

# **24-Port Gigabit + 4-Port Gigabit Combo Base-T/SFP L2 Managed PoE Switch**



## **User Manual**

**Copyright Statement**

Our company reserves all copyrights of this document. Any reproduction, excerption, backup, modification, transmission, translation or commercial use of this document or any portion of this document, in any form or by any means, without the prior written consent of our company is prohibited.

**Exemption Statement**

This document is provided "as is". The contents of this document are subject to change without any notice. Please obtain the latest information through our company website. Our company endeavors to ensure content accuracy and will not shoulder any responsibility for losses and damages caused due to content omissions, inaccuracies or errors.

# Table of Contents

<b>1. Product Introduction .....</b>	<b>- 1 -</b>
1.1. Product Overview.....	- 1 -
1.2. Features .....	- 1 -
1.3. External Component Description .....	- 2 -
1.3.1. Front Panel .....	- 2 -
1.3.2. Rear Panel.....	- 3 -
1.4. Package Contents.....	- 4 -
<b>2. Installing and Connecting the Switch .....</b>	<b>- 5 -</b>
2.1. Installation .....	- 5 -
2.1.1. Desktop Installation .....	- 5 -
2.1.2. Rack-mountable Installation in 19-inch Cabinet.....	- 5 -
2.1.3. Power on the Switch .....	- 6 -
2.2. Connect Computer (NIC) to the Switch .....	- 6 -
<b>3. How to Login the Switch .....</b>	<b>- 7 -</b>
3.1. Switch to End Node .....	- 7 -
3.2. How to Login the Switch .....	- 7 -
<b>4. WEB Configuration Guide .....</b>	<b>- 9 -</b>
4.1. Basic Setting .....	- 9 -
4.1.1. System Info.....	- 9 -
4.1.2. General Setup.....	- 10 -
4.1.3. IP Setup .....	- 11 -
4.1.3.1. Vlan interface.....	- 11 -
4.1.3.2. Vlan interface Config.....	- 12 -
4.1.4. Port Setup.....	- 13 -
4.2. Advanced Application .....	- 15 -
4.2.1. VLAN.....	- 16 -
4.2.1.1. VLAN Status .....	- 17 -
4.2.1.2. VLAN Port Settings .....	- 17 -
4.2.1.3. Static VLAN .....	- 19 -
4.2.2. MAC Address Forwarding .....	- 20 -
4.2.3. Loopback Detection .....	- 22 -
4.2.4. Spanning Tree Protocol.....	- 22 -
4.2.4.1. Spanning Tree Protocol Status .....	- 23 -
4.2.4.2. Spanning Tree Configuration .....	- 24 -

4.2.4.3. Compatible/Rapid Spanning Tree Protocol .....	- 25 -
4.2.4.4. Multiple Spanning Tree Protocol .....	- 28 -
4.2.5. Bandwidth Control .....	- 29 -
4.2.6. Broadcast Storm Control .....	- 29 -
4.2.7. Mirroring.....	- 31 -
4.2.8. Link Aggregation.....	- 32 -
4.2.8.1. Link Aggregation status.....	- 32 -
4.2.8.2. Link Aggregation Setting .....	- 33 -
4.2.8.3. Link Aggregation Control Protocol .....	- 34 -
4.2.9. POE Settings .....	- 34 -
4.2.9.1. POE Settings .....	- 35 -
4.2.9.2. POE Port Settings .....	- 36 -
4.2.10. Classifier .....	- 37 -
4.2.11. Policy Rule .....	- 37 -
4.2.12. Queuing Method .....	- 38 -
4.2.13. Multicast.....	- 40 -
4.2.13.1. Multicast Status .....	- 40 -
4.2.13.2. Multicast Settings .....	- 40 -
4.2.13.3. IGMP Snooping Dney VLAN .....	- 41 -
4.2.13.4. IGMP Filtering Profile .....	- 42 -
4.2.14. IPv6 Multicast .....	- 43 -
4.2.14.1. IPv6 Multicast Status.....	- 44 -
4.2.14.2. IPv6 Multicast Setting.....	- 44 -
4.2.14.3. MLD Snooping Dney VLAN.....	- 46 -
4.2.15. Dos attack protect.....	- 46 -
4.2.16. DHCP Snooping Setting.....	- 47 -
4.2.16.1. DHCP Snooping Setting.....	- 48 -
4.2.16.2. IP Source Guard.....	- 49 -
4.2.17. SNTP Setting .....	- 50 -
4.2.18. LLDP Protocol.....	- 52 -
4.2.18.1. LLDP Status .....	- 52 -
4.2.18.2. LLDP Setting .....	- 53 -
4.2.19. AAA.....	- 54 -
4.2.19.1. 802.1x.....	- 54 -
4.2.19.2. Radius Domain.....	- 55 -
4.2.19.3. Remote Authentication.....	- 56 -
4.2.19.4. TACACS+ Server Setup.....	- 56 -
4.2.19.5. Radius Server Setup .....	- 57 -
4.2.20. EEE .....	- 58 -
4.2.21. ARP Safeguarding .....	- 59 -
4.3. Management .....	- 60 -
4.3.1. Management & Maintenance.....	- 60 -
4.3.2. Access Control.....	- 61 -
4.3.2.1. SNMP .....	- 61 -

4.3.2.2. User Information.....	- 63 -
4.3.2.3. Logins .....	- 64 -
4.3.3. Diagnostic .....	- 65 -
4.3.4. Syslog .....	- 66 -
4.3.4.1. Syslog Setup .....	- 67 -
4.3.4.2. Syslog Server Setup.....	- 68 -
<b>Appendix: Technical Specifications.....</b>	<b>- 70 -</b>

# 1. Product Introduction

Congratulations on your purchasing of the 24-Port Gigabit + 4-Port Gigabit Combo Base-T/SFP L2 Managed PoE Switch. Before you install and use this product, please read this manual carefully for full exploiting the functions of this product.

## 1.1. Product Overview

The Switch is a high performance the second managed gigabit switch. Provides twenty-four 10/100/1000Mbps self-adaption RJ45 ports, plus four gigabit Combo ports, it can be used to link bandwidth higher upstream equipment. Support VLAN ACL based on port, easily implement network monitoring, traffic regulation, priority tag and traffic control. Support traditional STP/RSTP/MSTP 2 link protection technology; greatly improve the ability of fault tolerance, redundancy backup to ensure the stable operation of the network. Support ACL control based on the time, easy control the access time accurately. Support 802.1x authentication based on the port and MAC, easily set user access. Perfect QOS strategy and plenty of VLAN function. PoE ports can automatically detect and supply power with those IEEE 802.3at/af compliant Powered Devices (PD). In this situation, the electrical power is transmitted along with data in one single cable allowing you to expand your network where there are no power lines or outlets, where you wish to fix devices such as AP, IP Cameras or IP Phones, etc

## 1.2. Features

- Comply with IEEE802.3i, IEEE802.3u, IEEE802.3ab, IEEE802.3x, IEEE802.3z, IEEE802.3ad ,standards
- Supports IEEE802.3at/af PoE standards
- Supports PoE power up to 30W for each PoE port, total power up to 370W for all PoE ports
- Supports IEEE802.3x flow control for Full-duplex Mode and backpressure for Half-duplex Mode
- Supports MAC address auto-learning and auto-aging
- Store and forward mode operates
- Support SNMP/RMON/TELENT
- Supports IEEE802.1Q VLAN,4K VLAN Table
- Support IEEE802.1p Priority Queues
- Support 2K+256-entry ingress and egress ACL
- Support Storm Control
- Support QoS, Port Mirroring, Link Aggregation Protocol
- LED indicators for monitoring PSE, Link/Activity/Speed
- Web-based Management Support

### 1.3. External Component Description

#### 1.3.1. Front Panel

The front panel of the Switch consists of a series of LED indicators, a reset button, 24 x 10/100/1000Mbps RJ-45 ports, 4 x Combo ports and a console port.



Figure 1 - Front Panel

#### LED indicators:

The LED Indicators will allow you to monitor, diagnose and troubleshoot any potential problem with the Switch, connection or attached devices.

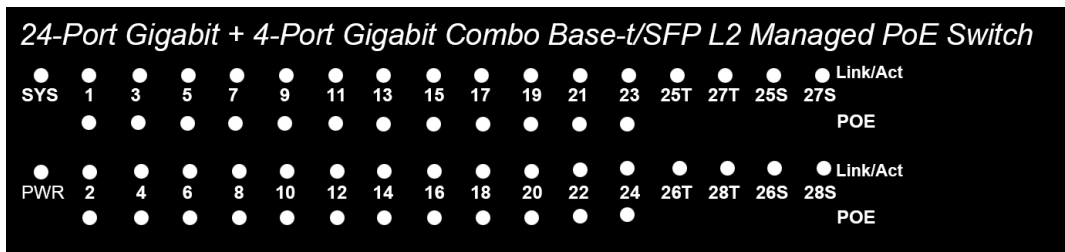


Figure 2 - LED Indicator

The following chart shows the LED indicators of the Switch along with explanation of each indicator.

LED Indicator	Faceplate Marker	Status	Indication
Power Indicator	PWR	Off	Power Off
		Solid green	Power On
System Indicator	SYS	Off	System not started
		Blinking green	System is normal
10/100 BASE-T adaptive Ethernet port indicators (1-24, 25T-28T)	Link/Act/Speed	Off	The port is NOT connected.
		Solid green	The port is connected at 1000Mbps.
		Solid orange	The port is connected at 100/10Mbps.
		Blinking	The port is transmitting or receiving data.

SFP port indicators (25-28S)	Link/Act	Off	The port is NOT connected.
		Solid green	The port is connected
		Blinking	The port is transmitting or receiving data.
PoE status indicators	POE	Off	No PD is connected to the corresponding port, or no power is supplied according to the power limits of the port
		Solid yellow	A Powered Device is connected to the port, which supply power successfully.
		Blinking	The PoE power circuit may be in short or the power current may be overloaded

#### 10/100/1000 Mbps RJ-45 ports (1~24):

Designed to connect to the device with a bandwidth of 10Mbps, 100Mbps. Each has a corresponding Link/Act/Speed indicator.

#### Combo ports (25-28S, 25-28T):

Designed to install the SFP module. The switch features four SFP receiver slots, which are Shared with four related RJ45 ports (25-28T). An SFP port and a related RJ45 port are called "composite" ports, which means that they can't be used at the same time, only the SFP port works or only the RJ45 port works simultaneously.

#### Console port (Console):

Designed to connect with the serial port of a computer or terminal for monitoring and configuring the Switch.

### 1.3.2. Rear Panel

The rear panel of the Switch contains one Grounding Terminal and AC power connector shown as below.



Figure 3 - Rear Panel



**Grounding Terminal:**

Located on the left side of the power supply connector, use wire grounding to lightning protection.

**AC Power Connector:**

Power is supplied through an external AC power adapter. It supports AC 100~240V, 50/60Hz.

## **1.4. Package Contents**

Before installing the Switch, make sure that the following the "packing list" listed OK. If any part is lost and damaged, please contact your local agent immediately. In addition, make sure that you have the tools install switches and cables by your hands.

- One 24-Port Gigabit + 4-Port Gigabit Combo Base-T/SFP L2 Managed PoE Switch
- One Installation Component.
- One AC power cord.
- One User Manual.

## 2. Installing and Connecting the Switch

This part describes how to install your Ethernet Switch and make connections to it. Please read the following topics and perform the procedures in the order being presented.

### 2.1. Installation

Please follow the following instructions in avoid of incorrect installation causing device damage and security threat.

- Put the Switch on stable place or desktop in case of falling damage.
- Make sure the Switch works in the proper AC input range and matches the voltage labeled on the Switch.
- To keep the Switch free from lightning, do not open the Switch's shell even in power failure.
- Make sure that there is proper heat dissipation from and adequate ventilation around the Switch.
- Make sure the cabinet to enough back up the weight of the Switch and its accessories.

#### 2.1.1. Desktop Installation

Sometimes users are not equipped with the 19-inch standard cabinet. So when installing the Switch on a desktop, please attach these cushioning rubber feet provided on the bottom at each corner of the Switch in case of the external vibration. Allow adequate space for ventilation between the device and the objects around it.

#### 2.1.2. Rack-mountable Installation in 19-inch Cabinet

The Switch can be mounted in an EIA standard-sized, 19-inch rack, which can be placed in a wiring closet with other equipment. To install the Switch, please follow these steps:

- A. attach the mounting brackets on the Switch's side panels (one on each side) and secure them with the screws provided.

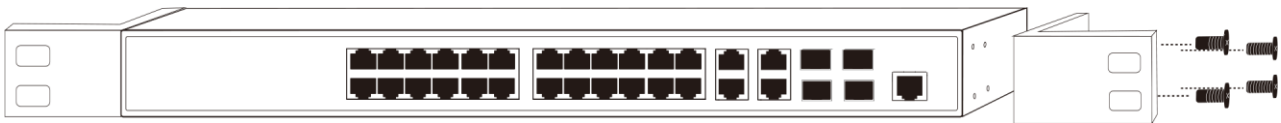


Figure 4 - Bracket Installation

- B. Use the screws provided with the equipment rack to mount the Switch on the rack and tighten it.

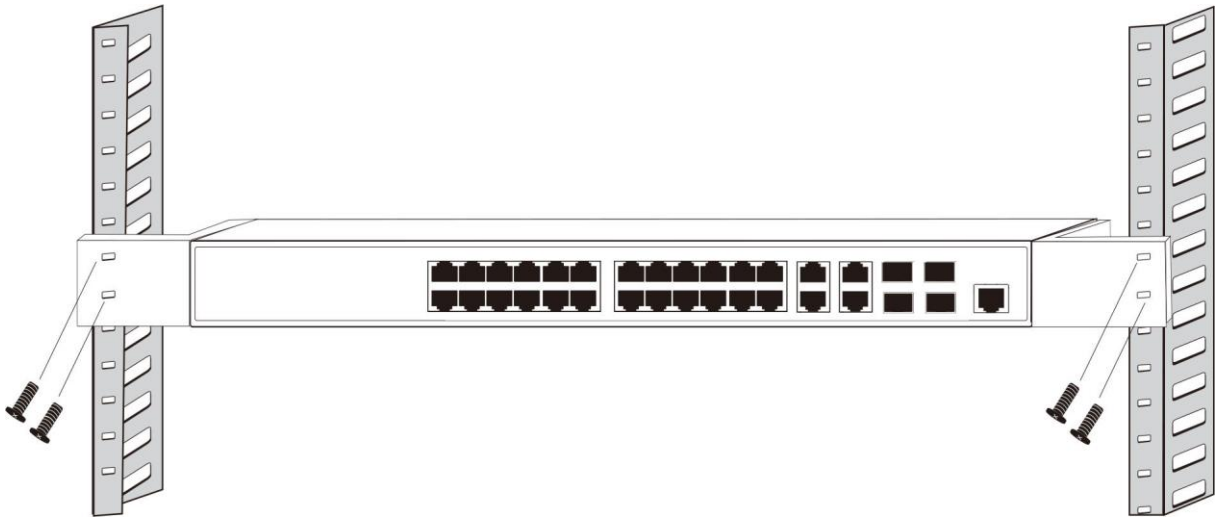


Figure 5 - Rack Installation

### 2.1.3. Power on the Switch

The Switch is powered on by the AC 100-240V 50/60Hz internal high-performance power supply. Please follow the next tips to connect:

#### AC Electrical Outlet:

It is recommended to use single-phase three-wire receptacle with neutral outlet or multifunctional computer professional receptacle. Please make sure to connect the metal ground connector to the grounding source on the outlet.

#### AC Power Cord Connection:

Connect the AC power connector in the back panel of the Switch to external receptacle with the included power cord, and check the power indicator is ON or not. When it is ON, it indicates the power connection is OK.

## 2.2. Connect Computer (NIC) to the Switch

Please insert the NIC into the computer, after installing network card driver, please connect one end of the twisted pair to RJ-45 jack of your computer, the other end will be connected to any RJ-45 port of the Switch, the distance between Switch and computer is around 100 meters. Once the connection is OK and the devices are power on normally, the LINK/ACT/Speed status indicator lights corresponding ports of the Switch.

## 3. How to Login the Switch

### 3.1. Switch to End Node

Use standard Cat.5/5e Ethernet cable (UTP/STP) to connect the Switch to end nodes as described below. Switch ports will automatically adjust to the characteristics (MDI/MDI-X, speed, duplex) of the device to which is connected.

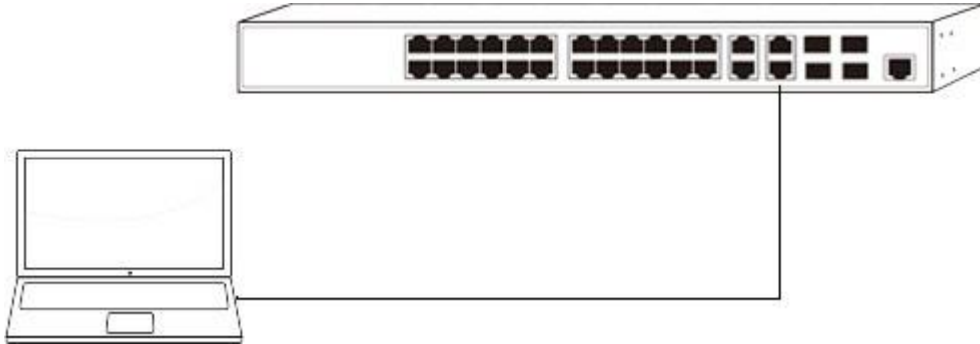


Figure 6 - Connect PC to Switch

Please refer to the LED Indicators. The LINK/ACT/Speed LEDs for each port lights on when the link is available.

