52-Port Managed Gigabit L2+ Switch

User's Manual

V1.0.0

Foreword

General

This manual introduces the functions and operations of the 52-Port Managed Gigabit L2+ Switch with 48 × Gigabit Ports and 4 × 10G SFP+ (hereinafter referred to as "the switch").

Safety Instructions

The following categorized signal words with defined meaning might appear in the manual.

Signal Words	Meaning
DANGER	Indicates a high potential hazard which, if not avoided, will result in death or serious injury.
WARNING	Indicates a medium or low potential hazard which, if not avoided, could result in slight or moderate injury.
CAUTION	Indicates a potential risk which, if not avoided, could result in property damage, data loss, lower performance, or unpredictable result.
TIPS	Provides methods to help you solve a problem or save you time.
NOTE	Provides additional information as the emphasis and supplement to the text.

Revision History

Version	Revision Content	Release Time
V1.0.0	First release.	July 2020

About the Manual

- The manual is for reference only. If there is inconsistency between the manual and the actual product, the actual product shall prevail.
- We are not liable for any loss caused by the operations that do not comply with the manual.
- The manual would be updated according to the latest laws and regulations of related jurisdictions. For detailed information, refer to the paper manual, CD-ROM, QR code or our official website. If there is inconsistency between paper manual and the electronic version, the electronic version shall prevail.
- All the designs and software are subject to change without prior written notice. The product updates might cause some differences between the actual product and the manual. Please contact the customer service for the latest program and supplementary documentation.
- There still might be deviation in technical data, functions and operations description, or errors in print. If there is any doubt or dispute, we reserve the right of final explanation.
- Upgrade the reader software or try other mainstream reader software if the manual (in PDF format) cannot be opened.
- All trademarks, registered trademarks and the company names in the manual are the properties of their respective owners.
- Please visit our website, contact the supplier or customer service if there is any problem occurring when using the device.
- If there is any uncertainty or controversy, we reserve the right of final explanation.

Important Safeguards and Warnings

The manual helps you to use our product properly. To avoid danger and property damage, read the manual carefully before using the product, and we highly recommend you to keep it well for future reference.

Operating Requirements

- Do not expose the device directly to the sunlight, and keep it away from heat.
- Do not install the device in the damp environment, and avoid dust and soot.
- Make sure the device is in horizontal installation, and install the device on solid and flat surface to avoid falling down.
- Avoid liquid spattering on the device. Do not place object full of liquid on the device to avoid liquid flowing into the device.
- Install the device in the well-ventilated environment. Do not block the air vent of the device.
- Use the device at rated input and output voltage.
- Do not dissemble the device without professional instruction.
- Transport, use, and store the device in allowed ranges of humidity and temperature.

Power Supply Requirements

- Use the battery properly to avoid fire, explosion, and other dangers.
- Replace the battery with battery of the same type.
- Use locally recommended power cord in the limit of rated specifications.
- Use the standard power adapter. We will assume no responsibility for any problems caused by nonstandard power adapter.
- The power supply shall meet the SELV requirement. Use the power supply that conforms to Limited Power Source, according to IEC60950-1. Refer to the device label.
- Adopt GND protection for I-type device.
- The coupler is the disconnecting apparatus. Keep it at the angle for easy to operate.

Table of Contents

1 Product Introduction

1.1 Product Overview

The Switch can provide forty-eight 10/100/1000Mbps self-adaption RJ45 port, plus four 10G SFP+ optical port; 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, easy to maintenance and management, meet the networking and access requirements of enterprises, intelligent village, hotel, office network and campus network. Built-in high reliability, design for wide voltage input application power supply, even if the voltage is not stable of power grid, also can guarantee the equipment can work normally.

48 ports have PoE power supply function, support IEEE802.3at standard, 802.3af downward compatibility, power supply equipment for Ethernet, can automatically detect identification standard of electrical equipment, and through the cable for the power supply.

1.2 Features

- Supports IEEE 802.3i, IEEE 802.3u, IEEE802.3ab, IEEE802.3z, IEEE802.3ae, IEEE802.3x, IEEE802.3at, IEEE802.3af, IEEE802.3az.
- Supports PoE power up to 30W for each PoE port, all power up to 400W.
- Integrated High-Performance Cortex-A9 processor.
- Supports MAC address auto-learning and auto-aging.
- Forty-eight 10/100/1000Mbps self-adaption RJ45 port, plus four 10G SFP+ port, it can be used to link bandwidth higher upstream equipment.
- Store and forward mode operates.
- LED indicators for monitoring power, link/activity, Speed, PoE.
- Support QoS, port mirroring, link aggregation protocol.
- 19 inches full metal iron shell and internal 450W high performance power supply design, suitable for rack installation.

1.3 External Component Description

1.3.1 Front Panel

The front panel of the Switch consists of a series of LED indicators, 1 x Reset button, 48 x 10/100/1000Mbps RJ-45 ports, 1x Console port, ,and 4x SFP+ ports as shown as below.

Figure 1-1 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 1-2 LED Indicator

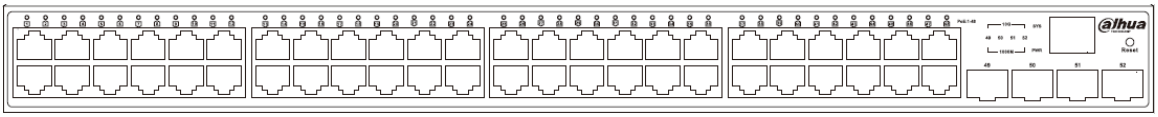


Table 1-1 LED Indicator

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 starting or the system starts successfully
10/100/1000 BASE-T adaptive Ethernet port indicators (1-48)	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 (49-52)	Link/Act	Off	The port is NOT connected.
		Solid green	The port is connected at 10Gbps.
		Solid orange	The port is connected at 1000Mbps.
		Blinking	The port is transmitting or receiving data.

- Reset button (Reset):
  Keep the device powered on and push a paper clip into the hole. Press down the button for 5 seconds to restore the Switch to its original factory default settings.
- Console port (Console):
  Designed to connect with the serial port of a computer or terminal for monitoring and configuring the Switch.
- 10/100/1000Mbps RJ-45 ports (1~48):
  Designed to connect to the device with a bandwidth of 10Mbps, 100Mbps or 1000Mbps.

Each has a corresponding Link/Act/Speed.

- SFP ports (49~52):
  Four SFP transceiver module ports, each port corresponds to two SFP indicator lights, the top is a 10G green light, the bottom is a gigabit orange light.

1.3.2 Rear Panel

The rear panel of the Switch contains AC Power and Grounding Terminal shown as below.

Figure 1-3 Rear Panel

- AC Power Connector:
  Power is supplied through an external AC power adapter. It supports AC 100~240V, 50/60Hz.
- Grounding Terminal:
  Located on the right side of the power supply connector, use wire grounding for lightning protection.

WARNING

Please connect the three-core plug of the power cord with the ground safely.

2 Installing and Connecting the Switch

Please follow the steps below to install and connect the Ethernet switch.

2.1 Unpacking Inspection

Open the packaging box and check the accessories in the box:

- One PoE Web Ethernet Switch.
- One Installation Component
- One AC power cord.
- One User Manual.

