User Manual

8 Port SNMP Managed Layer2 + 2SFP Switch

NEXT-3008GL2

ABOUTTHISMANUAL

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

AudienceThis 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), Standard and Simple Network Management Protocol(SNMP).

Publication Date: Feb, 2015
Version 1.00

CONTENTS

REVISION HISTORY

ABOUT THIS MANUAL

CONTENTS

FIGURES

TABLES

CHAPTER1INTRODUCTION

Product Overview

Features

Specifications

Performance

Package Contents

CHAPTER 2HARDWARE DESCRIPTION

Physcial Dimensions / Weight

Front Panel

LED Indicator

Rear Panel

Hardware Installation

CHAPTER 3WEB MANAGEMENT

Initial Switch Configuration

Web Interface

Configuration Option

Front Panel

Menu Tree

Publication Date: Feb, 2015
Version 1.00

CHAPTER 4WEB CONFIGURATION

- Configuration
  - System
    - Information
    - IP
    - IPv6
    - NTP
    - Time
    - Log
  - Power Reduction
    - LED
    - EEE
  - Ports
  - Security
    - Switch
      - Users
      - Privilege Levels
      - Auth Method
      - SSH
      - HTTPS
      - Access Management
      - SNMP
        - System
        - Communities
        - Users
        - Groups
        - Views
        - Access
      - RMON
        - Statistics
        - History
        - Alarm
        - Event
    - Network
      - Limit Control
      - NAS
      - ACL

- Ports
- Rate Limiters
- Access Control List
- DHCP
  - Snooping
  - Relay
- IP Source Guard
  - Configuration
  - Static Table
- ARP Inspection
  - Configuration
  - Static Table
- AAA
- Aggregation
  - Statics
  - LACP
- Loop Protection
- Spanning Tree
  - Bridge Settings
  - MSTI Mapping
  - MSTI Priority
  - CIST Ports
  - MSTI Ports
- MVR
- IPMC
  - IGMP Snooping
    - Basic Configuration
    - VLAN Configuration
    - Port Group Filtering
  - MLD Snooping
    - Basic Configuration
    - VLAN Configuration
    - Port Group Filtering
- LLDP
  - LLDP
  - LLDP-MED
- MAC Table

- VLANs
  - VLAN Membership
  - Ports
- Private VLANs
  - PVLAN Membership
  - Port Isolation
- QoS
  - Port Classification
  - Port Policing
  - Port Scheduler
  - Port Shaping
  - Port Tag Remarking
  - Port DSCP
  - DSCP-Based QoS
  - DSCP Translation
  - DSCP Classification
  - QoS Control List
  - Storm Control
- Mirroring
- UPnP
- sFlow

CHAPTER 5WEB MONITOR

- Monitor
  - System
    - Information
    - CPU Load
    - Log
    - Detailed Log
  - Ports
    - State
    - Traffic Overview
    - QoS Statistics
    - QCL Status
    - Detailed Statistics
  - Security

- Access Management Statistics
- Network
  - Port Security
    - Switch
    - Port
  - NAS
    - Switch
    - Port
  - ACL Status
  - DHCP
    - Snooping Statistics
    - Relay Statistics
  - ARP Inspection
  - IP Source Guard
- AAA
  - RADIUS Overview
  - RADIUS Details
- Switch
  - RMON
    - Statistics
    - History
    - Alarm
- LACP
  - System Status
  - Port Status
  - Port Statistics
- Loop Protection
- Spanning Tree
  - Bridge Status
  - Port Status
  - Port Statistics
- MVR
  - Statistics
  - MVR Channel Groups
  - MVR SFM Information
- IPMC
  - IGMP Snooping

- Status
- Groups Information
- IPv4 SFM Information
- MLD Snooping
  - Status
  - Groups Information
  - IPv6 SFM Information
- LLDP
  - Neighbours
  - LLDP-MED Neighbours
  - EEE
  - Port Statistics
- MAC Table
- VLANs
  - VLAN Membership
  - VLAN Port
- VCL
  - MAC-based VLAN
- sFlow

CHAPTER 6WEB DIAGNOSTICS

- Diagnostics
  - Ping
  - Ping6

CHAPTER 7WEB MAINTENANCE

- Maintenance
  - Restart Device
  - Factory Defaults
  - Software
    - Upload
    - Image Select
  - Configuration
    - Save
    - Upload

Chaper 1 INTRODUCTION

This chapter provides an overview of this Web Smart switch, and introduces thekey features and supported specificationsof thisWeb Smart switches.

PRODUCT OVERVIEW

This switch is a Web Smart switch equiped with 8-ports 10/100/1000BaseT(X) and 2-ports gigabit SFP open slots. It provides a broad range of features for Layer2 switching.

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

Table 1. Features

Features	Descriptions
Dual Images	Prevent any kind of upgrading process failure
IPv4	Supports IPv4 addressing, management and QoS
IPv6	Supports IPv6 addressing, management and MLD snooping
	Support local and remote syslog server with 3 levels(Info, Warning, Error)
Power Saving	LED Power management 802.3az EEE
Security	Private VLAN(Static) ACLs for filtering, policing, and port copy, including ACL wizar

Table 1. Features	**(continued)**
Authentication	Telnet, Web - username/password Telnet - SSH SNMP v1/v2c – 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 Aggregation	IEEE 802.3ad Link Aggregation, static and LACP
Spanning Tree Algorithm	Supports standard STP, Rapid Spanning Tree Protocol (RSTP), (Multiple Spanning Tree Protocol (MSTP)
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

Table 2, Specifications

Standard
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
24 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
RFC 3621 Power Ethernet

PERFORMANCES

Table 3, Performance

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

Chaper 2 HARDWARE DESCRIPTION

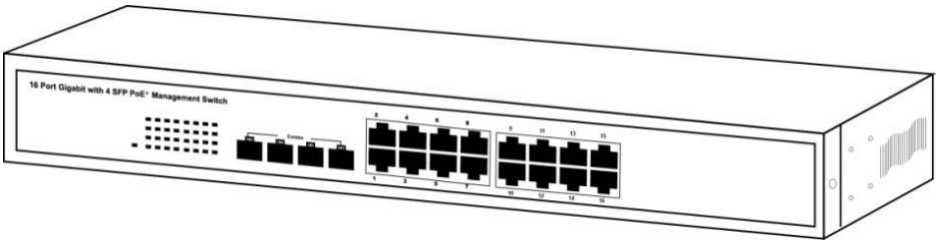
This chapter primarily presents hardware of the switch, physical dimenstions and functional overview would be described.

PHYSICAL DIMENSION AND WEIGHT

~~100 x 100 x 100 mm (H x W x D) / 4.6kg~~

FRONT PANEL

The Front Panel of the Web Smart 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.

Table 4, LED INDICATORS

LED	Status	Description
Power	On	System on
	OFF	System off
Link/ACT	Flashing	Link and Data Activating
	OFF	Port is disable or disconnected

REAR PANEL

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

HARDWARE INSTALLATION

The Attach with a PICTURE with Power cord, RJ45 cable, And SFP if needed. Then step1~4 to describe

Chaper 3 WEB MANAGEMENT

This chapter provides the entire Web Smart 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:
   Table. 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 theusername "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.**

Figure 3-2

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:

Table. 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 statesmanually. Click the each port image will open detailed statstics of selected port.

Figure 3-3.

MENU TREE There isa 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.

Table. MENU TREE

Menu	Descriptions
▶**Configuration**	
▶System	
■Information	Configures system contact, name, location and timezone offset
■IP	Configures IPv4 (Static IP Address, DHCP client), VLAN ID settings
■IPv6	Configures IPv6 (Static IP address. DHCP client)
■NTP	NTP server setting (Max: 5)
■Time	Configures Time Zone & Daylight Saving Time
■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
■EEE	Enable/disable EEE and Configures EEE urgent Queues
■Ports	Configures ports' connection settings

Table. MENU TREE (Continue)

Menu	Descriptions
▶Secuirty	
▶Switch	
■Users	Creates users account/password and privilege level
■Auth Method	Configures authentication method for console and web access via local database and RADIUS
■SSH	Enable/Disable SSH
■HTTPS	Enable/Disable HTTPS and auto-redirect setting
■Access management	Enable/Disable Access management, set IP address range for HTTP/HTTPS, SNMP and TELNET/SSH access
▶SNMP	
■System	Configures SNMP, version(v1, v2c, v3), Read/Write commnity & Trap
■Communities	Sets community for SNMPv3 & source IP address
■Users	Configures SNMPv3 User
■Groups	Configures SNMP Group
■Views	Configures View Name & Type
■Access	Configures Access Authority
▶RMON	
■Statistics	Configures RMON statistics table
■History	Configures RMON history table
■Alarm	Configures RMON Alarm table
■Event	Configures RMON Event table
▶Network	
■Limit Control	Limiting the number of users on a given port

Table. MENU TREE (Continue)

Menu	Descriptions
■NAS	Configures Network Access Server
▶ACL	
■Ports	Configures the ACL parameters of each switch port
■Rate Limiters	Configures the rate limiters for the ACL of the switch
■Access Control List	Shows the Access Control List
▶DHCP	
■Snooping	Enable/Disable DHCP Snooping
■Relay	Enable/Disable DHCP Relay & setup for Relay Server
▶IP Source Guard	
■Configuration	Enable/Disable IP Source guard & setup each port's max dynamic clients
■Static Table	Insert IP Source Guard table manually
▶ARP Inspection	
■Configuration	Enable/Disable Global ARP inspection
■Static Table	Insert ARP Inspection table manually
■AAA	Configures the Authentication Servers

Table. MENU TREE (Continue)

Menu	Descriptions
▶Aggregation	
■Static	Configures the Aggregation has mode & aggregation group
■LACP	Inspect the current LACP port configurations & possibly change them as well
■Loop Protection	Configure ports to shutdown if the ports are in loop
▶Spanning Tree	
■Bridge Settings	1. Configures global bridge setting for STP and RSTP 2. Configures edge port setting for BPDU filtering, BPDU guard and port error recovery
■MSTI Mapping	Map VLANs to a specific MSTP instance
■MSTI Priorities	Configures the priority for each MSTI
■VLAN Membership	Configures VLAN groups
■Ports	Specifies default PVID and VLAN atrributes
■CIST Ports	Configures the interface settings for STA
■MSTI Ports	Configures the interface settings for a MST instance
■MVR	Configures Multicast VLANs registration

Table. MENU TREE (Continue)

Menu	Descriptions
▶IPMC	
▶IGMP Snooping	
■Basic Configuration	Configures the global and port settings for multicast filtering
■VLAN Configuration	Configures IGMP Snooping for each VLAN interface
■Port Group Filtering	Configures ports to specific filtering group
▶MLD Snooping	
■Basic Configuration	Configures the global and port settings for multicast filtering
■VLAN Configuration	Configures IGMP Snooping for each VLAN interface
■Port Group Filtering	Configures ports to specific filtering group
▶LLDP	
■LLDP	Configures the global paramters and port's Optional TLVs
■LLDP-MED	Configures LLDP-MED attributes
■MAC Table	Configures aging time, dynamic learning & static addresses
▶VLANs	
■VLAN Memberships	Configures VLAN groups
■Ports	Configures VLAN setting for each port

Table. MENU TREE (Continue)

Menu	Descriptions
▶Private VLANs	
■PVLAN Membership	Configures PVLAN groups
■Port isolation	Configures Port isolation
▶VCL	
■MAC-based VLANs	Maps specific source MAC Address to a VLAN
▶Protocol-based VLANs	
■Protocol to Group	Create a specific protocol group
■Group to VLAN	Maps specific protocol group to a VLAN
■IP Subnet-based VLAN	Assign a subnet IP to a specific VLAN
■Configuration	Configures global settings,allowing or blocking voice vlan by port setting
■OUI	Configures the Voice VLAN and OUI mapping table
▶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
■Port Scheduler	Provides an overview of Egress priority status for each port & set Egress queue mode and sharper

Table. MENU TREE (Continue)

Menu	Descriptions
■Port Shaping	Provides an overview of Egress sharper for each port & set Egress queue mode and sharper
■Port Tag Remarking	Provides an overview of Egress Tag Remarking & set tag remarking mode
■Port DSCP	Configures the Ingress translation and classification, sets Egress DSCP rewrite value
■DSCP-Based QoS	Configures Ingress classification setting for DSCP-based QoS
■DSCP Translation	Sets translation of Ingress classification & Egress DP lv.
■DSCP Classification	Maps DSCP value to QoS class & DP level
■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
■Mirroring	Set source and destination port for mirroring
■UPnP	Enable/disable UPnP & TTL and AD settings
■sFlow	Enable sFlow and Configures flow and counter samplers for each port

Table. MENU TREE (Continue)

Publication Date: Feb, 2015
Version 1.00

Menu	Descriptions
■Mirroring	Set source and destination port for mirroring
■UPnP	Enable/disable UPnP & TTL and AD settings
■sFlow	Enable sFlow and Configures flow and counter samplers for each port
▶**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
▶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

Table. MENU TREE (Continue)

Publication Date: Feb, 2015
Version 1.00

Menu	Descriptions
▶Security	
■Access Management statistics	Overview of incoming management packets, included HTTP,HTTPS, SNMP,TELNET,SSH
▶Network	
▶Port Security	
■Switch	Shows the module legend & each port's status include MAC address learning and max allowed MAC count
■Port	Shows each port's MAC address , VLAN ID,state, Time of addition, age/hold timer
▶NAS	
■Switch	Shows each port's authentication service status and information
■Port	Shows the authentication statistics or port status and authentication method
■ACL Status	Shows the ACL status by different ACL users
▶DHCP	
■Snooping Statistics	Shows the statistics of each packet type
■Relay Statistics	Show the DHCP relay statistics

Table. MENU TREE (Continue)

Publication Date: Feb, 2015
Version 1.00

Menu	Descriptions
■ARP Inspection	Shows the dyamic ARP inspection table, sorted by port number, VLAN ID, MAC address an IP address
■IP Source Guard	Shows the IP Source Guard table, sorted by port number, VLAN ID, IP Address
▶AAA	
■RADIUS Overview	Displays the status of associated authentication RADIUS servers
■RADIUS Details	Displays the traffic and status of each associated RADIUS server
▶Switch	
▶RMON	
■Statistics	Provides an overview of RMON Statistics entries
■History	Provides an overview of RMON History entries
■Alarm	Provides an overview of RMON Alarm entries
■Event	Provides an overview of RMON Event table entries
▶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

Table. MENU TREE (Continue)

Publication Date: Feb, 2015
Version 1.00

Menu	Descriptions
■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
▶MVR	
■Statistics	Shows the IGMP/MLD statistics used by MVR
■MVR Channel Groups	Shows the MVR channel information, included VLAN ID groups & port members
■MVR SFM Information	Shows the MVR SFM(Source-Filtered Multicast) information, included SSM(Source-Specific Multicast) information
▶IPMC	
▶IGMP Snooping	
■Status	Displays statistics related to IGMP packets passed upstream to the IGMP Querier or downstream to multicast clients

Table. MENU TREE (Continue)

Publication Date: Feb, 2015
Version 1.00

Menu	Descriptions
■Groups Information	Shows IGMP snooping groups information
■IPv4 SFM Information	Shows the IGMP SFP(Source-filtered Multicast) information, included SSM(Source-Specific Multicast)
▶MLD Snooping	
■Status	Shows MLD snooping Status and Statistics
■Groups Information	Shows the MLD Group table and it sorted first by VLAN ID then by group
■IPv6 SFM Information	Shows the MLD SFM(Source-Filtered Multicast) information Table, included the SSM(Source-Specific Multicast) information
▶LLDP	
■Neighbours	Shows the LLDP information of remote device which is connected to a port of this switch
■LLDP-MED Neighbours	Shows the remote device information which is advertising LLDP-MED
■EEE	Provides an overview of EEE information exchanged by LLDP
■Port Statistics	Provides an overview of all LLDP traffic

Table. MENU TREE (Continue)

Publication Date: Feb, 2015
Version 1.00

Menu	Descriptions
■MAC Table	Shows the Dynamic & Static MAC address table
▶VLANs	
■VLAN Membership	Show the port members for specific VLAN ID
■VLAN Port	Shows the VLAN Port Status for Static user
▶VCL	
■MAC-based VLAN	Shows MAC-based VLAN entries configured by various MAC-based VLAN users
■sFlow	Shows receiver and per-port sFlow statistics
▶Diagnostics	
■Ping	Tests specific IP Address by using ping function
■Ping6	Test specific IPv6 address by using ping function

Table. MENU TREE (Continue)

Publication Date: Feb, 2015
Version 1.00

Menu	Descriptions
▶**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

Publication Date: Feb, 2015
Version 1.00

This chapter describes all of the configuration for this Web Smart Switch.

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)

Note the unit of system timezone is minute

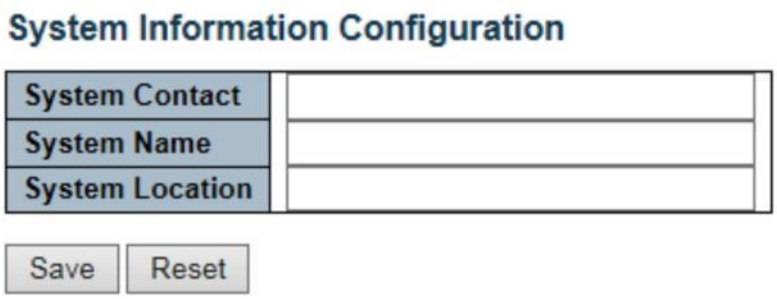
WEB Interface

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**



Figure

System/IP

Using IP page to Configure Static IP Address or DHCP client

LOCATION：

▼ Configuration

▼ System

▪IP

PARAMETERS：

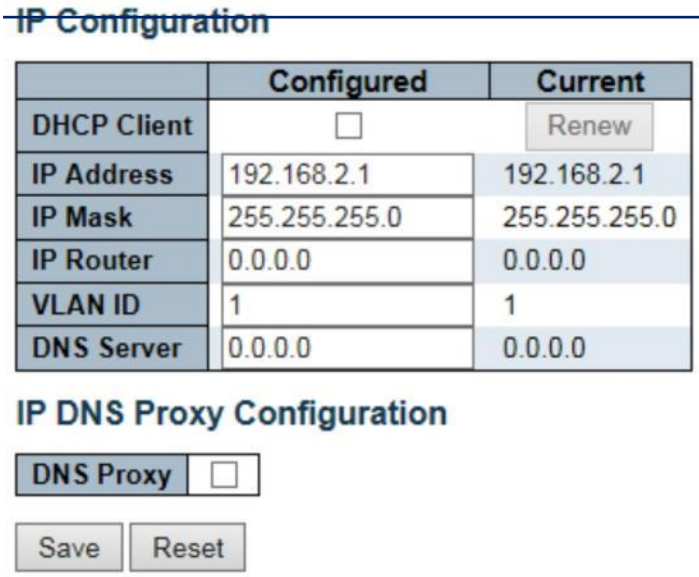
Items	Description
DHCP Client	Sets the checkbox in configured column to enable DHCP client or uncheck for static IP Address
IP Address	Address of the VLAN specified in the VLAN ID field. It should match with your management PC/NB's setting.(Default IP：192.168.2.1)
IP Mask	This mask identifies the host 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)
DNS Server	A domain name server which client requests the host name to IP address
DNS Proxy	Enable this switch to maintain a DNS database
Renew	Renew a DHCP lease

WEB Interface

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

A. **Click *Configuration/System/IP***
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**
F. **Check the DNS Proxy to maintain a local DNS database**



IP Configuration

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

IP DNS Proxy Configuration

DNS Proxy	☐

Save Reset

Figure

System/IPv6

Using IPv6 page to Configure Static IPv6 Address or DHCP client

LOCATION：

▼ Configuration

▼ System

▪IPv6

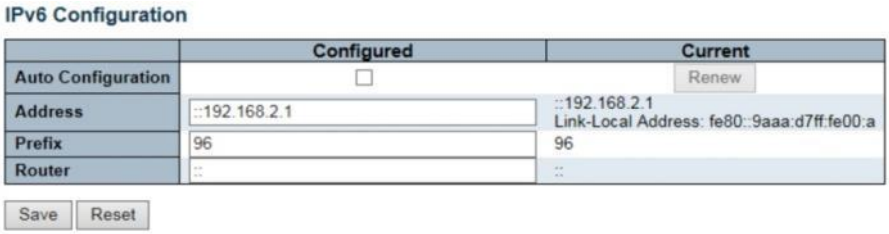
PARAMETERS：

Items	Description
Auto Configuration	Sets the checkbox in configured column to enable DHCP client or uncheck for static IP Address
Address	The IPv6 Address must follow the RFC2373 “IP Version 6 Addressing Architecture” format.IPv6 address is in 128-bit records represented as eight fileds of up to four hexadecimal digits with a colon separating each field(:)
Prefix	Provides the IPv6 Prefix of this switch. The allowed range is 1to 128
Router	Provides The IPv6 gateway of this switch

WEB Interface

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

A. **Click *Configuration/System/IP***
B. **Enable DHCP client vis set checkbox**
C. **Specify the IP address and Prefix. Router is optional.**
D. **Click Renew button to renew IPv6 Address under Auto Configuration Enable mode**
E. **Click Save to apply the setting or Reset to restore the previous setting**



Figure

System/NTP

Using NTP Configuration page to set 5(MAX) NTP Servers

LOCATION：

▼ Configuration

▼ System

▪NTP

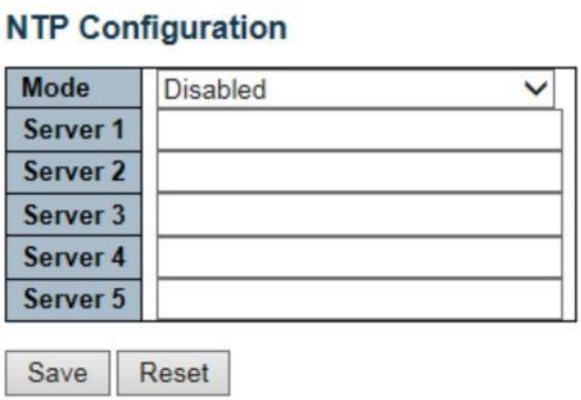
PARAMETERS：

Items	Description
Mode	Enable or Disable NTP Client mode
Server 1~5	Set IPv4 or IPv6 of a NTP Server, Maximum NTP server is 5

WEB Interface

A. Click *Configuration/System/NTP*

B. Enable NTP Mode, enter NTP Server's IP Address in Server 1~5



Figure

System/Time

Using This page to configure Time Zone & Daylight saving Time.

LOCATION：

▼ Configuration

▼ System

▪Time

PARAMETERS：

Items	Description
Time Zone	Lists various Time Zones word wide. Select appropriate Time Zone from the drop down and click Save to set.
Acronym	Sets the acronym of the time zone,UP to 16 alpha-numeric characters and can contain '-','_' or '.'
Daylight Saving Time	Select 'recurring' and configure the Daylight Saving Time duration to repeat every year Select 'Non-Recurring' and configure the Daylight Saving Time duration for single time configuration
Month	Selects the month
Date	Selects the date
Year	Selects the year
Hours	Selects the hour
Minutes	Selects the minute
Offset	Enters the number of minutes to add during Daylight Saving Time (Range: 1 to 1440)

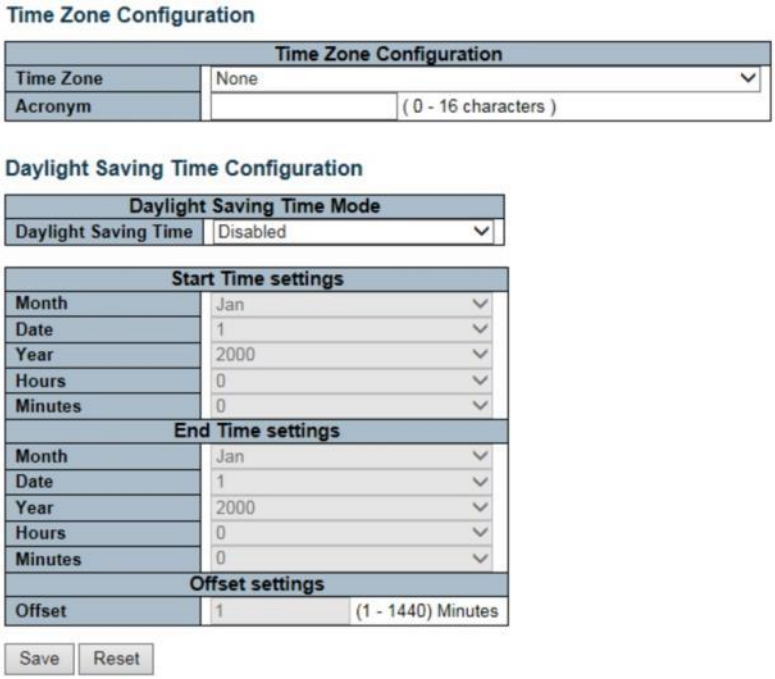
PS. there are Start Time & End time setting

WEB Interface

A. Click *Configuration/System/Time*

B. Select The Time Zone front the drop down list.

C. Enable Daylight Saving Time & set “Start Time & End time” setting for duration, and set Offset time.



Figure

System/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

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

Figure

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

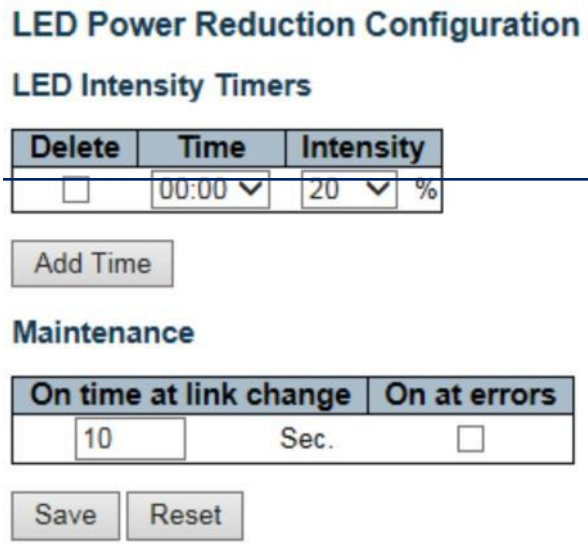
▪LED

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 On at errors	LED set full powr for a period of time(second) when a link change occurs. 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
G. Set the duration of LED full power when a link error occurs
H. Click Save to apply the setting or Reset to restore the previous setting



Figure

Power Reduction/EEE

EEE is a power saving option that reduces that power usage when there is low or no traffic utilization. Using this page to set EEE and urgent Queues.

LOCATION：

▼ Configuration

▼ Power Reduction

▪EEE

PARAMETERS：

Items	Description
Enable EEE Urgent Queue	Enable/Disable EEE for each ports Queues set will activate transmission of frames as soon as any data is available, Otherwise the queue will postpone the transmission until 3000 bytes are read to be transmitted.

PS. Ports that are not EEE-capable are grayed out and thus impossible to enable EEE for.

WEB Interface

A. Click *Configuration/Power Reduction/EEE*

B. Select the ports to enable EEE

C. Select the urgent Queue if necessary

EEE Configuration

		EEE Urgent Queues							
Port	Enabled	1	2	3	4	5	6	7	8
*	☐	☐	☐	☐	☐	☐	☐	☐	☐
1	☐	☐	☐	☐	☐	☐	☐	☐	☐
2	☐	☐	☐	☐	☐	☐	☐	☐	☐
3	☐	☐	☐	☐	☐	☐	☐	☐	☐
4	☐	☐	☐	☐	☐	☐	☐	☐	☐
5	☐	☐	☐	☐	☐	☐	☐	☐	☐
6	☐	☐	☐	☐	☐	☐	☐	☐	☐
7	☐	☐	☐	☐	☐	☐	☐	☐	☐
8	☐	☐	☐	☐	☐	☐	☐	☐	☐
9	☐	☐	☐	☐	☐	☐	☐	☐	☐
10	☐	☐	☐	☐	☐	☐	☐	☐	☐

Save Reset

Figure

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-duplexfor

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 Collision Mode	Configure port transmit collision behavior 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	X	X	☑	9600	Discard	Disabled
3	Down		Auto	X	X	☑	9600	Discard	Disabled
4	Down		Auto	X	X	☑	9600	Discard	Disabled
5	Down		Auto	X	X	☑	9600	Discard	Disabled
6	Down		Auto	X	X	☑	9600	Discard	Disabled
7	Down		Auto	X	X	☑	9600	Discard	Disabled
8	Down		Auto	X	X	☑	9600	Discard	Disabled
9	Down		Auto	X	X	☑	9600		
10	Down		Auto	X	X	☑	9600		

Save Reset

Figure

Security/Switch/Users

You can configure username/password authority for different privilege level(1-15).