### 3.2. How to Login the Switch

As the Switch provides Web-based management login, you can configure your computer's IP address manually to log on to the Switch. The default settings of the Switch are shown below.

Parameter	Default Value
Default IP address	192.168.0.1
Default user name	admin
Default password	admin

You can log on to the configuration window of the Switch through following steps:

1. Connect the Switch with the computer NIC interface.
2. Power on the Switch.
3. Check whether the IP address of the computer is within this network segment: 192.168.0.xxx ("xxx" ranges 2~254), for example, 192.168.0.100.
4. Open the browser, and enter <http://192.168.0.1> and then press "Enter". The Switch login window appears, as shown below.

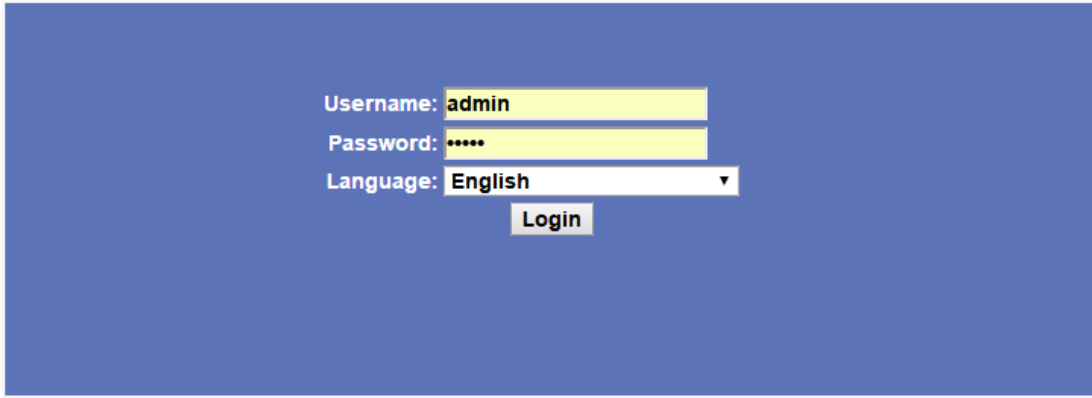
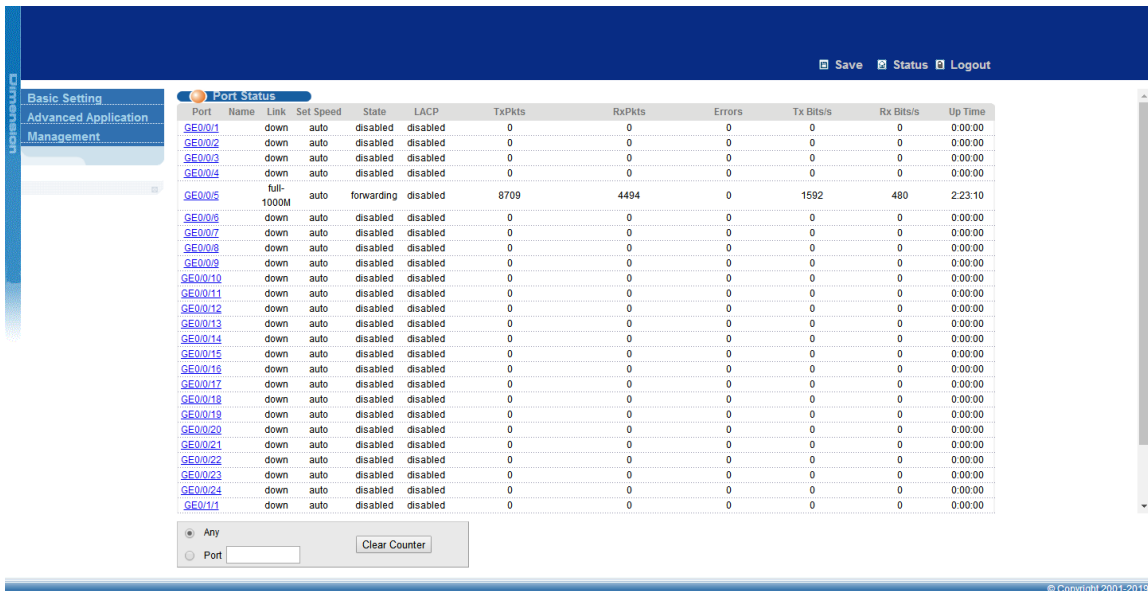


Figure 7- Login Windows

5. Switching language to English .Enter the Username and Password (The factory default Username is **admin** and Password is **admin**), and then click "**Login**" to log in to the Switch configuration window



## 4. WEB Configuration Guide

Switch configuration interface consists of 3 main areas, areas for the status bar at the top, the area on the left menu bar, right the main configuration window. Select the different functions in the function menu bar, you can modify all settings in the main configuration window.

Port	Name	Link	Set Speed	State	LACP	TxPkts	RxPkts	Errors	Tx Bits/s	Rx Bits/s	Up Time
GE0/0/1		down	auto	disabled	disabled	0	0	0	0	0	0:00:00
GE0/0/2		down	auto	disabled	disabled	0	0	0	0	0	0:00:00
GE0/0/3		down	auto	disabled	disabled	0	0	0	0	0	0:00:00
GE0/0/4		down	auto	disabled	disabled	0	0	0	0	0	0:00:00
GE0/0/5		full-100M	auto	forwarding	disabled	8709	4494	0	1592	480	2:23:10
GE0/0/6		down	auto	disabled	disabled	0	0	0	0	0	0:00:00
GE0/0/7		down	auto	disabled	disabled	0	0	0	0	0	0:00:00
GE0/0/8		down	auto	disabled	disabled	0	0	0	0	0	0:00:00
GE0/0/9		down	auto	disabled	disabled	0	0	0	0	0	0:00:00
GE0/0/10		down	auto	disabled	disabled	0	0	0	0	0	0:00:00
GE0/0/11		down	auto	disabled	disabled	0	0	0	0	0	0:00:00
GE0/0/12		down	auto	disabled	disabled	0	0	0	0	0	0:00:00
GE0/0/13		down	auto	disabled	disabled	0	0	0	0	0	0:00:00
GE0/0/14		down	auto	disabled	disabled	0	0	0	0	0	0:00:00
GE0/0/15		down	auto	disabled	disabled	0	0	0	0	0	0:00:00
GE0/0/16		down	auto	disabled	disabled	0	0	0	0	0	0:00:00
GE0/0/17		down	auto	disabled	disabled	0	0	0	0	0	0:00:00
GE0/0/18		down	auto	disabled	disabled	0	0	0	0	0	0:00:00
GE0/0/19		down	auto	disabled	disabled	0	0	0	0	0	0:00:00
GE0/0/20		down	auto	disabled	disabled	0	0	0	0	0	0:00:00
GE0/0/21		down	auto	disabled	disabled	0	0	0	0	0	0:00:00
GE0/0/22		down	auto	disabled	disabled	0	0	0	0	0	0:00:00
GE0/0/23		down	auto	disabled	disabled	0	0	0	0	0	0:00:00
GE0/0/24		down	auto	disabled	disabled	0	0	0	0	0	0:00:00
GE0/1/1		down	auto	disabled	disabled	0	0	0	0	0	0:00:00

### 4.1. Basic Setting

Choose Basic Setting, and the following page appears. There are "System Info", "General Setup", "IP Setup" and "Port Setup" configuration web pages.

Basic Setting
Advanced Application
Management
System Info
General Setup
IP Setup
Port Setup

#### 4.1.1. System Info

Selecting "Basic Setting>System Information settings" in the navigation bar, you can view the basic information of System and configure the IP address and System name.

##### 【Parameter Description】

Parameter	Description
Product description	Brief description of device type.
Software version	Show switch's current Software version.
MAC address	Show switch's physical address
IP Address	The management IP of Switch
Subnet Mask	Config the corresponding subnet mask of the

Parameter	Description
	IP address specified above. The default is 255.255.255.0.
Gateway	Specify a gateway address for the switch.
System name	System name
System Location	Specify the system location

#### 【Instructions】

You can view and configure Running System status.

### 4.1.2. General Setup

Selecting "**Basic Setting>General Setup**" in the navigation bar, you can view the basic information of Switch, Such as System description and so on. You can also modify System name, System contact and System location.

#### 【Parameter Description】

Parameter	Description
System name	System name
System Location	Specify the system location
System contact	Including company or related URL
Product description	Brief description of device type.

#### 【Configuration example】

To configure general system information:

1. Click Basic Setting > General Setup.
2. Specify the system name as Switch, location as office, and contact information as admin for the system administrator.
3. Click Apply

### 4.1.3. IP Setup

Selecting “**Basic Setting>IP Setup**” in the navigation bar, you can configure IP.

**Basic Setting**  
Advanced Application  
Management

System Info  
General Setup  
**IP Setup**  
Port Setup

**Vlan Interface** [VlanInterfaceConf](#)

Create:

Interface: vlan-interface  
Vlan ID: 1

Add Cancel Clear

List:

Index	Name	Primary ipaddress	VLAN	Status	Delete
1	<a href="#">VLAN-IF1</a>	192.168.1.1	1	Up	<input type="checkbox"/>

Delete Cancel

#### 4.1.3.1. Vlan interface

Selecting “**Basic Setting>IP Setup>Vlan interface**” in the navigation bar, you can configure Vlan interface.

**Vlan Interface** [VlanInterfaceConf](#)

Create:

Interface: vlan-interface  
Vlan ID: 1

Add Cancel Clear

List:

Index	Name	Primary ipaddress	VLAN	Status	Delete
1	<a href="#">VLAN-IF1</a>	192.168.1.1	1	Up	<input type="checkbox"/>

Delete Cancel

#### 【Parameter Description】

Parameter	Description
Interface	Selecting the interface: vlan-interface Supervlan-interface
Vlan ID	You can specify the vlan ID
Name	The name of interface



### 4.1.3.2. Vlan interface Config

Selecting “**Basic Setting>IP Setup>Vlan interface**” in the navigation bar, you can configure Vlan interface.

**Vlan Interface Config**
[VlanInterface](#)

**Interface:**

Interface name	VLAN-IF1 ▾
Vlan ID	1

**IP Add:**

Mode	Ip Address ▾
Ip Address	<input type="text"/>
Mask	<input type="text"/>
Override	<input type="checkbox"/>

**IP List:**

Index	Ip	Mask	Primary	Delete
<a href="#">1</a>	192.168.1.1	255.0.0.0	<input checked="" type="radio"/>	<input type="checkbox"/>

#### 【Parameter Description】

Parameter	Description
Interface name	Name of interface
Vlan ID	You can specify the vlan ID
IP Address	User login in Switch using the IP Address
Override	You can override former original primary IP or not

#### 【Configuration example】

To configure general system information:

1. Click Basic Setting > IP Setup >Vlan interface Config .
2. Specify the IP Address as 192.168.2.1.
3. Click Add.

**Vlan Interface Config** [VlanInterface](#)

**Interface:**

Interface name: VLAN-IF1  
 Vlan ID: 1

Apply Cancel

**IP Add:**

Mode: Ip Address  
 Ip Address: 192.168.2.1  
 Mask: 255.255.255.0  
 Override:

Add Cancel Clear

**IP List:**

Index	Ip	Mask	Primary	Delete
1	192.168.1.1	255.0.0.0	<input checked="" type="radio"/>	<input type="checkbox"/>

Modify Delete Cancel

#### 4.1.4. Port Setup

Selecting “**Basic Setting>Port Setup**” in the navigation bar, you can configure the related parameter of port.

**Basic Setting** **Port basic settings**

Advanced Application Management

System Info General Setup IP Setup **Port Setup**

Port Number [Click for selecting]

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

Port basic settings Ethernet 1000M Port[1]

Port	Status	Link	Priority	Set speed	Mode	Actual speed	Port description (0-128 chars)
GE0/0/1	enable	down	0	auto	auto	unknown	

Refresh Modify

Ethernet 1000M Port

Port	Status	Link	Priority	Set speed	Mode	Actual speed	Port description (0-128 chars)
GE0/0/1	enable	down	0	auto	auto	unknown	
GE0/0/2	enable	down	0	auto	auto	unknown	
GE0/0/3	enable	down	0	auto	auto	unknown	
GE0/0/4	enable	down	0	auto	auto	unknown	
GE0/0/5	enable	up	0	auto	auto	full-1000M	
GE0/0/6	enable	down	0	auto	auto	unknown	
GE0/0/7	enable	down	0	auto	auto	unknown	
GE0/0/8	enable	down	0	auto	auto	unknown	
GE0/0/9	enable	down	0	auto	auto	unknown	
GE0/0/10	enable	down	0	auto	auto	unknown	
GE0/0/11	enable	down	0	auto	auto	unknown	
GE0/0/12	enable	down	0	auto	auto	unknown	
GE0/0/13	enable	down	0	auto	auto	unknown	
GE0/0/14	enable	down	0	auto	auto	unknown	
GE0/0/15	enable	down	0	auto	auto	unknown	
GE0/0/16	enable	down	0	auto	auto	unknown	
GE0/0/17	enable	down	0	auto	auto	unknown	

**【Parameter Description】**

Parameter	Description
Port	Port number
status	Choose whether to close link port
link	Status: Down up
priority	Set port priority, the range of 0-7
Set speed	Choose the following modes: 10/100Mbps ports: full-10 half-10 auto-10 full-100 half-100 auto-100 10/100/1000Mbps ports: full-10 half-10 auto-10 full-100 half-100 auto-100 full-1000 half-1000 auto-1000 auto 1000MbpsSFP port: full-1000 Full-duplex: Ports operating in Full-duplex mode can send and receive packets concurrently. Half-duplex: Ports operating in Half-duplex mode can either send or receive packets at a given time. Auto: Auto-negotiation, ports operating in Auto-negotiation mode determine their duplex mode through auto-negotiation with peer ports. By default, Auto (Auto-negotiation) is enabled for the Speed/Duplex option.
Mode	Choose the following kinds: auto slave master
Actual speed	The actual speed of the port
Port description	The port is described

**【Configuration example】**

To configure static routes:

1. Click Basic Setting > Port Setup

2. Configure the related parameters for port 1, Status is "enable", Priority is "1", Set speed is "auto", Mode is "auto", Port description is "port 1".

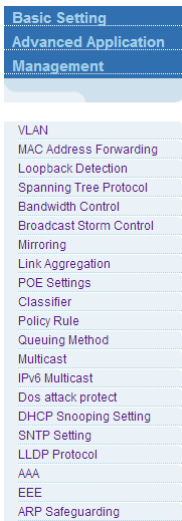
3. Click Modify.

Port basic settings Ethernet 1000M Port[1]

Port	Status	Link	Priority	Set speed	Mode	Actual speed	Port description (0-128 chars)
GE0/0/1	<input type="button" value="enable"/>	down	<input type="text" value="1"/>	<input type="button" value="auto"/>	<input type="button" value="auto"/>	unknown	<input type="text" value="port1"/>

## 4.2. Advanced Application

Choose Advanced Application, and the following page appears. There are "VLAN", "MAC Address Forwarding", "Spanning Tree Protocol", "ERPS Protocol", "EAPS Protocol", "Layer 2 Tunneling Protocol", "PPPOE IA", "Bandwidth Control", "Broadcast Storm Control", "Mirroring", "Link Aggregation", "POE Settings", "Port Security", "Classifier", "Policy Rule", "Queuing Method", "Multicast", "IPv6 Multicast", "Dos attack protect", "DHCP Snooping Setting", "SNTP Setting", "QinQ", "LLDP Protocol" and "AAA" configuration web pages.



## 4.2.1. VLAN

Selecting “**Advanced Application>VLAN**” in the navigation bar, you can configure VLAN.

The screenshot shows the VLAN configuration interface. On the left is a navigation menu with 'VLAN' selected. The main content area is titled 'VLAN Status' and includes a search bar for 'VLAN Search by VID'. Below the search bar, it states 'The Number of VLAN: 1. Current Page: 1 of 1.' A table displays the following information:

Index	VID	Elapsed Time	Status
1	1	3:01:26	Static

Below the table is a port assignment grid for VID 1:

VID	Port Number													
	1	3	5	7	9	11	13	15	17	19	21	23	25	27
1	U	U	U	U	U	U	U	U	U	U	U	U	U	U
	U	U	U	U	U	U	U	U	U	U	U	U	U	U

At the bottom, there is a 'Change Pages' section with 'Previous' and 'Next' buttons.

### 【Instructions】

The traditional Ethernet is a data network communication technology basing on CSMA/CD (Carrier Sense Multiple Access/Collision Detect) via shared communication medium. Through the traditional Ethernet, the overfull hosts in LAN will result in serious collision, flooding broadcasts, poor performance or even breakdown of the Internet. Though connecting the LANs through switches can avoid the serious collision, the flooding broadcasts cannot be prevented, which will occupy plenty of bandwidth resources, causing potential serious security problems.