If any part is lost and damaged, please contact your local agent immediately. Please keep in case it needs to be returned to the factory for replacement.

2.2 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.
- Before cleaning the switch, remove the power adapter from the switch. Don't wipe with a wet cloth and don't clean with liquid.

2.2.1 Desktop Installation

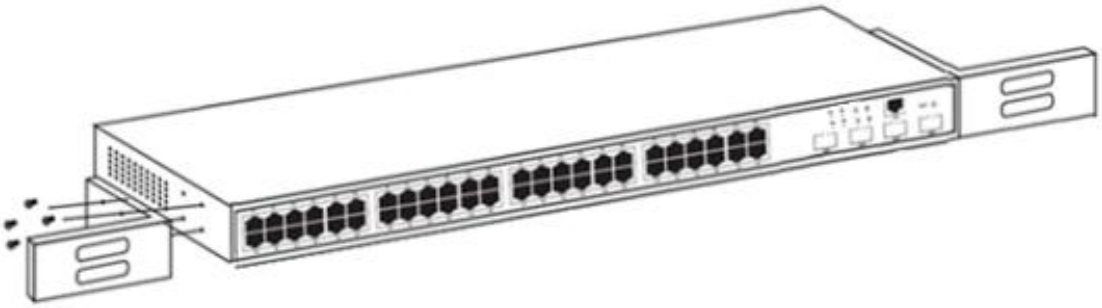
When installing the Switch on a desktop, please attach these cushioning rubber feet provided on the bottom at each corner of the Switch in case of the external vibration. Allow adequate space for ventilation between the device and the objects around it.

2.2.2 Rack-mountable Installation

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:

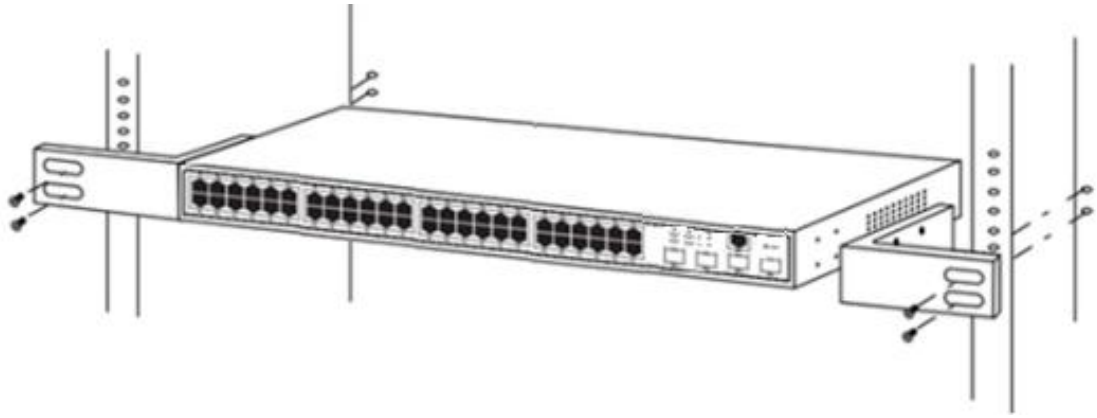
Step 1 Attach the mounting brackets on the Switch's side panels (one on each side) and secure them with the screws provided.

Figure 2-1 Mounting bracket



Step 2 Use the screws provided with the equipment rack to mount the Switch on the rack and tighten it.

Figure 2-2 Mounting to bracket



2.2.3 Power on

It is powered on by the AC 100-240V 50/60Hz internal high-performance power supply.

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.

2.3 Connect the Switch

2.3.1 Connected Computer (NIC)

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 LNK/ACT/Speed status indicator lights corresponding ports of the Switch.

2.3.2 Connected Load

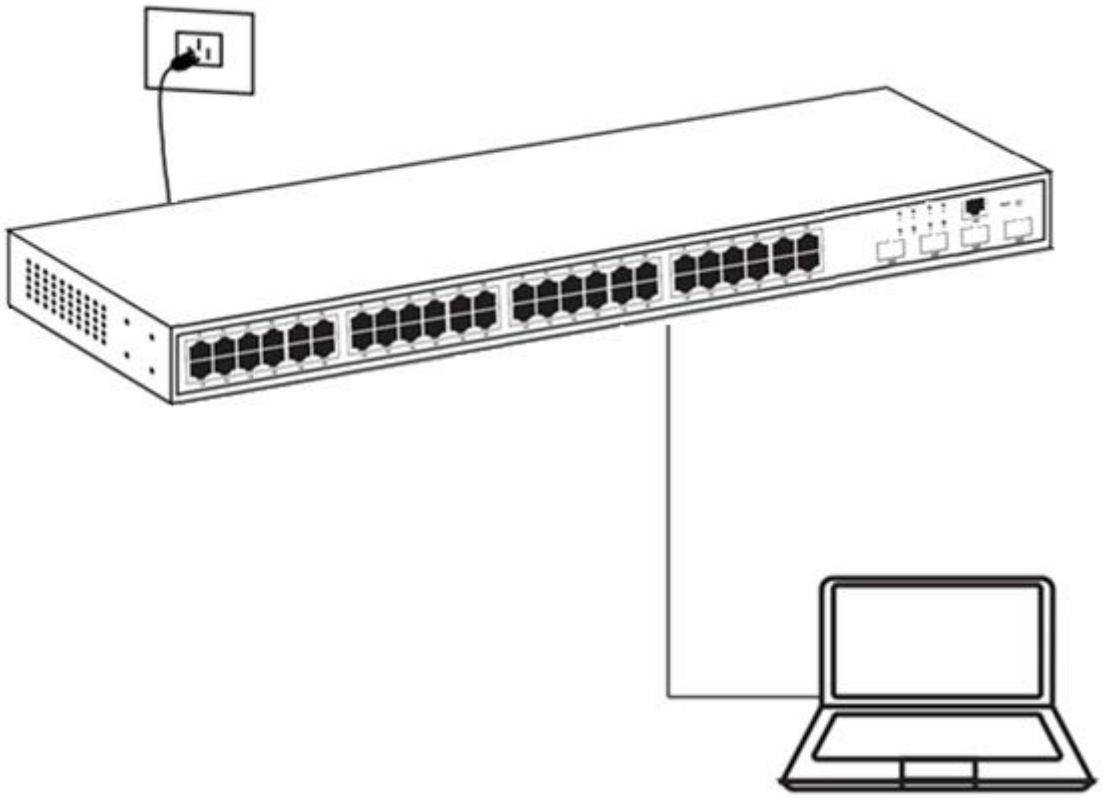
1-48 ports of the Switch have PoE power supply function, the maximum output power up to 30W each port, it can make PD devices, such as internet phone, network camera, wireless access point work. You only need to connect the Switch PoE port directly connected to the PD port by network cable.

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 3-1 Connect to the switch



The LINK/ACT/Speed LEDs for each port lights on when the link is available.

3.2 Login

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.

Table 3-1 Default Settings

Parameter	Default Value
Default IP address	192.168.1.110
Default Username	admin
Default Password	admin

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

Step 1 Connect the Switch with the computer NIC interface and power it on.