LOCATION：

▼ Configuration

▼ Security

▼ Switch

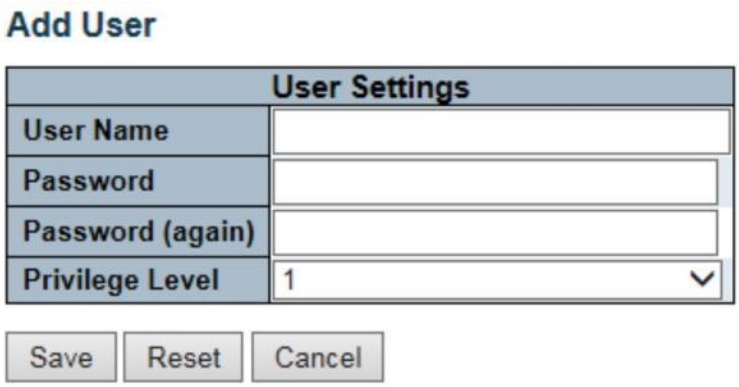
- Users

PARAMETERS：

Items	Description
User Name	Username(length:1~31, letters, numbers & underscores are allowed)
Password	The password of the user(Lengh: 1~31)
Privilege Level	Range: 1~15,

WEB Interface

A. **Click *Configuration/Security/Switch/Users***
B. **Enter Username, passwod and select the Privilege level.**
C. **Click Save to apply the setting.**



Figure

Security/Switch/Privilege

Using the Privilege Levels page to set the privilege level required to read or configure specific software module or system setting

LOCATION：

▼ Configuration

▼ Security

▼ Switch

- Privilege Levels

PARAMETERS：

Items	Description
Group Name	The name identifying the privilege group, included System, Security,IP,Port,Diagnostics,Maintenance, and debug PS. Debug present in CLI only
Privilege Level	Range: 1~15,

Privilege Level Configuration

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

Save Reset

Figure

Security/Switch/Auth Method

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

LOCATION：

▼ Configuration

▼ Security

▼ Switch

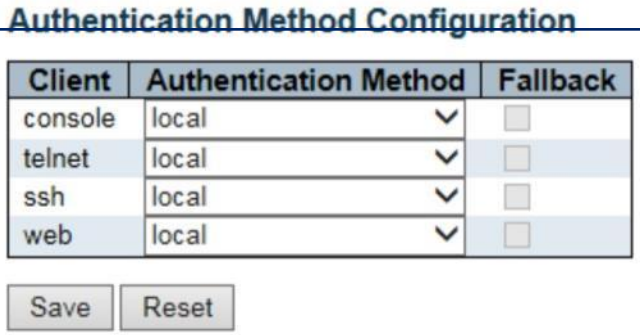
- Auth Method

PARAMETERS：

Items	Description
Client	Specify the authentication Method for Administrator
Authentication Method	There are 4 options for Console and Web None：disablesaccess vis specified management interface Local：checks by password RADIUS：authenticated via RADIUS Server TACACS+: authenticated by TACACS+ server
Fallback	This only works for Authentication Method ="RADIUS" and "TACACS+". 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, telnet, ssh and web, specify the Fallback check if needed.**
C. **Click Save to apply the settingor Reset to restore the previous setting.**



Figure

Security/Switch/SSH

Using SSH configuation page to setup Secure shell management interface.

LOCATION：

▼ Configuration

▼ Security

▼ Switch

▪ SSH

PARAMETERS：

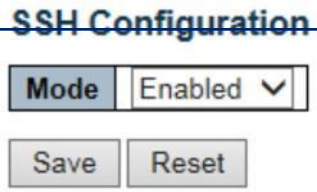
Items	Description
Mode	You can enable SSH by setting Mode enable. SSH service on this switch supports password authentication only. It can be authenticated by RADIUS, TACACS+ or locally

WEB Interface

A. Click *Configuration/Security/Switch/SSH*

B. Set Mode Enable or Disabled

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



Figure

Security/Switch/HTTPS

Using HTTPS Configuration page to enable Secure Hypertext Transfer Protocol(HTTPS) over the Secure Socket Layer (SSL)

LOCATION：

▼ Configuration

▼ Security

▼ Switch

▪ HTTPS

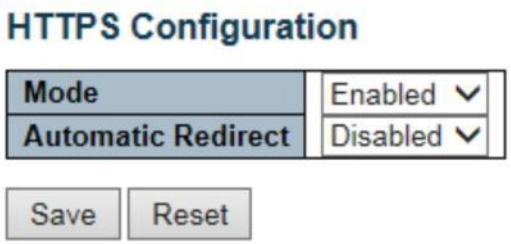
PARAMETERS：

Items	Description
Mode	You can enable HTTPS by set Enabled to Mode field or disable HTTPS by set disable
Automatic Redirect	It only significant if HTTPS mode “Enabled” is selected. Automatically redirects web brower to an HTTPS connection when both HTTPS mode

	and Automatic Redirect are enabled.

WEB Interface

A. **Click *Configuration/Security/Switch/HTTPS***
B. **Select Mode Enabled or Disabled**
C. **Select Automatic Redirect Enabled or Disabled if Mode=Enabled**
D. **Click Save to apply the setting or Reset to restore the previous setting**



Figure

Security/Switch/Access Management

Using access management page to create a list of up to16 IP address or IP address groups that allow management access throuh the HTTP/HTTPS/SNMP/TELNET/SSH.

LOCATION：

▼ Configuration

▼ Security

▼ Switch

▪ Access Management

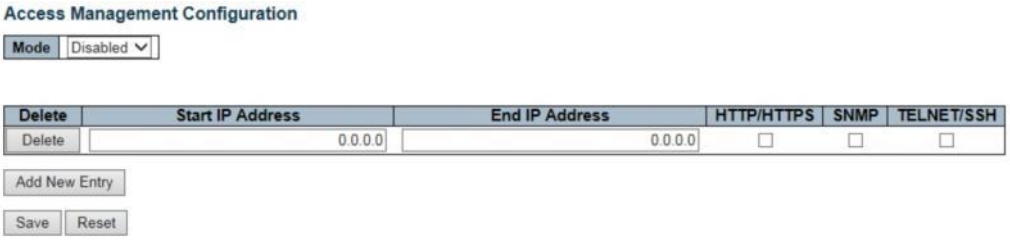
PARAMETERS：

Items	Description
Mode	Select Enabled/Disabled to set Access Management or not
Add New Entry	Click this button to create a IP Address

	range to access “HTTP/HTTPS, SNMP,TELNET/SSH”

WEB Interface

A. **Click *Configuration/Security/Switch/Access Management***
B. **Select Mode Enabled or Disabled**
C. **If Mode= Enabled, click “Add New Entry” to setup a list of access rule for HTTP/HTTPS, SNMP,TELNET/SSH**
D. **Click Save to apply the setting or Reset to restore the previous setting**



Figure

Security/Switch/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

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.**

SNMP System Configuration

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

SNMP Trap Configuration

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

Save Reset

Figure

Security/Switch/SNMP/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

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.**

SNMPv3 Community Configuration

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

Add New Entry | Save | Reset

Figure

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	The methods for authentication

Protocol	(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

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 Entry | Save | Reset

Figure

Security/Switch/SNMP/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

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.**

SNMPv3 Group Configuration

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

Add New Entry　Save　Reset

Figure

Security/Switch/SNMP/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

A. **Click*Configuration/Security/Switch/SNMP/Views***
B. **Click "Add New Entry" 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.**

SNMPv3 View Configuration

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

Add New Entry | Save | Reset

Figure

Security/Switch/SNMP/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

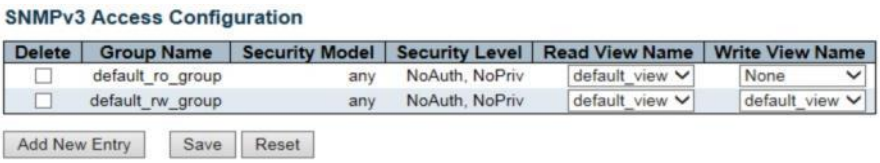
PARAMETERS：

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

A. **Click*Configuration/Security/Switch/SNMP/Access***
B. **Click "Add New Entry" to create a new Access**
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.**



Figure

Security/Switch/RMON/Statistics

Using RMON statistics Configuration page to set MIBs ID to store real-time LAN statistics, e.g utilization, collisions, CRC errors

LOCATION：

▼ Configuration

▼ Security

▼ RMON

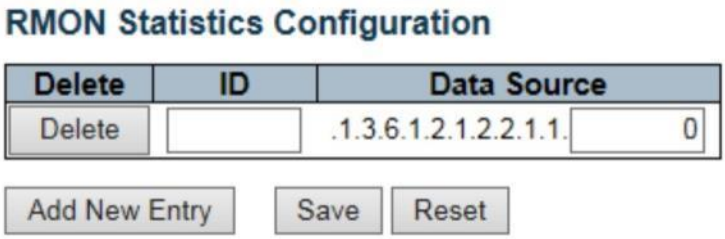
- Statistics

PARAMETERS：

Items	Description
Delete	Delete the Entry of MIBs
ID	Indicates the index of the entry. The range is from 1 to 65535
Data Source	Indicates the port ID which wants to be monitored. (The number = port number)

WEB Interface

A. **Click*Configuration/Security/Switch/RMON/Statistics***
B. **Click "Add New Entry" to create a new MIBs**
C. **.Set ID & Data Source number**
D. **Click Save to apply the setting or Reset to restore the previous setting.**



Figure

Security/Switch/RMON/History

Using RMON History Configuration page to select history of selected LAN statistics,utilization, collisions, CRC errors

LOCATION：

▼ Configuration

▼ Security

▼ RMON

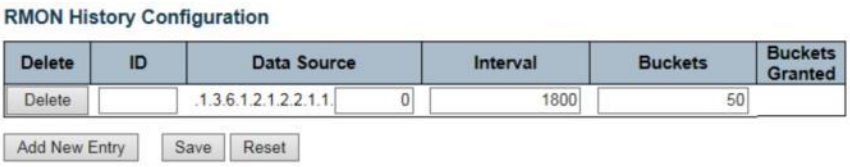
▪ History

PARAMETERS：

Items	Description
Delete	Delete the Entry of History configuration
ID	Indicates the index of the entry. The range is from 1 to 65535
Data Source	Indicates the port ID which wants to be monitored. (The number = port number)
Interval Buckets Buckets Granted	Indicates the interval in seconds for sampling the history statistics data. The range is from 1 to 3600, default value is 1800 seconds
Buckets Granted	The number of data shall be saved in the RMON

WEB Interface

A. **Click*Configuration/Security/Switch/RMON/History***
B. **Click "Add New Entry" to create a new rule**
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.**



Figure

Security/Switch/RMON/Alarm

Using RMON Alarm Configuration page to set the threshold for sending SNMP trap

LOCATION：

▼ Configuration

▼ Security

▼ RMON

▪ Alarm

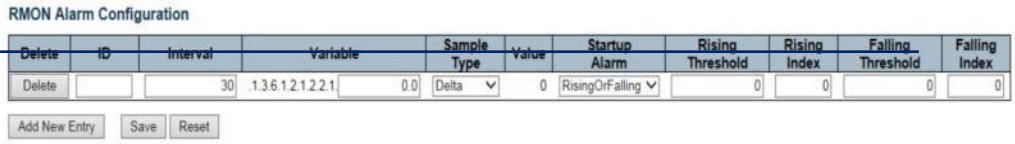
PARAMETERS：

Items	Description
Delete	Delete the Entry of Alarm configuration
ID	Indicates the index of the entry. The range is from 1 to 65535
Interval	Indicates the interval in seconds for sampling and comparing the rising and falling threadhold. The range is 1 to 2^31-1
Variable	Indicates the particular variable to be sampled, the possible variables:
[InOctets]	The total number of octets received on the interface, including framing characters
[InUcastPkts]	The number of uni-cast packets deliverd to a higher-layer protocol
[InNUcastPkts]	The number of broad-cast and multi-cast packets delivered to a higher-layer protocol
[InDiscards]	The number of inbound packets that are discarded even the packets are normal
[InErrors]	The number of inbound packets that contained errors preventing them from

[InUnknownProtos]	being deliverable to a hugher-layer protocol
[OutOctets]	The number of the inbound packets that were discarded because of the unknown or un-support protocol
[OutUcastPkts]	The number of octets transmitted out of the interface, including framing characters
[OutNUcastPkts]	The number of uni-cast packets that request to transmit
[OutDiscards]	The number of broad-cast and multi0cast packets that request to transmit
[OutErrors]	The number of outbound packets that are discarded even the packets is normal
[OutQlen]	The number of outbound pakets that could not be transmitted because of errors
Sample Type	The length of the output packet queue(in packets)
	The method of sampling the selected variable and calculating the value to be compared against the threshold, possible sample types are:
[Absolute]	Get The sample directly
[Delta]	Calculate the difference between samples(default)
Value	The value of the statistic during the last sampling period
Startup Alarm	The method of sampling the selected variable and calculating the value to be compared against the thresholds, possible sample types are:
Rising	Trigger alarm when the first value is larger than the rising threshold
Falling	Trigger alarm when the first value is less than the falling threshold
RisingOrFalling	Trigger alarm when the first value is larger than the rising threshold or less than the falling threshold(default)

WEB Interface

A. Click*Configuration/Security/Switch/RMON/Alarm*
B. Click "Add New Entry" to create a new rule
C. Set ID, sampling interval, MIBs variable, Sample type, Startup Alarm timing, Rising threshold, Rising Index, Falling Threshold, Falling Index.
D. Click Save to apply the setting or Reset to restore the previous setting.



Figure

Security/Switch/RMON/Event

Using RMON Event Configuration page to setup a trigger when the condition is happened in the Alarm group.

LOCATION：

▼ Configuration

▼ Security

▼ RMON

▪ Event

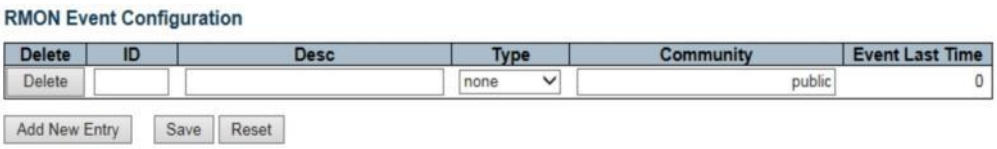
PARAMETERS：

Items	Description
Delete	Delete the Entry of Event configuration
ID	Indicates the index of the entry. The range

	is from 1 to 65535
Desc	Indicates this event, the string length is from 0 to 127, default is null string
Type	Indicates the notification of the event, the possible types are:
[none]	The total number of octets received on the interface, including framing characters
[log]	The number of uni-cast packets delivered to a higher-layer protocol
[snmptrap]	The number of broad-cast and multi-cast packets delivered to a higher-layer protocol
[logandtrap]	The number of inbound packets that are discarded even the pakets are normal.
Community	Specify the community when trap is sent, the string length is from 0 to 127, default is “public”
Event Last Time	Indicates the value of sysUpTime at the time this event entry last generated an event

WEB Interface

A. **Click*Configuration/Security/Switch/RMON/Event***
B. **Click “Add New Entry” to create a new rule**
C. **Set ID, sampling interval, MIBs variable, Sample type, Startup Alarm timing, Rising threshold, Rising Index, Falling Threshold, Falling Index.**
D. **Click Save to apply the setting or Reset to restore the previous setting.**



Figure

Security/Network/Limit Control

Use the port Security Limit Control configuration page to limit the number of users accessing the specific port. A user is identified by a MAC address and VLAN ID. If Limit Control is enabled on a port, the limit specifies the maximum number of users on the port. If this number is exceeded, an action is taken. The action can be one of the four different actions as described below.

LOCATION：

▼ Configuration

▼ Security

▼ Network

▪ Limit Control

PARAMETERS：

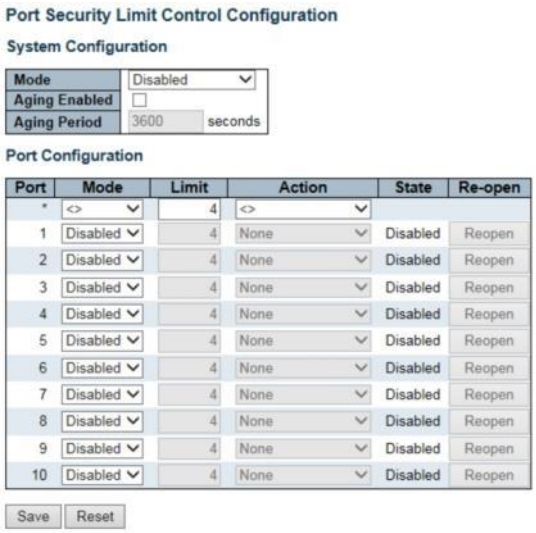
Items	Description
System Configuration	
Mode	Enabled/Disabled Limit Control
Aging Enabled	If checked, secured MAC addresses are subject to aging as discussed under aging period
Aging Period	If “Aging Enabled” is checked, the aging period is controlled with this input.This value is from 10 to 10,000,000 seconds
Port Configuration	
Port	The port number to which the configuration below applies
Mode	Controls whether Limit Control is enabled on this port. Both this and the Global Mode must be set to Enabled for Limit Control to be in effect. Notice that other modules may still use the underlying port security

	features without enabling Limit Control on a given port.
Limit	The maxmium number of MAC addresses that can be secured on this port. This number cannot exceed 1024. If the limit is exceeded, the corresponding action is taken.The switch is “born” with a total number of MAC addresses from which all ports draw whenever a new MAC address is seen on a Port Security-enabled port. Since all ports draw from the same pool, it may happen that a configured maximum cannot be granted, if the remaining ports have already used all available MAC addresses.
Action	If Limit is reached, the switch can take one of the following actions:
[none]	Do not allow more thatn Limit MAC addresses on the port. But take no further action.
[Trap]	If Limit +1 MAC addresses is seen on the port, send an SNMP trap. If Aging is disabled, only one SNMP trap will be sent, but with Aging enabled, new SNMP traps will be sent evert time the limit get exceeded.
[Shutdown]	If Limit+1 MAC addresses is seen on the port, shut down the port. This implies that all secured MAC addresses will be removed from the port, and no new address will be learned. Even if the link is physically disconnected and reconnected on the port(by disconnecting the cable), the port will remain shut down. There are three ways to re-open the port: 1) Boot the switch, 2) Disable and re-enable Limit Control on

	the port or the switch 3) Click the reopen button.
[Trap&Shutdown]	If Limit+ 1 MAC address is seen on the port, both the “Trap” and the “Shutdown” actions described above will be taken
State	This column shows the current state of the port as seen from the Limit Control’s point of view. The state takes on of four values:
[Disabled]	Limit Control is either globally disabled or disabled on the port
[Ready]	The limit is not yet reached, This can be shown for all actions.
[Limit Reached]	Indicates that the limit is reached on this port. This state can only be shown if Action is set to None or Trap.
[Shutdown]	Indicates that the port is shut down by the Limit Control module. This state can only be shown if Action is set to Shutdown or Trap & Shutdown
Re-open Button	If a port is shutdown by this module, you may reopen it by clicking this button, which will only be enabled if this is the case. For other methods, refer to Shutdown in the Action section. Note. Clicking the reopen button causes the page to be refreshed, so non-committed changes will be lost.

WEB Interface

A. **Click*Configuration/Security/Network/Limit Control***
B. **Select Enabled Limit Control & set aging period**
C. **Set each port’s configuration, included Mode, Limit number, Action,**
D. **If state is Shutdown, user can click reopen to enable the given port.**
E. **Click Save to apply the setting or Reset to restore the previous setting.**



Figure

Security/Network/NAS

Using Network Access Server Configuration page to setup the IEEE 802.1X and MAC-based authentication system and port setting.

The IEEE 802.1X standard defines a port-based access control procedure that prevents unauthorized access to a network by requiring users to first submit credentials for authentication, One or more central servers, the backend servers, determine whether the user is allowed access to the network. These backedn(RADIUS) servers are configured on the "Configuration→Security→AAA" page.

The IEEE 802.1X standard defines port-based operation, but non-standard variants overcome security limitations as shall be explored below.

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

PARAMETERS：

Items	Description
System Configuration	
Mode	Indicates if NAS is globally enabled or disabled on the switch, if globally disabled, all ports are allowed forwarding of frames
Reauthentication Enabled	If checked, successfully authenticated supplicants/clients are reauthenticated after the interval specified by the REauthentication Period. Reauthentication for 802.1X-enabled ports can be used to detect if a new device is plugged into a switch port or if a supplicant is no longer attached For MAC-based ports. Reauthentication is only useful if the RADIUS server configuration has changed. It does not involve communication between the switch and the client, and therefore doesn't imply that a client is still present on a port.
Reauthentication Period	Determines the period, in seconds, after which is connected client must be reauthenticated. This is only active if the Reauthentication Enabled checkbox is checked. Valid values are in the range 1 to 3600 seconds
EAPOL Timeout	Determines the time for retransmission of Request Identity EAPOL frames.Valid values are in the range 1 to 65535 seconds. This has no effect for MAC-based ports.
Aging Period	The setting applies to the following mode: 1) Single 802.1X 2) Multi 802.1X 3) MAC-Based Auth. When the NAS mododule users the Port Security modules to secure MAC

Hold Time	addresses, the Port Security modules needs to check for activity on the MAC address in question at regular intervals and free resources if no activity is seen within a given period of time. This parameter controls exactly this period and can be set to a number between 10 and 1000000 seconds. If reauthentication is enabled and the port is in an 802.1X-based mode, this is not so critical, since suplicants that are not longer attached to the port will removed upon the next reauthentication, which will ail. But if reauthentication is not enabled, the only way to free resource is by aging the entries. For ports in MAC-based Auth. Mode , reauthentication doesn't cause direct communication between the switch and the client, so this will not detect whether the client is still attached or not, and the only way to free any resources is to age the entry. This setting applies to the following modes, i.e. modes using the Port Security functionality to secure MAC addresses: 1) Single 802.1X 2) Multi 802.1X 3) MAC-Based Auth. If a client is denied access- either because the RADIUS server denies the client access or because the RADIUS server request times out(according to the timeout speficied on the "Configuration→Security→AAA" page)- the client is put on hold in the Unauthorized state. The hold timer

	doesn't count during an on-going authentication. In MAC-based Auth. Mode, the switch will ignore new frames coming from the client during the hold time. The Hold Time can be set to a number between 10 and 1000000 seconds
RADIUS-Assigned QoS Enable	RADIUS-assigned QoS provides a means to centrally control the traffic class to which traffic coming from a successfully authenticated supplicant is assigned on the switch. The RADIUS server must be configured to transmit special RADIUS attributes to take adventage of this feature. The "RADIUS-Assigned QoS Enabled" checkbox provides a qucik way to globally enabled/disabled RADIUS-server assigned QoS class functionality. When checked, the individual ports' ditto setting determine whether RADIUS-assigned QoS is enabled on that port. When unchecked, RADIUS-server assigned QoS Class is disabled on all ports.
RADIUS-Assigned VLAN Enabled	RADIUS-assigned VLAN provides a means to centrally control the VLAN on which a successfully authenticated supplicant is placed on the switch. Incoming traffic will be classified to and switched on the RADIUS-assigned VLAN. The RADIUS server must be configured to transmit speical RADIUS attributes to take advantage of this feature. The "RADIUS-Assigned VLAN Enabled" checkbox provides a quick way to globally enabled/disabled RADIUS-server assigned VLAN functionality. When

Guest VLAN Enabled	checked, the individual ports' ditto setting determine whether RADIUS-assigned VLAN is enabled on that port. When unchecked, RADIUS-server assigned VLAN is disabled on all ports.
Guest VLAN ID	A Guest VLAN is a special VLAN – typeically with limited network access – on which 802.1X-unaware clients are placed after a network adaministrator-defined timeout. The switch follows a set of rules for entering and leaving the Guest VLAN as listed below. The "Guest VLAN Enabled" checkbox provides a quick way to globally enabled/disabled Guest VLAN functionality. When checked, the individual ports' ditto setting determine whether the port can be moved into Guest VLAN. When unchecked, the ability to move to the Guest VLAN is disabled on all ports.
Allow Guest VLAN if EAPOL Seen	This is the value that a port's Port VLAN ID is set to if a port is moved into the Guest VLAN It is only changeable if the Guest VLAN option is globally enabled. Valid values are in the ramge[1-255] The switch remebers if an EAPOL frame has been received on the port for the life-time of the port. Once the switch considers whether to enter the Guest VLAN, it will first check if this option is enabled or disabled. If disabled (unchecked;default), the switch will only enter the Guest VLAN if an EAPOL frame has ot been received on the port for the life-time of the port. If enabled(checked), the switch will consider entering the Guest VLAN even if an EAPOL frame has been

	received on the port for the life-time of the port. The value can only be changed if the Guest VLAN option is globally enabled.
Port Configuration	
Port	The port number to which the configuration below applies
Admin State	If NAS is globally enabled, this selection controls the port's authentication mode. The following modes are available:
[Force Authorized]	In this mode, the switch will send one EAPOL Success frame when the port link comes up, and any client on the port will be allowed network access without authentication
[Force Unauthorized]	In this mode, the switch will send one EAPOL failure frame when the port link comes up, and any client on the port will be disallowed network access
[Port-Based 802.1X]	In the 802.1X-word, the user is called the supplicant, the switch is the authenticator, and the RADIUS server is the authentication server. The authenticator acts as the man-in-the-middle, forwarding requets and responses between the supplicant and the autentication server.
[Single 802.1x]	At most one supplicant can get authenticated on the port at a time. IF more than one supplicant is connected to a port, the one that comes first when the port's link comes up will be the first one considered. If first one fails the authentication, the second one gets a chenace.
[Multi 802.1X]	One or more supplicants can get authenticated on the same port at the same time. Each supplicant is

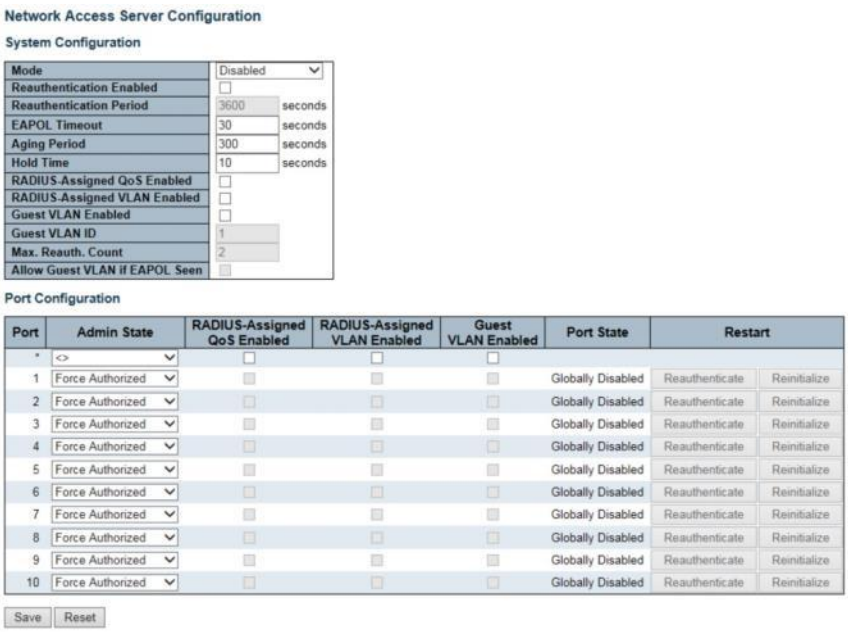
	authenticated individually and secured in the MAC table using the port Security module. In Multi 802.1X it is not possible to use the multicast BPDU MAC address as destination MAC address for EAPOL frames sent from the switch toward the suplicant, since that would cause all supplicants attached to the port to reply the requests sent from the switch.
[MAC-based Auth]	Unlike port-based 802.1X, MAC-based authentication is not a standard. But merely a best-practices method adopted by the industry. In MAC-Based authentication, users are called clients, and the switch acts as the supplicant on behalf of clients, The initial frame(any kind of frame) sent b a client is snooped by the switch, which in turn uses the client's MAC address as both username and password in the subsquent EAP exchanged with the RADIUS server. The 6-byte MAC address is converted to a string on the following form "xx-xx-xx-xx-xx-xx", that is , as dash(-) is use as separator between the lower-cased hexadecimal digits. The switch only supports the MD5-Challenge authenciation method, so the RADIUS server must be configured accordingly. When authentication is complete, the RADIUS server sends a success or failure indication, which in turn causes the switch to open ip or block traffic for that particular client, using the Port Security module Only then will frames from the client be forwarded on the switch. There are no EAPOL frames involved in this

	authentication and therefore.
[RADIUS-Assigned QoS Enabled]	Enabled/disabled this feature for a given port.
[RADIUS-Assigned VLAN Enabled]	Enabled/disabled this feature for a given port.
[Guest VLAN Enabled]	Enabled/disabled this feature for a given port.
Port State	The current state of the port:
[Globally Disabled]	802.1X and MAC-based authentication are globally disabled
[Link Down]	802.1X and MAC-based authentication is enabled, but no link on the given port.
[Authorized]	The port is in Force Authorized mode,or a single-supplicant mode and the supplicant is authorized
[Unauthorized]	The port is in Force Unauthorized mode, or a single-supplicant mode and the supplicant is not successfully authorized by the RADIUS Server
[X Auth/Y Unauth]	The port is in a multi-supplicant mode, X clients are currently authorized and Y are unauthorized
Restart	Restart client authentication using the following methods:
[Reauthenticate]	Schedules reauthentication to whenever the quiet-period of the port runs out(EAPOL-based authentication). For MAC-based authentication, reauthentication will be attempted immediately. The button only has effect for successfully authenticated clients on the port and will not cause the clients to get temporarily unauthorized.
[Reinitialize]	Forces a reinitialization of the clients on the port and thereby a reauthentication immediately, The clients will transfer to the

	unauthorized state while the reauthentication is in progess

WEB Interface

A. **Click*Configuration/Security/Network/NAS***
B. **Configure the System Configuration**
C. **Configure the Port Configuration**
D. **Click Save to apply the setting or Reset to restore the previous setting.**



Figure

Security/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	The logical port for the settings contained in the same row
Policy ID	Specify the Policy ID to apply th this port (Range：0-255)
Action	Permit or deny the forwarding if policy is Matched(Default is “Permit”
Rate limiter ID	Specify a Rate Limiter ID, the mapping table is in “Rate Limiters” page.(Range:1-16, default is “Disabled”)
Port Redirect	Select which port frames are redirected on. The allowed values are “Disabled” or specific port number and it can’t be set when action is permitted. The default value is “Disabled”
Mirror	Specify the logging operation of this port. The allowed values are:
[Enabled]	Frames received on the port are mirrored.
[Disabled]	Frames received on the port are not mirrored.
	The default value is “Disabled”

Logging	Specify the logging operation of this port. The allowed values are;
[Enabled]	Frames received on the port are store in the System log.
[Disabled]	Frames received on the port are not logged
Shutdown	Specify the logging operation of this port. The allowed values are:
[Enabled]	If a frame is received on the port. The port will be disabled.
[Disabled]	Port shut down is disabled The default value is “Disabled”
State	Specify the port state of this port. The allowed values are:
[Enable]	To reopen ports by changing the volatile port configuration of the ACL user module.
[Disabled]	To close ports by changing the volatile port configuration of the ACL user module. The fedault value is “Enabled”
Counter	Counts the number of frames that match this ACE

WEB Interface

A. **Click*Configuration/Security/Network/ACL/Ports***
B. **Assign A Policy ID to a given port and set related ACE parameters, included “Action”, “Rate Limiter ID”,“Port Redirect”, “Mirror”, “Logging”, “Shutdown”, “State”.**
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**

Figure

Security/Network/ACL/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	The rate limiter ID for the settings contained in the same row(Range：1-16)
Rate	The dropping threshold, the allowed

	value：
	0-3276700 in pps,or 0, 100, 2*100, 3*100…100000 in kbps
Unit	Specify the rate unit. The allowed values:
[pps]	Packets per second
[kbps]	Kbits per second

WEB Interface

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

Save Reset

Figure

Security/Network/ACL/Access Control List

Using Access Control List page to make up of ACE s define 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	Indicates the ingress port of the ACE.
	Possible values are:
[All]	The ACE will match all ingress port.
[Port]	The ACE will match a specific ingress port.
Policy/Bitmask	Indicate the Policy and Bitmask of the ACE
Frame Type	Indicate the frame type of ACE.Possible value 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 frame.

