Web Manual

HR600-AXGM-SWG2086AS PoE Switch

Stp. 15, 2019

Ver. 1.0

Revision history

Date	Version	Description
Stp. 15, 2019	V 1.0	The first edition

0 Foreword

0.1 Target Audience

This manual is prepared for the installers and system administrators who are responsible for network installation, configuration and maintenance. It assumes that you've understood all network communication and management protocols, as well as the technical terms, theoretical principles, practical skills, and expertise of devices, protocols and interfaces related to networking. Work experience in Graphical User Interface (GUI), Command-line Interface, Simple Network Management Protocol (SNMP) and Web Explorer is also required.

0.2 Manual Convention

The following approaches should prevail.

GUI Convention	Description
🕮 Description	Describe operations and add necessary information.
⚠ Caution	Remind you of cautions as improper operations will result in data loss or equipment damage.

1 Management Software Specification

1. Layer 2 Functions			
1.1	Port Management	Enable/disable port	
		Configure speed, duplex and MTU	
		Configure flow control	
		Check port information	
1.2	Mirroring	Support the ingress and egress directions to ports	
1.3	Rate Limit	Bit rate is determined by chips.	
1.4	Port Isolation	Support port isolation configuration	
1.5	Storm Policing	Suppress the storms of broadcast, unknown unicast and multicast	
1.6	Link Aggregation	Static aggregation in manual mode	
		Dynamic aggregation in LACP mode	
1.7	VLAN	Access	
		Trunk	
		Hybrid	
1.8	MAC	Add or delete statically	
		Learn limited MAC addresses	
		Set dynamic aging time	
1.9	Spanning Tree	802.1d (STP) available	ERPS (proprietary protocol) is also available.
		802.1w (RSTP) available	
		802.1s (MSTP) available	
1.10	IGMP Snooping	Add or delete statically	
		Snoop the v1/2/3 dynamic multicast	
2. Layer 3 and Routing Functions			
2.1	Interface Configuration	VLAN interface available	
2.2	ARP	Check ARP	
2.3	Routing	Static routing	

3. Extended Functions			
2.1	ACL	Port numbers based on Source/Destination MAC, protocol type, Source/Destination IP, and L4 port.	
		Time-range management	
2.2	QoS	Classed by 802.1p (CoS)	
		Classed by DSCP	
		Classed by Source/Destination IP and port	
		Support SP, WRR and DRR scheduling algorithms	
		Support committed access rate (CAR)	
2.3	LLDP	Support Link Layer Discovery Protocol (LLDP)	
2.4	User Configuration	Add/delete a user	
2.5	Log	Login, operation, status and event logs	
2.6	Attack Resistance	DoS defense	
		Protect CPU and restrict message uploading rate	
		ARP binding (IP, MAC, Port)	
2.7	Network Diagnostics	Support Ping, Telnet and traceroute	
2.8	System Management	Unit resetting, configuration saving/restoring, upgrade, time setting, etc.	
4. Management Functions			
3.1	CLI	Manage serial port command lines	
3.2	Telnet	Remotely control Telnet	
3.3	Web	Support Layer 2 configuration	
5. Other Functions			
5.1	Support DHCP Snooping		
5.2	Support ring protection, namely the ERPS aforesaid.		
5.3	Support SNMP v1/v2c/v3		

2 Web Page Login

2.1 Log in the Network Management Client

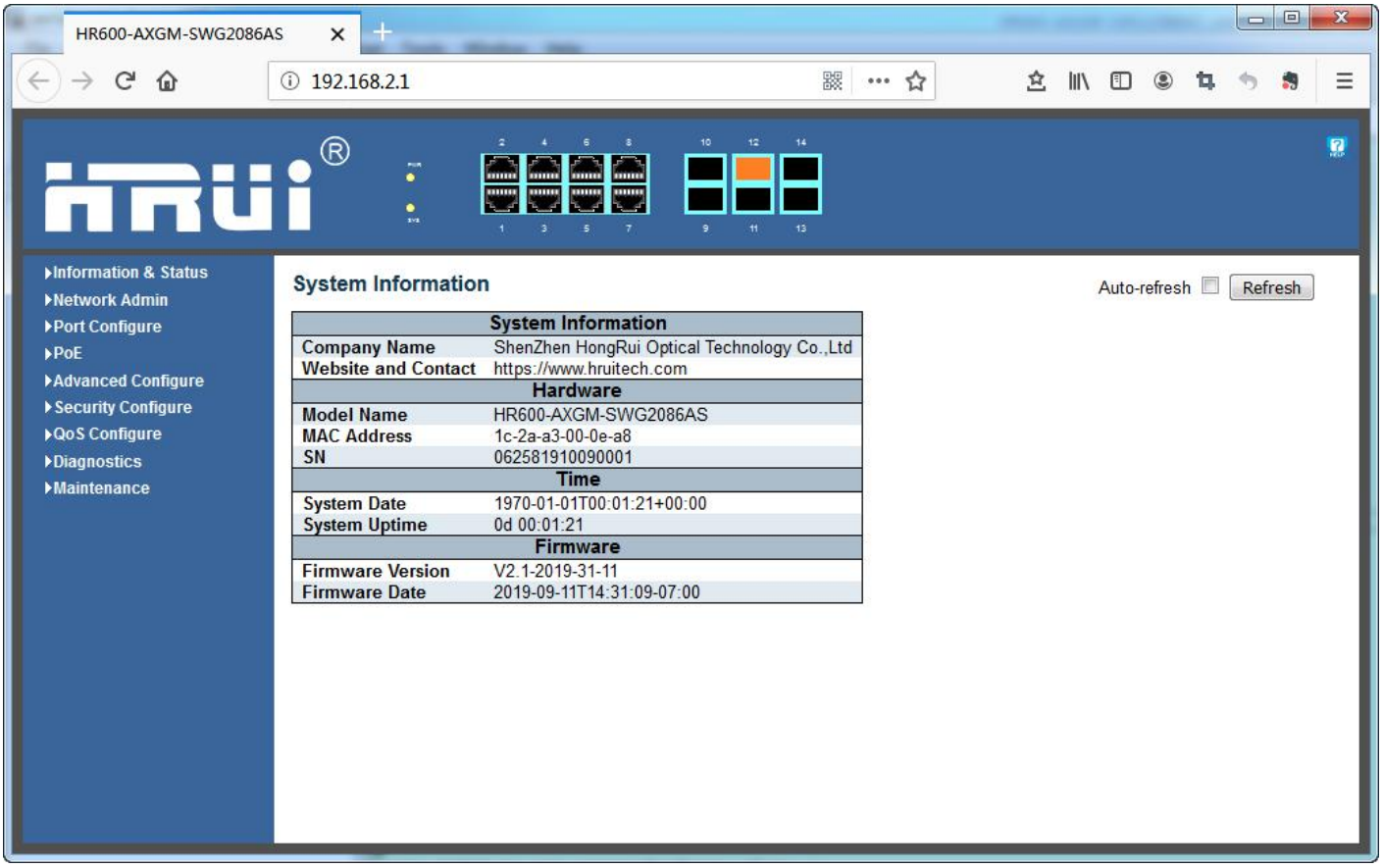
Type in the default switch address: http://192.168.2.1 in the browser and click the “Enter”.

📖 Description:

Keep the IP network segment of PC consistent with that of switch but differentiate the IP address as you log in. Set PC’s IP address of 192.168.2.x and the subnet mask of 255.255.255.0 for the first login (1< x ≤254).

A login window appears as follows. Type in the default username of “admin” and the password of “admin”. Click the “Log in” to see the switch system.

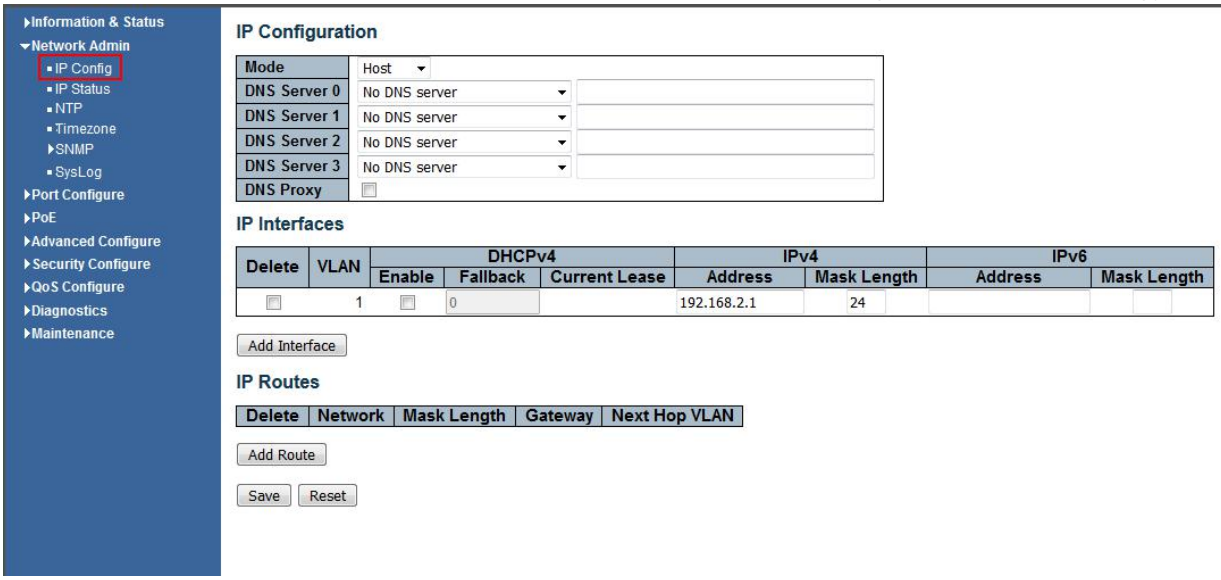
After login, you will see:



3 Network Admin

3.1 IP Config

Click the “Network Admin-IP Config” as follows.



Description about IP Config:

Configuration Items	Description
Mode	Select from Host mode and Router mode
DNS Server	Select from No DNS Server, Configurable IPv4, IPv4, From any DHCPv4 interface, and From this DHCPv4 interface
DNS Proxy	DNS Proxy
Interface Name	Display the name of system interface.
VLAN	Enter the VLAN to access and manage the switch.
IPv4 DHCP	- Enabled status refers to that VLAN interface dynamically obtains the switch IPv4 address through IPv4 DHCP Client. Otherwise the static IP configuration will take place. - Waiting time (unit: s) refers to the period when the switch tries to get dynamic IP address through DHCP. It will never time out in case of 0 second. - Current IP address is obtained through DHCP.
IPv4	- IP address: the static IPv4 address entered by a user. - IP mask: the static IPv4 subnet mask entered by a user.
IPv6	- IP address: the static IPv6 address entered by a user. - IP mask: the static IPv6 subnet mask entered by a user.
IP Routes	- Destination segment: the IPv4 address entered by a user.

	- IP mask: the static IPv4 subnet mask entered by a user. - Next hop address: the next IPv4 address entered by a user.

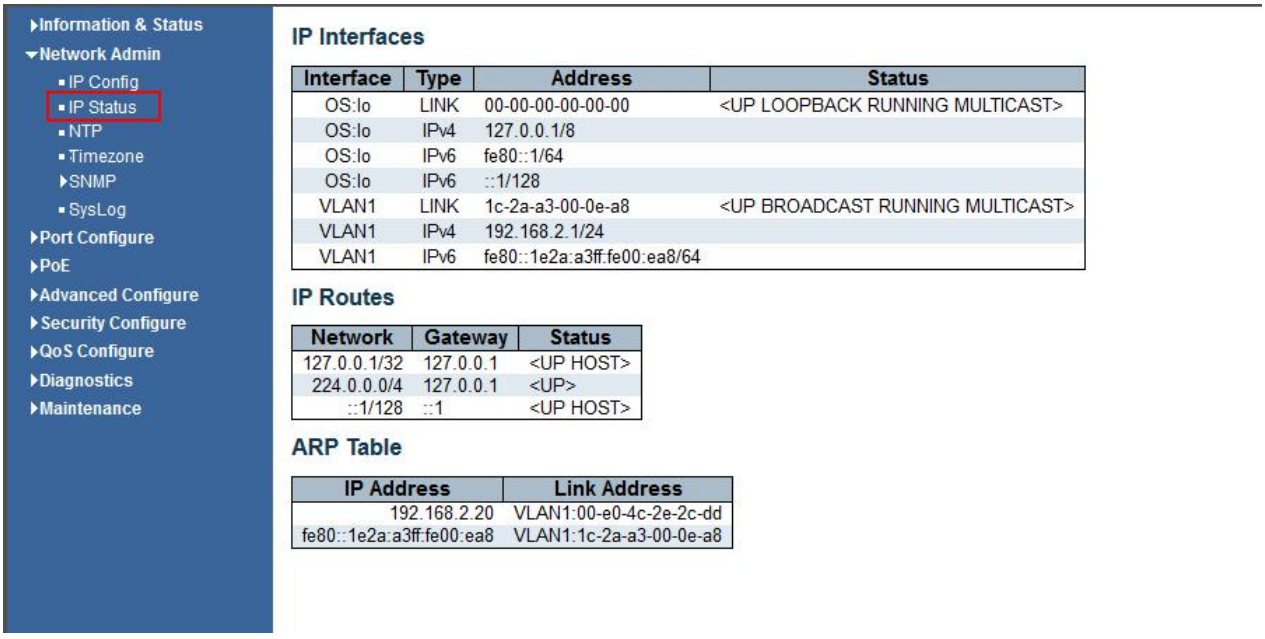
Click “Add” to create new Management VLAN and IP addresses and “Save” and finish.

🕮 Description:

Note: The switch creates VLAN1 only by default. Users who need to use other management switches should add the VLAN and related ports in the VLAN module first to realize the Layer 3 communication between VLANs.

3.2 IP Status

Click the “Network Admin-IP Status” as follows.



Description about IP Status:

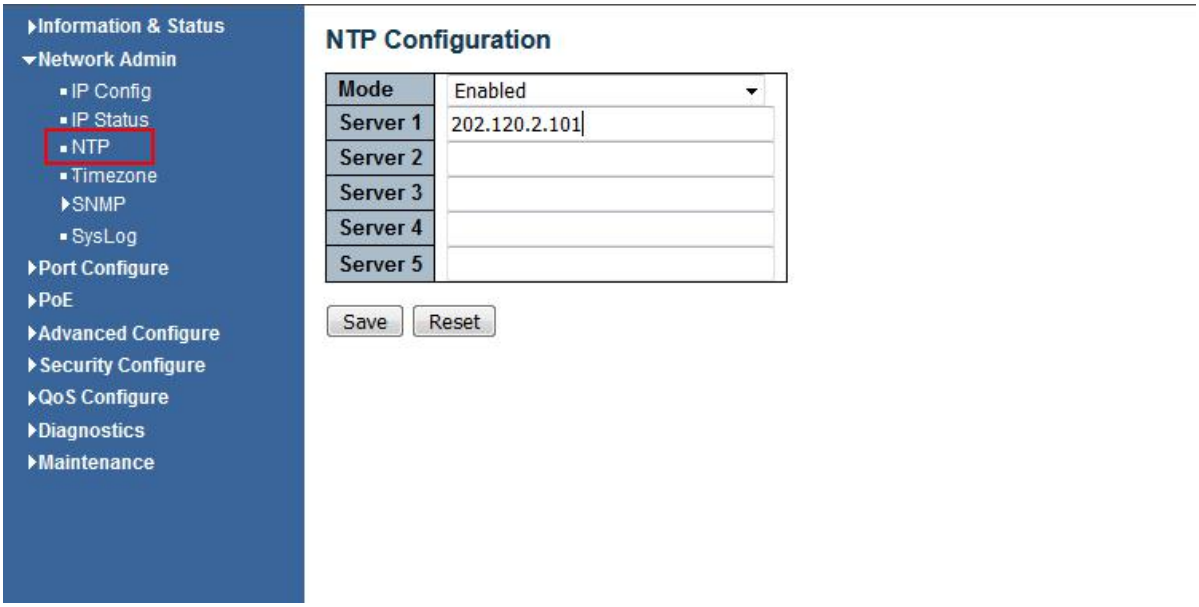
Configuration Items	Description
IP Interfaces	Check the IP Port Table
IP Routes	Check the IP Routing Table
ARP Table	Check the ARP Table

3.3 NTP

Applied for the clock synchronization between distributed time servers and clients, NTP (Network Time Protocol) is at the application layer of TCP/IP protocol family, which is realized based on IP and UDP. NTP message is transmitted through UDP with No. 123 port. Clock synchronization in all network devices will play a decisive role in the context of increasingly complex network topology. So NTP emerges since administrators' manual modification of system clock will lead to huge workload and inaccurate time.

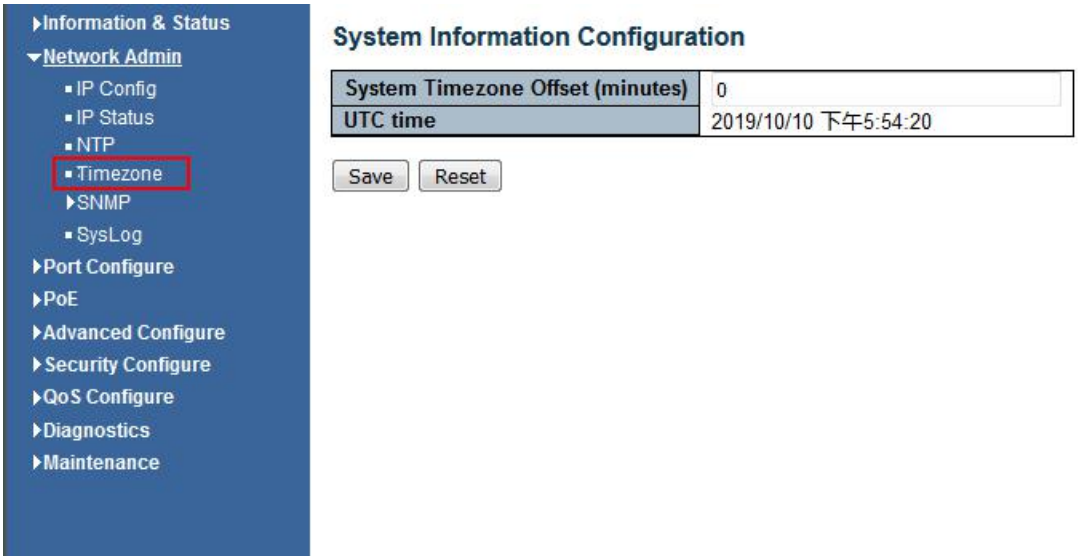
Instructions

1. Click the "Network Admin-NTP" in the navigation bar as follows.



Configuration Items	Description
Mode	Enable or disable NTP by dropping down the list.
NTP Server	Its IP address and NTP info will be obtained from NTP servers.

1. Click the "Network Admin-Timezone" in the navigation bar as follows.



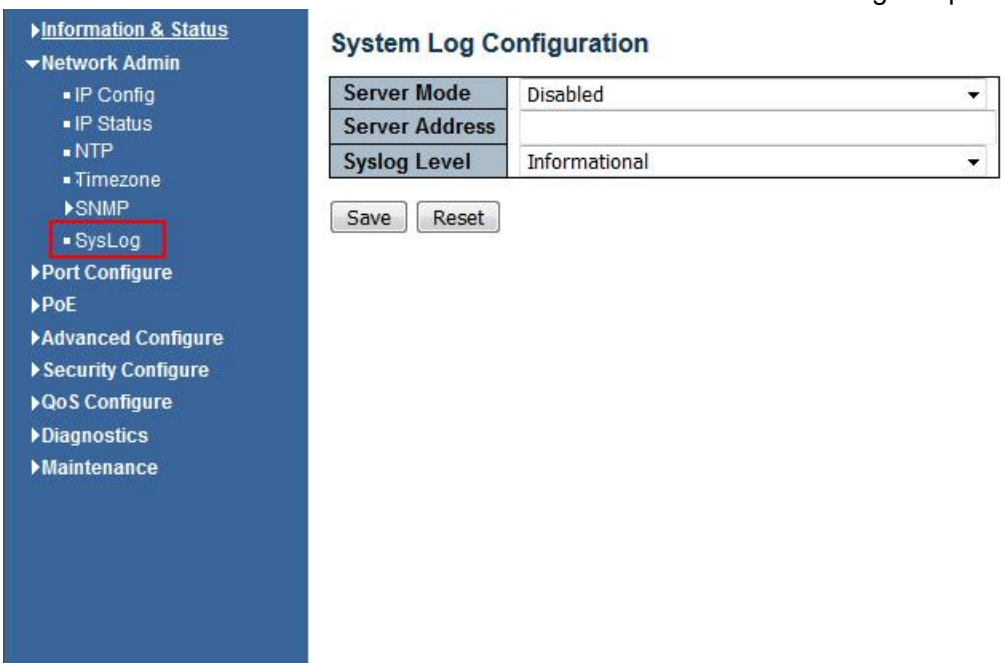
Configuration Items	Description
System Time-zone Offset (minutes)	Set the time to be modified.
UTC Time	Current Internet time

3.4 Syslog

Users can upload the switch logs to the TFTP Server.

Instructions

1. Click the “Network Admin-SysLog” as follows:



Configuration Items	Description
Mode	Enable or disable the Syslog function. The switch will send the syslogs to the specified servers if enable.
Server IP Address	IP addresses of the specified log servers
Log Levels	Specified levels including: **Info**: information, warnings and errors. **Warning**: warnings and errors. **Error**: errors.

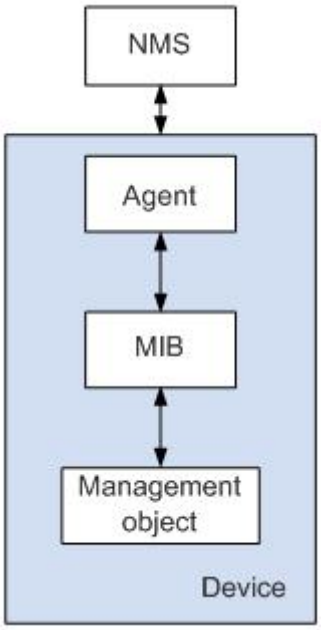
3.5 SNMP

SNMP (Simple Network Management Protocol) is widely used in TCP/IP network. It manages devices by the central computer which operates network management software (i.e. network management workstation). SNMP is: Simple: The polling-driving SNMP has the fundamental functionality set that is applicable to small-scale environment with fast speed and low cost. Besides, UDP-driven SNMP is compatible with most devices. Powerful: SNMP aims to ensure the management info transmission between two nodes so that administrators can retrieve, modify and troubleshoot the info easily. There are 3 common versions, namely SNMPv1, v2c and v3. Its system contains NMS (Network Management System), Agent, Management object and MIB (Management Information Base).

NMS, as the management center, will manage all devices. Each device under management includes the resident Agent, MIB and management objects. NMS interacts with the Agent running on the management object which will

operate the MIB to execute NMS orders.

SNMP management model



NMS

- As the network administrator, NMS manages/monitors network devices by SNMP on its server. It can require the Agent to inquire or modify configuration item value(s). NMS can receive the Trap actively sent by the Agent to be updated with the statuses of the managed devices.

Agent

- As a agent process of the managed devices, it maintains device data and responds to the NMS requests by reporting management data. Agent will fulfill relevant orders through MIB Table and send the results back to NMS after receiving its request. Devices will take the initiative to send info related to the current statues of devices to NMS through Agent once a failure or other event occurs.

Management object

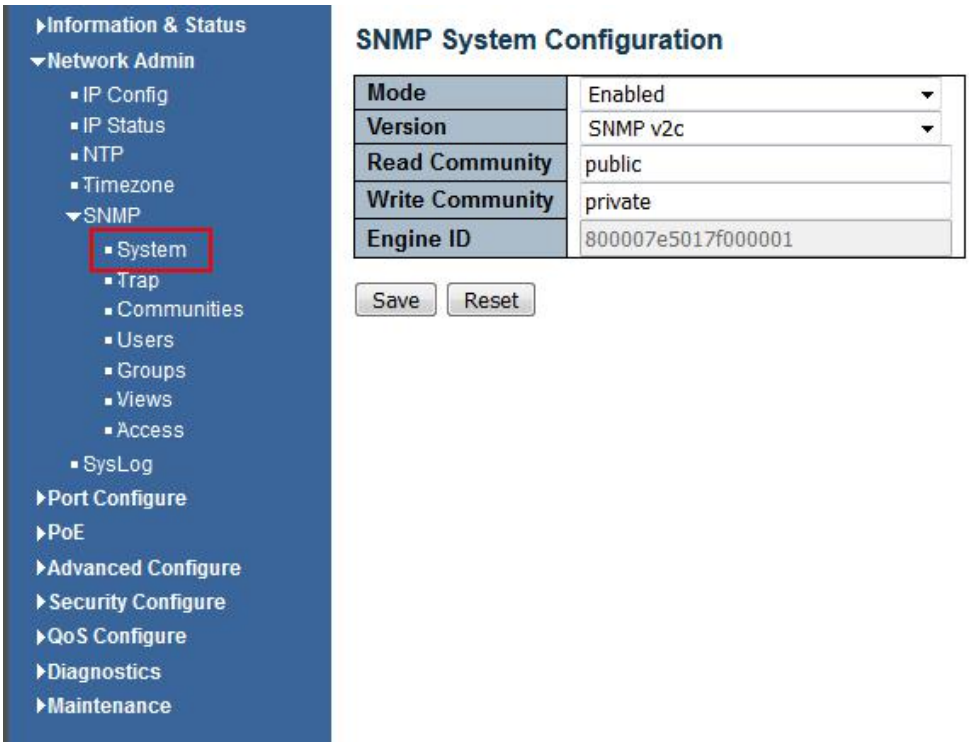
- It refers to the object under management. Each device may have more than one objects, including a piece of hardware (e.g. an interface board), partial hardware and software (e.g. routing protocol), as well as other configuration item sets.

MIB

- MIB is a database specifying the variables maintained by the management object (i.e. the info that can be inquired and set by the Agent). MIB defines the attributes of the management object, including the name, status, access right and data type. The following functions can be realized through MIB: Agent will master the instant device info by inquiring MIB, and set the status configuration items by changing MIB.

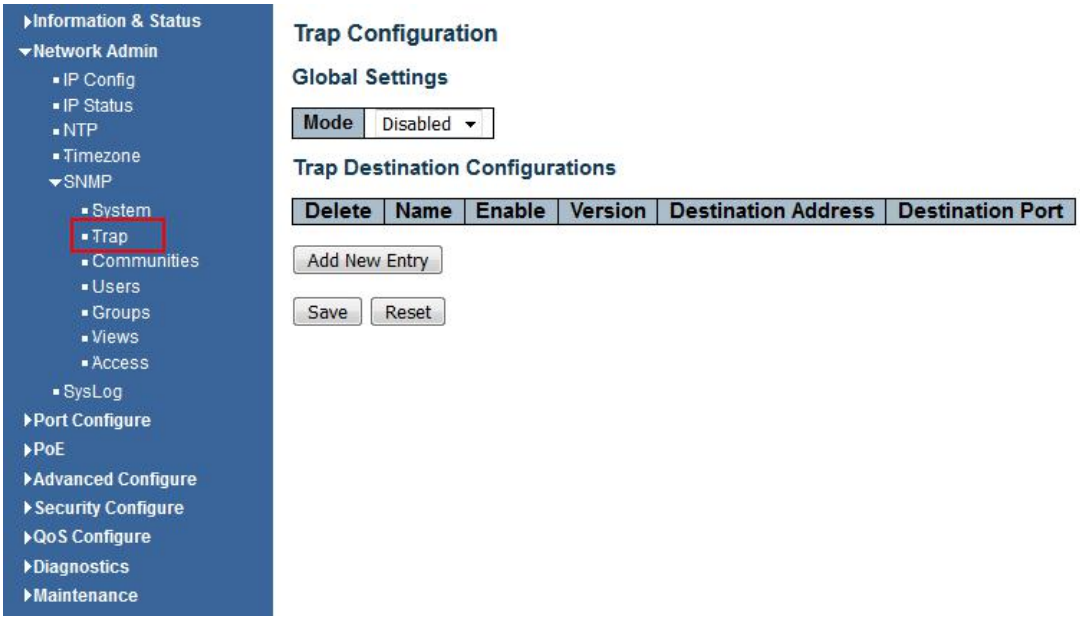
Instructions

1. Click the “Network Admin -SNMP” in the navigation tree to the “SNMP System Configuration” as follows.



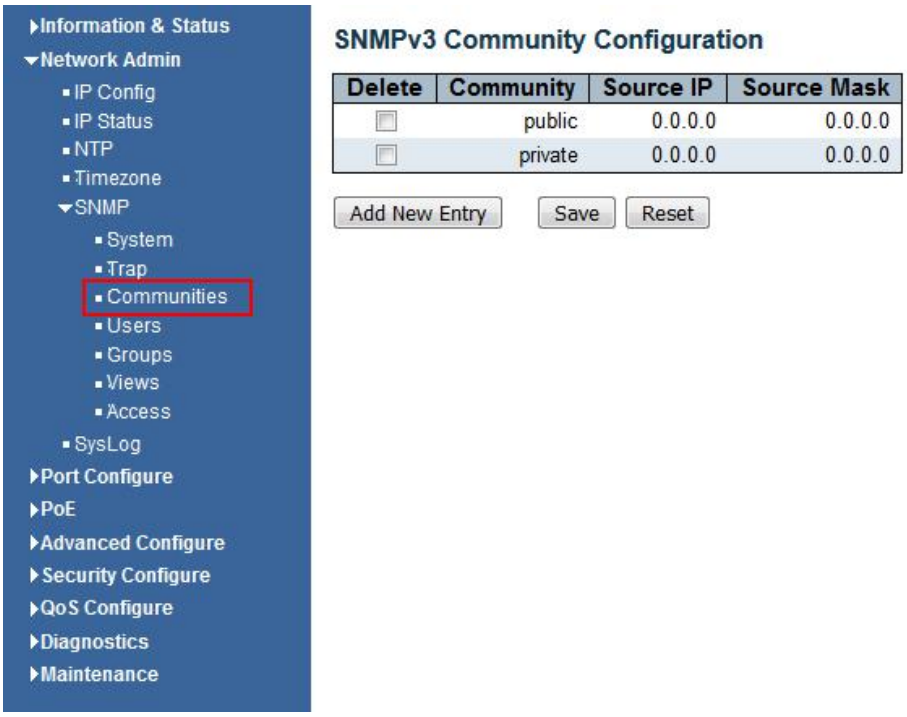
Configuration Items	Description
SNMP Mode	Enable or disable SNMP functions
Version	Select SNMPv1, v2c or v3 by dropping down the list
Read Community	Authorized management site can read the MIB object, which is called “public” by default
Write Community	Authorized management site can read and modify the MIB object, which is called “private” by default

2. Users can enable and disable the SNMP Trap and SNMP authentication trap functions of the switch. Click the “Network Admin-SNMP-Trap” as follows:



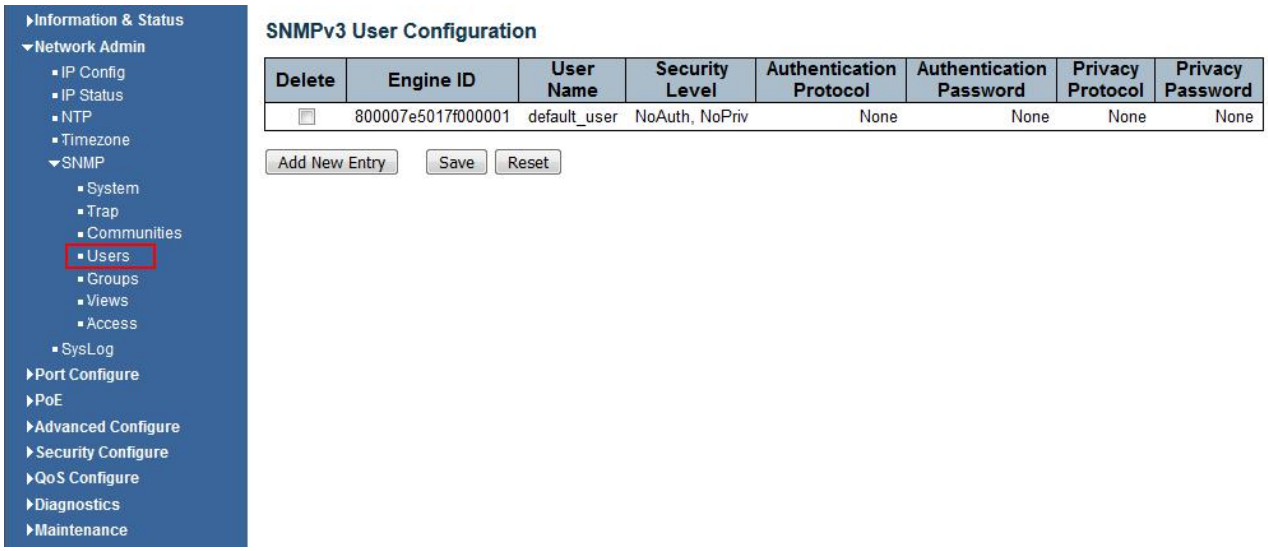
Configuration Items	Description
Trap Name	SNMP Trap alias
Trap Mode	Enabled or disabled SNMP Trap
Trap Version	SNMPv1, v2c and v3
Trap Community	Group name of the specified SNMP Trap Community
Trap Destination IP Address	IP address of the specified SNMP Trap Server
Trap Destination UDP Port	UDP port No. of the specified SNMP Trap Server
Trap Inform/Response Mode	Enabled or disabled
Trap Inform/Response Timeout (seconds)	Period
Trap Inform/Response Retry Times	Number of times

3. Users can rename the community. Click the “Network Admin-SNMP-Communities” as follows:



Configuration Items	Description
Community	Enter the new name
Source IP	Enter the IPv4 source address
Source Mask	Enter the IPv4 subnet mask

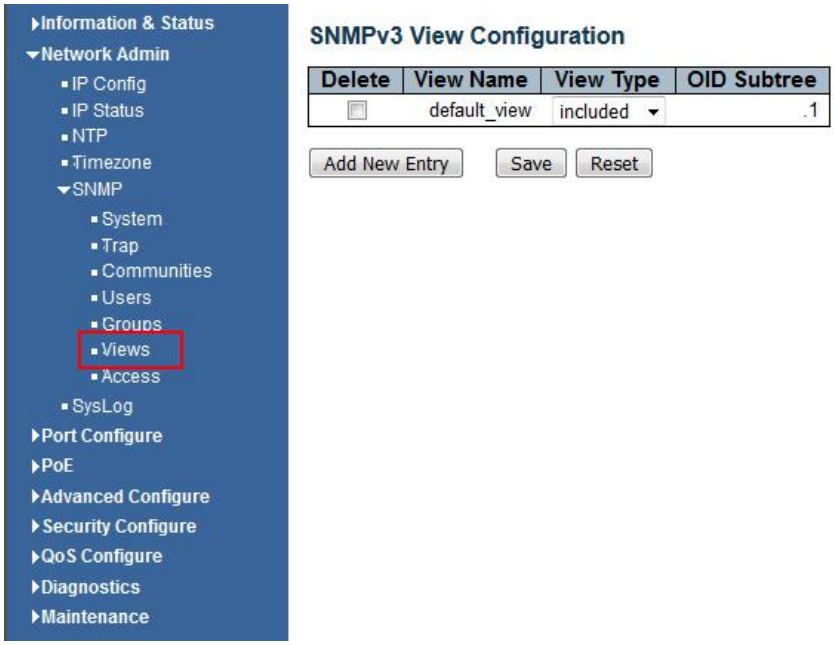
4. Create a SNMP v3 User and select the way of privacy. Click the “Network Admin-SNMP-Users” as follows:



Configuration Items	Description
Engine ID	The default 800007e5017f000001 is recommended for the switch.
Username	Enter the new name of SNMPv3 user
Security Level	Select a method of encryption from noAuthnoPriv, authNoPriv, and authPriv by dropping down the list.
Authentication Protocol	Select a privacy protocol from MD5 or SHA by dropping down the list.
Authentication Password	Type in the privacy password
Privacy Protocol	Select a privacy protocol from DES or AES by dropping down the list.
Privacy Password	Type in the privacy password

"Save" and finish.