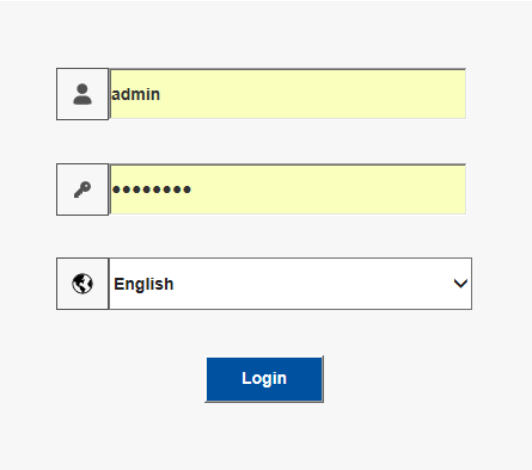
Step 2 Check whether the IP address of the computer is within this network segment: 192.168.1.xx (“xxx” ranges 2~254), for example, 192.168.1.100.

Step 3 Open the browser, and enter http://192.168.1.1 and then press Enter.

Step 4 Enter the username and password (factory default username admin, password admin). Clink Login to log in to the switch configuration window.

Select Chinese in the drop-down box of the interface to switch the language to Chinese.

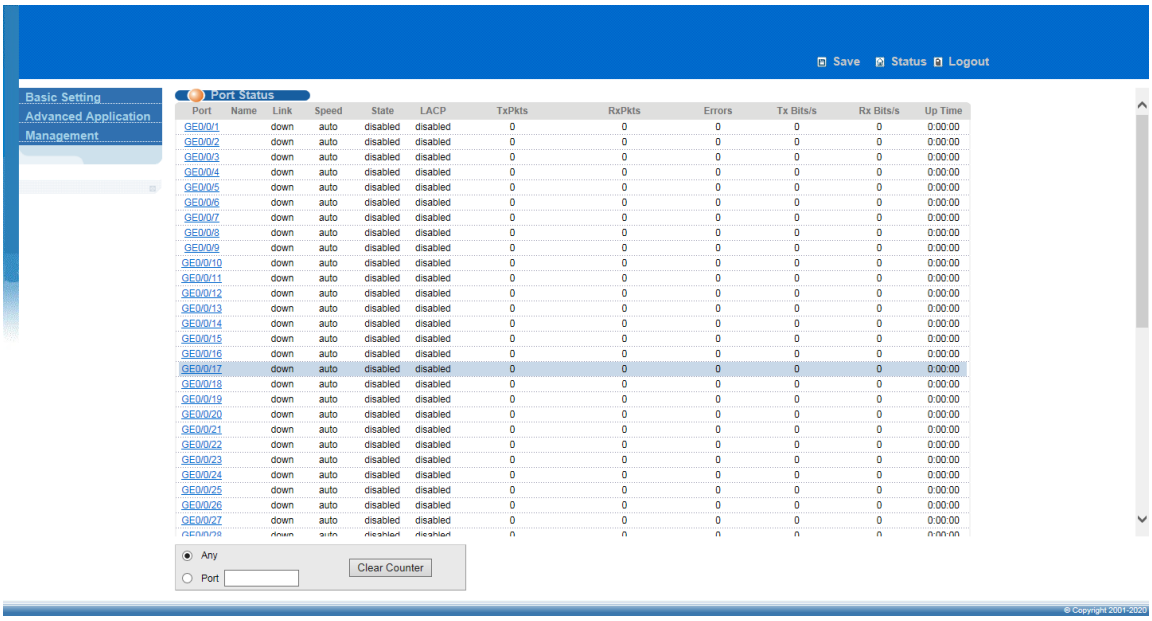
Figure 3-2 Login Page



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.

Figure 4-1 WEB Configuration



Click the menu tree on the left to expand the corresponding submenu link, click a submenu, expand the configuration item under the submenu, and configure it.

- Click **Save** to save the device to device configuration for this login.
- Click **Status** to view port status information.
- Click **Logout** to log out to the login screen.

4.2 Basic Setting

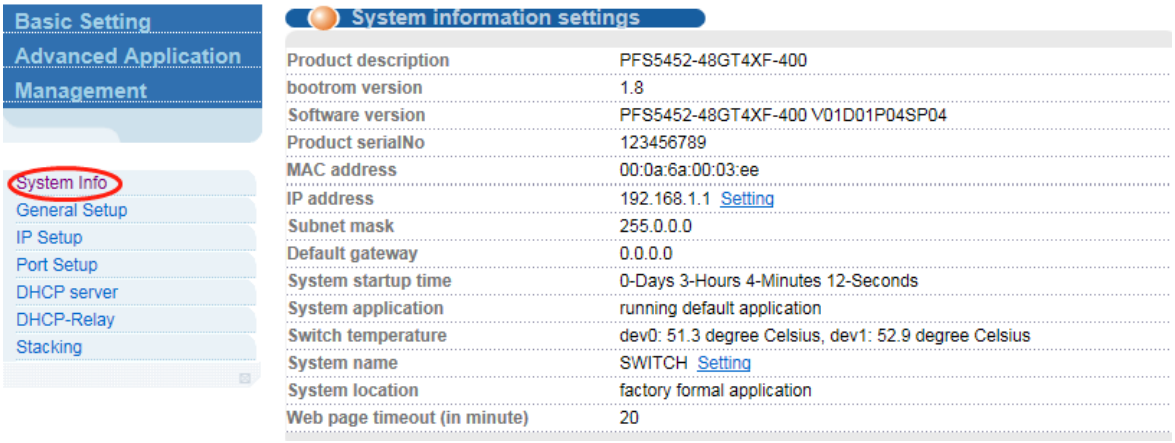
Select **Basic Setting**, you can make settings such as system information, general setup, IP setup and port setup.

Figure 4-2 Basic Setting

4.2.2 System Info

Select **Basic Setting > System Info** in the navigation bar, you can view the basic information of System and configure the IP address and System name.

Figure 4-3 System Info



Parameter Description

- IP Address: The management IP of Switch.
- System name: System name.

Instructions

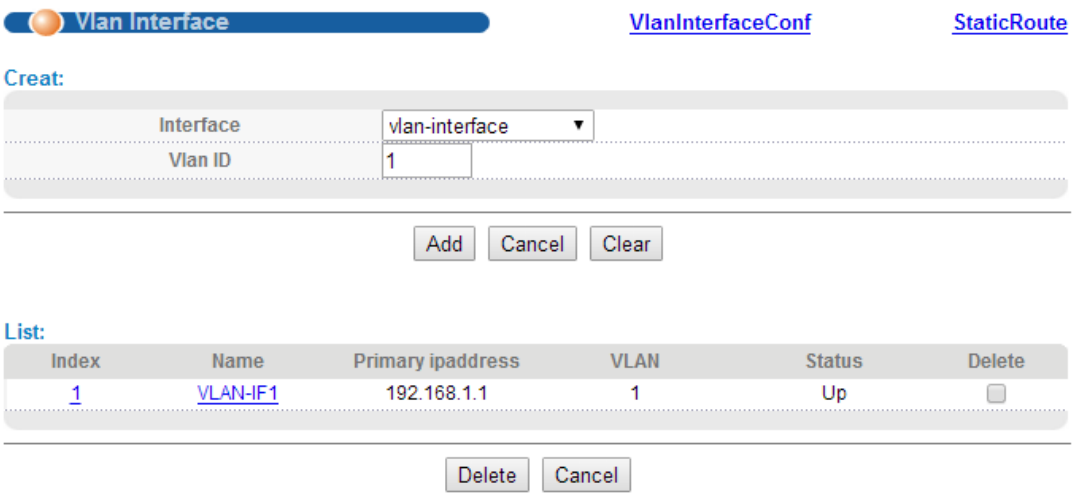
You can view and configure Running System status.