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	Specifiy the mirror operation of this port, Frames matching the ACE are mirrored to the destination mirror port. The allowed values are:
[Enabled]	Frames received on the port are mirrored
[Disabled]	Frames received on the port are not mirrored The default value is “Disabled”
Counter	The counter indicates the number of times the ACE was hit by a frame
Modification Buttons	You can modify each ACE(Access Control Entry) in the table using the following buttons:
[⊕]	Inserts a new ACE before the current row
[ⓔ]	Edits the ACE row
[⊙]	Moves the ACE up the list

[⊕]	Moves the ACE down the list
[⊗]	Deletes the ACE
[⊕]	The lowest plus sign adds a new entry at the botton of the ACE listings.

WEB Interface

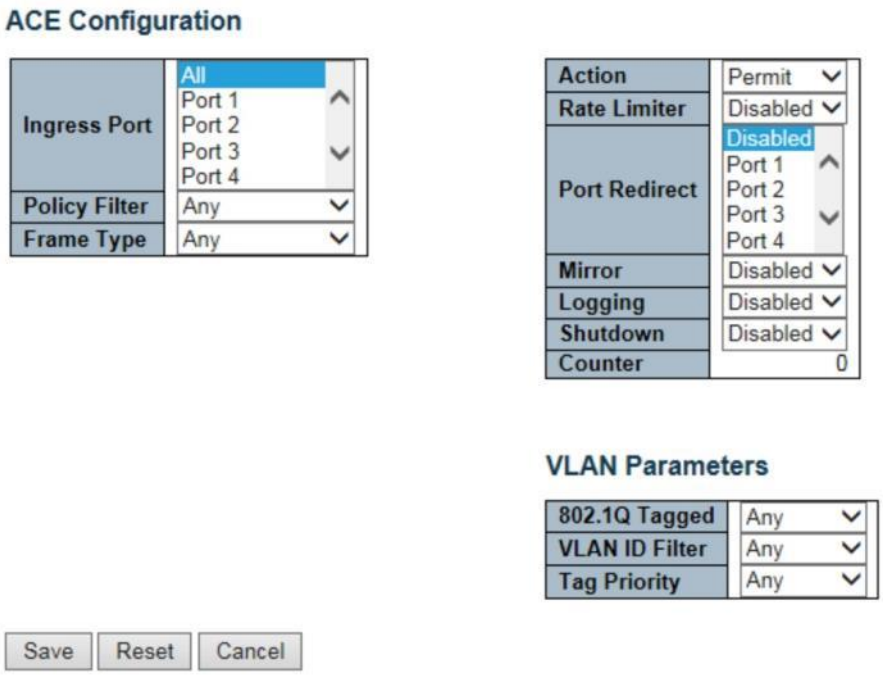
A. Click *Configuration/Security/Network/ACL/Access Control List*

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**



Figure

Figure

Security/Network/DHCP/Snooping

Use the DCHP Snooping Configuration page to filter IP traffic on insecure ports for which the source address cannot be identified via DCHP snooping.

LOCATION：

▼ Configuration

▼ Security

▼ Network

▼ DHCP

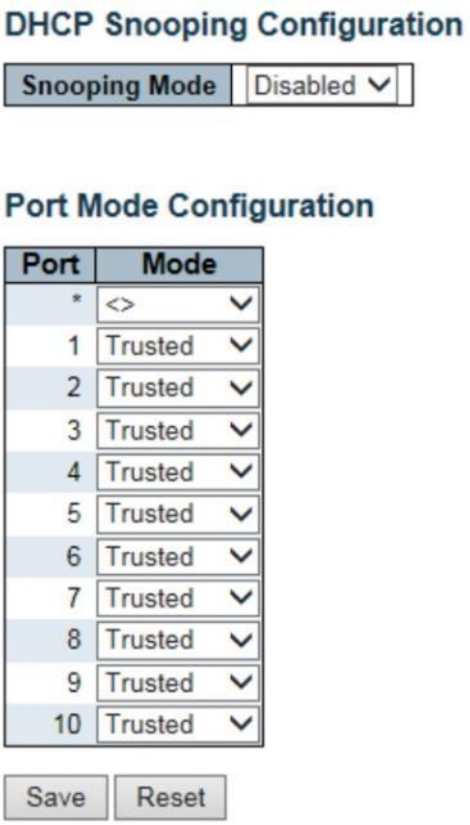
▪ Snooping

PARAMETERS：

Items	Description
Snooping Mode	
Snooping mode [Enabled] [Disabled]	Indicates the DHCP snooping mode operation Possible modes are: Enable DHCP snooping mode operation. When DHCP snooping mode operation is enabled, the DHCP request messages will be forwarded to trusted ports and only allow rely packets from trusted ports. Disable DHCP snooping mode operation
Port Mode Configuration	
Port Mode Configuration [Trusted] [Untrusted]	Indicates the DHCP snooping port mode. Possible port modes are: Configures the port as trusted source of the DHCP messages. Configures the port as untrusted source of the DHCP messages

WEB Interface

A. **Click *Configuration/Security/Network/DHCP/Snooping***
B. **Select Enabled/Disabled Snooping Mode & set Trusted/Untrusted for each port.**
C. **Click Save to apply the setting or Reset to restore the previous setting.**



Figure

Security/Network/DHCP/Relay

Use the DCHP Relay Configuration page to configure DHCP relay service for attached host devices. If a subnet doesn't include a DHCP server, you can relay DHCP client request to a DHCP serveron another subnet.

LOCATION：

▼ Configuration

▼ Security

▼ Network

▼ DHCP

▪ Relay

PARAMETERS：

Items	Description
Relay Mode	Indicates the DHCP relay mode operation. Possible modes are:
[Enable]	Enable DHCP relay mode operation. When DHCP relay mode operation is enabled, the agent forwards and transfers DHCP messages between the clients and the server when they are not in the same subnet domain. And the DHCP broadcast message won't be flooded for security considerations.
[Disabled]	Disable DHCP relay mode operation.
Relay Server	Indicates the DHCP relay server IP address. A DHCP relay agent is used to forward and transfer DHCP messages between the clients and the server when

	they are not in the ame subnet domain.
Relay Information mode	Indicates the DHCP relay information mode option operation. The option 82 circuit ID format as “[vlan_id][module_id][port_no]”. The first four charactes represent the VLAN ID, the fifth and sixth characters are the module ID(in this switch is “0”), and the last tow characters are the port number. For example, “00030002” means the DHCP message receive from VLAN ID 3, this switch, port No 2. And the option 82 remote ID value is equal the switch MAC address. Possible modes are:
[Enable]	Enable DHCP relay information mode operation. When DHCP relay information mode operation is enabled, the agent inserts speific information(option 82) into a DHCP message when forwarding to DHCP server and removes it from a DHCP message when transferring to DHCP client. It only works when DHCP relay operation mode is enabled.
[Disabled]	Disable DHCP relay information mode operation
Relay Information Policy	Indicates the DHCP relay information option policy. When DHCP relay information mode operation is enabled, if agent receives a DHCP message that already contains relay agent information it will enforce the policy. The “Replace’ option is invalid when relay information mode is disabled. Possible policies are:
[Replace]	Replace the original replay information when a DHCP message that already contains it is received.
[Keep]	Keep the original relay information when a

	DHCP message that already contains it is received.
[Drop]	Drop the package when a DHCP message that already contains replay information is received

WEB Interface

A. **Click *Configuration/Security/Network/DHCP/Relay***
B. **Select Enabled/Disabled Relay Mode & specify the Relay Server and Relay Information Mode & policy settings**
C. **Click Save to apply the setting or Reset to restore the previous setting.**

DHCP Relay Configuration

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

Save Reset

Figure

Security/Network/IP Source Guard/Configuration

Using the IP Source Guard table(manually insert MAC Addres table) or DHCP Snooping table(dynamic MAC Address table) to filter IP trafficon switch ports.

LOCATION :

▼ Configuration

▼ Security

▼ Network

▼ IP Source Guard

▪ Configuration

PARAMETERS :

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

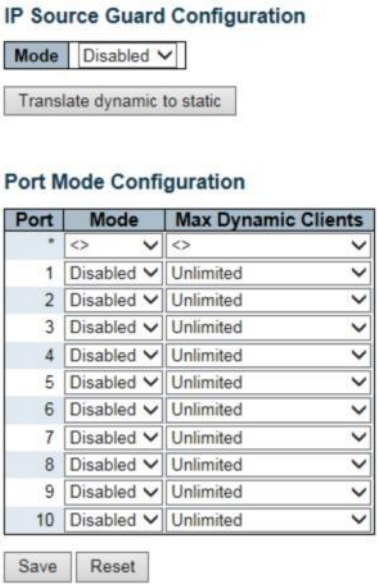
WEB Interface

A. Click *Configuration/Security/Network/ IP Source Guard/Configuration*

B. Select Enabled/Disabled IP Source Guard Mode

C. Set IP Source Guard for each port &Max number of allowing clients

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



Figure

Security/Network/IP Source Guard/Static Table

Creating a Static Port-VLAN-IP Address-MAC address mapping table for IP Source Guard usage.

LOCATION：

▼ Configuration

▼ Security

▼ Network

▼ IP Source Guard

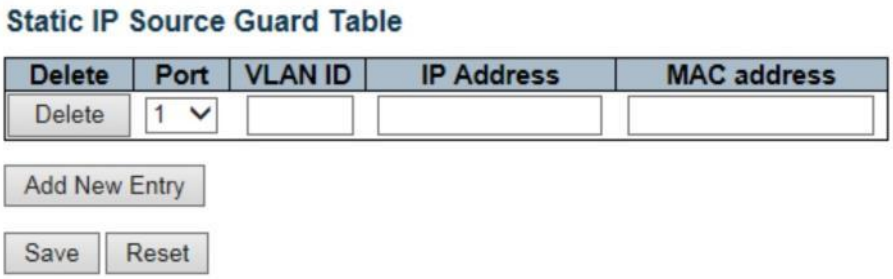
▪ Static Table

PARAMETERS :

Items	Description
Delete	Check to delete the entry. It will be deleted during the next save
Port	The logical port for the settings
VLAN ID	The vlan id for the setting
IP address	Allowed Source IP address
MAC address	Allowed Source MAC address

WEB Interface

A. **Click *Configuration/Security/Network/ IP Source Guard/Static Table***
B. **Click "Add New Entry" to create a new data with Port number, VLAN ID, IP Address & MAC Address**
C. **Click Save to apply the setting or Reset to restore the previous setting.**



Figure

Security/Network/ARP Inspection/Configuration

ARP Inspection is a protection for a certain "man-in-the-middle" attacks. It will validate the ARP request & response packet by interception with MAC-to-IP databae(dynamic:DHCP Snooping table, static: Static table)

LOCATION：

▼ Configuration

▼ Security

▼ Network

▼ IP Source Guard

▪ Static Table

PARAMETERS：

Items	Description
Mode	Enable the Global ARP Inspection or disable the Global ARP Inspection
Port Mode Configuration	Specify ARP Inspection is enabled on which ports. Only when both Global Mode and Port Mode on a given port are enabled, ARP Inspection is enabled on this given port.

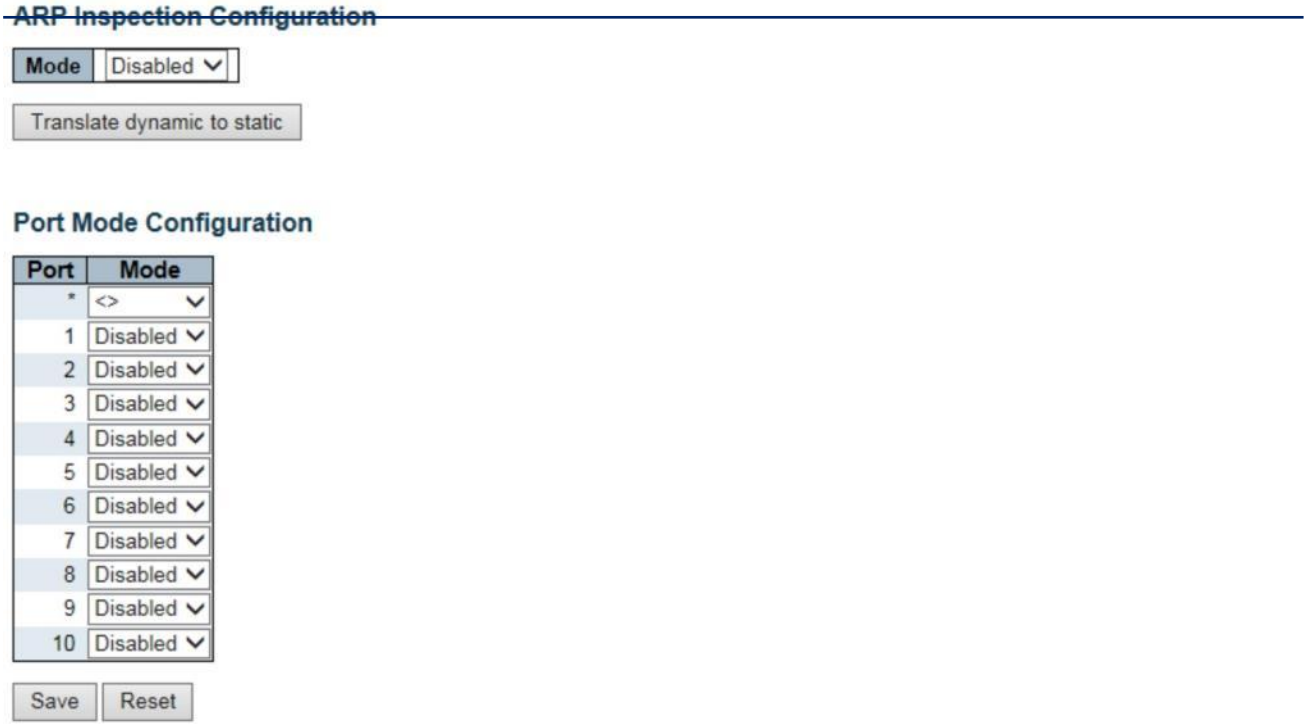
WEB Interface

A. Click *Configuration/Security/Network/ ARP Inspection/Configuration*

B. Select Enabled/Disabled ARP Inspection Mode

C. Select Enabled/Disabled ARP Inspection Mode for each port.

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



Figure

Security/Network/ARP Inspection/Static Table

Using the Static ARP Inspection table to create a database for validation.

The switch first compares ARP packets to any entries specified in the static ARP table. If No static entry matches the packets, then the DHCP snooping bindings database determines their validity

PARAMETERS：

Items	Description
Delete	Check the delete the entry. It will be deleted during the next save.
Port	The logical port for the settings.
VLAN ID	The valn id for the settings.
MAC Address	Allowed Source MAC address in ARP request packets
IP Address	Allowed Source IP address in ARP request packets

WEB Interface

A. Click *Configuration/Security/Network/ ARP Inspection/Static Table*
B. Click "Add New Entry" to create a new Static ARP inspection record for a given port, included Port number, VLAN ID, MAC Address and IP Address
C. Click Save to apply the setting or Reset to restore the previous setting.

Static ARP Inspection Table

Delete	Port	VLAN ID	MAC Address	IP Address
Delete	1			

Add New Entry

Save Reset

Figure

Security/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

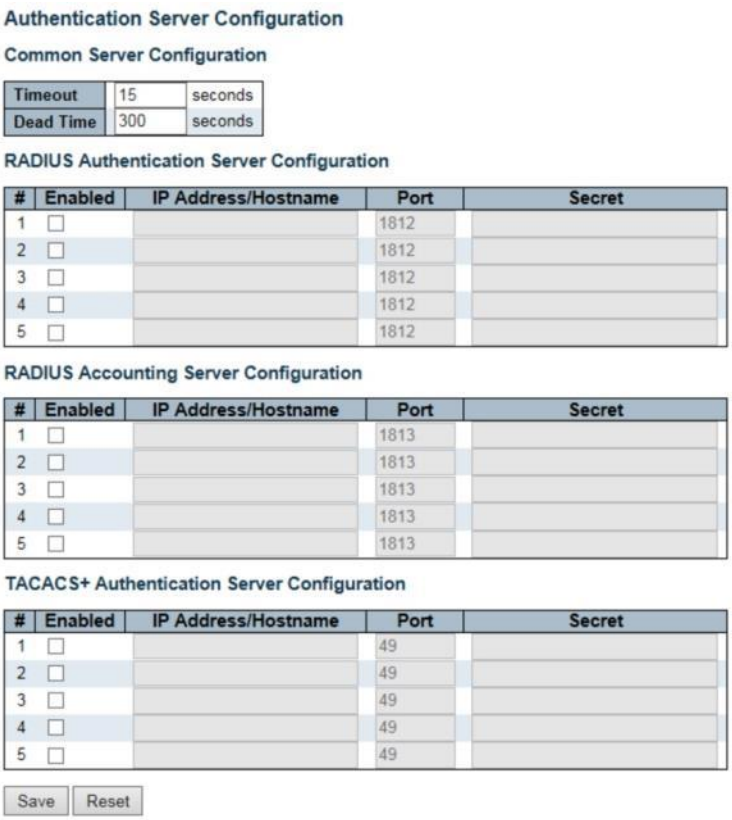
	dead if it does not reply. (Range : 0~3600 seconds)
RADIUS Authentication Server Configuration	
Enable	Enable the RADIUS Authentication Server by Check this box
IP Address	IP Address of RADIUS server
Port	The UDP port to use on the RADIUS authentication Server.
Secret	Encryption key(Maximum characters：29)

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.**

Figure



Authentication Server Configuration

Common Server Configuration

Timeout	15	seconds
Dead Time	300	seconds

RADIUS Authentication Server Configuration

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

RADIUS Accounting Server Configuration

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

TACACS+ Authentication Server Configuration

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

Save Reset

Figure

Aggregation/Static

Using Aggregation Mode Configuration page to create multiple links between devices that works as one virutal aggregated link. In this page, we can create static trunk groups.

LOCATION：

▼ Configuration

▼ Port Trunking

- Static

PARAMETERS：

Items	Description
Hash Code Contributors	
Source MAC Address	The Source MAC address can be used to calculate the destination port for the frame. Check to enable the use of the Source MAC address, or uncheck to disable. By default, Source MAC address is enabled.
Destination MAC Address	The Destination MAC Address can be used to calculate the destination port for the frame. Check to enable the use of the Destination MAC Address, or uncheck to disable. By default, Destination MAC Address is disabled.
IP Address	The IP Address can be used to calculate the destination port for the frame. Check to enable the use of the IP Address, or uncheck to disable. By default, IP Address is enabled.
TCP/IP Port Number	The TCP/IP port number can be used to calculate the destination port for the frame. Check to enable the use of the TCP/IP Port Number, or uncheck to disable. By default, TCP/UDP Port Number is enabled.
Aggregation Group Configuration	
Group ID	Indicates the group ID for the settings contained in the same row. Group ID “Normal” indicates there is no aggregation. Only one group ID is valid per port.
Port Members	Each switch port is listed for each group ID. Select a radio button to include a port in an aggregation, or clear the radio button to remove the port from the aggregation. By default, no ports belong to any aggregation group. Only full duplex ports can join an

aggregation and ports must be in the same speed in each group.

WEB Interface

A. **Click *Configuration/Agregation/Static***
B. **Select load-balancing method in hash code contributors,included “Source MAC Address”, “Destination MAC Address”, “IP Address” and “TCP/UDP” Port Number”**
C. **Assign port members to specific trunking group**
D. **Click Save to apply the setting or Reset to restore the previous setting.**

Aggregation Mode Configuration

Hash Code Contributors	
Source MAC Address	☑
Destination MAC Address	☐
IP Address	☑
TCP/UDP Port Number	☑

Aggregation Group Configuration

	Port Members									
Group ID	1	2	3	4	5	6	7	8	9	10
Normal	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉
1	○	○	○	○	○	○	○	○	○	○
2	○	○	○	○	○	○	○	○	○	○
3	○	○	○	○	○	○	○	○	○	○
4	○	○	○	○	○	○	○	○	○	○
5	○	○	○	○	○	○	○	○	○	○

Save Reset

Figure

Aggregation/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	Controls 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.
Timeout	The Timeout controls the period between BPDU transmissions. Fast Will transmit LACP packets each seconds, while Slow will wait for 30 seconds before sending a LACP Packet.
Prio	The Prio controls the priority of the port. If the LACP partner wants to form a larger group than is supported by this device then this parameter will control which ports will be

active and which ports will be in a backup role. Lower number means greater priority.

WEB Interface

A. **Click *Configuration/AggregationLACP***
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.**

LACP Port Configuration

Port	LACP Enabled	Key		Role	Timeout	Prio
*	☐	<>		<>	<>	32768
1	☐	Auto		Active	Fast	32768
2	☐	Auto		Active	Fast	32768
3	☐	Auto		Active	Fast	32768
4	☐	Auto		Active	Fast	32768
5	☐	Auto		Active	Fast	32768
6	☐	Auto		Active	Fast	32768
7	☐	Auto		Active	Fast	32768
8	☐	Auto		Active	Fast	32768
9	☐	Auto		Active	Fast	32768
10	☐	Auto		Active	Fast	32768

Save Reset

Figure

Loop Protection

Using Loop Protection page to configure loop protection

LOCATION：

▼ Configuration

▪ Loop Protection

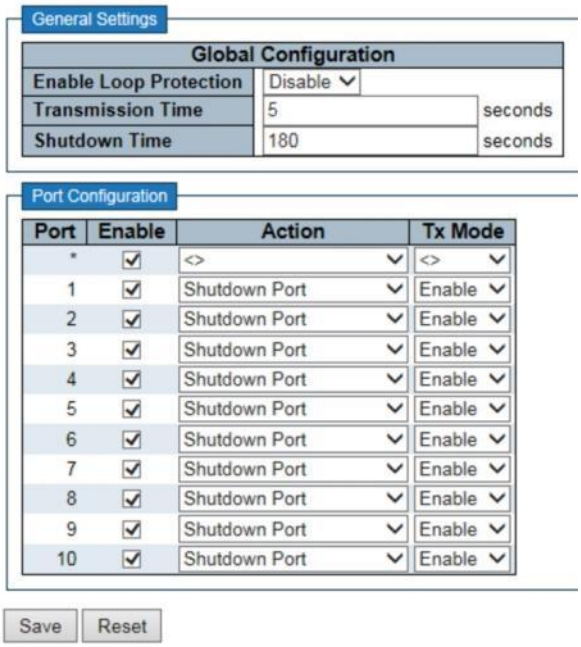
PARAMETERS：

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.**



Figure

Spanning Tree/Bridge Settings

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

LOCATION：

▼ Configuration

▼ Spanning Tree

▪ Bridge Settings

PARAMETERS：

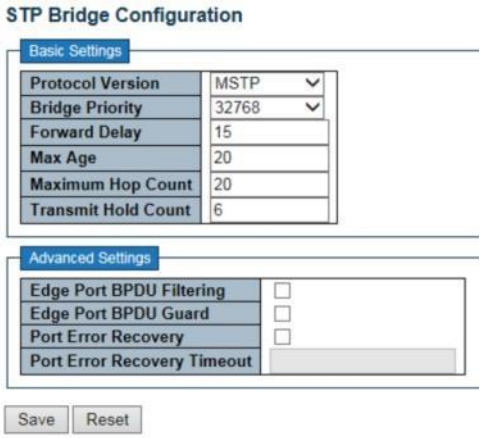
Items	Description
Basic Settings	
Protocol Version	The STP protocol version setting, the Valid

	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

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.**



Figure

Spanning Tree/ MSTI Mapping

Using MSTI Mapping page to inspect the current STP MSTI bridge instance priority configuration and possibly change them as well.

LOCATION：

▼ Configuration

▼ Spanning Tree

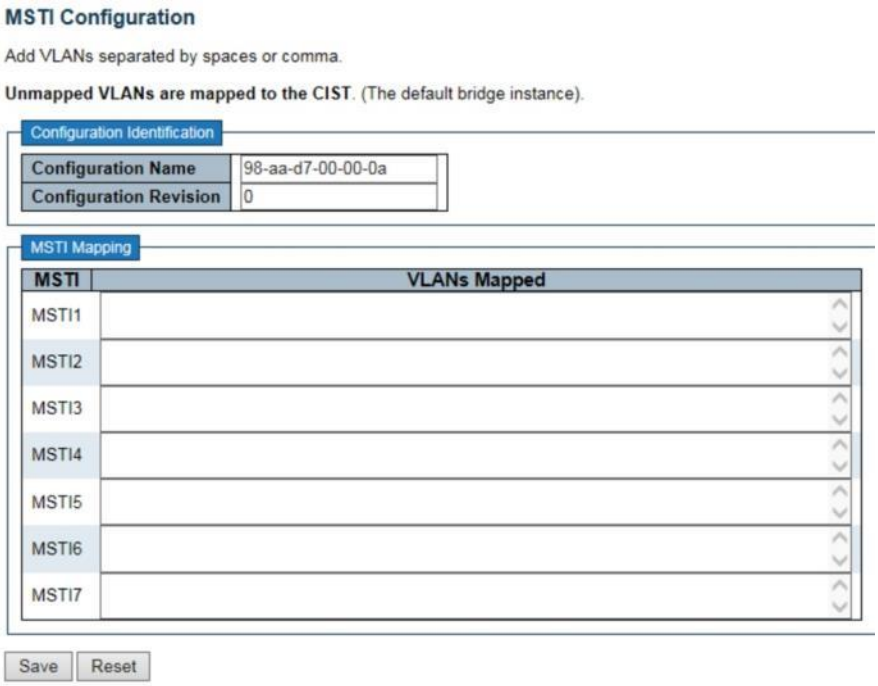
▪ MSTI Mapping

PARAMETERS :

Items	Description
Configuration Identification	
Configuration Name	The name identifying the VLAN to MSTI mapping. Bridges must share the name and revision (see below), as well as VLAN-to-MSTI mapping configuration in order to share spanning trees for MSTI's (intra-region). The name is at most 32 characters
Configuration Revision	The revision of the MSTI configuration named above. This must be an integer between 0 and 65535
MSTI Mapping	
MSTI	The bridge instance. The CIST is not available for explicit mapping, as it will receive the VLANs not explicitly mapped.
VLANs Mapped	The list of VLANs mapped to the MSTI. The VLANscan be given as a single(xx, xx being between 1 and 4094) VLAN, or a range(xx-yy), each of which must be separated with comma and/or space. A VLAN can only be mapped to one MSTI. An unused MSTI should just be left empty.(i.e. not having any VLANs mapped to it).Example 2,5,20-40

WEB Interface

A. **Click *Configuration/Spanning Tree/MSTI Mapping***
B. **Configure Identification and MSTI Mapping table**
C. **Click Save to apply the setting or Reset to restore the previous setting.**



Figure

Spanning Tree/MSTI Priorities

Using MSTI Priorities page to configure the bridge priority for the CIST and any configured MSTI. RSTP looks upon each MST Instance as a single bridge node.

