management PC/NB's VLAN ID. (Range：1~4096)
SNTP Server	SNTP Server's IP address
Renew	Clicks renew button to renew IP address

WEB Interface

To Configure Static IP address & DHCP Client enable/disable：

A. **Click *Configuration/System/IP&Time***
B. **Enable DHCP client vis set checkbox**
C. **Specify the IP address, IP Mask, IP Router and SNTP Server IP address**
D. **Click Renew button to renew IP Address under DHCP Client Enable mode**
E. **Click Save to apply the setting or Reset to restore the previous setting**



Log

Using Log page to configure remote system log server.

LOCATION：

▼ Configuration

▼ System

■ Log

PARAMETERS：

Items	Description
Server Mode	Enable or Disable remote system logging function
Server Address	Set IP address of remote system log server
Syslog Level	Choose the logging event level.

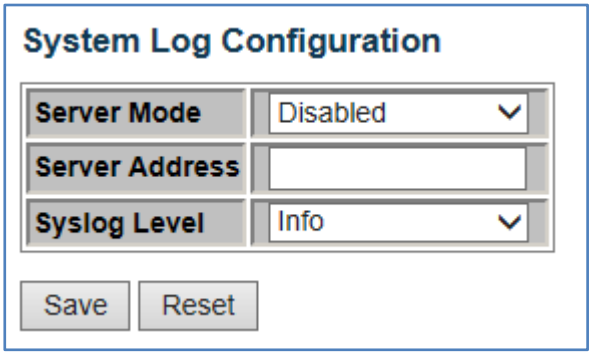
Info：send info, Warnings, Errors.

Warning：send Warnings and Errors

Error：send Errors

WEB Interface

A. **Click *Configuration/System/Log***
B. **Enable remote system logging, enter Server's IP Address, and choose what kind of logging level to record**
C. **Click Save to apply the setting or Reset to restore the previous setting**



Power Reduction (LED)

Using LED Power Reduction page to reduce LED intensity during specificed hour(s), the maximum setting range is 24 hours.

LOCATION：

▼ Configuration

▼ Power Reduction

- LED

PARAMETERS：

Items	Description
LED Intensity Timers	
Time Intensity	Time at which LED intensity is set LED Intensity (10 levels increase by 10%, 0%=LED off, 100%=LED full power)
Maintenance	
On time at link change	LED set full powr for a period of time(second) when a link change occurs.
On at errors	LED set full power when a link error occurs.

WEB Interface

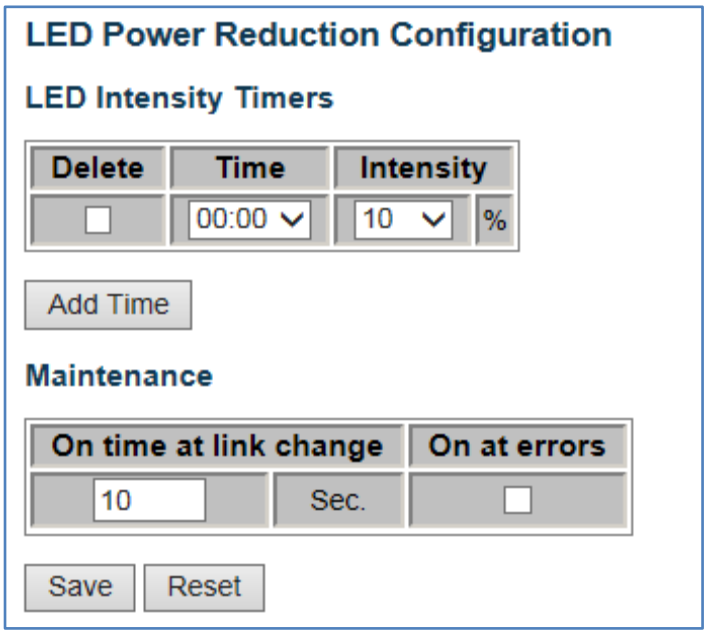
A. Click *Configuration/Power Reduction/LED*

B. Set LED intensity for corresponding hours, then click Add button to attach list

C. Set the duration of LED full power when a link change occurs

D. Set the duration of LED full power when a link error occurs

E. Click Save to apply the setting or Reset to restore the previous setting



Thermal Protection

Using the Thermal Protection page to set temperature priority levels and assign to designated port. The port will be shutdown if the temperature exceeds the set value.

LOCATION：

▼ Configuration

- Thermal Protection

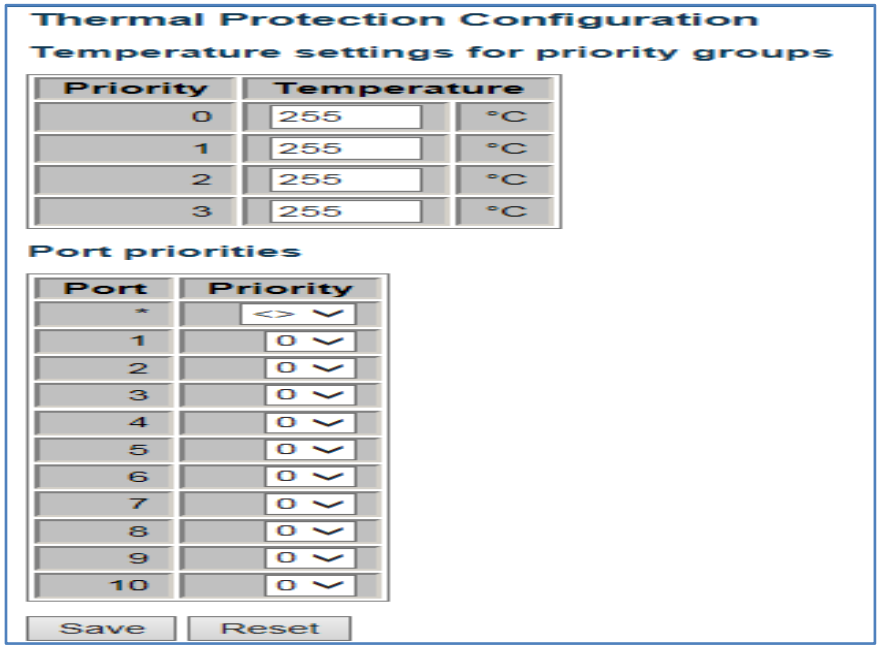
PARAMETERS：

Items	Description
Temperature settings for priority groups	
Temperature	Assign specific temperature for each priority (total = 4)
Port priorities	
Priority	Assign priority for each port

WEB Interface

A. Click *Configuration/Thermal Protection*

B. Set temperature for echo priority
C. Set each port with corresponding priority
D. Click Save to apply the setting or Reset to restore the previous setting



Ports

Using Port Configuration page to configure the detail parameters for each port. You can enable/disable each port and set port speed such as Auto, half-duplex, full-duplex for 10Mbps, 100Mbps, 1Gbps and disabled. It also allows to set frame size , collision policy and Power control.

LOCATION：

▼ Configuration

- Port

PARAMETERS：

Items	Description

Link Speed	Displays the status of the ports Current：Displays the current speed Configured ：There are 7 options Disabled ：disables the port interface Auto ：Enables auto-negotiation 10Mbps HDX：Support 10Mbps half-duplex 10Mbps FDX：Support 10Mbps full-duplex 100Mbps HDX：Support 100Mbps half-duplex 100Mbps FDX：Support 100Mbps full-duplex 1Gbps FDX：Support 1Gbps full-duplex
Flow Control	Current TX and Current RX indicate the Flow control state of TX and RX. Checks the configured box to enable Flow Control Flow control can eliminate packet loss. When auto-negotiation mode is set, this switch advertises the flow control information to linked partner. When the manual speed is set, the Current TX field indicates if the pause frame be transmitted from this port, and the Current RX field indicates whether the pasue frame are obeyed on this port
Maximum Frame Size	Set the Maximum frame size allows to transfer for each port
Excessive	Configure port transmit collision behavior

Collision Mode	Discard：Discards the frames after 16 collision happened. Restart：Restarts the backoff algorithm after 16 collision happened.
Power Control	There are 3 options for automatic power saving mode： ActiPHY：It will detect unused Ethernet ports on Network devices and power them down. PerfectReach：an intelligent algorithm that actively adjusts the power level needed based on cable length. Enabled：Enables both ActiPHY and PerfectReach Disabled：Disables power saving mechanism

WEB Interface

A. Click *Configuration/Port*

B. Specify the Speed Configured, Flow Control, Maximum Frame Size, Excessive Collision Mode and Power Control.

C. Click Save to apply the setting or Reset to restore the previous setting

- **Refresh button：Re-load information of the page manually.**

Port Configuration

Port	Link	Speed		Flow Control			Maximum Frame Size	Excessive Collision Mode	Power Control
		Current	Configured	Current Rx	Current Tx	Configured			
*			<>			☐	9600	<>	<>
1	🟢	100fdx	Auto	✕	✕	☐	9600	Discard	Disabled
2	🔴	Down	Auto	✕	✕	☐	9600	Discard	Disabled
3	🔴	Down	Auto	✕	✕	☐	9600	Discard	Disabled
4	🔴	Down	Auto	✕	✕	☐	9600	Discard	Disabled
5	🔴	Down	Auto	✕	✕	☐	9600	Discard	Disabled
6	🔴	Down	Auto	✕	✕	☐	9600	Discard	Disabled
7	🟢	1Gfdx	Auto	✕	✕	☐	9600	Discard	Disabled
8	🔴	Down	Auto	✕	✕	☐	9600	Discard	Disabled
9	🔴	Down	Auto	✕	✕	☐	9600		
10	🔴	Down	Auto	✕	✕	☐	9600		

Save Reset

Security

You can configure user authentication for management access and control client access ports

Password

Using this Password page to change the administrator's password.

LOCATION：

▼ Configuration

▼ Security

▼ Switch

- Password

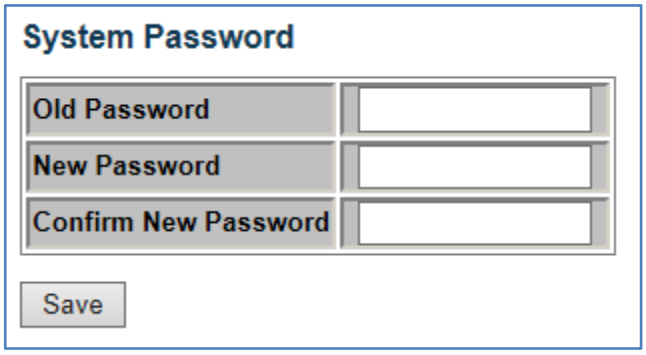
PARAMETERS：

Items	Description
Old Password	Insert the old password (Default is blank)
New Password	Inserts new password (Case sensitive, Maximum is 31 characters)
Confirm New	Re-types the same string as New

Password	Password field.

WEB Interface

A. **Click *Configuration/Security/Switch/Password***
B. **Enter Old Password, New Password, and Confirm New Password.**
C. **Click Save to apply the setting.**



Security

Auth Method

Using Authentication Method Configuration page to specify the authentication Method for access management via console and web. Access can be controlled by local(Password) or remote access authentication(RADIUS Server).

LOCATION：

▼ Configuration

▼ Security

▼ Switch

▪ Auth Method

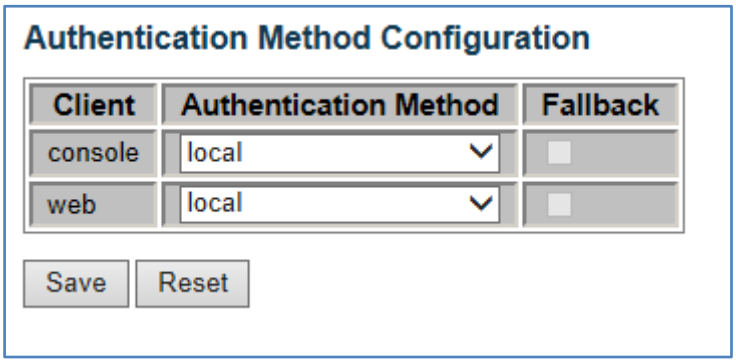
PARAMETERS：

Items	Description
Client	Specify the authentication Method

	for Administrator
Authentication Method	There are 3 options for Console and Web None：disables access vis specified management interface Local：checks by password RADIUS：checks vis RADIUS Server
Fallback	This only works for Authentication Method ="RADIUS". When Radius Server authentication fail, it will check by local password if fallback is checked

WEB Interface

A. **Click *Configuration/Security/Switch/Auth Method***
B. **Select Authentication Method for console and web, specify the Fallback check if needed.**
C. **Click Save to apply the setting or Reset to restore the previous setting.**



SNMP

Any Network Management System (NMS) running the Simple Network Management Protocol(SNMP) can

manage the device which equipped with SNMP agent and attached with Management information Bases(MIBs). The SNMP is a common comminunication protocol for managing devices on a network. SNMP is typically using for configuring and monitoring devices.
The switch supports SNMPv1, v2c and v3. It continously monitors the status of the switch hardware as well as the traffic passing through its' ports.

SNMP System

Using the SNMP System Configuration page 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 switch. So, both parties must have the same community name.

LOCATION：

▼ Configuration

▼ Security

▼ Switch

▼ SNMP

- System

PARAMETERS：

Items	Description
SNMP System Configuration	
Mode	Enables or disables SNMP service
Version	Specifies the SNMP version (SNMP v1, SNMP v2c, SNMP v3)
Read Community	The community for Read access
Write Community	The community for Read/Write access

Engine ID	The SNMP v3 Engine ID,It is only available for SNMP v3 (10-64 HEX digits, excluding a string of all 0's or F's)
SNMP Trap Configuration	
Trap Mode	Enables or disables SNMP traps
Trap Version	Specifies the Trap Version (SNMP v1, SNMP v2c, SNMP v3)
Trap Community	Specifies the community string for SNMP trap packets
Trap Destination Address	Specifies the IP Address of management PC/NB to get trap packets
Trap Authentication Failure	Issues a notification message to specified IP trap managers whenever of a SNMP request fails.
Trap Link-up and Link-down	Issues a notification message to specified IP trap managers whenever a port link is established or broken
Trap Inform Mode	Enables or disables sending notification as inform message. It is only available for SNMP v2c and SNMP v3. Inform mode can guarantee the message is received.
Trap Inform Timeout	The time for waiting a ACK (Range：0-2147, unit：second)
Trap Inform Retry Times	The Maximum numbers of re-try times before gotting ACK
Trap Probe Security Engine ID	Specifies whether or not to use the engine ID of the SNMP trap probe in trap and inform messages(It is only available for SNMP v3)
Trap Security Engine ID	Displays the SNMP Trap security engine ID. (It is only available for SNMP v3)

Trap Security Name	Displays the Trap security Name (It is only available for SNMP v3)