Configuration Example

For example, set the IP address to“192.168.2.1” and the system name to “Switch”.

Vlan Interface

Figure 4-4 Vlan Interface



- Interface: You can select the way of interface, including vlan-interface and

supervlan-interface.

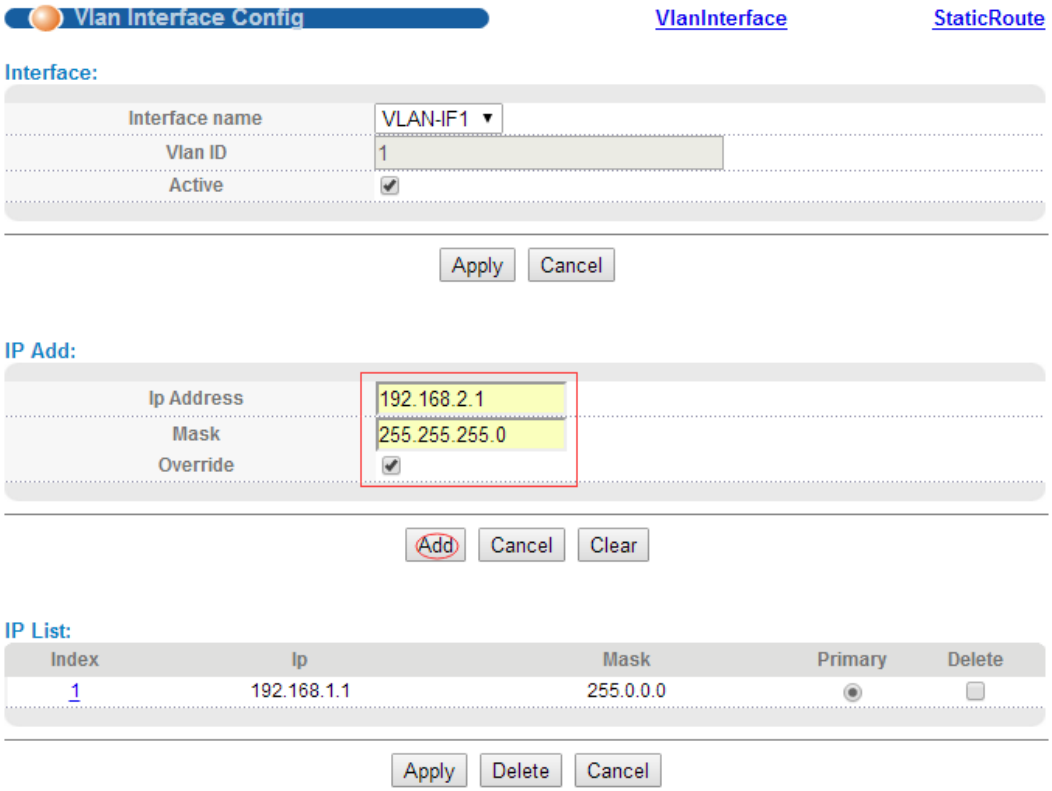
- Vlan ID: You can choose the Vlan ID.

Vlan Interface Config

Set IP address as 192.168.2.1 and mask as 255.255.255.0, and then selecting override.

Override: You can override or not override original main IP address.

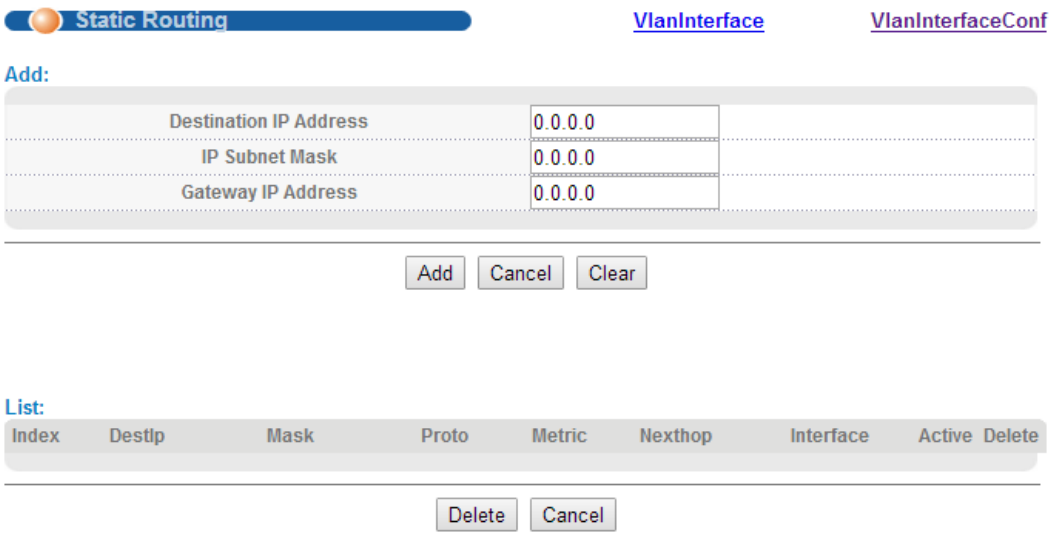
Figure 4-5 Vlan Interface Config



Static Routing

Static Routing is one that specifies one or more address.

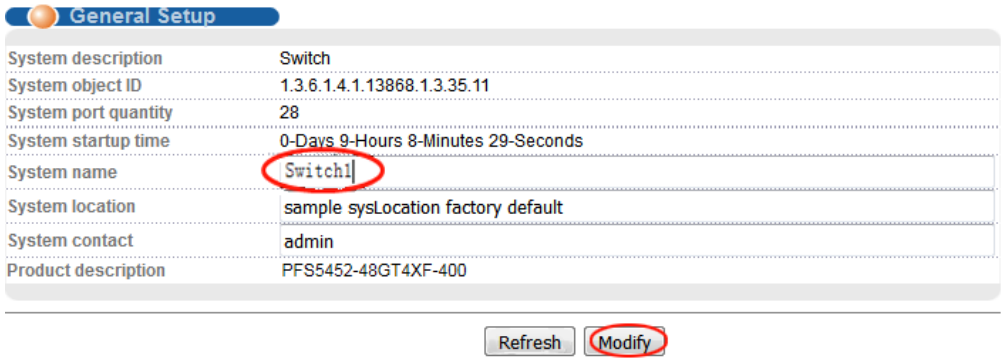
Figure 4-6 Static Routing



- Destination IP Address: Setting destination IP Address of Static Routing.
- IP Subnet Mask: Setting IP Subnet Mask.
- Gateway IP Address: Setting IP Address.