LOCATION：

▼ Configuration

▼ Spanning Tree

- MSTI Priorities

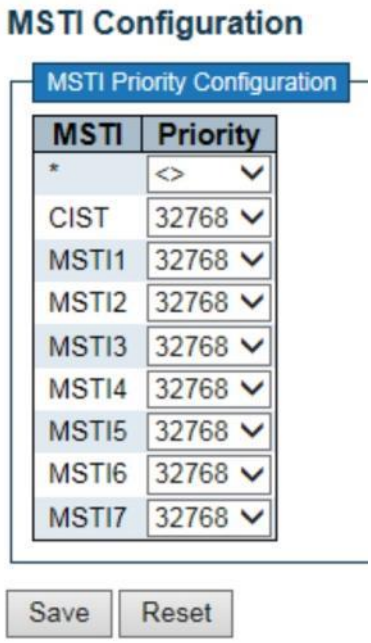
PARAMETERS：

Items	Description
MSTI	The bridge instance. The CIST is the

Priority	default instance, which is always active Controls the bridge priority, lower numeric values have better priority. The bridge priority plus the MSTI instance number, concatednated with the 6-byte MAC address of the switch forms a Bridge Identifier

WEB Interface

A. **Click *Configuration/Spanning Tree/MSTI Priorities***
B. **Set Priority for CIST and MIST1~7**
C. **Click Save to apply the setting or Reset to restore the previous setting.**



Figure

Spanning Tree/CIST 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

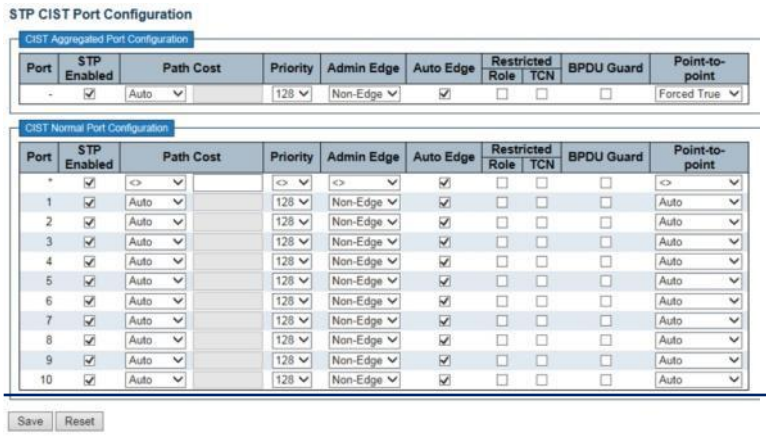
	to an end node or at the end o the bridge.
Auto Edge	Control whether automatic edge detection is enabled on a bridge port
Restricted Role	If enabled, cause the port not to be selected as Root port for the CIST, even if it has the best spanning tree priority vector. This features is also known as “Root 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

A. Click *Configuration/Spanning Tree/CIST Ports*

B. **Configure the required attributes**

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



Figure

Spanning Tree/MSTI Ports

This MSTI ports configuration page allows the user to inspect the current STP MSTI port configurations and possibly change them as well. An MSTI port is a virtual port, which is instantiated separately for each active CIST(physical) port for each MSTI instance configured on and applicable to the port.The MSTI instance must be selected before displaying actual MSTI port configuration options

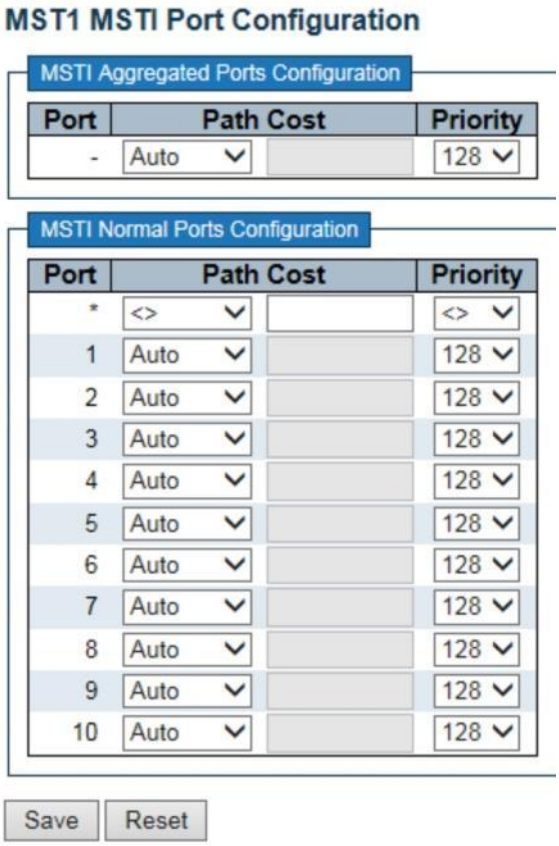
PARAMETERS：

Items	Description
MSTI Aggregated Ports Configuration	
Port	The switch port number of the corresponding STP CIST(and MSTI) 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

Priority	topology of the network. Low path cost ports are chosen as forwarding ports in favour of higher path cost ports. (Range：1-200000000) Controls the port priority. This can be used to control priority of ports having identical port cost.

WEB Interface

A. **Click *Configuration/Spanning Tree/MSTI Ports***
B. **Select MSTI then click "get" button**
C. **Set STA parameters for ports.**
D. **Click Save to apply the setting or Reset to restore the previous setting.**



Figure

MVR

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

PARAMETERS：

Items	Description
MVR Mode	Enable/Disable the Global MVR. The Unregistered Flooding control depends on the current configuration in IGMP/MLD snooping It is suggested to enable Unregistered Flooding control when the MVR group table is full
Delete	Check the delete the entry. The designated entry will be deleted during the next save
MVR VID	Specify the Multicast VLAN ID Be Caution: MVR source ports are not

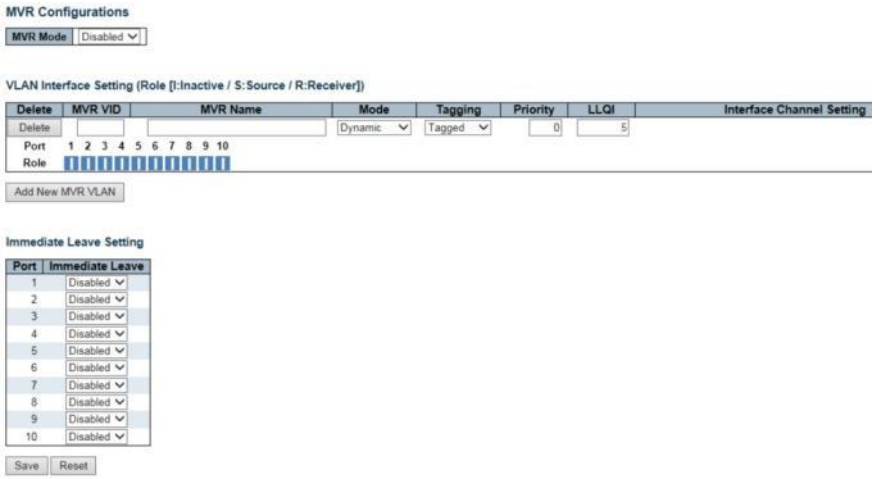
	recommended to be overlapped with management VLAN ports
MVR Name	MVR Name is an optional attribute to indicate the name of the specific MVR VLAN. Maximum length of the MVR VLAN Name string is 32. MVR VLAN Name can only contain alphabets or numbers. When the optional MVR VLAN name is given, it should contain at least one alphabet. MVR VLAN name can be edited for the existing MVR VLAN entries or it can be added to the new enteries.
Mode	Specify the MVR mode of operation. In Dynamic mode, MVR allows dynamic MVR membership reports on source ports. In Compatible mode, MVR memership reports are forbidden on source ports. The default is Dynamic mode.
Tagging	Specify whether the traversed IGMP/MLD control frames will be sent as Untagged or Tagged with MVR VID. The default is Tagged.
Priority	Specify how the traversed IGmP/mld control frames will be sent in prioritized manner. The default Priority is 0.
LLQI	Define the maximum time to wait for IGMP/MLD report memberships on a receiver port before removing the port from multicast group membership. The value is in units of tenths of a seconds. The range is from 0 to 31744. The default LLQI is 5 tenths or one-half second.
Interface Channel Setting	When the MVR VLAN is created, click the Edit symbol to expand the corresponding multicast channel settings for the specific MVR VLAN. Summary about the

	Interface Channel Setting(of the MVR VLAN) will be shown besides the Edit symbol
Port	The logical port for the setting
Port Role	Configure an MVR port of the designated MVR VLAN as one of the following roles.
[Inactive]	The designated port does not participate MVR operations
[Source]	Configure iplink ports that receive and send multicast data as source ports. Subscribers cannot be directly connected to source ports
[Receiver]	Configure a port as a receiver port if it is a subscriber port and should only receive multicast data. It does not receive data unless it becomes a member of the multicast group by issuing IGMP/MLD messages.
[Be Caution]	MVR source ports are not recommended to be overlapped with management VLAN ports.
	Select the port rule by clicking the Role symbol to switch the setting.
	“I” indicates Inactive, “S” indicates source;”R” indicates Receiver, the default Role is Inactive.

WEB Interface

A. **Click *Configuration/MVR***
B. **Enable MVR globally on the switch & select MVR VLAN.**
C. **Set VLAN interface setting**
D. **You can also check enable “fast leaving” for each port**

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



Figure

IPMC/IGMP/Snooping/Basic Configuration

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

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

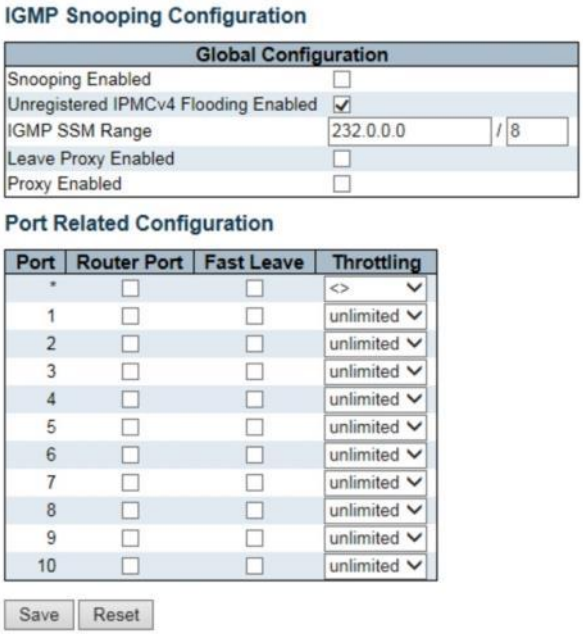
PARAMETERS :

Items	Description
Global Configuration	
Snooping Enabled	Control whether the IGMP snooping is enabled
Unregistered IPMCv4 Flooding Enabled	Enable unregistered IPMCv4 traffic flooding. The flooding control takes effect only when IGMP Snooping is enable. When IGMP Snooping is disabled, unregistered IPMCv4 traffic flooding is always active in spite of this setting.
IGMP SSM Range	SSM(Source-Specific Multicast) Range allows the SSM-aware hosts and routers run the SSM service model for the groups in the address range.
Leave Proxy Enable	Enable IGMP Leave Proxy. This feature can be used to avoid forwarding unnecessary leave messages to the router side
Proxy Enabled	Enable IGMP Proxy. This feature can be used to avoid forwarding unnecessary join and leave messages to the router side
Port Related Configuration	
Port	Port Identifier
Router Port	Specify which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or IGMP

	querier. If an aggregation member port is selected as a router port, the whole aggregation will act as a router port.
Fast Leave	Enable the fast leave on the port.
Throttling	Enable to limit the number of multicast groups to which a switch port can belong

WEB Interface

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.**



Figure

IGMP Snooping/VLAN Configuration

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

LOCATION：

▼ Configuration

▼ IPMC

▼ IGMP Snooping

▪ VLAN Configuration

PARAMETERS：

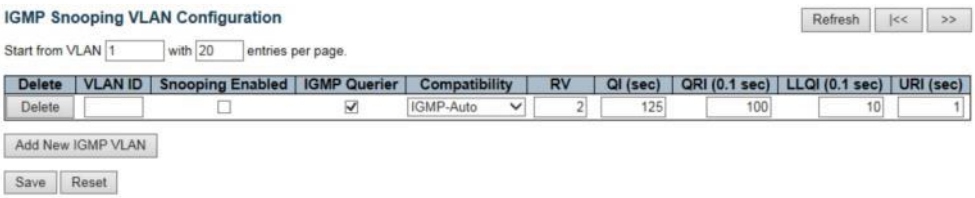
Items	Description
Delete	Check the delete the entry. The desginated entry will be deleted during the next save
VLAN ID	The VLAN ID of the entry
IGMP Snooping Enabled	Enable the per-VLAN IGMP Snooping. Up to 32 VLANs can be selected for IGMP Snooping.
IGMP Querier Compatiblity	Enable the IGMP Querier in the VLAN Compatibility is maintained by hosts and routers taking appropriate actions depending on the versions of IGMP

	operating on hosts and routers within a network. The allowed selection is IGMP-Auto,Forced IGMPv1, Forced IGMPv2, Forced IGMPv3, default compatibility value is IGMP-Auto
RV	Robustness Variable. The Robustness Variable allows tuning for the expected packet loss on a network. The allowed range is 1 to 255, default robustness variable is 2
QI	Query Interval. The Query Interval is the interval between General Queries sent by the Querier. The allowed range is 1 to 31744 seconds. Default query interval is 125 seconds
QRI	Query Response Interval. The maximum Response Delay used to calculate the Maximum Response Code inserted into the periodic General Queries. The allowed range is 0 to 31744 in tenths of seconds, default query response interval is 100 in tenths of seconds(10 seconds)
LLQI(LMQI for IGMP)	Last Member Query Interval. The last Member Query Time is the time value represented by the Last Member Query Interval, multiplied by the Last Member Query Count. The allowed range is 0 to 31744 in tenths of seconds, default last member query intervall is 10 in tenths of seconds (1 second)
URI	Unsolicited Report Interval. The Unsolicited Report Interval is the time between repetitions of a host's initial report of membership in a group. The allowed range is 0 to 31744 seconds,

	default unsolicited report interval is 1 second

WEB Interface

A. **Click *Configuration/IPMC/IGMP Snooping/VLAN Configuration***
B. **Click "Add New IGMP VLAN" to add new entry**
C. **Click Save to apply the setting, Reset to restore the previous setting.**
D. **Refresh Button：It will update the displayed table starting from that or the next closest VLAN Table Match.**



Figure

IPMC/IGMP Snooping/Port Group Filtering

Using Port Group Filtering Configuration page to filter specific multicast traffic

LOCATION：

▼ Configuration

▼ IPMC

▼ IGMP Snooping

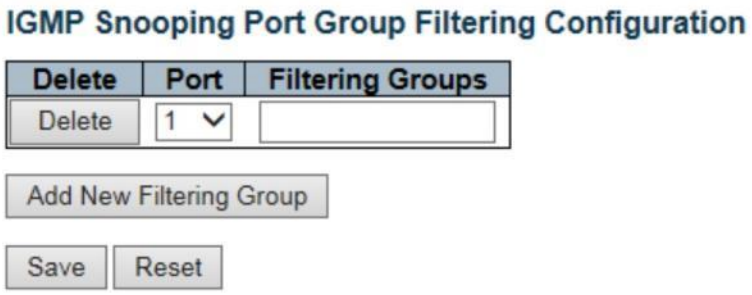
- VLAN Configuration

PARAMETERS :

Items	Description
Delete	Check the delete the entry. It will be deleted during the next save
Port	The logical port for the settings.
Filtering Groups	The IP Multicast Group that will be filtered.
Add New Filtering Group	Click"Add New Filtering Group" to add a new entry to the Group Filtering table. Specify the Port, and Filtering Group of the new entry.

WEB Interface

A. **Click *Configuration/IPMC/IGMP Snooping/Port Group Filtering***
B. **Click "Add New Filtering Group" to add new entry**
C. **Click Save to apply the setting, Reset to restore the previous setting.**



Figure

IPMC/MLD Snooping/Basic Configuration

Multicast Listener Discovery snooping is running on IPv6 network and performs a similar function to IGMP for IPv4

LOCATION：

▼ Configuration

▼ IPMC

▼ MLD Snooping

▪ Basic Configuration

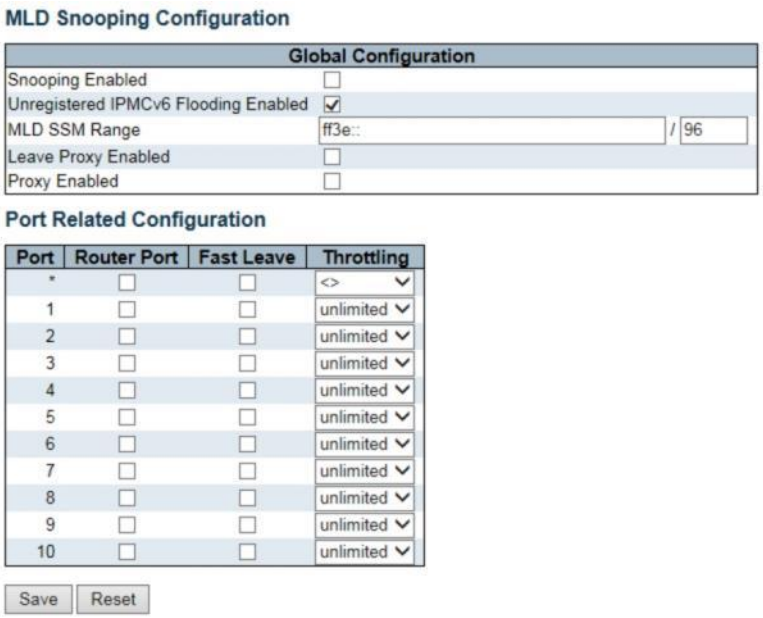
PARAMETERS：

Items	Description
Snooping Enabled	Enable the Global MLD Snooping
Unregistered IPMCv6 Flooding Enabled	Enable unregistered IPMCv6 traffic flooding. The flooding control takes effect only when MLD Snooping is enabled. When MLD Snooping is disabled, unregistered IPMCv6 traffic flooding is always active in spite of this setting.
MLD SSM Range	SSM (Source-Specific Multicast) Range allows the SSM-aware hosts and routers run the SSM service model for the groups in the address range.
Leave Proxy Enabled	Enable MLD leave Proxy, This feature can be used to avoid fowarding unnecessary leave messages to the router side.
Proxy Enabled	Enable MLD Proxy. This feature can

	be used to avoid forwarding unnecessary join and leave messages to the router side.
Router Port	Specify which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or MLD querier. If an aggregation member port is selected as a router port, the whole aggregation will act as a router port.
Fast leave	Enable the fast leave on the port
Throttling	Enable to limit the number of multicast groups to which a switch port can belong.

WEB Interface

A. **Click *Configuration/IPMC/MLD Snooping/Basic Configuration***
B. **Configre the MLD related parameters.**
C. **Click Save to apply the setting, Reset to restore the previous setting.**



Figure

IPMC/MLD Snooping/VLAN Configuration

Using the MLD Snooping VLAN Configuration page to configure MLD snooping and query for a VLAN interface

LOCATION：

▼ Configuration

▼ IPMC

▼ MLD Snooping

▪ VLAN Configuration

PARAMETERS：

Items	Description
Delete	Check the delete the entry. The designated entry will be delete during the next save.
VLAN ID	The VLAN ID of the entry
MLD Snooping Enabled	Enable the per-VLAN MLD Snooping. Up to 32 VLANs can be selected for MLD Snooping
MLD Querier Compatibilty	Enable the IGMP Querier in the VLAN Compatibility is maintained by hosts and routers taking appropriate actions depending on the versions of MLD operating on hosts and routers within a network. The allowed selection is “MLD-Auto”, “Forced-MLDv1”, “Forced MLDv2”, default compatibility value is

	“MLD-auto”
RV	Robustness Variable, the Robustness Variable allows tuning for the expected packet loss on a link. The allowed range is 1 to 255, default robustness variable value is 2.
QI	Query Interval, The Query Interval is the interval between General Queries sent by the Querier. The allowed range is 1 to 31744 seconds, default query interval is 125 seconds.
QRI	Query Response Interval. The maximum Response Delay used to calculate the Maximum Response Code inserted into the periodic General Queries. The allowed range is 0 to 31744 in tenths of seconds, default query response interval is 100 in tenths of seconds (10 seconds)
LLQI	Last listener Query Interval. The Last Listener Query Interval is the Maximum Response Delay used to calculate the Maximum Response Code inserted into Multicast Address Specific Queries sent in response to Version 1 Multicast Listener Done messages. It is also the Maximum Response Delay used to calculate the Maximum Response Code inserted into Multicast Address and Source Specific query message. The allowed range is 0 to 31744 in tenths of seconds, default last listener query interval is 10 in tenths of seconds(1 second).
URI	Unsolicited Report Interval. The Unsolicited Report Interval is the time between repetitions of a node’s initial report of interest in a multicast address. The allowed range is 0 to 31744 seconds, default

unsolicited report interval is 1 second.

WEB Interface

A. **Click *Configuration/IPMC/MLD Snooping/VLAN Configuration***
B. **Click "Add New MLD VLAN" to create a new MLD VLAN entry.**
C. **Click Save to apply the setting, Reset to restore the previous setting.**
D. **Refresh button: It will update the displayed table starting from that or the next closest VLAN Table Match**

Figure

IPMC/MLD Snooping/Port Group Filtering

Using MLD Snooping Port Group Filtering Configuration page to filter specific Multicast traffic.

LOCATION：

▼ Configuration

▼ IPMC

▼ MLD Snooping

▪ Port Group Filtering

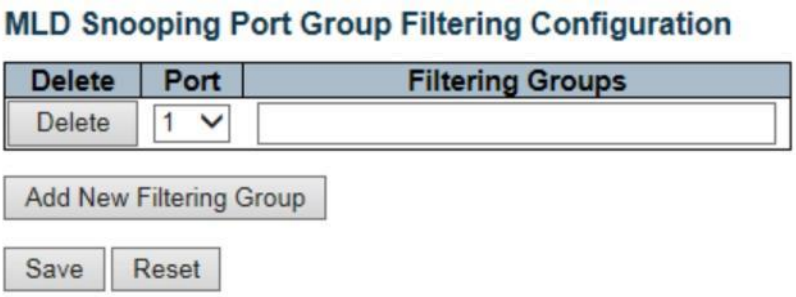
PARAMETERS：

Items	Description

Delete	Check the delete the entry. The designated entry will be delete during the next save.
Port	The logical port for the settings
Add New Filtering Group	Click “Add New Filtering Group” to add a new entry to the Group Filtering table. Specify the port, and Filtering Group of the new entry. Click “Save”

WEB Interface

A. **Click *Configuration/IPMC/MLD Snooping/Port Group Filtering***
B. **Click “Add New Filtering Group” to add new entry**
C. **Click Save to apply the setting, Reset to restore the previous setting.**



Figure

LLDP/LLDP

Link Layer Discovery Protocol is used to discover the basic information about neighbour device. According IEEE 802.1AB standard, it broadcasts the Advertised information to neighbours and gathered the information.

Using the LLDP Configuration page to set the timing parameters for LLDP advertisements and the device information which is advertised.

LOCATION：

▼ LLDP

▪ LLDP

PARAMETERS：

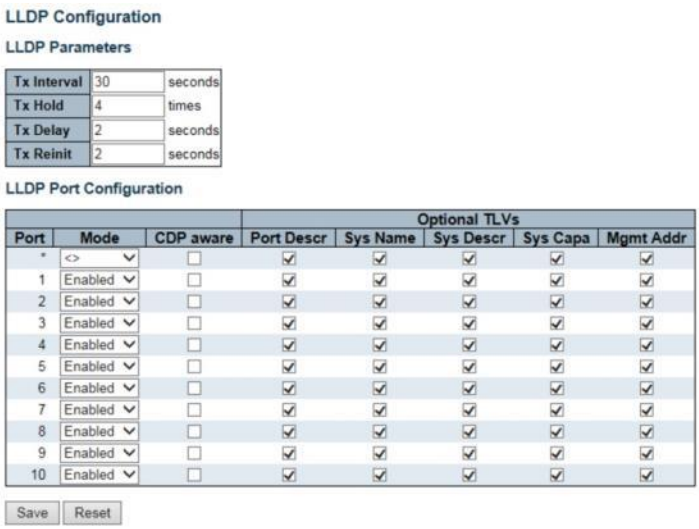
Items	Description
LLDP Parameters	
Tx Interval	The switch periodically transmits LLDP frames to its neighbours for having the netework discovery information up-to-date. The interval between each LLDP frame is determined by the Tx Interval value. Valid values are restricted to 5 ~ 32768 seconds.
Tx Hold	Each LLDP frame contains information about how long the information in the LLDP frame shall be considered valid. The LLDP information valid period is set to Tx Hold multiplied by Tx Interval seconds. Valid values are restricted to 2-10 times.
Tx Delay	If some configuration is changed (e.g. the IP address) a new LLDP frame is transmitted, but the time between the LLDP frames will always be at least the value of Tx Delay seconds. Tx Delay cannot be larger than 1/4 of the Tx Interval value. Valid values are restricted to 1~8192 seconds
Tx Reinit	When a port is disabled, LLDP is disabled or the switch is rebooted, an LLDP shutdown frame is transmitted to the neighboring units, signalling that the LLDP information isn't valid anymore. Tx Reinit controls the amount of seconds between the shutdown frame and a new LLDP initialization. Valid values are restricted to 1~10 seconds
LLDP Port Configuration	

Port	The switch port number of the logical LLDP port
Mode	Select LLDP mode
[Rx only]	The switch will not send out LLDP information, but LLDP information from neighbour units is analyzed.
[Tx only]	The switch will drop LLDP information received from neighbours, but will send out LLDP information.
[Disabled]	The switch will not send out LLDP information, and will drop LLDP information received from neighbours.
[Enabled]	The switch will send out LLdP information, and will analyze LLDP information received from neighbours.
CDP Aware	Select CDP awareness. The CDP operation is restircted to decoding incoming CDP frames(The switch doesn't transmit CDP frames). CDP frames are only decoded If LLDP on the port is enabled. Only CDP TLVs that can be mapped to a corresponding field in the LLDP neighbours' table are decoded. All other TLVs are discarded(Unrecognized CDP TLVs and discarded CDP frames are not shown in the LLDP statistics.) CDP TLVs are mapped onto LLDP neighbours' table as shown below. CDP TLV "Device ID" is mapped to the LLDP "Chassis ID" field. CDP TV "Address" is mapped to the LLDP "Management Address" field. The CDP address TLV can contain multiple addresses, but only the first address is shown in the LLDP neighbours table. CDP TLV "Port ID" is mapped to the LLDP "Port ID" field.

	CDP TLV “Version and Platform” is mapped to the LLDP “System Description” field. Both the CDP and LLDP support “system capabilities”, but the CDP capabilities cover capabilities that are not part of the LLDP. These capabilities are shown as “others” in the LLDP neughbours’ table.If all ports have CDP awareness disabled the switch forwards CDP frames received from neighbour devices. If at least one port has CDP awareness enabled all CDP frames are terminated by the switch. Note: When CDP awareness on a port is disabled the CDP information isn’t removed immediately, but gets removed when the hold time is exceeded.
Port Descr	Optional TLV: When checked the “port description” is included in LLDP information transmitted.
Sys Name	Optional TLV: When checked the “system name” is included in LLDP information transmitted.
Sys Capa	Optional TLV: When checked the “system capability” is included in LLDP information transmitted
Mgmt Addr	Optional TLV: When checked the “management address” is included in LLDP information transmitted

WEB Interface

A. **Click *Configuration/LLDP/LLDP***
B. **Set LLDP Parameters**
C. **Configure LLPD Mode, CDP aware and Optional TLVs parameters.**
D. **Click Save to apply the setting, Reset to restore the previous setting.**



LLDP Configuration

LLDP Parameters

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

LLDP Port Configuration

			Optional TLVs				
Port	Mode	CDP aware	Port Descr	Sys Name	Sys Descr	Sys Capa	Mgmt Addr
*	<>	☐	☑	☑	☑	☑	☑
1	Enabled	☐	☑	☑	☑	☑	☑
2	Enabled	☐	☑	☑	☑	☑	☑
3	Enabled	☐	☑	☑	☑	☑	☑
4	Enabled	☐	☑	☑	☑	☑	☑
5	Enabled	☐	☑	☑	☑	☑	☑
6	Enabled	☐	☑	☑	☑	☑	☑
7	Enabled	☐	☑	☑	☑	☑	☑
8	Enabled	☐	☑	☑	☑	☑	☑
9	Enabled	☐	☑	☑	☑	☑	☑
10	Enabled	☐	☑	☑	☑	☑	☑

Save Reset

Figure

LLDP/LLDP-MED

Using the LLDP-MED Configuration page to set the device information which is advertised for other devices

LOCATION：

▼ LLDP

- LLDP-MED

PARAMETERS：

Items	Description
Fast start repeat count	

Fast start repeat count	Rapid startup and Emergency Call Service Location Identification Discovery of endpoints is a critically important aspect of VoIP systems in general. In addition, it is best to advertise only those pieces of information which are specifically relevant to particular endpoint types (for example only advertise the voice network policy to permitted voice-capable devices), both in order to conserve the limited LLDPU space and to reduce security and system integrity issues that can come with inappropriate knowledge of the network policy. With this in mind LLDP-MED defines an LLDP-MED Fast Start interaction between the protocol and the application layers on top of the protocol, in order to achieve these related properties. Initially, a Network Connectivity Device will only transmit LLDP TLVs in an LLDPDU. Only after an LLDP-MED Endpoint Device is detected, will an LLDP-MED capable Network Connectivity Device start to advertise LLDP-MED TLVs in outgoing LLDPDUs on the associated port. The LLDP-MED application will temporarily speed up the transmission of the LLDPDU to start within a second, when a new LLDP-MED neighbour has been detected in order share LLDP-MED information as fast as possible to new

	neighbours. Because there is a risk of an LLDP frame being lost during transmission between neighbours, it is recommended to repeat the fast start transmission multiple times to increase the possibility of the neighbours receiving the LLDP frame. With **Fast start repeat count** it is possible to specify the number of times the fast start transmission would be repeated. The recommended value is 4 times, given that 4 LLDP frames with a 1 second interval will be transmitted, when an LLDP frame with new information is received. It should be noted that LLDP-MED and the LLDP-MED Fast Start mechanism is only intended to run on links between LLDP-MED Network Connectivity Devices and Endpoint Devices, and as such does not apply to links between LAN infrastructure elements, including Network Connectivity Devices, or other types of links.
Coordinates Location	
Latitude	Latitude SHOULD be normalized to within 0-90 degrees with a maximum of 4 digits.It is possible to specify the direction to either North of the equator or South of the equator.
Longitude	Longitude SHOULD be normalized to within 0-180 degrees with a maximum of 4 digits. It is possible to specify the

	diretion to either East of the prime meridian or West of the prime meridian
Altitude	Altitude SHOULD be normalized to within -32767 to 32767 with a maximum of 4 digits.It is possible to select between two altitude types(floors or meters). Meters: Representing meters of Altitude defined by the vertical datum specified Floors: Representing altitude in a from more erlevant in buildings which have different floor-to-floor dimensions. An altitude = 0.0 is meaningful even outside a building, and represents ground level at the given latitude and longitude. Inside a building, 0.0 represents the floor level associated with ground level at the main entrance.
Map Datum	The **Map Datum** is used for the coordinates given in these options: **WGS84:** (Geographical 3D)-World Geodesic System 1984, CRS Code 4327, Prime Meridian Name: Greenwich **NAD83/NAVD88:** North American Datum 1983, CRS Code 4269, Prime Meridian Name: Greenwich; The associated vertical datum is the North American Vertical Datum of 1988(NAVD88). This datum pair is to be used when referencing locations on land, not near tidal water(which would use Datum= NAD83/MLLW) **NAD83/MLLW:** North American Datum 1983, CRS Code 4269, Prime Meridian Name: Greenwich; The associated

	vertical datum is Mean Lower Low Water(MLLW). This datum pair is to be used when referencing locations on wate/sea/ocean.
Civic Address Location	
Country Code	The two-letter ISO 3166 country code in capital ASCII letters- Example: DK, DE or US.
State	National subdivisions(state, canton, region, province, prefecture).
County	County, parish, gun(Japan), district
City	City, township, shi(Japan)- Example: Copenhagen.
City district	City division, borough, city district, ward, chou(Japan).
Block(Neighbourhood)	Neighbourhood, block.
Street	Street- Example: Poppelvej.
Leading street diredtion	Leading street direction – Example : N
Trailing street suffix	Trailing street suffix – Example: SW
Street suffix	Street suffix – Example: Ave, Platz.
House no.	House number – Example : 21
House no. suffix	House number suffix – Example: A, 1/2
Landmark	Landmark or vanity address – Example: Columbia University
Additional location info	Additional location info –Example: South Wing.
Name	Name(residence and office occupant) – Example: Flemming Jahn.
Zip code	Postal/zip code – Example: 2791
Buidling	Building (structure) – Example: Low Library
Apartment	Unit(Apartment, suit) – Example: Apt 42.
Floor	Floor – Example: 4
Room no.	Room number – Example: 450F
Place type	Place type – Example: Office