A Virtual Local Area Network (VLAN) is a network topology configured according to a logical scheme rather than the physical layout. The VLAN technology is developed for switches to control broadcast in LANs. By creating VLANs in a physical LAN, you can divide the LAN into multiple logical LANs, each of which has a broadcast domain of its own. Hosts in the same VLAN communicate with one another as if they are in a LAN. However, hosts in different VLANs cannot communicate with one another directly. Therefore, broadcast packets are limited in a VLAN. Hosts in the same VLAN communicate with one another via Ethernet whereas hosts in different VLANs communicate with one another through the Internet devices such as Router, the Layer3 switch, etc. The following figure illustrates a VLAN implementation.

### 4.2.1.1. VLAN Status

Selecting “**Advanced Application>VLAN>VLAN Status**”, in the navigation bar, you can view VLAN status.

The screenshot shows the 'VLAN Status' page with a search bar for 'VLAN Search by VID' and a 'Search' button. Below the search bar, it indicates 'The Number of VLAN: 1. Current Page: 1 of 1.' A table lists the VLAN configuration:

Index	VID	Elapsed Time	Status
1	1	1:31:01	Static

Below the table is a detailed view for VID 1, showing a grid of port numbers (1-28) with 'U' indicating up status for all ports.

#### 【Parameter Description】

Parameter	Description
VLAN Status	View all vlans configured in the device
VLAN Search by VID	Enter VID to view the specified VLAN

#### 【Configuration example】

Such as: View the VLAN of VID as “1”.

This screenshot shows the same 'VLAN Status' page, but with the search bar containing the value '1'. The table below shows the search results for VID 1, with an elapsed time of 1:33:06.

Index	VID	Elapsed Time	Status
1	1	1:33:06	Static

The detailed view for VID 1 also shows the port status grid, which remains the same as in the previous screenshot.

### 4.2.1.2. VLAN Port Settings

Selecting “**Advanced Application>VLAN>VLAN Port Settings**”, in the navigation bar, you can set VLAN port.

**VLAN Port Settings** [Static VLAN](#) [VLAN Status](#)

Global GVRP

permit vlan

PORT ID

port forbidden vlan

[Show Garp Information:](#)

Port	PVID	Acceptable Frame	Port Mode	Port GVRP	Ingress Check
*		All	Hybrid	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<b>Ethernet 1000M Port</b>					
GE0/0/1	1	All	Hybrid	<input type="checkbox"/>	<input checked="" type="checkbox"/>
GE0/0/2	1	All	Hybrid	<input type="checkbox"/>	<input checked="" type="checkbox"/>
GE0/0/3	1	All	Hybrid	<input type="checkbox"/>	<input checked="" type="checkbox"/>
GE0/0/4	1	All	Hybrid	<input type="checkbox"/>	<input checked="" type="checkbox"/>
GE0/0/5	1	All	Hybrid	<input type="checkbox"/>	<input checked="" type="checkbox"/>
GE0/0/6	1	All	Hybrid	<input type="checkbox"/>	<input checked="" type="checkbox"/>
GE0/0/7	1	All	Hybrid	<input type="checkbox"/>	<input checked="" type="checkbox"/>
GE0/0/8	1	All	Hybrid	<input type="checkbox"/>	<input checked="" type="checkbox"/>
GE0/0/9	1	All	Hybrid	<input type="checkbox"/>	<input checked="" type="checkbox"/>
GE0/0/10	1	All	Hybrid	<input type="checkbox"/>	<input checked="" type="checkbox"/>
GE0/0/11	1	All	Hybrid	<input type="checkbox"/>	<input checked="" type="checkbox"/>
GE0/0/12	1	All	Hybrid	<input type="checkbox"/>	<input checked="" type="checkbox"/>
GE0/0/13	1	All	Hybrid	<input type="checkbox"/>	<input checked="" type="checkbox"/>
GE0/0/14	1	All	Hybrid	<input type="checkbox"/>	<input checked="" type="checkbox"/>
GE0/0/15	1	All	Hybrid	<input type="checkbox"/>	<input checked="" type="checkbox"/>
GE0/0/16	1	All	Hybrid	<input type="checkbox"/>	<input checked="" type="checkbox"/>

**【Parameter Description】**

Parameter	Description
PVID	The PVID of the port can be modified, the default port PVID is "1"
Acceptable Frame	Choose the following kinds: All Tagged only Untagged only
Port Mode	Choose the following modes: Hybrid: The port can be either a tag member or untag member in a VLAN and can be a member port for multiple vlans. Trunk: The port can only be an tag member in a VLAN and can be a member port for multiple vlans Access: The port can only be a member of untag in VLAN and the port can only be in a VLAN.
Port GVRP	Select open or close GVRP, dynamic VLAN learning function, port mode must be Trunk mode
Ingress Check	Open port filtering function. If the port settings only receive the Tagged type of message, if the Ingress Check function is opened, the Untagged type of message will be discarded when the port receives the message of the untagged type of message, otherwise it can be forwarded. The default port

Parameter	Description
	filtering function opens.

**【Instructions】**

Hybrid port to packet:

Receives a packet, judge whether there is a VLAN information: if there is no play in port PVID, exchanged and forwarding, if have, whether the Hybrid port allows the VLAN data into: if can be forwarded, or discarded (untag on port configuration is not considered, untag configuration only work when to send it a message).

Hybrid port to send packet:

1. Determine the VLAN in this port attributes (disp interface can see the port to which VLAN untag, which VLAN tag).
2. If it is untag stripping VLAN information, send again, if the tag is sent directly.

**【Configuration example】**

1. Click Advanced Application > VLAN> VLAN Port Settings.
2. The PVID of port 1 is set to "1", the frame type is set to "All", the port mode is set to "Hybrid", and the port GVRP is not turned on and the entry inspection function is opened.
3. Click Apply.

GE0/0/1    1    All    Hybrid       

**4.2.1.3. Static VLAN**

Selecting "Advanced Application>Static VLAN" in the navigation bar, you can configure Static VLAN.

**Static VLAN**
[VLAN Port Settings](#)
[VLAN Status](#)

Current static VLAN

0001

Port Number <a href="#">[Click for changing or selecting]</a>													
1	3	5	7	9	11	13	15	17	19	21	23	25	27
U	U	U	U	U	U	U	U	U	U	U	U	U	U
U	U	U	U	U	U	U	U	U	U	U	U	U	U
2	4	6	8	10	12	14	16	18	20	22	24	26	28

Port Number [\[Select all: - \[None\] T \[Tagged\] U \[Untagged\]\]](#)

VLAN List    1       

---

Name

Total 1 records



## 【Parameter Description】

Parameter	Description
VLAN List	VLAN Group ID
Name	VLAN Group name

## 【Configuration example】

To Add and delete VLAN members

1. Click Advanced Application > VLAN > Static VLAN.
2. Adding a new VLAN, VLAN Group ID 120 contains non-untag member port 1-4. Tag member port 5-8. The user can modify the port member by clicking on the white area below the port number.
3. Click Apply.

Static VLAN

Current static VLAN

0001

Port Number [Click for changing or selecting]

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

Port Number [Select all: - [None] T [Tagged] U [Untagged]]

VLAN List: 120 [Add] [Delete]

Name: [Modify] [Cancel]

Total 1 records

#### 4.2.2. MAC Address Forwarding

Selecting “**Advanced Application > MAC Address Forwarding**” in the navigation bar, you can configure MAC Address Forwarding.

**【Parameter Description】**

Parameter	Description
MAC Type	MAC Type: Static MAC Dynamic MAC Blackhole MAC Permanent MAC

**【Instructions】**

Blackhole MAC: If a PC's MAC address is configured on a switch to be a blackhole MAC, then the PC's package will be discarded by the switch and not forwarded to the network.

**【Configuration example】**

1. Click Advanced Application > MAC Address Forwarding.
2. MAC Address Forwarding

3. Unknown source mac packet drop settings.

Port Number [unknown source mac packet drop settings]

1	3	5	7	9	11	13	15	17	19	21	23	25	27
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2	4	6	8	10	12	14	16	18	20	22	24	26	28

Port Number [Apply all: ]

**Modify**

4. Click Modify.

### 4.2.3. Loopback Detection

Selecting “Advanced Application>Loopback Detection”, in the navigation bar, you can configure Loopback Detection. Loopback Detection allows the switch to detect loops in the network. When a loop is detected on a port, the switch will display an alert on the management interface and further block the corresponding port according to your configurations.

**Basic Setting**

**Advanced Application**

**Management**

---

VLAN

MAC Address Forwarding

**Loopback Detection**

Spanning Tree Protocol

Bandwidth Control

Broadcast Storm Control

Mirroring

Link Aggregation

POE Settings

Classifier

Policy Rule

Queueing Method

Multicast

IPv6 Multicast

Dos attack protect

DHCP Snooping Setting

SNTP Setting

LLDP Protocol

AAA

EEE

ARP Safeguarding

**Loopback Detection**

Action:  Discarding  Shutdown

Interval Time(s):

Recover Time(s):

Trap:  Enable  Disable

Port	Active
*	<input type="checkbox"/>
GE0/0/1	<input type="checkbox"/>
GE0/0/2	<input type="checkbox"/>
GE0/0/3	<input type="checkbox"/>
GE0/0/4	<input type="checkbox"/>
GE0/0/5	<input type="checkbox"/>
GE0/0/6	<input type="checkbox"/>
GE0/0/7	<input type="checkbox"/>
GE0/0/8	<input type="checkbox"/>
GE0/0/9	<input type="checkbox"/>
GE0/0/10	<input type="checkbox"/>
GE0/0/11	<input type="checkbox"/>
GE0/0/12	<input type="checkbox"/>
GE0/0/13	<input type="checkbox"/>
GE0/0/14	<input type="checkbox"/>
GE0/0/15	<input type="checkbox"/>
GE0/0/16	<input type="checkbox"/>

**【Parameter Description】**

Parameter	Description
Interval Times	Set the interval of sending loopback detection packets.
Recover Times	Set the recovery time globally

### 4.2.4. Spanning Tree Protocol

Selecting “Advanced Application>Spanning Tree Protocol”, in the navigation bar, you can configure

spanning tree protocol. STP (Spanning Tree Protocol), subject to IEEE 802.1D standard, is to disbranch a ring network in the Data Link layer in a local network. Devices running STP discover loops in the network and block ports by exchanging information, in that way, a ring network can be disbranched to form a tree-topological ring-free network to prevent packets from being duplicated and forwarded endlessly in the network.

**Basic Setting**

**Advanced Application Management**

VLAN

MAC Address Forwarding

Loopback Detection

**Spanning Tree Protocol**

Bandwidth Control

Broadcast Storm Control

Mirroring

Link Aggregation

POE Settings

Classifier

Policy Rule

Queuing Method

Multicast

IPv6 Multicast

Dos attack protect

DHCP Snooping Setting

SNTP Setting

LLDP Protocol

AAA

EEE

ARP Safeguarding

**Spanning Tree Protocol Status**

[Configuration](#) [STP/RSTP](#) [MSTP](#)


**Spanning Tree Protocol: RSTP**

Global Spanning Tree		Enable
Our Bridge ID	32768-000a.6a00.03ee	
Root Bridge ID	32768-000a.6a00.03ee	
Root Path Cost	0	
Hello Time (second)	2	
Max Age (second)	20	
Forwarding Delay (second)	15	
Topology Changed Times	0	

Port	Active	Pathcost	Priority	Role	State
GE0/0/1	enable	200000	128	designatedPort	disabled
GE0/0/2	enable	200000	128	designatedPort	disabled
GE0/0/3	enable	200000	128	designatedPort	disabled
GE0/0/4	enable	200000	128	designatedPort	disabled
GE0/0/5	enable	20000	128	designatedPort	forwarding
GE0/0/6	enable	200000	128	designatedPort	disabled
GE0/0/7	enable	200000	128	designatedPort	disabled
GE0/0/8	enable	200000	128	designatedPort	disabled
GE0/0/9	enable	200000	128	designatedPort	disabled
GE0/0/10	enable	200000	128	designatedPort	disabled
GE0/0/11	enable	200000	128	designatedPort	disabled
GE0/0/12	enable	200000	128	designatedPort	disabled
GE0/0/13	enable	200000	128	designatedPort	disabled
GE0/0/14	enable	200000	128	designatedPort	disabled

#### 4.2.4.1. Spanning Tree Protocol Status

Selecting “**Advanced Application>Spanning Tree Protocol>Spanning Tree Protocol status**”; in the navigation bar, you can view spanning tree protocol status.

 **Spanning Tree Protocol Status**
[Configuration](#) [STP/RSTP](#) [MSTP](#)
**Spanning Tree Protocol: RSTP**

Global Spanning Tree	Enable
Our Bridge ID	32768-000a.6a00.03ee
Root Bridge ID	32768-000a.6a00.03ee
Root Path Cost	0
Hello Time (second)	2
Max Age (second)	20
Forwarding Delay (second)	15
Topology Changed Times	0

Port	Active	Pathcost	Priority	Role	State
GE0/0/1	enable	200000	128	designatedPort	disabled
GE0/0/2	enable	200000	128	designatedPort	disabled
GE0/0/3	enable	200000	128	designatedPort	disabled
GE0/0/4	enable	200000	128	designatedPort	disabled
GE0/0/5	enable	20000	128	designatedPort	forwarding
GE0/0/6	enable	200000	128	designatedPort	disabled
GE0/0/7	enable	200000	128	designatedPort	disabled
GE0/0/8	enable	200000	128	designatedPort	disabled
GE0/0/9	enable	200000	128	designatedPort	disabled
GE0/0/10	enable	200000	128	designatedPort	disabled
GE0/0/11	enable	200000	128	designatedPort	disabled
GE0/0/12	enable	200000	128	designatedPort	disabled
GE0/0/13	enable	200000	128	designatedPort	disabled
GE0/0/14	enable	200000	128	designatedPort	disabled

**【Parameter Description】**

Parameter	Description
Root Path Cost	Configure Root Path Cost
Hello time(second)	Switches sends bpdu in packet interval
Max age(second)	Ports are not yet received a message in the time, will initiate topology changes
Forwarding delay(second)	The state of the port switch time
Topology changed times	The number of topology changes

**4.2.4.2. Spanning Tree Configuration**

Selecting "**Advanced Application>Spanning Tree Protocol>Spanning Tree configuration**", in the navigation bar, you can configure spanning tree.

Spanning Tree Configuration
Status

Spanning Tree Mode

IEEE compatible Spanning Tree  
 Rapid Spanning Tree  
 Multiple Spanning Tree

Global Spanning Tree status

Enable  
 Disable

**【Parameter Description】**

Parameter	Description
Spanning Tree Mode	Spanning tree mode: IEEE Compatible Spanning Tree Rapid Spanning Tree Multiple Spanning Tree
Global Spanning Tree Status	Select open or close Global Spanning

#### 4.2.4.3. Compatible/Rapid Spanning Tree Protocol

Selecting “**Advanced Application>Spanning Tree Protocol>Compatible/Rapid Spanning Tree Protocol**”, in the navigation bar, you can configure Compatible/Rapid Spanning Tree Protocol.

Compatible/Rapid Spanning Tree Protocol		Status
Bridge Priority	32768 ▼	
Hello Time	2	Seconds
MAX Age	20	Seconds
Forwarding Delay	15	Seconds

(Notice:When the port is a member of an aggregation group, the configuration is based on the maximum port configuration of the member.)

Port	Active	Priority	Path Cost	Path Cost Default Value
*	<input type="checkbox"/>			<input type="checkbox"/>
GE0/0/1	<input checked="" type="checkbox"/>	128	200000	<input checked="" type="checkbox"/>
GE0/0/2	<input checked="" type="checkbox"/>	128	200000	<input checked="" type="checkbox"/>
GE0/0/3	<input checked="" type="checkbox"/>	128	200000	<input checked="" type="checkbox"/>
GE0/0/4	<input checked="" type="checkbox"/>	128	200000	<input checked="" type="checkbox"/>
GE0/0/5	<input checked="" type="checkbox"/>	128	20000	<input checked="" type="checkbox"/>
GE0/0/6	<input checked="" type="checkbox"/>	128	200000	<input checked="" type="checkbox"/>
GE0/0/7	<input checked="" type="checkbox"/>	128	200000	<input checked="" type="checkbox"/>
GE0/0/8	<input checked="" type="checkbox"/>	128	200000	<input checked="" type="checkbox"/>
GE0/0/9	<input checked="" type="checkbox"/>	128	200000	<input checked="" type="checkbox"/>
GE0/0/10	<input checked="" type="checkbox"/>	128	200000	<input checked="" type="checkbox"/>
GE0/0/11	<input checked="" type="checkbox"/>	128	200000	<input checked="" type="checkbox"/>
GE0/0/12	<input checked="" type="checkbox"/>	128	200000	<input checked="" type="checkbox"/>
GE0/0/13	<input checked="" type="checkbox"/>	128	200000	<input checked="" type="checkbox"/>
GE0/0/14	<input checked="" type="checkbox"/>	128	200000	<input checked="" type="checkbox"/>

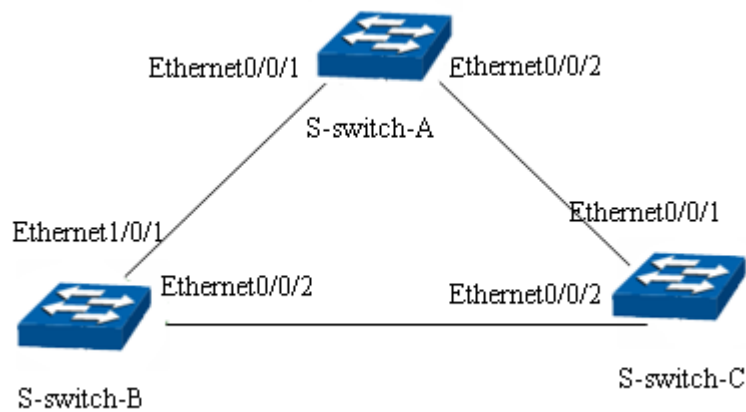
#### 【Parameter Description】

Parameter	Description
Bridge Priority	Set bridge priority, the default instance bridge priority for 32768
Hello Time	Switches sends bpd in packet interval
Max Age	Ports are not yet received a message in the time, will initiate topology changes
Forwarding Delay	The state of the port switch time
Port Priority	Set port instance priority, defaults to 128
Path Cost	Configure port costs

#### 【Configuration example】

As shown in the figure, configure S-switch-A as root bridge and S-switch-B as Designated Bridge.