Setting System name as “Switch”

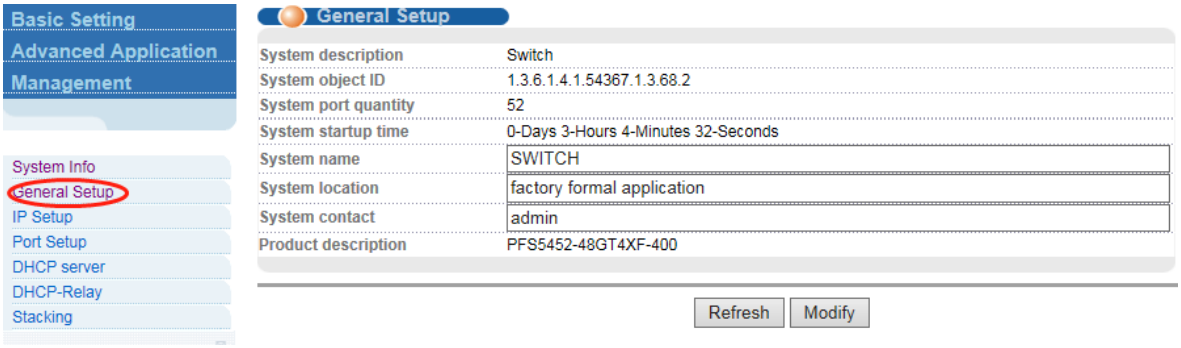
Figure 4-7 System name(1)



4.2.3 General Setup

Select **Basic Setting > General Setup** to view or configure Switch information. Such as view System description, system object id, configure system name, system location, system contact.

Figure 4-8 General Setup



Parameter Description

- System name: System name.
- System contact: including Company or related URL.

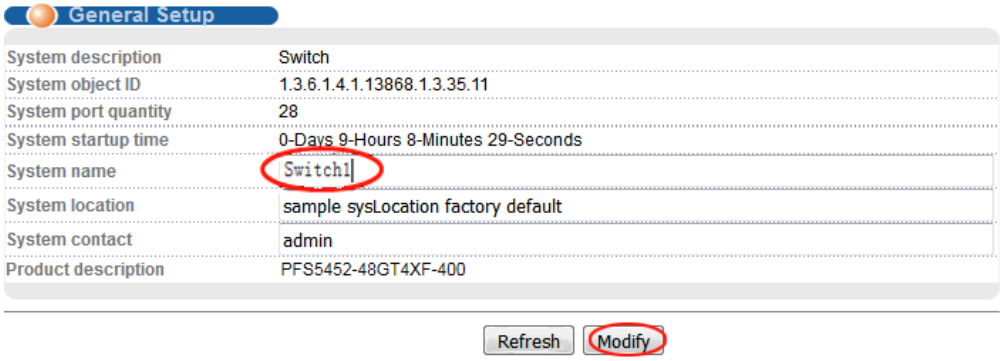
Instructions

You can view and configure Running System information.

Configuration Example

For example, set the system name to “Switch1”.

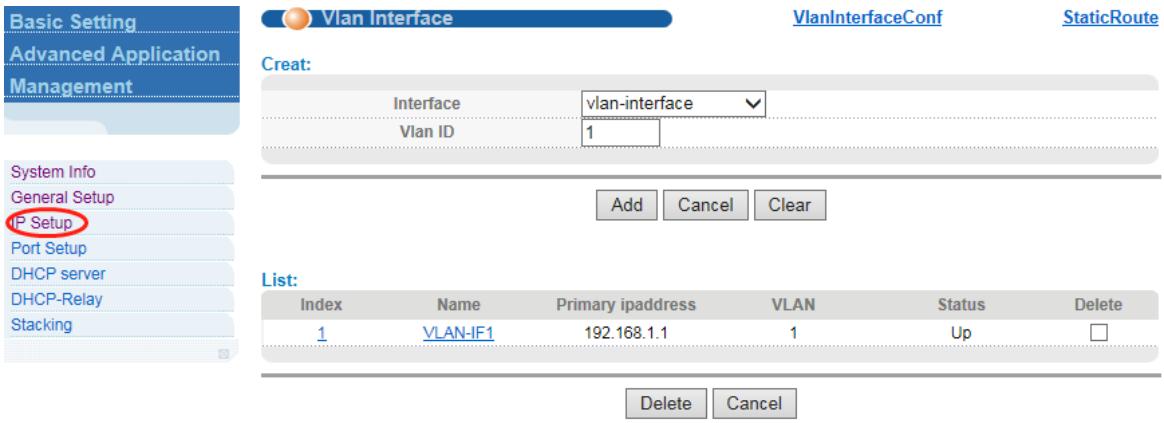
Figure 4-9 System name(2)



4.2.4 IP Setup

Select **Basic Setting > IP Setup**, you can configure IP.

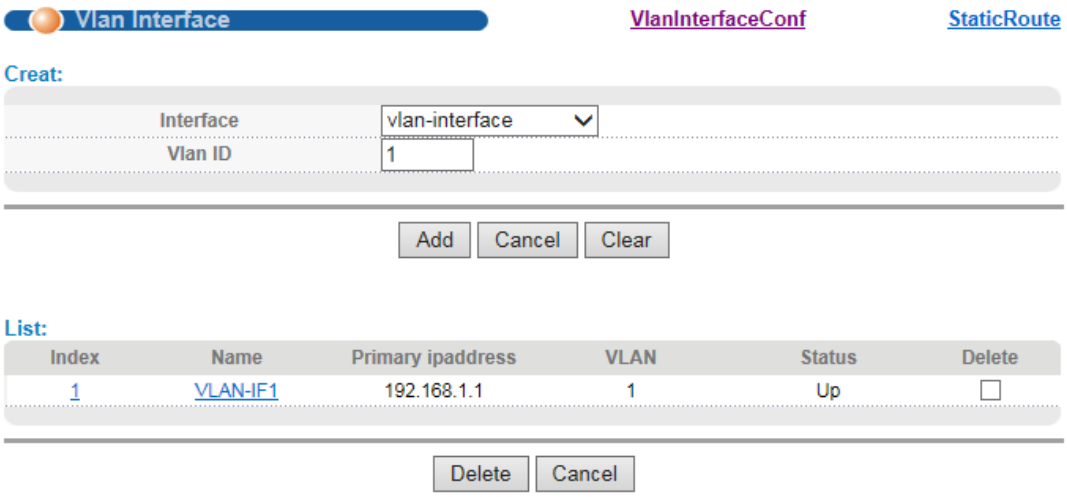
Figure 4-10 IP Setup



4.2.4.2 Vlan interface

Select **Basic Setting > IP Setup > Vlan interface** to set the Vlan interface.