Postal community name	Postal community name – Example: Leonia.
P.O. Box	Post office box(P.O.BOX)- Example – 12345
Additional code	Additional code – Example: 1320300003
Emergency Call Service	
Emergency Call Service	**Emergency Call Service** ELIN identifier data format is defined to carry the ELIN identifier as used during emergency call setup to a traditional CMAM or ISDN trunk-based PSAP. This format consists of a numerical digit string, corresponding to the ELIN to be used for emergency calling
Policies	
Policies	Network Policy Discovery enables the efficient discovery and diagnosis of mismatch issues with the VLAN configuration, along with the associated Layer 2 and Layer 3 attributes. **Policies** are only intended for use with applications that have specific "real-time" network policy requirements, such as interactive voice and/or video service. The network policy attributes advertised are: 1. Layer 2 VLAN ID(IEEE 802.1Q) 2. Layer 2 priority value(IEEE 802.1D) 3. Layer 3 Diffserv code point(DSCP) value(IETF RFC 2474) This network policy is potentially advertised and associated with multiple sets of application types supported on a given port. The

	application types specifically addressed are: 1. Voice 2. Guest Voice 3. Softphone Voice 4. Video Conferencing 5. Streaming Video 6. Control/Signalling(conditionally supporta separate network policy for the media type above)
Delete	Check to delete the policy, it will be deleted during the next save
Policy ID	ID for the policy, This is auto generated and shall be used when selecting the policies that shall be mapped to the specific ports.
Application Type	Intended use of the application types:
1.Voice	For use by dedicated IP Telephony handsets and other similar appliances supporting interactive voice services. These devices are typically deployed on a separate VLAN for ease of deployment and enhanced security by isolation from data applications
2.Voice Signalling(conditional)	For use in network topologies that require a different policy for the voice signalling than for the voice media. This application type should not be advertised if all the same network policies apply as those advertised in the Voice application policy.
3.Guest Voice	Support a separate “limited feature-set” voice service for guest users and visitors with their own IP Telephony handsets and other similar appliances supporting interactive voice services

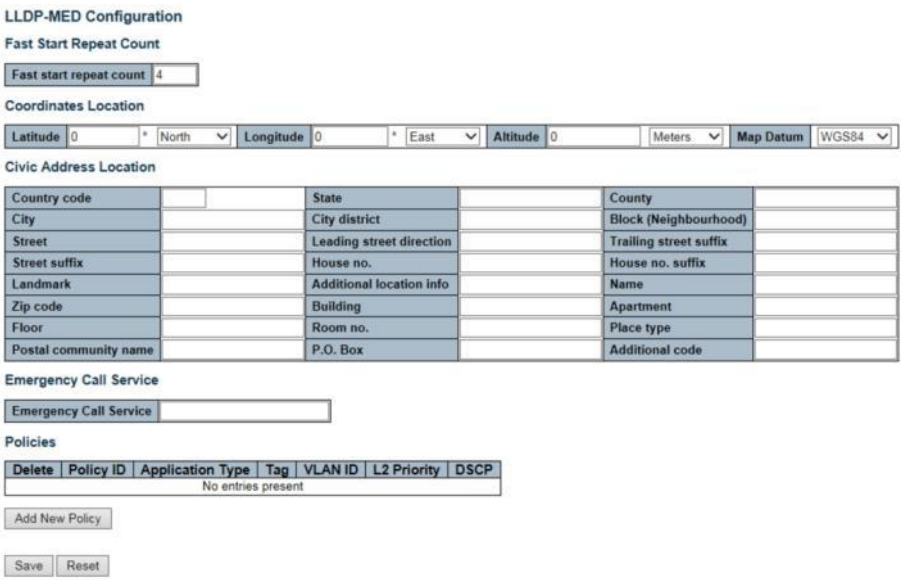
4.Guest Voice Signalling (conditional)	For use in network topologies that require a different policy for the guest voice signalling than for the guest voice media. This application type should not be advertised if all the same network policies apply as those advertised in the Guest Voice application policy.
5.Softphone Voice	For use by softphone application on typical data centric devices, such as PCs or laptops.This class of endpoints frequently does not support multiple VLANs, if at all, and are typically configured to use an “untagged” VLAN or a single “tagged” data specific VLAN. Whena network policy is defined for use with an “untagged” VLAN(see Tagged flag below), then the L2 priority field is ignored and only the DSCP value has relevance.
6.Video Conferencing	For use by dedicated Video Conferencing equipment and other similar appliance supporting real-time interactive video/audio services.
7.Streaming Video	For use by broadcast or multicast based video content distribution and other similar applications supporting streaming video services that require specific network policy treatment. Video applications relying on TCP with buffering would not be an intended use of this application ype.
8.Video Signallingconditional)	For use in network topologies that require a separate policy for the video signalling than for the video media. This application type should not be advertised if all the same network

	policies apply as those advertised in the **Video Conferencing** application policy
Tag	**Tag** indicating whether the specified application type is using a “Tagged” or an “untagged” VLAN **Untagged** indicates that the device is using an untagged frame format and as such does not include a tag header as defined by IEEE 802.1Q-2003. In this case, both the VLAN ID and Layer 2 priority fields are ignored and only the DSCP value has relevance. **Tagged** indicates that the device is using the IEEE 802.1Q tagged frame format, and that both the VLAN ID and the Layer 2 priority values are being used, as well as the DSCP value. The tagged format includes an additional field, known as the tag header. The tagged frame format also includes priority tagged frames as defined by IEEE 802.1Q-2003
VLAN ID	VLAN identifier (VID) for the port as defined in IEEE 802.1Q-2003
L2 Priority	**L2 Priority** is the Layer 2 priority to be used for the specified application type. **L2 Priority** may specify on of eight priority levels (0 through 7), as defined by IEEE 802.1D-2004. Avalue of 0 represents use the default priority as defined in IEEE 802.1D-2004
DSCP	**DSCP** value to be used to provide Diffserv node behaviour for the specified application type as defined in IETF RFC2474. DSCP may contain one of 64 code point values (0 through

63). A value of 0 represents use of the default DSCP value as defined in RFC 2475

WEB Interface

A. **Click *Configuration/LLDP/LLDP-MED***
B. **Set LLDP-MED Parameters**
C. **Click Save to apply the setting, Reset to restore the previous setting.**



Figure

MAC Table

Using the MAC Address Table Configuration page to configure dynamic address learning or to assign static addresses to specific ports

LOCATION：

▼ Configuration

▪ MAC Table

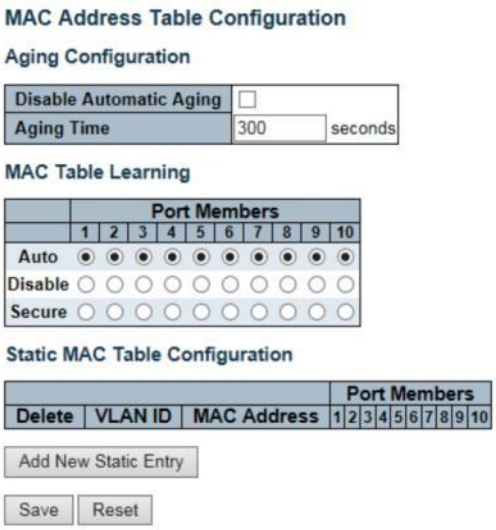
PARAMETERS：

Items	Description
Aging Configuration	
Disable Automatic Aging	Check to disable Automatic Aging time,default dynamic entries are removed from MAC Table after 300 seconds
Aging Time	Configure aging time by entering a value here in seconds;The allowed range is 10 to 1000000 seconds
MAC Table Learning	
	If the learning mode for a given port is greyed out, another module is in control of the mode, so that it can't be changed by the user. Example,such a module is the MAC-Based Authentication under 802.1X
Auto	Learning is done automatically as soon as frame with unknown SMAC is received
Disable	No learning is done.
Secure	Only static MAC entries are learned, all other frames are dropped. Note: Make sure that the link used to managing switch is added to the Static MAC Table before changing to secure learning mode, otherwise the management link is lost and can only to restored by using another non-secure port

	or by connecting to the switch via the serial interface.

WEB Interface

A. **Click *Configuration/MAC Table***
B. **Configure MAC Table and change the aging time if required**
C. **Specify the learning method for each port.**
D. **Click Save to apply the setting, Reset to restore the previous setting.**



Figure

VLANs/VLAN Membership

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.

The VLAN Membership Configuration for the switch can be monitored and modified here. Up to 4096 VLANs are supported

LOCATION：

▼ Configuration

▼ VLANs

▪ VLAN Membership

PARAMETERS：

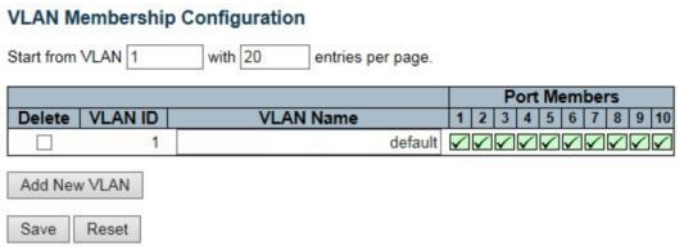
Items	Description
Delete	To delete a VLAN entry, check this box. The entry will be deleted during the next save.
VLAN ID	ID of this particular VLAN (Range：1-4096)
VLAN Name	Indicates the name of the VLAN. VLAN name can be null. If it is not null, it must contain alphabets or numbers. At least one alphabet must be present in a non-null VLAN name. VLAN name can be edited for the existing VLAN entries or it can be added to the new entries.(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

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.



Figure

VLANs/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 checkingthe box. This parameter affects VLAN ingressprocessing. If ingress filtering is enabled andthe ingress port is not a member of theclassified VLAN of the frame, the frame isdiscarded. By default, ingress filtering isdisabled.
Frame Type	Determines whether the port accepts all frames or only tagged/untagged frames. Thisparameter affects VLAN ingress processing.If the port only accepts tagged frames,untagged frames received on this port will bediscarded
Port VLAN mode	Configure VLAN mode to “None” or Specific”, None：a VLAN tag with classified VLAN ID isInserted 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

Port VLAN ID	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. Configures the VLAN identifier for the port. The allowed values are 1 through 4095. Thedefault 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 configuredPVID will be tagged. Tag_all - All VLANs aretagged. Untag_all - All VLANs are untagged

WEB Interface

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.**

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

  Starting from the first entry of the VLAN table.

Ethertype for Custom S-ports 0x 88A8

VLAN Port Configuration

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

Save Reset

Figure

Private VLAN/PVLAN Membership

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.

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

LOCATION：

▼ Configuration

▼ Private VLANs

▪ PVLAN Membership

PARAMETERS：

Items	Description
Delete	To delete a private VLAN entry, check this box. The entry will be deleted during the next save.
Private VLAN ID	Indicates the ID of this paritcular 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

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.**

Private VLAN Membership Configuration

		Port Members									
Delete	PVLAN ID	1	2	3	4	5	6	7	8	9	10
☐	1	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑

Add New Private VLAN

Save Reset

Figure

VLANs/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：

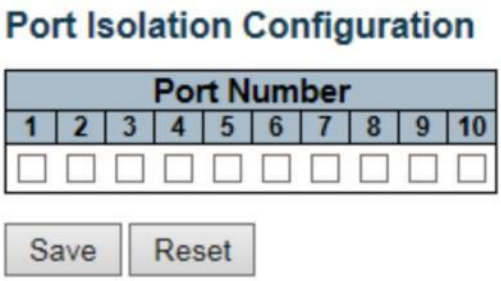
Items	Description
Port Members	A check box is provided for each port of a private VLAN. When checked, port isolation is enabled on that port. When unchecked, port isolation is disabled on that port. By default, port isolation is disabled on all ports.

WEB Interface

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.



Figure

VCL/MAC-based VLAN

Using MAC-Based VLAN Membership Configuration to configure VLAN based on MAC addresses. It will assign a VLAN ID for the ingess untagged frame by the source MAC address. If it didn't match by the database, it will be assigned by Port VLAN ID.

LOCATION：

▼ Configuration

▼ VCL

▪ MAC-based VLAN

PARAMETERS：

Items	Description
Delete	To delete a MAC-based VLAN entry, check this box and press save. The entry will be deleted in the stack.
MAC Address	Indicates the MAC Address
VLAN ID	Indicates the VLAN ID.
Port Members	A row of check boxes for each port is displayed for each MAC-based VLAN entry. To include a port in a MAC-based VLAN, check the box. To remove or exclude the port from the MAC-based VLAN, make sure the box is unchecked. By default, no ports are members, and all boxes are unchecked.

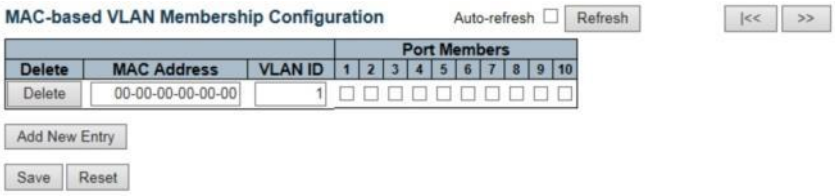
WEB Interface

A. Click *Configuration/VCL/MAC-based VLAN*

B. Click "Add New Entry" to create a new entry

C. Insert the MAC Address and VLAN ID and select applied ports.

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



Figure

VCL/Protocol-based VLAN/Protocol to Group

This function can assign a specific protocol frame into a VLAN group. When a frame is received in a port, its VLAM membership can then be determined based on the protocol type being used by the inbound packets

LOCATION：

▼ Configuration

▼ VCL

▼ Protocol-based VLAN

▪ Protocol to Group

PARAMETERS：

Items	Description
Delete	To delete a Protocol to Group Name map entry, check this box. The entry will be deleted on the switch during the next Save
Frame Type	Frame Type can have one of the following values: **1. Ethernet** **2. LLC**

	3. **SNAP** 4. Note: On changing the Frame type field, valid value of the following text field will vary depending on the new frame type you selected
Value	Valid value that can be entered in the text field depends on the option selected from the preceding Frame Type selection menu.Below is the criteia for three different Frame Types:
[For Ethernet]	Values in the text field when Ethernet is selected as a Frame Type is call etype. Valid values for etype ranges from 0x0600-0xffff
[For LLC]	Valid value in this case is comprised of two different sub-values: a. **DSAP:** 1-byte long string(0x00-0xff) b. **SSAP:** 1-byte long string(0x00-0xff)
[For SNAP]	Valid value in this case also is comprised of two different sub-values: a. **OUI:** OUI(Organizationally Unique Identifier) is value in format of xx-xx-xx where each pair(xx) in string is a hexadecimal value ranges from 0x00-0xff. b. **PID:** if the OUI is hexadecimal 000000, the protocol ID is the Ethernet type(EtherType) field value for the protocol running on top of SNAPI if the OUI is an OUI for a particular organization, the protocol ID is a value assigned by that organization to the protocol running on top of SNAP. In other word, if value of OUI field is 00-00-00 then value of PID will be etype (0x0600-0xffff) and if value of OUI is other than 00-00-00 then valid value of PID will be any value from 0x000 to 0xffff
Group Name	A valid Group Name is unique 16-characterslong string for every entry which

consists of a combination of alphabets (a-z or A-Z) and integers(0-9)
Note: special character and underscore(_) are not allowed.

WEB Interface

A. **Click *Configuration/VCL/Protocol-Based VLAn/Protocol to Group***
B. **Click "Add New Entry" to create a new entry**
C. **Select Frame Type, Etype value and Group Name**
D. **Click Save to apply the setting, Reset to restore the previous setting.**

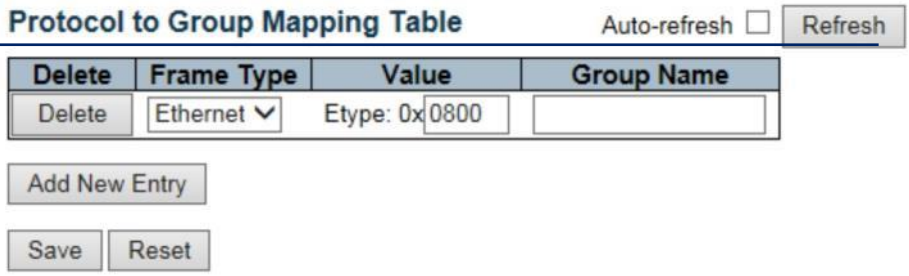


Figure.

VCL/Protocol-based VLAN/Group to VLAN

The Group Name to VLAN mapping Table allows you to add new protocols to Group Name(unique for each Group) mapping entries as well as allow you to see ad delete already mapped entries for the switch.

LOCATION：

▼ Configuration

▼ VCL

▼ Protocol-based VLAN

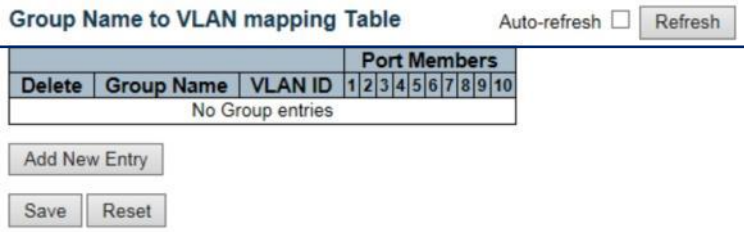
- Group to VLAN

PARAMETERS :

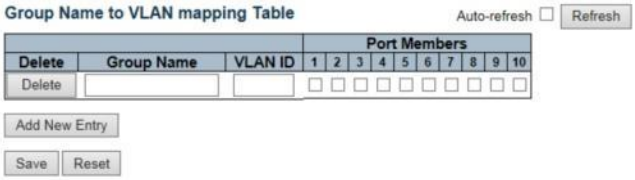
Items	Description
Delete	To delete a Group Name map entry, check this box. The entry will be deleted on the switch during the next Save.
Group Name	A valid Group Name is a string at the most 16 characters which consists of a combination of alphabets (a-z or A-Z) and inteers(0-9), no special character is allowed. Whichever Group Name you try map to a VLAN must be present in Protocol to Group mapping table and must not be pre-used by any other existing entry on this page.
VLAN ID	Indicates the ID to which Group Name will be mapped. A valid VLAN ID ranges from 1-4095
Port Members	A row of check boxes for each port is displayed for each Group Name to VLAN ID mapping. To include a port in a mapping, check the box. To remove or exclude the port from the mapping, make sure the box is unchecked. By default, no ports are members. And all boxes are unchecked

WEB Interface

A. **Click *Configuration/VCL/Protocol-Based VLAn/Protocol to Group***
B. **Click "Add New Entry" to create a new entry**
C. **Select Frame Type, Etype value and Group Name**
D. **Click Save to apply the setting, Reset to restore the previous setting.**



Figure



Figure

VCL/Protocol-based VLAN/IP Subnet-based VLAN

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

LOCATION：

▼ Configuration

▼ VCL

▪ IP Subnet-based VLAN

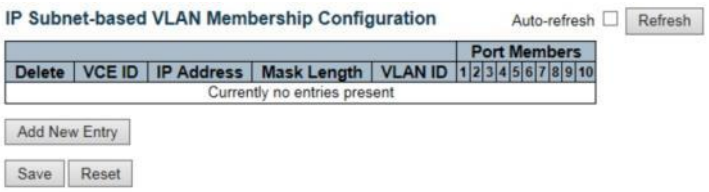
PARAMETERS：

Items	Description
Delete	To delete a IP subnet-based VLAN entry, check this box and press save. The entry will be deleted in the stack.
VCE ID	Indicates the index of the entry. It is users configurable. It's value ranges from 0-128. If a VCD ID is 0, application will auto-generate

	the VCE ID for that entry. Deletion and lookup of IP subnet-based VLAN are based on VCE ID
IP Address	Indicates the IP Address
Mask Length	Indicates the network mask length
VLAN ID	Indicates the VLAN ID. VLAN ID can be changed for the existing entries
Port Members	A row of check boxes for each port is displayed for each IP subnet-based VLAN entry. To include a port in a IP subnet-based VLAN, check the box. To remove or exclude the port from the IP subnet-based VLAN, make sure the box is unchecked. By default, no ports are members, and all boxes are unchecked.

WEB Interface

A. **Click *Configuration/VCL/IP Subnet-based VLAN***
B. **Click "Add New Entry" to create a new entry**
C. **Set VCE ID, IP Address, subnet Mask, VLAN ID and port members.**
D. **Click Save to apply the setting, Reset to restore the previous setting.**



Figure

Voice VLAN/Configuration

Using the Voice VLAN Configuration page to configure the switch for VoIP service. The Voice VLAN feature enables voice traffic forwarding on the Voice VLAN, then the switch can classify and schedule network traffic. It is recommended that there be two VLANs on a port- one for voice, one for data. Before connecting the IP device to the switch, the IP phone should configure the voice VLAN ID correctly, It should be configured through its own GUI.

LOCATION：

▼ Configuration

▼ Voice VLAN

▪ Configuration

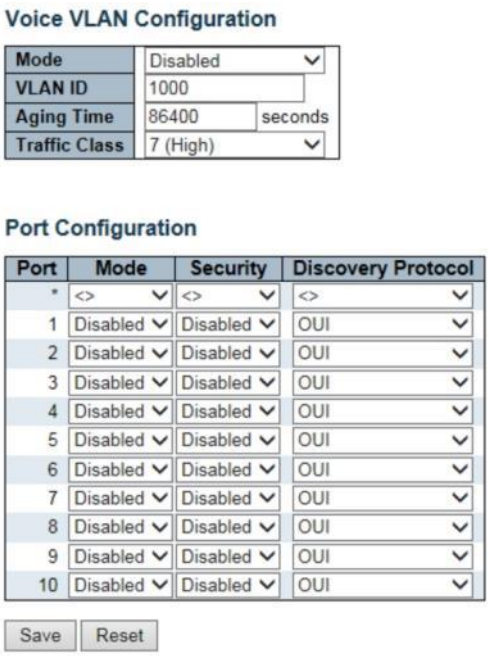
PARAMETERS：

Items	Description
Mode	Indicates the Voice VLAN mode operation. We must disable MSTP feature before we enable Voice VLAN. It can avoid the conflict of ingress filtering. Possible modes are: **Enable:** Enable Voice VLAN mode operation **Disabled:** Disable Voice VLAN mode operation
VLAN ID	Indicates the Voice VLAN ID. It should be a unique VLAN ID in the system and cannot equal each port PVID. It is a conflict in configuration if the value equals management VID, MVR VID, PVID etc. The allowed range is 1 to 4095

Aging Time	Indicates the Voice VLAN secure learning aging time. The allowed range is 10 to 10000000 seconds. It is used when security mode or auto detect mode is enabled. In other cases, it will be based on hardware aging time. The actual aging time will be situated between the [age_time;2*age]time] interval.
Traffic Class	Indicates the Voice VLAN traffic class. All traffic on the Voice VLAN will apply this class.
Port Mode	Indicates the Voice VLAN port mode.Possible port modes are: **Disabled:** Disjoin from Voice VLAn **Auto:** Enable auto detect mode. It detects whether there is VoIP phone attached to the specific port and configures the Voice VLAN members automatically. **Forced:** Force join the Voice VLAN
Port Discovery Protool	Indicates the Voice VLAN port discovery protocol. It will only work when auto detect mode is enabled. We should enable LLDP feature before configuring discovery protocol to “LLDP” or “Both”. Changing the discovery potocol to “OUI” or “LLDP” will restart auto detect process. Possible discovery protocols are: **OUI:** Detect telephony device by OUI address **LLDP:** Detect telephony device by LLDP. **Both:** Both OUI and LLDP.

WEB Interface

A. **Click *Configuration/Voice VLAN/Configuration***
B. **Configure any required changes to VoIP setting for the switch or specific port.**
C. **Click Save to apply the setting, Reset to restore the previous setting.**



Figure

Voice VLAN/OUI

Using Voice VLAN OUI Tabe to set identity Table of VoIP devices in this switch. The maximum number of entries is 16. Modifying The OUI table will restart auto detection of OUI process.

LOCATION：

▼ Configuration

▼ Voice VLAN

▪ OUI

PARAMETERS：

Items	Description
Delete	Check to delete the entry. It will be deleted during the next save.
Telephony OUI	A telephony OUI address is a globally unique identifier assigned to a vendor by IEEE. It must be 6 characters long and the input format is “xx-xx-xx”(x is a hexadecimal digit)
Description	The description of OUI address. Normally, it describes which vendor telephony device it belongs to. The allowed string length is 0 to 32.

WEB Interface

A. **Click *Configuration/Voice VLAN/OUI***
B. **Click “Add New Entry” to add new entry**
C. **Click Save to apply the setting, Reset to restore the previous setting.**

Voice VLAN OUI Table

Delete	Telephony OUI	Description
☐	00-01-e3	Siemens AG phones
☐	00-03-6b	Cisco phones
☐	00-0f-e2	H3C phones
☐	00-60-b9	Philips and NEC AG phones
☐	00-d0-1e	Pingtel phones
☐	00-e0-75	Polycom phones
☐	00-e0-bb	3Com phones
Delete		

Add New Entry

Save Reset

Figure

QoS/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, All frames are classified to a DP level. If the port is VLAN aware, The frame is tagged and Tag Class. Is enabled, then the frame is classified to a DP level that is mapped from the PCP and DEI value in the tag. Otherwise the frame is classified to the default DP level.The classified DP level can be overruled by a QCL entry
PCP	Controls the default Priority Code Point(PCP) All frames are classified to a PCP value. If the port is VLAN aware and the frame is tagged, then the frame is classified to the PCP value in the tag. Otherwise the frame is classified to the default PCP value
DEI	Controls the default Drop Eligible Indicator (DEI) for untagged frames.All frames are classified to a DEI value. If the port is VLAN aware and the frame is tagged, then the frame is classified to the DEI value in the tag. Otherwise the frame is classified to the default DEI value.
Tag Class	Shows the classification mode for tagged frames on this port. **Disabled:** Use default QoS class and DP level for tagged frames. **Enabled:** Use mapped versions of PCP and DEI for tagged frame Click on the mode in order to configure the mode and/or mapping **Note:** This setting has no effect if the port is VLAN unaware. Tagged frames received on VLAN unaware ports are always classified to the default QoS class and DP level.

WEB Interface

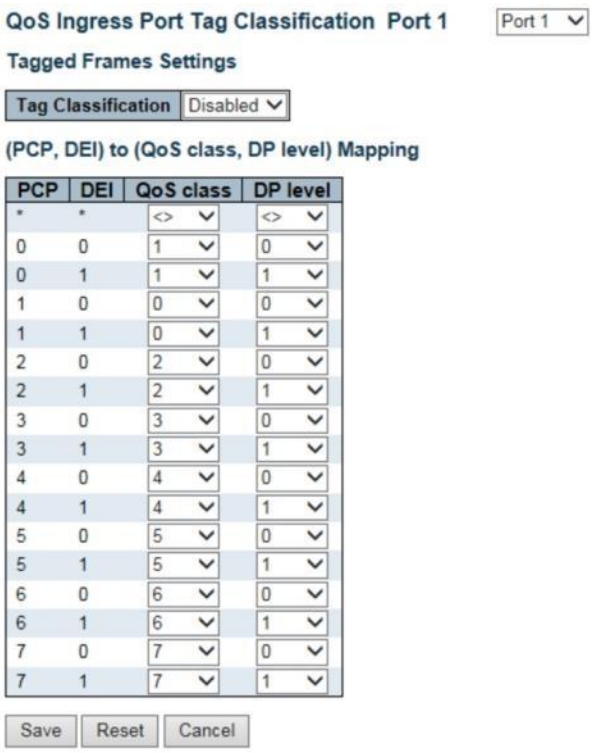
A. Click *Configuration/QoS/Port Classification*
B. Set QoS Class priority for each port, DP Level and PCP, DEI for untagged frames.
C. Or choose Tagged Class. setting
D. Click Save to apply the setting, Reset to restore the previous setting.

QoS Ingress Port Classification

Port	QoS class	DP level	PCP	DEI	Tag Class.	DSCP Based
*	<>	<>	<>	<>		☐
1	0	0	0	0	Disabled	☐
2	0	0	0	0	Disabled	☐
3	0	0	0	0	Disabled	☐
4	0	0	0	0	Disabled	☐
5	0	0	0	0	Disabled	☐
6	0	0	0	0	Disabled	☐
7	0	0	0	0	Disabled	☐
8	0	0	0	0	Disabled	☐
9	0	0	0	0	Disabled	☐
10	0	0	0	0	Disabled	☐

Save Reset

Figure



Figure

QoS/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

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 Ingress Port Policers

Port	Enabled	Rate	Unit	Flow Control
*	☐	500	<>	☐
1	☐	500	kbps	☐
2	☐	500	kbps	☐
3	☐	500	kbps	☐
4	☐	500	kbps	☐
5	☐	500	kbps	☐
6	☐	500	kbps	☐
7	☐	500	kbps	☐
8	☐	500	kbps	☐
9	☐	500	kbps	☐
10	☐	500	kbps	☐

Save Reset

Figure

QoS/Port Scheduler

Using the QoS Egress Port Schedulers to show an overview of the Egress Port Scheduling Table, included queue mode and Weight. Click Port number to configure.