The links connected by S-switch -B and S-switch -C are backup links. When the links connected by S-switch -B, S-switch -A and S-switch -C fail, the backup link will come into effect.



#### S-switch-A Configuration:

1. Configure Ethernet0/0/1 and Ethernet0/0/2 as trunk port.
2. Configure spanning-tree priority as 0.
3. Enable RSTP globally.

#### S-switch-B Configuration:

1. Configure Ethernet0/0/1 and Ethernet0/0/2 as trunk port.
2. Configure spanning-tree priority as 4096, and configure the ethernet0/0/1 port path cost and the ethernet0/0/2 port path cost as 10.
3. Enable RSTP globally.

#### S-switch-C Configuration:

1. Configure Ethernet0/0/1 and Ethernet0/0/2 as trunk port.
2. Configure the ethernet0/0/1 port path cost and ethernet0/0/2 port path cost as 10 to ensure that link between S-switch-B and S-switch-C as main link.
3. Enable RSTP globally.



#### 4.2.4.4. Multiple Spanning Tree Protocol

Selecting “**Advanced Application>Spanning Tree Protocol>Multiple Spanning Tree Protocol**”, in the navigation bar, you can configure Multiple Spanning Tree Protocol.

**Multiple Spanning Tree Protocol** [Status](#)

**Bridge:**

Hello Time	2	seconds
MAX Age	20	seconds
Forwarding Delay	15	seconds
Maximum hops	20	
Configuration Name		
Revision Number	0	

**Instance:**

Instance	0 ▼
Bridge Priority	32768 ▼
VLAN Range	

Instance	Bridge Priority	VLAN Mapped
0	32768	1-4094
1	32768	
2	32768	
3	32768	
4	32768	
5	32768	

#### 【Parameter Description】

Parameter	Description
Hello Time	Switches sends bpd in packet interval
Max age	Ports are not yet received a message in the time, will initiate topology changes
Forwarding Delay	The state of the port switch time
Maximum Hops	Set the maximum number of hops that BPDUs can support in the spanning tree
Configuration Name	Fill in configuration name
Revision Number	Set revision number
Instance	Instance number
Bridge Priority	Priority setting bridge example, the default instance bridge priority for 32768
VLAN Range	Set VLAN range
Port Priority	Set port instance priority, defaults to 128
Path Cost	Configure port costs

#### 4.2.5. Bandwidth Control

Selecting “**Advanced Application>Bandwidth Control**”, in the navigation bar, you can configure Bandwidth Control.

Basic Setting		Bandwidth Control		
Advanced Application Management		Port	Ingress Rate(unit: 16kbps)	Egress Rate(unit: 16kbps)
VLAN		*		
MAC Address Forwarding		GE0/0/1	0	0
Loopback Detection		GE0/0/2	0	0
Spanning Tree Protocol		GE0/0/3	0	0
Bandwidth Control		GE0/0/4	0	0
Broadcast Storm Control		GE0/0/5	0	0
Mirroring		GE0/0/6	0	0
Link Aggregation		GE0/0/7	0	0
POE Settings		GE0/0/8	0	0
Classifier		GE0/0/9	0	0
Policy Rule		GE0/0/10	0	0
Queuing Method		GE0/0/11	0	0
Multicast		GE0/0/12	0	0
IPv6 Multicast		GE0/0/13	0	0
Dos attack protect		GE0/0/14	0	0
DHCP Snooping Setting		GE0/0/15	0	0
SNTP Setting		GE0/0/16	0	0
LLDP Protocol		GE0/0/17	0	0
AAA		GE0/0/18	0	0
EEE		GE0/0/19	0	0
ARP Safeguarding		GE0/0/20	0	0
		GE0/0/21	0	0
		GE0/0/22	0	0
		GE0/0/23	0	0
		GE0/0/24	0	0

#### 【Instructions】

1 Mbit/s = 1000 Kbit/s = 1000 / 8 KB/s = 125 KB/s. That is, the theoretical rate of 1M bandwidth is 125 KB/s.

#### 【Configuration example】

To configure bandwidth control of port8.

- 1.Click Basic Setting > Bandwidth Control.
- 2.Configure port-8 Ingress Rate is 64kbps, Egress Rate is 128kbps.

GE0/0/8	64	128
GE0/0/9	0	0
GE0/0/10	0	0

3. Click Apply.

#### 4.2.6. Broadcast Storm Control

Selecting “**Advanced Application>Broadcast Storm Control**”; in the navigation bar, you can configure Broadcast Storm Control.

**Basic Setting**

Advanced Application Management

VLAN

MAC Address Forwarding

Loopback Detection

Spanning Tree Protocol

Bandwidth Control

**Broadcast Storm Control**

Mirroring

Link Aggregation

POE Settings

Classifier

Policy Rule

Queuing Method

Multicast

IPv6 Multicast

Dos attack protect

DHCP Snooping Setting

SNTP Setting

LLDP Protocol

AAA

EEE

ARP Safeguarding

**Broadcast Storm Control**

storm-suppression mode pkt

Port	Broadcast(unit:64pps)		Multicast(unit:64pps)		Unicast(unit:64pps)	
*		pps		pps		pps
GE0/0/1	0	pps	0	pps	0	pps
GE0/0/2	0	pps	0	pps	0	pps
GE0/0/3	0	pps	0	pps	0	pps
GE0/0/4	0	pps	0	pps	0	pps
GE0/0/5	0	pps	0	pps	0	pps
GE0/0/6	0	pps	0	pps	0	pps
GE0/0/7	0	pps	0	pps	0	pps
GE0/0/8	0	pps	0	pps	0	pps
GE0/0/9	0	pps	0	pps	0	pps
GE0/0/10	0	pps	0	pps	0	pps
GE0/0/11	0	pps	0	pps	0	pps
GE0/0/12	0	pps	0	pps	0	pps
GE0/0/13	0	pps	0	pps	0	pps
GE0/0/14	0	pps	0	pps	0	pps
GE0/0/15	0	pps	0	pps	0	pps
GE0/0/16	0	pps	0	pps	0	pps
GE0/0/17	0	pps	0	pps	0	pps
GE0/0/18	0	pps	0	pps	0	pps
GE0/0/19	0	pps	0	pps	0	pps

**【Parameter Description】**

Parameter	Description
Broadcast	Broadcast rate limitation(the range of: 64-32000000, unit: pps, you must enter multiple of 64, default to 49984)
Multicast	Multicast rate limitation(the range of: 64-32000000, unit: pps, you must enter multiple of 64, default to 49984)
Unicast	Unicast rate limitation(the range of: 64-32000000, unit: pps, you must enter multiple of 64, default to 49984)

**【Instructions】**

1 Mbit/s = 1000 Kbit/s = 1000 / 8 KB/s = 125 KB/s. That is, the theoretical rate of 1M bandwidth is 125 KB/s.

**【Configuration example】**

To configure broadcast storm control of port1.

1. Click Basic Setting > Broadcast Storm Control.
2. Set Port1 broadcast as 6400 pps, multicast as 3200 pps, unicast as 3200 pps.
3. Click Apply.

Port	Broadcast(unit:64pps)		Multicast(unit:64pps)		Unicast(unit:64pps)	
*		pps		pps		pps
GE0/0/1	6400	pps	3200	pps	3200	pps
GE0/0/2	0	pps	0	pps	0	pps

## 4.2.7. Mirroring

Selecting “**Advanced Application>Mirroring**”, in the navigation bar, you can configure mirroring.

Port	Mirrored	Direction
*	<input type="checkbox"/>	Ingress ▼
GE0/0/1	<input type="checkbox"/>	Ingress ▼
GE0/0/2	<input type="checkbox"/>	Ingress ▼
GE0/0/3	<input type="checkbox"/>	Ingress ▼
GE0/0/4	<input type="checkbox"/>	Ingress ▼
GE0/0/5	<input type="checkbox"/>	Ingress ▼
GE0/0/6	<input type="checkbox"/>	Ingress ▼
GE0/0/7	<input type="checkbox"/>	Ingress ▼
GE0/0/8	<input type="checkbox"/>	Ingress ▼
GE0/0/9	<input type="checkbox"/>	Ingress ▼
GE0/0/10	<input type="checkbox"/>	Ingress ▼
GE0/0/11	<input type="checkbox"/>	Ingress ▼
GE0/0/12	<input type="checkbox"/>	Ingress ▼
GE0/0/13	<input type="checkbox"/>	Ingress ▼
GE0/0/14	<input type="checkbox"/>	Ingress ▼
GE0/0/15	<input type="checkbox"/>	Ingress ▼
GE0/0/16	<input type="checkbox"/>	Ingress ▼
GE0/0/17	<input type="checkbox"/>	Ingress ▼
GE0/0/18	<input type="checkbox"/>	Ingress ▼
GE0/0/19	<input type="checkbox"/>	Ingress ▼
GE0/0/20	<input type="checkbox"/>	Ingress ▼
GE0/0/21	<input type="checkbox"/>	Ingress ▼
GE0/0/22	<input type="checkbox"/>	Ingress ▼

### 【Parameter Description】

Parameter	Description
Active	Select open or close Mirroring
Monitor Port	Set up the monitoring port and forward the flow data of the source port to the message analyzer to analyze the message and then forward to the monitoring port
Mirrored	Check the box to configure the mirror source port
Direction	Configure the direction of the mirror message, choose: Ingress, Egress, Both

### 【Configuration example】

1. Click Advanced Application > Mirroring.
2. Open mirroring, configure monitoring port is port 8, the source port is port 7, and the mirror message is in both direction.
3. Click Apply.

**Mirroring**

Active

Monitor Port

Port	Mirrored	Direction
*	<input type="checkbox"/>	Ingress ▼
GE0/0/1	<input type="checkbox"/>	Ingress ▼
GE0/0/2	<input type="checkbox"/>	Ingress ▼
GE0/0/3	<input type="checkbox"/>	Ingress ▼
GE0/0/4	<input type="checkbox"/>	Ingress ▼
GE0/0/5	<input type="checkbox"/>	Ingress ▼
GE0/0/6	<input type="checkbox"/>	Ingress ▼
GE0/0/7	<input checked="" type="checkbox"/>	Both ▼

#### 4.2.8. Link Aggregation

Selecting “**Advanced Application>Link Aggregation**”, in the navigation bar, you can configure link aggregation. With the LAG (Link Aggregation Group) function, you can aggregate multiple physical ports into a logical interface to increase link bandwidth and configure the backup ports to enhance the connection reliability. You can configure LAG in two ways:

- Static LAG: The member ports are manually added to the LAG.
- LACP (Link Aggregation Control Protocol): The switch uses LACP to implement dynamic link aggregation and disaggregation by exchanging LACP packets with its partner. LACP extends the flexibility of the LAG configuration.

**Basic Setting**

**Advanced Application Management**

VLAN

MAC Address Forwarding

Loopback Detection

Spanning Tree Protocol

Bandwidth Control

Broadcast Storm Control

Mirroring

**Link Aggregation**

POE Settings

Classifier

Policy Rule

Queuing Method

Multicast

IPv6 Multicast

Dos attack protect

DHCP Snooping Setting

SNTP Setting

LLDP Protocol

AAA

EEE

ARP Safeguarding

**Link Aggregation Status**

[Link Aggregation Setting](#)

Group ID	Enabled Ports	Synchronized Ports	Aggregator ID	Criteria	Status
T1	-	-	-	-	-
T2	-	-	-	-	-
T3	-	-	-	-	-
T4	-	-	-	-	-
T5	-	-	-	-	-
T6	-	-	-	-	-
T7	-	-	-	-	-

##### 4.2.8.1. Link Aggregation status

Selecting “**Advanced Application>Link Aggregation>Link Aggregation Status**”, in the navigation bar, you can view link aggregation status, you can view Group ID, Enabled Ports, Synchronized Ports, Aggregator ID, Criteria, Status.

Link Aggregation Status			Link Aggregation Setting		
Group ID	Enabled Ports	Synchronized Ports	Aggregator ID	Criteria	Status
T1	-	-	-	-	-
T2	-	-	-	-	-
T3	-	-	-	-	-
T4	-	-	-	-	-
T5	-	-	-	-	-
T6	-	-	-	-	-
T7	-	-	-	-	-

#### 4.2.8.2. Link Aggregation Setting

Selecting “**Advanced Application>Link Aggregation>Link Aggregation Setting**”, in the navigation bar, you can set Link Aggregation.

Link Aggregation Setting		Status	LACP
Port	Group ID	Port LACP Mode	
GE0/0/1	none ▼	active ▼	
GE0/0/2	none ▼	active ▼	
GE0/0/3	none ▼	active ▼	
GE0/0/4	none ▼	active ▼	
GE0/0/5	none ▼	active ▼	
GE0/0/6	none ▼	active ▼	
GE0/0/7	none ▼	active ▼	
GE0/0/8	none ▼	active ▼	
GE0/0/9	none ▼	active ▼	
GE0/0/10	none ▼	active ▼	
GE0/0/11	none ▼	active ▼	
GE0/0/12	none ▼	active ▼	
GE0/0/13	none ▼	active ▼	
GE0/0/14	none ▼	active ▼	
GE0/0/15	none ▼	active ▼	
GE0/0/16	none ▼	active ▼	
GE0/0/17	none ▼	active ▼	
GE0/0/18	none ▼	active ▼	
GE0/0/19	none ▼	active ▼	
GE0/0/20	none ▼	active ▼	
GE0/0/21	none ▼	active ▼	
GE0/0/22	none ▼	active ▼	
GE0/0/23	none ▼	active ▼	
GE0/0/24	none ▼	active ▼	

#### 【Parameter Description】

Parameter	Description
Group ID	Add the port to the specified Aggregation Group ID

Parameter	Description
Port LACP mode	Configure port aggregation(static/active/passive)
Criteria	Configure the Aggregation Group load balancing (src-mac/dst-mac/src-dst-mac/src-ip/dst-ip/src-dst-ip)

#### 4.2.8.3. Link Aggregation Control Protocol

Selecting “**Advanced Application>Link Aggregation>Link Aggregation Control Protocol**”, in the navigation bar, you can configure Link Aggregation Control Protocol.

 **Link Aggregation Control Protocol**
[Link Aggregation Setting](#)

System Priority	32768
-----------------	-------

Group ID	Active	Eth-trunk Mode	Load-balance Mode
T1	<input type="checkbox"/>	static ▼	none ▼
T2	<input type="checkbox"/>	static ▼	none ▼
T3	<input type="checkbox"/>	static ▼	none ▼
T4	<input type="checkbox"/>	static ▼	none ▼
T5	<input type="checkbox"/>	static ▼	none ▼
T6	<input type="checkbox"/>	static ▼	none ▼
T7	<input type="checkbox"/>	static ▼	none ▼

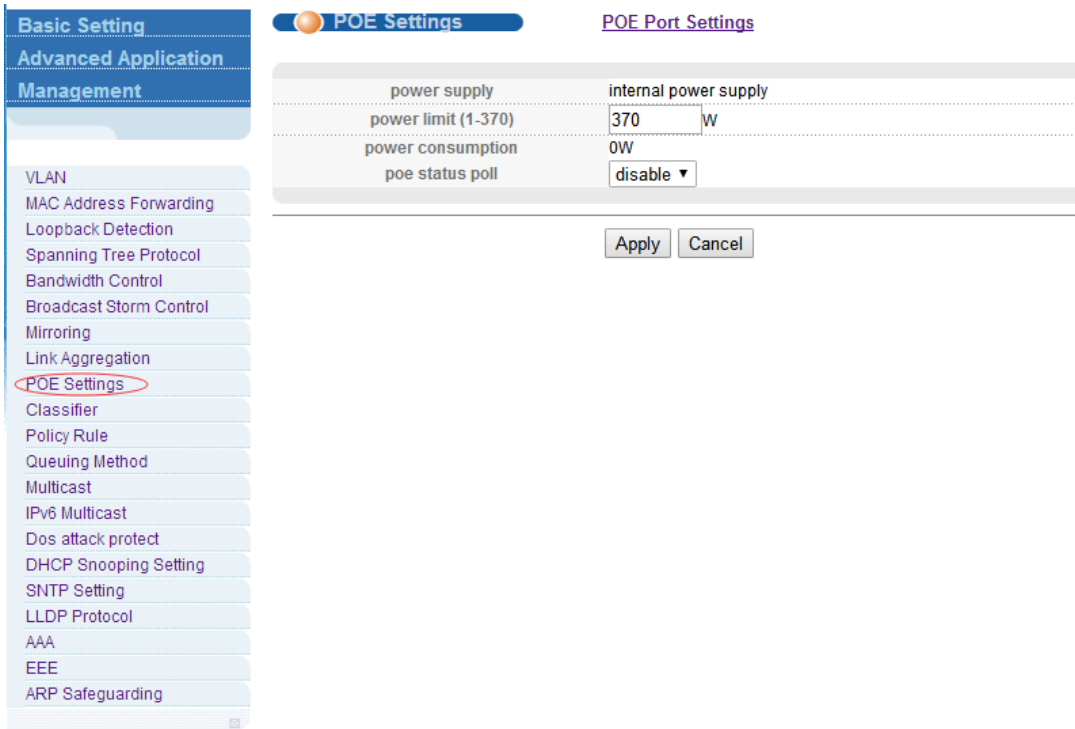
Port	Port Priority
*	
GE0/0/1	128
GE0/0/2	128
GE0/0/3	128
GE0/0/4	128
GE0/0/5	128
GE0/0/6	128
GE0/0/7	128
GE0/0/8	128
GE0/0/9	128
GE0/0/10	128
GE0/0/11	128

#### 【Parameter Description】

Parameter	Description
System priority	Aggregation group system priority, the default is 32768( the range of 1-65535)

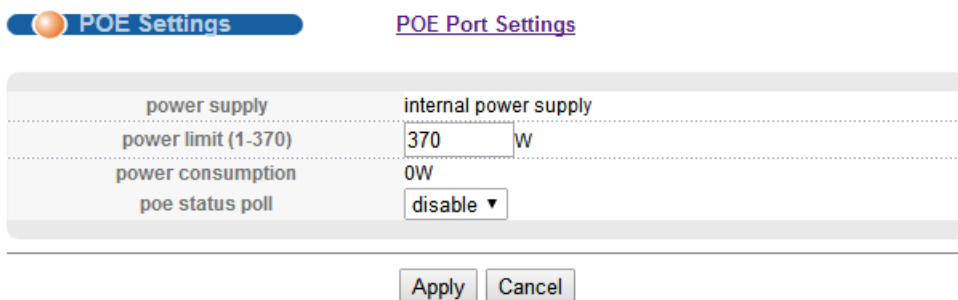
#### 4.2.9. POE Settings

Selecting “**Advanced Application>POE Settings**”, you can configure POE.