Figure 4-11 Vlan interface



Parameter Description

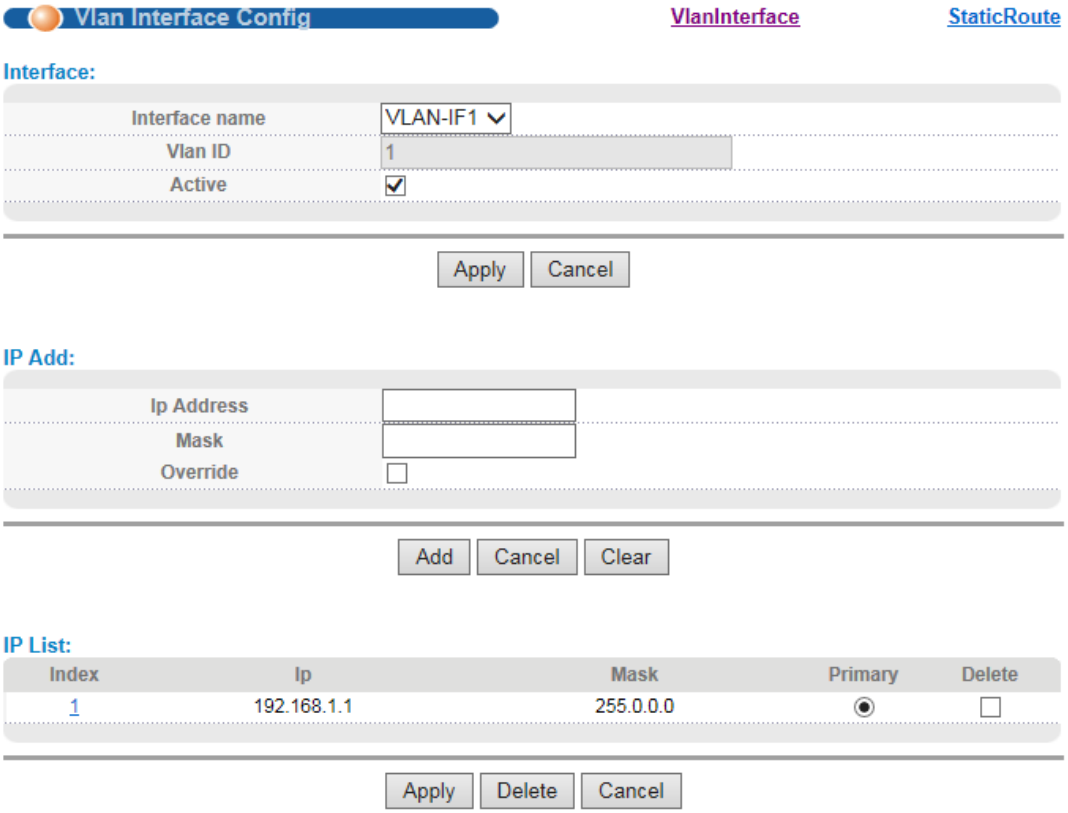
Table 4-1 Vlan interface parameter description

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

4.2.4.3 Vlan interface Config

Select **Basic Setting > IP Setup > Vlan interface Config**, configure Vlan interface Config.

Figure 4-12 Vlan interface Config



Parameter Description

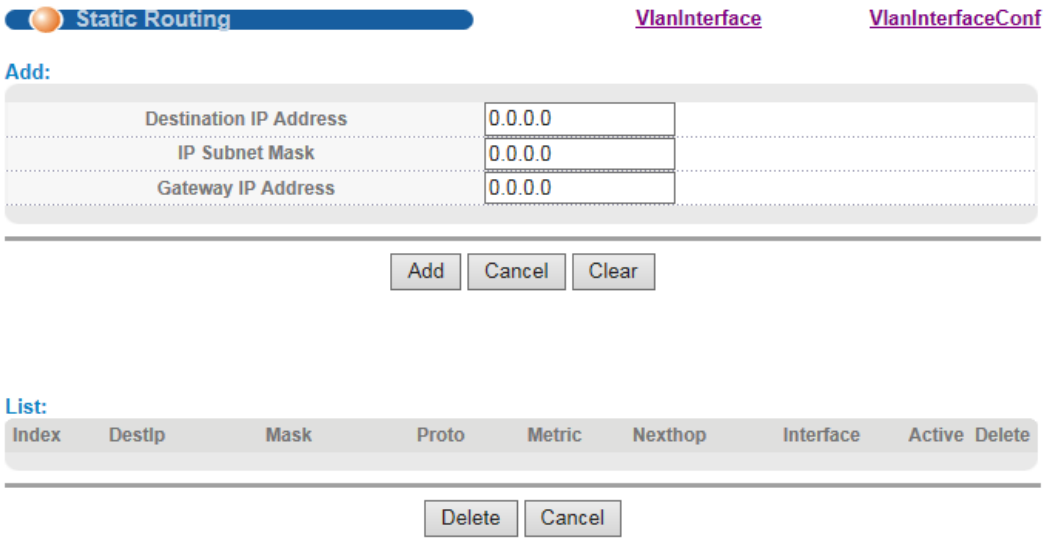
Table 4-2 Vlan Interface Config parameter description

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 formeroriginal primary IP or not

4.2.4.4 Static Routing

Select **Basic Setting > IP Setup > Static Routing** to specify some routing manually.

Figure 4-13 Static Routing



Parameter Description

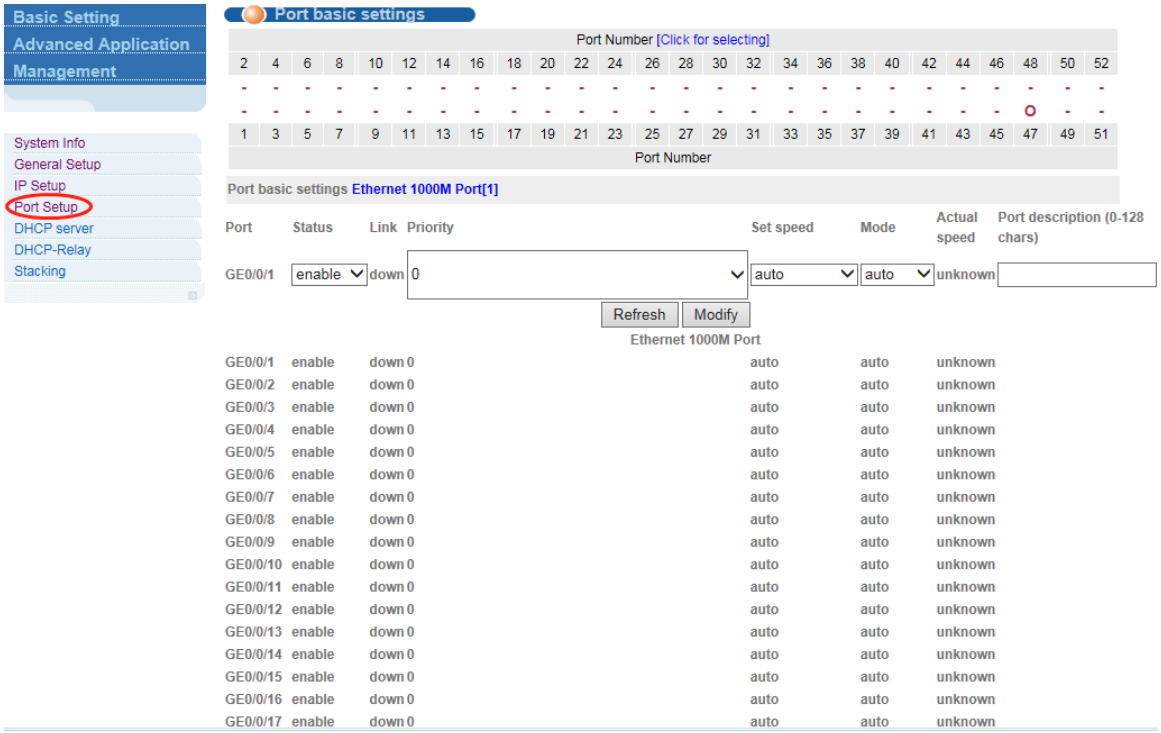
Table 4-3 Static Routing parameter description

Parameter	Description
Destination IP Address	Setting destination IP Address of Static Routing.
IP Subnet Mask	Setting IP Subnet Mask.
Gateway IP Address	Setting IP Address.