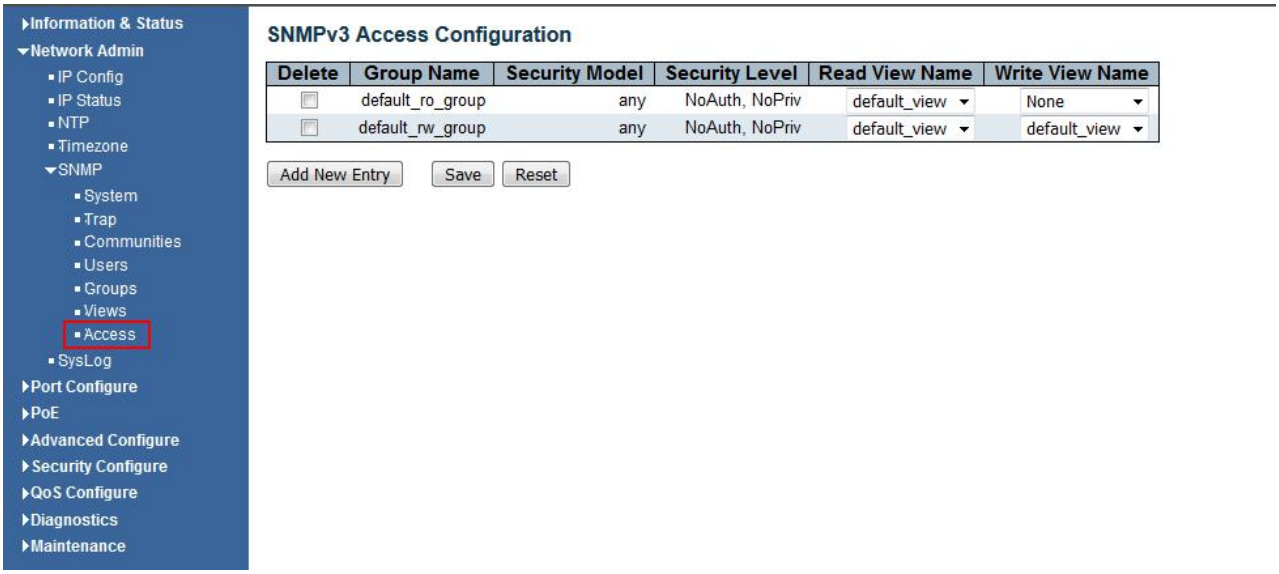
5. Users can create a new view of SNMPv3. Click the "Network Admin-SNMP-Views" as follows:



Configuration Items	Description
View Name	Enter the name

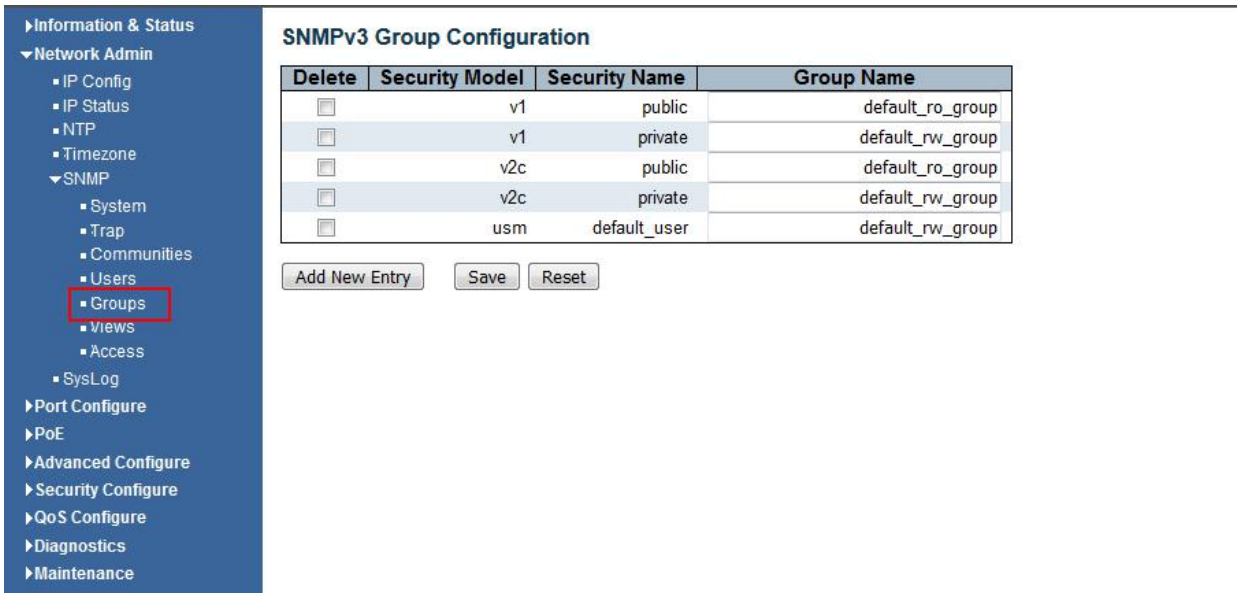
View Type	Select from included and excluded by dropping down the list
OID Subtree	Enter the OID subtree, e.g. 1.2

6. Users can call the created Views through a new Access. Click the “Network Admin-SNMP-Access” as follows:



Configuration Items	Description
Group Name	Enter the name
Security Model	Select from any, v1, v2c, and usm by dropping down the list
Security Level	Select a method of encryption from noAuthnoPriv, authNoPriv, and authPriv by dropping down the list
Read View Name	Choose a created view by dropping down the list
Write View Name	Choose a created view by dropping down the list

7. Users can call the created Users and Access through a new Group. Click the “Network Admin-SNMP-Groups” as follows:



Configuration Items	Description
Security Model	Select from v1, v2c and usm by dropping down the list
Security Name	Drop down and select from the created usernames, group names (v1 v2c), and the usernames (usm)
Group Name	Enter the allowed access name

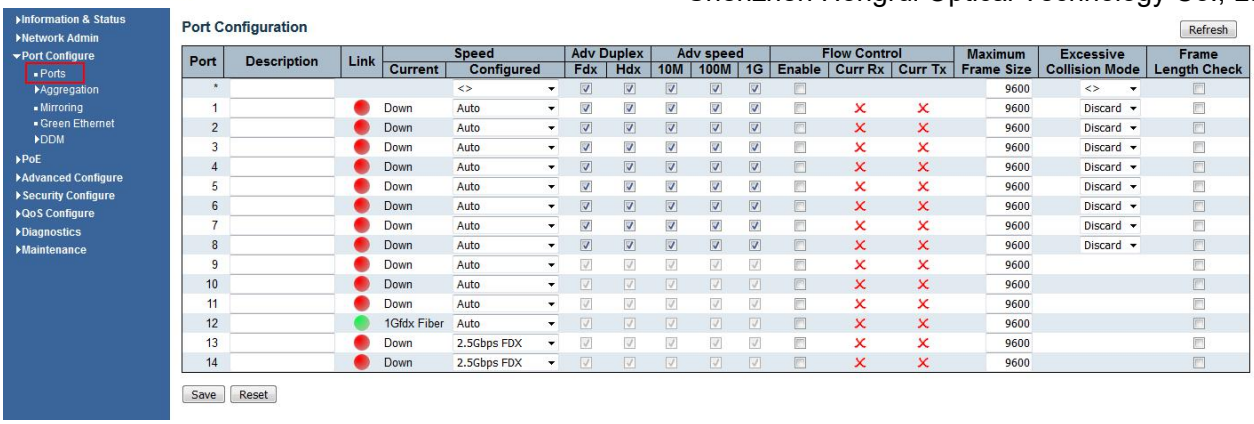
4 Port Configure

4.1 Ports

Interfaces should be identified so that users can inquire and configure Ethernet interfaces as required.

Instructions

1. Click the “Port Configure-Ports” in the navigation bar.
2. Select the data for configuration and the port description of configuration items, “Autonegotiation”, “Flow Control”, and “Maximum Frame Size” as follows.



Configuration items are as follows.

Configuration Items	Description
Autonegotiation	Configurable autonegotiation with mandatory 10 Mb, 100 Mb and 1,000 Mb statuses. Interface rates including 10 Mbits/s, 100 Mbits/s and 1,000 Mbit/s are available to Ethernet electrical interfaces and are optional as required; ports 13 and 14 support a 2.5G rate.
Flow Control	After it is enabled on both local network and opposite network devices, the local one will notify the other to stop sending messages in the presence of network congestion. The opposite one will execute the command temporarily to ensure zero message loss. Disable-Disabled reception and transmission of PAUSE frame; Rx (RX Pause)-To receive the PAUSE frame; Both (Rx/Tx Pause)-To receive and transmit the PAUSE frame; Tx (Tx Pause)-To transmit the PAUSE frame.
Maximum Frame Size	9,600
Enabled	Switch the ports
Port Description	Describable ports

📖 Description：

Ports 13 and 14 support a 2.5G rate.

4.2 Aggregation

Link Aggregation increases bandwidth and reliability by bundling a group of physical interfaces into a single logical interface.

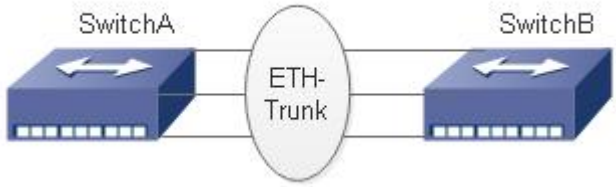
Link Aggregation Group (LAG) is a logical link bundled by multiple Ethernet links (Eth-Trunk).

Ceaselessly expanding network size increases users' demands of link bandwidth and reliability. Traditionally, high-speed interface board or the compatible equipment is usually replaced to optimize bandwidth, which is expensive and inflexible.

Link Aggregation Technology bundles multiple physical interfaces into a single logical interface without upgrading hardware. Its backup mechanism not only improves reliability, but also shares the flow load on different physical links.

As shown below, Switch A is linked with Switch B through three Ethernet links which are bundled into an Eth-Trunk logical link. Its bandwidth equals to that of the three links in total, thus broadening the bandwidth. Meanwhile, these three links back up mutually to be more reliable.

Link Aggregation diagram



Link Aggregation can meet the following demands:

Insufficient bandwidth of two switches connected with one link.

Insufficient reliability of two switches connected with one link.

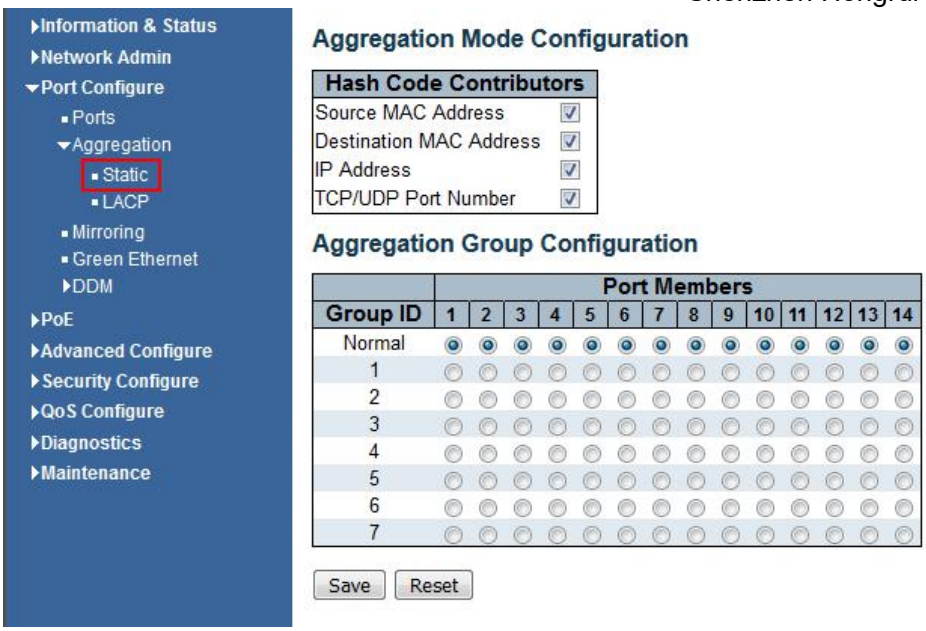
Link Aggregation can be divided into Manual Mode and LACP Mode in accordance with Link Aggregation Control Protocol (LACP) status.

In the first mode, Eth-Trunk establishment, member interface access should be added manually without LACP. It is also called the Load-sharing Mode because all links are involved in data forwarding and load sharing. In case any active link fails, LAG will average load with the remaining ones. This mode is preferred under the circumstance that two directly-connected devices require a larger link bandwidth but has no access to LACP.

4.2.1 Static

Instructions of adding a Static Link Aggregation (i.e. manual mode):

1.Click the "Port Configure-Aggregation-Static" to "Add a static link aggregation"; select a Group ID (1-16), a load-sharing method (Src Mac, Dst Mac, IP Address, TCP/UDP Port Number) and a port for aggregation; and click the "Add" option as follows.

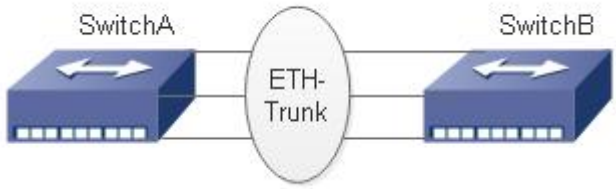


Interface data are as follows

Configuration Items	Description
Group ID	There are 16 aggregation groups and LAG IDs numbering from 1 to 16.
Load-sharing Method	Src Mac, Dst Mac, IP Address, TCP/UDP Port Number
Port List	Up to 8 ports are available.

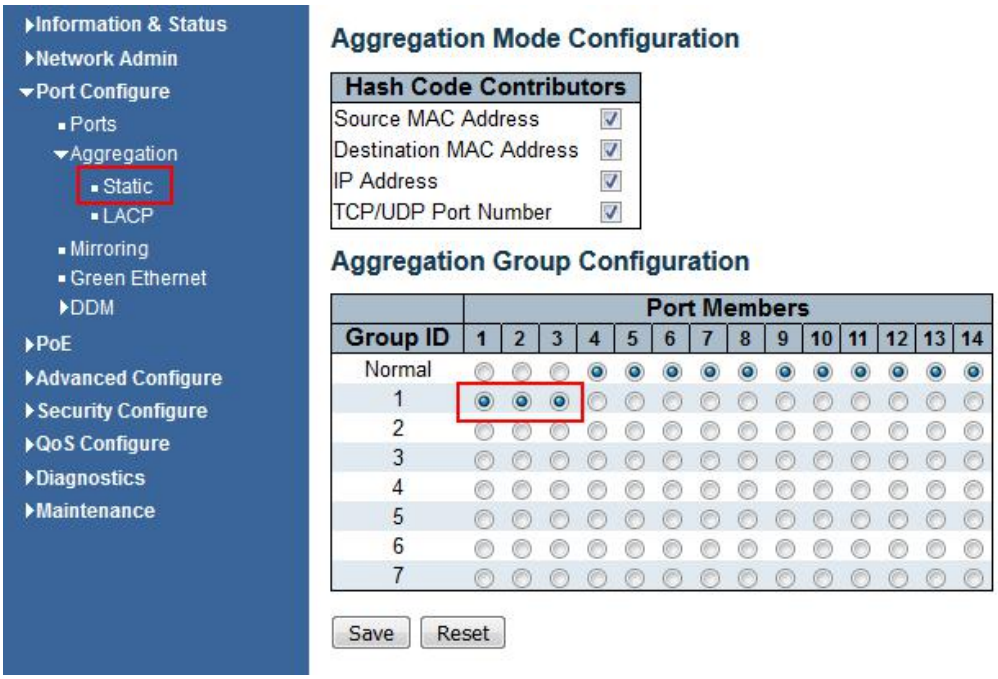
Illustrations

Ethernet Switch A aggregates 3 ports from GE1 to GE3 to Switch B, so as to share the load of each member port. The following configurations are exampled by means of static aggregation.



Instructions

1. Similar to the step of Switch B configuration, Switch A creates an Eth-Trunk interface and accesses member interfaces, in order to broaden link bandwidth. Click the “Port Configure-Aggregation-Static” to “Add a static link aggregation” to select the Group ID “1”, a load-sharing mode (Src Mac, Dst Mac, IP Address), and a port to be aggregated (GE1-1, GE1-2, and GE1-3) as follows.



4.2.2 LACP

Dynamic Link Aggregation

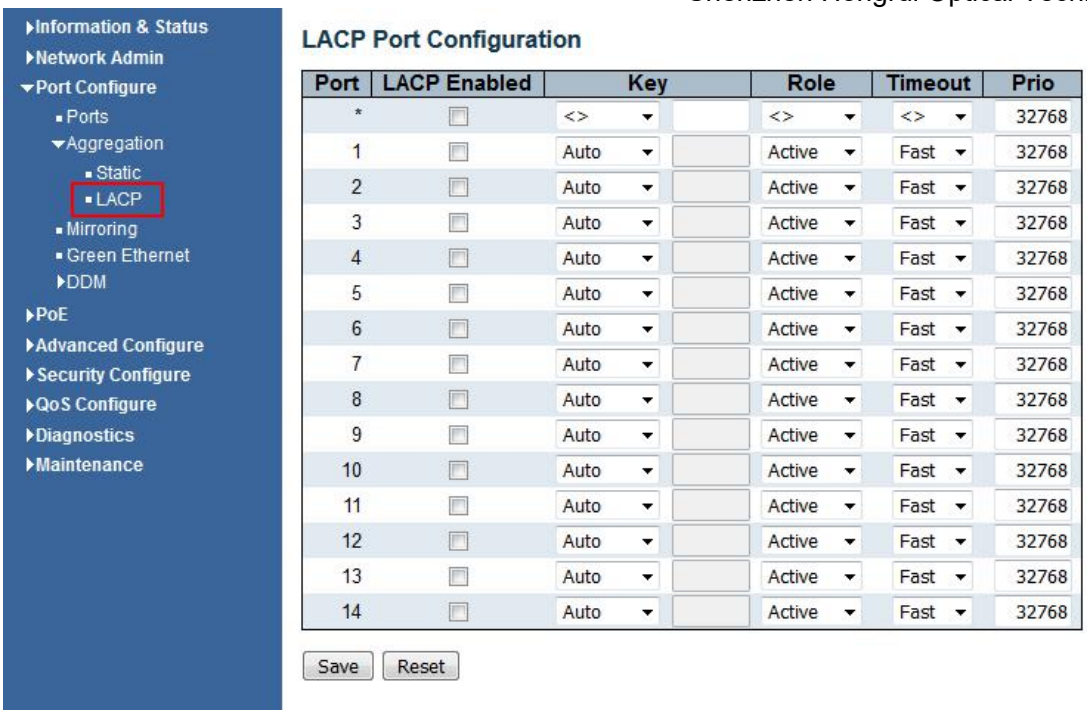
LACP (Link Aggregation Control Protocol), based on IEEE 802.3ad Standard, dynamically aggregates and disaggregates links. LACP exchanges info with the opposite network device through LACPDU (Link Aggregation Control Protocol Data Unit).

After a port uses LACP, it will inform the opposite network device of system priority, system MAC, port priority and No., and operation Key by sending a LACPDU. The opposite device will compare such info with that saved by other ports after receiving it, thus reaching an agreement on port participation in or quitting from a dynamic aggregation.

Dynamic LACP aggregation is automatically created or deleted by system, that is, internal ports can be added or removed by themselves. Only the ports connected to a same device with the same rate, duplex, and basic configuration can be aggregated.

Instructions for adding a dynamic link aggregation:

1. Click the “Port Configure-Aggregation-LACP” in the navigation bar to select a port, a type (LACP), a mode (Active or Passive), and a port priority (from 0-65,535, with 32,768 by default) as follows.



Interface data are as follows

Configuration Items	Description
LACP Enabled	Enabled and Disabled
Mode	Active or Passive Passive Port sends LACP packets manually and responds to the packets sent by the opposite network device only. Active Port sends LACP data package automatically. The links with one or two active LACP ports can be dynamically aggregated. However, it won't occur to two connected passive LACP ports since both of them are waiting for the packet from the other side.
Port Priority	LACP will determine the group member of dynamic aggregation based on the port ID priority. Among them, device ID consists of 2-byte system priority and 6-byte system MAC. In other words, a device ID is made up of the system priority and MAC. Compare the system priority first and the system MAC address next if they are the same. One with smaller value will be preferred. Scope: 0 to 65,535, with 32,768 by default.
Key	Auto and Manual Modes

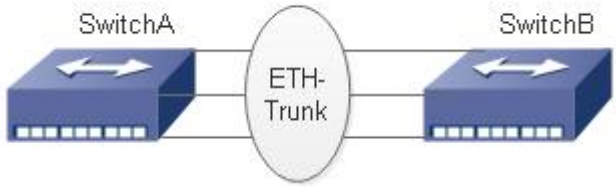
📖 Description:

Please make sure that there is no member interface access to Eth-Trunk before changing its work pattern, otherwise it won't be changed.

Work patterns of the local and opposite network devices should be the same.

Illustrations

Ethernet Switch A aggregates 3 ports from GE1 to GE3 to Switch B, so as to share the load of each member port. The following configurations are exampled by means of dynamic aggregation.



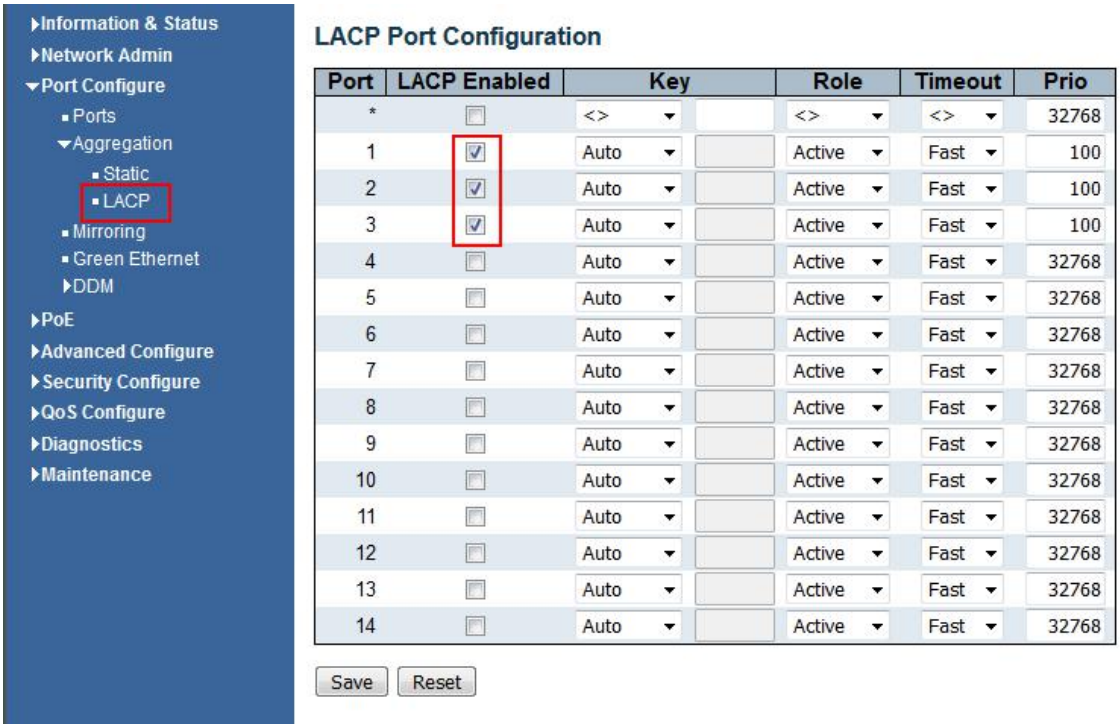
Instructions

📖 Description:

The followings are configuration of Switch A only, which should stay the same with those of Switch B to aggregate ports.

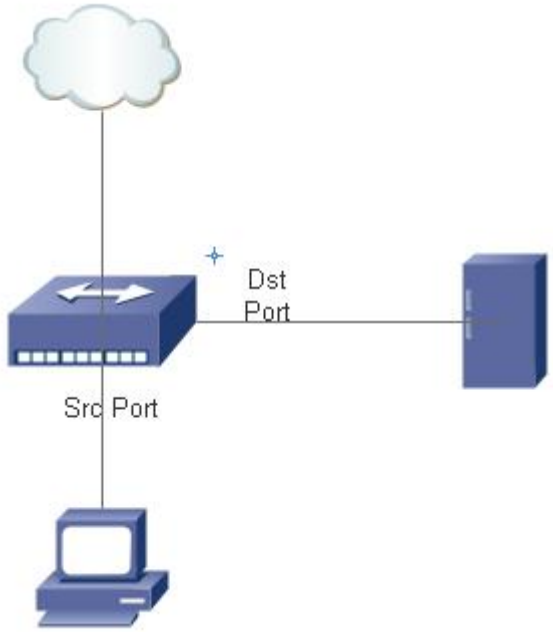
Instructions

1. Set the system priority to Level 100 on Switch A to serve as the LACP active port. Click the "Port Configure-Aggregation-LACP" in the navigation bar to set the priority to "100" as follows.



4.3 Mirroring

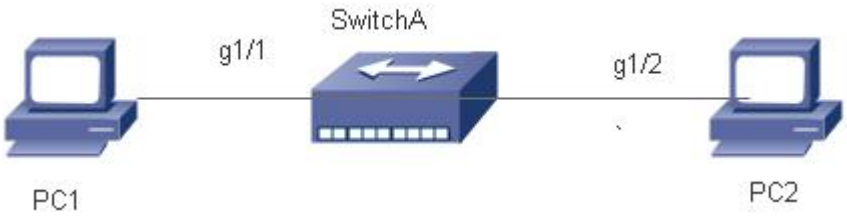
Port Mirroring copies the message of a specified switch port to a destination port. The copied port is the Source Port, and the copying port is the Destination Port. Destination Port will make use of data inspection devices for users to analyze the received messages to monitor and troubleshoot the network as follows:



Configuration example

PC1 accesses Switch A through interface GE1-1, and PC2 is directly connected to interface GE1-2.

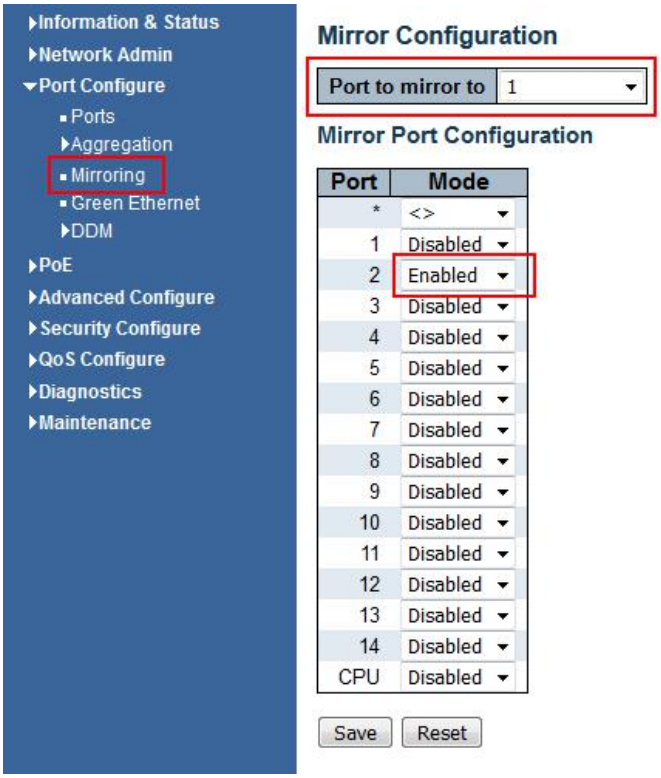
Users intend to monitor the messages sent from PC2 to PC1 by relevant devices.



Instructions

1. Click the “Port Configure-Mirroring” in the navigation bar to select a session ID.

2. Check the source port GE1-2, select the destination port GE1-1 and the “Enabled” mode, and add them as follows.



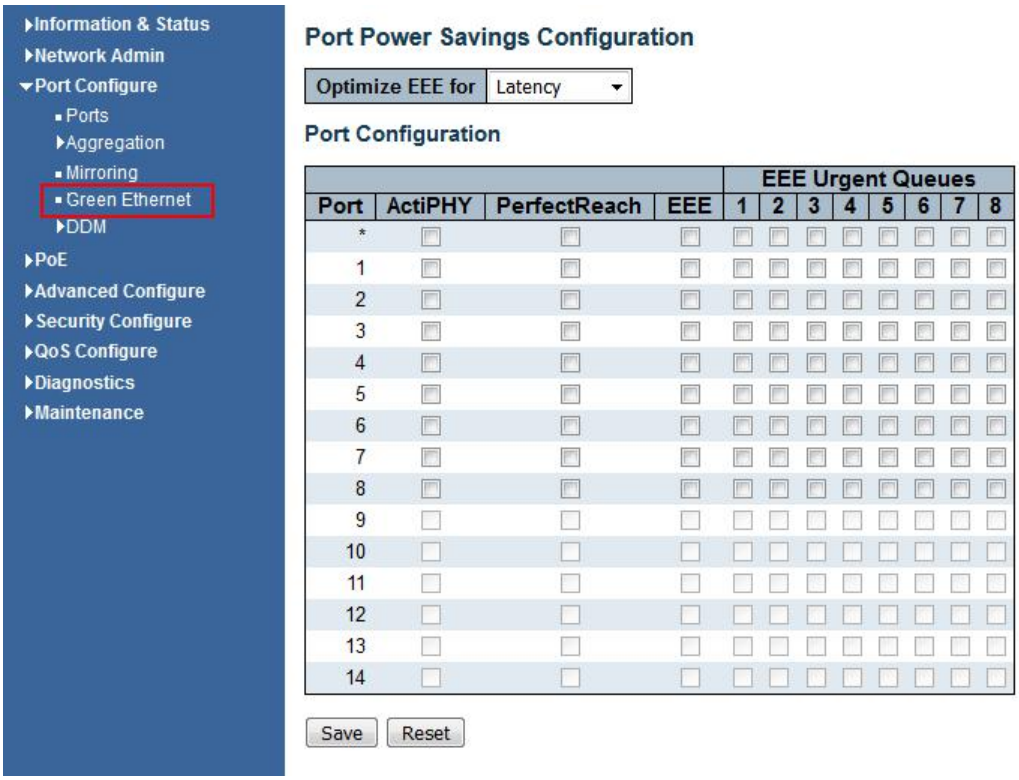
Interface data are as follows

Configuration Items	Description
Source Port	Multiple ports are available.
Destination Port	Only one port can be selected, excluding link sink port and source port.
Direction	Tx “Mirroring Ingress Port”: any received message will be mirrored to the destination port. Rx “Mirroring Egress Port”: any sent message will be mirrored to the destination port. Enable “Mirror Ingress/Egress Port” mirrors all sent and received messages to the destination port.