WEB Interface

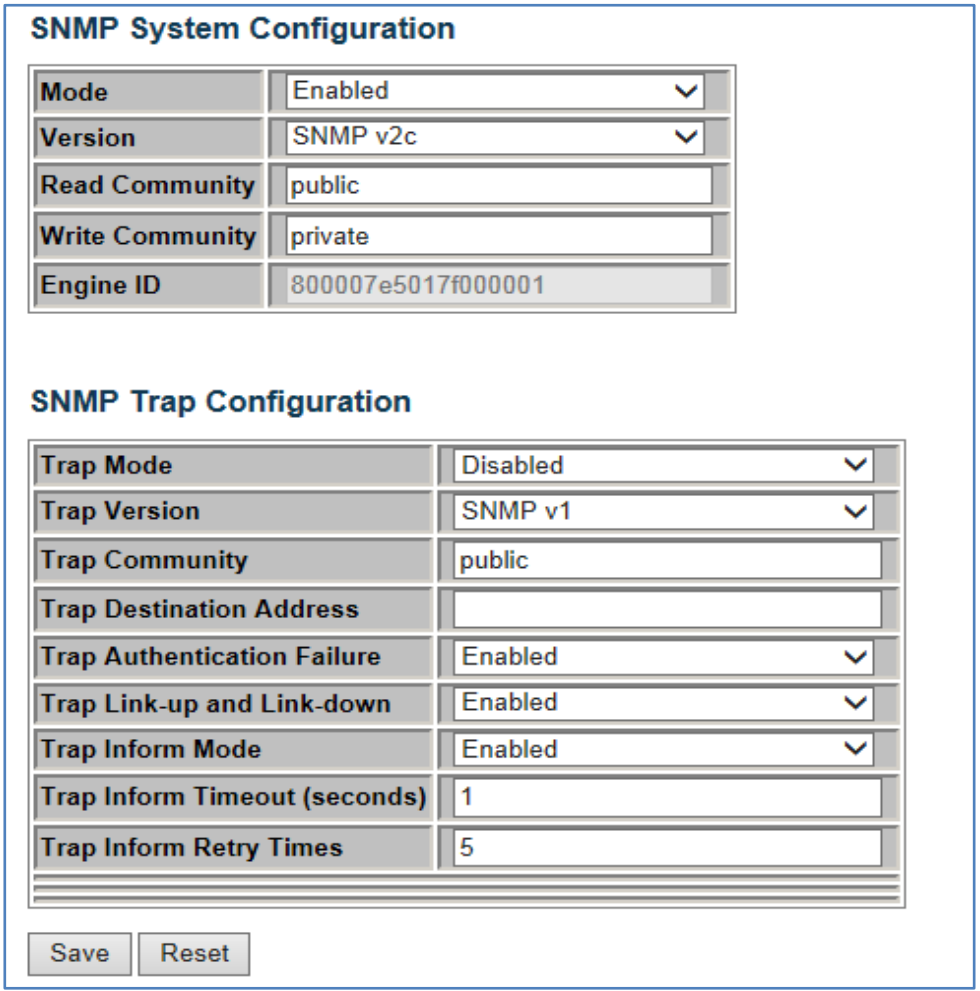
To setup SNMP System & Trap Configuration

A. Clicks *Configuration/Security/Switch/SNMP/System*

B. Set Mode to Enable SNMP service and specify SNMP version then change the Read and Write Community access strings if required and set the engine ID

C. In the SNMP Trap Configuration table, enable Trap mode to allow the switch to send SNMP traps. Specifies the trap version, trap community and IP Address of management PC/NB which will receive the trap messages. Select inform mode for SNMP v2c and SNMP v3 clients. Set Security engine ID for SNMP v3 client.

D. Click Save to apply the setting or Reset to restore the previous setting.



Communities

Using SNMPv3 Community Confugration page to set access community strings. It should include all community strings for SNMPv1, SNMPv2c and SNMPv3.

LOCATION：

▼ Configuration

▼ Security

▼ Switch

▼ SNMP

- Communities

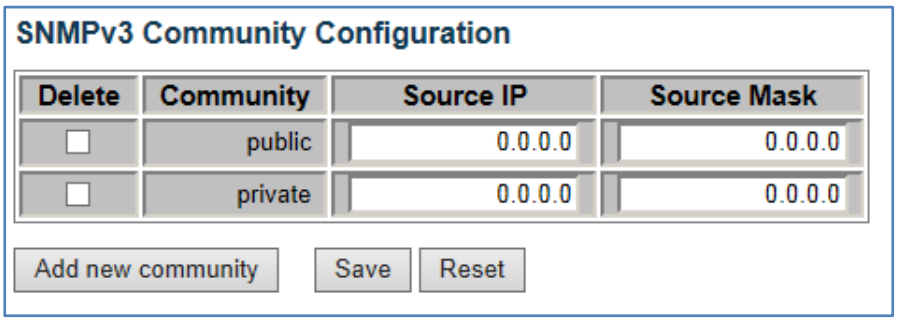
PARAMETERS：

Items	Description
Community	Specifies the community string to allow access the SNMP agent.(Range：1-32)
Source IP	Specifies the IP Address of the SNMP client
Source Mask	Specifies the subnet mask of the SNMP client

WEB Interface

To setup SNMP Community access string：

A. **Clicks *Configuration/Security/Switch/SNMP/Communities***
B. **Set the IP Address and subnet mask for the default community string or delete for security.**
C. **Add any new Community strings by click Add new community button**
D. **Click Save to apply the setting or Reset to restore the previous setting.**



Users

Using SNMPv3 User Configuration page to set a specific Engine ID, Name, security level and the types of authentication and privacy for each SNMPv3 user.

LOCATION：

▼ Configuration

▼ Security

▼ Switch

▼ SNMP

- Users

PARAMETERS：

Items	Description
Engine ID	The engine identifier for SNMP agent. (It is only available for SNMPv3)
User Name	The unique username for SNMP agent (Range：1-32 characters)
Security Level	There are 3 options: NoAuth, NoPriv：no authentication and encryption during the communication Auth,NoPriv：with authentication but no encryption during the cummunication Auth,Priv： with both authentication and encryption during the

	communication
Authentication Protocol	The methods for authentication (None, MD5, SHA,)
Authentication Password	A plain text as password(Range：1-32 characters)
Privacy Protocol	The encryption algorithm (none or 56-bit DES)
Privacy password	A string for Privacy pass phrase (Range：8-40 characters)

WEB Interface

To setup SNMPv3 User：

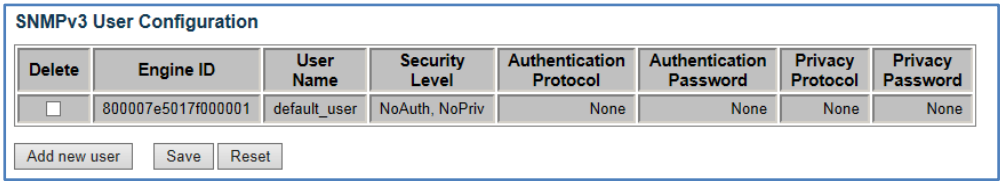
A. Clicks *Configuration/Security/Switch/SNMP/Users*

B. Clicks "Add new user" to configure a username

C. Enters a remote Engine ID

D. Defines username, security level, authentication and privacy settings

E. Click Save to apply the setting or Reset to restore the previous setting.



SNMPv3 User Configuration

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

Add new user　Save　Reset

Groups

Using SNMPv3 Group Configuration page to configure SNMPv3 Group, it defines a specific SNMPv3 group and restricts assigned user's access policy for read and write views.

LOCATION：

▼ Configuration

▼ Security

▼ Switch

▼ SNMP

- Groups

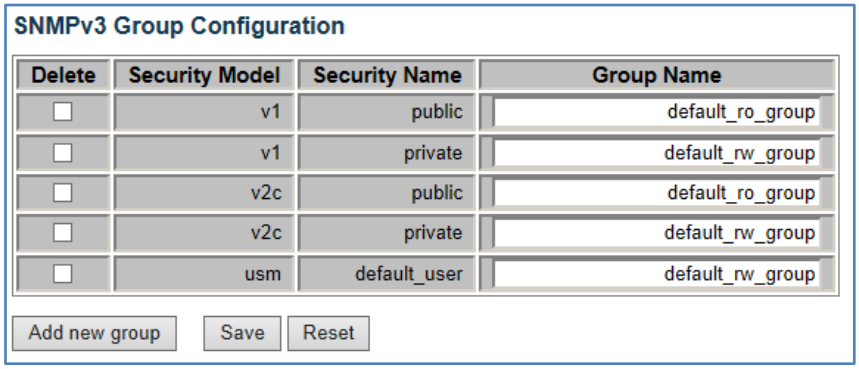
PARAMETERS：

Items	Description
Secuirty Model	The user security model, 3 options： (v1, v2, usm=User-based security Model)
Security Name	The username which connect to SNMP agent(Range：1-32 characters)
Group Name	The name of SNMP group

WEB Interface

To setup SNMPv3 Group：

A. **Click *Configuration/Security/Switch/SNMP/Groups***
B. **Click "Add new group" to create a new group**
C. **Select a Security Model(SNMPv1, SNMPv2c or User-based Security Model)**
D. **Select a Security Name**
E. **Enter a Group Name**
F. **Click Save to apply the setting or Reset to restore the previous setting.**



Views

Using SNMPv3 View Configuration page to define the restricts access policy for specific MIB tree The default_view includes access ability for whole MIB tree.

LOCATION：

▼ Configuration

▼ Security

▼ Switch

▼ SNMP

- Views

PARAMETERS：

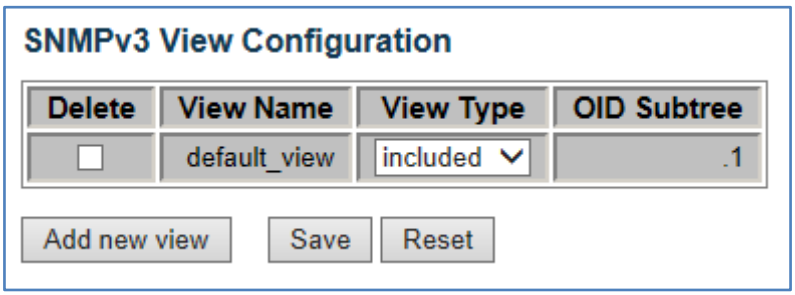
Items	Description
View Name	The Name of SNMP view (Range：1-32 characters)
View Type	Indicates the OID is included or excluded in this SNMP view
OID Subtree	Object identifiers of branches within the MIB tree

WEB Interface

To setup SNMPv3 Views：

A. **Click *Configuration/Security/Switch/SNMP/Views***
B. **Click "Add new view" to create a new view**
C. **Enter a View Name, Type and OID Subtree**
D. **Click Save to apply the setting or Reset to restore**

the previous setting.



Access

Using SNMPv3 Access Configuration page to define the Access rights for portion of MIB tree. You can have more than one Access policy for SNMPv3 group.

LOCATION：

▼ Configuration

▼ Security

▼ Switch

▼ SNMP

- Access

PARAMETERS：

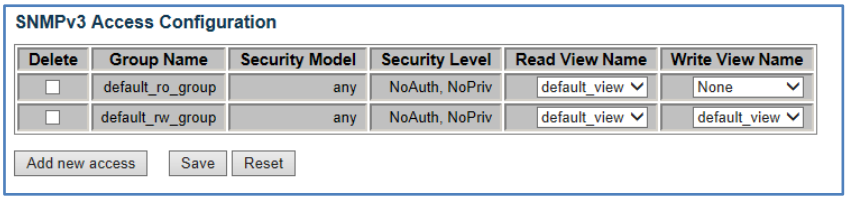
Items	Description
Group Name	The Name of SNMP group (Range：1-32 characters)
Security Model	The user security model, 3 options： (v1, v2, usm=User-based security Model)
Security Level	There are 3 options: NoAuth, NoPriv：no authentication and encryption during

	the communication Auth,NoPriv：with authentication but no encryption during the cummunication Auth,Priv： with both authentication and encryption during the communication
Read View Name	Select View Name for Read Access
Write View Name	Select Write Name for Write Access

WEB Interface

To setup SNMPv3 Accesss：

A. **Click *Configuration/Security/Switch/SNMP/Access***
B. **Click "Add new access" to create a new view**
C. **Select a Group Name, security model, security level, Read View and Write View.**
D. **Click Save to apply the setting or Reset to restore the previous setting.**



Network

ACL ports

Using ACL Ports Configuration page to specify the

assigned port's re-actions when certain kind of frames are matchs. These behaviors include "Port Redirect", "Mirror", "Logging" and "Shutdown".

LOCATION：

▼ Configuration

▼ Security

▼ Network

▼ ACL

- Ports

PARAMETERS：

Items	Description
Port	Port Number
Policy ID	Specify the Policy ID (Range：0-255)
Action	Permit or deny the forwarding if policy is matched
Rate limiter ID	Specify a Rate Limiter ID, the mapping table is in "Rate Limiters" page
Port Redirect	Specify the packets redirect to which port if policy matched
Mirror	Specify the packets also forward to predefined mirror port if policy matched
Logging	Enable logging the matched frames to system log
Shutdown	Shut down the port if policy matched
Counter	Show the number of frames which match the specific policy

WEB Interface

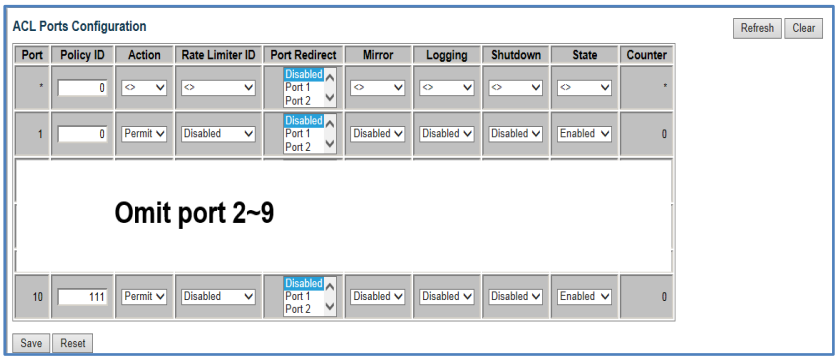
To Configure ACL policies and its' re-action：

A. Click *Configuration/Security/Network/ACL/Ports*

B. Assign policy which is set on ACE Configuration page. Specify re-action behaviors when frames matcheds, it includes "Port Redirect", "Mirror", "Logging", "Shutdown".

C. Click Save to apply the setting or Reset to restore the previous setting.

- **Refresh Button：Refresh the Counter of frames matched the policy.**
- **Clear Button：Clean the Counter of frames matched the policy**



Rate Limiters

Using ACL Rate Limiter Configuration page to configure up to 16 Rate Limit options

LOCATION：

▼ Configuration
  ▼ Security
    ▼ Network

▼ ACL

- Rate Limiters

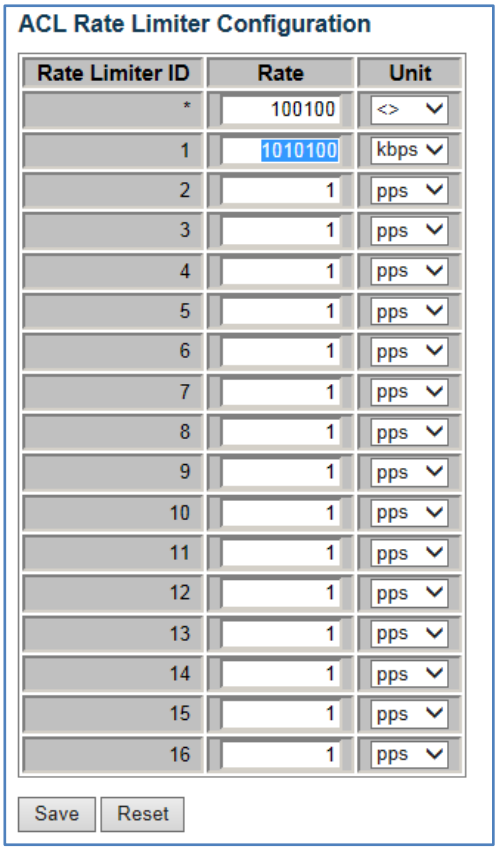
PARAMETERS：

Items	Description
Rate Limiter ID	Rate Limit Identifier (Range：1-16)
Rate	The dropping threshold, the allowed value： 0-3276700 in pps,0, 100, 2*100, 3*100…100000 in kbps
Unit	Unit of measure(pps, kbps)

WEB Interface

To Configure ACL Rate limitation：

A. **Click *Configuration/Security/Network/ACL/Rate Limiters***
B. **Specify Rate and Unit for Rate Limiter ID(1-16)**
C. **Click Save to apply the setting or Reset to restore the previous setting.**



ACL Rate Limiter Configuration

Rate Limiter ID	Rate	Unit
*	100100	<>
1	1010100	kbps
2	1	pps
3	1	pps
4	1	pps
5	1	pps
6	1	pps
7	1	pps
8	1	pps
9	1	pps
10	1	pps
11	1	pps
12	1	pps
13	1	pps
14	1	pps
15	1	pps
16	1	pps

Save Reset

Access Control List

Using Access Control List page to make up of ACE s deine on this switch. Each row describes the ACE that is defined. You can define filtering rules for an ACL policy, for a specific port or for all ports.