LOCATION：

▼ Configuration

▼ QoS

▪ Port Scheduler

PARAMETERS：

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

WEB Interface

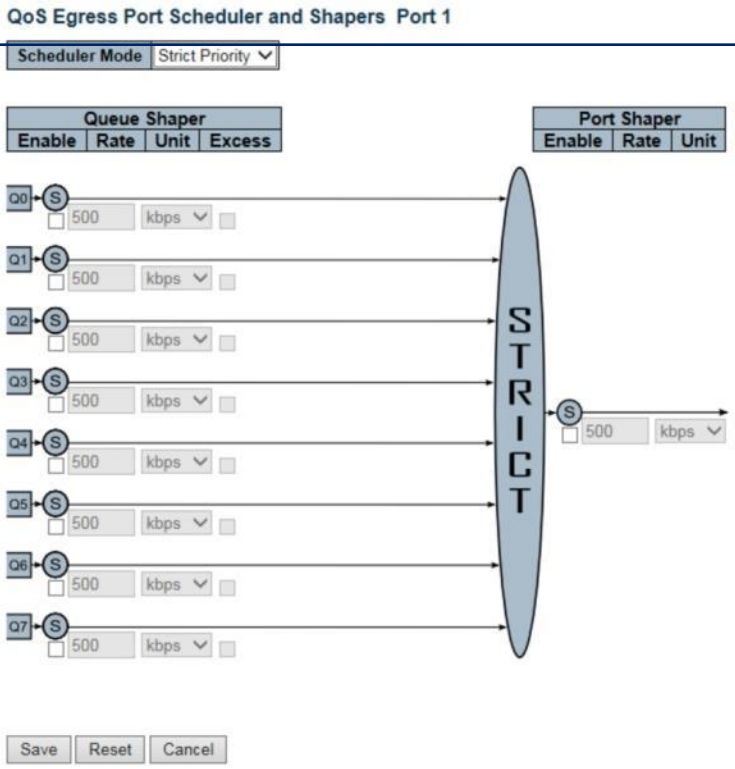
A. Click *Configuration/QoS/Port Scheduler*

B. **During the overview page, Click port number into Scheduler setting fo specific port**
C. **Click Save to apply the setting, Reset to restore the previous setting.**

QoS Egress Port Schedulers

Port	Mode	Weight					
		Q0	Q1	Q2	Q3	Q4	Q5
1	Strict Priority	-	-	-	-	-	-
2	Strict Priority	-	-	-	-	-	-
3	Strict Priority	-	-	-	-	-	-
4	Strict Priority	-	-	-	-	-	-
5	Strict Priority	-	-	-	-	-	-
6	Strict Priority	-	-	-	-	-	-
7	Strict Priority	-	-	-	-	-	-
8	Strict Priority	-	-	-	-	-	-
9	Strict Priority	-	-	-	-	-	-
10	Strict Priority	-	-	-	-	-	-

Figure



Figure

QoS/Port Shaping

Using the QoS Egress Port shapers to show an overview of the QoS Egress Port Shapers. Include rate of each queue and port.Click Port number to configure.

LOCATION：

▼ Configuration

▼ QoS

▪ Port Shaping

PARAMETERS：

Items	Description
Port	The logical port for the settings contained in the same row. Click on the port number in order to configure the shapers.

Qn	Shows “disabled” or actual queue shaper rate – e.g. “800 Mbps”
Port	Show “disabled” or actual port shaper rate – e.g. “800Mbps”

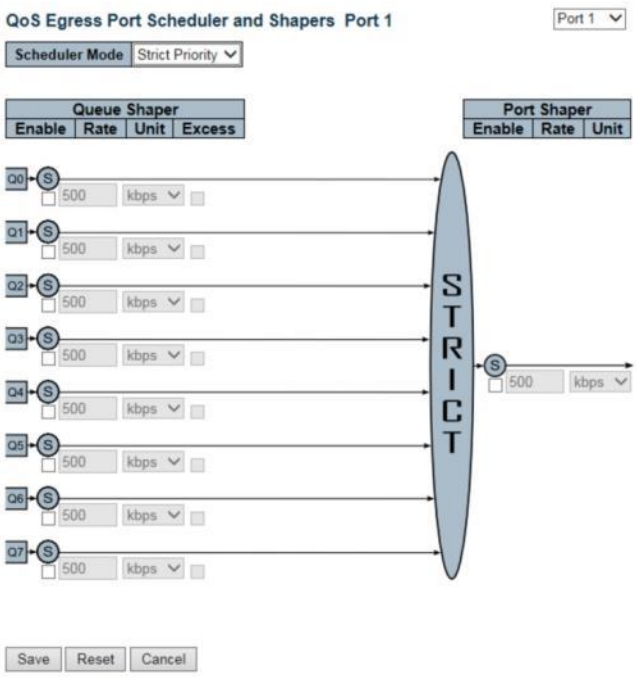
WEB Interface

A. **Click *Configuration/QoS/Port Shaper***
B. **During the overview page, Click port number into Shaping setting fo specific port**
C. **Click Save to apply the setting, Reset to restore the previous setting.**

QoS Egress Port Shapers

Port	Shapers								
	Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Port
1	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
2	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
3	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
4	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
5	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
6	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
7	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
8	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
9	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
10	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled

Figure



Figure

QoS/Port Tag Remarking

Using the QoS Egress Port Tag Remarking page to show an overview of QoS Egress Port Tag Remarking mode. Click port number to configure.

LOCATION：

▼ Configuration

▼ QoS

▪ Port Tag Remarking

PARAMETERS：

Items	Description
Port	The logical port for the settings contained in the same row. Click on the port number in order to configure tag remarking
Mode	Shows the tag remarking mode for this port. **Classified:** Use classified PCP/DEI values **Default:** Use default PCP/DEI values **Mapped:** Use mapped versions of QoS class and DP Level

WEB Interface

A. **Click *Configuration/QoS/Port Tag Remarking***
B. **During the overview page, Click port number into Tag Remarking setting fo specific port**
C. **Click Save to apply the setting, Reset to restore the previous setting.**

QoS Egress Port Tag Remarking

Port	Mode
1	Classified
2	Classified
3	Classified
4	Classified
5	Classified
6	Classified
7	Classified
8	Classified
9	Classified
10	Classified

Figure

QoS Egress Port Tag Remarking Port 1

Port 1

Tag Remarking Mode	Classified

Save Reset Cancel

Figure

QoS Egress Port Tag Remarking Port 1 Port 1

Tag Remarking Mode Mapped

(QoS class, DP level) to (PCP, DEI) Mapping

QoS class	DP level	PCP	DEI
*	*	<>	<>
0	0	1	0
0	1	1	1
1	0	0	0
1	1	0	1
2	0	2	0
2	1	2	1
3	0	3	0
3	1	3	1
4	0	4	0
4	1	4	1
5	0	5	0
5	1	5	1
6	0	6	0
6	1	6	1
7	0	7	0
7	1	7	1

Save Reset Cancel

Figure

QoS/Port DSCP

Using the QoS Port DSCP Configuration page to configure Ingress translation and classification settings and Egress re-writing of DSCP values.

LOCATION：

▼ Configuration

▼ QoS

- Port DSCP

PARAMETERS：

Items	Description
Port	The Port column shows the list of ports for which you can configure DSCP Ingress and Egress setting
Ingress	In Ingress settings you can change Ingress translation and classification settings for individual ports. There are 2 configuration parameters available in Ingress: 1. Translate 2.Classify
[Translate]	To enable the Ingress Translation click the checkbox
[Classify]	Classification for a port have 4 different values: **Disable:** No Ingress DSCP Classification **DSCP=0:** Classify if incoming (or translated if enabled) DSCP is 0 **Selected:** Classify only selected DSCP for which classification is enabled as specified in DSCP Translation window for the specific DSCP **All:** Classify all DSCP
Egress	Port Egress Rewriting can be one of following **Disable:** No Egress rewrite **Enable:** Rewrite enabled without remapping **Remap DP Unaware:** DSCP from analyzer is remapped and frame is remarked with remapped DSCP value. The remapping DSCP value is always taken from the “DSCP Translation0>Egress Remap DP0” table

	Remap DP Aware: DSCP from analyzer is remapped and frame is remarked with remapped DSCP value. Depending on the DP level of the frame, the remapped DSCP value is either taken from the “DSCP Translation->Egress Remap DP0” table from the “DSCP Translation->Egress Remap DP1” table

WEB Interface

A. **Click *Configuration/QoS/Port DSCP***
B. **Set the required Ingress and Egress parameters**
C. **Click Save to apply the setting, Reset to restore the previous setting.**

QoS Port DSCP Configuration

Port	Ingress		Egress
	Translate	Classify	Rewrite
*	☐	<>	<>
1	☐	Disable	Disable
2	☐	Disable	Disable
3	☐	Disable	Disable
4	☐	Disable	Disable
5	☐	Disable	Disable
6	☐	Disable	Disable
7	☐	Disable	Disable
8	☐	Disable	Disable
9	☐	Disable	Disable
10	☐	Disable	Disable

Save Reset

Figure

QoS/DSCP-Based QoS

Using the DSCP-Based QoS Ingress Classification page to configure the basic QoS DSCP based QoS Ingress Classificaton settings for all switches.

LOCATION：

▼ Configuration

▼ QoS

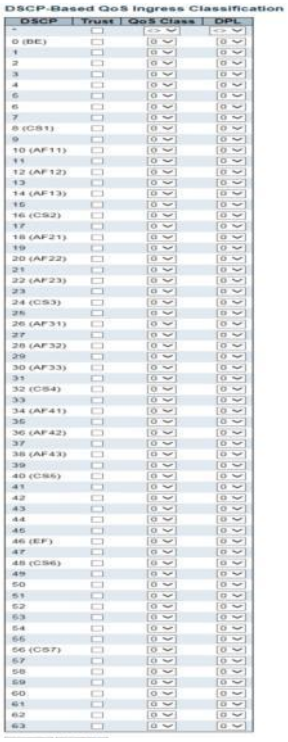
▪ DSCP-Based QoS

PARAMETERS：

Items	Description
DSCP	Maximum number of supported DSCP values are 64
Trust	Controls whether a specific DSCP value is trusted. Only frames with trusted DSCP values are mapped to a specific QoS class and Drop Precedence Level. Frames with untrusted DSCP values are treated as a non-IP frame
QoS Class	QoS class value can be any of (0-7)
DPL	Drop Precedence Level(0-1)

WEB Interface

A. **Click *Configuration/QoS/DSCP-Based QoS***
B. **Specify whether the DSCP value is trusted or not and set the corresponding QoS value and DP level for ingress frames.**
C. **Click Save to apply the setting, Reset to restore the previous setting.**



Figure

QoS/DSCP Translation

Using the DSCP Translation page to configure DSCP Translation for Ingress traffic or DSCP remapping for Egress traffic

LOCATION：

▼ Configuration

▼ QoS

▪ DSCP Translation

PARAMETERS：

Items	Description
DSCP	Maximum number of supported DSCP values

	are 64 and valid DSCP value range from 0 to 63
Ingress	Ingress side DSCP can be first translated to new DSCP before using the DSCP for QoS class and DPL map. There are 2 configuration parameters for DSCP Translation – 1. Translate, 2. Classify
Egress	There are the following configurable parameters for Egress side 1. Remap DP0: Controls the remapping for frames with DP level 0 2. Remap DP1: Controls the remapping for frames with DP level 1

WEB Interface

A. **Click *Configuration/QoS/DSCP Translation***
B. **Set the required Ingress translation and Egress remapping parameters**
C. **Click Save to apply the setting, Reset to restore the previous setting.**

DSCP Translation

DSCP	Ingress		Egress	
	Translate	Classify	Remap DP 0	Remap DP 1
*	<>		<>	<>
0 (BE)	0 (BE)		0 (BE)	0 (BE)
1	1		1	1
2	2		2	2
3	3		3	3
4	4		4	4
5	5		5	5
6	6		6	6
7	7		7	7
8 (CS1)	8 (CS1)		8 (CS1)	8 (CS1)
9	9		9	9
10 (AF11)	10 (AF11)		10 (AF11)	10 (AF11)
11	11		11	11
12 (AF12)	12 (AF12)		12 (AF12)	12 (AF12)
13	13		13	13
14 (AF13)	14 (AF13)		14 (AF13)	14 (AF13)
15	15		15	15
16 (CS2)	16 (CS2)		16 (CS2)	16 (CS2)
17	17		17	17
18 (AF21)	18 (AF21)		18 (AF21)	18 (AF21)
19	19		19	19
20 (AF22)	20 (AF22)		20 (AF22)	20 (AF22)
21	21		21	21
22 (AF23)	22 (AF23)		22 (AF23)	22 (AF23)
23	23		23	23
24 (CS3)	24 (CS3)		24 (CS3)	24 (CS3)
25	25		25	25
26 (AF31)	26 (AF31)		26 (AF31)	26 (AF31)
27	27		27	27
28 (AF32)	28 (AF32)		28 (AF32)	28 (AF32)
29	29		29	29
30 (AF33)	30 (AF33)		30 (AF33)	30 (AF33)
31	31		31	31
32 (CS4)	32 (CS4)		32 (CS4)	32 (CS4)
33	33		33	33
34 (AF41)	34 (AF41)		34 (AF41)	34 (AF41)
35	35		35	35
36 (AF42)	36 (AF42)		36 (AF42)	36 (AF42)
37	37		37	37
38 (AF43)	38 (AF43)		38 (AF43)	38 (AF43)
39	39		39	39
40 (CS5)	40 (CS5)		40 (CS5)	40 (CS5)
41	41		41	41
42	42		42	42
43	43		43	43
44	44		44	44
45	45		45	45
46 (EF)	46 (EF)		46 (EF)	46 (EF)
47	47		47	47
48 (CS6)	48 (CS6)		48 (CS6)	48 (CS6)
49	49		49	49
50	50		50	50
51	51		51	51
52	52		52	52
53	53		53	53
54	54		54	54
55	55		55	55
56 (CS7)	56 (CS7)		56 (CS7)	56 (CS7)
57	57		57	57
58	58		58	58
59	59		59	59
60	60		60	60
61	61		61	61
62	62		62	62
63	63		63	63

Save Reset

Figure

QoS/DSCP Classification

Using DSCP Classification page to map DSCP values to a QoS class and drop precedence level.

LOCATION：

▼ Configuration

▼ QoS

▪ DSCP Classification

PARAMETERS：

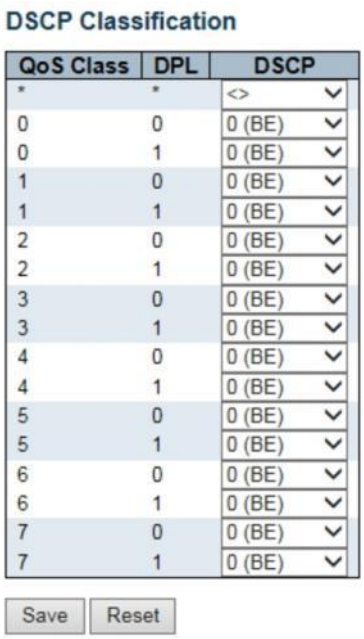
Items	Description
QoS Class	Actual QoS class
DPL	Acutal Drop Precedence Level
DSCP	Select the classified DSCP value(0-63)

WEB Interface

A. Click *Configuration/QoS/DSCP Classification*

B. Map DSCP values to a corresponding QoS class and DP level

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



Figure

QoS/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：

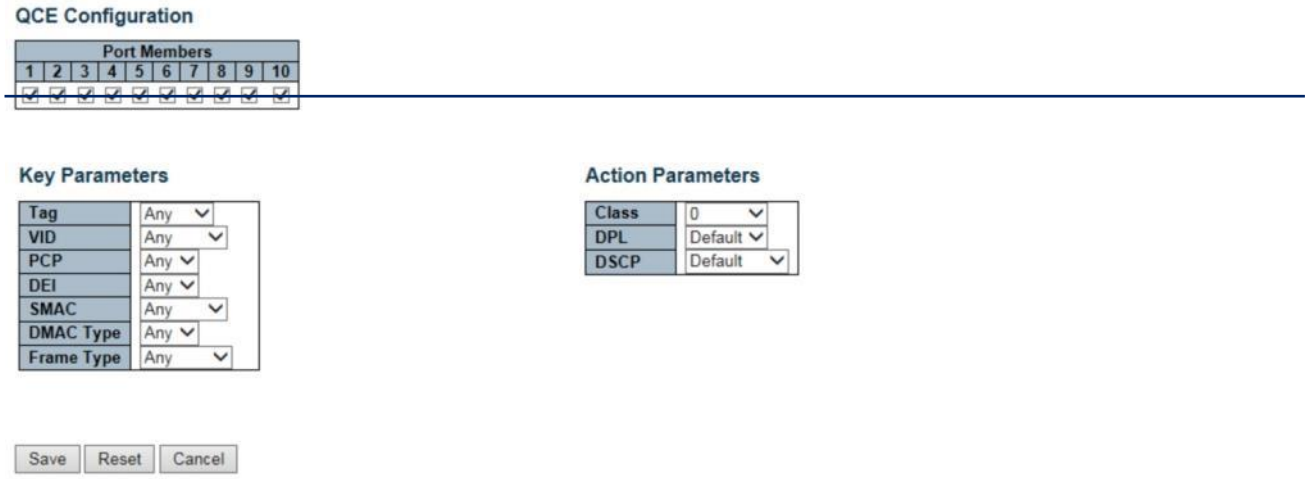
Items	Description
QCE#	Indicate the index of QCE.
Port	Indicates the list of ports configured with the QCE.
Frame Type	Indicates the type of frame to look for incomming frames. Possible frame types are： Any:：The QCE will match all frame type. Ethernet:：Only Ethernet frames (with Ether Type 0x600-0xFFFF)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

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.**



Figure

QoS/Strom 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：

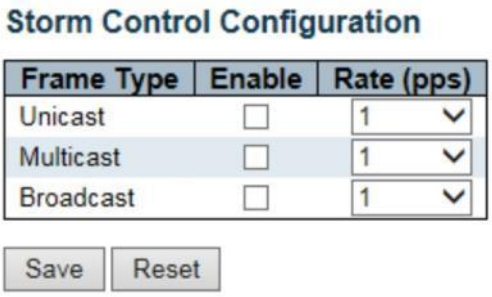
Items	Description
Frame Type	The settings in a particular row apply to the frame type listed here: Unicast, Multicast or Broadcast.
Enable	Enable or disable the storm control status for the given frame type.
Rate	The rate unit is packets per second (pps). Valid values are：1, 2, 4, 8, 16, 32, 64, 128,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

WEB Interface

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.**



Figure

Mirroring

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

LOCATION：

▼ Configuration

▪ Mirroring

PARAMETERS：

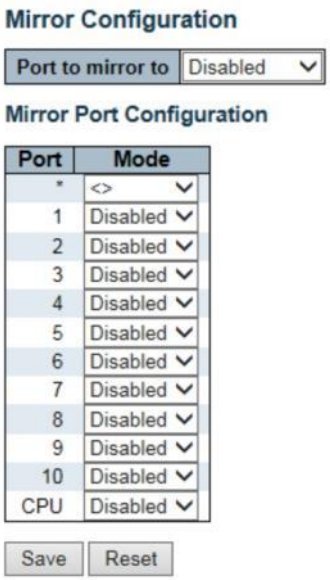
Items	Description
Port	The logical port for the settings contained in the same row.
Mode	Select mirror mode. **Rx only**：Frames received on this port are mirrored on the mirror port. Frames transmitted are not mirrored. **Tx only**：Frames transmitted on this port are mirrored on the mirror port. Frames 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.

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.



Figure

UPnP

Using The UPnP Configuration page to setup UPnP. Universal Plug and Play is a set of protocols that allows devices to deploy easily.

LOCATION：

▼ Configuration

▪ UPnP

PARAMETERS：

Items	Description
Mode	Indicates the UPnP operation mode. Possible modes are: **Enabled:** Enable UPnP mode operation **Disabled:** Disable UPnP mode operation When the mode is enabled, two ACEs are added automatically to trap UPNP related packets to CPU. The ACEs are automatically remove when the mode is disabled.
TTL	The TTL value is used by UPNP to send SSDP advertisement messages. Valid Values are in the range 1 to 255.
Advertising Duration	The duration, carried in SSDP packets, is used to inform a control point or control points how often it or they should receive and SSDP advertisement message from this switch. If a control point does not receive any message within the duration, it will think that the switch no longer exists. Due to the unreliable nature of UDP, in the standard it is recommended that such refreshing of advertisements to be done at less than one-half of the advertising duration. In the implementation, the switch sends ssdp messages periodically at the interval one-half of the advertising duration minus 30 seconds. Valid values are in the range 100 to 86400.

WEB Interface

A. **Click *Configuration/UPnP***
B. **Set required UPnP related parameters**
C. **Click Save to apply the setting, Reset to restore the previous setting.**

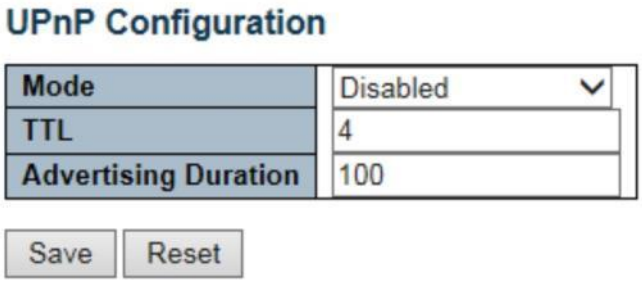


Figure.

sFlow

sFlow is an industry standard technology for monitoring switched networks through random sampling of packets on switch ports and time-based sampling of port counts. The sampled packets and counters are sent as sFlow UDP datagrams to a central network traffic monitoring server.The central server is called an sFlow receiver or sFlow collector

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

LOCATION：

▼ Configuration

▪ sFlow

PARAMETERS：

Items	Description
Receiver Configuration	

Owner	Basically,sFlow can be configured in two ways: Through local management using the Web or CLI interface or through SNMP. This read-only field shows the owner of the current sFlow configuration and assumes values as follows: ● If sFlow is currently unconfigured/unclaimed, Owner contains <none> ● If sFlow is currently configured through Web or CLI, Owner contains <Configured through local management> ● If sFlow is currently configured through SNMP, Owner contains a string identifying the sFlow receiver. If sFlow is configured through SNMP, all controls –except for the Release-button- are disabled to avoid inadvertent reconfiguration.
IP Address/ Hostname	The IP address or hostname of the sFlow receiver. Both IPv4 and IPv6 addresses are supported
UDP Port	The UDP port on which the sFlow receiver listens to sFlow datagrams. If set to 0 (zero), the default port (6343) is used.
Timeout	The number of seconds remaining before sampling stops and the current sFlow owner is released. While active, the current time left can be updated with a clock on the Refresh-button. If locally managed, the timeout can be changed on the fly without affecting any other settings.
Max. Datagram Size	The maximum number of data bytes that can be sent in a single sample datagram. This should be set to a value that avoids fragmentation of the sFlow datagrams.Valid range is 200 to 1468 bytes with default being 1400 bytes

Port Configuration	
Port	The port number for which the configuration below applies
Flow Sampler Enabled	Enables/disables flow sampling on this port
Flow Sampler Sampling Rate	Thestatistical sampling rate for packet sampling. Set to N to sample on average 1/Nth of the packets transmitted/received on the port. Not all sampling rates are achievable. If an unsupported sampling rate is requested, the switch will automatically adjust it to the closest achievable. This will be reported back in this field.
Flow Sampler Max. Header	The maximum number of bytes that should be copied from a sampled packet to the sFlow datagram. Valid range is 14 to 200 bytes with default being 128 bytes. If the maximum datagram size does not take into account the maximum header size, samples may be dropped.
Coounter Poller Enabled	Enables/disables counter polling on this port.
Counter Poller Interval	With counter polling enabled, this specifies the interval – in seconds – between counter poller samples.

WEB Interface

A. **Click *Configuration/sFlow***
B. **Set required sFlow related parameters**
C. **Click Save to apply the setting, Reset to restore the previous setting.**

sFlow Configuration

Refresh

Receiver Configuration

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

Port Configuration

Port	Flow Sampler			Counter Poller	
	Enabled	Sampling Rate	Max. Header	Enabled	Interval
*	☐	0	128	☐	0
1	☐	0	128	☐	0
2	☐	0	128	☐	0
3	☐	0	128	☐	0
4	☐	0	128	☐	0
5	☐	0	128	☐	0
6	☐	0	128	☐	0
7	☐	0	128	☐	0
8	☐	0	128	☐	0
9	☐	0	128	☐	0
10	☐	0	128	☐	0

Save Reset

Figure

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

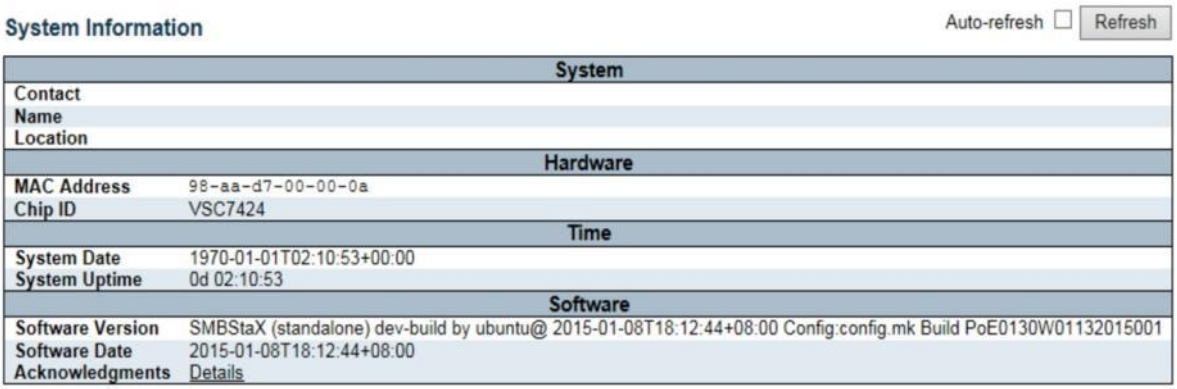
	server running on the switch, if any.
System Uptime	The period of time the device has been operational.
Software Version	The software version of this switch
Software Date	The date when the switch software was produced

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**



Figure

System/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

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

- **Default the"Auto-refresh" checkbox is checked to update page information automatically**

Figure

System/Log

Using the System Log Information page to display event messages

LOCATION：

▼ Monitor

▼ System

▪ Log

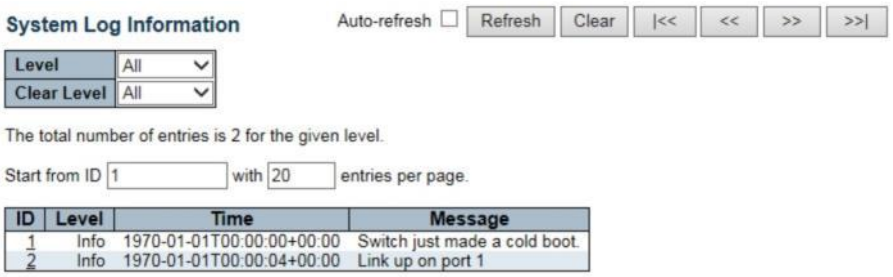
PARAMETERS：

Items	Description
ID	Event log ID(>=1)
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.

WEB Interface

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

System/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

A. Click *Monitor/System/Detailed Log.*

B. Specify the Detailed system log.

Figure

Ports/State

The Port State page provides an overview of all port's current state, you can click port icon to get specific port's detailed statistics

LOCATION :

▼ Monitor

▼ Ports

▪ State

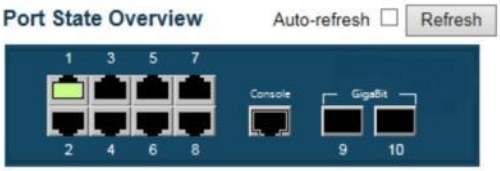
PARAMETERS :

Items	Description

Port State	The port states are illustrated as follows： 
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

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



Figure

Ports/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

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

B. Check "Auto-refresh" to update the switch's port state automaticallyand 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	2144	7329	326201	1112566	0	0	0	0	303
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

Figure

Ports/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

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	2189	0	0	0	0	0	0	0	0	0	0	0	0	0	0	7399
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

Figure

Ports/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

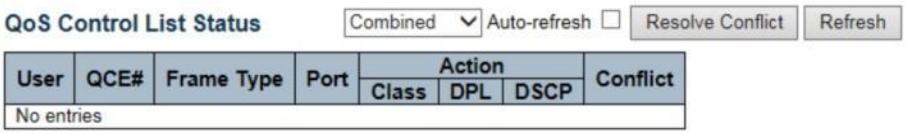
PARAMETERS：

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

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.**



Figure

Ports/Detailed Statistics

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 Transmit Size Counters	The number of received and transmitted (good and bad) packets split into categories based on their respective frame sizes.
Receive and Transmit Queue Counters	The number of received and transmitted packets per input and output queue.
Receive Error Counters	
Rx Drops	The number of frames dropped due to lack of receive buffers or egress congestion.
Rx CRC /Alignment	The number of frames received with CRC or alignment errors.
Rx Undersize	The number of short[1] frames received with valid CRC.
Rx Oversize	The number of long[2] frames received with valid CRC.
Rx Fragments	The number of short[1] frames received with invalid CRC.
Rx Jabber	The number of long [2] frames received with invalid CRC.
Rx Filtered	The number of received frames filtered by the forwarding process.

[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

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	623	Tx Packets	363
Rx Octets	81756	Tx Octets	205444
Rx Unicast	356	Tx Unicast	279
Rx Multicast	164	Tx Multicast	82
Rx Broadcast	103	Tx Broadcast	2
Rx Pause	0	Tx Pause	0
Receive Size Counters		**Transmit Size Counters**	
Rx 64 Bytes	275	Tx 64 Bytes	4
Rx 65-127 Bytes	245	Tx 65-127 Bytes	95
Rx 128-255 Bytes	7	Tx 128-255 Bytes	17
Rx 256-511 Bytes	96	Tx 256-511 Bytes	139
Rx 512-1023 Bytes	0	Tx 512-1023 Bytes	15
Rx 1024-1526 Bytes	0	Tx 1024-1526 Bytes	93
Rx 1527- Bytes	0	Tx 1527- Bytes	0
Receive Queue Counters		**Transmit Queue Counters**	
Rx Q0	623	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	363
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	201		

Figure

Security/Access Management Statistics

Using Access Management Statistics page to monitor the management traffic through 5 interfaces, included HTTP, HTTPS, SNMP, TELNET and SSH.