4.4 Green Ethernet

Port power will be turned down in case of zero or less flow.

Click the “Port Configure-Green Ethernet” as follows:



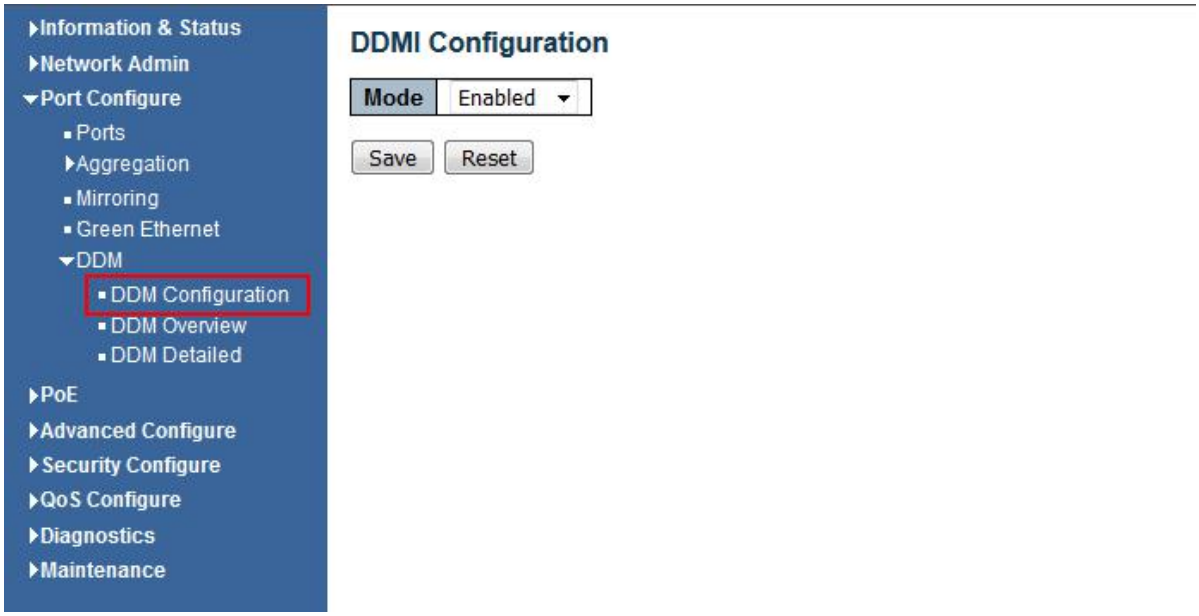
Interface data are as follows

Configuration Items	Description
Optimize EEE for	Select from power and latency
Port Configuration	Select from “ActiPHY, PerfectReach, EEE, and EEE Urgent Queues”

4.5 DDM

DDM can view the info of the optical module.

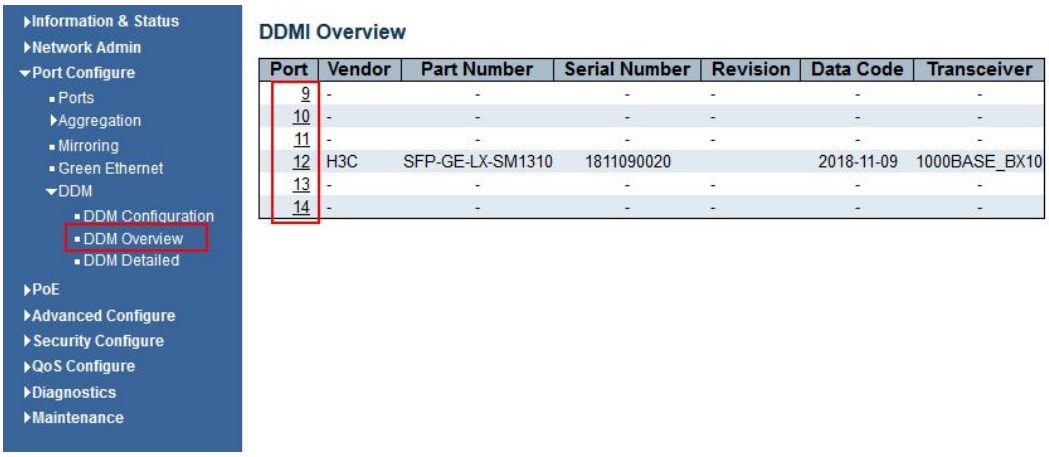
1. Click the “Port Configure-DDM-DDMI Configuration” as follows:



Interface data are as follows

Configuration Items	Description
DDMI Configuration	Enabled and Disabled

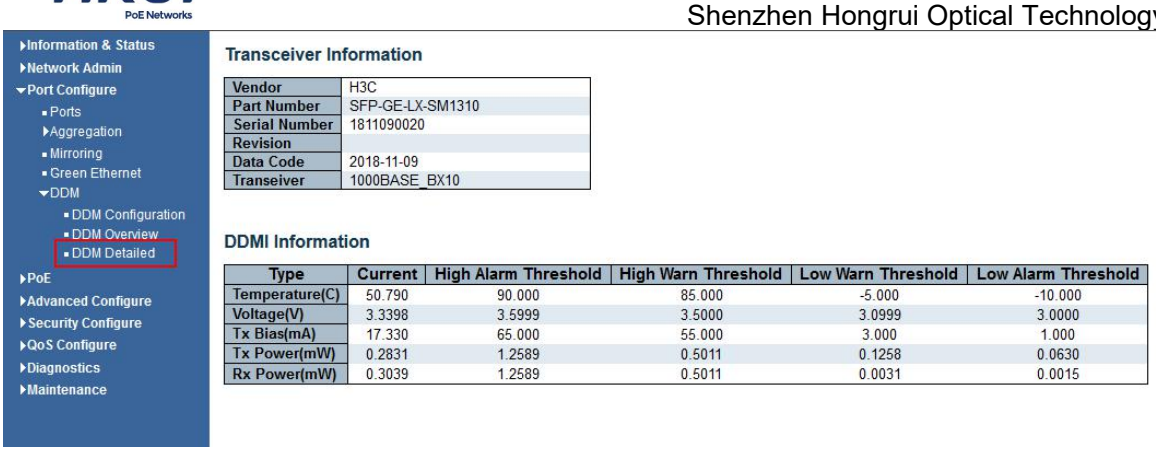
2. Click the “Port Configure-DDM-DDMI Overview” as follows:



Interface data are as follows

Configuration Items	Description
DDMI Overview	Display the info of “Port, Vendor, Part Number, Serial Number, Revision, Data Code, and Transceiver”

3. Click the “Port Configure-DDM-DDM Detailed” as follows:



Interface data are as follows

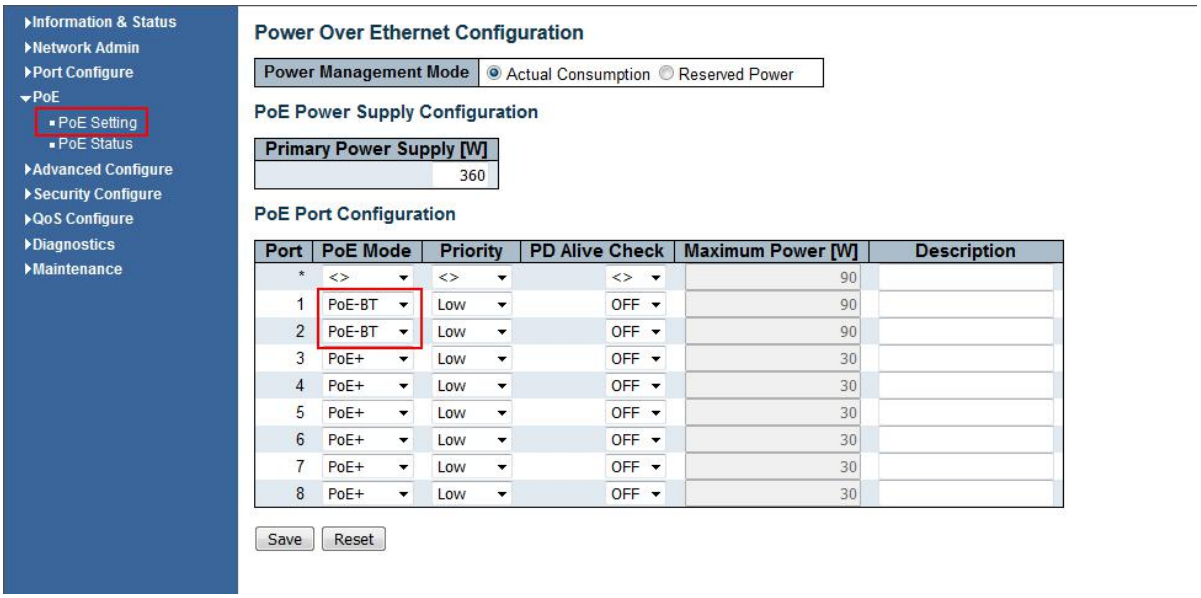
Configuration Items	Description
DDMI Detailed	Display the info of “Transceiver Information and DDMI Information”

5 PoE

PoE (Power over Ethernet) transmits data signal for the terminals based on IP (e.g. IP phone, WAP, and IP camera) and supplies the devices with direct current, without changing the existing Cat-5 network cabling status. It ensures safe structured cabling and normal network operation to minimize the cost.

5.1 PoE Setting

1. Click the “PoE- PoE Setting” in the navigation bar as follows.



Interface data are as follows

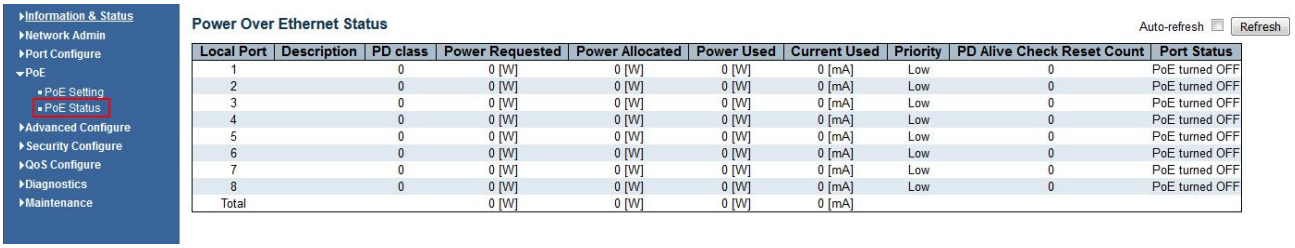
Configuration Items	Description
Power Reserve Mode	Two modes are available in this switch: Auto distribution: Switch port allocates the max power automatically subject to the inspected PD Class. Please refer to the definitions of 802.3af/802.3at in the corresponding power table. Manual distribution: The max reserved power will be defined by users.
Power Management Mode	Two modes are available in this switch: 1. Actual consumption: In this work pattern, the port with the lowest priority will be turned off when the actual consumed power is more than the rated power of switch. The port with the highest priority will be turned off if all priorities are at the same level. 2. Reserved power: In this work pattern, the port with a new PD device will be disabled when the max reserved power of all ports exceeds the rated power of the switch.
Max (Rated) Power Supply	Users can set the max power (120W by factory default) by themselves.
PoE Mode	The switch supports 802.3af (PoE) and 802.3at (PoE+) and 802.3bt modes. And 802.3at is the factory default.
Priority	Specify the priority of PoE port from low to high (Low, High, Critical)
Maximum Power (W)	“Manual Allocation” mode for power reservation specifies the max power supply of the port.

📖 Description：

Port 1 and port 2 support 802.3bt.

5.2 PoE Status

1. Click the “PoE-PoE Status” as follows.



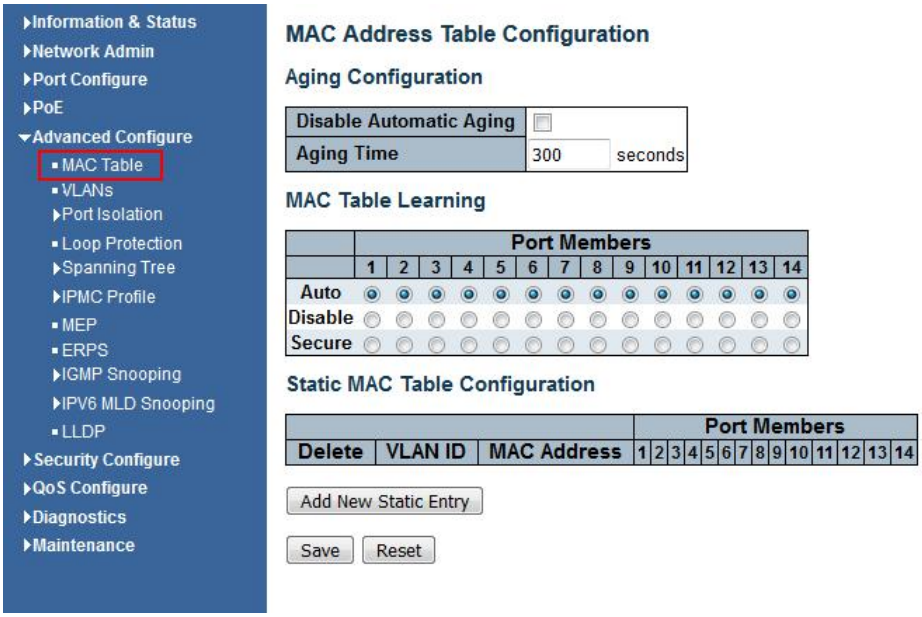
Interface data are as follows

Configuration Items	Description
Power Over Ethernet Status	Display the info of “Local Port, Description, PD Class, Power Requested, Power Allocated, Power Used, Current Used, Priority, and Port Status”

6 Advanced Configure

6.1 MAC Table

Users can adjust the configurations related to MAC address in the switch.
Click the “Advanced Configure-MAC Table” as follows:



Interface data are as follows

Configuration Items	Description
Disable Automatic Aging	The dynamic MAC address learned by the switch won’t age automatically if this option is checked.
Aging Time	The dynamic MAC address learned by the switch will automatically age after 300s by factory default. The period ranges from 10s to 1,000,000s.
Learn the MAC Address Table	The switch is compatible with 3 learning modes of MAC address: Auto mode: ports will learn the MAC address automatically; Disabled mode: ports won’t learn MAC address; Safe mode: ports forward the data flow of the configured static (source) MAC addresses.

6.2 VLANS

VLAN is formulated without the restrictions of physical locations, which means the hosts in a same VLAN can be placed separately. As shown below, each VLAN, as a broadcast domain, divides a physical LAN into several logical LANs. Hosts can exchange messages in a traditional communication way. For those in different VLANs, devices such as routers or Layer 3 switches are necessary.

VLAN is superior to the traditional Ethernet in terms of:

Broadcast domain coverage: the broadcast message in a LAN is limited in a VLAN to save the bandwidth and handle the network-related issues more efficiently.

LAN secuirty: VLAN hosts fail to communicate with each other since the messages are separated by the broadcast domain in the data link layer. They need a router or a Layer 3 switch for Layer 3 forwarding.

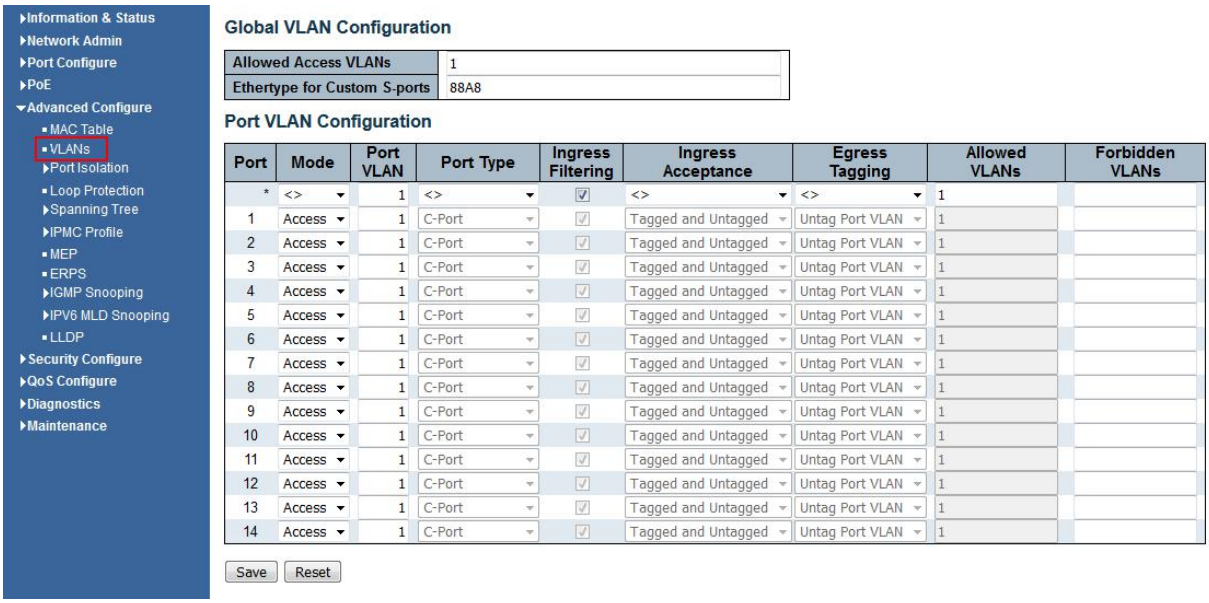
Flexibility of creating a virtual working team: VLAN can create a virtual working team beyond the control of physical network. Users have access to the network without changing the configuration if their physical locations are moving within the scope.

This management switch supports VLAN types based on IEEE 802.1Q, protocols, MAC, and ports. For default configuration, 802.1Q VLAN mode should be adopted.

Port-based VLAN is divided subject to a switch's interface No. Network administrator give each switch interface a different PVID, namely a port default VLAN. If a data frame without a VLAN tag flows into a switch interface with a PVID, it will be marked with the same PVID, or it will get rid of an additional tag even though the interface has a PVID.

The solution to a VLAN frame depends on the interface type, which eases member definition but re-configures VLAN in case of member mobility.

1. Click the "Advanced Configure-VLANs" as follows.



Interface data are as follows.

Configuration Items	Description
Allowed Access	Display the ID List of allowed access VLANs, with VLAN 1

VLANs	by factory default. Add an ID for a new VLAN.
Ethertype for Custom S-ports	This field specifies the Ethertype/TPID (specified in hexadecimal) used for Custom S-ports. The setting is in force for all ports whose Port Type is set to S-Custom-Port.
Mode	The port mode (default is Access) determines the fundamental behavior of the port in question. A port can be in one of three modes as described below. Whenever a particular mode is selected, the remaining fields in that row will be either grayed out or made changeable depending on the mode in question. Grayed out fields show the value that the port will get when the mode is applied. Access: Access ports are normally used to connect to end stations. Access ports have the following characteristics: • Member of exactly one VLAN, the Port VLAN (a.k.a. Access VLAN), which by default is 1 • Accepts untagged and C-tagged frames • Discards all frames that are not classified to the Access VLAN • On egress all frames classified to the Access VLAN are transmitted untagged. Other (dynamically added VLANs) are transmitted tagged Trunk: Trunk ports can carry flow on multiple VLANs simultaneously, and are normally used to connect to other switches. Trunk ports have the following characteristics: • By default, a trunk port is member of all VLANs (1-4094). • The VLANs that a trunk port is member of may be limited by the use of Allowed VLANs. • Frames classified to a VLAN that the port is not a member of are discarded. • By default, all frames but frames classified to the Port VLAN (a.k.a. Native VLAN) get tagged on egress. Frames classified to the Port VLAN do not get C-tagged on egress.

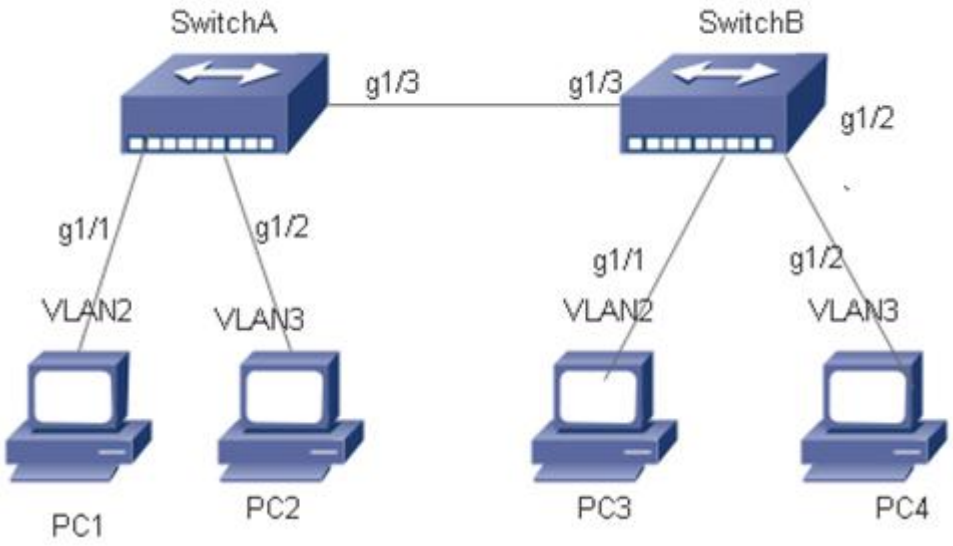
	• Egress tagging can be changed to tag all frames, in which case only tagged frames are accepted on ingress. Hybrid: Hybrid ports resemble trunk ports in many ways, but adds additional port configuration features. In addition to the characteristics described for trunk ports, hybrid ports have these abilities: • Can be configured to be VLAN tag unaware or, C-tag aware, S-tag aware, or S-custom-tag aware; • Ingress filtering can be controlled; • Ingress acceptance of frames and configuration of egress tagging can be configured independently;
Port VLAN	Determines the port's VLAN ID (a.k.a. PVID). Allowed VLANs are in the range 1 through 4094, default being 1. On ingress, frames get classified to the Port VLAN if the port is configured as VLAN unaware, the frame is untagged, or VLAN awareness is enabled on the port, but the frame is priority tagged (VLAN ID = 0). On egress, frames classified to the Port VLAN do not get tagged if Egress Tagging configuration is set to untag Port VLAN. The Port VLAN is called an "Access VLAN" for ports in Access mode and Native VLAN for ports in Trunk or Hybrid mode.
Port Type	Ports in hybrid mode allow for changing the port type, that is, whether a frame's VLAN tag is used to classify the frame on ingress to a particular VLAN, and if so, which TPID it reacts on. Likewise, on egress, the Port Type determines the TPID of the tag, if a tag is required. Unaware: On ingress, all frames, whether carrying a VLAN tag or not, get classified to the Port VLAN, and possible tags are not removed on egress. C-Port: On ingress, frames with a VLAN tag with TPID = 0x8100 get

	classified to the VLAN ID embedded in the tag. If a frame is untagged or priority tagged, the frame gets classified to the Port VLAN. If frames must be tagged on egress, they will be tagged with a C-tag. S-Port: On ingress, frames with a VLAN tag with TPID = 0x8100 or 0x88A8 get classified to the VLAN ID embedded in the tag. If a frame is untagged or priority tagged, the frame gets classified to the Port VLAN. If frames must be tagged on egress, they will be tagged with an S-tag. S-Custom-Port: On ingress, frames with a VLAN tag with a TPID = 0x8100 or equal to the Ethertype configured for Custom-S ports get classified to the VLAN ID embedded in the tag. If a frame is untagged or priority tagged, the frame gets classified to the Port VLAN. If frames must be tagged on egress, they will be tagged with the custom S-tag.
Ingress Filter	Hybrid ports allow for changing ingress filtering. Access and Trunk ports always have ingress filtering enabled. If ingress filtering is enabled (checkbox is checked), frames classified to a VLAN that the port is not a member of get discarded. If ingress filtering is enabled (checkbox is checked), frames classified to a VLAN that the port is not a member of get discarded. However, the port will never transmit frames classified to VLANs that it is not a member of.。
Ingress Acceptance	Hybrid ports allow for changing the type of frames that are accepted on ingress. Tagged and Untagged Both tagged and untagged frames are accepted. Tagged Only Only tagged frames are accepted on ingress. Untagged frames are discarded. Untagged Only Only untagged frames are accepted on ingress. Tagged frames are discarded.
Egress Tagging	Ports in Trunk and Hybrid mode may control the tagging of

	frames on egress. Untag Port VLAN Frames classified to the Port VLAN are transmitted untagged. Other frames are transmitted with the relevant tag. Tag All All frames, whether classified to the Port VLAN or not, are transmitted with a tag. Untag All All frames, whether classified to the Port VLAN or not, are transmitted without a tag. This option is only available for ports in Hybrid mode.
Allowed VLANs	Ports in Trunk and Hybrid mode may control which VLANs they are allowed to become members of. Access ports can only be member of one VLAN, the Access VLAN. The field's syntax is identical to the syntax used in the Enabled VLANs field. By default, a Trunk or Hybrid port will become member of all VLANs, and is therefore set to 1-4094. The field may be left empty, which means that the port will not become member of any VLANs.
Forbidden VLANs	A port may be configured to never be member of one or more VLANs. This is particularly useful when dynamic VLAN protocols like MVRP and GVRP must be prevented from dynamically adding ports to VLANs. The trick is to mark such VLANs as forbidden on the port in question. The syntax is identical to the syntax used in the Enabled VLANs field. By default, the field is left blank, which means that the port may become a member of all possible VLANs.
Non-static port	Click the radio button and specify the port as a non-static port. Click the “Select all” to check all ports.

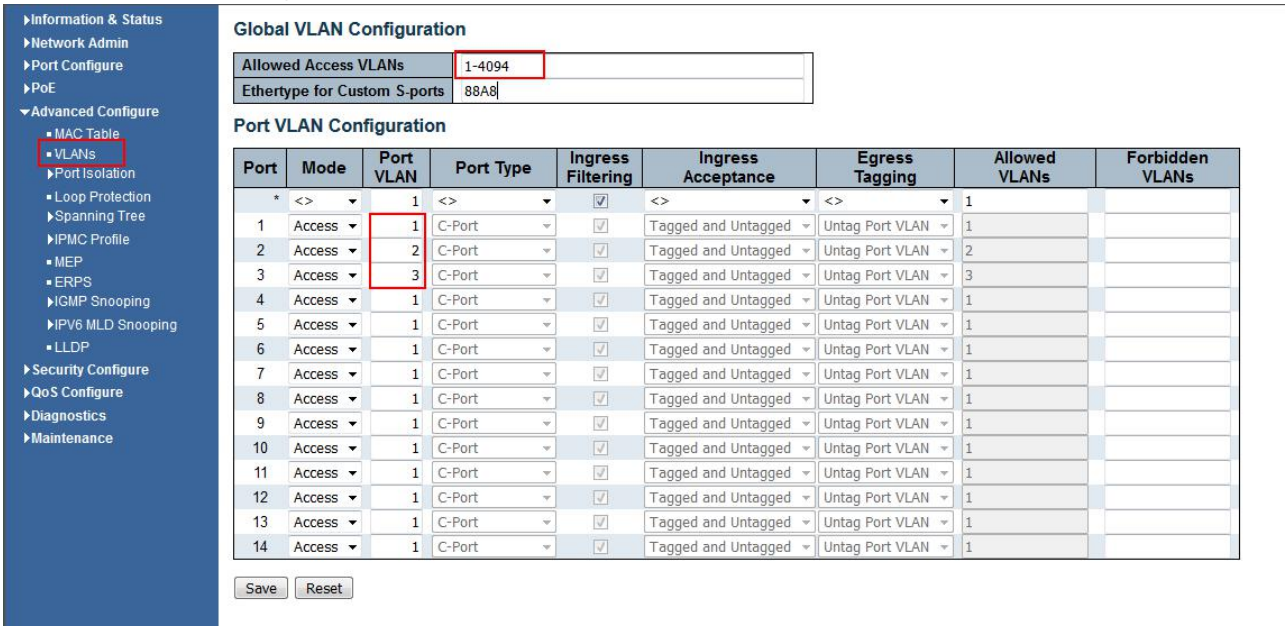
Configuration illustration

Connection interfaces and 2 VLANs should be added to support the user communication in VLAN 2 and 3 of the links between Switch A and Switch B. That is, VALN 2 and 3 should be added and the GE1-3 Ethernet Interfaces of Switch A and Switch B should be configured.



Instructions：

1. Create VLAN 2 and 3 in Switch A, add VLANs to the user interfaces, and set the GE1-3 in the trunk mode. With similar steps of Switch B, please click the “Advanced Configure-VLANs” in the navigation tree, fill in relevant items, and save the configuration as follows.



2. Configure the type of Switch A’s interface connected to Switch B, as well as the passed VLAN. With similar steps of Switch B, please click the “Advanced Configure-VLANs” in the navigation tree, fill in relevant items, and save the configuration as follows. The following shows how to add a VLAN 2, which is similar to the steps of adding VLAN 3.

3. Verify the configuration result

Configure User 1 and 2 in a same segment like 192.168.100.0/24; and configure User 3 and 4 in a same segment like 192.168.200.0/24.

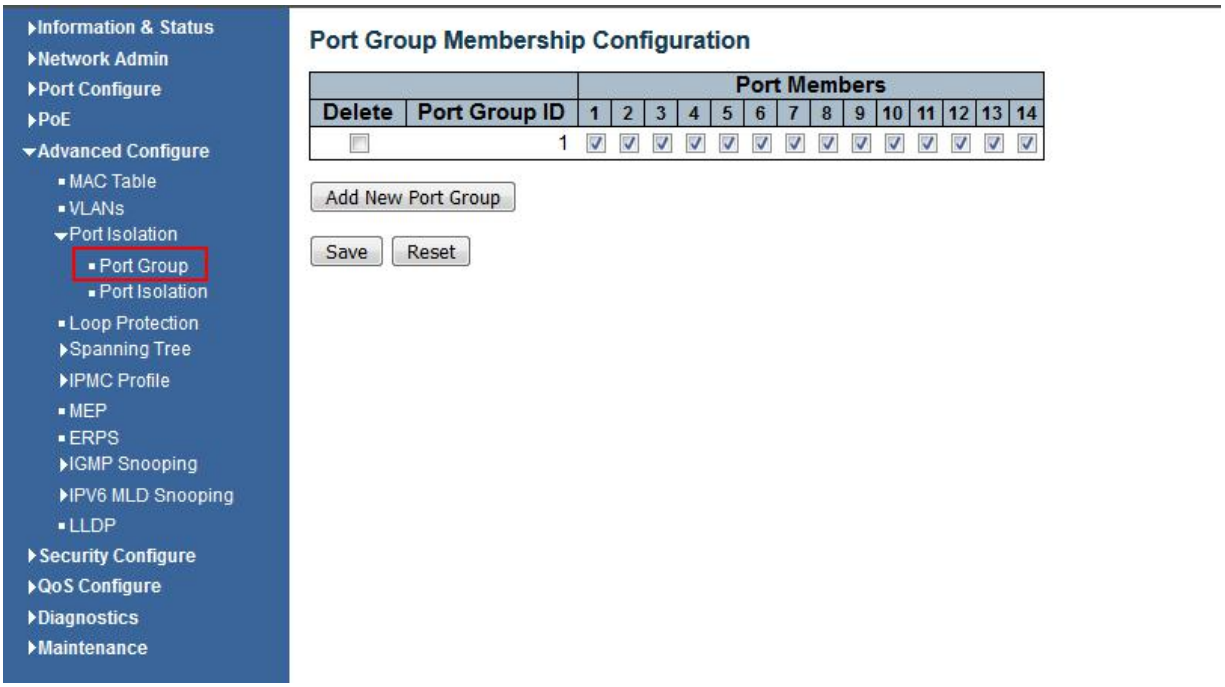
User 1 and 2 can ping each other, but they cannot ping User 3 or 4, vice versa.