#### 4.2.9.1. POE Settings

Selecting “Advanced Application>POE Settings”, you can configure POE.



#### 【Parameter Description】

Parameter	Description
power limit	The power of switch POE can be limited

#### 【Configuration example】

Such as: set power limit is 360 W.



**POE Settings** POE Port Settings

power supply	internal power supply	
power limit (1-370)	360	W
power consumption	0W	
poE status poll	disable ▾	

#### 4.2.9.2. POE Port Settings

Selecting “**Advanced Application>POE Port Settings**”, in the navigation bar, you can configure POE Port.

**POE Port Settings** POE Settings

Port Number <small>(Click for selecting)</small>												
1	3	5	7	9	11	13	15	17	19	21	23	
○	-	-	-	-	-	-	-	-	-	-	-	-
2	4	6	8	10	12	14	16	18	20	22	24	
Port Number poe												

POE Port Settings **Ethernet 1000M Port[1]**

Port No.	Enable	Standard	Priority	Class	Power Limit(1-30):W	Power Consumption:W	Voltage:V	Status
GE0/0/1	enable ▾	ieee802.3at ▾	low ▾	5	30	0	0.0	status: Port is off - Detection is in process

(Note: It may take some time to display all ports information, please be patient.)

#### 【Parameter Description】

Parameter	Description
Enable	Turn the port POE power on and off and the default is open
Standard	Configure ieee802.3af, ieee802.3at mode, default to ieee802.3at
Priority	Configure port Priority low, critical, high, the default priority is low
Power limit	The power of switch POE can be limited

#### 【Configuration example】

Such as: Configure the POE for port 1.

POE Port Settings **Ethernet 1000M Port[1]**

Port No.	Enable	Standard	Priority	Class	Power Limit(1-30):W	Power Consumption:W	Voltage:V	Status
GE0/0/1	enable ▾	ieee802.3af ▾	high ▾	5	28	0	0.0	status: Port is off - Detection is in process

(Note: It may take some time to display all ports information, please be patient.)

### 4.2.10. Classifier

Selecting “Advanced Application>Classifier”, in the navigation bar, you can configure Classifier.

**【Parameter Description】**

Parameter	Description
Active	Active Classifier

### 4.2.11. Policy Rule

Selecting “Advanced Application>Policy Rule”, in the navigation bar, you can configure Policy Rule.

## 【Parameter Description】

Parameter	Description
Active	Active Classifier

## 4.2.12. Queuing Method

Selecting “**Advanced Application>Queuing Method**”, in the navigation bar, you can configure queuing method.

The screenshot shows the configuration interface for the 'Queuing Method'. On the left, a navigation menu lists various settings, with 'Queuing Method' circled in red. The main configuration area has a header 'Queuing Method' and a table with the following structure:

Method	Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7
SPQ								

Below the table are 'Apply' and 'Cancel' buttons.

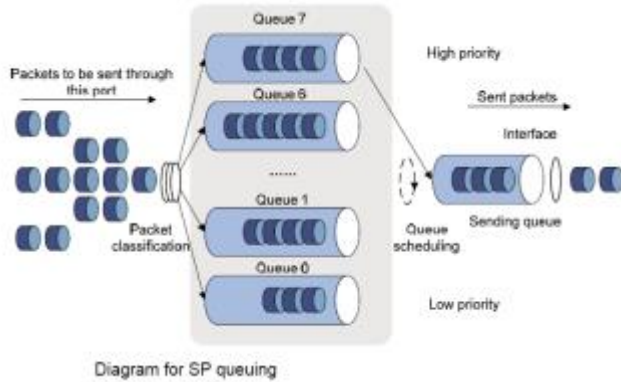
## 【Parameter Description】

Parameter	Description
Method	Five method: SPQ,WRR,SP+WRR,WFQ,SP+WFQ

## 【Instructions】

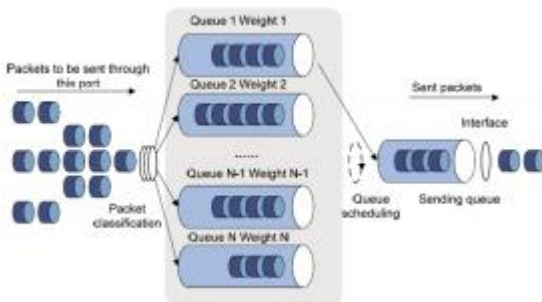
➤ SP(Strict-Priority) and WRR (Weighted Round Robin).

1) Strict Priority Queueing



Strict Priority Queueing is specially designed to meet the demands of critical services or applications. Critical services or applications such as voice are delay-sensitive and thus require to be dequeued and sent first before packets in other queues are dequeued on a congested network. For example, 4 egress queues 3, 2, 1 and 0 with descending priority are configured on a port. Then under SP algorithm, the port strictly prioritizes packets from higher priority queue over those from lower priority queue. Namely, only after packets in highest priority queue are emptied, can packets in lower priority queue be forwarded. Thus High-priority packets are always processed before those of less priority. Medium-priority packets are always processed before low-priority packets. The lowest priority queue would be serviced only when highest priority queues had no packets buffered. Disadvantages of SP: The SP queueing gives absolute priority to high-priority packets over low-priority traffic; it should be used with care. The moment a higher priority packet arrived in its queue, however, servicing of the lower priority packets would be interrupted in favor of the higher priority queue or packets will be dropped if the amount of high-priority traffic is too great to be emptied within a short time.

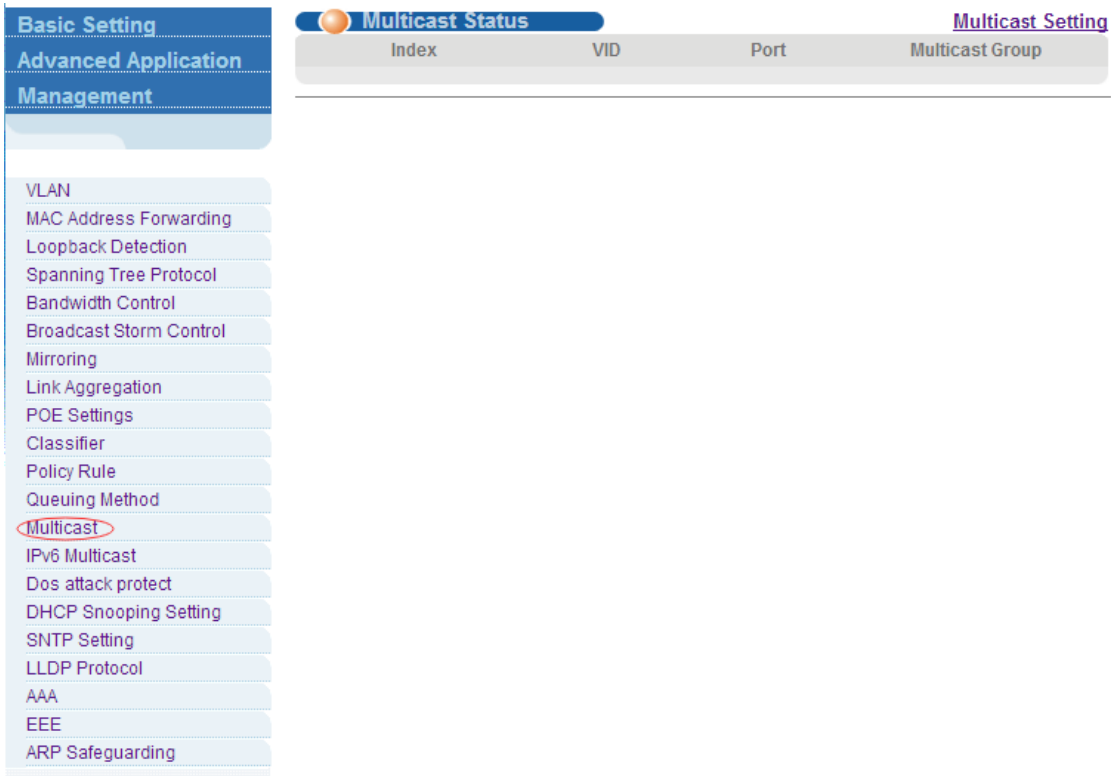
## 2) WRR



WRR queue scheduling algorithm ensures every queue a guaranteed service time by taking turns to schedule all queues. Assume there are 4 egress queues on the port. The four weight values (namely,  $w_3$ ,  $w_2$ ,  $w_1$ , and  $w_0$ ) indicate the proportion of resources assigned to the four queues respectively. On a 100M port, if you set the weight values of WRR queue-scheduling algorithm to 25, 15, 5 and 5 (corresponding to  $w_3$ ,  $w_2$ ,  $w_1$ , and  $w_0$  respectively). Then the queue with the lowest priority can be ensured of, at least, 10 Mbps bandwidth, thus avoiding the disadvantage of SP queue-scheduling algorithm that packets in low-priority queues may not be served during a long time. Another advantage of WRR queue-scheduling algorithm is that though the queues are scheduled in turn, the service time for each queue is not fixed, that is to say, when a queue is emptied, the next queue will be scheduled immediately. Thus, bandwidth resources are fully utilized.

### 4.2.13. Multicast

Selecting "**Advanced Application>Multicast**", in the navigation bar, you can configure Multicast.



#### 4.2.13.1. Multicast Status

Selecting "**Advanced Application>Multicast>Multicast Status**", in the navigation bar, you can view all multicast. This includes the static configuration and the multicast that is learned through the IGMP-Snooping protocol.



#### 4.2.13.2. Multicast Settings

Selecting "**Advanced Application>Multicast>Multicast Settings**", in the navigation bar, you can set multicast.

**Multicast Setting**[Multicast Status](#)[Deny VLAN](#)[IGMP Filtering Profile](#)

## IGMP Snooping:

Active	<input type="checkbox"/>
Querier	<input type="checkbox"/>
Host Timeout	300 seconds
IGMP Route Port Forward	<input type="checkbox"/>

## Port Information:

Port	Max Group Limit	Fast Leave	Multicast Vlan	IGMP Filtering Profile
*		<input type="checkbox"/>		
GE0/0/1	507	<input type="checkbox"/>	0	
GE0/0/2	507	<input type="checkbox"/>	0	
GE0/0/3	507	<input type="checkbox"/>	0	
GE0/0/4	507	<input type="checkbox"/>	0	
GE0/0/5	507	<input type="checkbox"/>	0	
GE0/0/6	507	<input type="checkbox"/>	0	
GE0/0/7	507	<input type="checkbox"/>	0	
GE0/0/8	507	<input type="checkbox"/>	0	
GE0/0/9	507	<input type="checkbox"/>	0	
GE0/0/10	507	<input type="checkbox"/>	0	
GE0/0/11	507	<input type="checkbox"/>	0	
GE0/0/12	507	<input type="checkbox"/>	0	
GE0/0/13	507	<input type="checkbox"/>	0	
GE0/0/14	507	<input type="checkbox"/>	0	
GE0/0/15	507	<input type="checkbox"/>	0	
GE0/0/16	507	<input type="checkbox"/>	0	
GE0/0/17	507	<input type="checkbox"/>	0	

## 【Parameter Description】

Parameter	Description
Active	Open IGMP-snooping
Querier	Open IGMP-snooping timed query function
Host Timeout	Configure the dynamic group sowing time (default 300s)
IGMP Route Port Forward	Open IGMP Route Port Forward
Max Group Limit	Max learning group of configuration port ( default 1020)
Fast Leave	Open port quick exit function (i.e., when the port receives the IGMP and leaves the message, immediately remove the port from the reshuffle group)
Multicast Vlan	The configuration group multicast the default VLAN
IGMP Filtering Profile	The configuration port refers to the multicast preview, which can only be learned to the group broadcast group that is allowed in the group broadcast preview, and cannot be learned to the multicast group which is forbidden by the group broadcast preview

**4.2.13.3. IGMP Snooping Deny VLAN**

Selecting "**Advanced Application>Multicast>IGMP Snooping Deny VLAN**", in the navigation bar, you can preview the banned group broadcast group, unable to learn the multicast group that is prohibited by the group preview.

**IGMP Snooping Deny VLAN** [Multicast Setting](#)

Vid

---

Deny VLAN(s)

**【Parameter Description】**

Parameter	Description
Vid	Vlan's ID

**4.2.13.4. IGMP Filtering Profile**

Selecting “**Advanced Application>Multicast>IGMP Filtering Profile**”, in the navigation bar, you can add and remove the preview feature of the modified group.

**IGMP Filtering Profile** [Multicast Setting](#)

**Profile Setup**

Profile ID

Profile Description

Profile Limit  permit  deny

---

Index	Profile ID	Profile Description	Profile Limit	Referred Port

---

Profile ID

Input Format  IP  MAC

Start Address

End Address

VLAN

---

---

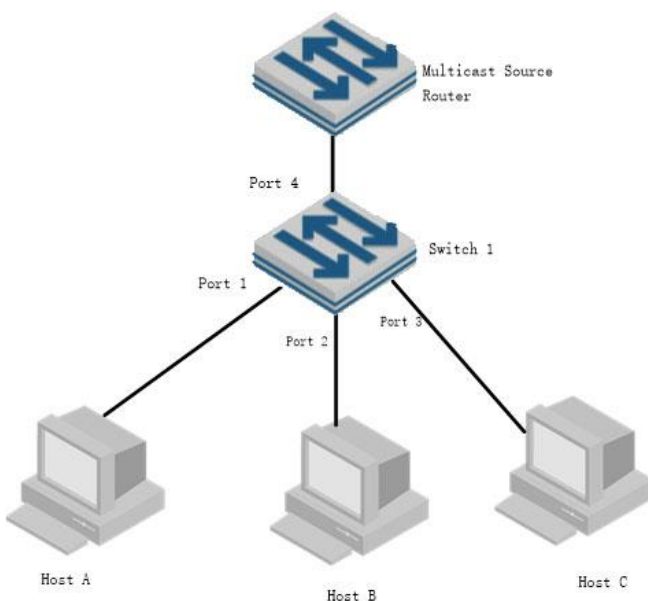
Profile ID	Index	Start Addr	End Addr	VLAN	Delete

**【Parameter Description】**

Parameter	Description
Profile ID	The range of 1-128
Profile Limit	Profile rules can be permit or deny
Input Format	The preview address can be configured to be either IP or MAC

**【Configuration example】**

As shown in the figure, the host-A, host-B and host-C belong to VLAN2, VLAN3 and VLAN4 respectively. The configuration enables the three hosts to receive the data of the multicast group with the group address of 224.0.1.1 ~ 224.0.1.3.



1. Enable igmp-snooping function.
2. Add different ports to different vlans.
3. The host sends the report message to the switch, and the switch learns to multicast group.
4. The multicast source router sends a query message to the switch, which will learn the routing port table entry.
5. The multicast source router sends a multicast traffic stream to the switch and the switch distribute it to the hosts.

**4.2.14. IPv6 Multicast**

Selecting "**Advanced Application>IPv6 Multicast**", in the navigation bar, you can configure IPv6 Multicast.