LOCATION：

▼ Configuration
  ▼ Security
    ▼ Network
      ▼ ACL
        ▪ Access Control List

PARAMETERS：

Items	Description

Ingress Port	Specific port or All ports
Policy/Bitmask	Indicate the Policy and Bitmask of the ACE
Frame Type	Indicate the frame type of ACE. Any：match any frames Ethernet：match Ethernet type frames ARP：match ARP/RARP frames IPv4：matchIPv4 frames IPv4/ICMP：match IPv4 frames with ICMP Protocol IPv4/UDP：match IPv4 frames with UDP Protocol IPv4/TCP：match IPv4 frames with TCP Protocol IPv4/Other：match IPv4 frames which are not ICMP/UDP/TCP
Action	Permit or deny frames when the frames matched
Rate Limiter	Indicate the rate limiter number of the ACE.
Port Redirect	Indicate the port redirect operation of the ACE
Mirror	Specify the mirror operation of this port
Counter	Indicate the number of times the ACE was hit by a frame
Modification Buttons	⊕ Insert a new ACE before the current

row

Edit the ACE row

Move the ACE up the list

Move the ACE down the list

Delete the ACE

The lowest plus sign adds a new entry at the buttom of the ACE listings

WEB Interface

To Configure ACL Rate limitation：

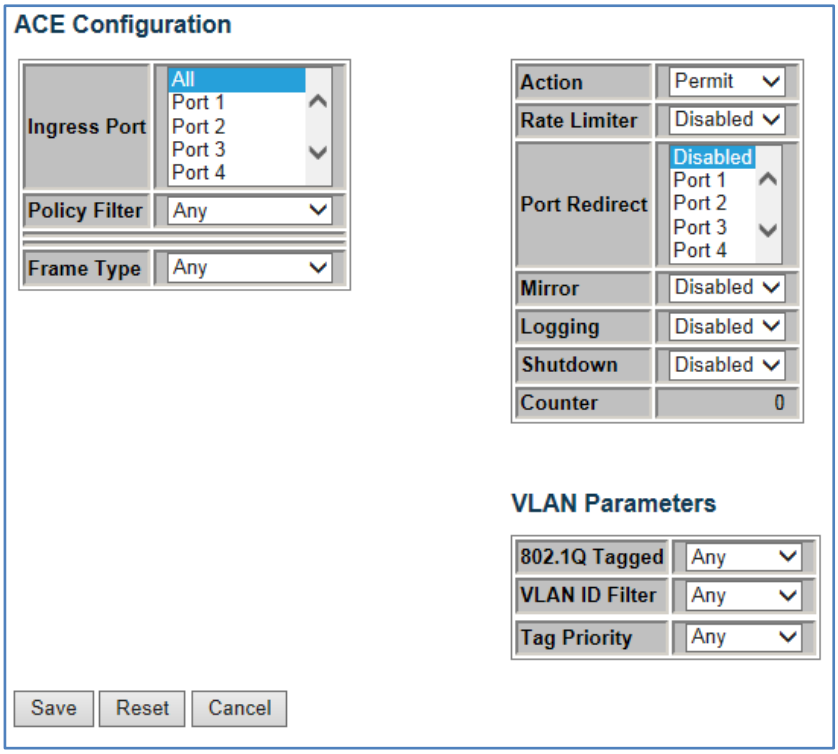
A. Click *Configuration/Security/Network/ACL/Access Control List*

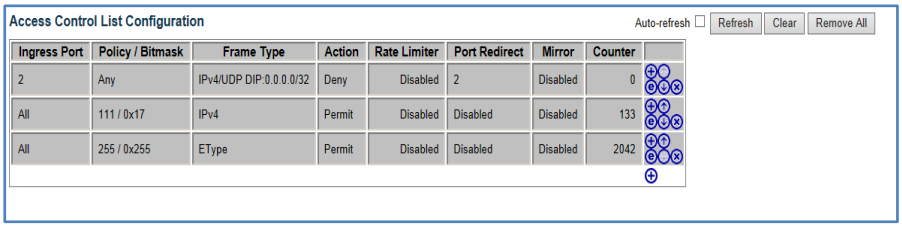
B. Click the button to add new ACE, or use the button to modify the ACE row

C. Specify the parameters of the ACE

D. Click Save to apply the setting, Reset to restore the previous setting or Cancl to back ACE list

- **Clear Button：Clean the Counter of frames matched the policy**
- **Remove All Button：Delete all ACE rows**
- **Auto-refresh：Refresh the page automatically**





AAA

Using the Authentication Server Configuration page to build up an authenticated mechanism with RADIUS server.

LOCATION：

▼ Configuration

▼ Security

- AAA

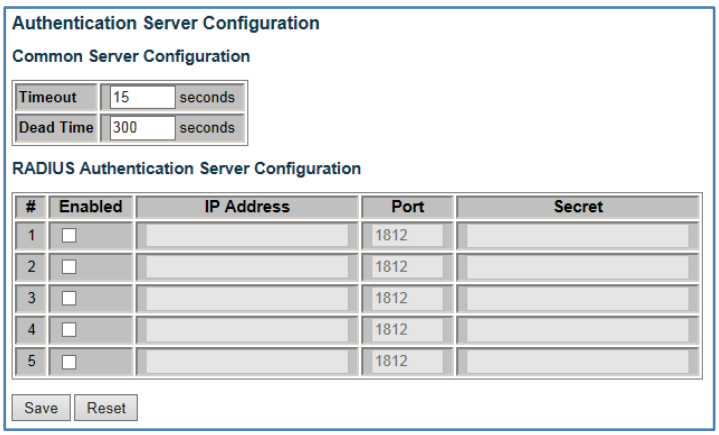
PARAMETERS：

Items	Description
Common Server Configuration	
Timeout	The maximum waiting time to wait for a reply from server (Range：3-3600 seconds)
Dead Time	The time after which the switch Considers an authentication server to be dead if it does not reply
RADIUS Authentication Server Configuration	
Enable	Enable the RADIUS Authentication Server by Check this box
IP Address	IP Address of RADIUS server
Port	The UDP port to use on the RADIUS authentication Server.
Secret	Encryption key(Maximum characters：29)

WEB Interface

To Configure ACL Rate limitation：

A. **Click *Configuration/Security/AAA***
B. **Specify the parameters of the RADIUS Authentication Server.**
C. **Click Save to apply the setting or Reset to restore the previous setting.**



Port Trunking(Static)

Using Aggregation Mode Configuration page to configure the Aggregation Mode and Members of each static group.

LOCATION：

▼ Configuration
  ▼ Port Trunking
    ▪ Static

PARAMETERS：

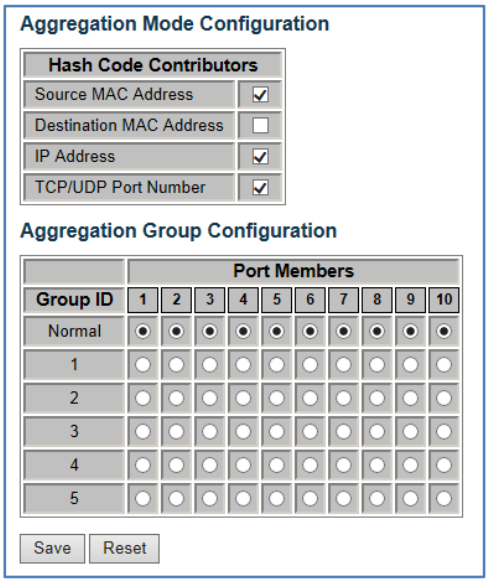
Items	Description
Hash Code Contributors	
Source MAC Address	Enable：The source MAC Address can be used to calculate the destination port for the frame.(Disable is not)
Destination MAC Address	Enable：The Destination MAC Address can be used to calculate the destination port for the frame. (Disable is not)
IP Address	Enable：The IP Address can be used to calculate the destination port for the frame.(Disable is not)
TCP/IP Port Number	Enable：The TCP/IP port number canbe used to caclulate the destination port for the frame.(Disable is not)
Port Members	

Group ID	Normal：There is no aggregation Note：Only one group ID is valid per port.
Port Members	Port Identifier

WEB Interface

To Configure a Static Trunk：

A. **Click *Configuration/Port Trunking/Static***
B. **Select load-balancing method in hash code contributors**
C. **Assign port members to specific trunking group**
D. **Click Save to apply the setting or Reset to restore the previous setting.**



Port Trunking(LACP)

Using LACP Port configuration page to enable LACP on selected ports, configure key and LACP mode.

LOCATION：

▼ Configuration

▼ Port Trunking

- LACP

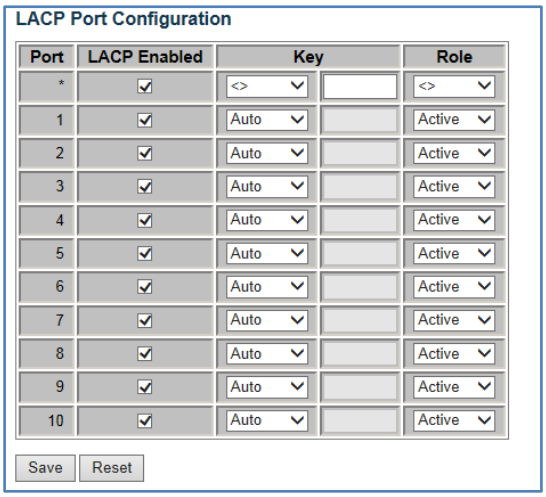
PARAMETERS：

Items	Description
Port	Port Identifier
LACP Enabled	Control whether LACP is enabled on this switch port. LACP will from an aggregation when 2 or more ports are connected to the same partner. LACP can from max 12 LLAGs per switch and 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. The same key setting ports can participate in the same aggregation group.
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.

WEB Interface

To Configure the LACP：

A. **Click *Configuration/Port Trunking/LACP***
B. **Enable LACP on all of the ports in an LAG**
C. **Divide the LAG by different key**
D. **Set one Active role port in one LAG at least**
E. **Click Save to apply the setting or Reset to restore the previous setting.**



Loop Protection

Using Loop Protection page to configure loop protection

LOCATION：

▼ Configuration

- Loop Protection

PARAMETERS：

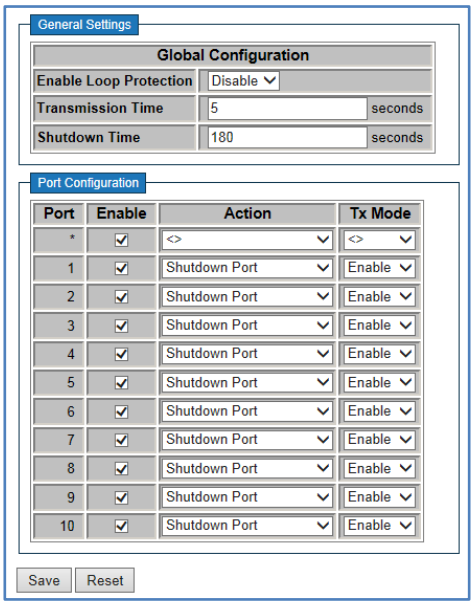
Items	Description
General Settings	
Enable Loop Protection	Controls whether loop protections is enabled
Transmission Time	The interval between each loop protection PDU sent on each port. Valid values are 1 to 10 seconds
Shutdown Time	The period(in seconds) for which a port will be kept disabled in the event of 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	Port identifier
Enable	Control whether loop protection is enabled on this switch port
Action	Configure the action performed when a loop protection is detected on a port. Valid values are “Shutdown Port”, “Shutdown Port and Log”, or “Log only”
Tx mode	Control whether the port is actively generating loop protection PDU’s, or whether it is just passively looking for looped PDU’s

WEB Interface

To Configure the Loop Protection：

A. **Click *Configuration/Loop Protection***
B. **Enable Loop Protection, configure Transmission Time and Shutdown Time**
C. **Specify reaction for each port when loop protection is detected**
D. **Click Save to apply the setting or Reset to restore the previous setting.**



Spanning Tree

The Spanning Tree Algorithm can be used to detect and disable network loops and provide backup links between switches, bridges and routers. This allows the switch to cooperate with other bridging devices.

Spanning Tree (Bridge Settings)

Using the STP Bridge Settings page to configure settings for STA which apply globally setting.

LOCATION：

▼ Configuration
  ▼ Spanning Tree
    ▪ Bridge Settings

PARAMETERS：

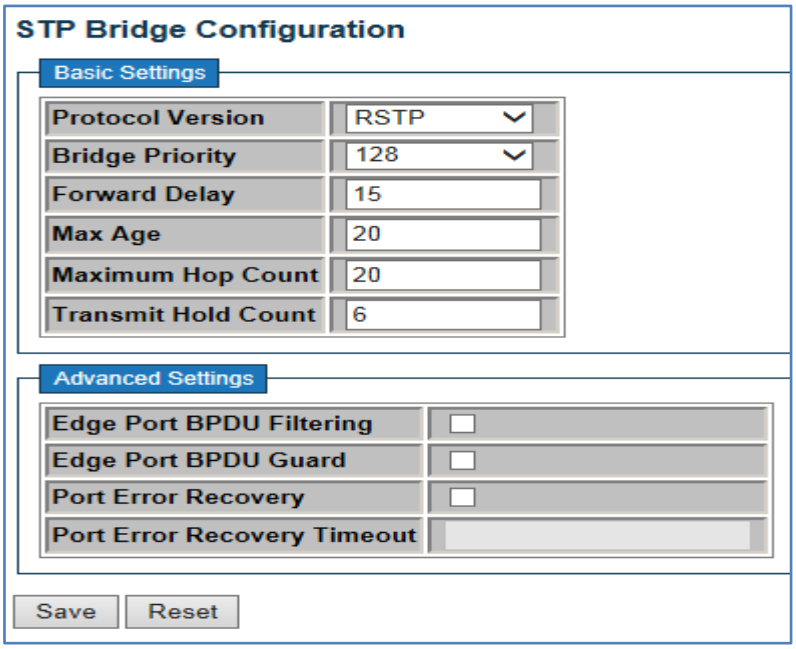
Items	Description
Basic Settings	
Protocol Version	The STP protocol version setting, the Valid values are STP(IEEE 802.1D) and RSTP(IEEE 802.1w).
Bridge Priority	Control the bridge priority, low numeric values have higher priority
Forward Delay	The delay used by STP Bridges to transit Root and Designated Ports to forwarding(used in STP compatible mode). (Range：4-30 seconds)
Max Age	The Maximum age of information transmitted by the Bridge when it is

	the Root Bridge. (Range：6-40 seconds). Max Age must be <=(FwdDelay-1)*2
Maximum Hop Count	This define the initial value of remaining Hops for MSTI information generated at the boundary of an MSTI region. (Range：6-40 hops)
Transmit Hold Count	The number of BPDU's bridge port can send per seconds. When exceed, transmission of the next BPDU will delay. (Range：1-10 BPDUs per second)
Advanced Settings	
Edge Port BPDU filtering	Control whether the 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 BPDUs. The port will enter the error-disables state and will be removed from the active topology.
Port Error Recovery	Control whether a port in the error-disable state automatically will be enabled after a certain time. If recovery is not enabled, ports have to be disabled and re-enabled from normal STP operation. The condition is also cleared by a system reboot.
Port Error Recovery Timeout	The time to pass beofre a port in the error-disabled state can be enabled.(Range：30-86400seconds)

WEB Interface

To Configure STP Configuration：

A. **Click *Configuration/Spanning Tree/Bridge Settings***
B. **Configure the required attributes**
C. **Click Save to apply the setting or Reset to restore the previous setting.**