6.3 Port Isolation

Port Group

One port can be subordinate to multiple port groups at the same time. Any two ports can forward data flow if they are in a same group.

1. Click the “Advanced Configure-Port Isolation”, check the port to build an isolation group, and save it as follows.

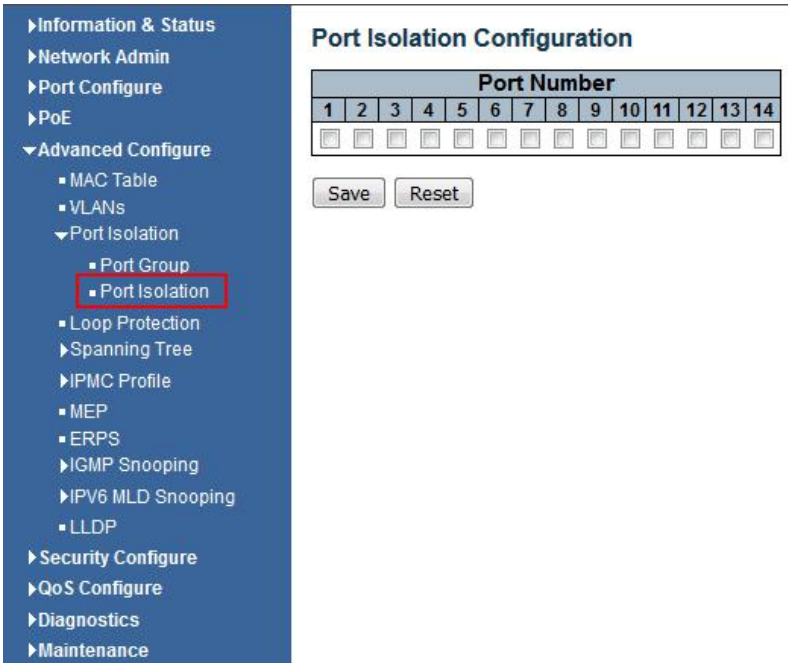


Port Isolation

The interfaces in a same group will be isolated from each other, which will not occur to those in different groups.

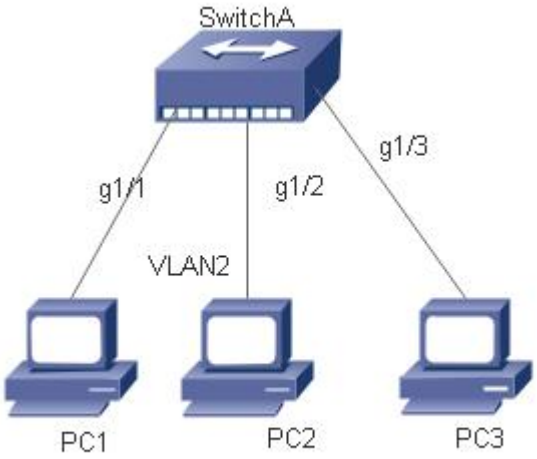
Instructions

1. Click the “Advanced Configure-Port Isolation”, check the port to build an isolation group, and save it as follows.



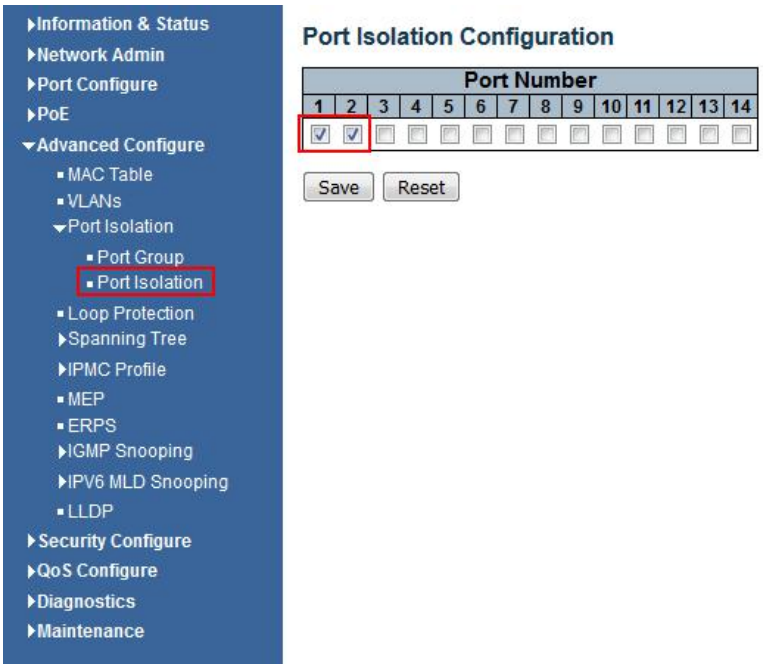
The following example shows that PC1, 2 and 3 are subordinate to VLAN 1. Users aim to block the access between PC1 and 2 in VLAN 1, but allow access between PC1 and 3, as well as PC2 and 3.

Networking diagram of port isolation configuration example



Instructions

1. For GE1-1 and GE1-2 port isolation configuration, click the “Port Configure-Port Isolation-Port Isolation”, check the port GE1-1 and GE1-2 to build an isolation group, and save it as follows.



2. Verify the configuration results

Neither PC1 nor PC2 can ping each other.

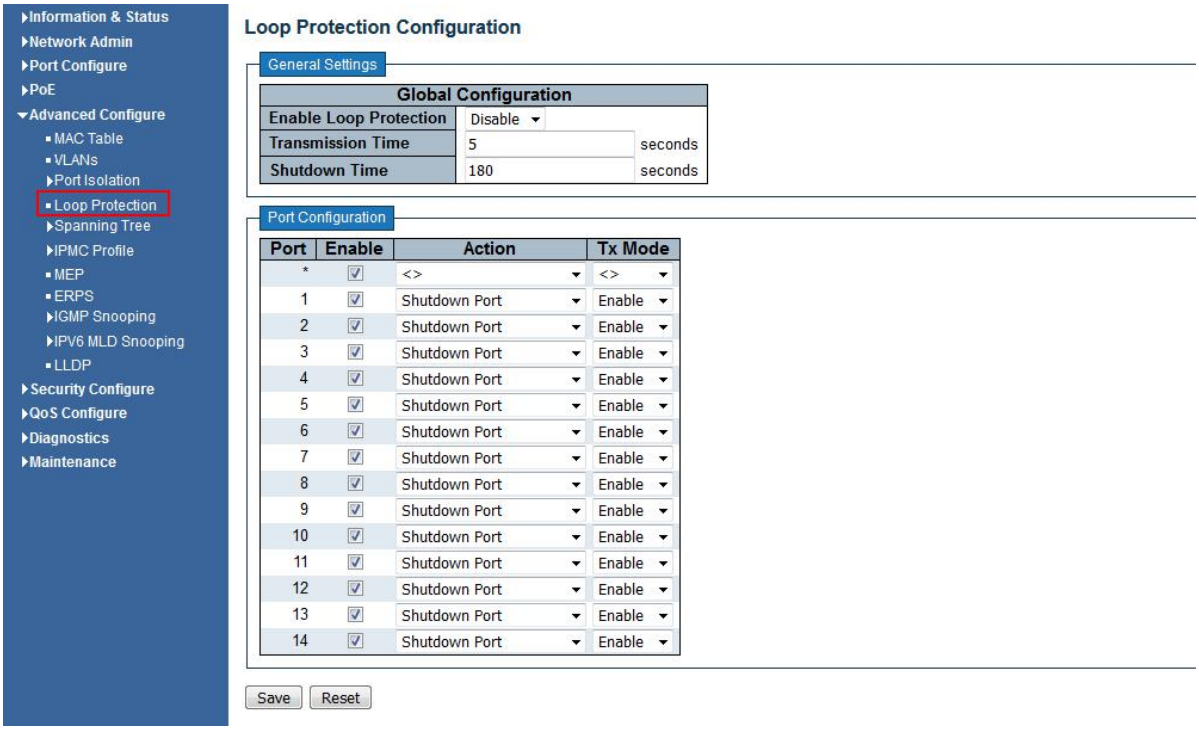
PC1 and PC3 can ping each other.

PC2 and PC3 can ping each other.

6.4 Loop Protection

Loop Protection is configured as follows: it enables the global ring network and disables the configuration of switch ports so that users can modify the inspection intervals and the port shutdown time. It configures the loops of one or more ports and determines whether to adopt auto inspection mode or not under the circumstance of enabling the global ring network. There are 3 ways to handle when a ring network is detected by ports: disabling the ports, disabling the ports while keeping logs, and keeping logs only;

Click the “Advanced Configure-Loop Protection” as follows.



Interface data are as follows.

Configuration Items	Description
General Settings	Select from Enable Loop Protection, Transmission Time, and Shutdown Time
Port Configuration	Select from Enable, Action and Tx Mode

6.5 Spanning Tree

In order to backup the links and enhance network reliability, switching Ethernet usually makes use of redundant links. However, such links will generate loops on the switching network, leading to broadcast storm, unstable MAC address list and other failures, thus worsening users' communication quality, or even interrupting the communication. As a result, STP (Spanning Tree Protocol) emerges.

Same with how other protocols are developed, from the original STP defined in IEEE 802.1D, to the RSTP (Rapid Spanning Tree Protocol) defined in IEEE 802.1W, and to the MSTP (Multiple Spanning Tree Protocol) defined in the recent IEEE 802.1S, STP keeps upgrading.

MSTP is compatible with RSTP and STP while RSTP is compatible with STP. The contrasts among these 3 protocols are as follows.

The contrasts among 3 protocols:

STP	Features	Application

STP	A loop-free tree is formed as the solution to broadcast storm and redundant backups. It converges slowly.	All VLANs share a same spanning tree without the discrimination for user or business flow.
RSTP	A loop-free tree is formed as the solution to broadcast storm and redundant backups. It converges rapidly.	
MSTP	A loop-free tree is formed as the solution to broadcast storm and redundant backups. It converges rapidly. Spanning trees balance the load among VLANs. Flow of different VLANs will be forwarded subject to paths.	User flow and business flow should be distinguished for the purpose of load sharing. Different VLANs forward flow through separate spanning trees.

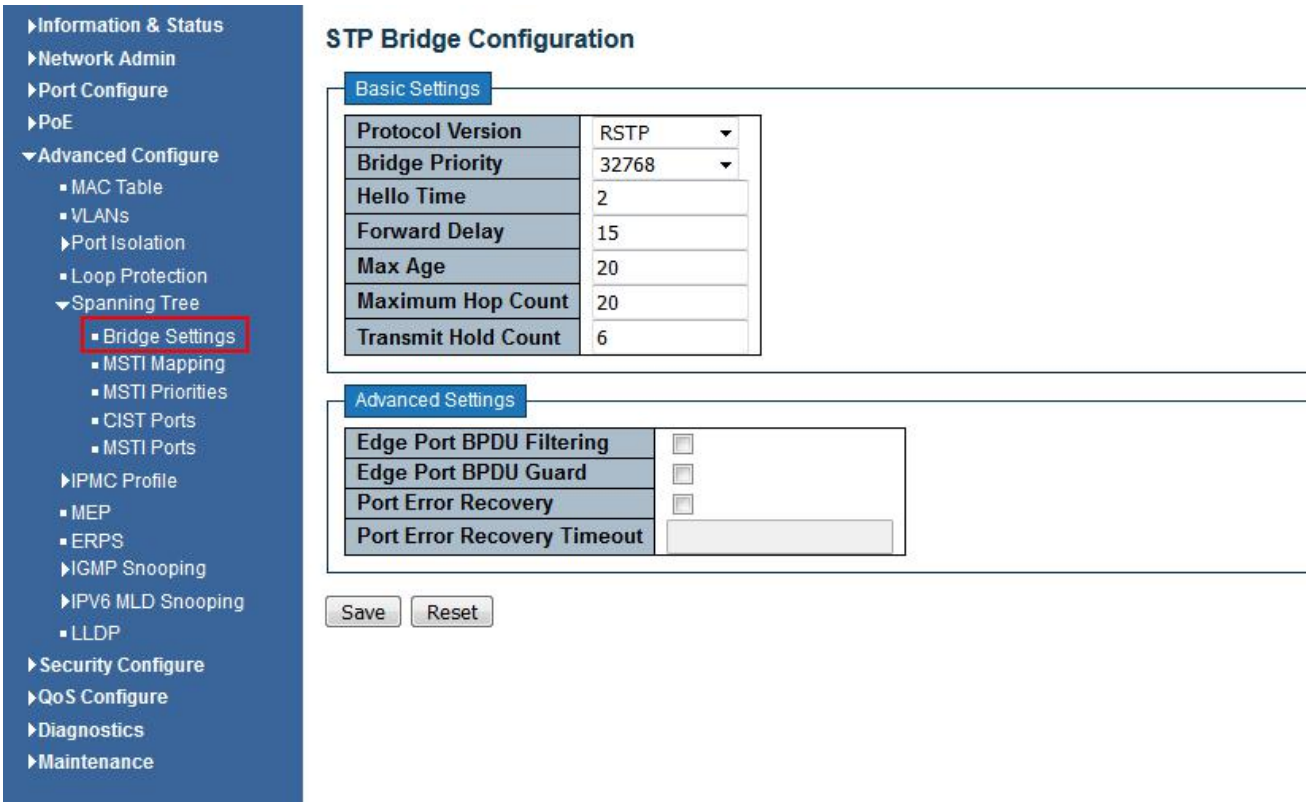
After STP is deployed, it will calculate the network loops with topology, thus achieving:

- Loop elimination: eliminate the possible communication loops in the network by blocking redundant links.
- Link backups: activate the redundant links to restore network connectivity if the active paths fail.

6.5.1 Bridge Configuration

Users can configure the global items of STP Bridge in this page.

Click the “Advanced Configure-Spanning Tree-Bridge Settings” as follows:



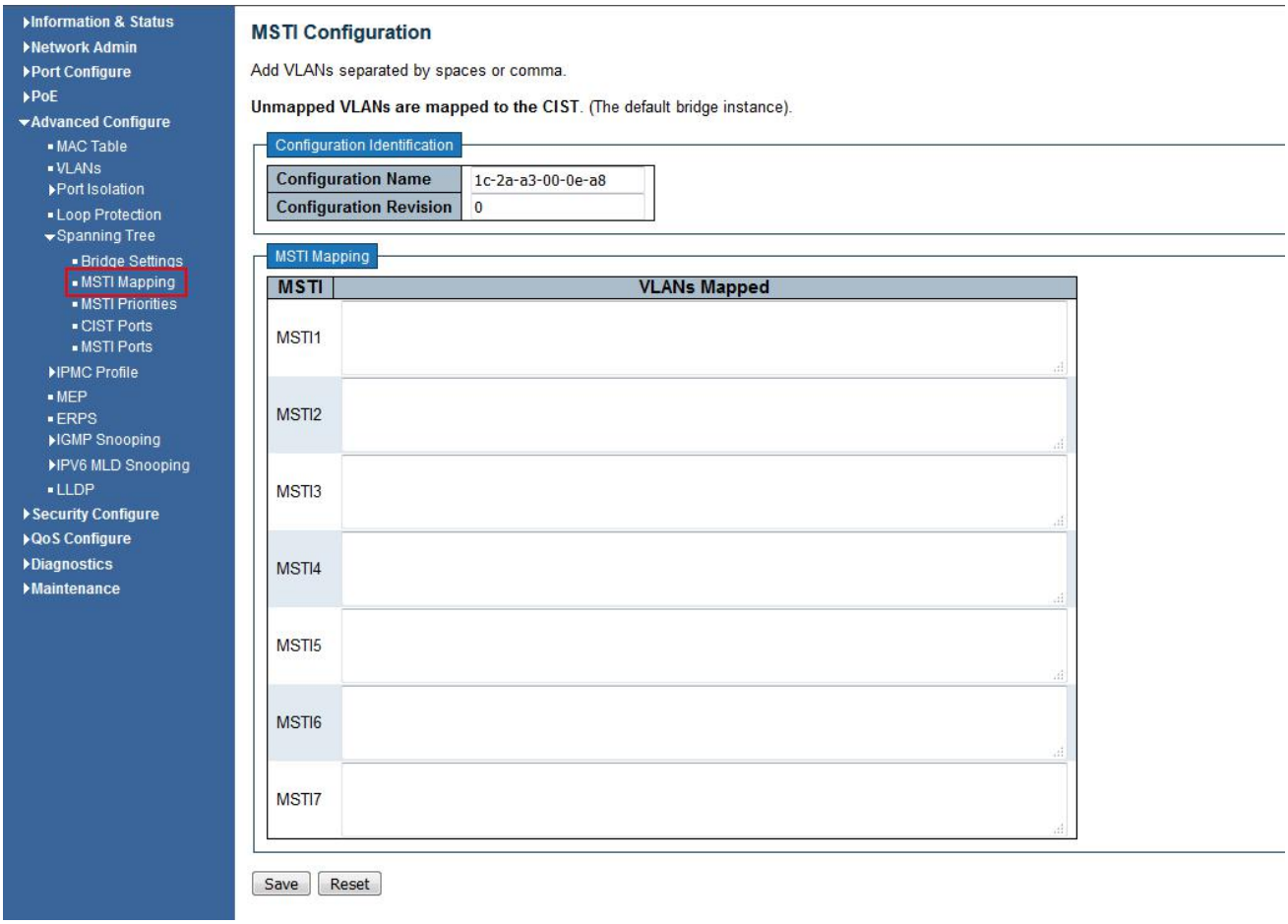
Interface data are as follows.

Configuration Items	Description
Protocol Ver.	Select the STP Ver. to be executed on the switch by dropping down the list from: STP-to globally set an STP on the switch. RSTP-to globally set a RSTP on the switch. MSTP-to globally set an MSTP on the switch.
Bridge Priority	Control the bridge priority. Lower numeric values have better priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch forms a Bridge Identifier.
Forward Delay (4-30s)	It ranges from 4s to 30s, with 15s by default.
Max Age (6-40s)	Max aging time is set to keep old information away from endless loop in redundant paths and to prevent the effective spread of new information. The aging time is 20s by default.
Max hops (6-40)	Set the hops between devices in the spanning tree area before the BPDU (Bridge Protocol Data Unit) packet sent by the switch is discarded. Hops will be reduced by one each time when a packet flows through a switch. Users can set the number of hops from 6 to 40, with 20 by default.

Transmit Hold Count (1-10)	Set the max number of Hello packets to be transmitted at each interval, ranging from 1 to 10, with 6 by default.

6.5.2 MSTI Mapping

Click the “Advanced Configure-Spanning Tree-MSTI Mapping” as follows:



Interface data are as follows.

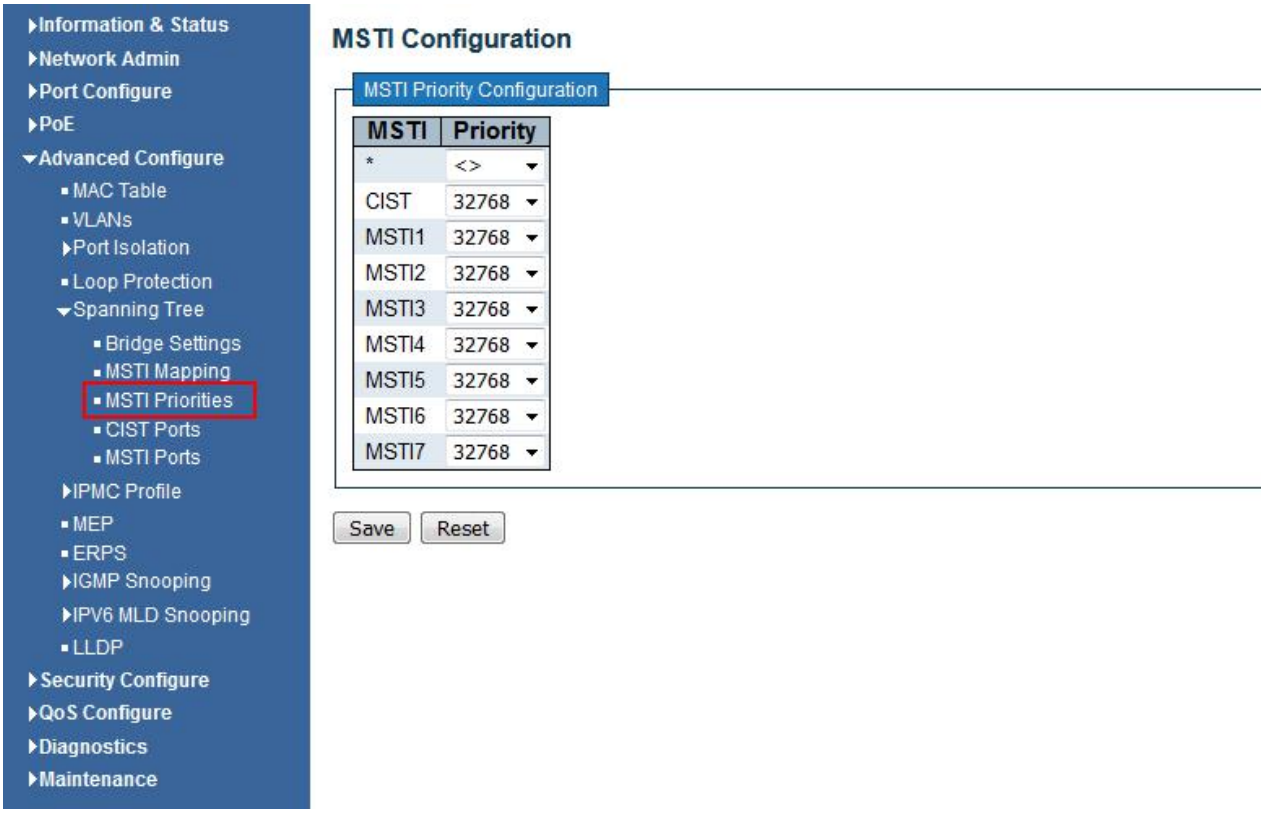
Configuration Items	Description
Configuration Name	Configure the MSTP domain name
Configuration Revision	Configuration the revision
MSTI Mapping	Enter the VLAN to be mapped

Description:

An instance is a group of VLANs that reduces communication cost and resource utilization rate. Each instance, independently calculated with topology, can balance the load. VLANs with the same topology can be mapped to a same instance, and they are forwarded according to the port status in corresponding MSTP instances.
In simple terms, one or more VLANs are mapped to a spanning tree in the MSTP instances at a time.

6.5.3 MSTI Priorities

Click the “Advanced Configure-Spanning Tree-MSTI Priorities” as follows:



Interface data are as follows.

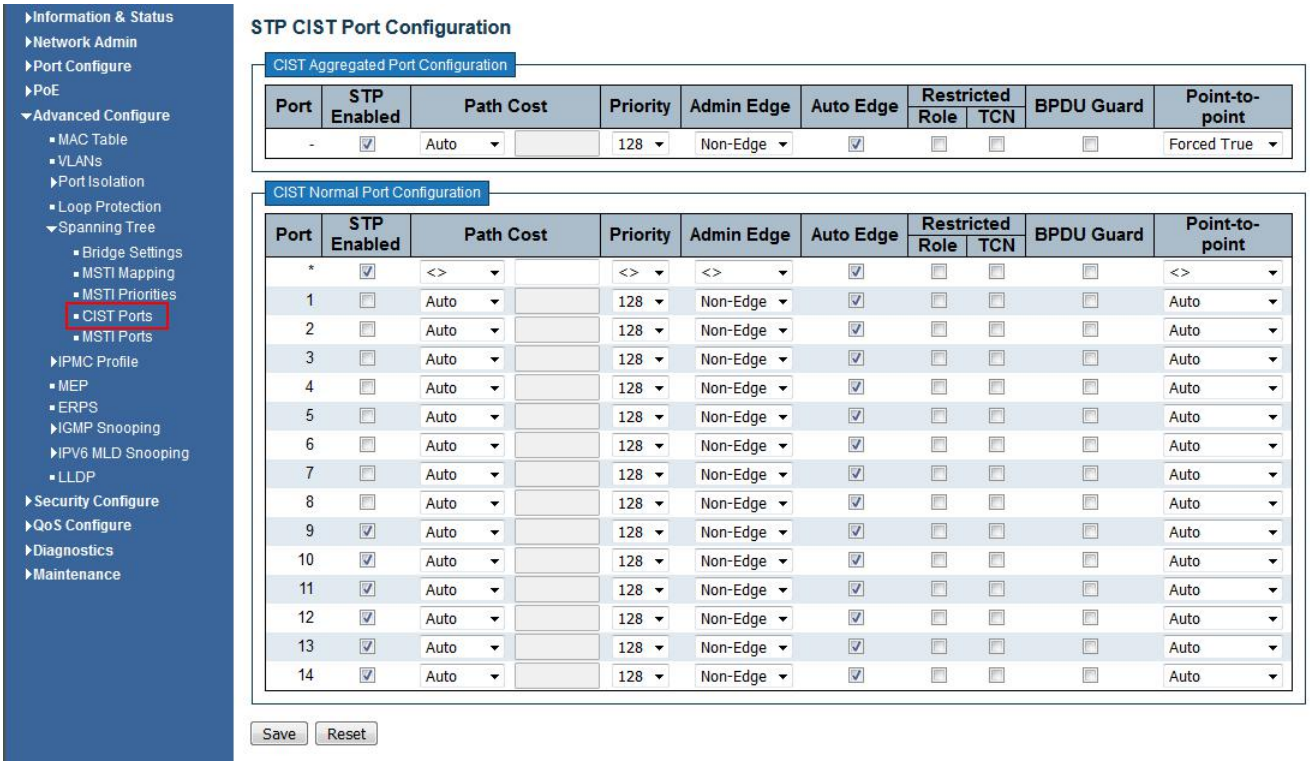
Configuration Items	Description
MSTI Priorities	The configured instance priorities range from 0 to 61,440.

Description:

Note: The configured instance priorities must be a multiple of 4,094 ranging from 0 to 61,440.

6.5.4 CIST Ports

Click the “Advanced Configure-Spanning Tree-CIST Ports” as follows:



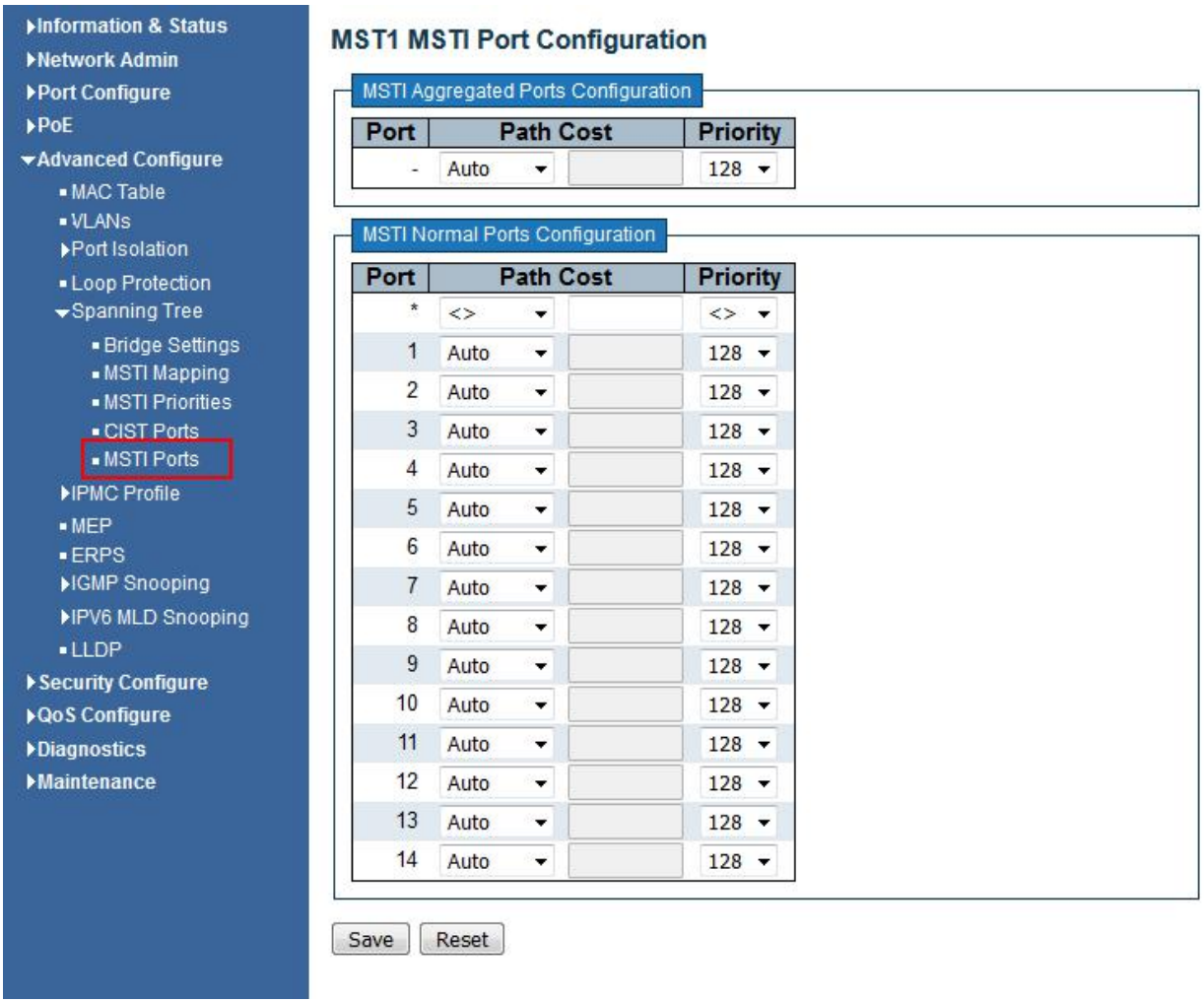
Interface data are as follows.

Configuration Items	Description
Ring Network Enabled	Check to enable the port’s STP functions.
Path Cost (0=Auto)	Automatically define the cost measure associated with forwarding packets to a specified port list, with 0 (auto) by default. The smaller the number, the more likely it will be to use this port for packet forwarding Control the path cost incurred by the port. The Auto setting will set the path cost as appropriate by the physical link speed, using the 802.1D recommended values. Using the Specific setting, a user-defined value can be entered. The path cost is used when establishing the active topology of the network. Lower path cost ports are chosen as forwarding ports in favor of higher path cost ports. Valid values are in the range from 1 to 200,000,000.

Priority	Priority will determine the forwarding state of ports when path costs are the same.
Auto Boundary	Appoint the port as a boundary port by choosing True mode. The port will be out of the boundary state by choosing “False” mode. Besides, the boundary state will be judged by the BPDU message received by the port if the “Auto” mode is chosen.
Restricted Role	Drop down the list to switch the restricted role subject to the True and False modes (with “False” mode by default). It won’t be a root port in the “True” mode.
Restricted TCN	A TCN is a simple BPDU that the bridge sends to its root port, which is switched between True and False modes, with “False” mode by default.
BPDU Protection	Port will be disabled (shut down) upon receiving a BPDU message if this function is enabled.
P2P	Links are shared peer to peer under the True mode. P2P port is similar to an edge port, with “Auto” mode by default.

6.5.5 MSTI Ports

Users can configure the priority and path cost of an instance port.
Click the “Advanced Configure-Spanning Tree-MSTI Ports” as follows:



Interface data are as follows.

Configuration Items	Description
Path Cost	Automatically define the cost measure associated with forwarding packets to a specified port list, with 0 (auto) by default. The smaller the number, the more likely it will be to use this port for packet forwarding Control the path cost incurred by the port. The Auto setting will set the path cost as appropriate by the physical link speed, using the 802.1D recommended values. Using the Specific setting, a user-defined value can be entered. The path cost is used when establishing the active topology of the network. Lower path cost ports are chosen as forwarding ports in favor of higher path cost ports. Valid values are in the range from 1 to 200,000,000.
Priority	Priority will determine the forwarding state of ports when path costs are the same.

6.6 IPMC Profile

Users can configure a filter multicast list

Click the “Advanced Configure-IPMC Profile-Address Entry” as follows:

Interface data are as follows.