4.2.5 Port Setup

Select **Basic Setting > Port Setup** to configure the related parameter of port.

Figure 4-14 Port Setup



Parameter Description

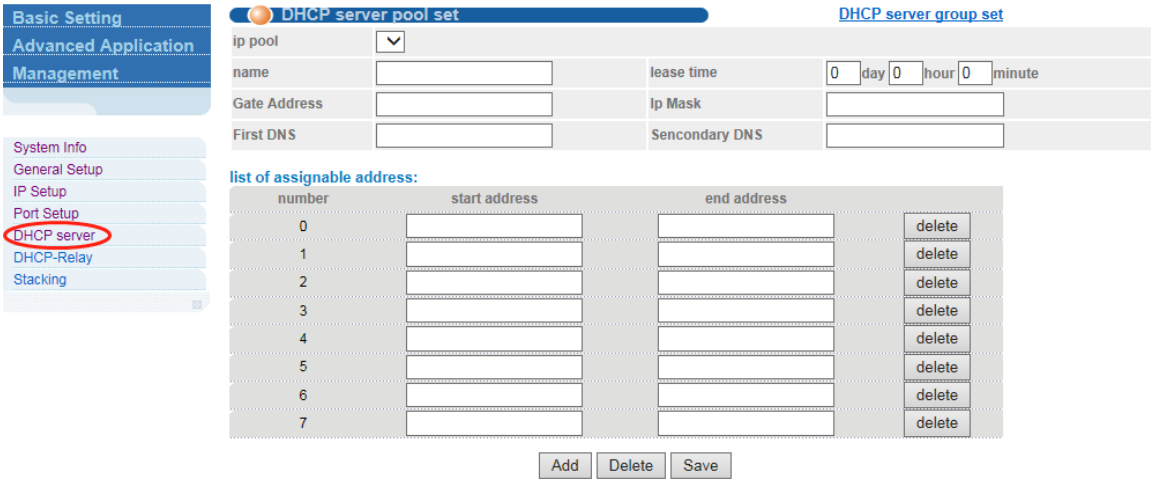
Table 4-4 Port Setup parameter description

Parameter	Description
Port	Port number.
status	The port state can be set to disable to close the port, and the default state is to enable.
link	“Down” is the unconnected state and “up” is the connected state.
priority	Set port priority, the range of 0-7.
Set speed	Select the following modes: ● 10/100/1000Mbps Ethernet port Auto, half-100, full-100, half-1000, full-1000 ● 1000/10000Mbps SFP+ Full-1000M, Full-10G
Mode	Select the following kinds: auto, sub, main.
Actual speed	The actual speed of the port.
Port description	The port is described.

4.2.6 DHCP Server

Select **Basic Setting > DHCP Server** to configure DHCP server pool and DHCP server group.

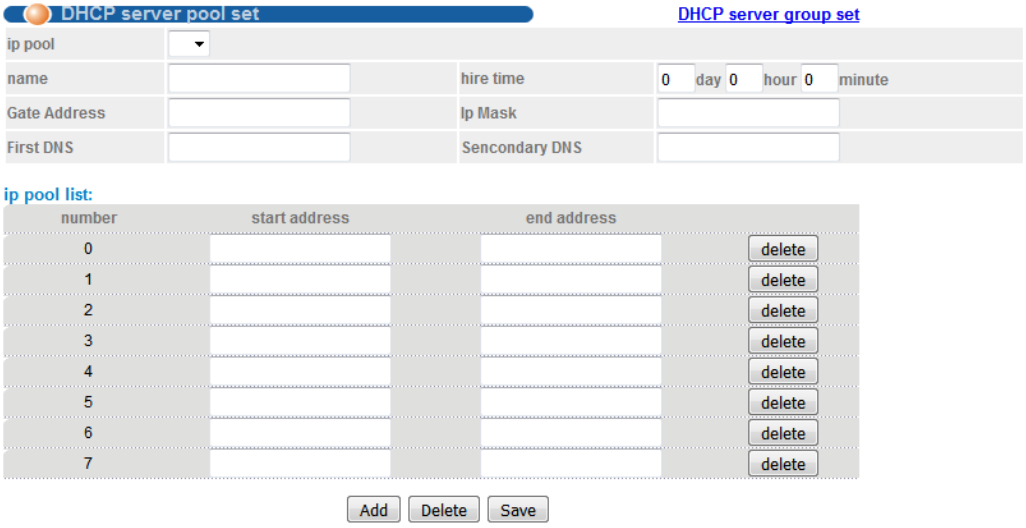
Figure 4-15 DHCP Server



4.2.6.2 DHCP server pool set

Select **Basic Setting > DHCP server > DHCP server pool set** to configure DHCP Server pool set.

Figure 4-16 DHCP Server pool set



Parameter Description

Table 4-5 DHCP Server pool set parameter description

Parameter	Description
ip pool	IP pool ID.
name	Set the name of IP pool.
hire time	Set hire time.
Gate Address	Set Gate Address.
Ip Mask	Set IP Mask.
First DNS	Set First DNS.

Secondary DNS	Set Secondary DNS.

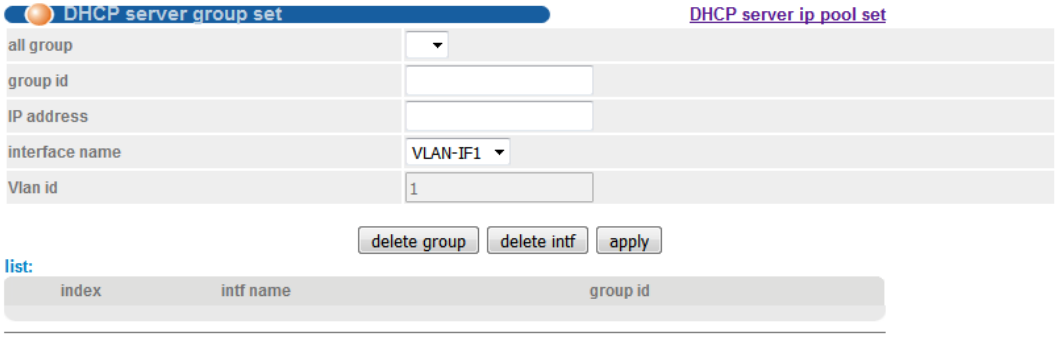
Instructions

Configure DHCP server address pool functionality, including subnet addresses, subnet masks, lease times, etc.