Spanning Tree
(Bridge Ports)

Using the STP CIST Ports Configuration page to configure STA attributes for interfaces when the Spanning Tree mode is set to STP or RSTP or for Interfaces in the CIST. STA interface attributes include path cost, priority, edge port, automatic detection of an edge port and PtP link type

LOCATION：

▼ Configuration
  ▼ Spanning Tree

- Bridge Ports

PARAMETERS：

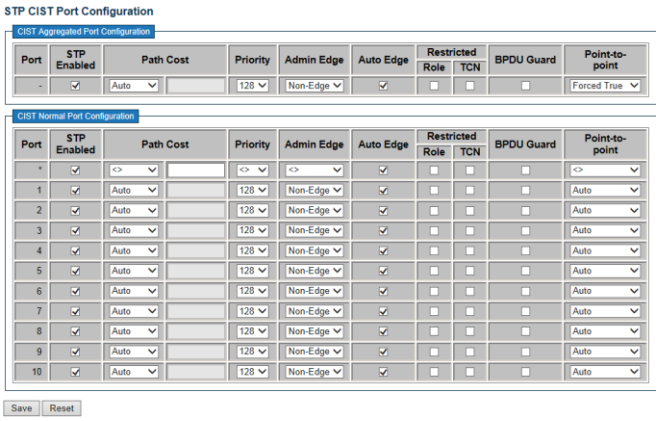
Items	Description
CIST Aggregation Port Configuration	
STP Enable	Control whether STP is enabled on this switch port
Path Cost	Control the Path Cost incurred by this port. The “Auto” setting will set the path cost as approciate by physical link speed, using the 802.1D recommended values. Using “specific” settings, a user-defined value can be entered. The path cost is used when establishing the active topology of the network. Low path cost ports are chosen as forwarding ports in favour of higher path cost ports. (Range：1-200000000)
Priority	Control the port priority. This can be used to control priority of the ports having identical port cost.
Admin Edge	Enable this option if this port is connected to an end node or at the end o the bridge.
Auto Edge	Control whether automatic edge detection is enabled on a bridge port
Restricted Role	If enabled, cause the port not to be selected as Root port for the CIST, even if it has the best spanning tree priority vector. This features is also known as “Root Guard”
Restricted TCN	If enabled, cause 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 spannig tree's active topology as a result of persistently incorrect learned station location information. It is set by a network administrator to prevent bridges extenal 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, cause the port to disable itself upon receiving valid BPDU's. Contrary to the similar bridge setting, the port Edge status desn't effect this settings.
Point-to-Point	Control whether the port connects to a point-to-point LAN rather than a shared medium. This can be automatically determined, or forced either true or false. Transtion to the forwarding state is faster for point-to-point LAns than for shared media.

WEB Interface

To Configure STP CIST Port Configuration：

A. **Click *Configuration/Spanning Tree/Bridge Port s***
B. **Configure the required attributes**
C. **Click Save to apply the setting or Reset to restore the previous setting.**



IGMP SNOOPING

Multi-casting is using to support real-time applications such as video-conferencing or streaming audio. A multicast server doesn't have to establish a separate connection to each client. It merely broadcasts its' service to the network. By this approach, it will increase a lot of broadcast traffic in the network.
This switch can use IGMP to filter multi-cast traffic. IGMP snooping can be used to passively monitor or snoop the packets exchanging between multi-cast hosts and clients. Then, it can set its filters

IGMP SNOOPING
Basic Configuration

Using the IGMP Snooping Configuration page to configure Global and Port Related settings to control the forwarding of multi-cast traffic. This can decrease broadcast traffic to improve the network performance.

LOCATION：

▼ Configuration
  ▼ IPMC
    ▼ IGMP Snooping
      ▪ Basic Configuration

PARAMETERS：

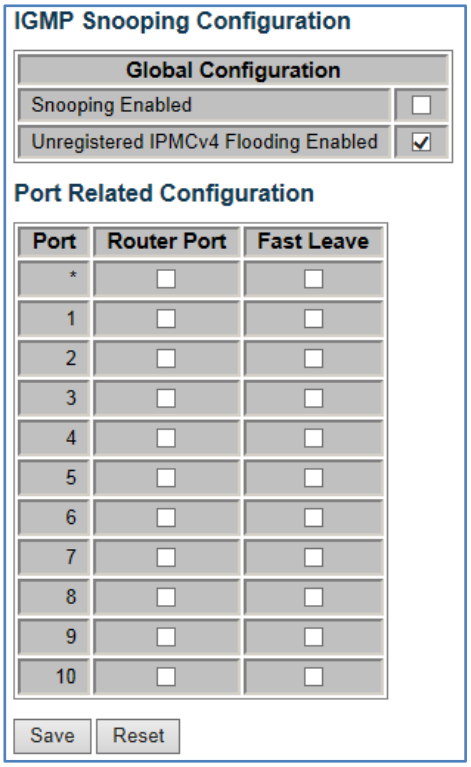
Items	Description
Global Configuration	
Snooping Enabled	Control whether the IGMP snooping is enabled
Unregistered IPMCv4 Flooding Enabled	Enable unregistered IPMCv4 Flooding
Port Related Configuration	
Port	Port Identifier
Router Port	Specify which porta act as router ports.A Router port is a port on the Ethernet switch that leads toward the layers multi-cast 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	Delete a member port of mult-cast Service immediately if a leave packet is received at this portEnable Fast Leave on this port.

WEB Interface

To Configure Global and Port related settings for IGMP Snooping：

A. Click *Configuration/IPMC/IGMP Snooping/Basic Configuration*
B. Specify the required IGMP Snooping Settings
C. Click Save to apply the setting, Reset to restore

the previous setting.



IGMP SNOOPING

VLAN Configuration

Using the IGMP Snooping VLAN Configuration page to configure IGMP Snooping settings.

LOCATION：

▼ Configuration

▼ IPMC

▼ IGMP Snooping

- VLAN Configuration

PARAMETERS：

Items	Description
VLAN ID	VLAN Identifier
Snooping Enabled	Enable the per-VLAN IGMP Snooping. Up to 32 VLANs can be selected for IGMP Snooping.
Port	Port Identifier

WEB Interface

To Configure IGMP Snooping VLAN：

A. Click *Configuration/IPMC/IGMP Snooping/VLAN Configuration*
B. Specify the required IGMP Snooping VLAN Settings
C. Click Save to apply the setting, Reset to restore the previous setting.

Refresh Button：Refresh the Display table

Starting from the first entry of the VLAN table.

Power Over Ethernet

This Switch provides IEEE 802.3af/at PoE functions, it provides PD class power allocation and power reserved manually with different priority policy. The total power is 120 Watt.

Using Power Over Ethernet Configuration to set PoE mode,

its priority and Maximum power per port：

LOCATION：

▼ Configuration

- PoE

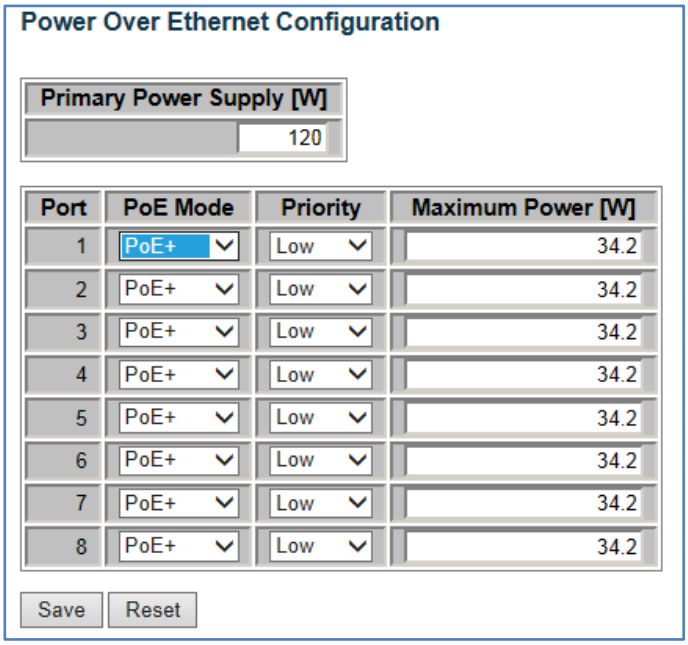
PARAMETERS：

Items	Description
Primary Power Supply[W]	It depends on power supply. We provides 120 Watt for this model
Port	Port identifier
PoE Mode	The PoE Mode represents the PoE operating mode for the port. Disabled：Turn the PoE off PoE：Enable 802.3af(Class 4 PD Maximum power is 15.4Watt) PoE+：Enable 802.3at(Class 4 PD Maximum power is 34.2Watt)
Priority	There are 3 priority levels.(Low, High, Critical). The priority is used in the case where the remote devices requires more power than power supply can deliver. In this case the port with lowest priority will be turn off starting from the port with the highest port number.

WEB Interface

To Configure PoE functions：

A. **Click *Configuration/PoE***
B. **Specify Disabled/PoE/PoE+ and priority for each port**
C. **Click Save to apply the setting, Reset to restore the previous setting.**



IEEE 802.1Q VLAN

This switch provides Layer 2 VLAN for following reasons; By appropriated settings to eliminate broadcast storms in large networks. This also provide a more secure and cleaner network environment.
VLAN provides greater network performance by reducing broadcast traffic and also provides high level of network security since traffic must pass through a configured Layer 3 link to reacha different VLAN.

VLAN Configuration

Using VLAN Membership Configuration page to set VLAN group：

LOCATION：

▼ Configuration
  ▼ VLANs

    ▪ VLAN Membership

PARAMETERS：

Items	Description
VLAN ID	ID of this particular VLAN (Range：1-4096)
VLAN Name	The name of VLAN (Range：up to 32 characters)
Port Members	A row of checkboxes for each port is displayed for each VLAN ID Check the box ✓. to include a port in a VLAN Check the box as shown ✕ to include a port in a forbidden port list. Uncheck the box ☐.. to remove a port from a VLAN

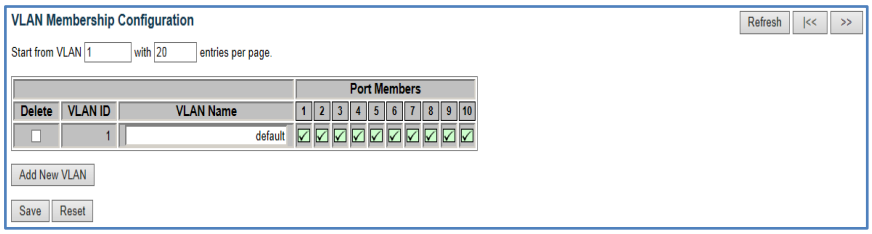
WEB Interface

To Configure IEEE 802.1Q VLAN groups：

A. Click *Configuration/VLANs/VLAN Membership*
B. Change Default VLAN ID=1, if necessary.
C. Click "Add New Entry" to create a new VLAN group with ID, Name and port members.
D. Click Save to apply the setting, Reset to restore the previous setting.

- **Refresh Button：Refresh the Display table**

  Starting from the first entry of the VLAN table.



VLAN Ports

Using VLAN Ports Configuration page to set VLAN attributes for specific interfaces, including processing frames with embedded tags, Ingress filtering, setting the accepted frame types and assigning Port VLAN ID.

LOCATION：

▼ Configuration
  ▼ VLANs
    ▪ Ports

PARAMETERS：

Items	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.
Port	The logical port number of this row
Port Type	Port can be one of the following types： Unaware, Customer port(C-port), Service Port(S-port), Custom Service port(S-custom-port). If Port Type is Unaware, all frames are classified to the Port VLAN ID and tags are

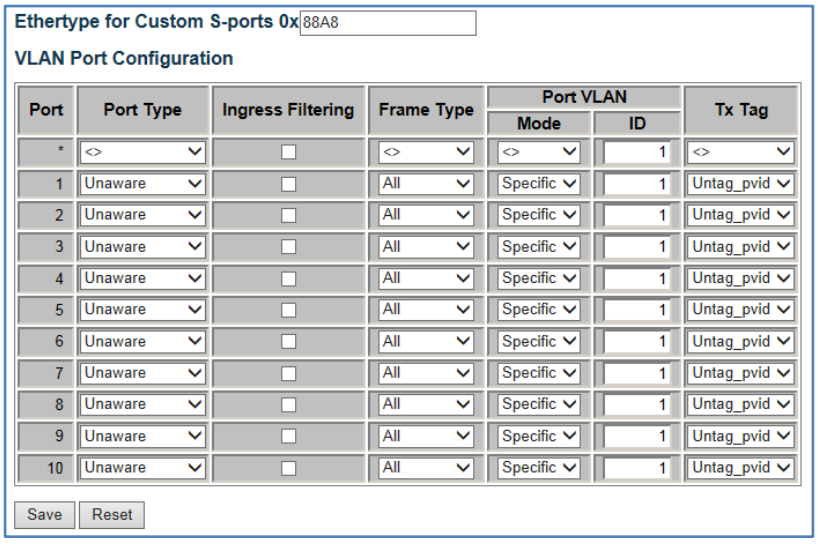
	not removed
Ingress filtering	Enable ingress filtering on a port by checking the box. This parameter affects VLAN ingress processing. If ingress filtering is enabled and the ingress port is not a member of the classified VLAN of the frame, the frame is discarded. By default, ingress filtering is disabled.
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 this port will be discarded
Port VLAN mode	Configure VLAN mode to “None” or “Specific”, None：a VLAN tag with classified VLAN ID is Inserted in frames transmitted on the port.This mode is normally used for ports connected to VLAN aware swithces. Specific：a Port VLAN ID can be configured. Untagged frames received on the port are classified to the Port VLAN ID. If If VLAN awareness is disabled, all frames received on the port

	are classified to the Port VLAN ID. If the classified VLAN ID of a frame transmitted on the port is different from the Port VLAN ID, a VLAN tag with the classified VLAN ID is inserted in the frame.
Port VLAN ID	Configures the VLAN identifier for the port. The allowed values are 1 through 4095. The default value is 1. Note： The port must be a member of the same VLAN as the Port VLAN ID.
Tx Tag	Determines egress tagging of a port. Untag_pvid - All VLANs except the configured PVID will be tagged. Tag_all - All VLANs are tagged. Untag_all - All VLANs are untagged

WEB Interface

To Configure attributes for VLAN port member：

A. Click *Configuration/VLANs/Ports*
B. Configure the required settings for each interface.
C. Click Save to apply the setting, Reset to restore the previous setting.



Port	Port Type	Ingress Filtering	Frame Type	Port VLAN Mode	Port VLAN ID	Tx Tag
*	<>	☐	<>	<>	1	<>
1	Unaware	☐	All	Specific	1	Untag_pvid
2	Unaware	☐	All	Specific	1	Untag_pvid
3	Unaware	☐	All	Specific	1	Untag_pvid
4	Unaware	☐	All	Specific	1	Untag_pvid
5	Unaware	☐	All	Specific	1	Untag_pvid
6	Unaware	☐	All	Specific	1	Untag_pvid
7	Unaware	☐	All	Specific	1	Untag_pvid
8	Unaware	☐	All	Specific	1	Untag_pvid
9	Unaware	☐	All	Specific	1	Untag_pvid
10	Unaware	☐	All	Specific	1	Untag_pvid

Private VLAN

Private VLAN provides port-base security and isolation between ports within assigned VLAN. Data Traffic on ports assigned to a private VLAN can only be forwarded to or from uplinks ports. Ports isolated in the private VLAN are designated as downlink ports and can only communicate to uplink ports with the same private VLAN.

PVLAN Membership

Using the private VLAN Membership Configuation page to assign ports to specific private VLAN.