Configuration Items	Description
Entry Name	Enter the multicast name to be filtered
Start Address	Enter the start multicast address
End Address	Enter the end multicast address

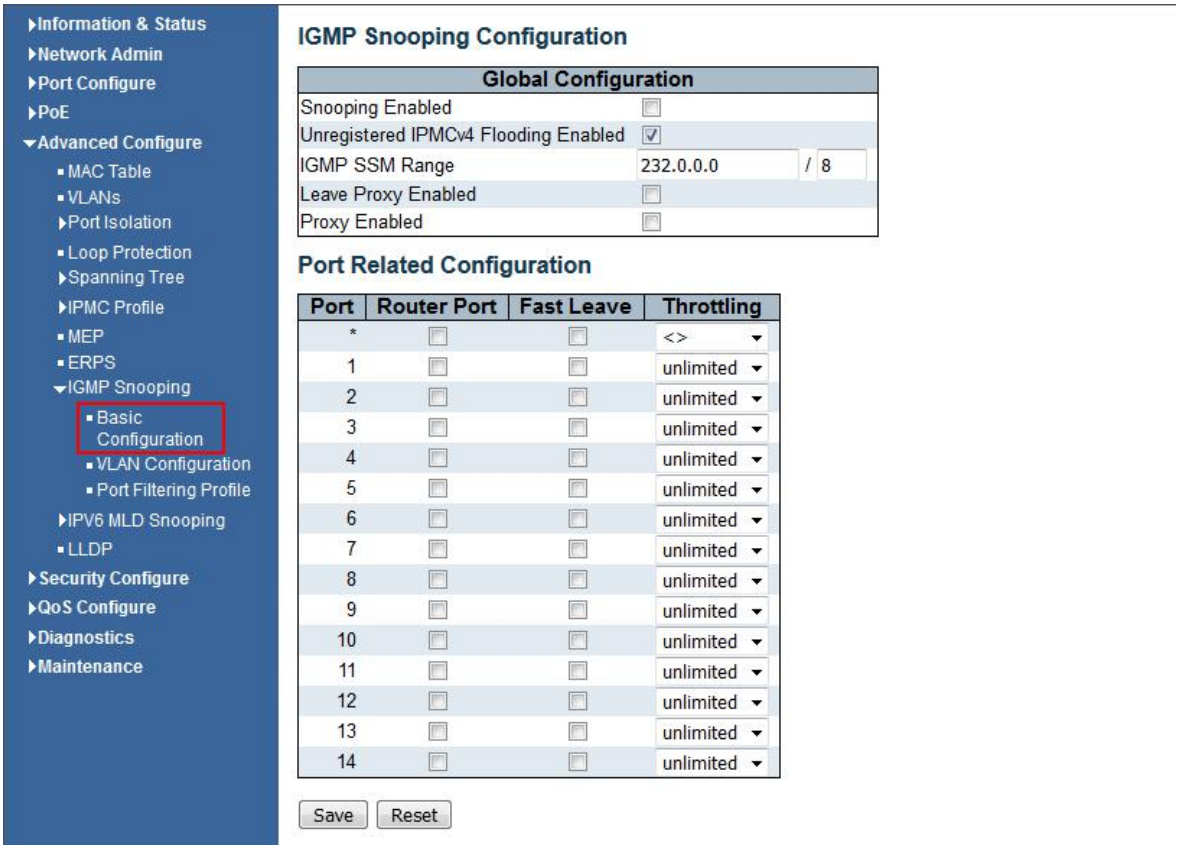
6.7 IGMP Snooping

IGMP Snooping (Internet Group Management Protocol Snooping) is a multicast management and control mechanism that works on a Layer 2 Ethernet switch.

The switch maps its interfaces with multicast group addresses and forwards the multicast data streams accordingly by snooping the IGMP message received by each interface when IGMP Snooping is enabled.

6.7.1 Basic Configuration

Click the "Advanced Configure-IGMP Snooping-Basic Configuration" to check the configuration info of IGMP Snooping as follows:

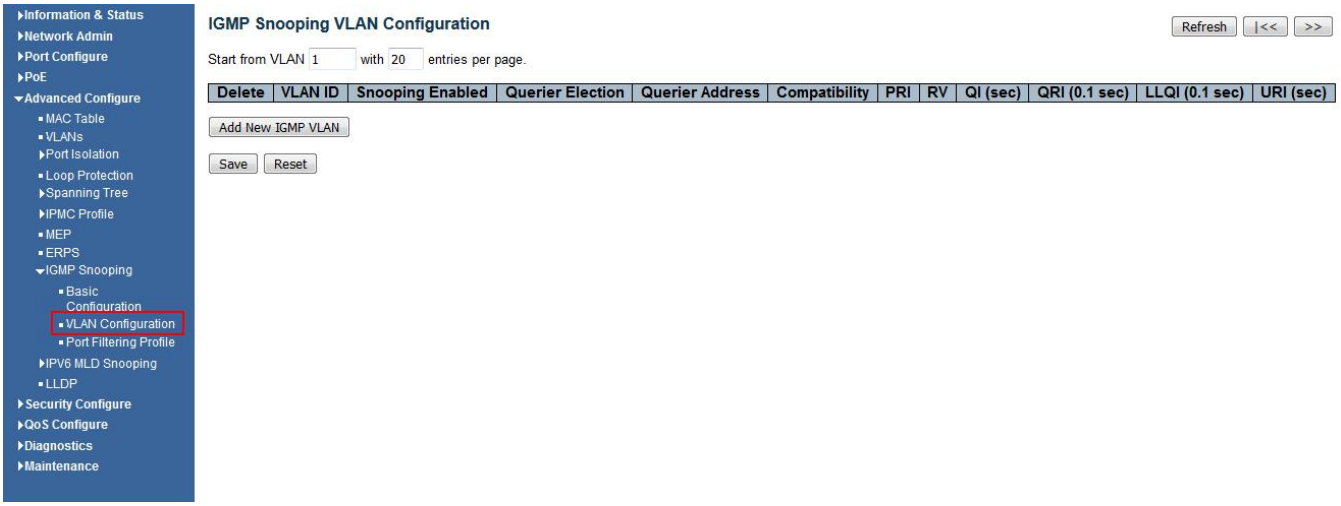


Interface data are as follows.

Configuration Items	Description
Snooping Enabled	Enable or disable IGMP Snooping.
Unregistered IPMCv4 Flooding Enabled	
Routing Port	It refers to the port connected to a Layer 3 multicast router or IGMP Querier. 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	Fast leave performs deleting MAC forward entry immediately upon receiving message for group de-registration

6.7.2 VLAN Configuration

Click the “Advanced Configure-IGMP Snooping-VLAN Configuration” to check the configuration info of IGMP Snooping as follows:

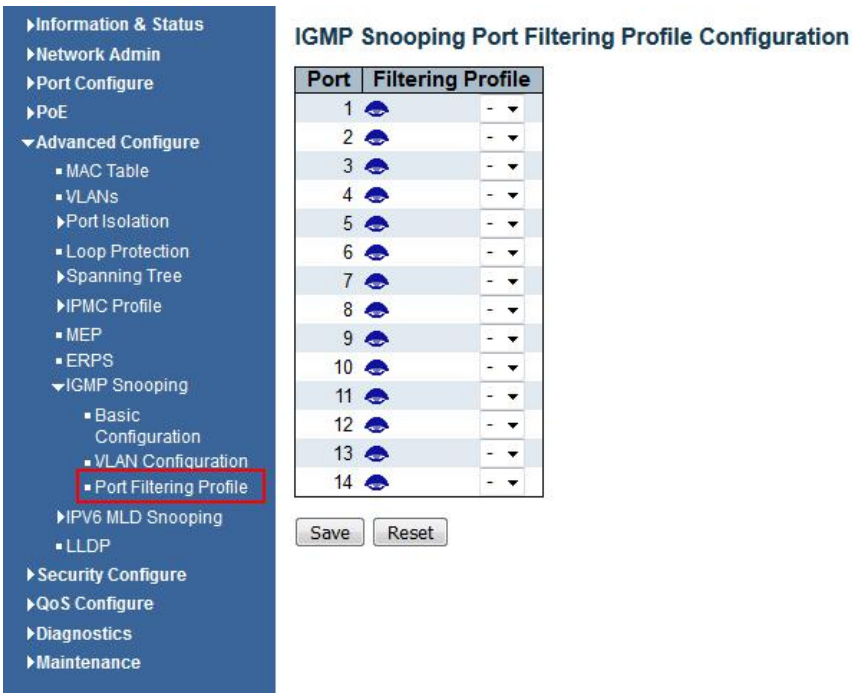


Interface data are as follows.

Configuration Items	Description
VLAN ID	
Snooping Enabled	Enable or disable the per-VLAN IGMP Snooping. Up to 32 VLANs can be selected for IGMP Snooping.
Querier Election	Enable or disable the IGMP Querier election. Enable to join IGMP Querier election in the VLAN. Disable to act as an IGMP Non-Querier.
Querier Address	Define the IPv4 address as source address used in IP header for IGMP Querier election. When the Querier address is not set, system uses IPv4 management address of the IP interface associated with this VLAN. When the IPv4 management address is not set, system uses the first available IPv4 management address. Otherwise, system uses a pre-defined value. By default, this value will be 192.0.2.1.

6.7.3 Port Filtering Profile

Click the “Advanced Configure-IGMP Snooping-Port Filtering Profile” to call the multicast list configured by IPMC Profile.



Interface data are as follows.

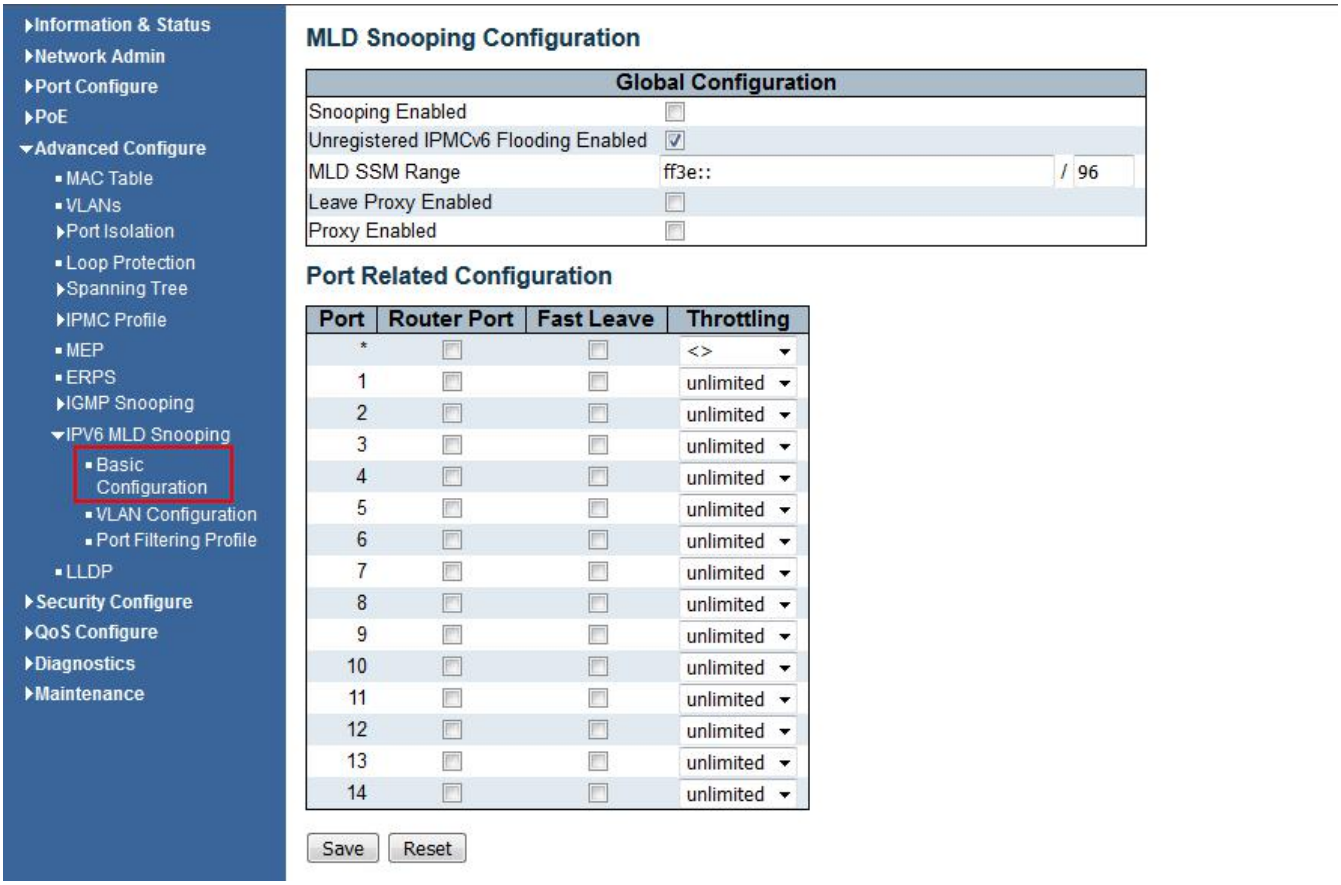
Configuration Items	Description
VLAN ID	
Snooping Enabled	Enable or disable the per-VLAN IGMP Snooping. Up to 32 VLANs can be selected for IGMP Snooping.
Querier Election	Enable or disable the IGMP Querier election. Enable to join IGMP Querier election in the VLAN. Disable to act as an IGMP Non-Querier.
Querier Address	Define the IPv4 address as source address used in IP header for IGMP Querier election. When the Querier address is not set, system uses IPv4 management address of the IP interface associated with this VLAN. When the IPv4 management address is not set, system uses the first available IPv4 management address. Otherwise, system uses a pre-defined value. By default, this value will be 192.0.2.1.

6.8 IPv6 MLD Snooping

IPv6 MLD Snooping is a multicast management and control mechanism that works on a Layer 2 Ethernet switch. The switch maps its interfaces with multicast group addresses and forwards the multicast data streams accordingly by snooping the IPv6 MLD message received by each interface when IPv6 MLD Snooping is enabled.

6.8.1 Basic Configuration

Click the "Advanced Configure-IPv6 MLD Snooping-Basic Configuration" to check the configuration info as follows:



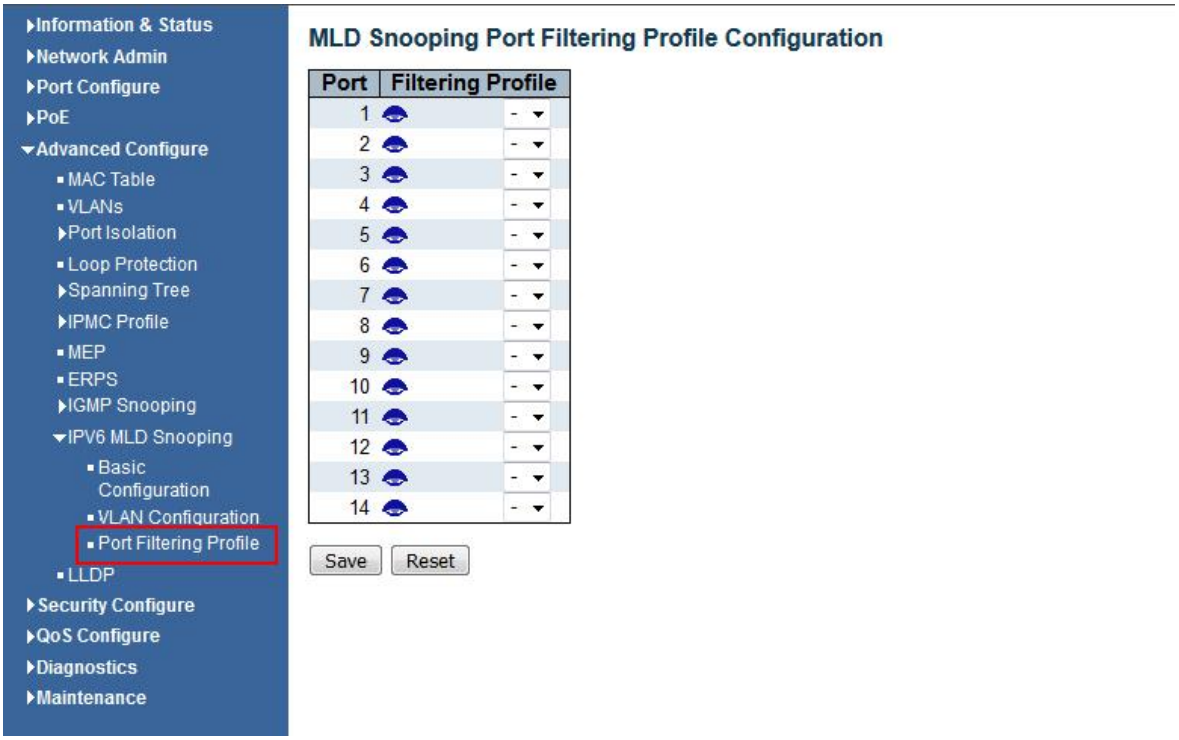
Interface data are as follows.

Configuration Items	Description
Enable Snooping	Enable or disable IPv6 MLD Snooping
Unregistered IPMCv6 Flooding Enabled	
Routing port	It refers to the port connected to a Layer 3 multicast router or IGMP Querier. 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	Fast leave performs deleting MAC forward entry immediately upon receiving message for group de-registration

6.8.3 Port Filtering Profile

Click the “Advanced Configure-IPv6 MLD Snooping-VLAN Configuration” to check the configuration info as follows:



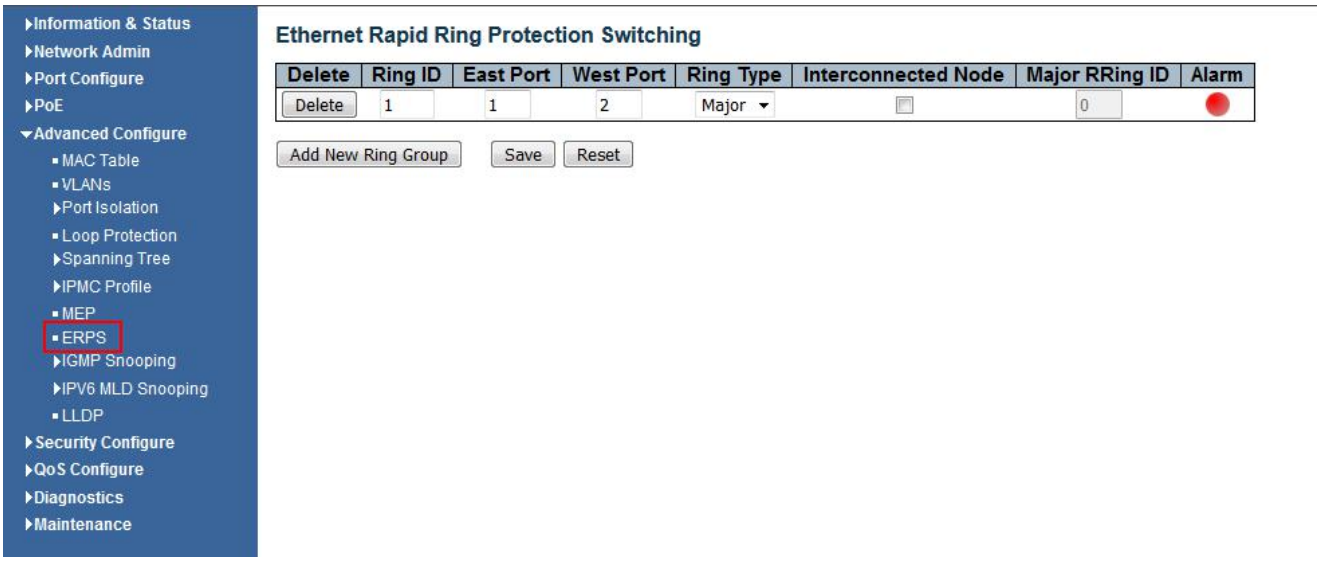
Interface data are as follows.

Configuration Items	Description
VLAN ID	
Snooping Enabled	Enable or disable the per-VLAN MLD Snooping. Up to 32 VLANs can be selected for IGMP Snooping. Enable the per-VLAN IGMP Snooping. Up to 32 VLANs can be selected for IGMP Snooping.
Querier Election	Enable or disable the MLD Querier election. Enable to join MLD Querier election in the VLAN. Disable to act as an MLD Non-Querier.

6.9 ERPS

ERPS (Ethernet Ring Protection Switching):
As the latest mature standard of ERPS, ITU-TG.8032 ERPS supports multi-ring and multi-domain structures, absorbs the advantages of EAPS, RPR, SDH, STP, etc., and optimizes the inspection mechanism in terms of two-way faults. In addition, it supports main device backups, load sharing and other work methods in 50ms switching.
Note: Disable STP before enabling ERPS.

Click the “Advanced Configure-ERPS” as follows:



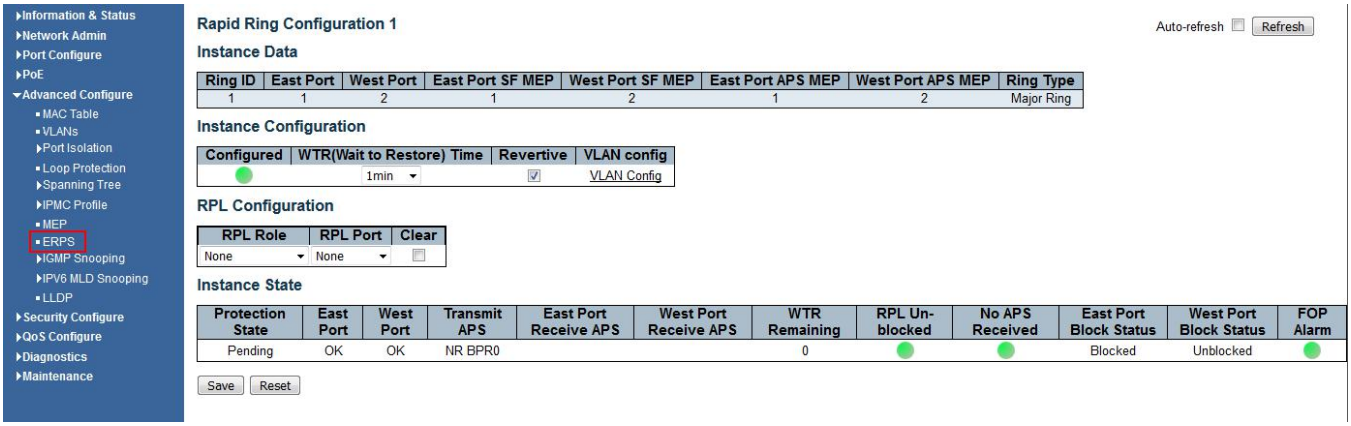
Interface data are as follows.

Configuration Items	Description
Ring ID	ID of ERPS Ring Instances
East Port	Choose a port No. involved in Ring protection
West Port	Choose another port No. involved in Ring protection
Ring Type	Select from “Main Ring” or “Sub-Ring” (only deployed in multi-ring applications), with “Main Ring” by default.
Interconnection Node	It refers to the node connecting 2 or more rings in a multi-ring application at the same time

Main Ring ID	Main Ring shares the same ID with Ring in a single ring application. Sub-Ring has to fill in the Main Ring ID in a multi-ring application.
R-APS VLAN(1-4,094)	The VLAN used as R-APS VLAN.

Click the “Add New Ring Group”;

Click the link in the “Ring ID” list to configure the ERPS Ring as follows:



Configuration Items	Description
WTR Time (5-12s)	Check the box and enter the WTR Time of R-APS function, which by default is 1 minute.
Restore the Revertive Mode	Check the box to enable or disable the R-APS restore option by dropping down the list.
VLAN Protection	Click the “VLAN Protection” to edit the protected VLAN group.
RPL Role	Select from “None”, “RPL Owner” and “RPL Neighbor” by dropping down the list.
RPL Port	Select from “None”, “East Port” and “West Port” by dropping down the list.

“Save” and finish.

Click the “VLAN Config” to edit the protected VLAN configuration.

Note: Users can modify or add other VLANs (ID 1 by default) for protection in this page.

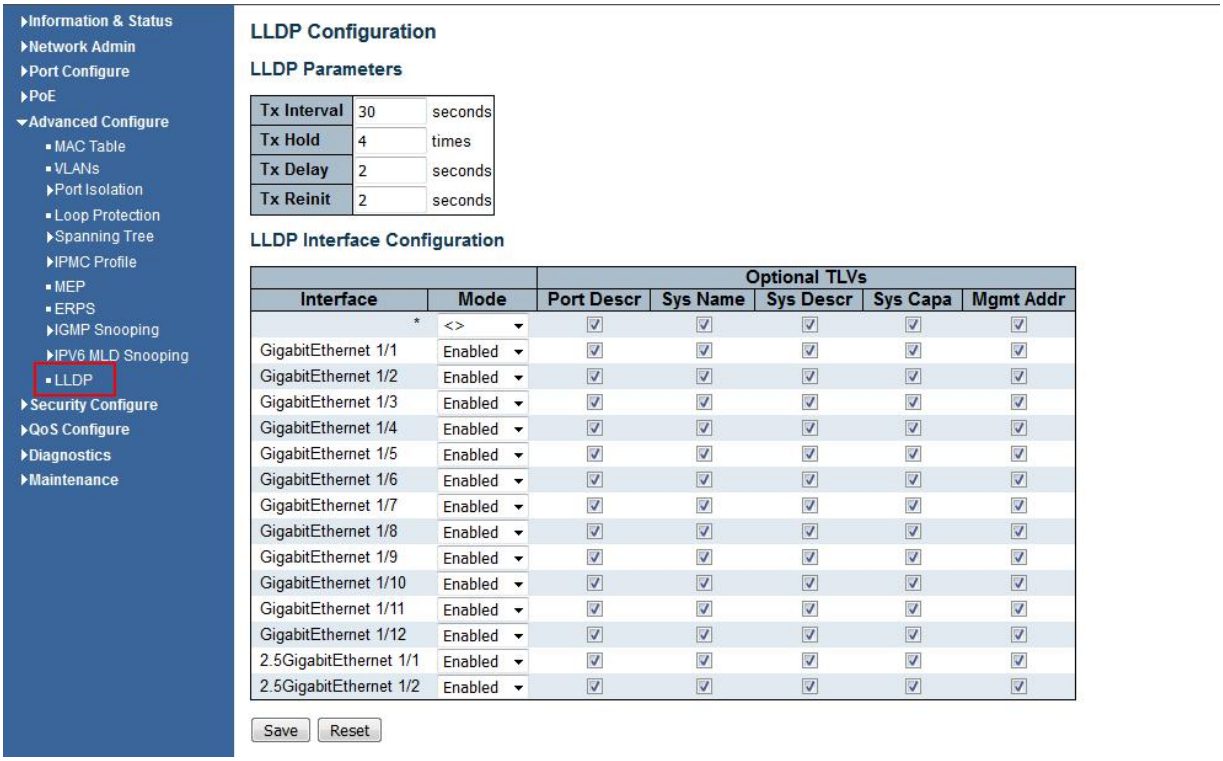
6.10 LLDP

Link Layer Discovery Protocol (LLDP) is a vendor-independent Layer 2 protocol that allows network devices to notify local subnets of the identifications and performance.

Currently, diversified network devices with complex configuration need a standard info exchange platform for manufacturers to discover others and exchange their unique systems and configuration info.

That's how LLDP comes out. It is a standard link layer discovery method which integrates the info such as main capabilities, management addresses, device and interface identifications of terminal devices into the TLV (Type/Length/Value), encapsulates it in LLDPDU (Link Layer Discovery Protocol Data Unit) and sends it to the directly connected neighbors. After receiving the info, they will save it in the form of standard MIB (Management Information Base) for NMS inquiry and link communication judgment.

Click the "Advanced Configure-LLDP" as follows:

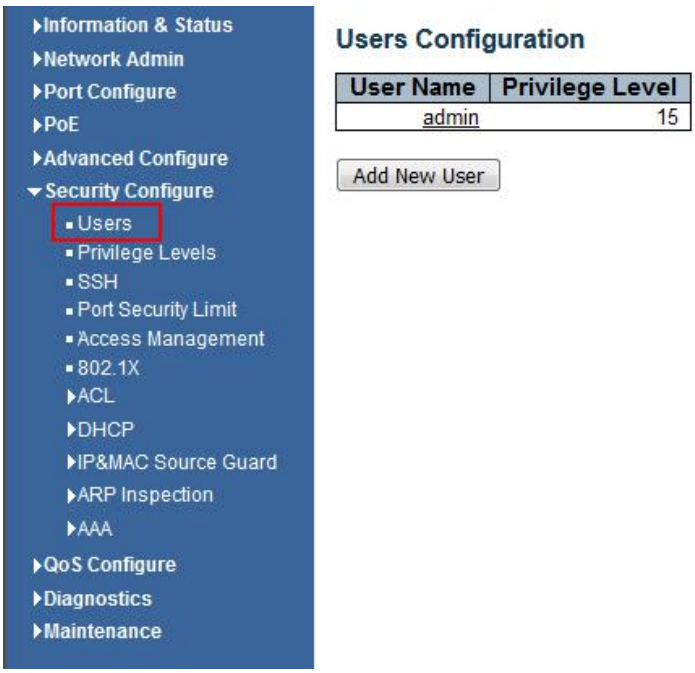


7 Security Configure

7.1 Users

Users can reset the passwords on the switch.

Click the “Security Configure-Users” as follows:

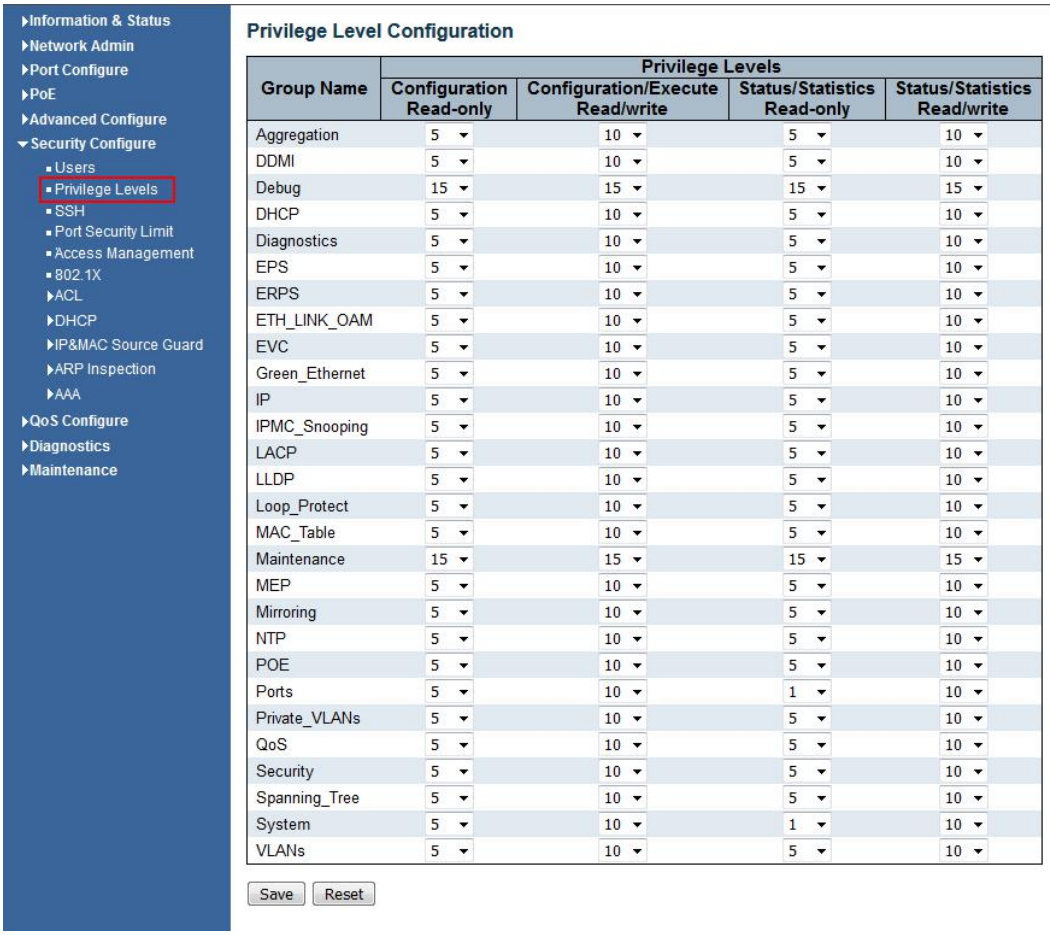


"Save" and finish.

7.2 Privilege Levels

Users can change the login level on the switch.

Click the "Security Configure-Privilege Levels" as follows:

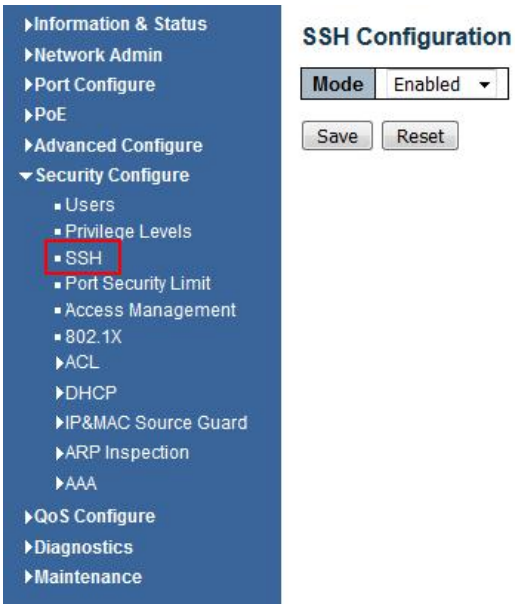


7.3 SSH

SSH (Secure Shell) is a security protocol based on the application layer and formulated by the Network Working Group of IETF. SSH provides safe network services in a reliable manner, especially the Rlogin Session service. It can prevent info disclosure during remote management.