The screenshot displays the IPv6 Multicast Status page. On the left, a navigation menu lists various settings, with 'IPv6 Multicast' circled in red. The main content area features a breadcrumb trail: 'IPv6 Multicast Status' (active) and 'IPv6 Multicast Setting' (link). Below the breadcrumb is a table with the following columns: Index, VID, Port, and IPv6 Multicast Group.

#### 4.2.14.1. IPv6 Multicast Status

Selecting “**Advanced Application>IPv6 Multicast>IPv6 Multicast Status**”, in the navigation bar, you can view all IPv6 Multicast groups.

The screenshot displays the IPv6 Multicast Setting page. The breadcrumb trail shows 'IPv6 Multicast Status' (active) and 'IPv6 Multicast Setting' (link). Below the breadcrumb is a table with the following columns: Index, VID, Port, and IPv6 Multicast Group.

#### 4.2.14.2. IPv6 Multicast Setting

Selecting “**Advanced Application>IPv6 Multicast>IPv6 Multicast Setting**”, in the navigation bar, you can configure IPv6 Multicast.

## IPv6 Multicast Setting

[IPv6 Multicast Status](#)[Deny VLAN](#)

## MLD Snooping:

Active	<input type="checkbox"/>
Querier	<input type="checkbox"/>
Host Timeout	300 seconds
MLD Route Port Forward	<input type="checkbox"/>

## Port Information:

Port	Max Group Limit	Fast Leave	IPv6 Multicast Vlan
*		<input type="checkbox"/>	
GE0/0/1	507	<input type="checkbox"/>	0
GE0/0/2	507	<input type="checkbox"/>	0
GE0/0/3	507	<input type="checkbox"/>	0
GE0/0/4	507	<input type="checkbox"/>	0
GE0/0/5	507	<input type="checkbox"/>	0
GE0/0/6	507	<input type="checkbox"/>	0
GE0/0/7	507	<input type="checkbox"/>	0
GE0/0/8	507	<input type="checkbox"/>	0
GE0/0/9	507	<input type="checkbox"/>	0
GE0/0/10	507	<input type="checkbox"/>	0
GE0/0/11	507	<input type="checkbox"/>	0
GE0/0/12	507	<input type="checkbox"/>	0
GE0/0/13	507	<input type="checkbox"/>	0
GE0/0/14	507	<input type="checkbox"/>	0
GE0/0/15	507	<input type="checkbox"/>	0
GE0/0/16	507	<input type="checkbox"/>	0
GE0/0/17	507	<input type="checkbox"/>	0

## 【Parameter Description】

Parameter	Description
Active	Enable or disable MLD snooping
Querier	Enable or disable MLD snooping timed Querier
Host Timeout	Configure Dynamic IPv6 multicast aging time (default 300s)
MLD Route Port Forward	Enable or disable MLD Route Port Forward
Max Group Limit	Configure maximum learning IPv6 Multicast message of port(default 1020)
Fast Leave	Enable or disable Fast Leave (That is, when the port receives IGMP leave message, the port is deleted immediately from the IPv6 multicast group)
IPv6 Multicast VLAN	Configure IPv6 multicast default VLAN

## 【Configuration Example】

**IPv6 Multicast Setting** [IPv6 Multicast Status](#) [Deny VLAN](#)

MLD Snooping:

Active	<input type="checkbox"/>
Querier	<input type="checkbox"/>
Host Timeout	300 seconds
MLD Route Port Forward	<input type="checkbox"/>

Port Information:

Port	Max Group Limit	Fast Leave	IPv6 Multicast Vlan
*		<input type="checkbox"/>	
GE0/0/1	507	<input checked="" type="checkbox"/>	1

#### 4.2.14.3. MLD Snooping Dney VLAN

Selecting “**Advanced Application>IPv6 Multicast>MLD Snooping Dney VLAN**”, in the navigation bar, you can configure MLD Snooping Dney VLAN.

**MLD Snooping Dney VLAN** [IPv6 Multicast Setting](#)

Vid

Deny VLAN(s)

#### 【Parameter Description】

Parameter	Description
Vid	Vlan ID

#### 4.2.15. Dos attack protect

Selecting “**Advanced Application>Dos attack protect**”, in the navigation bar, you can configure dos attack protect.

**Basic Setting**

**Advanced Application Management**

- VLAN
- MAC Address Forwarding
- Loopback Detection
- Spanning Tree Protocol
- Bandwidth Control
- Broadcast Storm Control
- Mirroring
- Link Aggregation
- POE Settings
- Classifier
- Policy Rule
- Queuing Method
- Multicast
- IPv6 Multicast
- Dos attack protect**
- DHCP Snooping Setting
- SNTP Setting
- LLDP Protocol
- AAA
- EEE
- ARP Safeguarding

**Dos Attack Protect**

**dos attack control:**

Dos attack packets class	drop Active
src mac and dst mac equal	<input type="checkbox"/>
src ip and dst ip equal	<input type="checkbox"/>
UDP with sport and dport equal	<input type="checkbox"/>
TCP with sport and dport equal	<input type="checkbox"/>
ICMPv4 payload maximum length	<input type="checkbox"/> 512
ICMPv6 payload maximum length	<input type="checkbox"/> 512
TCP control flags and sequence equal 0	<input type="checkbox"/>
TCP syn packets sport 0-1023, applies to unfragmented packets	<input type="checkbox"/>
enable dos attack ip first fragments	<input type="checkbox"/>
check minimum size of ipv6 fragments	<input type="checkbox"/> 1240
fragmented icmp packets	<input type="checkbox"/>
TCP fragments with offset value of 1(*8)	<input type="checkbox"/>
TCP with SYN & FIN bits	<input type="checkbox"/>
TCP with FIN,URG and PSH bits,and sequence equal 0	<input type="checkbox"/>
TCP frist fragments with minimum tcp header length	<input type="checkbox"/> 20

#### 【Parameter Description】

Parameter	Description
dos attack control	The DOS attack is controlled by the discarding behavior of the corresponding message

#### 4.2.16. DHCP Snooping Setting

Selecting “**Advanced Application>DHCP Snooping Setting**”, in the navigation bar, you can configure DHCP Snooping.

**Basic Setting**

**Advanced Application Management**

- VLAN
- MAC Address Forwarding
- Loopback Detection
- Spanning Tree Protocol
- Bandwidth Control
- Broadcast Storm Control
- Mirroring
- Link Aggregation
- POE Settings
- Classifier
- Policy Rule
- Queuing Method
- Multicast
- IPv6 Multicast
- Dos attack protect
- DHCP Snooping Setting**
- SNTP Setting
- LLDP Protocol
- AAA
- EEE
- ARP Safeguarding

**DHCP Snooping Setting** IP Source Guard

DHCP Snooping Enable  Close  Open

Port	Trust	Maxclients
*	<input type="checkbox"/>	
GE0/0/1	<input type="checkbox"/>	2048
GE0/0/2	<input type="checkbox"/>	2048
GE0/0/3	<input type="checkbox"/>	2048
GE0/0/4	<input type="checkbox"/>	2048
GE0/0/5	<input type="checkbox"/>	2048
GE0/0/6	<input type="checkbox"/>	2048
GE0/0/7	<input type="checkbox"/>	2048
GE0/0/8	<input type="checkbox"/>	2048
GE0/0/9	<input type="checkbox"/>	2048
GE0/0/10	<input type="checkbox"/>	2048
GE0/0/11	<input type="checkbox"/>	2048
GE0/0/12	<input type="checkbox"/>	2048
GE0/0/13	<input type="checkbox"/>	2048
GE0/0/14	<input type="checkbox"/>	2048
GE0/0/15	<input type="checkbox"/>	2048
GE0/0/16	<input type="checkbox"/>	2048
GE0/0/17	<input type="checkbox"/>	2048
GE0/0/18	<input type="checkbox"/>	2048
GE0/0/19	<input type="checkbox"/>	2048
GE0/0/20	<input type="checkbox"/>	2048
GE0/0/21	<input type="checkbox"/>	2048

#### 4.2.16.1. DHCP Snooping Setting

Selecting “**Advanced Application>DHCP Snooping Setting>DHCP Snooping Setting**”, in the navigation bar, you can configure DHCP Snooping. Nowadays, the network is getting larger and more complicated. The amount of the PCs always exceeds that of the assigned IP addresses. The wireless network and the laptops are widely used and the locations of the PCs are always changed. Therefore, the corresponding IP address of the PC should be updated with a few configurations. DHCP (Dynamic Host Configuration Protocol, the network configuration protocol optimized and developed basing on the BOOTP, functions to solve the above mentioned problems.

**DHCP Snooping Setting** IP Source Guard

DHCP Snooping Enable  Close  Open

Port	Trust	Maxclients
*	<input type="checkbox"/>	
GE0/0/1	<input type="checkbox"/>	2048
GE0/0/2	<input type="checkbox"/>	2048
GE0/0/3	<input type="checkbox"/>	2048
GE0/0/4	<input type="checkbox"/>	2048
GE0/0/5	<input type="checkbox"/>	2048
GE0/0/6	<input type="checkbox"/>	2048
GE0/0/7	<input type="checkbox"/>	2048
GE0/0/8	<input type="checkbox"/>	2048
GE0/0/9	<input type="checkbox"/>	2048
GE0/0/10	<input type="checkbox"/>	2048
GE0/0/11	<input type="checkbox"/>	2048
GE0/0/12	<input type="checkbox"/>	2048
GE0/0/13	<input type="checkbox"/>	2048
GE0/0/14	<input type="checkbox"/>	2048
GE0/0/15	<input type="checkbox"/>	2048
GE0/0/16	<input type="checkbox"/>	2048
GE0/0/17	<input type="checkbox"/>	2048
GE0/0/18	<input type="checkbox"/>	2048
GE0/0/19	<input type="checkbox"/>	2048
GE0/0/20	<input type="checkbox"/>	2048
GE0/0/21	<input type="checkbox"/>	2048

#### 【Parameter Description】

Parameter	Description
DHCP Snooping Enable	Enable or disable DHCP Snooping serve
Trust	Enable or disable the DHCP Snooping port trust property state
Maxclients	Set Maxclients

#### 【Configuration Example】

**DHCP Snooping Setting** IP Source Guard

DHCP Snooping Enable  Close  Open

Port	Trust	Maxclients
*	<input type="checkbox"/>	
GE0/0/1	<input checked="" type="checkbox"/>	2048

#### 4.2.16.2. IP Source Guard

Selecting "Advanced Application>DHCP Snooping Setting>IP Source Guard", in the navigation bar, you can configure IP Source Guard.

IP-Source-Guard		DHCP Snooping Setting	
System security settings			
Port		Mode	
*		Disable	▼
GE0/0/1		Disable	▼
GE0/0/2		Disable	▼
GE0/0/3		Disable	▼
GE0/0/4		Disable	▼
GE0/0/5		Disable	▼
GE0/0/6		Disable	▼
GE0/0/7		Disable	▼
GE0/0/8		Disable	▼
GE0/0/9		Disable	▼
GE0/0/10		Disable	▼
GE0/0/11		Disable	▼
GE0/0/12		Disable	▼
GE0/0/13		Disable	▼
GE0/0/14		Disable	▼
GE0/0/15		Disable	▼
GE0/0/16		Disable	▼
GE0/0/17		Disable	▼
GE0/0/18		Disable	▼
GE0/0/19		Disable	▼
GE0/0/20		Disable	▼
GE0/0/21		Disable	▼
GE0/0/22		Disable	▼
GE0/0/23		Disable	▼
GE0/0/24		Disable	▼
GE0/1/1		Disable	▼
GE0/1/2		Disable	▼

#### 【Parameter Description】

Parameter	Description
Disable unbinding entry to access network	Enable or Disable unbinding entry to access network

#### 【Instructions】

If you want to access shall be binding and switch the IP address of the same network segment.

### 4.2.17. SNTP Setting

Selecting “**Advanced Application>SNTP Setting**”, in the navigation bar, you can configure SNTP.

**Basic Setting**

**Advanced Application**

**Management**

---

VLAN

MAC Address Forwarding

Loopback Detection

Spanning Tree Protocol

Bandwidth Control

Broadcast Storm Control

Mirroring

Link Aggregation

POE Settings

Classifier

Policy Rule

Queuing Method

Multicast

IPv6 Multicast

Dos attack protect

DHCP Snooping Setting

**SNTP Setting**

LLDP Protocol

AAA

EEE

ARP Safeguarding

### SNTP Setup

SNTP Client Enable

SNTP Client Mode	broadcast ▾	
SNTP Client Poll Interval	1000	(64~1024)
SNTP Client Retransmit Times	3	(1~10)
SNTP Client Retransmit Interval	30	(3~30)
SNTP Client Broadcast Delay	3	(1~9999)ms
MD5 Authentication Enable	<input type="checkbox"/>	
Encrypt Enable	<input type="checkbox"/>	
SNTP Server IP Address	<input type="text"/>	(X.X.X.X)
Backup Server IP Address	<input type="text"/>	(X.X.X.X)
SNTP Server Key	<input type="text"/>	

#### Authentication Key List

KeyID	Key	Trusted
<input type="text"/>	<input type="text"/>	YES ▾

No Authentication Key configured.

#### Valid Server List

### 【Parameter Description】

Parameter	Description
SNTP Client Enable	Enable or disable SNTP Client
SNTP Client Mode	SNTP Client Mode: broadcast, anycast multicast unicast
SNTP Client Poll Interval	It's interval that SNTP Client sends requests to SNTP Server
SNTP Client Retransmit Times	If SNTP Client does not receive a response within a certain period of time after sending a request, it will resend the request until the number of retransmissions exceeds the set value
SNTP Client Retransmit Interval	It's interval that SNTP Client resends requests to SNTP Server
SNTP Server IP Address	Set SNTP Server IP Address
Valid Server List Server IP	SNTP only receives the messages from Valid Server List Server IP configured
SNTP Client Enable	Enable or disable SNTP Client
SNTP Client Mode	SNTP Client Mode: broadcast, anycast multicast



Parameter	Description
	unicast
SNTP Client Poll Interval	It's interval that SNTP Client sends requests to SNTP Server
SNTP Client Retransmit Times	If SNTP Client does not receive a response within a certain period of time after sending a request, it will resend the request until the number of retransmissions exceeds the set value
Valid Server List Server IP	SNTP only receives the messages from Valid Server List Server IP configured

【Instr  
actions

】

SNTP Client receives and transmits messages from any SNTP Server when work mode of SNTP Client is broadcast or multicast. Local time cannot be synchronized to standard time if there is a malicious attack server (which provides incorrect time)

## 4.2.18. LLDP Protocol

Selecting "**Advanced Application>LLDP Protocol**", in the navigation bar, you can configure LLDP.

Port	Mode	TxPkts	RxPkts	Neighbours
<a href="#">GE0/0/1</a>	RxTx	-	-	-
<a href="#">GE0/0/2</a>	RxTx	-	-	-
<a href="#">GE0/0/3</a>	RxTx	-	-	-
<a href="#">GE0/0/4</a>	RxTx	-	-	-
<a href="#">GE0/0/5</a>	RxTx	-	-	-
<a href="#">GE0/0/6</a>	RxTx	-	-	-
<a href="#">GE0/0/7</a>	RxTx	-	-	-
<a href="#">GE0/0/8</a>	RxTx	-	-	-
<a href="#">GE0/0/9</a>	RxTx	-	-	-
<a href="#">GE0/0/10</a>	RxTx	-	-	-
<a href="#">GE0/0/11</a>	RxTx	-	-	-
<a href="#">GE0/0/12</a>	RxTx	-	-	-
<a href="#">GE0/0/13</a>	RxTx	-	-	-
<a href="#">GE0/0/14</a>	RxTx	-	-	-
<a href="#">GE0/0/15</a>	RxTx	-	-	-
<a href="#">GE0/0/16</a>	RxTx	-	-	-
<a href="#">GE0/0/17</a>	RxTx	-	-	-
<a href="#">GE0/0/18</a>	RxTx	-	-	-
<a href="#">GE0/0/19</a>	RxTx	-	-	-
<a href="#">GE0/0/20</a>	RxTx	-	-	-
<a href="#">GE0/0/21</a>	RxTx	-	-	-
<a href="#">GE0/0/22</a>	RxTx	-	-	-
<a href="#">GE0/0/23</a>	RxTx	-	-	-
<a href="#">GE0/0/24</a>	RxTx	-	-	-
<a href="#">GE0/1/1</a>	RxTx	-	-	-
<a href="#">GE0/1/2</a>	RxTx	-	-	-
<a href="#">GE0/1/3</a>	RxTx	-	-	-
<a href="#">GE0/1/4</a>	RxTx	-	-	-

### 4.2.18.1. LLDP Status

Selecting "**Advanced Application>LLDP Protocol>LLDP Status**", in the navigation bar, you can view LLDP status.