LOCATION：

▼ Configuration
  ▼ Private VLANs
    ▪ PVLAN Membership

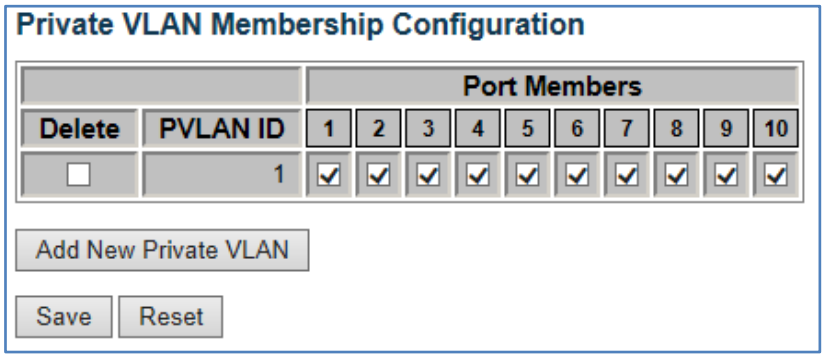
PARAMETERS：

Items	Description
PVLAN ID	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

WEB Interface

To Configure VLAN port member for PVLANs：

A. **Click *Configuration/Private VLANs/PVLAN Membership***
B. **Add or delete members of any existing PVLAN, or click "Add New Private VLAN" to create new PLVAN.**
C. **Click Save to apply the setting, Reset to restore the previous setting.**



Port Isolation

Using the Port Isolation Configuration page to prevent communications between customer ports within the same private VLAN

LOCATION：

▼ Configuration
  ▼ Private VLANs
    ▪ Port Isolation

PARAMETERS：

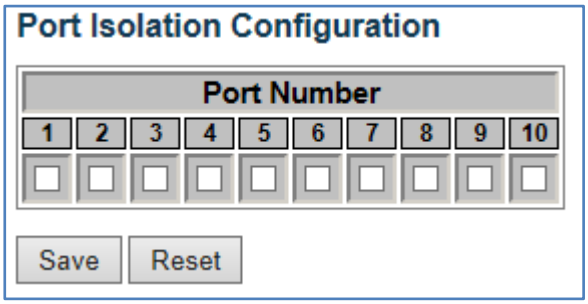
Items	Description
Port Members	A check box is provided for each port of a

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.

WEB Interface

To Configure PVLAN port isolation：

A. **Click *Configuration/Private VLANs/Port Isolation***
B. **Make the checked ports are isolated from each other.**
C. **Click Save to apply the setting, Reset to restore the previous setting.**



Quality of Service

The switch supports 4 QoS queues per port with stricted or weighted fair queuing scheduling. 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 guarantee to the frame according to what was configured for that specific QoS class.
The switch also allows you to configure QoS classification criteria and service polices. The switch's resources can be prioritized to meet the requirements of specific traffic

types on a per hop basis. Each packet is classified upon entry into network based on Ethernet type, TCP/UDP port, DSCP and ToS.

Port Classification

Using the QoS Ingress Port Configuration page to set the basic QoS parameters for a port, including the default traffic class, DP Level (IEEE 802.1p), user priority and drop eligible indicator.

LOCATION：

▼ Configuration
  ▼ QoS
    ▪ Port classification

PARAMETERS：

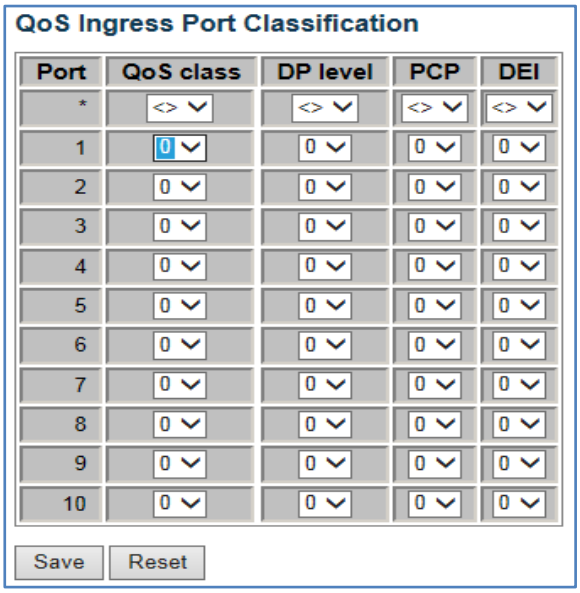
Items	Description
Port	The port number for which the configuration below applies.
QoS Class	Controls the default QoS class, i.e., the QoS class for frames not classified in any other way. There is a one to one mapping between QoS class, queue and priority. A QoS class of 0 (zero) has the lowest priority. 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
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 Priority Code Point(PCP) for untagged frames.
DEI	Controls the default Drop Eligible Indicator (DEI) for untagged frames.

WEB Interface

To use QoS Ingress Port Configuration：

A. Click *Configuration/QoS/Port Classification*
B. Set QoS Class priority for each port, DP Level and PCP, DEI for untagged frames.
C. Click Save to apply the setting, Reset to restore the previous setting.



Port Policing **The Port policing is useful in constraining traffic flows and marking frames avobe specific rates. Policing is primarily useful for data flows and voice or video flows because voice video usually maintains a steady rate of traffic.**

LOCATION：

▼ Configuration

▼ QoS

- Port Policing

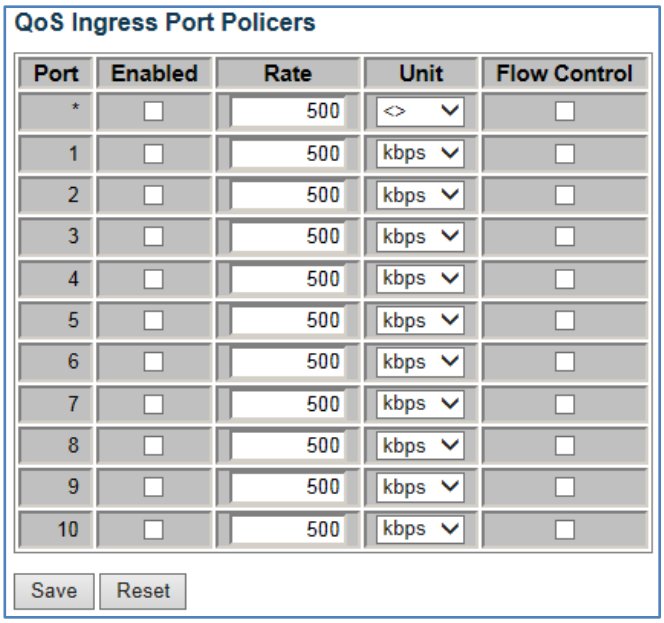
PARAMETERS：

Items	Description
Port	The port number for which the configuration below applies.
Enabled	Controls whether the policer is enabled on this switch port.
Rate	Controls the rate for the policer. The default value is 500. This value is restricted to 100-1000000 when the "Unit" is "kbps" or "fps", and it is restricted to 1-3300 when the "Unit" is "Mbps" or "kfps".
Unit	Controls the unit of measure for the policer rate as kbps, Mbps, fps or kfps . The default value is "kbps".
Flow Control	If flow control is enabled and the port is in flow control mode, then pause frames are sent instead of discarding frames.

WEB Interface

To Configure QoS Ingress Port Policiers：

A. **Click *Configuration/QoS/Port Policing.***
B. **Evoke which port need to enable the QoS Ingress Port Policers and type the Rate limitcondition**
C. **Scroll down to select Rate unit.**
D. **Click Save to apply the setting, Reset to restore the previous setting.**



QoS Control List

Using QoS Control List Configuration page to configure Quality of Service policies for handling ingress packets based on Ethernet type, VLAN ID, TCP/UDP port, DSCP, ToS or VLAN priority tag.

LOCATION：

▼ Configuration

▼ QoS

- QoS Control List

PARAMETERS：

Items	Description
QCE#	Indicate the index of QCE.
Port	Indicates the list of ports configured with the 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
SMAC	Display 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 allowedd. 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. DPL：Classified Drop Precedence Level. DSCP：Classified DSCP value.
Modification Buttons	Insert a new QCE before the current row Edit the QCE row Move the QCE up the list Move the QCE down the list Delete the QCE The lowest plus sign adds a new entry at the buttom of the QCE listings

WEB Interface

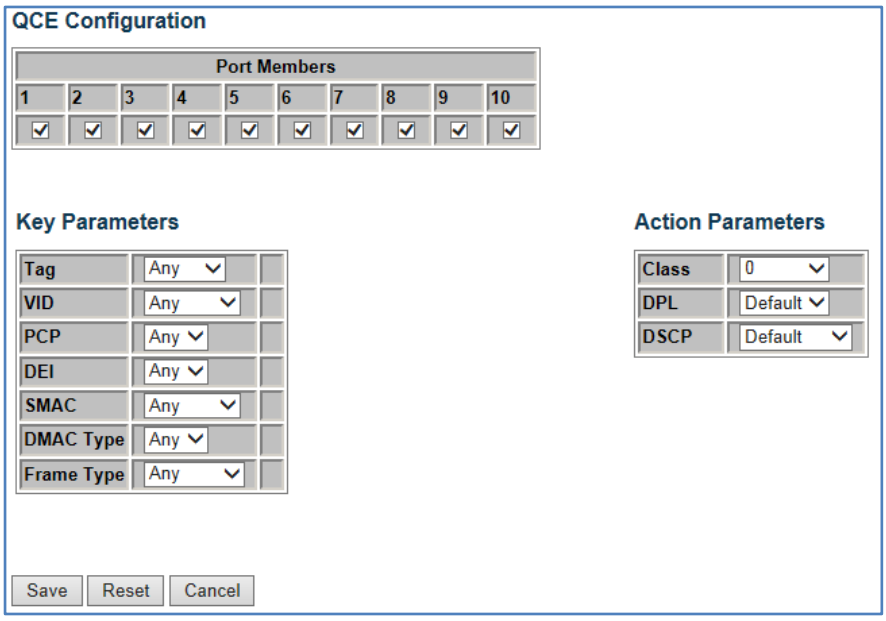
To Configure QCE Configuration：

A. **Click *Configuration/QoS/QoS Control List.***

B. **Click the ⊕ to add new QoS Control List**

C. **Scroll all parameters and evoke the Port Member to join the QCE rules.**

D. **Click Save to apply the setting, Reset to restore the previous setting.**



Storm Control

Using the Storm Control Configuration page to set limitation of broadcast, multi-cast and unknown uni-cast traffic to control traffic storms when switch device is malfunctioning. Traffic storm can degrade the network performance or halt the network.

LOCATION：

▼ Configuration

▼ QoS

- Storm Control

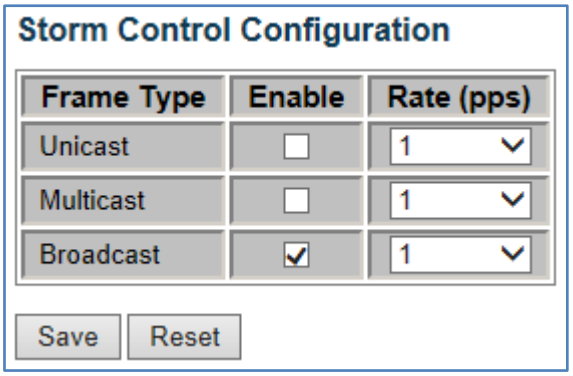
PARAMETERS：

Items	Description
Frame Type	The settings in a particular row apply to the frame type listed here: Unicast, Multicast or Broadcast.
Enable	Enable or disable the storm control status for the given frame type.
Rate	The rate unit is packets per second (pps). Valid values are：1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1K, 2K, 4K, 8K, 16K, 32K, 64K, 128K, 256K, 512K , 1024K, 2048K, 4096K, 8192K, 16384K or 32768K.

WEB Interface

To Configure QCE Configuration：

A. **Click *Configuration/QoS/Storm Control.***
B. **Enable Storm Control for Broadcast, Multi-cast and unknow uni-cast and Scroll down to select the Rate value.**
C. **Click Save to apply the setting, Reset to restore the previous setting.**



Port Mirroring

Using the Mirror Configuration page to mirror traffic from any source port to a target port.

LOCATION：

▼ Configuration

- Mirroring

PARAMETERS：

Items	Description
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.

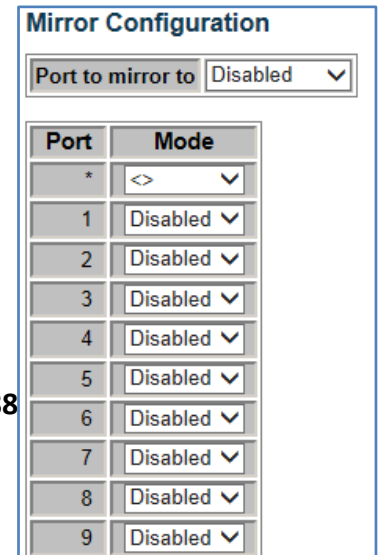
Enabled：Frames received and frames transmitted are mirrored on the mirror port.

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.

WEB Interface

To Configure Mirroring Configuration：

A. **Click *Configuration/Mirroring.***
B. **Select the destination port to which all mirrored traffic will be sent**
C. **Set the mirror mode on any of source ports to be mirrored.**
D. **Click Save to apply the setting, Reset to restore the previous setting.**



This chapter describes how to monitor all of the basic Functions, Configurations, System log, Traffic views and the switch (ports) states...etc.

Under the Monitor/System menu, it displays system information, Real-time CPU load, log and detailed syslog.

SYSTEM INFORMATION

Using System Information page to verfiy the firmware and hardware versions. It also displays System Contact, Device name, Location and System uptime.

LOCATION：

▼ Monitor
  ▼ System
    ▪ Information

PARAMETERS：

Items	Description
Contact	The system contact configured in Configuration| System | Information | System Contact.
Name	The system name configured in Configuration | System | Information |

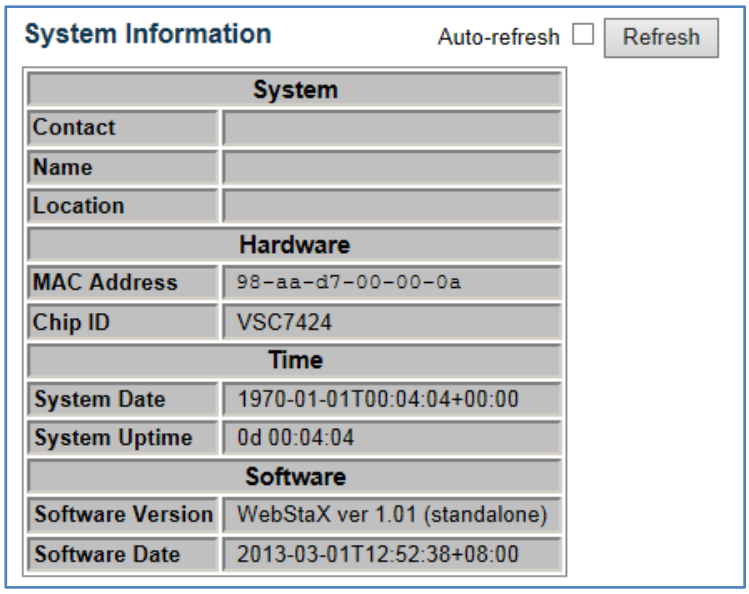
	System Name.
Location	The system location configured in Configuration | System | Information | System Location.
MAC Address	The MAC Address of this switch
Chip ID	The Chip ID of the switch
System Date	The current (GMT) system time and date. The system time is obtained through the Timing server running on the switch, if any.
System Uptime	The period of time the device has been operational.
Software Version	The software version of this switch
Software Date	The date when the switch software was produced

WEB Interface

To Update the System Information：

A. Click *Monitor/System/Information.*

- **Click "Refresh" button to refresh the page information manually.**
- **Check "Auto-refresh" checkbox to update page information automatically**



System Information

Auto-refresh ☐ Refresh

System	
Contact	
Name	
Location	
Hardware	
MAC Address	98-aa-d7-00-00-0a
Chip ID	VSC7424
Time	
System Date	1970-01-01T00:04:04+00:00
System Uptime	0d 00:04:04
Software	
Software Version	WebStaX ver 1.01 (standalone)
Software Date	2013-03-01T12:52:38+08:00

CPU Load

This page display the CPU Load, using an SVG graph. The load is measured as average over the last 100ms, 1 sec 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 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 plug-in installed to support SVG.