The switch manages SSH.

Click the “Security Configure-SSH” as follows:



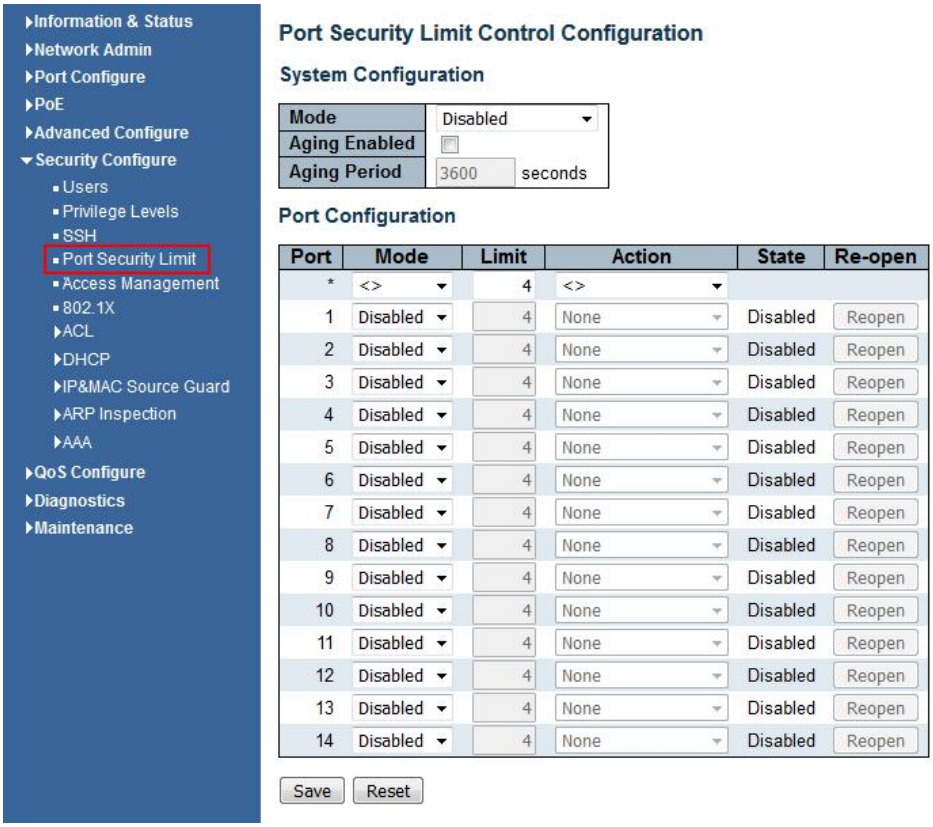
7.4 Port Security Limit

Port Security:

The number of restricted MAC addresses on a port.

The switch supports Port Security.

Click the “Security Configure-Port Security Limit” as follows:

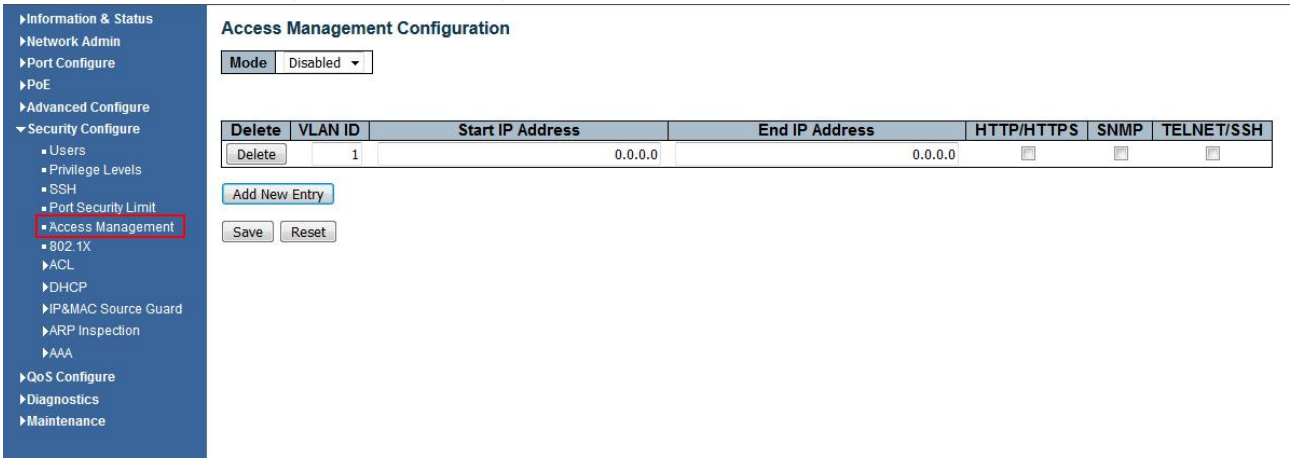


7.5 Access Management

Access Management Web service can help you safely access the switch resources.

The switch supports Access Management.

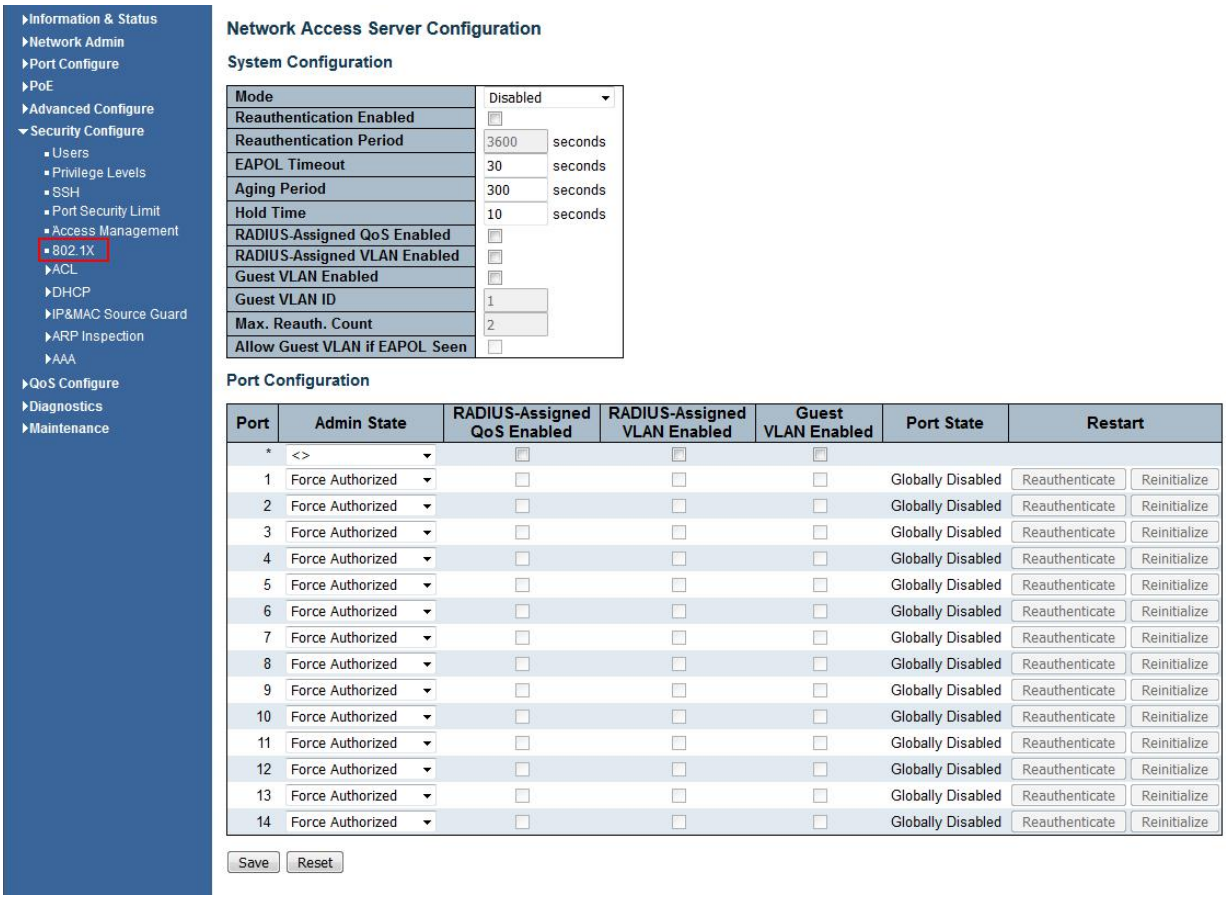
Click the “Security Configure-Access Management” as follows:



7.6 802.1X

802.1X is a Client/Server-based protocol for access control and authentication, which prevents the unauthorized users/devices from accessing a LAN/WLAN through an access port. 802.1X authenticates the users/devices connected to the port before acquiring the services provided by the switch or LAN. Prior to authentication, only EAPoL (Extensible Authentication Protocol over Lan) data can flow through the switch port. Normal data are also allowed to flow through the Ethernet port smoothly after authentication.

Click the “Security Configure-802.1X” as follows:



Interface data are as follows

Configuration Items	Description
System Configuration	Select from “Mode, Reauthentication Enabled, Reauthentication Period, 3,600 seconds, EAPOL Timeout, 30 seconds, Aging Period, 300 seconds, Hold Time, 10 seconds, RADIUS-Assigned QoS Enabled, RADIUS-Assigned VLAN Enabled, Guest VLAN Enabled, Guest VLAN ID 1, Max. Reauth Count 2, Allow Guest VLAN if EAPoL Seen”
Port Configuration	Select from “Port, Admin State, RADIUS-Assigned QoS Enabled, RADIUS-Assigned VLAN Enabled, Guest VLAN Enabled, Port State, Restart”

“Save” and finish.

7.7 ACL

Access Control List (ACL) is the instruction list of switch interfaces, which is used to control packet ingress and egress. It applies to all routed protocols, such as IP, IPX and AppleTalk.

Communication between information points and internal & external networks are essential business requirements of enterprise networks. For secure Intranet, access rights can be controlled by formulating security policies ensuring that unauthorized users can only use certain network resources. In short, ACL filtering flow is a network technology for access control.

ACL is configured to restrict network flow and authorized devices, forward specified port packets, etc. For example, external public network is beyond the reach of the devices in the LAN, or only FTP service is available. ACL can be configured either on routers or on the business software with ACL functions.

ACL, based on device hardware layer security, is an important technology to ensure system security in IoT. By controlling the access to communication between software devices and specifying the access rules programmatically, ACL separates illegal devices from damaging system security and obtaining data.

7.7.1 ACL Ports

Click the “Security Configure-ACL-Ports” as follows.

Interface data are as follows

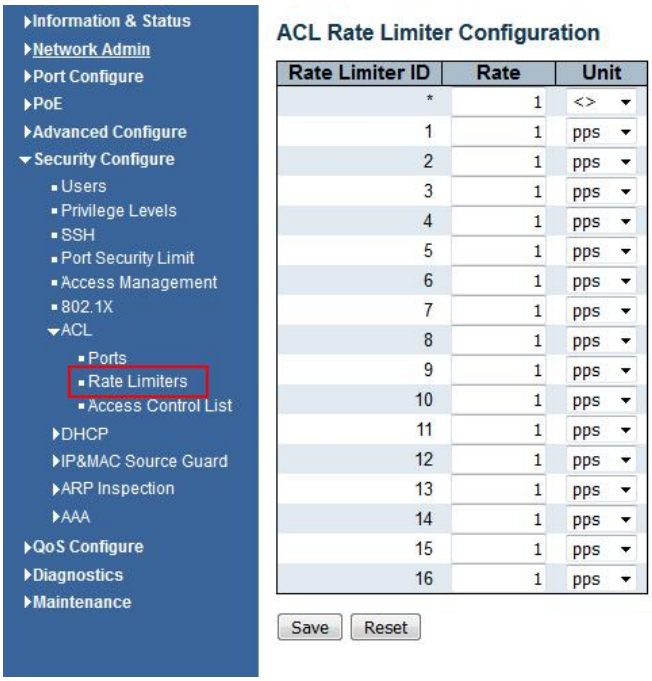
Configuration Items	Description

Action	“Permit”: data can flow through this port. “Deny”: data cannot flow through this port.
Rate Limiter ID	The Rate Limiter ID bundled with the port. See details in Rate Limiter Configuration.
Port Redirect	Select which port frames are redirected on. The allowed values are **Disabled** or a specific port number and it can't be set when action is permitted. The default value is “Disabled”.
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”.
Logging	
Shutdown	Specify the port shut down operation of this port. The allowed values are: **Enabled**: If a frame is received on the port, the port will be disabled. **Disabled**: Port shut down is disabled. The default value is “Disabled”. Note: The shutdown feature only works when the packet length is less than 1,518 (without VLAN tags).
State	Specify the port state of this port. The allowed values are: **Enabled**: To reopen ports by changing the volatile port configuration of the ACL user module. **Disabled**: To close ports by changing the volatile port configuration of the ACL user module. The default value is “Enabled”.
Counter	Counts the number of frames that match this rule.

“Save” and finish.

7.7.2 Rate Limiter

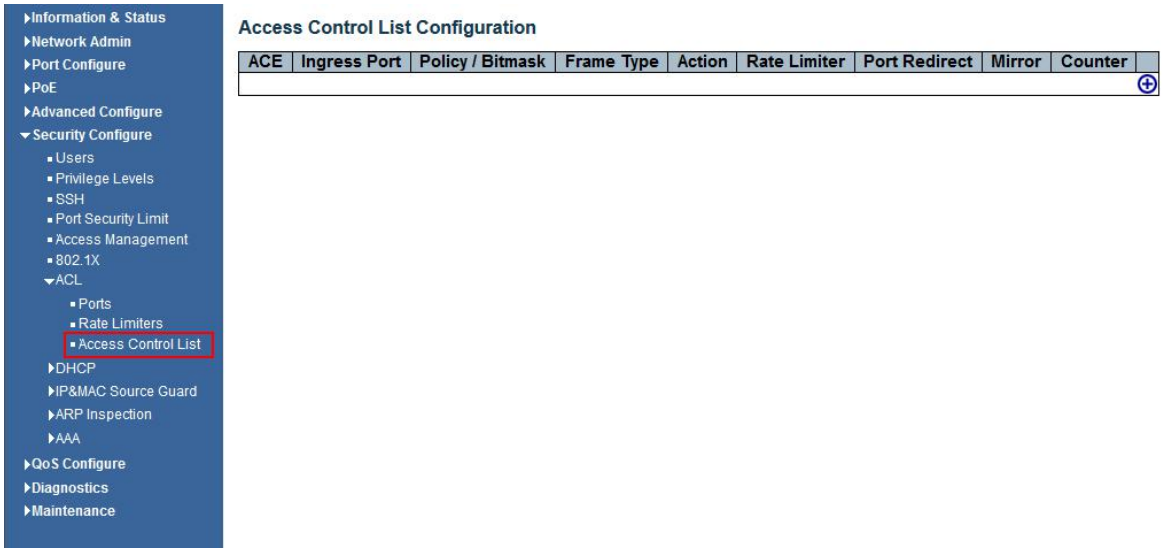
Click the “Security Configure-ACL-Rate Limiters” as follows.



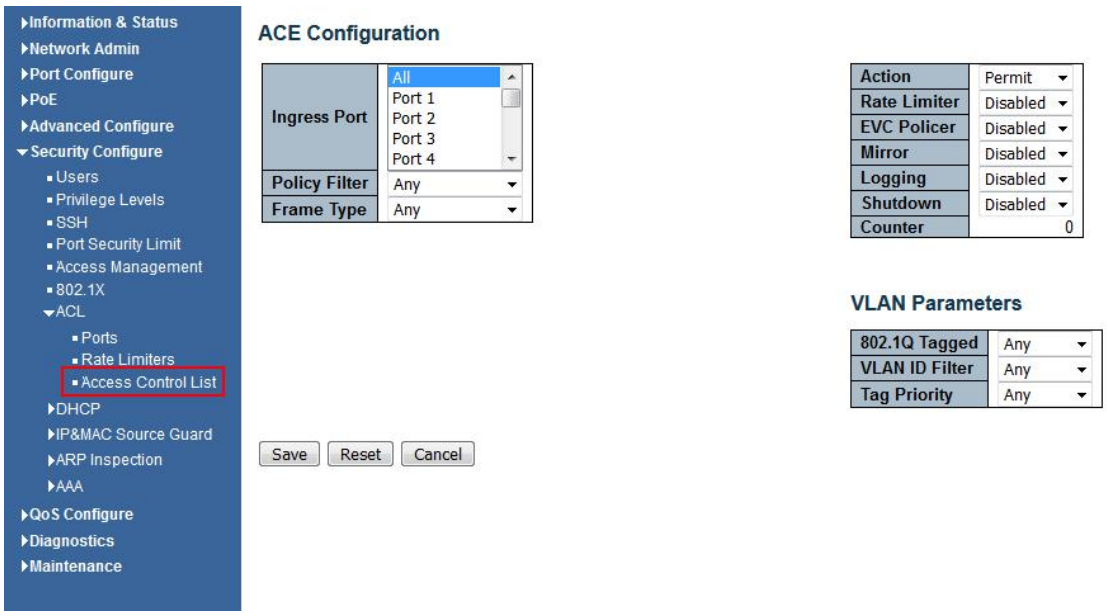
"Save" and finish.

7.7.3 Access Control List

Click the "Security Configure-ACL-Access Control List" as follows:



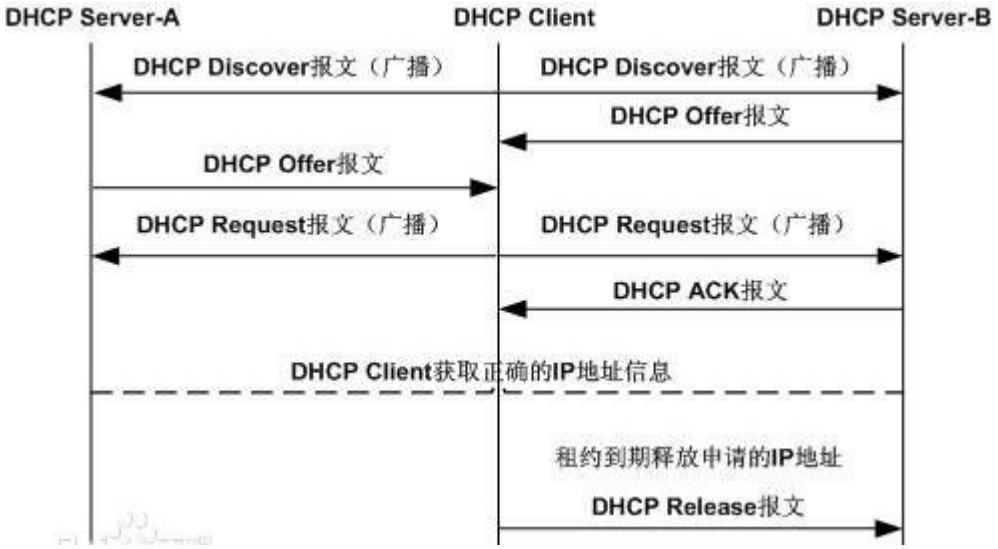
Click the "+" to edit the Access Control List.



7.8 DHCP Snooping

DHCP principle

DHCP takes UDP as the transmission protocol. The host sends a request to Port 68 of DHCP Server which replies to the Port 67 of the host. The interactive process is detailed as follows.



1. DHCP Client broadcasts a DHCP Discover message.
2. After receiving the message, all DHCP Severs will reply to DHCP Client a DHCP Offer message.

DHCP Server will send “Your (Client) IP Address” field as the IP Address in the message to DHCP Client, and put its own IP Address in the “Option” field for distinguishing. DHCP Server will record the assigned IP address after sending the message.

3. Generally speaking, DHCP Client can only process the first DHCP Offer message it receives.

It will broadcast a DHCP Request message and add the selected DHCP Server’s and the required IP address in the option field.

4. After receiving DHCP Request message, DHCP Server will compare the IP addresses with its own address. DHCP Server will only clear the corresponding records of IP address allocation if different; or it will respond to DHCP Client with a DHCP ACK message and add the lease term for the IP address in the option field.

5. DHCP Client will check the availability of the IP address assigned by DHCP Server in the DHCP ACK message. DHCP Client will own the IP address and renew the lease automatically if the address is valid, or it will send a DHCP Decline message to inform DHCP Server of disabling this IP address and applying for a new one.

6. DHCP Client can release the obtained IP address by sending a DHCP Release message at any time, and DHCP Server will recover and redistribute the corresponding IP address.

After half of the lease term, DHCP Client will send a DHCP Request message in unicast form to renew the IP address. Upon receiving the DHCP ACK message, DHCP Client should extend the term as required, otherwise, DHCP Client should continue to use this IP address.

After 87.5% of the lease term, DHCP Client will broadcast a DHCP Request message to renew the IP address. If DHCP Client receives a DHCP ACK message, the term will be extended as required; or DHCP Client has to continue to use the address until it expires. Then it should send a DHCP Release message to DHCP Server to release this IP address and apply for a new one.

What needs illustration is that DHCP Client may generally receive the first DHCP Offer packet from multiple DHCP Servers. In addition, the address [1] specified in the DHCP Offer sent by DHCP Server may not be the final address to be distributed, and it will be kept by DHCP Server till the Client makes a request.

DHCP Client sends a DHCP Request via broadcast packet to formally request DHCP Server for address distribution, so that other DHCP Servers sending Offer packets can also receive the Request packet, thereby releasing the IP addresses that have been offered (pre-allocated) to DHCP Client.

DHCP client will send a DHCP Decline info packet to DHCP Server to refuse the address that has been used by others.

DHCP Server will send a DHCP NAK message to DHCP Client for an address re-application during the negotiation due to incorrect address info (e.g. moving into a new subnet, or date expiration).

Steps are as follows.

DHCP Client broadcasts a DHCP Discover message to DHCP Server. It will re-send the message if DHCP Server fails to respond to it.

Upon receiving the message, DHCP Server will distribute resources (e.g. IP address) according to strategies and send a DHCP Offer message to DHCP Client.

DHCP Client will send a DHCP Request to apply for the server lease, and inform other servers of accepting this distributed address.

DHCP Server will send a DHCP ACK message for distributable resources, or a DHCP NAK message for non-distributable resources. DHCP Client can use the resources once it receives the DHCP ACK message, or it will re-send a DHCP Discover message if a DHCP NAK message is received.

DHCP Snooping principle

By snooping on the DHCP interactive messages between Client and Server, DHCP Snooping function will monitor users behaviors and filter DHCP messages and illegal servers by reasonable configuration. The followings interpret the terms and functions of DHCP Snooping:

1) DHCP Snooping Trust Port: Given that DHCP obtains IP interactive messages by broadcast, there are illegal servers that influence users to obtain normal IP, and some of them even cheat users and steal information. As a result, DHCP Snooping classifies the ports as the Trust port and the Untrust port. Devices only forward the DHCP Reply messages received from the Trust ports and abandon those from Untrust ports, in order to set the legal ports linked with DHCP Servers as Trust ports and others as Untrust ports, thus blocking the illegal servers.

2. DHCP Snooping binding database: Setting IP address privately is commonly seen in DHCP network, which not only increases the network maintenance difficulty, but also results in legal users failing to access the network due to conflicts. By snooping on the interactive messages between Client and Server, the IP, MAC, VID, PORT, lease and other information obtained by users are compiled into a user record entry to form the DHCP Snooping database. With the use of ARP inspection or check function, users' accesses to Internet will be controlled.

DHCP Snooping inspects the validity of messages flowing through the devices, abandons illegal ones, records user information, and creates a binding database for other functional queries. Here are some types of illegal messages:

1) The DHCP Reply messages received by Untrust port, including DHCP ACK, DHCP NACK, DHCP OFFER, etc.

2) The DHCP Reply messages received by Untrust port with network management info [giaddr].

3) During MAC verification, the DHCP Client field values of the Source MAC and DHCP messages respectively represent different packets.

4) With user information saved in the DHCP Snooping binding database, DHCP Release message has inconsistent port info with that saved in the database by devices.

7.8 Security-Related Functions of DHCP Snooping

In DHCP network environment, administrators often find that users modify and use static IP addresses rather than dynamic IP addresses without permission. Therefore, some users using dynamic IP addresses fail to access network normally, which complicates network application environment and increases the management difficulty of administrators. DHCP dynamic binding is a secure process in which a device obtains information by recording the IP of a legal user during DHCP Snooping. There are three control types. The first is to bind the address of a legal user with IP Source Guard. The second is to use the software's DAI (Dynamic ARP Inspection) to check the validity of a user by controlling the ARP. The last is to bind the legal user's ARP message by ARP Check. Note: when using the IP Source Guard to bind the address, the number of DHCP users that a switch can support is limited by hardware entries. Legal users may fail to add hardware entries and use network properly due to too many users. All ARPs are forwarded and processed by CPU when using the DAI function, which will seriously affect the switch performance.

The address binding relation between DHCP Snooping and IP Source Guard

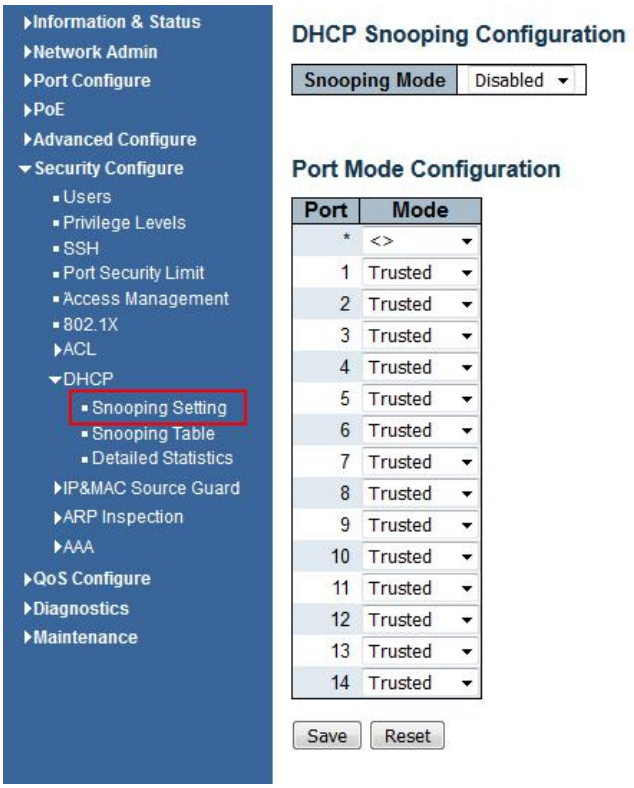
IP Source Guard maintains the IP Source address database by setting the user information [IP, MAC] in the database to the hardware filtering entries and restricting the users' network accesses. Please refer to the *IP&MAC Source Guard Configuration Section* for more info.

DHCP Snooping prevents users from setting up private IP addresses by snooping on DHCP process, maintaining the user IP database, and submitting the data to IP Source Guard for filtration to ensure that only users who obtain IP through DHCP have access to the network.

In addition, DHCP binding users' validity will be checked for higher security and problem prevention like ARP spoofing since DHCP binding filters IP messages only. Please refer to the *ARP Inspection Configuration Section* for more information.

7.8.1 DHCP Snooping

Click the "Security Configure-DHCP-Snooping Setting" as follows to check the switch configuration:



Interface data are as follows

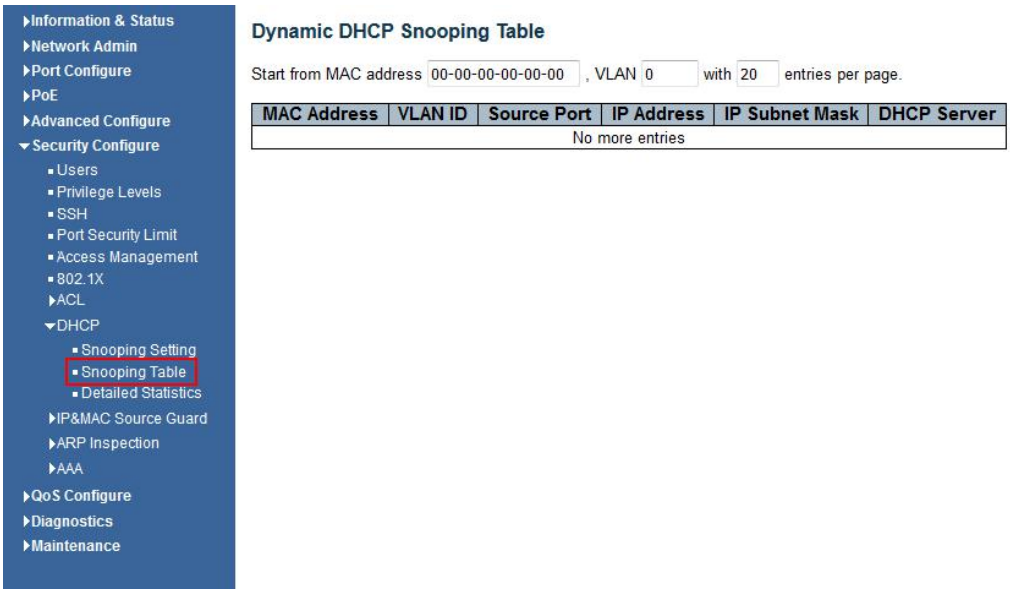
Configuration Items	Description
DHCP Snooping Mode	Enable or disable DHCP Snooping.

Port Mode	Indicates the DHCP snooping port mode. Possible port modes are: **Trusted**: Configures the port as trusted source of the DHCP messages. **Untrusted**: Configures the port as untrusted source of the DHCP messages.

Click the “Save” to save all changes.

7.8.2 DHCP Snooping Table

Click the “Advanced Configure-DHCP-Snooping Table” to check the DHCP Snooping configuration as follows:

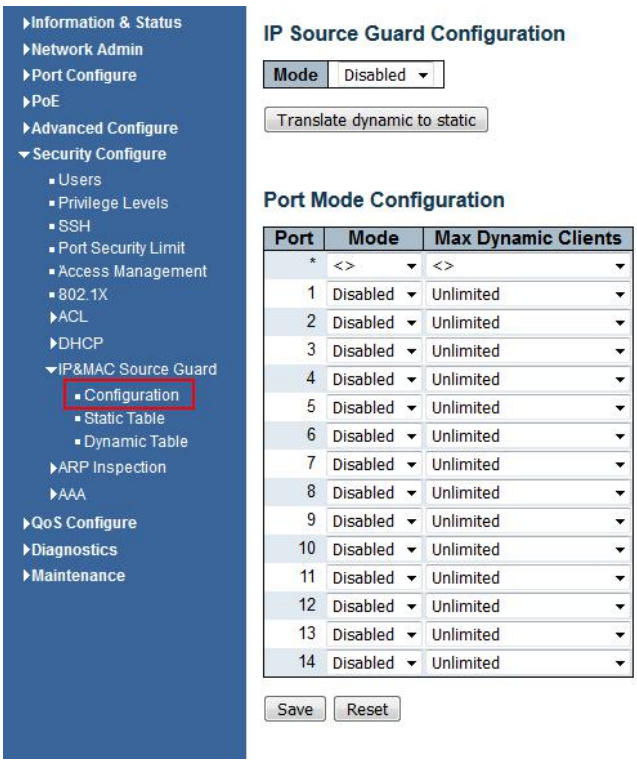


7.9 IP & MAC Source Guard

IP & MAC Source Guard maintains the Source IP & MAC binding database to filter the host messages based on Source IP & MAC on corresponding ports, thus ensuring the sole network access of the hosts of Source IP & MAC binding database.

7.9.1 Configuration

Click the “Security Configure-IP & MAC Source Guard-Configuration” as follows.



Interface data are as follows.