LLDP Status		LLDP Setting		
Port	Mode	TxPkts	RxPkts	Neighbours
<a href="#">GE0/0/1</a>	RxTx	-	-	-
<a href="#">GE0/0/2</a>	RxTx	-	-	-
<a href="#">GE0/0/3</a>	RxTx	-	-	-
<a href="#">GE0/0/4</a>	RxTx	-	-	-
<a href="#">GE0/0/5</a>	RxTx	-	-	-
<a href="#">GE0/0/6</a>	RxTx	-	-	-
<a href="#">GE0/0/7</a>	RxTx	-	-	-
<a href="#">GE0/0/8</a>	RxTx	-	-	-
<a href="#">GE0/0/9</a>	RxTx	-	-	-
<a href="#">GE0/0/10</a>	RxTx	-	-	-
<a href="#">GE0/0/11</a>	RxTx	-	-	-
<a href="#">GE0/0/12</a>	RxTx	-	-	-
<a href="#">GE0/0/13</a>	RxTx	-	-	-
<a href="#">GE0/0/14</a>	RxTx	-	-	-
<a href="#">GE0/0/15</a>	RxTx	-	-	-
<a href="#">GE0/0/16</a>	RxTx	-	-	-
<a href="#">GE0/0/17</a>	RxTx	-	-	-
<a href="#">GE0/0/18</a>	RxTx	-	-	-
<a href="#">GE0/0/19</a>	RxTx	-	-	-
<a href="#">GE0/0/20</a>	RxTx	-	-	-
<a href="#">GE0/0/21</a>	RxTx	-	-	-
<a href="#">GE0/0/22</a>	RxTx	-	-	-
<a href="#">GE0/0/23</a>	RxTx	-	-	-
<a href="#">GE0/0/24</a>	RxTx	-	-	-
<a href="#">GE0/1/1</a>	RxTx	-	-	-
<a href="#">GE0/1/2</a>	RxTx	-	-	-
<a href="#">GE0/1/3</a>	RxTx	-	-	-
<a href="#">GE0/1/4</a>	RxTx	-	-	-

#### 4.2.18.2. LLDP Setting

Selecting "Advanced Application>LLDP Protocol>LLDP Setting", in the navigation bar, you can configure LLDP.

LLDP Setting		LLDP Status	
Active	<input type="checkbox"/>		
Hello-time	30	seconds(5-32768)	
Hold-time	4	seconds(2-10)	

Port	Mode
*	Disable ▼
GE0/0/1	TxRx ▼
GE0/0/2	TxRx ▼
GE0/0/3	TxRx ▼
GE0/0/4	TxRx ▼
GE0/0/5	TxRx ▼
GE0/0/6	TxRx ▼
GE0/0/7	TxRx ▼
GE0/0/8	TxRx ▼
GE0/0/9	TxRx ▼
GE0/0/10	TxRx ▼
GE0/0/11	TxRx ▼
GE0/0/12	TxRx ▼
GE0/0/13	TxRx ▼
GE0/0/14	TxRx ▼
GE0/0/15	TxRx ▼
GE0/0/16	TxRx ▼
GE0/0/17	TxRx ▼
GE0/0/18	TxRx ▼
GE0/0/19	TxRx ▼
GE0/0/20	TxRx ▼
GE0/0/21	TxRx ▼

### 4.2.19. AAA

Selecting “Advanced Application>AAA”, in the navigation bar, you can configure AAA.

Basic Setting

Advanced Application

Management

802.1x

[AAA](#)   [MUSER](#)

EAP Forwarding Mode: eap-finish ▼

Quiet Period: 0 seconds(0-600)

Port	Active	Port Control	Reauthentication	Reauthentication Timer	Max User(s)
*	disable ▼	auto ▼	Off ▼		
GE0/0/1	disable ▼	auto ▼	Off ▼	3600 seconds	100
GE0/0/2	disable ▼	auto ▼	Off ▼	3600 seconds	100
GE0/0/3	disable ▼	auto ▼	Off ▼	3600 seconds	100
GE0/0/4	disable ▼	auto ▼	Off ▼	3600 seconds	100
GE0/0/5	disable ▼	auto ▼	Off ▼	3600 seconds	100
GE0/0/6	disable ▼	auto ▼	Off ▼	3600 seconds	100
GE0/0/7	disable ▼	auto ▼	Off ▼	3600 seconds	100
GE0/0/8	disable ▼	auto ▼	Off ▼	3600 seconds	100
GE0/0/9	disable ▼	auto ▼	Off ▼	3600 seconds	100
GE0/0/10	disable ▼	auto ▼	Off ▼	3600 seconds	100
GE0/0/11	disable ▼	auto ▼	Off ▼	3600 seconds	100
GE0/0/12	disable ▼	auto ▼	Off ▼	3600 seconds	100
GE0/0/13	disable ▼	auto ▼	Off ▼	3600 seconds	100
GE0/0/14	disable ▼	auto ▼	Off ▼	3600 seconds	100
GE0/0/15	disable ▼	auto ▼	Off ▼	3600 seconds	100
GE0/0/16	disable ▼	auto ▼	Off ▼	3600 seconds	100
GE0/0/17	disable ▼	auto ▼	Off ▼	3600 seconds	100
GE0/0/18	disable ▼	auto ▼	Off ▼	3600 seconds	100
GE0/0/19	disable ▼	auto ▼	Off ▼	3600 seconds	100

#### 4.2.19.1. 802.1x

Selecting “Advanced Application>AAA>802.1x”, in the navigation bar, you can configure 802.1x.

802.1x

[AAA](#)   [MUSER](#)

EAP Forwarding Mode: eap-finish ▼

Quiet Period: 0 seconds(0-600)

Port	Active	Port Control	Reauthentication	Reauthentication Timer	Max User(s)
*	disable ▼	auto ▼	Off ▼		
GE0/0/1	disable ▼	auto ▼	Off ▼	3600 seconds	100
GE0/0/2	disable ▼	auto ▼	Off ▼	3600 seconds	100
GE0/0/3	disable ▼	auto ▼	Off ▼	3600 seconds	100
GE0/0/4	disable ▼	auto ▼	Off ▼	3600 seconds	100
GE0/0/5	disable ▼	auto ▼	Off ▼	3600 seconds	100
GE0/0/6	disable ▼	auto ▼	Off ▼	3600 seconds	100
GE0/0/7	disable ▼	auto ▼	Off ▼	3600 seconds	100
GE0/0/8	disable ▼	auto ▼	Off ▼	3600 seconds	100
GE0/0/9	disable ▼	auto ▼	Off ▼	3600 seconds	100
GE0/0/10	disable ▼	auto ▼	Off ▼	3600 seconds	100
GE0/0/11	disable ▼	auto ▼	Off ▼	3600 seconds	100
GE0/0/12	disable ▼	auto ▼	Off ▼	3600 seconds	100
GE0/0/13	disable ▼	auto ▼	Off ▼	3600 seconds	100
GE0/0/14	disable ▼	auto ▼	Off ▼	3600 seconds	100
GE0/0/15	disable ▼	auto ▼	Off ▼	3600 seconds	100
GE0/0/16	disable ▼	auto ▼	Off ▼	3600 seconds	100
GE0/0/17	disable ▼	auto ▼	Off ▼	3600 seconds	100
GE0/0/18	disable ▼	auto ▼	Off ▼	3600 seconds	100
GE0/0/19	disable ▼	auto ▼	Off ▼	3600 seconds	100

## 【Parameter Description】

Parameter	Description
EAP Forwarding Mode	EAP Forwarding Mode : eap-finish, Eap-transfer
Quiet Period	If the same user fails to log in more than the allowed value, he or she will not be allowed to try to log in at a certain time
Active	Active: disable portbased(multi) portbased(single) macbased
Port Control	Port Control: auto forceauthorized forceunauthorized
Reauthentication	After user authentication is passed, the port can be configured to reauthenticate or periodically re-authenticate
Reauthentication Timer	Time range of Reauthentication Timer: 10-3600 seconds
Max user(s)	The maximum number of users: 1-100

## 【Configuration Example】

GE0/0/1     seconds

## 4.2.19.2. Radius Domain

Selecting “**Advanced Application>AAA>Radius Domain**”, in the navigation bar, you can configure Radius Domain.

[Domain](#)    [802.1x](#)    [MUSER](#)    [Radius](#)    [TACACS+](#)

Radius Domain:

Active	<input type="checkbox"/>
Domain Name	<input type="text"/>
Default Domain	<input type="checkbox"/>
Radius Service Name	<input type="text"/>
Force Max Number	<input checked="" type="radio"/> Disable <input type="radio"/> <input type="text" value="1"/> (1-640)

Domain Name	Radius Service Name	Active	Delete
<input type="button" value="Delete"/> <input type="button" value="Cancel"/>			

## 【Parameter Description】

Parameter	Description
-----------	-------------

Parameter	Description
Active	Enable or disable radius domain
Domain Name	Set domain name
Radius Server Name	Set Radius Server name
Force Max Number	Maximum number of user connections range: 1-640

【Instr

uctions】

It needs to provide user name and password when the client is authenticated. The user name information generally includes the ISP information of user, domain and the ISP one-to-one correspondence, the main information domain is the domain of the user is authenticated and accounted by which RADIUS server.

#### 4.2.19.3. Remote Authentication

Selecting “**Advanced Application>AAA>Remote Authentication**”, in the navigation bar, you can configure Remote Authentication.

The screenshot shows a web interface for configuring Remote Authentication. At the top, there is a navigation bar with several tabs: 'Remote Authentication' (selected), '802.1x', 'AAA', 'Radius', and 'TACACS+'. Below the navigation bar, there is a section for 'Authentication Mode' with a dropdown menu currently set to 'Local'. At the bottom of the page, there are two buttons: 'Apply' and 'Cancel'.

【Parameter Description】

Parameter	Description
Authentication Mode	Authentication Mode: Local, Radius, Tacacs+

#### 4.2.19.4. TACACS+ Server Setup

Selecting “**Advanced Application>AAA>TACACS+ Server Setup**”, in the navigation bar, you can configure TACACS+ Server Setup.

**TACACS+ Server Setup** AAA MUSER

**Authentication Server**

Authentication Type:  ▾

Encrypt Key:

Preemption Time:  min (0-1440)

Index	IP Address	TCP Port	Shared Secret	TimeOut	Delete
1	<input type="text" value="0.0.0.0"/>	<input type="text" value="49"/>	<input type="text"/>	<input type="text" value="5"/>	<input type="checkbox"/>
2	<input type="text"/>	<input type="text" value="49"/>	<input type="text"/>	<input type="text" value="5"/>	<input type="checkbox"/>

**【Parameter Description】**

Parameter	Description
Authentication Type	Authentication Mode: ascii, Chap, pap
Preemption Time	The time range of Preemption Time: 0-1440 minutes

**4.2.19.5. Radius Server Setup**

Selecting “**Advanced Application>AAA>Radius Server Setup**”, in the navigation bar, you can configure Radius Server Setup.

**RADIUS Server Setup** [AAA](#) [MUSER](#)

8021P Priority

H3C Cams

Bandwidth Limit

**Radius Host:**

Host Name

Preemption Time  min (0-1440)

Server	Index	IP Address	UDP Port	Shared Secret
Authentication Server	1	0.0.0.0	1812	Switch
	2	0.0.0.0	1812	
Accounting Server	1	0.0.0.0	1813	Switch
	2	0.0.0.0	1813	

Host	Authentication IP Address	Accounting IP Address	Delete
			<input type="button" value="Delete"/>

**【Parameter Description】**

Parameter	Description
8021P Priority	After this function is turned on, if the user authentication is pass, it will modify the PVID of the user's port.
H3C Cams	In this feature, you can configure the version information of transmitting clients to the radius server through the radius attribute client-version.
Bandwidth limit	After this function is turned on, if the user authentication is pass, it will modify the Bandwidth of the user's port.

#### 4.2.20. EEE

Selecting "**Advanced Application>EEE**", in the navigation bar, it could enable or disable the energy-efficient-ethernet function of interface in EEE web page.

Port	Enable
*	<input type="checkbox"/>
GE0/0/1	<input type="checkbox"/>
GE0/0/2	<input type="checkbox"/>
GE0/0/3	<input type="checkbox"/>
GE0/0/4	<input type="checkbox"/>
GE0/0/5	<input type="checkbox"/>
GE0/0/6	<input type="checkbox"/>
GE0/0/7	<input type="checkbox"/>
GE0/0/8	<input type="checkbox"/>
GE0/0/9	<input type="checkbox"/>
GE0/0/10	<input type="checkbox"/>
GE0/0/11	<input type="checkbox"/>
GE0/0/12	<input type="checkbox"/>
GE0/0/13	<input type="checkbox"/>
GE0/0/14	<input type="checkbox"/>
GE0/0/15	<input type="checkbox"/>
GE0/0/16	<input type="checkbox"/>
GE0/0/17	<input type="checkbox"/>
GE0/0/18	<input type="checkbox"/>
GE0/0/19	<input type="checkbox"/>
GE0/0/20	<input type="checkbox"/>
GE0/0/21	<input type="checkbox"/>
GE0/0/22	<input type="checkbox"/>
GE0/0/23	<input type="checkbox"/>
GE0/0/24	<input type="checkbox"/>
GE0/1/1	<input type="checkbox"/>
GE0/1/2	<input type="checkbox"/>
GE0/1/3	<input type="checkbox"/>

### 4.2.21. ARP Safeguarding

Selecting “Advanced Application>ARP Safeguarding”, The page can be configured to prevent arp flooding.

**Global Configuration**

ARP Anti-Flood: **DISABLE**    Action: **drop-arp**

Rate Limit: **16** (1~100)pps    Recover Time: **10** (0~1440)m

**Port Rate Limit Configuration**

Port	Rate Limit(1~100)pps	Port	Rate Limit(1~100)pps
GE0/0/1	0	GE0/0/2	0
GE0/0/3	0	GE0/0/4	0
GE0/0/5	0	GE0/0/6	0
GE0/0/7	0	GE0/0/8	0
GE0/0/9	0	GE0/0/10	0
GE0/0/11	0	GE0/0/12	0
GE0/0/13	0	GE0/0/14	0
GE0/0/15	0	GE0/0/16	0
GE0/0/17	0	GE0/0/18	0
GE0/0/19	0	GE0/0/20	0
GE0/0/21	0	GE0/0/22	0
GE0/0/23	0	GE0/0/24	0
GE0/1/1	0	GE0/1/2	0
GE0/1/3	0	GE0/1/4	0

**ARP Anti-Flood Entry**

Src MAC	Src IP	Port	VLAN	Recover Time(m)	Recover MAC

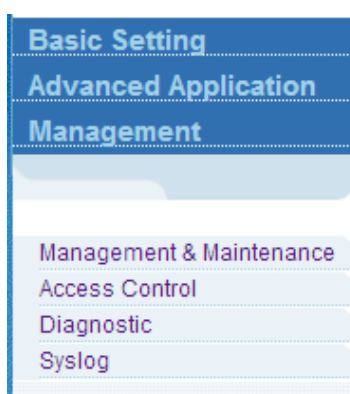
**【Parameter Description】**



Parameter	Description
Global Configuration	Enable or disable ARP Anti-flood
Port Rate Limit	It can set Arp message speed limit for specific interface. If it exceeds the speed limit, it is considered to be under attack.

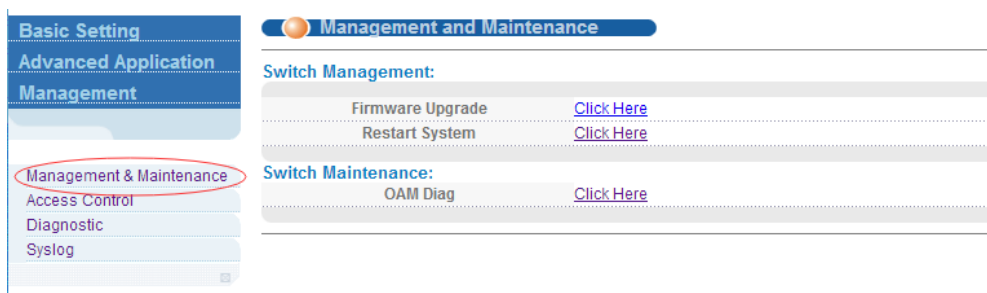
### 4.3. Management

Choose Management, and the following page appears. There are "**Management & Maintenance**", "**Access Control**", "**Diagnostic**", "**Syslog**", configuration web pages.



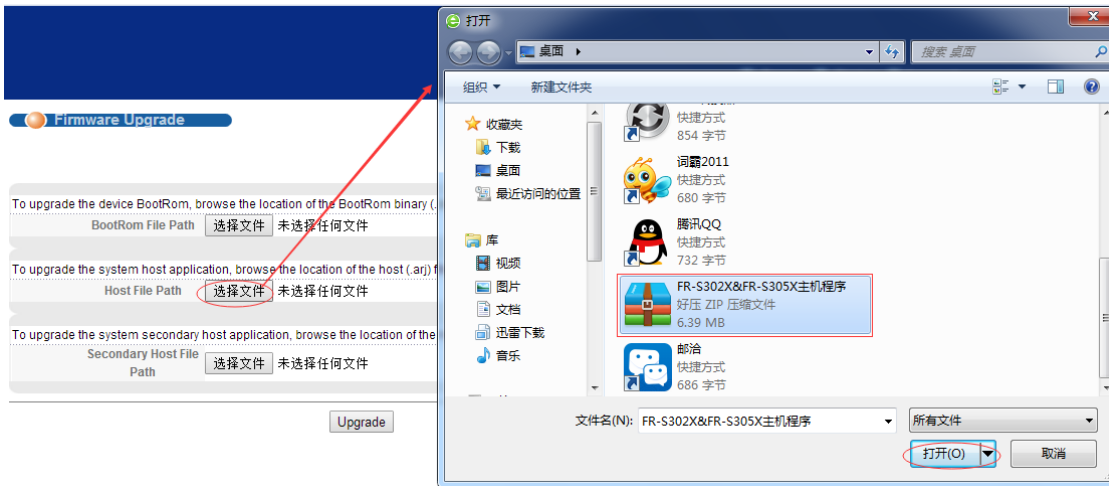
#### 4.3.1. Management & Maintenance

Selecting "**Management > Management & Maintenance**", in the navigation bar, you can Upgrade Firmware, Restart System and Maintenance switch.