LOCATION：

▼ Monitor

▼ Security

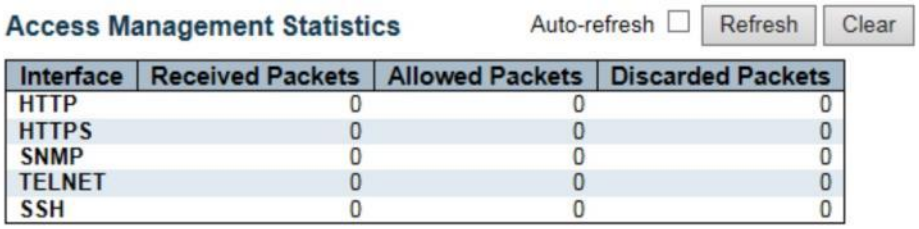
- ACL Status

PARAMETERS：

Items	Description
Interface	The interface type through which the remote host can access the switch
Received Packets	Number of received packets from the interface when access management mode is enabled.
Allowed Packets	Number of allowed packets from the interface when access management mode is enabled.
Discarded Packets	Number of discard packets from the interface when access management mode is enabled.

WEB Interface

A. **Click *Monitor/Security/Access Management Statistics***
B. **Check the "Auto-refresh" to refresh the page periodly.**



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

Figure

Security/Network/Port Security/Switch

The Page shows the Port Security status. Port Security is a module with no direct configuration. Confugration comes indirectly from other modules – the user modules. When a user module has enabled port security on a port, the port is set-up for software-based learning. In this mode, frames from unknown MAC addresses are passed on the port security module, which in turn asks all user modules whether to allow this new MAC address to forward or block it. For a MAC address to be set in the forwarding state, all enabled user modules must unanimously agree on allowing the MAC address to forward. If only one chooses to block it, it will be blocked until that user module decides otherwise.

The status page is divided into two sections – one with legend of user modules and one with the actual port status.

LOCATION：

▼ Monitor

▼ Security

▼ Network

▼ Port Security

▪ Switch

PARAMETERS：

Items	Description
User Module Legend	
User Module	The full name of a module that may request
Name	Port Security services
Abbr	A one-letter abbrevation of the user module. This is used in the Users column in the port

	status table
Port Status	
Port	The port number of which the status applies. Click the port number to see the status for this paritcular port.
Users	Each of the user modules has a column that shows whether that module has enabled Port Security or not. A”-“ means that the corresponding user module is not enabled, whereas a letter indicates that the user module abbreviated by that letter has enabled port secuirty.
State	Shows the current state of the port. It can take one of four values: Disabled: No user modules are currently using the Port Security Service. Ready: The Port Security service is in use by at least one user module, and is awaiting frames from unknow MAC addresses to arrive. Limit Reached: The Port Security service is enabled by at least the Limit Control user module, and that module has indicated that the limit is reached an no more MAC addresses should be taken in. Shutdown: The Port Security service is enabled by at least the Limit Control user module, and that module has indicated that the limit is exceed. No MAC addresses can be learned on that port until it is administratively re-open on the Limit Control configuration Web-page.
Mac Count (Current, Limit)	The two columns in indicate the number of currently learned MAC addresses(forwarding as well as blocked) and the maximum number of MAC addresses that can be learned on the port, respectively.

	If no user modules are enabled on the port, the Current column will show a dash (-). IF the Limit Control user module is not enabled on the port, the Limit column will show a dash (-).

WEB Interface

A. **Click *Monitor/Security/Network/Port Security/Switch to display information, included switch-level settings for Port Security module.***
B. **Check the "Auto-refresh" to refresh the page periodly.**

Port Security Switch Status Auto-refresh ☐ Refresh

User Module Legend

User Module Name	Abbr
Limit Control	L
802.1X	8
DHCP Snooping	D
Voice VLAN	V

Port Status

Port	Users	State	MAC Count	
			Current	Limit
1	----	Disabled	-	-
2	----	Disabled	-	-
3	----	Disabled	-	-
4	----	Disabled	-	-
5	----	Disabled	-	-
6	----	Disabled	-	-
7	----	Disabled	-	-
8	----	Disabled	-	-
9	----	Disabled	-	-
10	----	Disabled	-	-

Figure

Security/Network/Port Security/Port

Using Port Security Port Status page to show the entries which is authorized by port security, included MAC Address, VLAN ID, Time of Addition and Aging time/ Hold state.

LOCATION：

▼ Monitor

▼ Security

▼ Network

▼ Port Security

▪ Port

PARAMETERS：

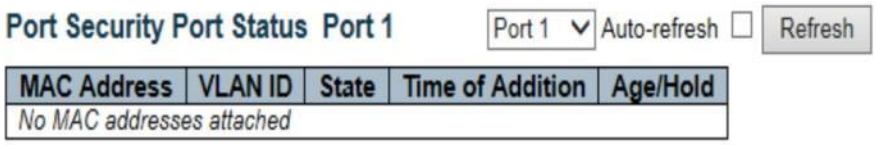
Items	Description
MAC Address & VLAN ID	The MAC Address and VLAN ID that is seen on this port. If no MAC addresses are learned, a single row stating “No MAC addresses attached” is displayed.
State	Indicates whether the corresponding MAC address is blocked or forwarding. In the blocked state, it will not be allowed to transmit or receive traffic.
Time of Addition	Shows the data and time when this MAC address was first seen on the port
Age/Hold	If at least one user module has decided to block this MAC address, it will stay in the blocked state until the hold time(measured in seconds) expires. If all user modules have decided to allow this MAC address to forward, and aging is enabled, the Port Security module will periodically check that this MAC address still forwards traffic. If the age period(measured in seconds) expires and no frames have been seen, the Mac address will be removed from the MAC table.Otherwise a new age period will begin. If aging is disabled or a user module has decided to hold the MAC address idenfinitely,

	a dash (-) will be shown.

WEB Interface

A. Click *Monitor/Security/Network/Port Security/Port to display information about MAC address learning.*

B. Check the "Auto-refresh" to refresh the page periodly.



Figure

Security/Network/NAS/Switch

Using Network Access Server Switch Status to show the port status for authentication services, included 802.1X security state, last Source address , last ID, QoS Class and Port VLAN ID.

LOCATION：

▼ Monitor

▼ Security

▼ Network

▼ NAS

▪ Switch

PARAMETERS：

Items	Description
Port	The switch port number. Click to navigate to detailed NAS statistics for this port.

Admin State	The port's current administrative state. Refer to NAS Admin State for a description of possible values
Port State	The current state of the port. Refer to NAS Port State for a description of the individual states.
Last Source	The source MAC address carried in the most recently received EAPOL frame for EAPOL-based authentication, and the most recently received frame from a new client for MAC-based authentication
Last ID	The user name (supplicant identity) carried in the most recently received Response Identity EAPOL frame for EAPOL-based authentication, and the source MAC address from the most recently received frame from a new client for MAC-based authentication.
QoS class	Qos Class assigned to the port by the RADIUS server if enabled.
Port VLAN ID	The VLAN ID that NAS has put the port in. The field is blank. If the Port VLAN ID is not overridden by NAS. If the VLAN ID is assigned by the RADIUS server, "(RADIUS-assigned)" is appended to the VLAN ID. Read more about RADIUS-assigned VLANs here. If the port is moved to the Guest VLAN,"(Guest)" is appended to the VLAN ID.

WEB Interface

A. **Click *Monitor/Security/Network/NAS/Switch to display information about Port status for authentication services.***
B. **Check the "Auto-refresh" to refresh the page periodly.**

Network Access Server Switch Status Auto-refresh ☐ Refresh

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

Figure

Security/Network/NAS/Port

Using the NAS Statistics Port page to show the authentication statistics for specific port.

LOCATION：

▼ Monitor

▼ Security

▼ Network

▼ NAS

▪ Port

PARAMETERS：

Items	Description
Port State	
Admin State	The port's current administrative state. Refer to NAS Admin State for a description of possible values
Port State	The current state of the port. Refer to NAS Port State for a description of the individual

	states.
QoS Class	The QoS class assigned by the RADIUS server. The field is blank if no Qos class is assigned.
Port VLAN ID	The VLAN ID that NAS has put the port in. The field is blank. If the Port VLAN ID is not overridden by NAS. If the VLAN ID is assigned by the RADIUS server, “(RADIUS-assigned)” is appended to the VLAN ID. Read more about RADIUS-assigned VLANs here. If the port is moved to the Guest VLAN,”(Guest)” is appended to the VLAN ID.
Port Counters	
EAPOL Counters	These supplicant frame counters are available for the following adminstrative states: ● Force Authorized ● Force Unauthorized ● Port-Based 802.1x ● Single 802.1X ● Multi 802.1X

EAPOL Counters			
Direction	**Name**	**IEEE Name**	**Description**
Rx	**Total**	dot1xAuthEapolFramesRx	The number of valid EAPOL frames of any type that have been received by the switch.
Rx	**Response ID**	dot1xAuthEapolRespIdFramesRx	The number of valid EAPOL Response Identity frames that have been received by the switch.
Rx	**Responses**	dot1xAuthEapolRespFramesRx	The number of valid EAPOL response frames (other than Response Identity frames) that have been received by the switch.
Rx	**Start**	dot1xAuthEapolStartFramesRx	The number of EAPOL Start frames that have been received by the switch.
Rx	**Logoff**	dot1xAuthEapolLogoffFramesRx	The number of valid EAPOL Logoff frames that have been received by the switch.
Rx	**Invalid Type**	dot1xAuthInvalidEapolFramesRx	The number of EAPOL frames that have been received by the switch in which the frame type is not recognized.
Rx	**Invalid Length**	dot1xAuthEapLengthErrorFramesRx	The number of EAPOL frames that have been received by the switch in which the Packet Body Length field is invalid.
Tx	**Total**	dot1xAuthEapolFramesTx	The number of EAPOL frames of any type that have been transmitted by the switch.
Tx	**Request ID**	dot1xAuthEapolReqIdFramesTx	The number of EAPOL Request Identity frames that have been transmitted by the switch.
Tx	**Requests**	dot1xAuthEapolReqFramesTx	The number of valid EAPOL Request frames (other than Request Identity frames) that have been transmitted by the switch.

Backend Server Counters	These backend (RADIUS) frame counters are available for the following administrative

states:

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

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

Last Supplicant/ Client Info

Information about the last supplicant/client that attempted to authenticate. This information is available for the following adminstrative states:

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

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

Select Counters

Selected Counters

The Selected Counters table is visible when the port is in one of the following adminstrative states:

- Multi 802.1X
- MAC-based Auth.

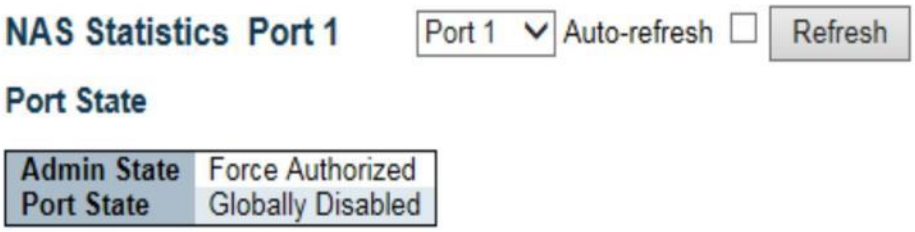
The table is identical to and is placed next to the Port Counters table, and will be empty if no MAC address is currently selected. To

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

	well as unsuccessful).

WEB Interface

A. **Click *Monitor/Security/Network/NAS/Switch to display information about Port status for authentication services.***
B. **Check the "Auto-refresh" to refresh the page periodly.**



Figure

Security/Network/ACL Status

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	Indicates the ingress port of the ACE.

Port	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.

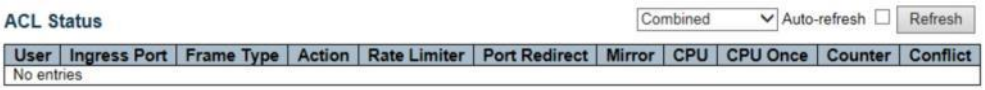
Action	Indicates the forwarding action of the ACE. Permit：Frames matching the ACE may be forwarded and learned. Deny：Frames matching the ACE are dropped.
Rate Limiter	Indicates the rate limiter number of the ACE. The allowed range is 1 to 16. When Disabled is displayed, the rate limiter operation is 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

A. Click *Monitor/Security/Network/ACL Status*

B. Select a software module from the scroll-down list.



Figure

Security/Network/DHCP/Snooping Statistics

Using the DHCP Snooping Port Statistics page to show statistics for various types of DHCP protocol packets

LOCATION :

▼ Monitor

▼ Security

▼ Network

▼ DHCP

- Snooping Statistics

PARAMETERS :

Items	Description
Rx and Tx Discover	The number of discover (option 53 with value 1) packets received and transmitted.
Rx and Tx Offer	The number of offer (option 53 with value 2) pakcets received and transmitted
Rx and Tx Request	The number of request (option 53 with value 3) packets received and transmitted.
Rx and Tx Decliine	The number of decline (option 53 with value 4) packets received and transmitted
Rx and Tx ACK	The number of ACK (option 53 with value 5) packets received and transmitted
Rx and TX NAK	The number of NAK (option 53 with value 6) packets received and transmitted
Rx and Tx Release	The number of Release (option 53 with value 7) packets received and transmitted
Rx and Tx Inform	The number of Inform (option 53 with value 8) packets received and transmitted
Rx and Tx Query	The number of Query (option 53 with value 10) packets received and transmitted
Rx and Tx Unassigned	The number of unassigned (option 53 with value 11) packets received and transmitted
Rx and Tx Unknown	The number of unknown (option 53 with value 12) packets received and transmitted
Rx and Tx Active	The number of Active (option 53 with value 13) packets received and transmitted

WEB Interface

A. Click *Monitor/Security/Network/DHCP/Snooping Statistics*

B. Select Port number from the scroll-down list.

DHCP Snooping Port Statistics Port 1 Port 1 Auto-refresh Refresh Clear

Receive Packets		Transmit Packets	
Rx Discover	0	Tx Discover	0
Rx Offer	0	Tx Offer	0
Rx Request	0	Tx Request	0
Rx Decline	0	Tx Decline	0
Rx ACK	0	Tx ACK	0
Rx NAK	0	Tx NAK	0
Rx Release	0	Tx Release	0
Rx Inform	0	Tx Inform	0
Rx Lease Query	0	Tx Lease Query	0
Rx Lease Unassigned	0	Tx Lease Unassigned	0
Rx Lease Unknown	0	Tx Lease Unknown	0
Rx Lease Active	0	Tx Lease Active	0

Figure

Security/Network/DHCP/Relay Statistics

Using the DHCP Relay Statistics page to show statistics for the DHCP Relay service supportd by this switch and DHCP Relay clients

LOCATION：

▼ Monitor

▼ Security

▼ Network

▼ DHCP

▪ Relay Statistics

PARAMETERS：

Items	Description
Server Statistics	
Transmit to Server	The number of packets that are relayed from client to server
Transmit Error	The number of packets that resulted in

	errors while being sent to clients
Receive from Server	The number of packets received from server
Receive Missing Agent Option	The number of packets received without agent information options
Receive Missing Circuit ID	The number of packets received with the Circuit ID option missing.
Receive Missing Remote ID	The number of packets received with the Remote ID option missing
Receive Bad Circuit ID	The number of packets whose Circuit ID option did not match known circuit ID
Receive Bad Remote ID	The number of packets whose Remote ID option did not match known Remote ID
Client Statistics	
Transmit to Client	The number of relayed packets from server to client
Transmit Error	The number of packet that resulted in error while being sent to servers
Receive from Client	The number of received packets from server
Receive Agent Option	The number of received packets with relay agent information option
Replace Agent Option	The number of packets which were replaced with relay agent information option.
Keep Agent Option	The number of packets whose relay agent information was retained.
Drop Agent Option	The nubmer of packets that were dropped which werer received with relay agent information.

WEB Interface

A. **Click *Monitor/Security/Network/DHCP/Relay Statistics***
B. **Check "Auto-refresh" to auto-refresh this page.**

DHCP Relay Statistics

Auto-refresh ☐ Refresh Clear

Server Statistics

Transmit to Server	Transmit Error	Receive from Server	Receive Missing Agent Option	Receive Missing Circuit ID	Receive Missing Remote ID	Receive Bad Circuit ID	Receive Bad Remote ID
0	0	0	0	0	0	0	0

Client Statistics

Transmit to Client	Transmit Error	Receive from Client	Receive Agent Option	Replace Agent Option	Keep Agent Option	Drop Agent Option
0	0	0	0	0	0	0

Figure.

Security/Network/ARP Inspection

Entries in the Dynamic ARP Inspection Table are shown on this page. The Dynamic ARP Inspection Table contains up to 1024 entries, and is sorted first by port, then by VLAN ID, then by MAC address ,and then by IP address

LOCATION：

▼ Monitor

▼ Security

▼ Network

▪ ARP Inspection

PARAMETERS：

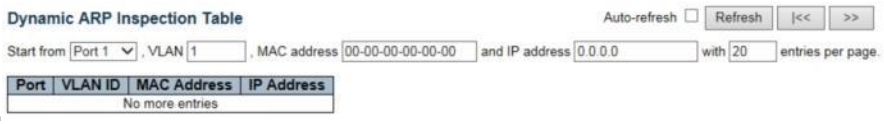
Items	Description
Port	Switch Port Number for which the entries are displayed
VLAN ID	VLAN ID in which the ARP traffic is permitted
MAC Address	User MAC address of the entry
IP Address	User IP address of the entry

WEB Interface

A. Click *Monitor/Security/Network/ARP Inspection*

B. Change the entries number to display more entries

C. Check “Auto-refresh” to auto-refresh this page.



Figure

Security/Network/IP Soruce Guard

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

LOCATION：

▼ Monitor

▼ Security

▼ Network

▪ IP Source Guard

PARAMETERS：

Items	Description
Port	Switch Port Number for which the entries are displayed
VLAN ID	VLAN ID in which the ARP traffic is permitted
MAC Address	Source MAC address
IP Address	User IP address of the entry

WEB Interface

A. Click *Monitor/Security/Network/IP Source Guard*
B. Change the entries number to display more entries
C. Check "Auto-refresh" to auto-refresh this page.

Figure

Security/AAA/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, IPcommunication 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

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 Accounting Server Status Overview

#	IP Address	Status
1	0.0.0.0:1813	Disabled
2	0.0.0.0:1813	Disabled
3	0.0.0.0:1813	Disabled
4	0.0.0.0:1813	Disabled
5	0.0.0.0:1813	Disabled

Figure

Security/AAA/RADIUS Details

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

LOCATION：

▼ Monitor

▼ Security

▼ AAA

- RADIUS Details

PARAMETERS：

Items	Description
Receive packets	The counters of Receive Packets, including 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

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

RADIUS Authentication Statistics for Server #1

Server #1 Auto-refresh Refresh Clear

Receive Packets		Transmit Packets	
Access Accepts	0	Access Requests	0
Access Rejects	0	Access Retransmissions	0
Access Challenges	0	Pending Requests	0
Malformed Access Responses	0	Timeouts	0
Bad Authenticators	0		
Unknown Types	0		
Packets Dropped	0		
Other Info			
IP Address			0.0.0.0:1812
State			Disabled
Round-Trip Time			0 ms

RADIUS Accounting Statistics for Server #1

Receive Packets		Transmit Packets	
Responses	0	Requests	0
Malformed Responses	0	Retransmissions	0
Bad Authenticators	0	Pending Requests	0
Unknown Types	0	Timeouts	0
Packets Dropped	0		
Other Info			
IP Address			0.0.0.0:1813
State			Disabled
Round-Trip Time			0 ms

Figure

Security/Switch/RMON

This page provide an overview of RMON Statistics entries.

LOCATION :

▼ Monitor

▼ Security

▼ Switch

▼ RMON

▪ Statistics

PARAMETERS：

Items	Description
ID	Indicates the index of Statistics entry
Data Source(ifIndex)	The port ID which wants to be monitored
Drop	The total number of events in which packets were dropped by the probe due to lack of resources
Octets	The total number of octets of data(including those in bad packets) received on the network
Pks	The total number of packets(including bad packets, broadcast packets, and multicast packets) received.
Broad-cast	The total number of good packets received that were directed to the broadcast address.
Multi-cast	The total number of good packets received that were directed to a multicast address
CRC Errors	The total number of packets received that had a length(excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had either a bad frame check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
Under-size	The total number of packets received that were less than 64 octets
Over-size	The total number of packets received that were longer than 1518 octets
Frag.	The number of frames which size is less than 64 octets received with invalid CRC
Jabb.	The number of frames which size is larger than 64 octets received with invalid CRC
Coll.	The best estimate of the total number of collisions on this Ethernet segment

64	The total number of packet(including bad packets) received that were 64 octets in length.
64~127	The total number of packet(including bad packets) received that were between 65 to 127 octets in length.
128~255	The total number of packet(including bad packets) received that were between 128 to 255 octets in length.
256~511	The total number of packet(including bad packets) received that were between 256 to 511 octets in length.
512~1023	The total number of packet(including bad packets) received that were between 512 to 1023 octets in length.
1024~1588	The total number of packet(including bad packets) received that were between 1024 to 1588 octets in length.

WEB Interface

A. Click *Monitor/Security/Switch/RMON/Statistics*

B. It will show up the Statistics

C. Check "Auto-refresh" to auto-refresh the page.

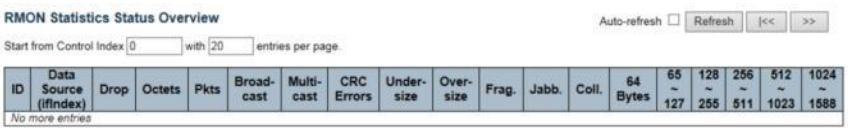


Figure.

Security/Switch/RMON/History

This page provides an overview of RMON History entries.

LOCATION：

▼ Monitor

▼ Security

▼ Switch

▼ RMON

▪ History

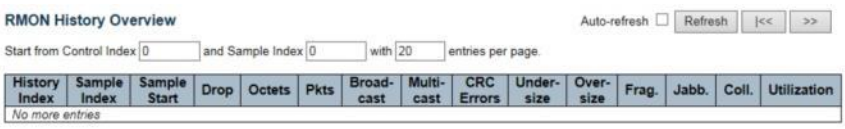
PARAMETERS：

Items	Description
History Index	Indicates the index of History control entry
Sample Index	Indicates the index of the data entry associated with the control entry
Sample Start	The value of sysUPTime at the start of the interval over which this sample was measured
Drop	The total number of events in which packets were dropped by the probe due to lack of resources
Octets	The total number of octets of data(including those in bad packets) received on the network
Pks	The total number of packets(including bad packets, broadcast packets, and multicast packets) received.
Broad-cast	The total number of good packets received that were directed to the broadcast address.
Multi-cast	The total number of good packets received that were directed to a multicast address
CRC Errors	The total number of packets received that had a

	length(excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had either a bad frame check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
Under-size	The total number of packets received that were less than 64 octets
Over-size	The total number of packets received that were longer than 1518 octets
Frag.	The number of frames which size is less than 64 octets received with invalid CRC
Jabb.	The number of frames which size is larger than 64 octets received with invalid CRC
Coll.	The best estimate of the total number of collisions on this Ethernet segment
Utilization	The best estimate of the mean physical layer network utilization on this interface during this sampling interval, in hundredths of a percent.

WEB Interface

A. **Click *Monitor/Security/Switch/RMON/History***
B. **It will show up the Statistics of History**
C. **Check "Auto-refresh" to auto-refresh the page.**



Figure

Security/Switch/RMON/Alarm

This page provides an overview of RMON Alarm entries.

LOCATION：

▼ Monitor

▼ Security

▼ Switch

▼ RMON

▪ Alarm

PARAMETERS：

Items	Description
ID	Indicates the index of Alarm control entry
Interval	Indicates the interval in seconds for sampling and comparing the rising and falling threshold
Variable	Indicates the partidular variable to be sampled
Sample Type	The method of sampling the selected variable and calculating the value to be compared against the thresholds
Value	The value of the statistic during the last sampling period
Satartup Alarm	The alarm that may be sent when this entry is first set to valid
Rising Threshold	Rising threshold value

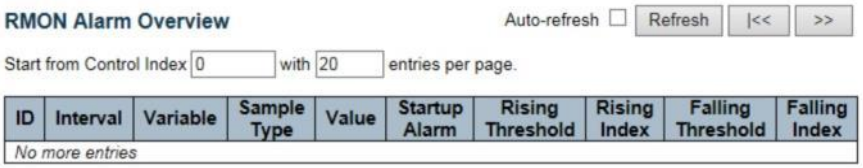
Rising Index	Rising event index
Falling Threshold	Falling threshold value
Falling Index	Falling event index

WEB Interface

A. Click *Monitor/Security/Switch/RMON/Alarm*

B. It will show up the Statistics of Alarm

C. Check "Auto-refresh" to auto-refresh the page.



Figure

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 System Status Auto-refresh ☐ Refresh

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

Figure

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.
Partner Prio	The partner's port priority
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	Partner Prio
1	No	-	-	-	-	-
2	No	-	-	-	-	-
3	No	-	-	-	-	-
4	No	-	-	-	-	-
5	No	-	-	-	-	-
6	No	-	-	-	-	-
7	No	-	-	-	-	-
8	No	-	-	-	-	-
9	No	-	-	-	-	-
10	No	-	-	-	-	-

Figure

LACP/Port Statistics

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 frames have been discarded at each 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 LACP Port Statistics for local ports :

A. Click *Monitor/LACP/Port Statistics*

LACP Statistics Auto-refresh ☐ Refresh Clear

Port	LACP Received	LACP Transmitted	Discarded	
			Unknown	Illegal
1	0	0	0	0
2	0	0	0	0
3	0	0	0	0
4	0	0	0	0
5	0	0	0	0
6	0	0	0	0
7	0	0	0	0
8	0	0	0	0
9	0	0	0	0
10	0	0	0	0

Figure

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.*

Loop Protection Status Auto-refresh ☐ Refresh

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

Figure

Spanning Tree/Bridge Status

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

WEB Interface

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

STP Bridges

Auto-refresh ☐ Refresh

MSTI	Bridge ID	Root			Topology Flag	Topology Change Last
		ID	Port	Cost		
CIST	32768.98-AA-D7-00-00-0A	32768.98-AA-D7-00-00-0A	-	0	Steady	-

Figure

Spanning Tree/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 Status Auto-refresh ☐ Refresh

Port	CIST Role	CIST State	Uptime
1	DesignatedPort	Forwarding	0d 05:25:52
2	Disabled	Discarding	-
3	Disabled	Discarding	-
4	Disabled	Discarding	-
5	Disabled	Discarding	-
6	Disabled	Discarding	-
7	Disabled	Discarding	-
8	Disabled	Discarding	-
9	Disabled	Discarding	-
10	Disabled	Discarding	-

Figure

Spanning Tree/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

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	9888	0	0	0	0	0	0	0	0	0

Figure

MVR/Statistics

Using the MVR Group Information page to display statistics for IGMP protocol message used by MVR

LOCATION :

▼ Monitor

▼ MVR

▪ Statistics

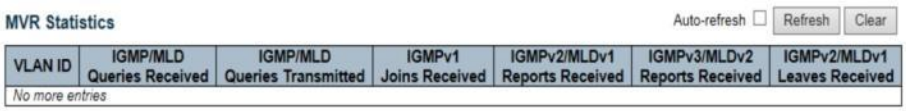
PARAMETERS :

Items	Description
VLAN ID	The Multicast VLAN ID
IGMP/MLD Queries Received	The number of Received Queries for IGMP and MLD, repectively.
IGMP/MLD Queries Transmitted	The number of Transmitted Queries for IGMP and MLD, repectively.

IGMPv1 Joins Received	The number of Received IGMPv1 Join's
IGMPv2/MLDv1 Report's Received	The number of Received IGMPv2 Join's and MLDv1 Report's. repectively
IGMPv3/MLDv2 Report's Received	The number of Received IGMPv1 join's and MLDv2 Report's, respectively.
IGMPv2/MLDv1 Leave's Received	The number of Received IGMPv2 Leave's and MLDv1 Done's, repectively
IGMPv3/MLDv2 Report's Received	The number of Received IGMPv1 join's and MLDv2 Report's, respectively.
IGMPv2/MLDv1 Leave's Received	The number of Received IGMPv2 Leave's and MLDv1 Done's ,respectively.

WEB Interface

A. Click *Monitor/MVR Statstics to display information for MVR Statistics.*



Figure

MVR/MVR Channel Groups

Entries in the MVR Channels(Groups) Information Table are shown on this page. The MVR Channels(Groups) Information Table is sorted first by VLAN ID, and then by group.

LOCATION :

▼ Monitor

▼ MVR

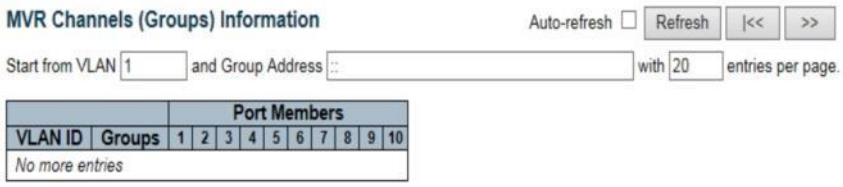
▪ MVR Channel Groups

PARAMETERS：

Items	Description
VLAN ID	VLAN ID of the group
Groups	Group ID of the group displayed
Port Members	Ports under this group

WEB Interface

A. Click *Monitor/MVR Channel Groups to display MVR Channels Groups information.*



Figure

MVR/MVR SFM Information

Entries in the MVR SFM Information Table are shown on this page. The MVR SFM (Source-Filtered Multicast) Information table also contains the SSM (Source-Specific Multicast) information. This table is sorted first by VLAN ID, then by group and then by Port. Different source addresses belong to the same group are treated as single entry.