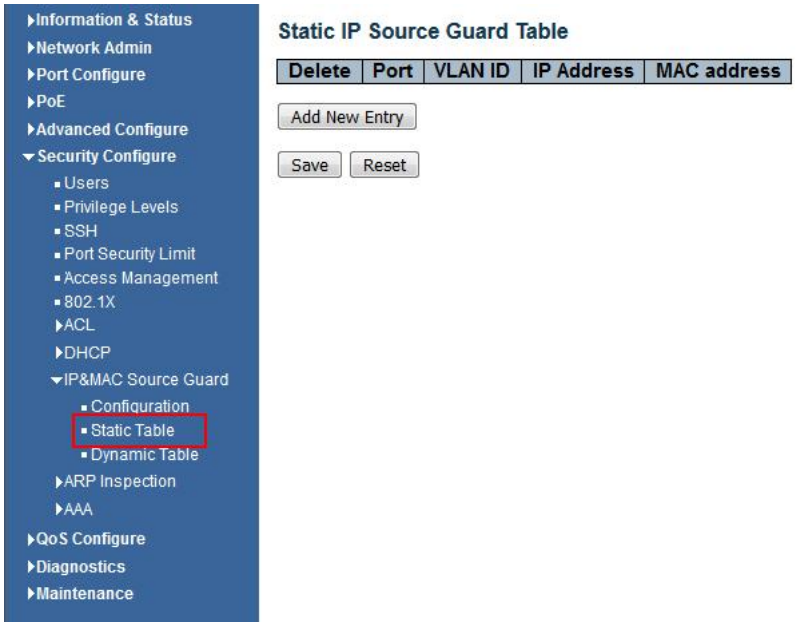
Configuration Items	Description
Global Pattern	Enable or disable IP & MAC Source Guard based on global pattern
Port Mode	Enable or disable IP & MAC Source Guard based on ports
Max Dynamic Clients	Select the max number of customers supported from: Unlimited, 0, 1, and 2.

"Save" and finish .

7.9.2 Static Table

Users can manually configure the binding entry of IP & MAC Guard to control the ports in this page.

Click the "Security Configure-IP & MAC Source Guard-Static Table" as follows.



Interface data are as follows

Configuration Items	Description
Port	Enter the port ID to be bound.
VLAN	Enter the VLAN ID to be bound.
IP Address	Enter the IP Address to be bound.
MAC Address	Enter the MAC Address to be bound.

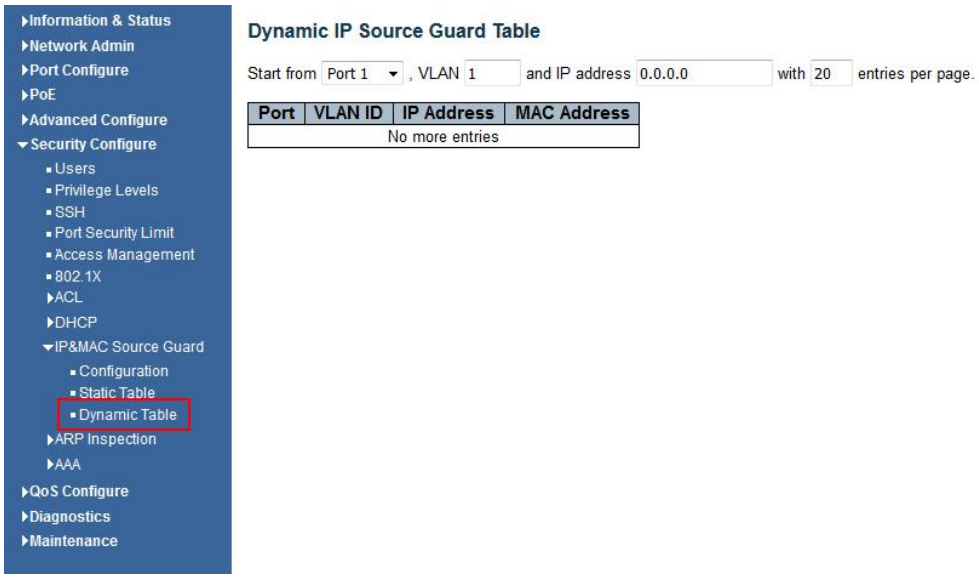
Click the “Add a New Entry” subject to the input info.

“Save” and finish.

7.9.3 Dynamic Table

Users can manually configure the binding entry of IP & MAC Guard to control the ports in this page.

Click the “Security Configure-IP & MAC Source Guard-Static Table” as follows.



Interface data are as follows

Configuration Items	Description
Port	Display the port ID
VLAN	Display the VLAN ID
IP Address	Display the IP Address
MAC Address	Display the MAC Address

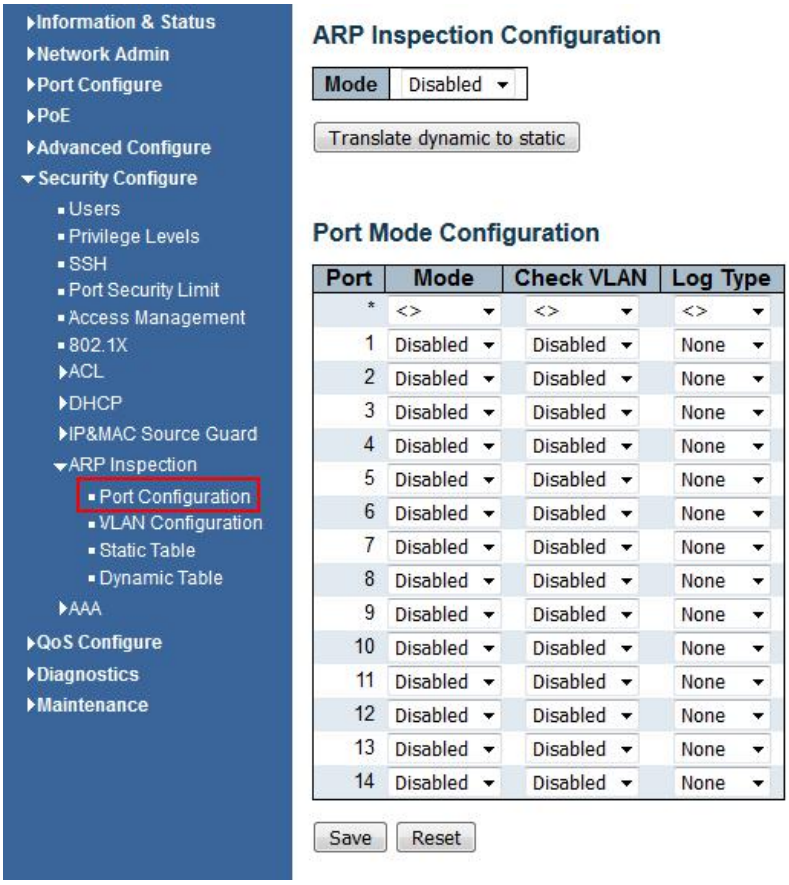
7.10 ARP Inspection

IP & MAC Source Guard maintains the Source IP & MAC binding database to filter the host messages based on Source IP & MAC on corresponding ports, thus ensuring the sole network access of the hosts of Source IP & MAC binding database.

7.10.1 Port Configuration

Users can edit the Port Configure in this page.

Click the “Security Configure-ARP Inspection-Port Configuration” as follows.



Interface data are as follows

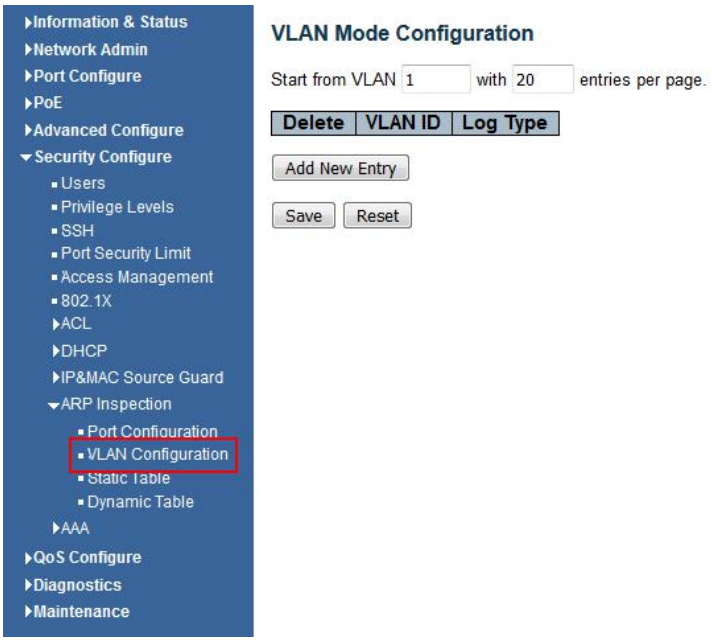
Configuration Items	Description
Global Pattern	Enable or disable ARP Inspection based on global pattern
Port Mode	Enable or disable ARP Inspection based on ports
Check VLAN	If you want to inspect the VLAN configuration, you have to enable the setting of "Check VLAN". The default setting of "Check VLAN" is disabled. When the setting of "Check VLAN" is disabled, the log type of ARP Inspection will refer to the port setting. And the setting of "Check VLAN" is enabled, the log type of ARP Inspection will refer to the VLAN setting. Possible setting of "Check VLAN" are: **Enabled**: Enable check VLAN operation. **Disabled**: Disable check VLAN operation.
Log Type	Only the Global Mode and Port Mode on a given port are enabled, and the setting of "Check VLAN" is disabled, the log type of ARP Inspection will refer to the port setting. There are four log types and possible types are: **None**: Log nothing. **Deny**: Log denied entries.

	Permit: Log permitted entries. **All:** Log all entries.

"Save" and finish.

7.10.2 VLAN Configuration

Click the "Security Configure-ARP Inspection-VLAN Configuration" as follows.



Interface data are as follows

Configuration Items	Description
VLAN ID	Per-VLAN configuration of ARP Inspection
Log Type	Enable or disable ARP Inspection based on ports.
Check VLAN	Specify ARP Inspection is enabled on which VLANs. First, you have to enable the port setting on Port mode configuration web page. Only when both Global Mode and Port Mode on a given port are enabled, ARP Inspection is enabled on this given port. Second, you can specify which VLAN will be inspected on VLAN mode configuration web page. The log type also can be configured on per VLAN setting. Possible types are: **None**: Log nothing. **Deny**: Log denied entries.

	Permit: Log permitted entries. **All:** Log all entries.

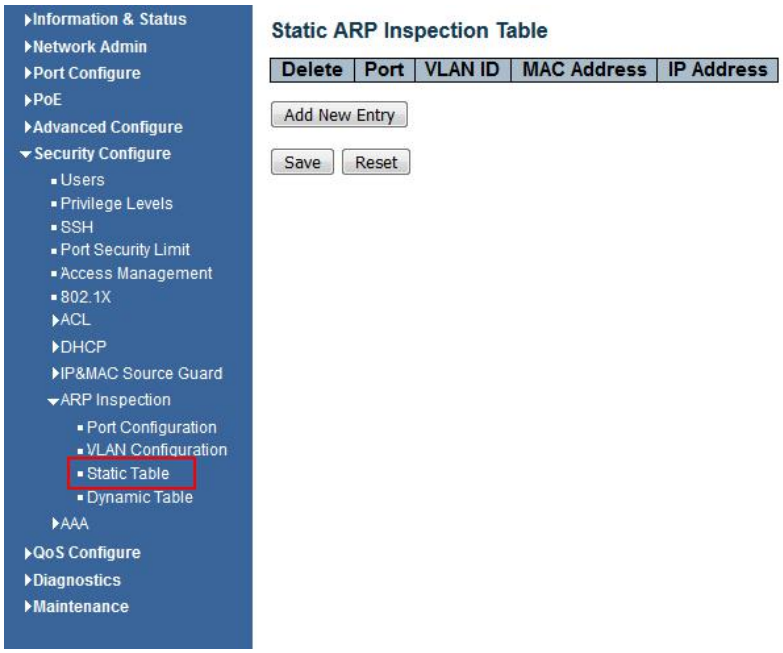
"Save" and finish.

Click the "Add New Entry" to create a new VLAN configuration.

7.10.3 Static Table

Users can manually configure the binding table of ARP Inspection to control the ports in this page.

Click the "Security Configure-ARP Inspection-Static Table" as follows.



Interface data are as follows

Configuration Items	Description
Port	Enter the port ID to be bound.
VLAN	Enter the VLAN ID to be bound.
IP Address	Enter the IP Address to be bound.
MAC Address	Enter the MAC Address to be bound.

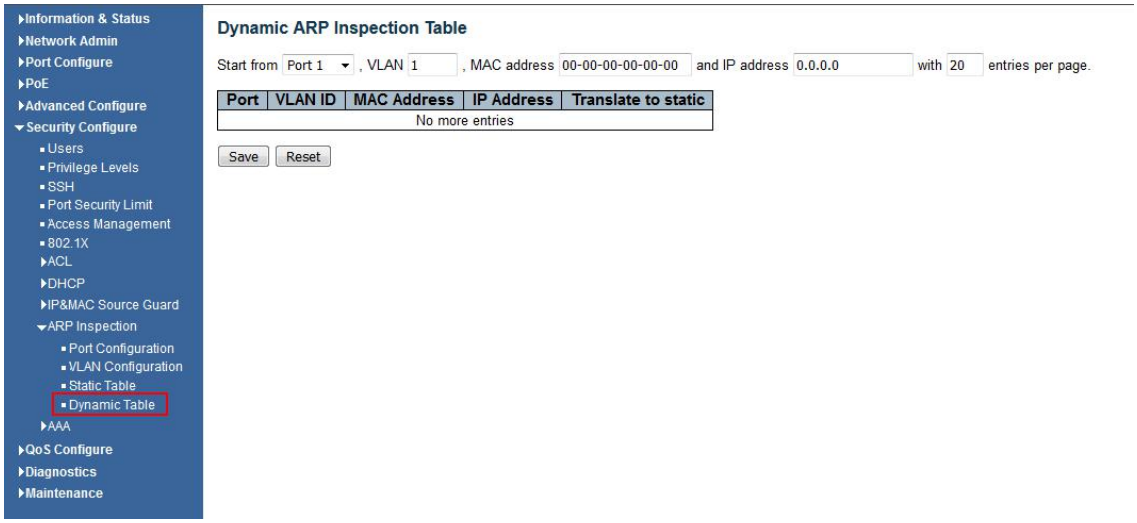
Click the "Add New Entry" subject to the input info.

"Save" and finish.

7.10.4 Dynamic Table

Users can manually configure the binding table of IP & MAC Guard to control the ports in this page.

Click the “Security Configure-ARP Inspection-Dynamic Table” as follows.



Interface data are as follows

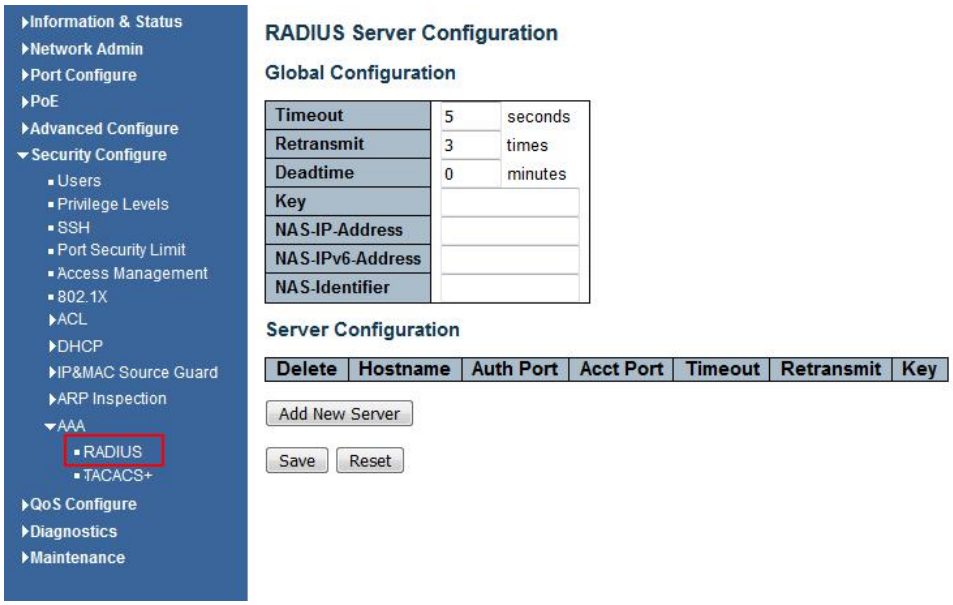
Configuration Items	Description
Port	Display the port ID
VLAN	Display the VLAN ID
IP Address	Display the IP Address
MAC Address	Display the MAC Address

7.11 AAA

AAA is the abbreviation of Authentication, Authorization and Accounting. It is a security management mechanism for network access control to provide three kinds of security services.

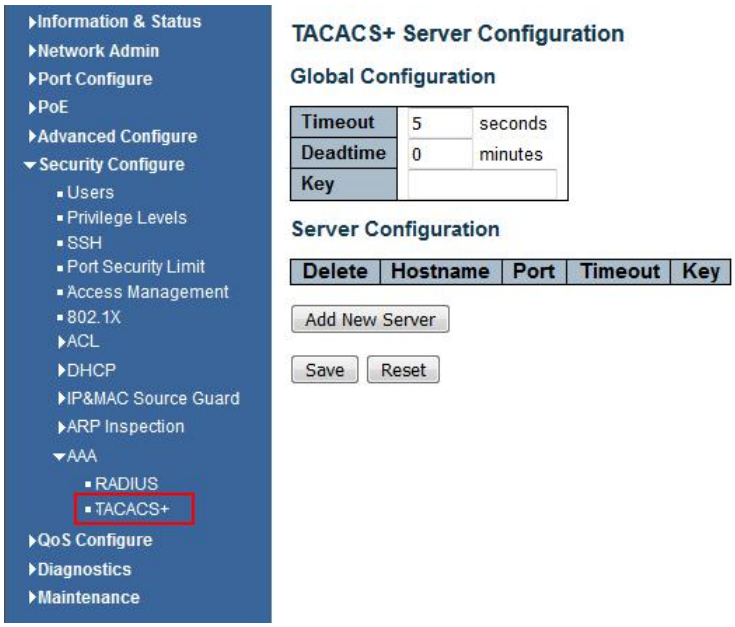
7.11.1 RADIUS

Click the “Security Configure-AAA-RADIUS” as follows:



7.11.2 TACACS+

Click the “Security Configure-AAA- TACACS+” as follows:



8 QoS

QoS (Quality of Service) assesses the ability of service providers to meet customer needs and the ability of sending packets over the Internet. Diversified services can be assessed based on different aspects. QoS usually refers to the

evaluation of service capabilities that support core requirements such as bandwidth, delay, delay variation, and packet loss rate during delivery. Bandwidth, also known as throughput, refers to the average rate of business flow in a given period of time, with the unit of kbit/s. Delay refers to the average time required for business flowing through the network. For a network device, the followings are general levels of delay requirements. There are two delay levels, that is, the high-priority business can be served as soon as possible by scheduling method of priority queue, while the low-priority business gets services after that. Delay variation refers to the time change of business flowing through the network. Packet loss rate refers to the percentage of lost business flow during transmission. As modern transmission systems are very reliable, information is often lost in network congestion. Packet loss due to queue overflow is the most common situation.

All messages in a traditional IP network are treated equally. Every network device processes messages on a FIFO basis, and makes every effort to send them to destinations without guaranteeing reliability, transfer delay, or other performance.

Network service quality is constantly improved as new applications keep springing up in the rapidly changing IP network. For example, VoIP, video and other delay-sensitive services have set higher standards on message transmission delay. Message transmission in a short period has been the common trend. In order to support voice, video and data services with different requirements, the network needs to identify business types and provide corresponding services.

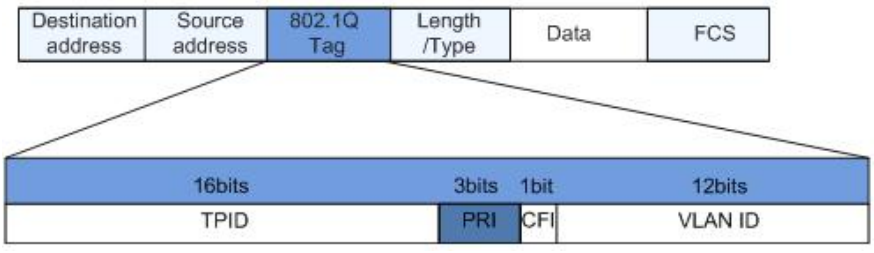
The ability to distinguish business types is the prerequisite to provide corresponding services, so the traditional best-effort service no longer meets the application needs. So QoS comes into being. It regulates the network flow to avoid and handle network congestion and reduce packet loss rate. Meanwhile, users can enjoy dedicated bandwidths while business can improve service quality, thus perfecting the network service capacity.

QoS priorities vary with message types. For instance, the VLAN message uses 802.1p, also known as the CoS (Class of Service) field, while the IP message uses DSCP. To maintain the priority, these fields need to be mapped at the gateway connected with various networks when messages flow through the network.

802.1p priority in the VLAN frame header

Typically, VLAN frames are interacted between Layer 2 devices. The PRI field (i.e. 802.1p priority), or CoS field, in the VLAN frame header identifies the quality of service requirements according to the definitions in IEEE 802.1Q.

802.1p priority in the VLAN frame

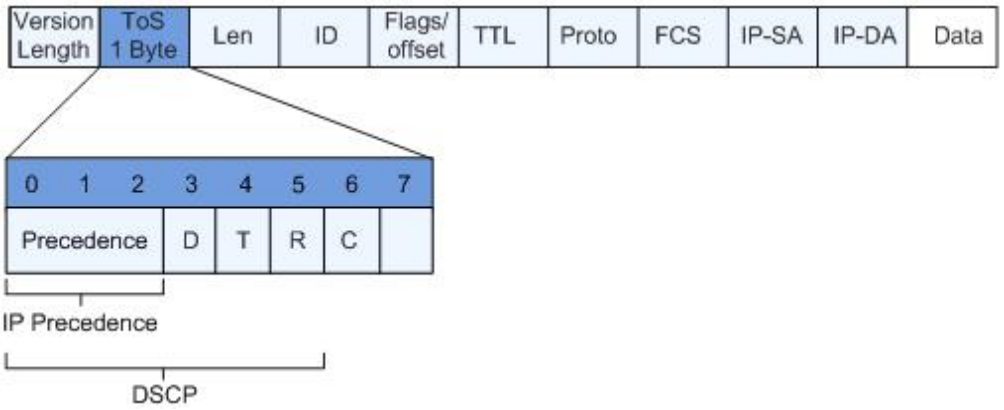


The 802.1Q header contains 3-bit PRI fields. PRI field defines 8 CoS of business priority ranging from 7 to 0 from high to low.

IP Precedence/DSCP Field

According to RFC791 definition, ToS (Type of Service) domain in the IP message header is composed of 8 bits. Among them, the 3-bit long Precedence field, as located in the following, identifies the IP message priority.

IP Precedence/DSCP Field



0 to 2 bits are Precedence fields representing the 8 priorities of message transmission ranging from 7 to 0 from high to low, with either Level 7 or 6 as the highest priority that is generally reserved for routing or updating network control communication. User-level applications only have access to Level 0 to 5.

ToS domain, in addition to Precedence fields, also includes D, T and R bits: D-bit represents the Delay requirement (0 for normal delay and 1 for low delay). T-bit represents the throughput (0 for normal throughput and 1 for high throughput). R-bit represents the reliability (0 for normal reliability and 1 for high reliability). ToS domain reserves the 6 and 7 bits.

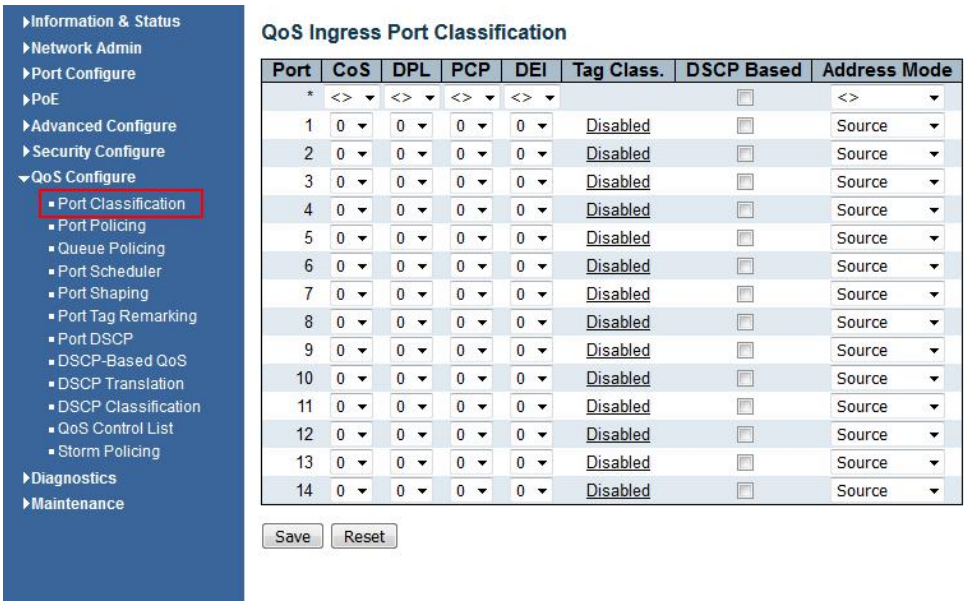
RFC1349 redefines the ToS domain by adding a C-bit to represent the Monetary Cost. The IETF DiffServ group then redefines the 0 to 5 bits of ToS domain in the IPv4 message header of RFC2474 as DSCP and renames it as DS (Differentiated Service) byte as shown in the figure above.

The first 6 bits (0-5 bits) of DS field distinguish the DSCP (DS Code Point), and the higher 2 bits (6-7 bits) are reserved. The lower 3 bits (0-2 bits) are CSCP (Class Selector Code Point), with the same CSCP value representing the DSCP of the same class. DS nodes select corresponding PHB (Per-Hop Behavior) according to DSCP values.

8.1 Port Classification

The switch configures 802.1p priority by default and distributes the info such as DPL, PCP and DEI to each port. The priority and valid priority are marked as 0 (the lowest) and 7 (the highest).

Click the “QoS Configure-Port Classification” as follows:



Interface data are as follows.

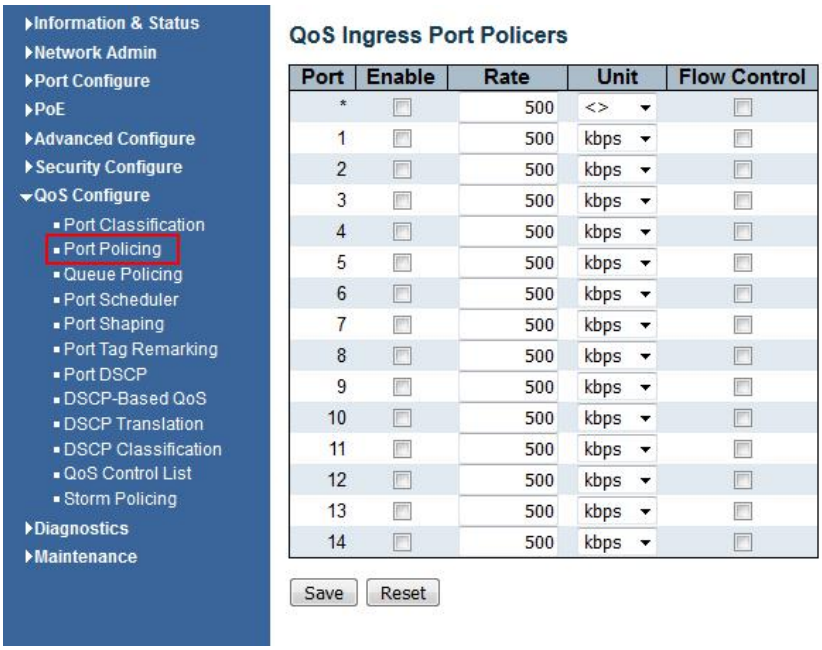
Configuration Items	Description
CoS	Controls the default class of service. All frames are classified to a CoS. There is a one to one mapping between CoS, queue and priority. A CoS of 0 (zero) has the lowest priority The classified CoS can be overruled by a QCL entry. Note: If the default CoS has been dynamically changed, then the actual default CoS is shown in parentheses after the configured default CoS.
DPL	Controls the default drop precedence level. All frames are classified to a drop precedence level. The classified DPL can be overruled by a QCL entry.
PCP	Controls the default PCP value. 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 DEI value. 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.
Address Mode	The IP/MAC address mode specifying whether the QCL classification must be based on source (SMAC/SIP) or destination (DMAC/DIP) addresses on this port. The allowed values are: Source: Enable SMAC/SIP matching. Destination: Enable DMAC/DIP matching.

"Save" and finish.

8.2 Port Policing

Click the "QoS Configure-Port Policing" as follows:



Interface data are as follows.

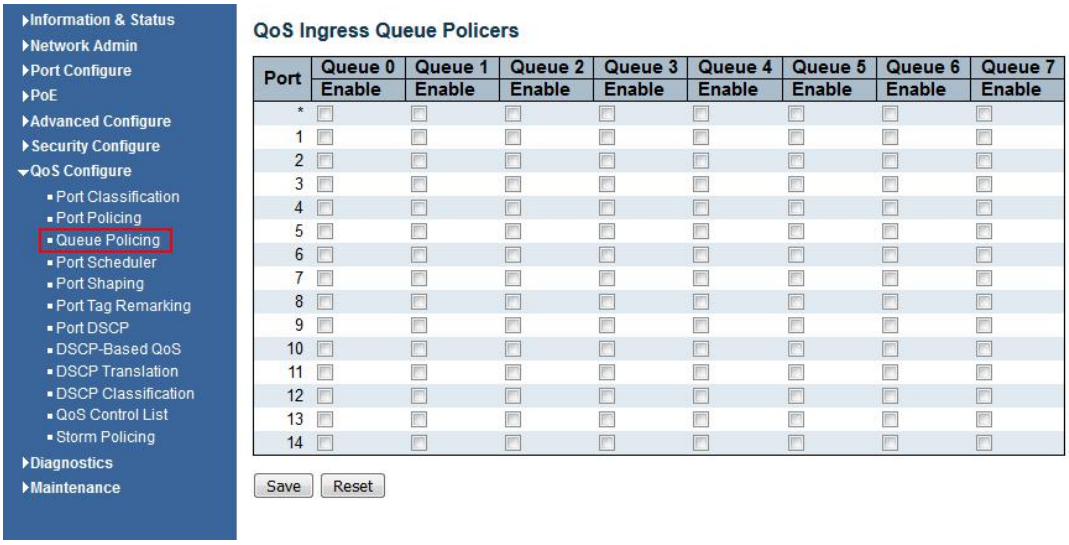
Configuration Items	Description
Enabled	Enable or disable the port ingress Policing.

Rate	Controls the rate for the policer. The default value is 500. This value is restricted to 100-1,000,000 when the “Unit” is “kbps” or “fps”, and it is restricted to 1-3,300 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.

“Save” and finish.

8.3 Queue Policing

Click the “QoS Configure-Queue Policing” as follows:



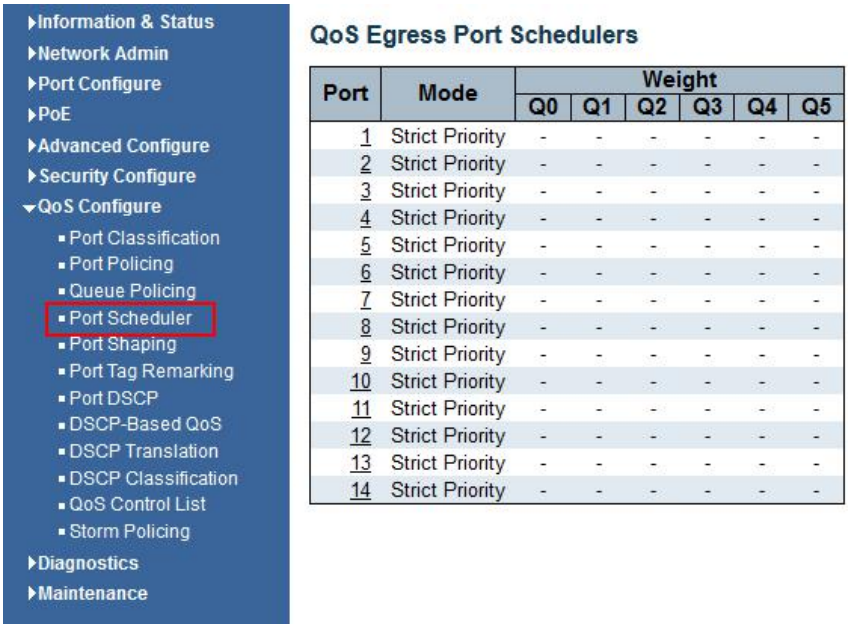
Interface data are as follows.

Configuration Items	Description
Queue0-7	Ingress queue policers

“Save” and finish.