LOCATION：

▼ Monitor

▼ System

▪ CPU Load

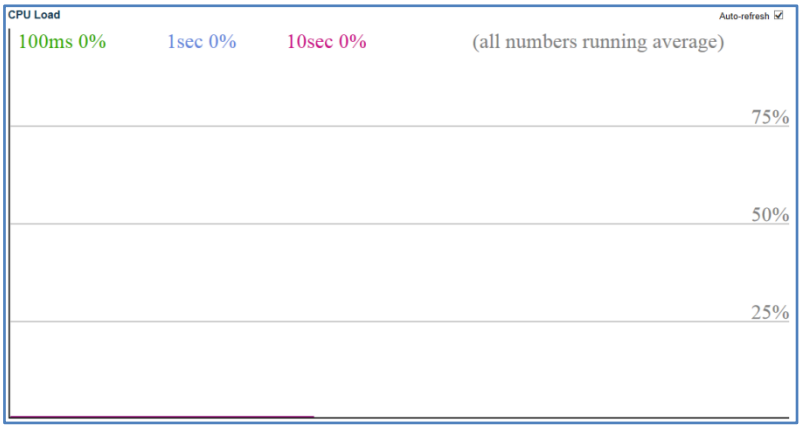
WEB Interface

To Update the System Information：

B. Click *Monitor/System/CPU Load.*

● **Default the "Auto-refresh" checkbox is checked**

to update page information automatically



Log

Using the System Log Information page to display event messages

LOCATION：

▼ Monitor

▼ System

■ Log

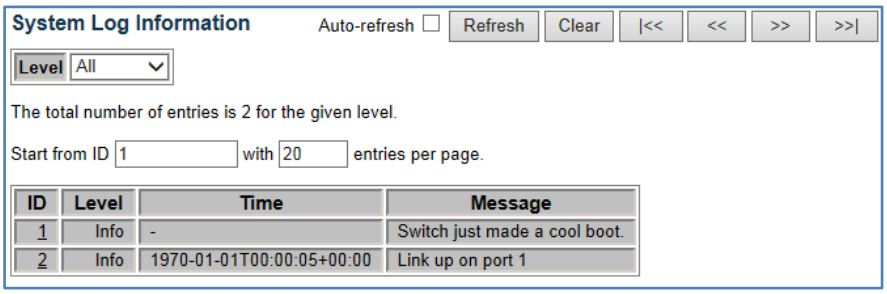
PARAMETERS：

Items	Description
ID	Event log ID
Level	The level of the system log entry. The following level types are supported: Info：Information level of the system log. Warning：Warning level of the system log.

	Error：Error level of the system log. All：All levels.
Time	The time of the system log entry.
Message	The message of the system log entry.
Buttons	Auto-refresh ☐：Check this box to enable an automatic refresh of the page at regular intervals. Refresh：Updates the system log entries, starting from the current entry ID. Clear：Flushes all system log entries. |<<：Updates the system log entries, starting from the first available entry ID. <<：Updates the system log entries, ending at the last entry currently displayed. >>：Updates the system log entries, starting from the last entry currently displayed. >>|：Updates the system log entries, ending at the last available entry ID.

To display the System Log：

A. **Click *Monitor/System/Log.***
B. **Specify the different level to show the log up.**
C. **Check the "auto-refresh" checkbox to update the system log automatically and click "clear" to clean the log.**



Figure

Detailed Log

Using the Detail System log information page to display the detail event log

LOCATION：

▼ Monitor
  ▼ System
    ▪ Detailed Log

PARAMETERS：

Items	Description
ID	Event log ID
Message	The detailed message of the system log entry.
Buttons	Refresh ：Updates the system log entries, starting from the current entry ID. |<< ：Updates the system log entries, starting from the first available entry

ID.

<< : Updates the system log entries, ending at the last entry currently displayed.

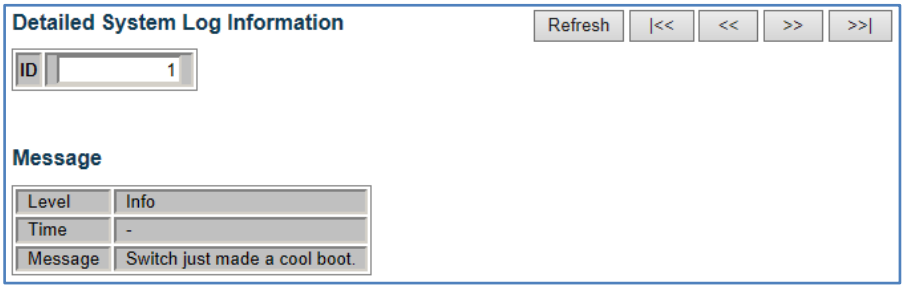
>> : Updates the system log entries, starting from the last entry currently displayed.

>>| : Updates the system log entries, ending at the last available entry ID.

WEB Interface

To display the Detailed System Log：

A. Click *Monitor/System/Detailed Log.*
B. Specify the Detailed system log.



Thermal Protection

Using the Thermal Protection Status page to show the thermal status for each port.

LOCATION：

▼ Monitor

- Thermal Protection

PARAMETERS：

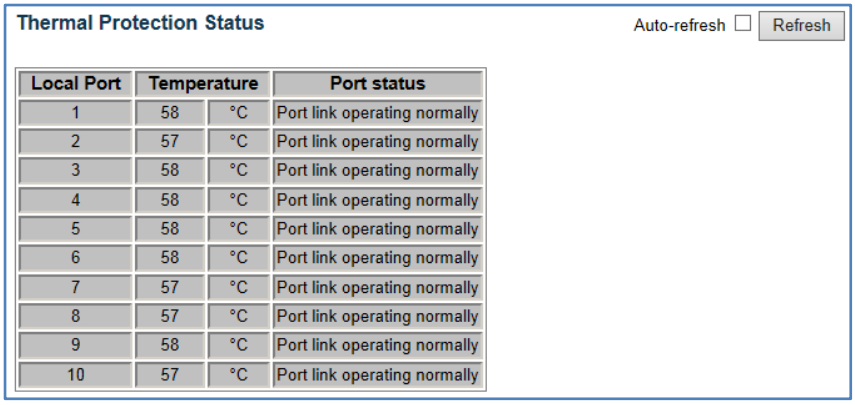
Items	Description
Thermal Portection Port Status	Shows if the port is thermally protected (link is down) or if the port is operating normally.
Port Status	Display Port Status, the port will shutdown if temperature exceed.
Buttons	Auto-refresh ☐ : Check this box to enable an automatic refresh of the page at regular intervals. Refresh : Updates the system log entries, starting from the current entry ID..

WEB Interface

To display each port's current temperature：

A. Click *Monitor/Thermal Protection.*

B. Display the current temperature for each port and port status.



Thermal Protection Status

Auto-refresh ☐ Refresh

Local Port	Temperature		Port status
1	58	°C	Port link operating normally
2	57	°C	Port link operating normally
3	58	°C	Port link operating normally
4	58	°C	Port link operating normally
5	58	°C	Port link operating normally
6	58	°C	Port link operating normally
7	57	°C	Port link operating normally
8	57	°C	Port link operating normally
9	58	°C	Port link operating normally
10	57	°C	Port link operating normally

FRONT PANEL

Using the Monitor/Ports menu to display the graphic image of

the front panel which indicates the connection state, basic statistics, the traffic crossing, the number of packets passing by each service queue and detailed statistics for each port.

Port s State

Using the Port State Overview page to display an image of switch's ports. Clicking specific port image to open detailed statistics of this port.

LOCATION：

▼ Monitor
  ▼ Ports
    ▪ State

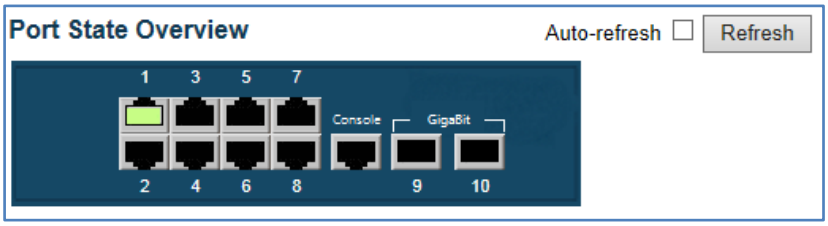
PARAMETERS：

Items	Description
Port State	The port states are illustrated as follows： RJ45 ports SFP ports State Disabled Down Link
Buttons	Auto-refresh ☐ ：Check this box to enable an automatic refresh of the page at regular intervals. Refresh ：Updates the system log entries, starting from the current entry ID.

WEB Interface

To display an image of the switch's ports：

A. Click *Monitor/Ports/State.*
B. Display current state of each port.
C. Check "Auto-refresh" to update the switch's port state automatically.



Traffic Overview

Using Port Statistics Overviewpage to display an overview of incoming and ongoing packets for each port.

LOCATION：

▼ Monitor
▼ Ports
■ Traffic Overview

PARAMETERS：

Items	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.

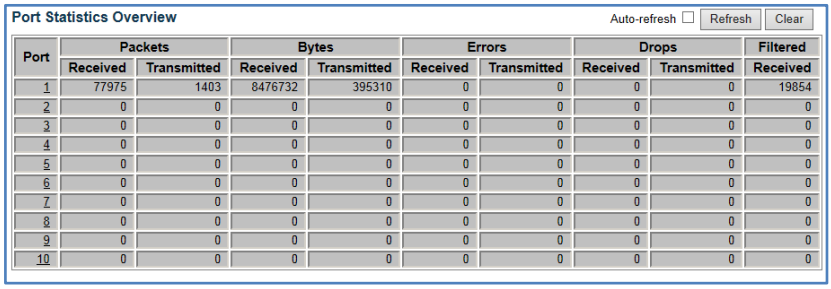
Errors	The number of frames received in error and the number of incomplete transmissions per port.
Drops	The number of frames discarded due to ingress or egress congestion.
Filtered	The number of received frames filtered by the forwarding process.
Buttons	Auto-refresh ☐ : Check this box to enable an automatic refresh of the page at regular intervals. Refresh : Updates the system log entries, starting from the current entry ID. Clear : Flushes all system log entries.

WEB Interface

To display a summary of port statistics：

A. Click *Monitor/Ports/Traffic Overview.*

B. Check "Auto-refresh" to update the switch's port state automatically and click "clear" to reset all data.



Port Statistics Overview

Auto-refresh ☐ Refresh Clear

Port	Packets		Bytes		Errors		Drops		Filtered
	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received
1	77975	1403	8476732	395310	0	0	0	0	19854
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

QoS Statistics

Using the Queuing Counters page to display the number of packets processed by each port.

LOCATION：

▼ Monitor
  ▼ Ports
    ■ QoS Statistics

PARAMETERS：

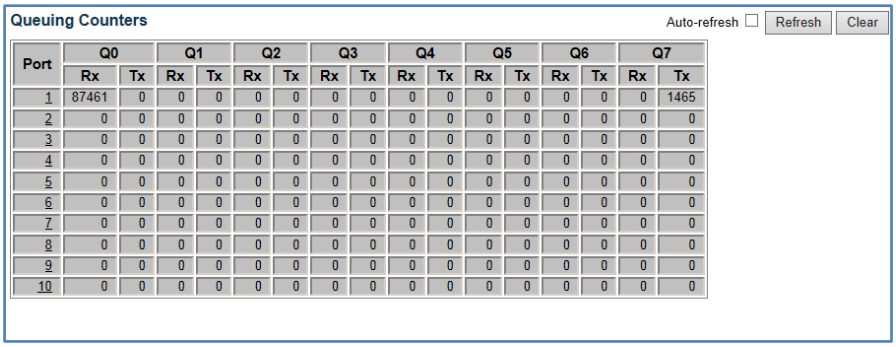
Items	Description
Port	The logical port for the settings contained in the same row.
Qn	There are 8 QoS queues per port. Q0 is the lowest priority queue.
RX/TX	The number of received and transmitted packets per queue.
Buttons	Auto-refresh ☐ ：Check this box to enable an automatic refresh of the page at regular intervals. Refresh ：Updates the system log entries, starting from the current entry ID. Clear ：Flushes all system log entries.

WEB Interface

To display a Queue Counters：

A. Click *Monitor/Ports/QoS Statistics.*
B. Check "Auto-refresh" to update the switch's port state automatically and click "clear" to

reset all data.



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	87461	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1465
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

QCL Status

Using QoS Control List Status to show QCE configured for different users or software modules and whether or not there is a conflict.

LOCATION：

▼ Monitor

▼ Ports

- QCL Status

PARAMETERS：

Items	Description
Users	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.

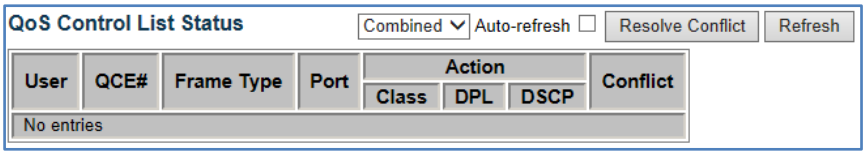
	LLC：Only (LLC) frames are allowed. SNAP：Only (SNAP) frames are allowed. IPv4：The QCE will match only IPV4 frames. IPv6：The QCE will match only IPV6 frames.
Port	Indicates the list of ports configured with the QCE.
Action	Indicates the classification action taken on ingress frame if parameters configured 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 Conflict status of QCL entries. As H/W resources are shared by multiple applications. It may happen that resources required to add a QCE may not be available, in that case it shows conflict status as 'Yes', otherwise it is always 'No'.

	Please note that conflict can be resolved by releaseing the H/W resources required to add QCL entry on pressing 'Resolve Conflict' button.
Buttons	Combined : Select the QCL Status from this drop down list. Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs at regular intervals. Resolve Conflict : Click to release the resources required to add QCL entry, incase conflict status for any QCL entry is 'yes' Refresh : Updates the system log entries, starting from the current entry ID.

WEB Interface

To display the status of QCE entries：

A. **Click *Monitor/Ports/QCL Status.***
B. **Select the user type to display from a dropdown list.**
C. **If any of the entries show the conflict, click "Rresolve Conflict" to resolve the conflict then click "refresh" to check the result.**



Detailed Port Statstics

Using the Detailed Port Statistics page to display the detailed statistic on network. All values have been accumulated since the system bootup.

LOCATION：

▼ Monitor

▼ Ports

- Detailed Statistics

PARAMETERS：

Items	Description
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	The number of received and transmitted

Transmit Size Counters	(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.

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

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

Transmit Error Counters

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

Buttons	Auto-refresh ☐ : Check this box to enable an automatic refresh of the page at regular intervals. Refresh : Updates the system log entries, starting from the current entry ID. Clear : Flushes all system log entries.

WEB Interface

To display the Detailed Port Statistics：

A. Click *Monitor/Ports/Detailed Statistics.*

B. Select the Port number to display Detailed Statistics of specific port.

Detailed Port Statistics Port 1 — Port 1 | Auto-refresh ☐ | Refresh | Clear

Receive Total		Transmit Total	
Rx Packets	119230	Tx Packets	1642
Rx Octets	12889147	Tx Octets	429224
Rx Unicast	2048	Tx Unicast	1631
Rx Multicast	34165	Tx Multicast	6
Rx Broadcast	83017	Tx Broadcast	5
Rx Pause	0	Tx Pause	0
Receive Size Counters		**Transmit Size Counters**	
Rx 64 Bytes	12791	Tx 64 Bytes	334
Rx 65-127 Bytes	91115	Tx 65-127 Bytes	441
Rx 128-255 Bytes	9286	Tx 128-255 Bytes	535
Rx 256-511 Bytes	4609	Tx 256-511 Bytes	166
Rx 512-1023 Bytes	1418	Tx 512-1023 Bytes	30
Rx 1024-1526 Bytes	11	Tx 1024-1526 Bytes	136
Rx 1527- Bytes	0	Tx 1527- Bytes	0
Receive Queue Counters		**Transmit Queue Counters**	
Rx Q0	119230	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	1642
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	30265		

ACL Status

This ACL Status page shows the 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 ACE is 256 on each switch.