LOCATION：

▼ Monitor

▼ MVR

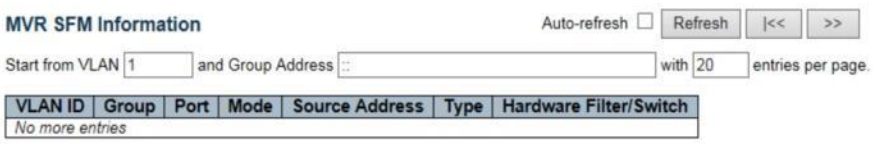
▪ MVR SFM Information

PARAMETERS：

Items	Description
VLAN ID	VLAN ID of the group
Groups	Group ID of the group displayed
Port	Switch port number
Mode	Indicates the filtering mode maintained per(VLAN ID, port number, Group Address) basis. It can be either Include or Exclude
Source Address	IP Address of the source. Currently, system limits the total number of IP source addresses for filtering to be 128. When there is no any source filtering address, the text “None” is shown in the Source Address field.
Type	Indicates the Type. It can be either Allow or Deny
Hardware Filter/ Switch	Indicates whether data plan destined to the specific group address from the source IPv4/IPv6 address could be handled by chip or not.

WEB Interface

A. Click *Monitor/MVR SFM Information to display MVR SFM information.*



Figure

IPMC/IGMP Snooping/Status

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

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

LOCATION：

▼ Monitor

▼ IPMC

▼ IGMP Snooping

▪ Status

PARAMETERS：

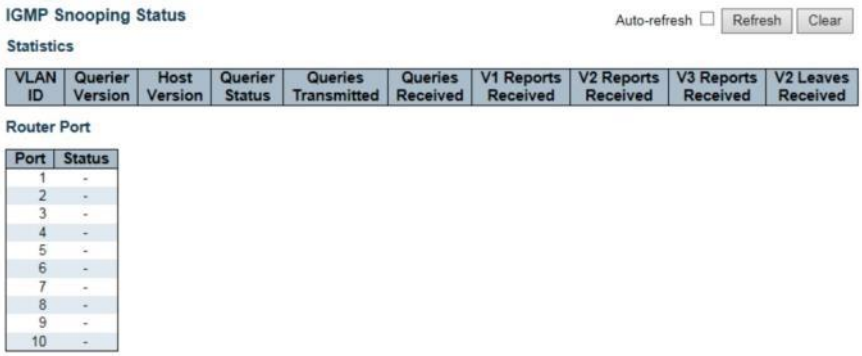
Items	Description
VLAN ID	The VLAN ID of the entry.
Querier Version	Working Querier Version currently.
Host Version	Working Host Version currently.
Querier Status	Shows the Querier status is "ACTIVE" or "IDLE". "DISABLE" denotes the specific interface is administratively disabled.
Queries Transmitted	The number of Transmitted Queries.
Queries Received	The number of Received Queries.
V1 Reports	The number of Received V1 Reports

Received 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.



IGMP Snooping Status

Auto-refresh ☐ Refresh Clear

Statistics

VLAN ID	Querier Version	Host Version	Querier Status	Queries Transmitted	Queries Received	V1 Reports Received	V2 Reports Received	V3 Reports Received	V2 Leaves Received

Router Port

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

Figure

IPMC/IGMP Snooping/Groups Information

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

LOCATION：

▼ Monitor

▼ IPMC

▼ IGMP Snooping

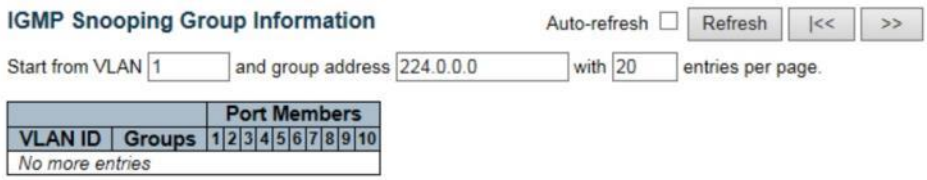
▪Groups Information

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

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



Figure

IPMC/IGMP Snooping/IPv4 SFM Information

Entries in the IGMP SFM Information Table are shown on this page. The IGMP SFM (Source-Filtered Multicast) Information Table also contains the SSM(Source-Specific Multicast) Information. This table is sorted first by VLAN ID, then by group and then by Port. Different source addresses belong to the same group are treated as single entry.

LOCATION：

▼ Monitor

▼ IPMC

▼ IGMP Snooping

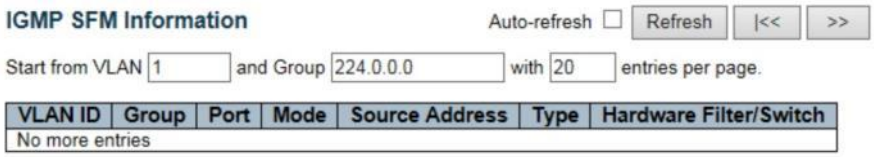
▪ Groups Information

PARAMETERS：

Items	Description
VLAN ID	The VLAN ID of the entry.
Group	Group address of the group displayed.
Port	Switch port number
Mode	Indicates the filtering mode maintained per (VLAN ID, port number, Group Address) basis. It can be either Include or Exclude.
Source Address	IP Address of the source. Currently, system limits the total number of IP source addresses for filtering to be 128.
Type	Indicates the Type. It can be either Allow or Deny
Hardware Filter/ Switch	Indicates whether data plane destined to the specific group address from the source IPv4 address could be handled by chip or not

WEB Interface

A. **Click *Monitor/IPMC/IGMP Snooping/IPv4 SFM Information* to display IGMP SFM information.**



Figure

IPMC/MLD Snooping/Status

This page provides MLD Snooping status

LOCATION：

▼ Monitor

▼ IPMC

▼ MLD

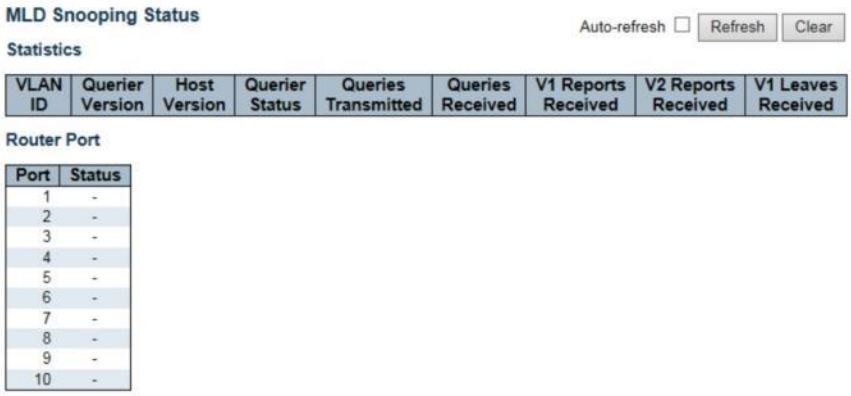
▪ Status

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 Received	The number of Received V2 Reports
V1 Leaves Received	The number of Received V1 Leaves
Router Port	Display which ports act as router pots. A router port is a port on the ehternet 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 learned to be a router port. Both denote the specific port is configured or learned to be a router port
Port	Switch port number
Status	Indicates whether specific port is a router port or not

WEB Interface

A. **Click *Monitor/IPMC/MLD Snooping/Status to display IGMP Snooping Status*.**



Figure

IPMC/MLD Snooping/Groups Information

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

LOCATION：

▼ Monitor

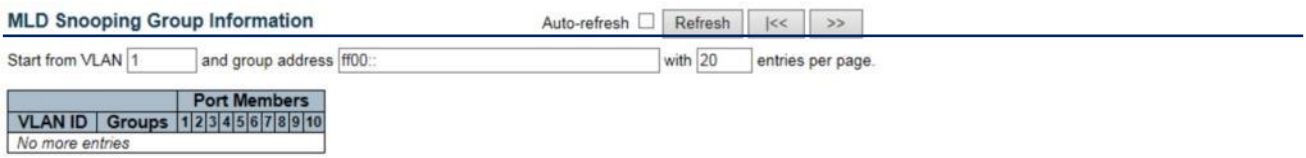
▼ IPMC

▼ MLD

▪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



Figure

IPMC/MLD Snooping/IPv6 SFM Information

Entries in the MLD SFM Information Table are shown on this page. The MLD SFM (Source-Filtered Multicast) Information Table also contains the SSM(Source-Specific Multicast) Information. This table is sorted first by VLAN ID, then by group and then by Port. Different source addresses belong to the same group are treated as single entry.

LOCATION：

▼ Monitor

▼ IPMC

▼ MLD

▪ IPv6 SFM Information

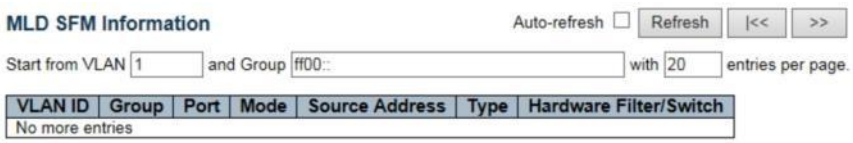
PARAMETERS：

Items	Description
VLAN ID	The VLAN ID of the entry.
Group	Group address of the group displayed.
Port	Switch port number
Mode	Indicates the filtering mode maintained per (VLAN ID, port number, Group Address) basis. It can be either Include or Exclude.
Source Address	IP Address of the source. Currently, system limits the total number of IP source addresses for filtering to be 128.
Type	Indicates the Type. It can be either Allow or Deny

Hardware Filter/ Switch	Indicates whether data plane destined to the specific group address from the source IPv4 address could be handled by chip or not

WEB Interface

A. **Click *Monitor/IPMC/IGMP Snooping/IPv6 SFM Information* to display MLD SFM information.**



Figure

LLDP/Neighbours

Using the LLDP Neighbour Information page to show information about LLDP neighbour devices connected directly to the switch.

LOCATION :

▼ Monitor

▼ LLDP

▪ Neighbours

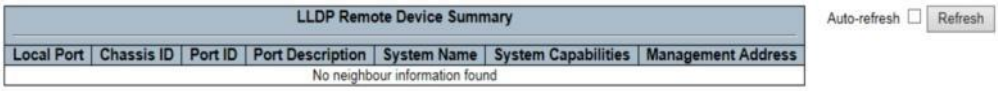
PARAMETERS :

Items	Description
Local Port	The port on which the LLDP frame was received
Chassis ID	The Chassis ID is the identification of the neighbour's LLD frames.

Port ID	The Port ID is the identification of the neighbour port.
Port Description	Port Description is the port description advertised by the neighbour unit
System Name	System name is the name advertised by the neighbour unit
System Capabilities	System Capabilities describes the neighbour unt's capabilities. The possible capabilities are: 1. Other 2. Repater 3. Bridge 4. WLAN Access Point 5. Router 6. Telephone 7. DOCSIS cable device 8. Station only 9. Reserved When a capability is enabled, the capability is followed by (+). If the capability is disabled, the capability is followed by(-)
Management Address	Management Address is the neighbour unit's address that is userd for higher layer entities to assist discovery by the network management. This could for instance hold the neighbour's IP Address

WEB Interface

A. **Click *Monitor/LLDP/Neighbours to display information about LLDP neighbours.***



Figure

LLDP/LLDP-MED Neighbours

Using the LLDP-MED Neighbour Information page to show information about remote device which is connected to switch and advertises LLDP-MED TLVs.

LOCATION：

▼ Monitor

▼ LLDP

▪ LLDP-MED Neighbours

PARAMETERS：

Items	Description
Port	The port on which the LLDP frame was received
Device Type	
LLDP-MED Devices are comprised of two primary **Device Types:** Network Connectivity Devices and Endpoint Devices. **LLDP-MED Network Connectivity Device Definition** LLDP-MED Network Connectivity Devices, as defined in TIA-1057, provide access to the IEEE 802 based LAN infrastructure for LLDP-MED Endpoint Devices. An LLDP-MED Network Connectivity Device is a LAN access device based on any of the following technologies: 1. LAN Switch/Router 2. IEEE 802.1 Bridge 3. IEEE 802.3 Repeater (included for historical reasons) 4. IEEE 802.11 Wireless Access Point 5. Any device that supports the IEEE 802.1AB and MED extensions defined by TIA-1057 and can relay IEEE 802	

frames via any method.

LLDP-MED Endpoint Device Definition

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

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

LLDP-MED Generic Endpoint (Class I)

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

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

LLDP-MED Media Endpoint (Class II)

The LLDP-MED Media Endpoint (Class II) definition is applicable to all endpoint products that have IP media capabilities however may or may not be associated with a particular end user. Capabilities include all of the capabilities defined for the previous Generic Endpoint Class (Class I), and are extended to include aspects related to media streaming.

Example product categories expected to adhere to this class include (but are not limited to) Voice / Media Gateways, Conference Bridges, Media Servers, and similar. Discovery services defined in this class include media-type-specific network layer policy discovery. LLDP-MED Communication Endpoint (Class III) The LLDP-MED Communication Endpoint (Class III) definition is applicable to all endpoint products that act as end user communication appliances supporting IP media. Capabilities include all of the capabilities defined for the previous Generic Endpoint (Class I) and Media Endpoint (Class II) classes, and are extended to include aspects related to end user devices. Example product categories expected to adhere to this class include (but are not limited to) end user communication appliances, such as IP Phones, PC-based softphones, or other communication appliances that directly support the end user. Discovery services defined in this class include provision of location identifier (including ECS / E911 information), embedded L2 switch support, inventory management	
LLDP-MED Capabilities	**LLDP-MED Capabilities** describes the neighbour unit's LLDP-MED capabilities. The possible capabilities are: 1. LLDP-MED capabilities 2. Network Policy 3. Location Identification 4. Extended Power via MDI - PSE 5. Extended Power via MDI - PD 6. Inventory 7. Reserved

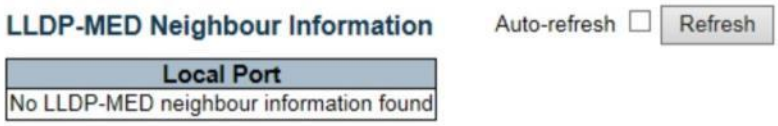
Application Type	**Application Type** indicating the primary function of the application(s) defined for this network policy, advertised by an Endpoint or Network Connectivity Device. The possible application types are shown below. 1. Voice - for use by dedicated IP Telephony handsets and other similar appliances supporting interactive voice services. These devices are typically deployed on a separate VLAN for ease of deployment and enhanced security by isolation from data applications. 2. Voice Signalling - for use in network topologies that require a different policy for the voice signalling than for the voice media. 3. Guest Voice - to support a separate limited feature-set voice service for guest users and visitors with their own IP Telephony handsets and other similar appliances supporting interactive voice services. 4. Guest Voice Signalling - for use in network topologies that require a different policy for the guest voice signalling than for the guest voice media. 5. Softphone Voice - for use by softphone applications on typical data centric devices, such as PCs or laptops. 6. Video Conferencing - for use by dedicated Video Conferencing equipment and other similar appliances supporting real-time interactive video/audio services. 7. Streaming Video - for use by broadcast or multicast based video content distribution and other similar applications supporting streaming video services that require specific network policy treatment. Video applications relying on TCP with buffering

	would not be an intended use of this application type. 8. Video Signalling - for use in network topologies that require a separate policy for the video signalling than for the video media.
Policy	Policy indicates that an Endpoint Device wants to explicitly advertise that the policy is required by the device. Can be either Defined or Unknown: **Unknown:** The network policy for the specified application type is currently unknow. **Defined:** The network policy is defined.
TAG	**TAG** is indicative of whether the specified application type is using a tagged or an untagged VLAN. Can be Tagged or Untagged. **Untagged:** The device is using an untagged frame format and as such does not include a tag header as defined by IEEE 802.1Q-2003. **Tagged:** The device is using the IEEE 802.1Q tagged frame format.
VLAN ID	**VLAN ID** is the VLAN identifier (VID) for the port as defined in IEEE 802.1Q-2003. A

	value of 1 through 4094 is used to define a valid VLAN ID. A value of 0 (Priority Tagged) is used if the device is using priority tagged frames as defined by IEEE 802.1Q-2003, meaning that only the IEEE 802.1D priority level is significant and the default PVID of the ingress port is used instead.
Priority	**Priority** is the Layer 2 priority to be used for the specified application type. One of the eight priority levels (0 through 7).
DSCP	**DSCP** is the DSCP value to be used to provide Diffserv node behavior for the specified application type as defined in IETF RFC 2474. Contain one of 64 code point values (0 through 63).
Auto-negotiation	**Auto-negotiation** identifies if MAC/PHY auto-negotiation is supported by the link partner.
Auto-negotiation status	**Auto-negotiation status** identifies if auto-negotiation is currently enabled at the link partner. If **Auto-negotiation** is supported and Auto-negotiation status is disabled, the 802.3 PMD operating mode will be determined the operational MAU type field value rather than by auto-negotiation.
Auto-negotiation Capabilities	Auto-negotiation Capabilities shows the link partners MAC/PHY capabilities

WEB Interface

A. **Click *Monitor/LLDP/LLED-MED to display information about LLDP-MED neighbours.***



Figure

LLDP/EEE

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

LOCATION：

▼ Monitor

▼ LLDP

▪ EEE

PARAMETERS：

Items	Description
Local Port	The port on which the LLDP frame was received
Tx Tw	The link partner's maximum time that transmit path can hold-off sending data after deassertion of LPI.
Rx Tw	The link partner's time that receiver would like the transmitter to hold-off to allow time for the receiver to wake from sleep.
Fallback Receive Tw	The link partner's fallback receive Tw. A receiving link partner may inform the transmitter of an alternate desired Tw_sys_tx. Since a receiving link partner is likely to have discrete levels for savings, this

	provides the transmitter with additional information that it may use for a more efficient allocation. Systems that do not implement this option default the value to be the same as that of the Receive Tw_sys_tx.
Eacho Tx Tw	The link partner's Echo Tx Tw value. The respective echo values shall be defined as the local link partners reflection (echo) of the remote link partners respective values. When a local link partner receives its echoed values from the remote link partner it can determine whether or not the remote link partner has received, registered and processed its most recent values. For example, if the local link partner receives echoed parameters that do not match the values in its local MIB, then the local link partner infers that the remote link partners request was based on stale information.
Echo Rx Tw	The link partner's Echo Rx Tw value.
Resolved Tx Tw	The resolved Tx Tw for this link. Note : NOT the link partner The resolved value that is the actual "tx wakeup time " used for this link (based on EEE information exchanged via LLDP).
Resolved Rx Tw	The resolved Rx Tw for this link. Note : NOT the link partner The resolved value that is the actual "tx wakeup time " used for this link (based on EEE information exchanged via LLDP).
EEE in Sync	Shows whether the switch and the link partner have agreed on wake times. Red - Switch and link partner have not agreed on wakeup times. Green - Switch and link partner have agreed on wakeup times.

WEB Interface

A. **Click *Monitor/LLDP/EEE to display information about LLDP EEE neighbours.***

LLDP Neighbors EEE Information

Auto-refresh ☐ Refresh

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

Figure

LLDP/Port Statistics

This page provides an overview of all LLDP traffic.

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

LOCATION：

▼ Monitor

▼ LLDP

▪ Port Statistics

PARAMETERS：

Items	Description
Global Counters	
Nieghbour entries were last changed	Shows the time when the last entry was last deleted or added. It also shows the time elapsed since the last change was detected.
Total Nieghbours Entries Added	Shows the number of new entries added since switch reboot.
Total Neighbours Entries Deleted	Shows the number of new entries deleted since switch reboot.
Total Neighbours Entries Dropped	Shows the number of LLDP frames dropped due to the entry table being full.
Total Neighbours Entries Aged Out	Shows the number of entries deleted due to Time-To-Live expiring.

Local Counters	
Local Port	The port on which LLDP frames are received or transmitted
Tx Frames	The number of LLDP frames transmitted on the port
Rx Frames	The number of LLDP frames received on the port
Rx Errors	The number of received LLDP frame containing some kind of error
Frames Discard	If an LLDP frame is received on a port, and the switch's internal table has run full, the LLDP frame is counted and discarded. This situation is known as "Too Many Neighbours" in the LLDP standard. LLDP frames require a new entry in the table when the Chassis ID or Remote Port ID is not already contained within the table. Entries are removed from the table when a given port's link is down, an LLDP shutdown frame is received, or when the entry ages out.
TLVs Discarded	Each LLDP frame can contain multiple pieces of information, known as TLVs (TLV is short for "Type Length Value"). If a TLV is malformed, it is counted and discarded.
TLVs Unrecognized	The number of well-formed TLVs, but with an unknown type value.
Org. Discarded	The number of organizationally received TLVs
Age-Outs	Each LLDP frame contains information about how long time the LLDP information is valid (age-out time). If no new LLDP frame is received within the age out time, the LLDP information is removed, and the Age-Out counter is incremented.

WEB Interface

A. **Click *Monitor/LLDP/Port Statistics to display information about LLDP traffics.***

LLDP Global Counters

Auto-refresh ☐ Refresh Clear

Global Counters	
Neighbour entries were last changed	1970-01-01T00:00:00+00:00 (27675 secs. ago)
Total Neighbours Entries Added	0
Total Neighbours Entries Deleted	0
Total Neighbours Entries Dropped	0
Total Neighbours Entries Aged Out	0

LLDP Statistics Local Counters

Local Port	Tx Frames	Rx Frames	Rx Errors	Frames Discarded	TLVs Discarded	TLVs Unrecognized	Org. Discarded	Age-Outs
1	924	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0

Figure

MAC Table

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

LOCATION：

▼ Monitor

▪ MAC Table

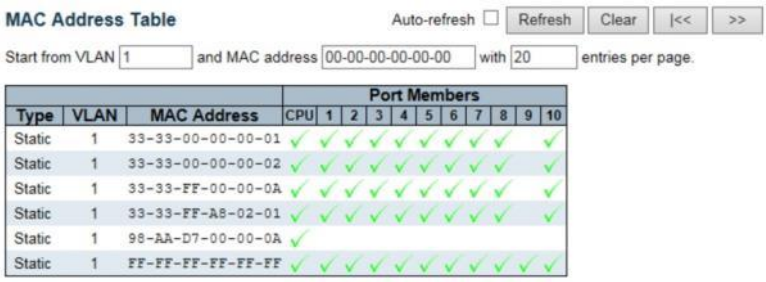
PARAMETERS：

Items	Description
Type	Indicates whether the entry is static or a

	dynamic entry
MAC Address	The MAC address of the entry
VLAN	The VLAN ID of the entry
Port Members	The ports that are members of the entry

WEB Interface

A. Click *Monitor/MAC Table to show Static MAC Address and Dynamic MAC address entries.*



Figure

VLANs/VLAN Membership

Using Monitor pages for VLANs to display port members of VLANs and its' VLAN attributes corresponding each port. Using VLAN Membership Status for specific users page to display the information of all VLAN status and reports.

LOCATION：

▼ Monitor

▼ VLANs

- VLAN Membership

PARAMETERS：

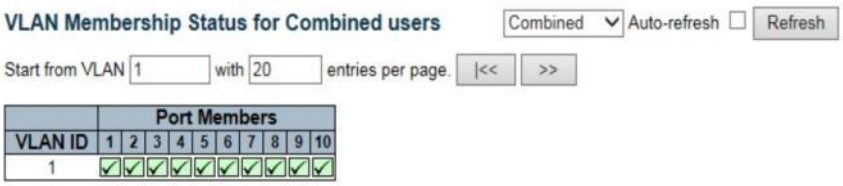
Items	Description
VLAN USER	VLAN User module uses services of the VLAN management functionality to configure VLAN memberships and VLAN port configurations such as PVID and UVID. Currently we support the following VLAN user types： **CLI/Web/SNMP**：These are referred to as static. **NAS**：NAS provides 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.



Figure

VLANs/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

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

VLAN Port Status for Static user

Static Auto-refresh Refresh

Port	PVID	Port Type	Ingress Filtering	Frame Type	Tx Tag	UVID	Conflicts
1	1	UnAware	Disabled	All	Untag_this	1	No
2	1	UnAware	Disabled	All	Untag_this	1	No
3	1	UnAware	Disabled	All	Untag_this	1	No
4	1	UnAware	Disabled	All	Untag_this	1	No
5	1	UnAware	Disabled	All	Untag_this	1	No
6	1	UnAware	Disabled	All	Untag_this	1	No
7	1	UnAware	Disabled	All	Untag_this	1	No
8	1	UnAware	Disabled	All	Untag_this	1	No
9	1	UnAware	Disabled	All	Untag_this	1	No
10	1	UnAware	Disabled	All	Untag_this	1	No

Figure

VCL/MAC-Based VLAN

Using the MAC-Based VLAN Membership Status for User Static to show MAC Address to VLAN mapping entries

LOCATION：

▼ Monitor

▼ VCL

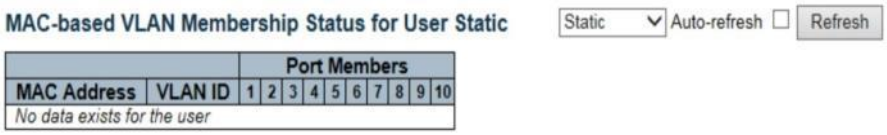
▪ MAC-based VLAN

PARAMETERS：

Items	Description
MAC Address	Indicates the MAC address
VLAN ID	Indicates the VLAN ID
Port Members	Port Members of the MAC-based VLAN entry

WEB Interface

A. Click *Monitor/VLC/MAC-Based VLAN* to show MAC Address to VLAN Mapping entries



Figure

sFlow

This page shows receiver and per-port sFlow statistics

LOCATION：

▼ Monitor

▪ sFlow

PARAMETERS：

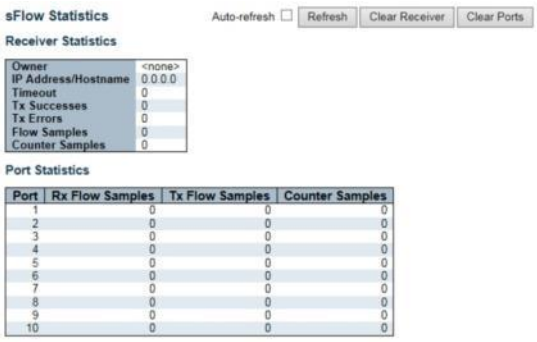
Items	Description
Receiver Statistic	

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

	statistics applies
Rx and Tx Flow Samples	The number of flow samples sent to the sFlow receiver originating from this port. Here, flow samples are divided into Rx and Tx flow samples, where Rx flow samples contains the number of packets that were sampled upon reception (ingress) on the port and Tx flow samples contains the number of packets that were sampled upon transmission (egress) on the port.
Counter Samples	The total number of counter samples sent to the sFlow receiver originating from this port.

WEB Interface

A. Click *Monitor/sFlow*to show sFlow Statistics



Figure

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

Diagnostics/Ping

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

LOCATION：

▼ Diagnostic

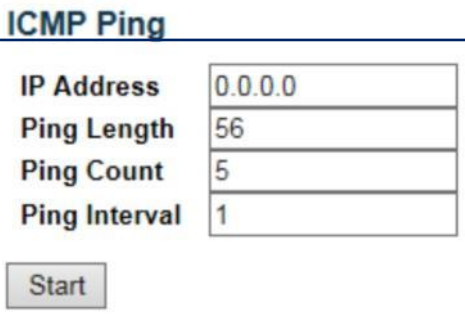
▪ Ping

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

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



Figure

Diagnostics/Ping6

Using ICMP Ping page to send ICMPv6 request packet to another connected point to check if it is connect.

LOCATION：

▼ Diagnostic

▪ Ping6

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

A. Click *Diagnostics/Ping6 to run the testing*.

ICMPv6 Ping

IP Address	0:0:0:0:0:0:0:0
Ping Length	56
Ping Count	5
Ping Interval	1

Start

Figure

CHAPTER 7

WEB MAINTENANCE
RESTART DEVICE

This chapter describes how to restart device, reload device tomanufactory default, saving or restore configuration andfirmware upgrading , swapping.

Maintenance/Restart Device

Using the Restart Device page to restart the switch.

LOCATION :

▼ Maintenance

▪ Restart Device

WEB Interface

A. Click Maintanence/*Restart Device to restart the switch*.

B. Click “Yes” to confirm the restart process and “No” to cancel the restart process.

Figure

Maintenance/Factory Defaults

Using Factory Defaults page to reset the switch to manufactory default setting.

LOCATION：

▼ Maintenance

▪ Factory Defaults

WEB Interface

A. Click Maintanence/*Factory Defaults to reset the switch to manufactory default settings*.
B. Click “Yes” to confirm the process and “No” to cancel.

Figure

Maintenance/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

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

Figure

Maintenance/Software/Image Select

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

LOCATION：

▼ Maintenance

▼ Software

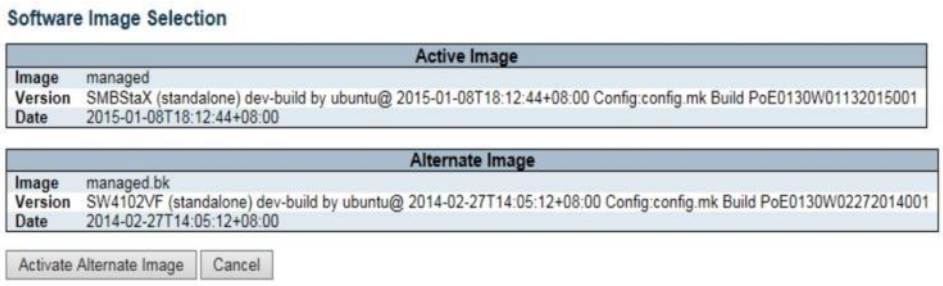
■ Image Select

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

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



Figure

Maintenance/Configuration/Save

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

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

Figure

Figure

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 Interface

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

제 품 보 증 서			
제 품 명	Giga 8Port Management L2 Layer(SFP x 2)	모 델 명	NEXT-3008GL2
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.

Publication Date: Feb, 2015
Version 1.00

H. 우편(택배)이나 퀵서비스를 통한 A/S접수 시 제품을 당사로 보내는 것은 소비자의 책임이며, 당사에서 소비자에게 보내는 것은 당사의 책임입니다.

Publication Date: Feb, 2015
Version 1.00