8.4 Port Scheduler

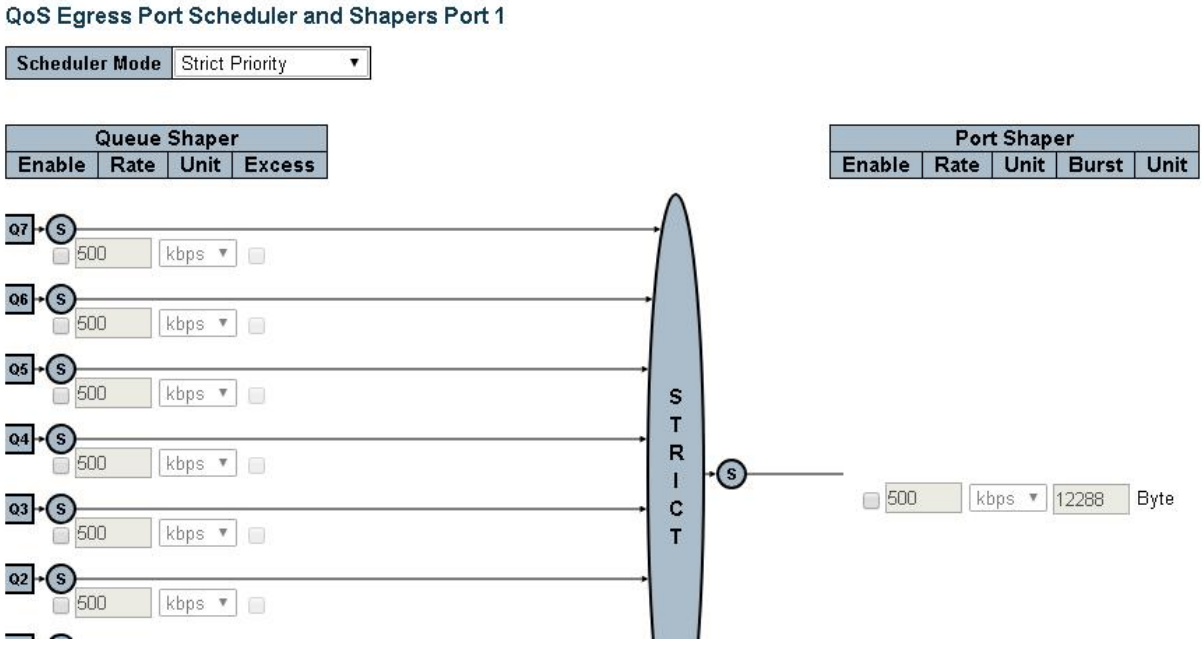
Click the “QoS Configure-Port Scheduler” as follows:



Interface data are as follows.

Configuration items	Description
QoS Egress Port Schedulers	Egress port schedulers

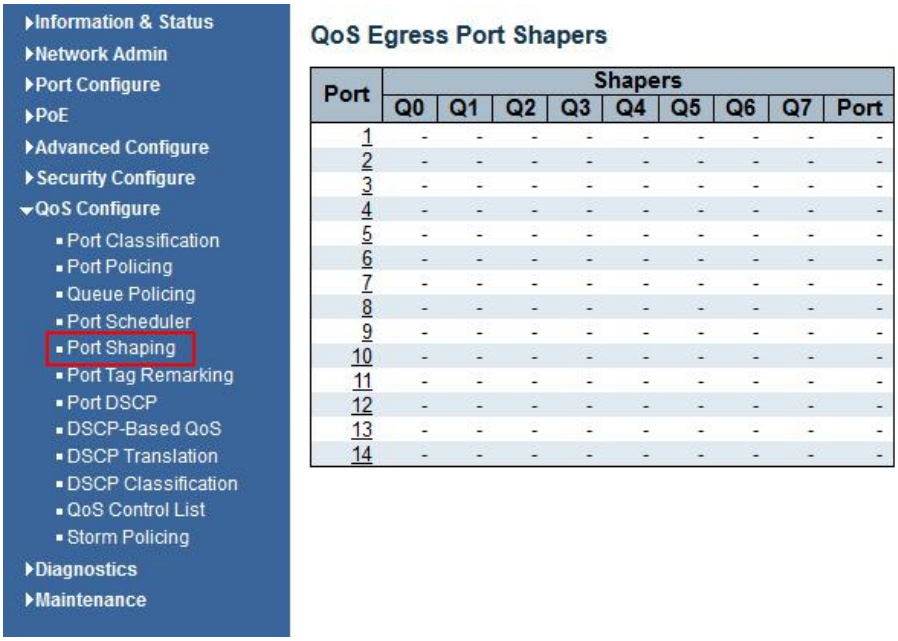
Click the “1”



“Save” and finish.

8.5 Port Shaping

Click the “QoS Configure-Port Shaping” as follows:



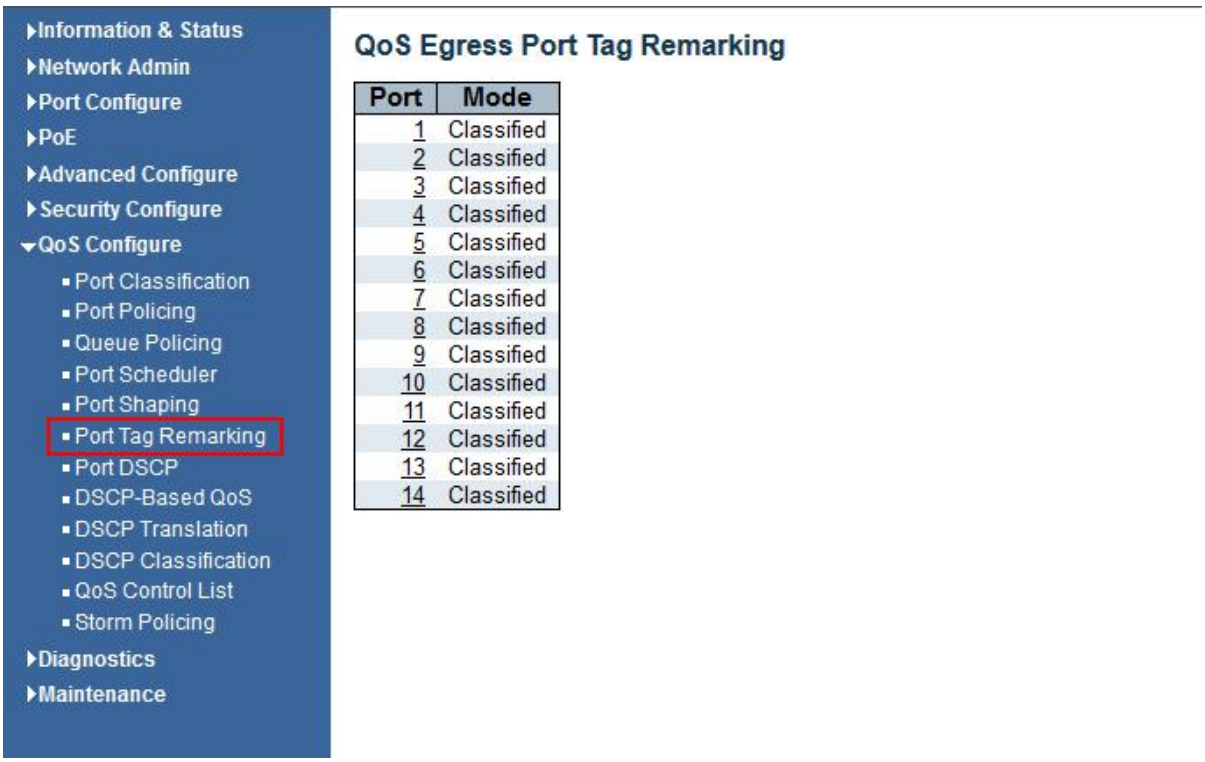
Interface data are as follows.

Configuration Items	Description
Scheduler Mode	Select the egress port scheduler from static and WRR

“Save” and finish.

8.6 Port Tag Remarking

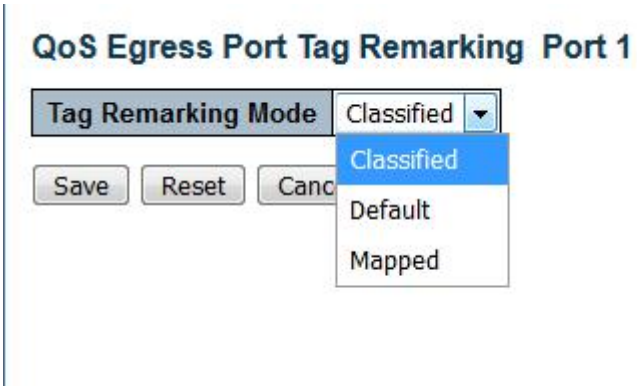
Click the “QoS Configure-Port Tag Remarking” as follows:



Interface data are as follows.

Configuration Items	Description
QoS Egress Port Tag Remarking	Egress port tag remarking

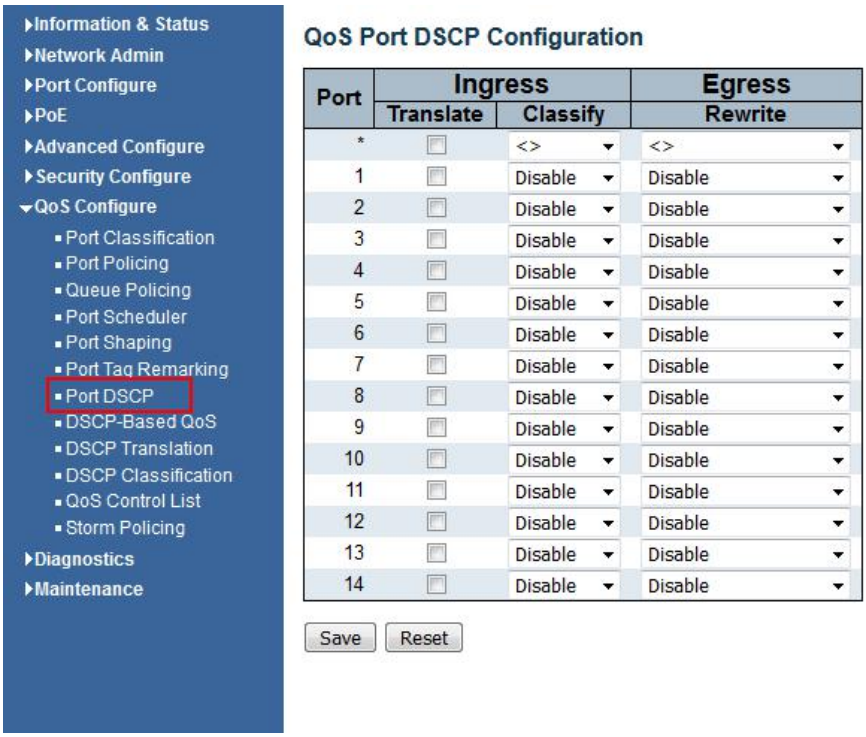
Click the “1”



“Save” and finish.

8.7 Port DSCP

Click the “QoS Configure-Port DSCP” as follows:



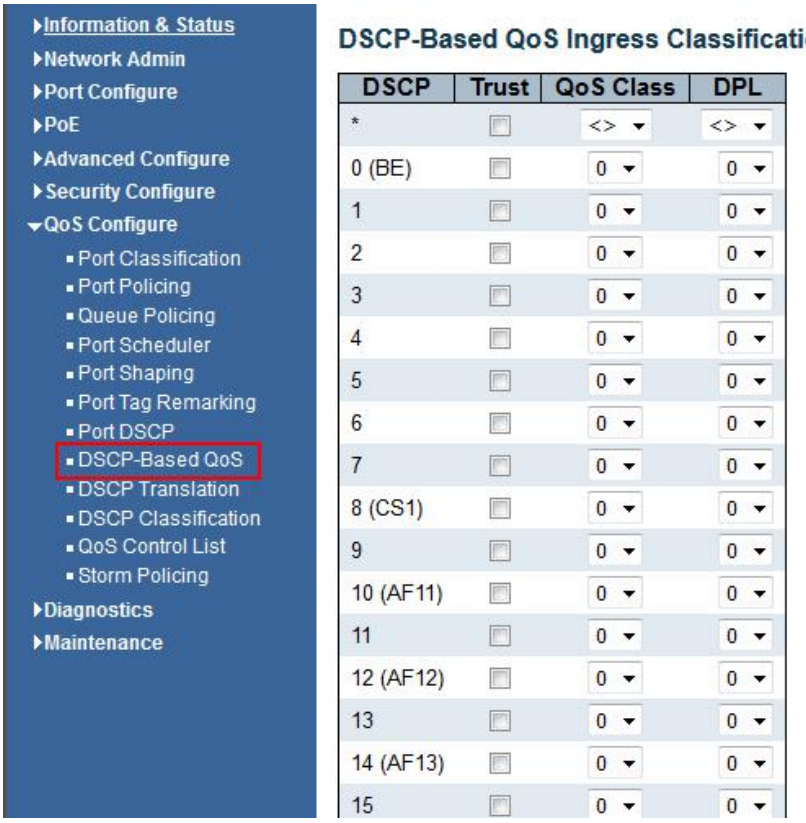
Interface data are as follows.

Configuration Items	Description
QoS Port DSCP Configuration	DSCP rewrite

“Save” and finish.

8.8 DSCP-Based QoS

Click the “QoS Configure- DSCP-Based QoS” as follows:



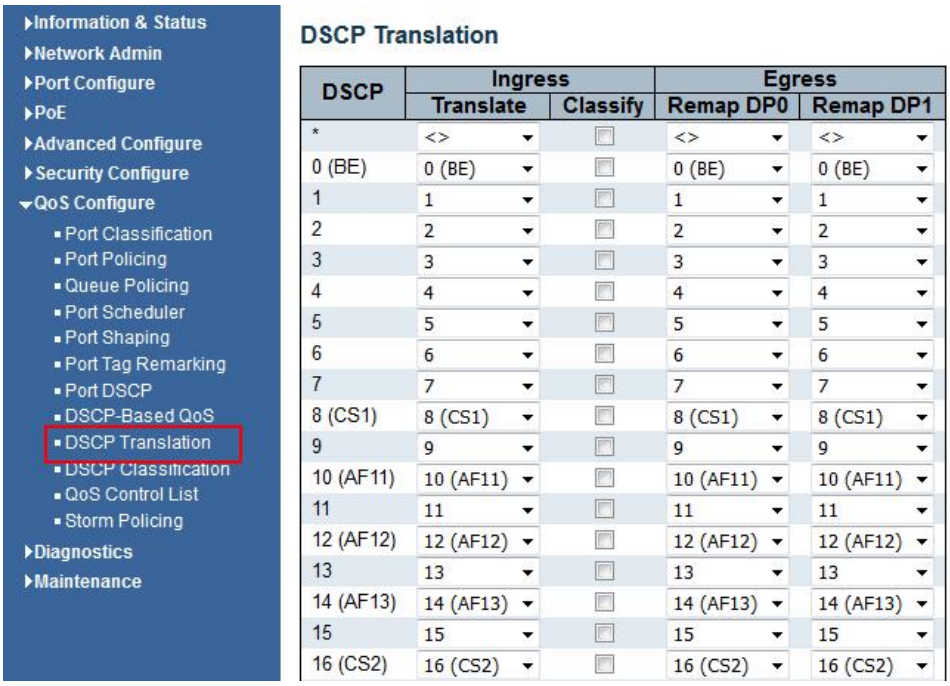
Interface data are as follows.

Configuration Items	Description
DSCP-Based QoS Ingress Classification	Select a trusted DSCP

"Save" and finish.

8.9 DSCP Translation

Click the "QoS Configure-DSCP Translation" as follows:



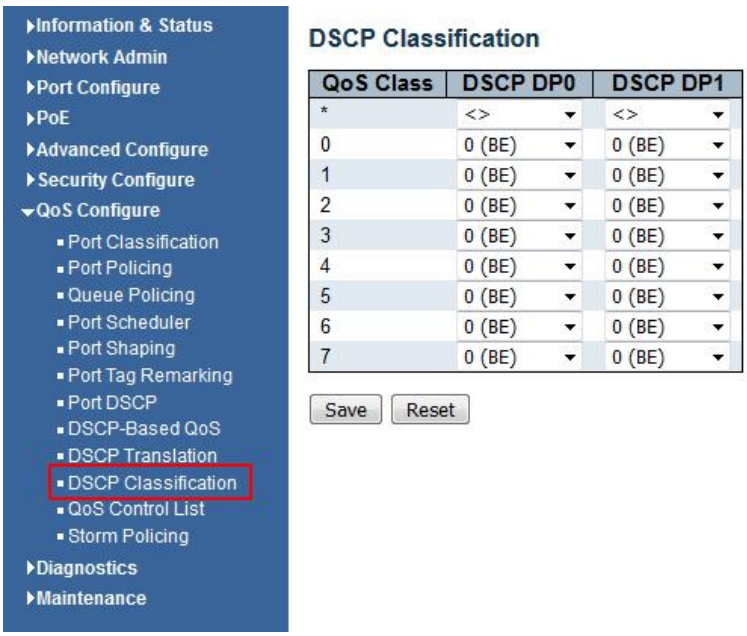
Interface data are as follows.

Configuration Items	Description
DSCP Translation	DSCP Translation

“Save” and finish.

8.10 DSCP Classification

Click the “QoS Configuration-DSCP Classification” as follows:



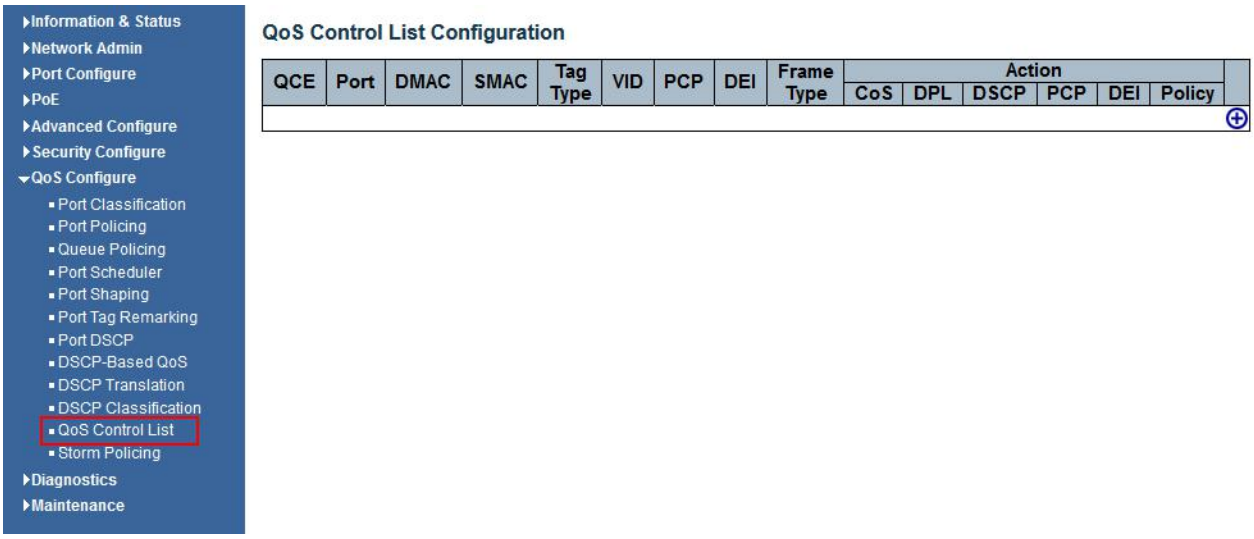
Interface data are as follows.

Configuration Items	Description
DSCP Classification	DSCP Classification

"Save" and finish.

8.11 QoS Control List

Click the "QoS Configure-QoS Control List" as follows:



Interface data are as follows.

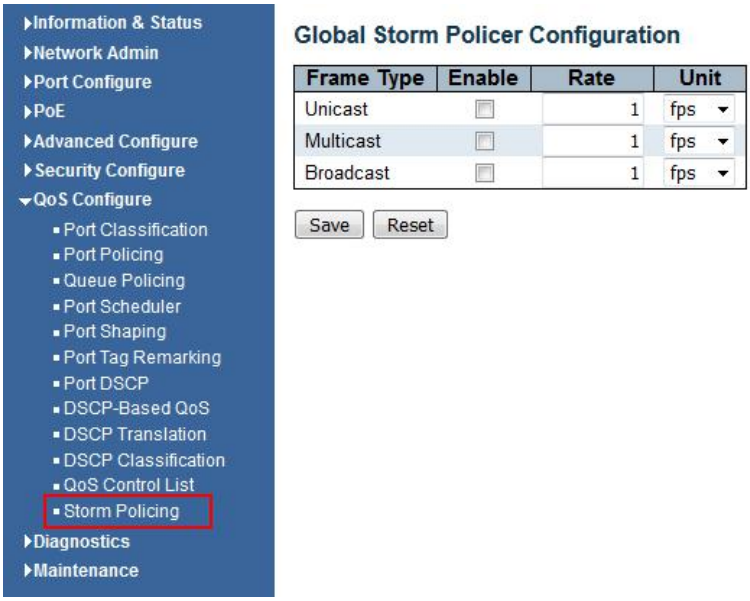
Configuration Items	Description
QCL	QoS ACL

Click the “+”

“Save” and finish.

8.12 Storm Policing

Click the “QoS Configure-Storm Policing” as follows:



Interface data are as follows.

Configuration Items	Description
Frame Type	The switch supports: Unknown Unicast, Unknown Multicast, and Broadcast
Enabled	Enable or disable the Storm Policing
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** or **1,024K**.

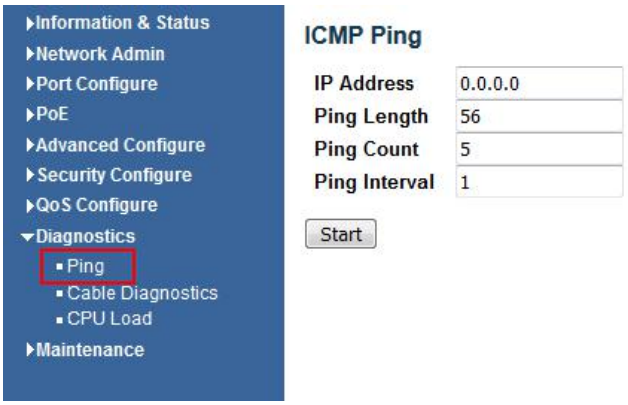
“Save” and finish.

9 Diagnostics

9.1 Ping

Destination node responds to the ICMP Echo packet sent from Ping to the specified IP address.

Click the “Diagnostics-Ping” as follows:



Followings are the fields that can be configured or displayed:

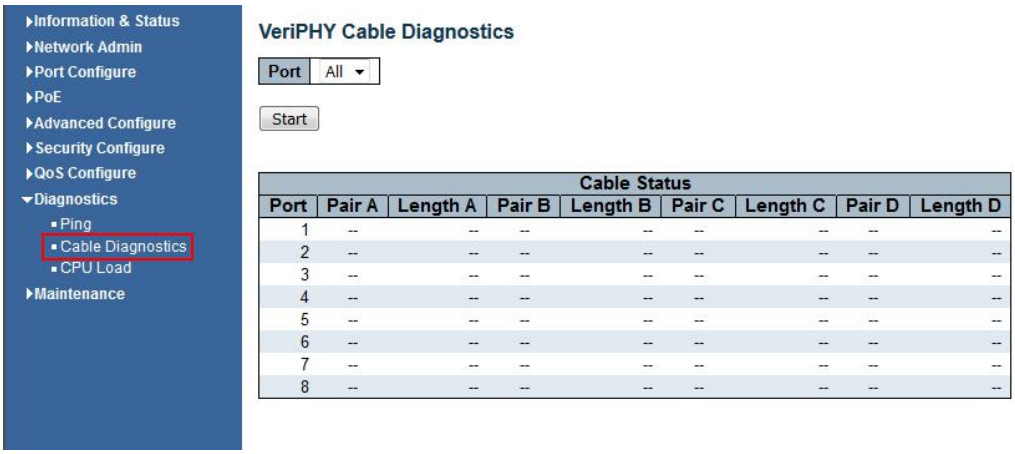
Configuration Items	Description
IP Address	Enter the IP Address to be pinged.
Ping Count	Enter the number of times (from 1 to 60) to ping the IPv4 or IPv6 address.
Ping Length	Enter a number ranging from 1-1,452, with 56 by default.
Ping Interval	Enter the ping interval

Click the “Start” for a ping test.

9.2 Cable Diagnostics

Use the cable states which can inspect the 10/100/1,000 BASE-T electrical interfaces, such as the state of open circuit, short circuit and length of line pairs.

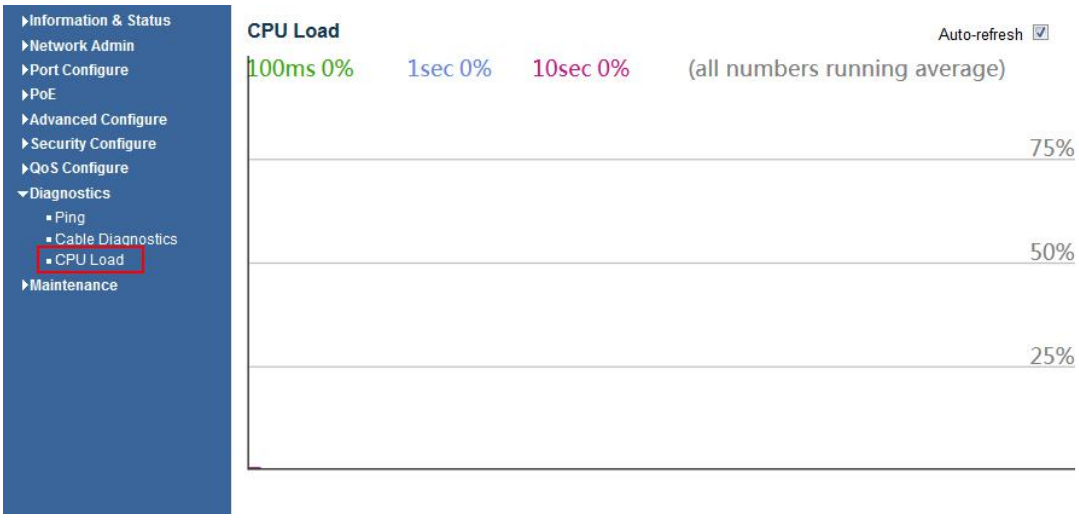
Click the “Diagnostics-Cable Diagnostics” as follows:



Click the “Start” for a “Cable Diagnostics” test.

9.3 CPU Load

Display the CPU load for users with an integer percentage and calculate the simple average at time intervals. Click the “Diagnostics-CPU Load” as follows:



10 Maintenance

10.1 Restart Device

Click the “Maintenance-Restart Device” to perform a restart.

Click the “Yes”.

10.2 Factory Defaults

Click the “Maintenance-Factory Defaults” to reset the configuration to factory defaults.

Click the “Yes”.

10.3 Firmware Upgrade

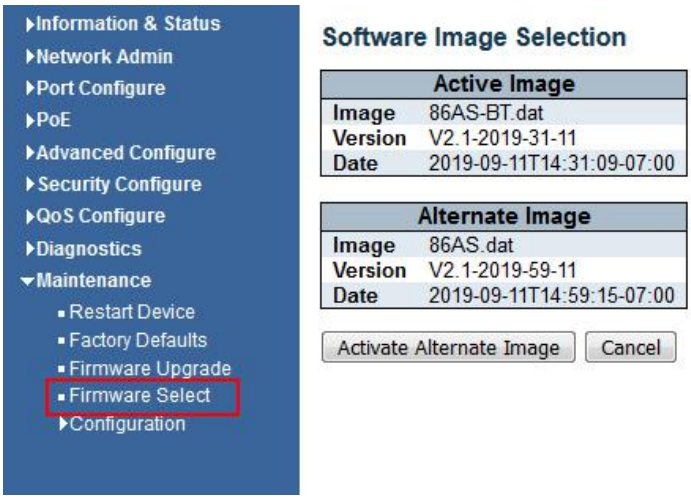
Click the “Maintenance-Firmware Upgrade” to upgrade.

Click the “Browse” to select the firmware documents for upgrade.

Click the “Upload” for firmware upgrade.

10.4 Firmware Select

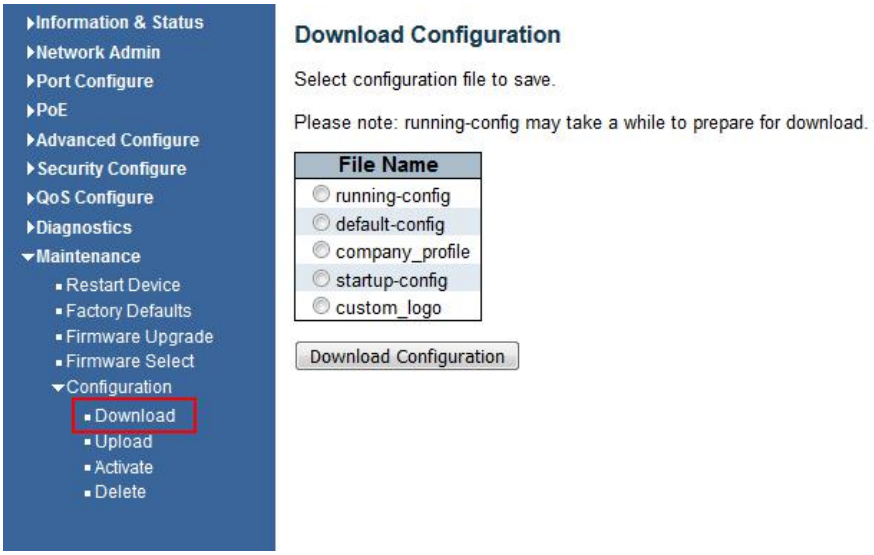
Click the “Maintenance-Firmware Select” to switch the spare firmware.



Click the “Activate Alternate Image” to switch firmware.

10.5 Configuration

1. Click the “Maintenance-Configuration-Download” to download the configuration-related documents.

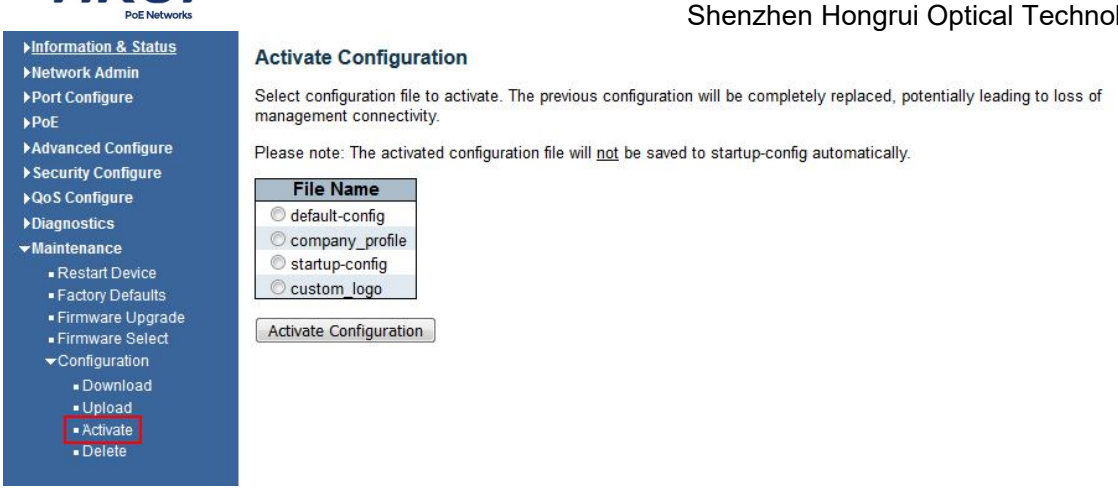


Click the “Download Configuration”.

2. Click the “Maintenance-Configuration-Upload” to upload the configuration-related documents.

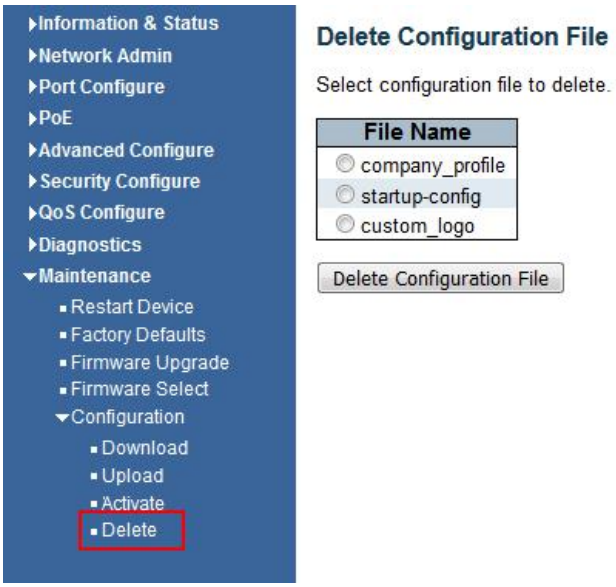
Click the “Upload”.

3. Click the “Maintenance-Configuration-Activate” to activate the configuration-related documents.



Click the “Activate Configuration”.

4. Click the “Maintenance – Configuration-Delete” to delete the configuration-related documents.



Click the “Delete Configuration File”.