LOCATION：

▼ Monitor
  ▼ Security
    ▼ Network
      ▪ ACL Status

PARAMETERS：

Items	Description
User	Indicates the ACL user.
Ingress Port	Indicates the ingress port of the ACE. Possible values are： All：The ACE will match all ingress port. Port：The ACE will match a specific ingress port.
Frame Type	Indicates the frame type of the ACE. Possible values are Any：The ACE will match any frame type. EType：The ACE will match Ethernet Type frames. Note that an Ethernet Type based ACE will not get matched by IP

	and ARP frames. ARP：The ACE will match ARP/RARP frames. IPv4：The ACE will match all IPv4 frames. IPv4/ICMP：The ACE will match IPv4 frames with ICMP protocol. IPv4/UDP：The ACE will match IPv4 frames with UDP protocol. IPv4/TCP：The ACE will match IPv4 frames with TCP protocol. IPv4/Other：The ACE will match IPv4 frames, which are not ICMP/UDP/TCP. IPv6: The ACE will match all IPv6 standard frames.
Action	Indicates the forwarding action of the ACE. Permit：Frames matching the ACE may be forwarded and learned. Deny：Frames matching the ACE are dropped.
Rate Limiter	Indicates the rate limiter number of the ACE. The allowed range is 1 to 16. When Disabled is displayed, the rate limiter operation is disabled.
Port Redirect	Indicates the port redirect operation of the ACE. Frames matching the ACE are redirected to the port number. The allowed values are

	Disabled or a specific port number. When Disabled is displayed, the port redirect operation is disabled.
Mirror	Specify the mirror operation of this port. The allowed values are： Enabled：Frames received on the port are mirrored. Disabled：Frames received on the port are not mirrored. The default value is "Disabled".
CPU	Forward packet that matched the specific ACE to CPU.
CPU Once	Forward first packet that matched the specific ACE to CPU.
Counter	The counter indicates the number of times the ACE was hit by a frame.
Conflict	Indicates the hardware status of the specific ACE. The specific ACE is not applied to the hardware due to hardware limitations.
Buttons	Combined：Select the QCL Status from this drop down list. Auto-refresh：Check this box to refresh the page automatically. Automatic refresh occurs at regular

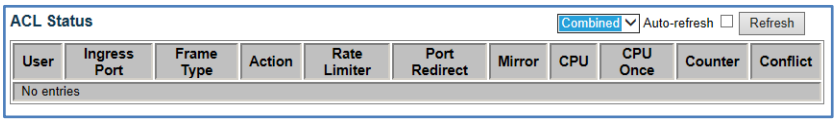
intervals.'

Refresh : Updates the system log entries, starting from the current entry ID.

WEB Interface

To display ACL Status：

A. Click *Monitor/Security/Network/ACL Status*
B. Select a software module from the scroll-down list.



RADIUS Overview

Using the RADIUS Overview page to display a list of configured RADIUS Server

LOCATION：

▼ Monitor
▼ Security
▼ AAA
■ RADIUS Overview

PARAMETERS：

Items	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.

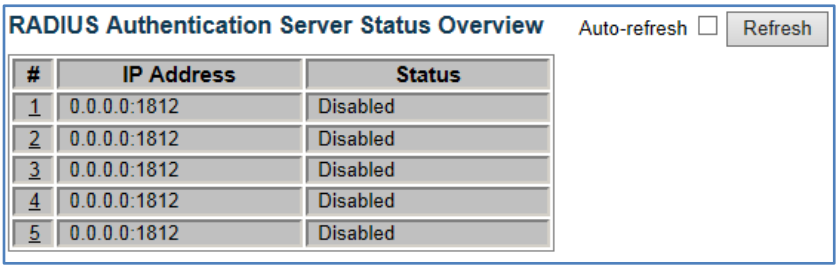
Status	The current status of the server. This field takes one of the following values： Disabled：The server is disabled. Not Ready：The server is enabled, but IP communication is not yet up and running. Ready：The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept access attempts. Dead (X seconds left)：Access attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.
Buttons	Combined：Select the QCL Status from this drop down list. Auto-refresh：Check this box to refresh the page automatically. Automatic refresh occurs at regular

	intervals.'
	Refresh : Updates the system log entries, starting from the current entry ID.

WEB Interface

To display a list of RADIUS Server：

A. Click *Monitor/Security/AAA/RADIUS Overview*



RADIUS Authentication Server Status Overview Auto-refresh ☐ Refresh

#	IP Address	Status
1	0.0.0.0:1812	Disabled
2	0.0.0.0:1812	Disabled
3	0.0.0.0:1812	Disabled
4	0.0.0.0:1812	Disabled
5	0.0.0.0:1812	Disabled

RADIUS Details

Using the RADIUS Details page to display statistics for RADIUS Server.

LOCATION：

▼ Monitor
  ▼ Security
    ▼ AAA
      ▪ RADIUS Details

PARAMETERS：

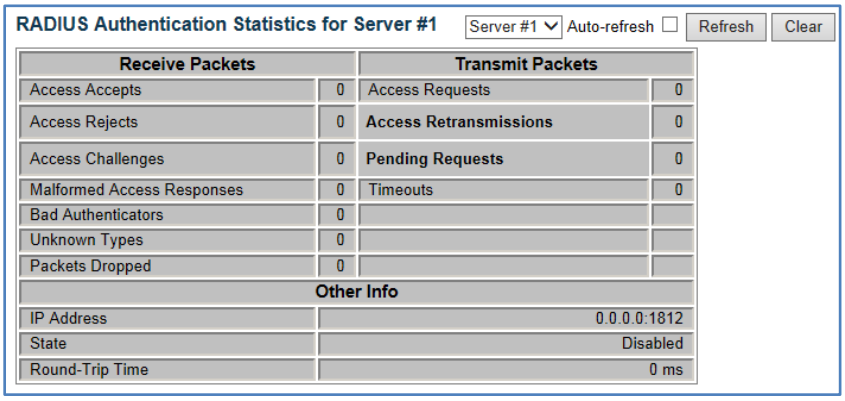
Items	Description
Receive	The counters of Receive Packets, including

packets	following parameters： (Access Accepts, Access Rejects, Access Challenges, Malformed Access Responses, Bad Authenticators, Unknown Types, Packets Dropped)
Transmit Packets	The counters of Transmit Packets, including following parameters： (Access Requests, Access Retransmissions, Pending Requests, Timeouts)
Other Info.	IP Address：Show the IP Address of RADIUS server. State：Show the state of RADIUS server Round-Trip Time：the handshake time between RADIUS Server and clients
Buttons	Auto-refresh ☐ ：Check this box to refresh the page automatically. Automatic refresh occurs at regular intervals.' Refresh ：Updates the system log entries, starting from the current entry ID. Clear ：Flushes all system log entries.

WEB Interface

To display a detail information of RADIUS Server：

A. Click *Monitor/Security/AAA/RADIUS Details*



LACP System Status

Using the LACP System Status page to display an overview of LACP groups.

LOCATION：

▼ Monitor

▼ LACP

- System Status

PARAMETERS：

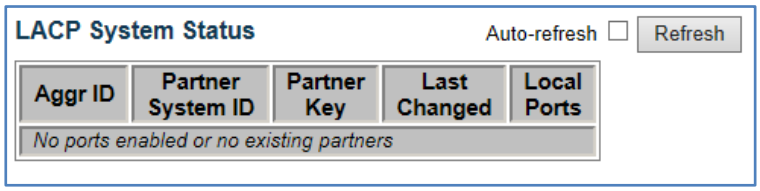
Items	Description
Aggr ID	The Aggregation ID associated with this aggregation instance. For LLAG the id is shown as 'isid:aggr-id' and for GLAGs as 'aggr-id'
Partner System ID	The system ID (MAC address) of the aggregation partner.
Partner Key	The Key that the partner has assigned to this aggregation ID
Last changed	The time since this aggregation changed.

Local Ports	Shows which ports are a part of this aggregation for this switch.
Buttons	Auto-refresh ☐ : Check this box to refresh the page automatically. Automatic refresh occurs at regular intervals.'
	Refresh : Updates the system log entries, starting from the current entry ID.

WEB Interface

To display an overview of LACP group active on this switch：

A. Click *Monitor/LACP/System Status*



LACP Port Status

Using the LACP Port Status page to display information on the LACP groups active on each port.

LOCATION：

▼ Monitor

▼ LACP

- Port Status

PARAMETERS：

Items	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.
Partner System ID	The partner's System ID (MAC address).
Partner Port	The partner's port number connected to this port.
Buttons	Auto-refresh ☐ : Check this box to refresh the page automatically. Automatic refresh occurs at regular intervals.' Refresh : Updates the system log entries, starting from the current entry ID.

WEB Interface

To display LACP Status for local ports：

A. Click *Monitor/LACP/Port 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	-	-	-	-

LACP Port Status

Using the LACP Port Statistics page to display statistics on LACP control packets cross on each port.

LOCATION：

▼ Monitor

▼ LACP

- Port Statistics

PARAMETERS：

Items	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

Buttons	frames have been discarded at each port. Auto-refresh ☐ : Check this box to refresh the page automatically. Automatic refresh occurs at regular intervals.' Refresh : Updates the system log entries, starting from the current entry ID. Clear : Flushes all system log entries.

WEB Interface

To display LACP Port Statistics for local ports：

A. Click *Monitor/LACP/Port Statistics*

Loop Protection

Using Loop Protection Status page to display the loop status.

LOCATION：

▼ Monitor

- Loop Protection

PARAMETERS：

Items	Description
Port	The switch port number of the logical port.
Action	The currently configured port action.

Transmit	The currently configured port transmit mode.
Loops	The number of loops detected on this port.
Status	The current loop protection status of the port.
Loop	Whether a loop is currently detected on the port.
Time of Last Loop	The time of the last loop event detected.
Buttons	Auto-refresh ☐ : Check this box to refresh the page automatically. Automatic refresh occurs at regular intervals.' Refresh : Updates the system log entries, starting from the current entry ID.

WEB Interface

To display the Loop Status for each port：

A. Click *Monitor/Loop Protection.*

INFORMATION OF SPANNING TREE

Using Monitor menu to display Spanning Tree bridge status, CIST port status for physical ports of the currently switch and statistics for STP packets.

Bridge Status

Using STP Detailed Bridge Status page to display STA information on the global bridge and individual ports.

LOCATION：

▼ Monitor

▼ Spanning Tree

- Bridge Status

PARAMETERS：

Items	Description
Bridge Instance	The Bridge instance - CIST, MST1, ...
Bridge ID	The Bridge ID of this Bridge instance.
Root ID	The Bridge ID of the currently elected root bridge.
Root Port	The switch port currently assigned the root port role.
Root Cost	Root Path Cost. For the Root Bridge this is zero. For all other Bridges, it is the sum of the Port Path Costs on the least cost path to the Root Bridge.
Regional Root	The Bridge ID of the currently elected regional root bridge, inside the MSTP region of this bridge. (For the CIST instance only).
Internal Root Cost	The Regional Root Path Cost. For the Regional Root Bridge this is zero. For all other CIST instances in the same MSTP region, it is the sum of the Internal Port Path Costs on the least cost path to the Internal Root Bridge. (For

	the CIST instance only).
Topology Flag	The current state of the Topology Change Flag of this Bridge instance.
Topology Change Count	The number of times where the topology change flag has been set (during a one-second interval).
Topology Last	The time passed since the Topology Flag was last set.

CIST Ports & Aggregations State

Port	The switch port number of the logical STP port.
Port ID	The port id as used by the STP protocol. This is the priority part and the logical port index of the bridge port.
Role	The current STP port role. The port role can be one of the following values: AlternatePort BackupPort RootPort DesignatedPort.
State	The current STP port state. The port state can be one of the following values: Discarding Learning Forwarding.
Path Cost	The current STP port path cost. This will either be a value computed from the Auto setting, or any explicitly configured value.
Edge	The current STP port (operational) Edge Flag. An Edge Port is a switch port to which no Bridges are attached. The flag may be automatically computed or explicitly

	configured. Each Edge Port transits directly to the Forwarding Port State, since there is no possibility of it participating in a loop.
Point2Point	The current STP port point-to-point flag. A point-to-point port connects to a non-shared LAN media. The flag may be automatically computed or explicitly configured. The point-to-point properties of a port affect how fast it can transit to STP state.
Uptime	The time since the bridge port was last initialized.
Buttons	Auto-refresh ☐ : Check this box to refresh the page automatically. Automatic refresh occurs at regular intervals.' Refresh : Updates the system log entries, starting from the current entry ID.

STP Detailed Bridge Status Auto-refresh ☐ Refresh

STP Bridge Status	
Bridge Instance	CIST
Bridge ID	80:00-98:AA:D7:00:00:0A
Root ID	80:00-00:4F:4A:A8:01:45
Root Cost	200000
Root Port	1
Regional Root	80:00-98:AA:D7:00:00:0A
Internal Root Cost	0
Topology Flag	Steady
Topology Change Count	4
Topology Change Last	0d 01:01:00

CIST Ports & Aggregations State

Port	Port ID	Role	State	Path Cost	Edge	Point2Point	Uptime
1	128:001	RootPort	Forwarding	200000	No	Yes	0d 01:01:03

WEB Interface

To display detailed information for the STP bridge instance, along with port state for all active ports associated：

A. Click *Monitor/Spanning Tree/Bridge Status* to display the information.

STP Port Status

Using STP Port Status page to display the STP CIST port status for physical ports of the currently selected.

LOCATION：

▼ Monitor
  ▼ Spanning Tree
    ▪ Port Status

PARAMETERS：

Items	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 BackupPort RootPort DesignatedPort Disabled.
CIST State	The current STP port state of the CIST port. The port state can be one of the following values: Discarding Learning Forwarding
Uptime	The time since the bridge port was last initialized.

Buttons	Auto-refresh ☐ : Check this box to refresh the page automatically. Automatic refresh occurs at regular intervals.' Refresh : Updates the system log entries, starting from the current entry ID.

WEB Interface

To display STP Port Status：

A. Click *Monitor/Spanning Tree/Port Status* to display the participating STP Ports Status.

STP Port Statistics

Using STP Port Statistics page to display statistics on Spanning Tree Protocol packets crossing each port.

LOCATION：

▼ Monitor
  ▼ Spanning Tree
    ▪ Port Statistics

PARAMETERS：

Items	Description
Port	The switch port number of the logical STP 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.
Buttons	Auto-refresh ☐ : Check this box to refresh the page automatically. Automatic refresh occurs at regular intervals.' Refresh : Updates the system log entries, starting from the current entry ID. Clear : Flushes all system log entries.

WEB Interface

To display information on STP Port Statstics：

A. Click *Monitor/Spanning Tree/Port Statstics* to display the STP Ports Statistics.

STP Statistics Auto-refresh ☐ Refresh Clear

Port	Transmitted				Received				Discarded	
	MSTP	RSTP	STP	TCN	MSTP	RSTP	STP	TCN	Unknown	Illegal
1	0	5	0	0	0	2283	0	0	0	0

SHOW IGMP SNOOPING INFORMATION

Using IGMP SNOOPING pages to display IGMP Snooping statistics, Router port status and group information.