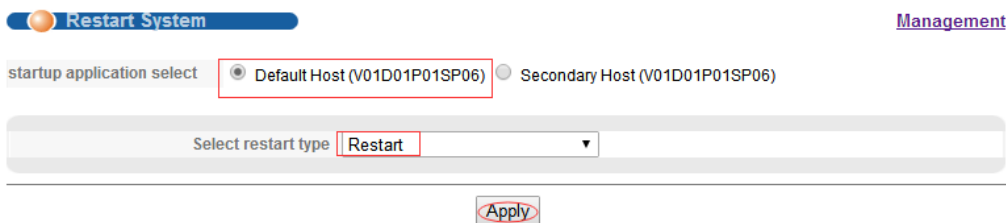


#### 【Configuration Example】

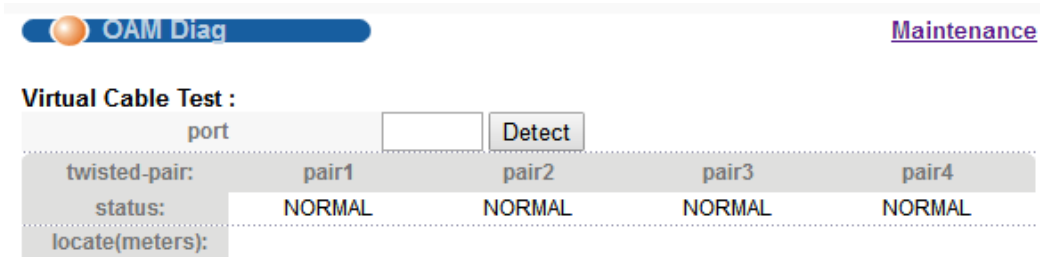
##### 1. Firmware Upgrade



2.Restart system. Restart type: Restart, Restart with Factory Defaults.

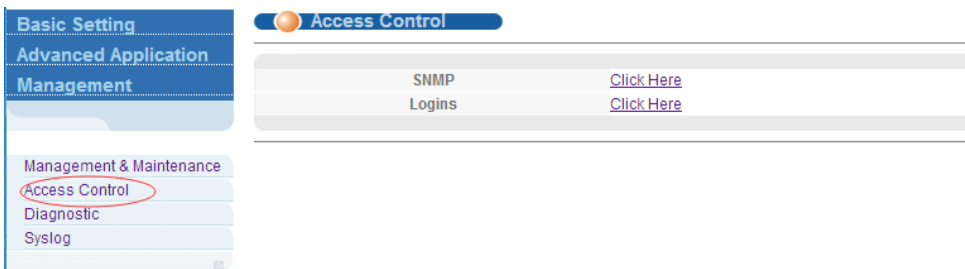


3.OAM Diag, Virtual cable can be tested.



### 4.3.2. Access Control

Selecting “Management> Access Control”, in the navigation bar, you can set SNMP and Logins.



#### 4.3.2.1. SNMP

Selecting “Management> Access Control>SNMP”, in the navigation bar, you can configure SNMP.

**SNMP** Access Control User

**General Setting**

Snm Server	ENABLE ▾
Community Name	<input type="text"/>
Access privilege	Read-write ▾

**Trap Destination**

Version	IP	Port	Username
v2c ▾	0.0.0.0	162	public
v2c ▾	0.0.0.0	162	public
v2c ▾	0.0.0.0	162	public
v2c ▾	0.0.0.0	162	public

**【Parameter Description】**

Parameter	Description
Community Name	Community string, is equal to the NMS and Snmp agent communication between the password
Access privilege	Read-only: specify the NMS (Snmp host) of MIB variables can only be read, cannot be modified Read- write: specify the NMS (Snmp host) of MIB variables can only read, can also be modified
Version	Set version: v1, v2c, v3
IP	Set the IP address of the trap host

**【Configuration Example】**

Such as: Add a group name public community, access to Read-Write. Set host 192.168.1.100 to receive trap messages. The specified version is v2c.

**SNMP** [Access Control](#) [User](#)

**General Setting**

Snm Server	ENABLE ▾
Community Name	public
Access privilege	Read-write ▾

**Trap Destination**

Version	IP	Port	Username
v2c ▾	192.168.1.100	162	public
v2c ▾	0.0.0.0	162	public
v2c ▾	0.0.0.0	162	public
v2c ▾	0.0.0.0	162	public

### 4.3.2.2. User Information

Selecting “**Management> Access Control>User Information**”, in the navigation bar, you can add user, set Security Level, Authentication, Privacy, Group, Password.

**SNMP** [Access Control](#) [User](#)

**General Setting**

Snm Server	ENABLE ▾
Community Name	
Access privilege	Read-write ▾

**Trap Destination**

Version	IP	Port	Username
v2c ▾	0.0.0.0	162	public
v2c ▾	0.0.0.0	162	public
v2c ▾	0.0.0.0	162	public
v2c ▾	0.0.0.0	162	public

#### 【Parameter Description】

Parameter	Description
Username	Snm username
Security Level	noauth auth pri
Authentication	MD5 SHA
Privacy	DES Privacy

Parameter	Description
Group	User group name
Password	Encrypted password

【Confi

guration Example】

Such as: Add group initial, add username user1.

### 4.3.2.3. Logins

Selecting “**Management>Access Control>Logins**”, in the navigation bar, you can modify admin password, configurable ordinary users.

Please record your new password whenever you change it. The system will lock you out if you have forgotten your password.

#### Edit Other Logins

Login	User Name	New Password	Retype to confirm	User privilege
1				0 Guest ▼
2				0 Guest ▼
3				0 Guest ▼
4				0 Guest ▼
5				0 Guest ▼
6				0 Guest ▼
7				0 Guest ▼
8				0 Guest ▼
9				0 Guest ▼
10				0 Guest ▼
11				0 Guest ▼
12				0 Guest ▼
13				0 Guest ▼
14				0 Guest ▼

【Parameter Description】

Parameter	Description
User privilege	0-1: Normal 2-15: administrator

【Configuration Example】

**Logins** [Access Control](#) [Super Password](#)

**Edit admin**

Old Password (1-32 characters)	•••••
New Password (1-32 characters)	•••••
Retype to confirm	•••••
User privilege (0:Guest 1:User 2-14:Operator 15:Manager)	15 Administrator

**Edit Other Logins**

Login	User Name	New Password	Retype to confirm	User privilege
1	Anne	•••••	•••••	0 Guest ▼
2				0 Guest ▼
3				0 Guest ▼
4				0 Guest ▼
5				0 Guest ▼
6				0 Guest ▼
7				0 Guest ▼
8				0 Guest ▼
9				0 Guest ▼
10				0 Guest ▼
11				0 Guest ▼
12				0 Guest ▼
13				0 Guest ▼
14				0 Guest ▼
15				0 Guest ▼

4.3.3. Diagnostic

Selecting “**Management> Diagnostic**”, in the navigation bar, you can Display or Clear System Log.

Basic Setting  
Advanced Application  
Management

Management & Maintenance  
Access Control  
**Diagnostic**  
Syslog

Diagnostic

- Info -

System Log    Display    Clear

### 【Configuration Example】

Such as: Display System Log.

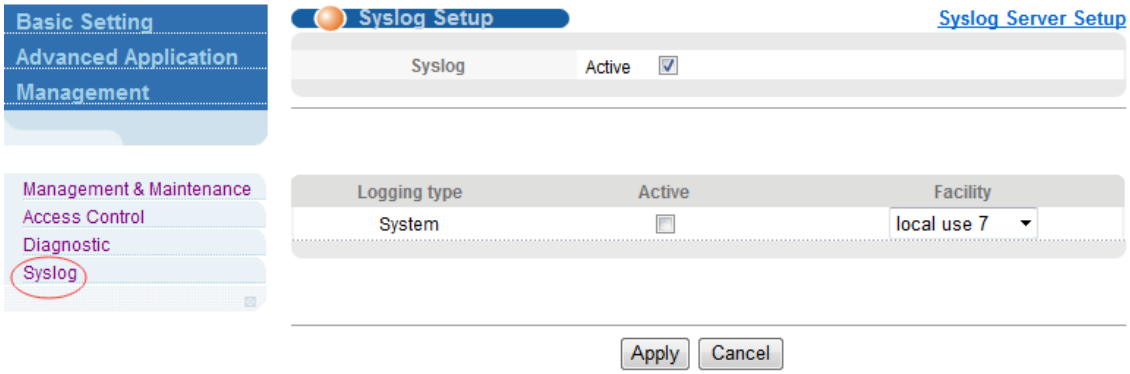
Diagnostic

```
2014/01/01 02:22:35: %OAM-5-LOGIN: The remote client
192.168.1.100 (admin) has logged in at web 1.
2014/01/01 02:22:28: %OAM-5-LOGOUT: The remote client
192.168.1.100 (admin) has logged out at web 1.
2014/01/01 02:21:47: %OAM-5-LOGIN: The remote client
192.168.1.100 (admin) has logged in at web 1.
2014/01/01 02:21:42: %OAM-5-LOGOUT: The remote client
192.168.1.100 (admin) has logged out at web 1.
2014/01/01 02:14:01: %OAM-5-LOGIN: The remote client
192.168.1.100 (admin) has logged in at web 1.
2014/01/01 02:13:52: %OAM-5-LOGOUT: The remote client
192.168.1.100 (admin) has logged out at web 1.
2014/01/01 02:11:40: %OAM-5-LOGIN: The remote client
192.168.1.100 (admin) has logged in at web 1.
2014/01/01 02:11:32: %OAM-5-LOGOUT: The remote client
```

System Log    **Display**    Clear

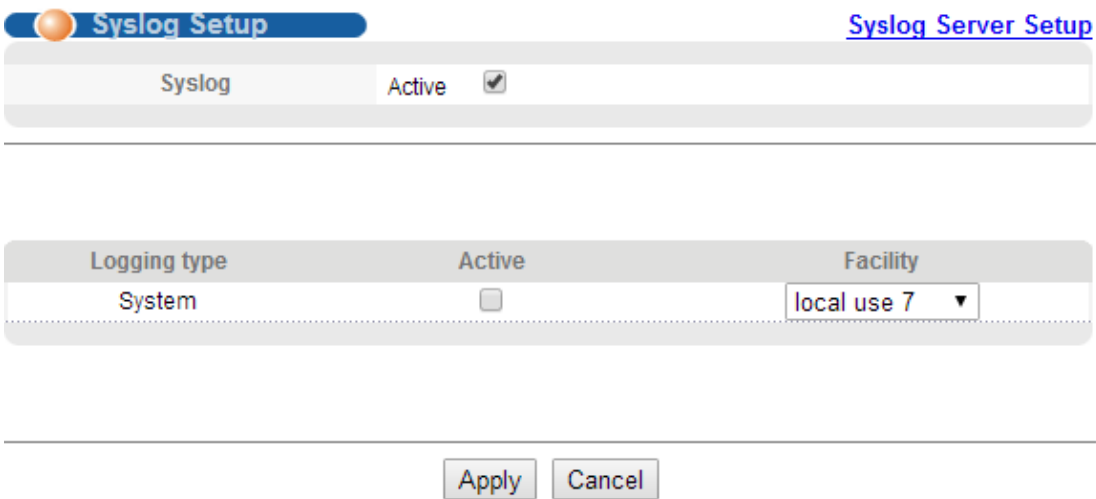
#### 4.3.4. Syslog

Selecting "**Management> Syslog**", in the navigation bar, you can configure syslog.



#### 4.3.4.1. Syslog Setup

Selecting “**Management>Syslog>Syslog Setup**”, in the navigation bar, you can start the logging function globally and the logging function of the corresponding module.



#### 【Parameter Description】

Parameter	Description
Facility	local use 0-7 kernel userlevel mail system security_1-2 sysogd lineprinter Networknews uucp clock_1-2 ftp logaudit logalert

#### 【Configuration Example】

Such as:



**Syslog Setup** [Syslog Server Setup](#)

Syslog  Active

---

Logging type	Active	Facility
System	<input checked="" type="checkbox"/>	local use 7

#### 4.3.4.2. Syslog Server Setup

Selecting “**Management>Syslog>Syslog Server Setup**”, in the navigation bar, you can set syslog server.

**Syslog Server Setup** [Syslog Setup](#)

Active

Server Address

Log Level

Index	Active	IP Address	Log Level	Delete
-------	--------	------------	-----------	--------

**【Parameter Description】**

Parameter	Description
Server Address	Syslog Server Address
Log Level	Level 0 Level 0-1 Level 0-2 Level 0-3 Level 0-4 Level 0-5 Level 0-6 Level 0-7
Server Address	Syslog Server Address

**【Instructions】**

Open the log switch, set up the syslog server, and the system log will be automatically pushed to the server.

**【Configuration Example】**

Such as: 1)set server address is 192.168.1.100.

**Syslog Server Setup** [Syslog Setup](#)

Active	<input checked="" type="checkbox"/>
Server Address	192.168.1.100
Log Level	Level 0 ▼

Index	Active	IP Address	Log Level	Delete
<a href="#">1</a>	Yes	192.168.1.100	0	<input type="checkbox"/>

## Appendix: Technical Specifications

Hardware Specifications		
Standards and Protocols	IEEE 802.3i, IEEE 802.3u, IEEE 802.3ab, IEEE802.3x, IEEE802.3z, IEEE802.3ad, IEEE802.1P, IEEE802.1Q, IEEE802.3at, IEEE802.3af	
Network Media	10BASE-T: UTP category 3,4,5 cable (maximum 100m) 100BASE-Tx: UTP category 5,5e cable (maximum 100m) 1000BASE-T: UTP category 5e,6 cable (maximum 100m) 1000Base-SX:62.5µm/50µm MMF(2m~550m) 1000Base-LX:62.5µm/50µm MMF(2m~550m) or 10µm SMF (2m~5000m)	
Transfer Method	Store-and-Forward	
Switching Capacity	56Gbps	
Packet Forwarding	41.66Mbps	
Packet Buffer	4.1Mbit	
MAC Address Table	8K	
Jumbo Frame	9KByte	
Number of Ports	24 x 10/100/1000Mbps Auto-Negotiation ports 4 x Gigabit Combo ports 1 x RJ45 Console Port	
PoE Ports(RJ45)	24* PoE ports compliant with IEEE802.3at/af	
Power Pin Assignment	1/2(+),3/6(-)	
PoE Budget	370W	
Indicators	Per Port	10/100Mbps Link/Act:Orange 1000Mbps Link/Act: Green PoE: Yellow
	Per Device	Power: Green SYS:Green
Power Supply	AC 100-240V/50-60Hz 400W internal power	
Power Consumption	Maximum:430W(220V/50Hz)	
Dimensions ( W x D x H )	440*208*44mm	
Environment	Operating Temperature: 0°C - 45°C Storage Temperature: -40°C - 70°C Operating Humidity: 10%~90% RH non-condensing Storage humidity: 5%~90% RH non-condensing	

<b>Hardware Specifications</b>		
<p><b>Basic function</b></p> <ul style="list-style-type: none"> <li>● Ethernet Setup</li> <li>● STP/RSTP/MSTP</li> <li>● Storm-control</li> <li>● Port Monitor</li> <li>● Port rate-limit</li> <li>● MAC filtering</li> <li>● Link Aggregation(static, LACP)</li> <li>● Jumbo Frame</li> <li>● Port security</li> <li>● Bandwidth Control</li> </ul>	<p><b>Three layers of functional</b></p> <ul style="list-style-type: none"> <li>● The ARP deception, the network cheating</li> <li>● Filtering the IP port</li> <li>● Static binding IP and MAC</li> <li>● Arp trust port</li> <li>● Static routing capacity</li> <li>● Ping and Traceroute</li> </ul>	<p><b>The security policy</b></p> <ul style="list-style-type: none"> <li>● ACE capacity</li> <li>● ACL</li> <li>● QoS</li> <li>● DAI</li> </ul>
<p><b>VLAN</b></p> <ul style="list-style-type: none"> <li>● Port based VLAN,Private VLAN</li> <li>● MAC based VLAN</li> <li>● Voice VLAN</li> <li>● Gvrp</li> <li>● 802.1Q VLAN</li> </ul>	<p><b>Safety features</b></p> <ul style="list-style-type: none"> <li>● Radius</li> <li>● Tacacs+</li> <li>● Preventing DOS attacks</li> <li>● dot1x</li> <li>● The gateway ARP deception</li> </ul>	<p><b>Application protocol</b></p> <ul style="list-style-type: none"> <li>● DHCP Relay</li> <li>● DHCP snooping</li> <li>● DHCP Client</li> <li>● FTP/TFTP</li> </ul>
<p><b>Management</b></p> <ul style="list-style-type: none"> <li>● HTTP WEB</li> <li>● Telnet</li> <li>● SSH</li> <li>● Console</li> </ul>	<p><b>Other function</b></p> <ul style="list-style-type: none"> <li>● LLDP</li> <li>● IGMP Snooping</li> <li>● SNMPV1,V2c,V3</li> <li>● RMON (1,2,3,9)</li> <li>● Virtual stack</li> </ul>	