IGMP Snooping Status

Using IGMP Snooping Status page to display IGMP querier status, snooping statistics for each VLAN

LOCATION：

▼ Monitor
  ▼ IPMC
    ▼ IGMP Snooping
      ▪ Status

PARAMETERS：

Items	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	The number of Received V2 Reports

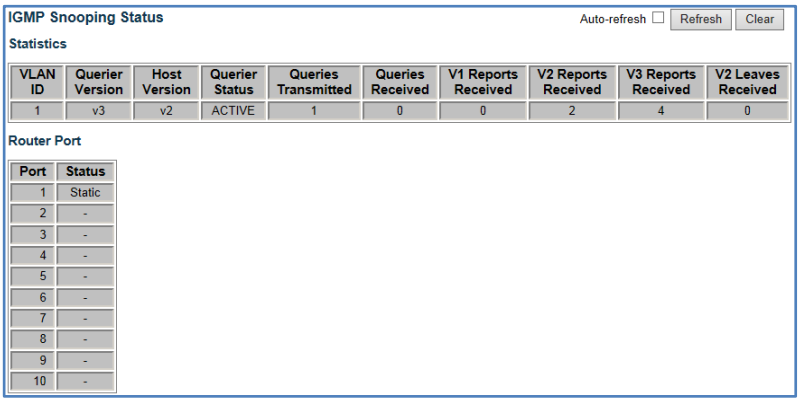
Received V3 Reports	The number of Received V3 Reports
Received V2 Leaves	The number of Received V2 Leaves.
Received Router Port	Display which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or IGMP querier. Static denotes the specific port is configured to be a router port. Dynamic denotes the specific port is learnt to be a router port. Both denote the specific port is configured or learnt to be a router port.
Port	Switch port number
Status	Indicate whether specific port is a router port or not.
Buttons	Auto-refresh ☐ : Check this box to refresh the page automatically. Automatic refresh occurs at regular intervals.' Refresh : Updates the system log entries, starting from the current entry ID.

Clear	: Flushes all system log entries.

WEB Interface

To display IGMP Snooping Status information :

A. Click *Monitor/IPMC/IGMP Snooping/Status* to display the STP Ports Statistics.



VLAN ID	Querier Version	Host Version	Querier Status	Queries Transmitted	Queries Received	V1 Reports Received	V2 Reports Received	V3 Reports Received	V2 Leaves Received
1	v3	v2	ACTIVE	1	0	0	2	4	0

Port	Status
1	Static
2	-
3	-
4	-
5	-
6	-
7	-
8	-
9	-
10	-

IGMP Snooping Group Information

Using IGMP Snooping Group Information page to display the port member of each service group.

LOCATION :

▼ Monitor
  ▼ IPMC
    ▼ IGMP Snooping
      ▪ Groups Information

PARAMETERS :

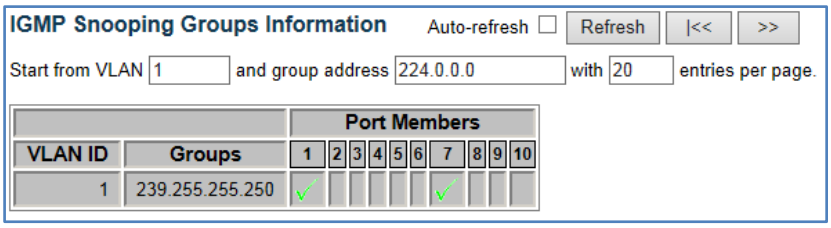
Items	Description
VLAN ID	The VLAN ID of the entry.
Groups	Group address of the group displayed.

Port Members	Ports under this group.
Buttons	Auto-refresh ☐ : Check this box to refresh the page automatically. Automatic refresh occurs at regular intervals.' Refresh : Updates the system log entries, starting from the current entry ID. |<< : Updates the table, starting with the first entry in the IGMP group table. << : Updates the table, starting with the entry after the last entry currently displayed..

WEB Interface

To display IGMP Snooping Group information：

A. **Click *Monitor/IPMC/IGMP Snooping/Groups information* to display group port members.**



SHOW
POWER OVER ETHERNET

Using Power Over Ethernet Status page to display total power consumption, PD Class, Power used, Current used, Priority and Port status for each port.

LOCATION：

▼ Monitor

- PoE

PARAMETERS：

Items	Description
Local Port	This is the logical port number for this row.
PD Class	Each PD is classified according to a class that defines the maximum power the PD will use. The PD Class shows the PDs class. Five Classes are defined： Class 0：Max. power 15.4 W Class 1：Max. power 4.0 W Class 2：Max. power 7.0 W Class 3：Max. power 15.4 W

	Class 4：Max. power 34.2 W
Power Requested	The Power Requested shows the requested amount of power the PD wants to be reserved.
Power Allocated	The Power Allocated shows the amount of power the switch has allocated for the PD.
Power Used	The Power Used shows how much power the PD currently is using.
Current Used	The Power Used shows how much current the PD currently is using.
Priority	The Priority shows the port's priority configured by the user.
Port Status	The Port Status shows the port's status.
Buttons	Auto-refresh ☐ ：Check this box to refresh the page automatically. Automatic refresh occurs at regular intervals.' Refresh ：Updates the system log entries, starting from the current entry ID.

WEB Interface

To display Power Over Ethernet information：

A. Click *Monitor/PoE* to display PoE information for each port and total power consumption.

DISPLAY INFORMATION OF VLANs

Using Monitor pages for VLANs to display port members of VLANs and its' VLAN attributes corresponding each port.

VLAN Membership

Using VLAN Membership Status for specific users page to display the information of all VLAN status and reports.

LOCATION：

▼ Monitor
  ▼ VLANs
    ▪ PoE

PARAMETERS：

Items	Description
VLAN USER	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. 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 ✓ will be displayed. If a port is included in a Forbidden port list, an image ✕ 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 class ified to the VLAN ID to be forwarded on the respective VLAN member ports.
Buttons	Static : Select VLAN Users from this drop down list. Auto-refresh : Check this box to refresh

	the page automatically. Automatic refresh occurs at regular intervals.'
	Refresh : Updates the system log entries, starting from the current entry ID.

WEB Interface

To display VLAN Membership Status for specific users：

A. Click *Monitor/VLANs/VLAN Membership* to display VLAN Membership information.

VLAN Port

Using VLAN Port Status for specific users page to display the information of all VLAN Port status.

LOCATION：

▼ Monitor

▼ VLANs

■ VLAN Port

PARAMETERS：

Items	Description
Port	The logical port for the settings contained in the same row.

PVID	Shows the VLAN identifier for that port. The allowed values are 1 through 4095. The default value is 1.
Port Type	Shows the Port Type. Port type can be any of Unaware, C-port, S-port, Custom S-port. If Port Type is Unaware, all frames are classified to the Port VLAN ID and tags are not removed. C-port is Customer Port. S-port is Service port. Custom S-port is S-port with Custom TPID.
Ingress Filtering	Shows the ingress filtering on a port. This parameter affects VLAN ingress processing. If ingress filtering is enabled and the ingress port is not a member of the classified VLAN, the frame is discarded.
Frame Type	Shows whether the port accepts all frames or only tagged frames. This parameter affects VLAN ingress processing. If the port only accepts tagged frames, untagged frames received on that port are discarded.
Tx Tag	Shows egress filtering frame status whether tagged or untagged.
UVID	Shows UVID (untagged VLAN ID). Port's UVID determines the packet's behaviour at the egress side.
Conflicts	Shows status of Conflicts whether exists

	or not. When a Volatile VLAN User requests to set VLAN membership or VLAN port configuration, the following conflicts can occur： Functional Conflicts between features. Conflicts due to hardware limitation. Direct conflict between user modules.
Buttons	Static : Select VLAN Users from this drop down list. Auto-refresh ：Check this box to refresh the page automatically. Automatic refresh occurs at regular intervals.' Refresh ：Updates the system log entries, starting from the current entry ID.

WEB Interface

To display VLAN Port Status for specific users：

A. Click *Monitor/VLANs/VLAN Port* to display VLAN Port information.

WEB DIAGNOSTICS PING

This chapter provides IPv4 ping for test the connectivity of network.

DIAGNOSTICS ICMP

IPv4 Ping

Using ICMP Ping page to send ICMP request packet to another connected point to check if it is connect.

LOCATION：

▼ Diagnostic

- Ping

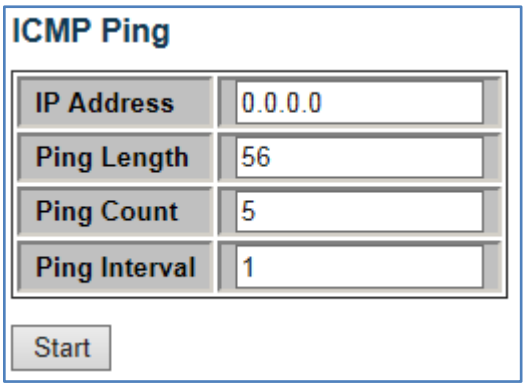
PARAMETERS：

Items	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.

WEB Interface

To Ping another IP device on the network：

A. Click *Diagnostics/Ping to run the testing*.


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

Chapter 4 *Web Maintenance* Restart Device

This chapter describes how to restart device, reload device
to manufactory default, saving or restore configuration and firmware upgrading , swapping.

RESTART DEVICE

Using the Restart Device page to restart the switch.

LOCATION：

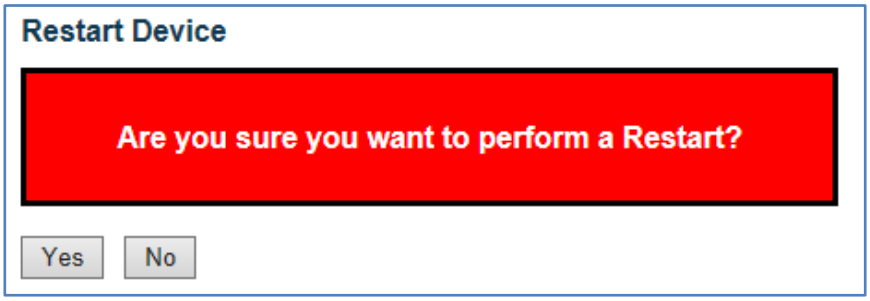
▼ Maintenance

- Restart Device

WEB Interface

To restart the switch：

A. Click Maintanence/*Restart Device to restart the switch*.
B. Click "Yes" to confirm the restart process and "No" to cancel the restart process.



FACTORY DEFAULTS

Using Factory Defaults page to reset the switch to

manufactory default setting.

LOCATION：

▼ Maintenance

- Factory Defaults

WEB Interface

To resett the switch：

A. Click Maintanence/*Factory Defaults to reset the switch to manufactory default settings*.

B. Click "Yes" to confirm the process and "No" to cancel.

SOFTWARE UPLOAD

Using Firmware Update page to upgrade the firmware of the switch.

LOCATION：

▼ Maintenance

▼ Software

- Upload

PARAMETERS：

Items	Description
Buttons	Browse to the location of a software image and click Upload After the software image is uploaded, a page announces that the firmware update is initiated. After about a minute, the firmware is updated and the switch restarts. *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.*

WEB Interface

To upgrade the firmware of the switch：

A. Click Maintanence/*Software/Upload* and browse the firmware file then click Upload.

SWAP IMAGE

Using Software Image Selection page to swap the firmware to alternative image.

LOCATION：

▼ Maintenance

▼ Software

- Image Select

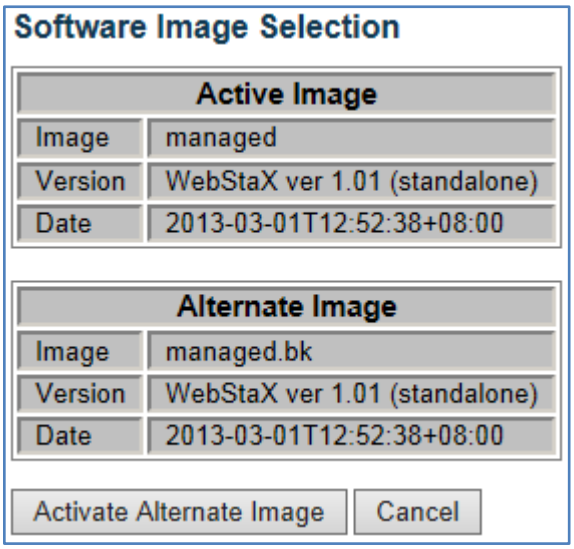
PARAMETERS：

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

WEB Interface

To swap the firmware to alternative image for the switch：

A. Click Maintanence/*Software/Image Select* to swap to alternative image.


Software Image Selection
Active Image
Image
managed
Version
WebStaX ver 1.01 (standalone)
Date
2013-03-01T12:52:38+08:00
Alternate Image
Image
managed.bk
Version
WebStaX ver 1.01 (standalone)
Date
2013-03-01T12:52:38+08:00
Activate Alternate Image
Cancel

SAVE CONFIGURATION

Using Configuration Save page to save your switch's configuration to management PC/NB.

LOCATION：

▼ Maintenance

▼ Configuration

■ Save

PARAMETERS：

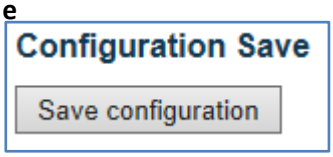
Items	Description
Buttons	Save configuration ：Click the button, it will pop out a file saving dialog, the default name is "config.xml"

WEB Interface

To click "Save configuration" to save config：

A. Click *Maintanence/Configuration/Save* to save to alternative image.

e



UPLOAD CONFIGURATION

Using Configuration Upload page to restore your switch's to backup configuration from management PC/NB.

LOCATION：

▼ Maintenance

▼ Configuration

- Upload

PARAMETERS：

Items	Description
Buttons	Browse to the location of configuration file and click Upload After the configuration file is uploaded, a page announces that the configuration upload done. Reset the device to make configuration applied

WEB Interfac

To click "Configuration Upload" to restore config：

Click *Maintanence/Configuration/Upload* to restore a backupconfiguration file.

제 품 보 증 서			
제 품 명	Giga 8Port Management POE L2 Layer(SFP x 2)	모 델 명	NEXT-POE4008L2-130
구입일자		보증 기간	2년
고객성명		전 화	
고객주소			
판 매 점		전 화	
판매점 주소			
제조자 (수입원)	(주)이지넷 유비쿼터스	전 화	02 - 715 - 0372
제조자 (수입원) 주소	WWW.EZ-NET.CO.KR 에서 확인을 하세요.		

주 의 사 항

A. 소비자는 제품보증서를 판매처(판매자)로부터 작성 제공 받아야 합니다. 그렇지 않을 경우 보증기간은 제품에 표시된 제조년월일을 기준으로 합니다.
B. 본 제품은 제조년월로부터 6개월 내에 판매 되어야 하며, 제조년월로부터 6개월이 지난 다음 판매된 경우 보증 기간은 제조년월로부터 12개월로 처리가 됩니다.
C. 슬림PC를 위한 LP브라켓등은 소모품으로 다시 지급되지 않으며 분실(파손)시 유상 구입하셔야 합니다.
D. 슬림PC를 위한 LP브라켓등의 유상구입은 제품보증기간 내에만 가능하나, 재고가 있으면 제품보증기간이 지나도 구입 가능 합니다.
E. 천재지변으로 인한 것은 유상수리입니다.
F. 소비자과실로 인한 고장은 무상수리가 되지 않을 수도 있습니다.
G. 본 제품의 A/S는 소비자가 A/S센터(고객지원센타)를 방문하는 것을 원칙으로 합니다.
H. 우편(택배)이나 퀵서비스를 통한 A/S접수 시 제품을 당사로 보내는 것은 소비자의 책임이며, 당사에서 소비자에게 보내는 것은 당사의 책임입니다.

- 본 설명서에 사용된 특정 단어들은 각각이 소유권회사에 있습니다.
- 본 설명서는 무단 복제를 금합니다.
- 본 설명서에 있는 내용은 편의성에 의하여 변경될 수 있습니다.
- 본 제품의 구성품 및 사양은 예고 없이 변경될 수 있습니다.