4.2.6.3 DHCP server group set

Select **Basic Setting > DHCP server > DHCP server group set** in the navigation bar, you can configure DHCP Server group.

Figure 4-17 DHCP Server group set



Parameter Description

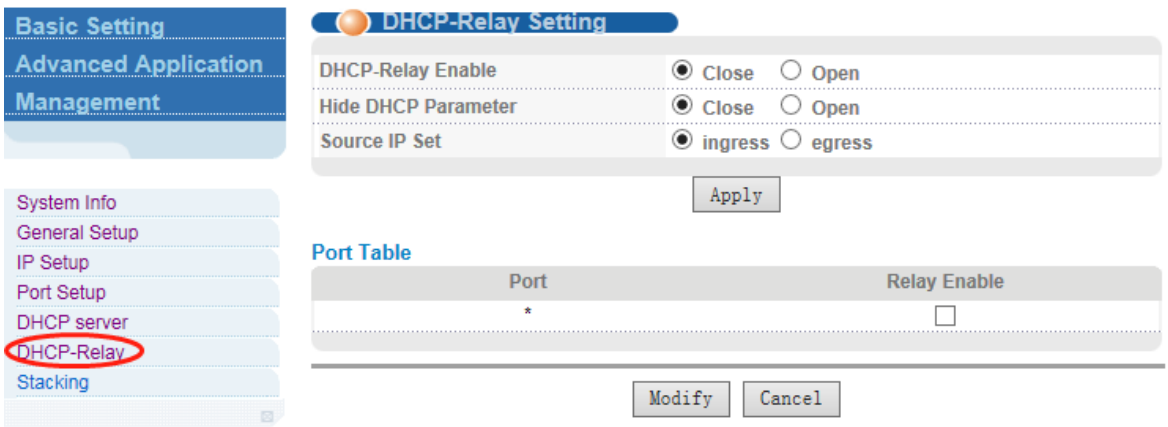
Table 4-6 DHCP Server group set parameter description

Parameter	Description
group id	DHCP server group id.
IP address	DHCP server IP address.

4.2.7 DHCP-Relay

Select **Basic Setting > DHCP-Relay** to turn on the DHCP relay function, Hidden DHCP Server. Set the source IP used.

Figure 4-18 DHCP-Relay



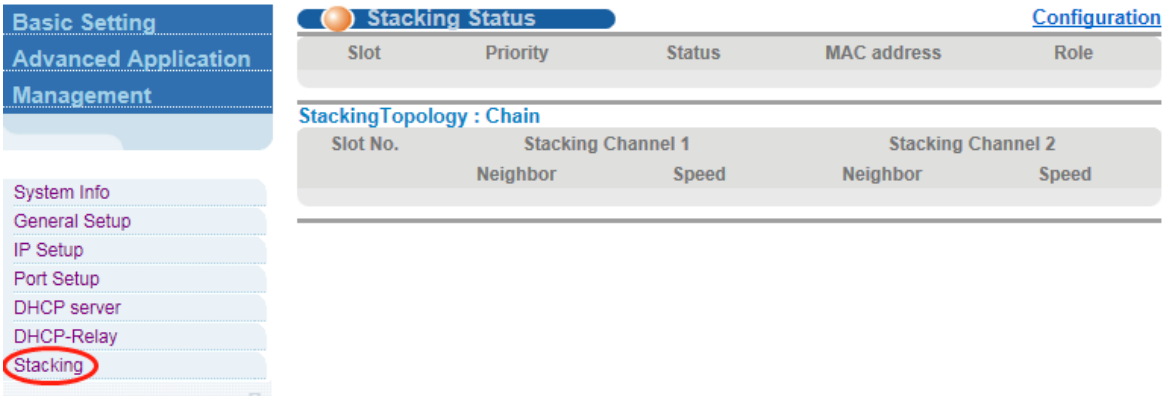
Instructions

Sometimes, for network security reasons, network administrators do not want DHCP clients to know the DHCP server's address. To meet this requirement, devices that enable DHCP relay can be configured to hide the address of the real DHCP server. Thus, the DHCP client considers the device on which DHCP relay is turned on to be a DHCP server in order to hide the real DHCP server. Of course, if the DHCP relay is enabled on a device that also happens to be a DHCP server, this feature is no longer applicable.

4.2.8 Stacking

Select **Basic Setting > Stacking** to view the stack interface information, neighbor interface information, start the stack function and set system priority.

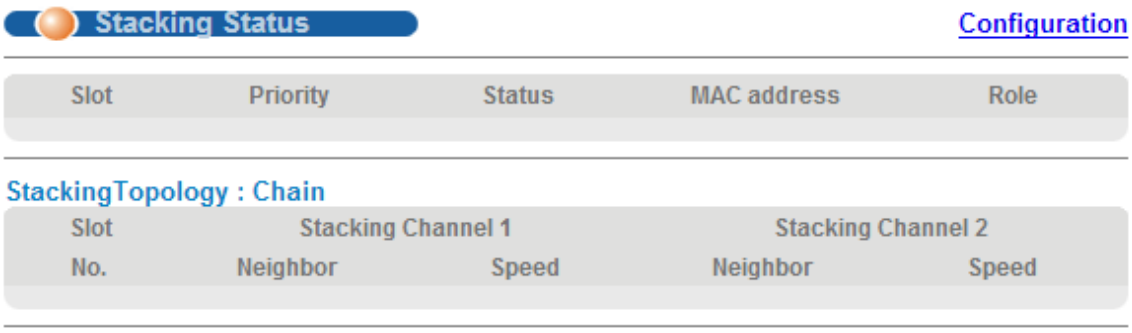
Figure 4-19 Stacking



4.2.8.2 Stacking Status

Select **Basic Setting > Stacking > Stacking Status** to view the stack interface information, neighbor interface information.

Figure 4-20 Stacking Status



Parameter Description

Table 4-7 Stacking Status parameter description

Parameter	Description

Slot	Each device in the system must manually specify an unrepeatable ID number to unique identify.
Status	Two different working modes: ● Single-machine mode: this mode is the same as the general switch, not to provide the stack function. ● Stack mode: this mode opens the stack function, can make up a stack system with other devices.
Priority	Each device in the system can be assigned a priority, devices with higher-priority more likely to be elected as main device.

Instructions

Stack is a virtual logical device that consists of multiple devices connected together by stacking ports. Users manage logical devices to complete the management of all physical devices. Stacks can now only use devices of the same capability, supporting both ring and linear topologies.

Stacking has the following major advantages:

- Network scalability

  In the early stage of network construction, fewer devices are used to network, while in the later stage, the number of ports and bandwidth are expanded by increasing the number of stacked devices.

- Reliability

  The stack system consists of a main device and multiple sub devices. The main device completes the management and maintenance of the stack system, while the subordinate device participates in business data processing. When the main device fails, the system will elect a new main device to complete the backup function of the device. In addition, physical ports between devices support the function of aggregation to complete the port backup function.

- Convenient management

  You can log in to the stack system for administrative configuration from any port of any device on the stack system, without the need for separate administrative configuration for each member device.

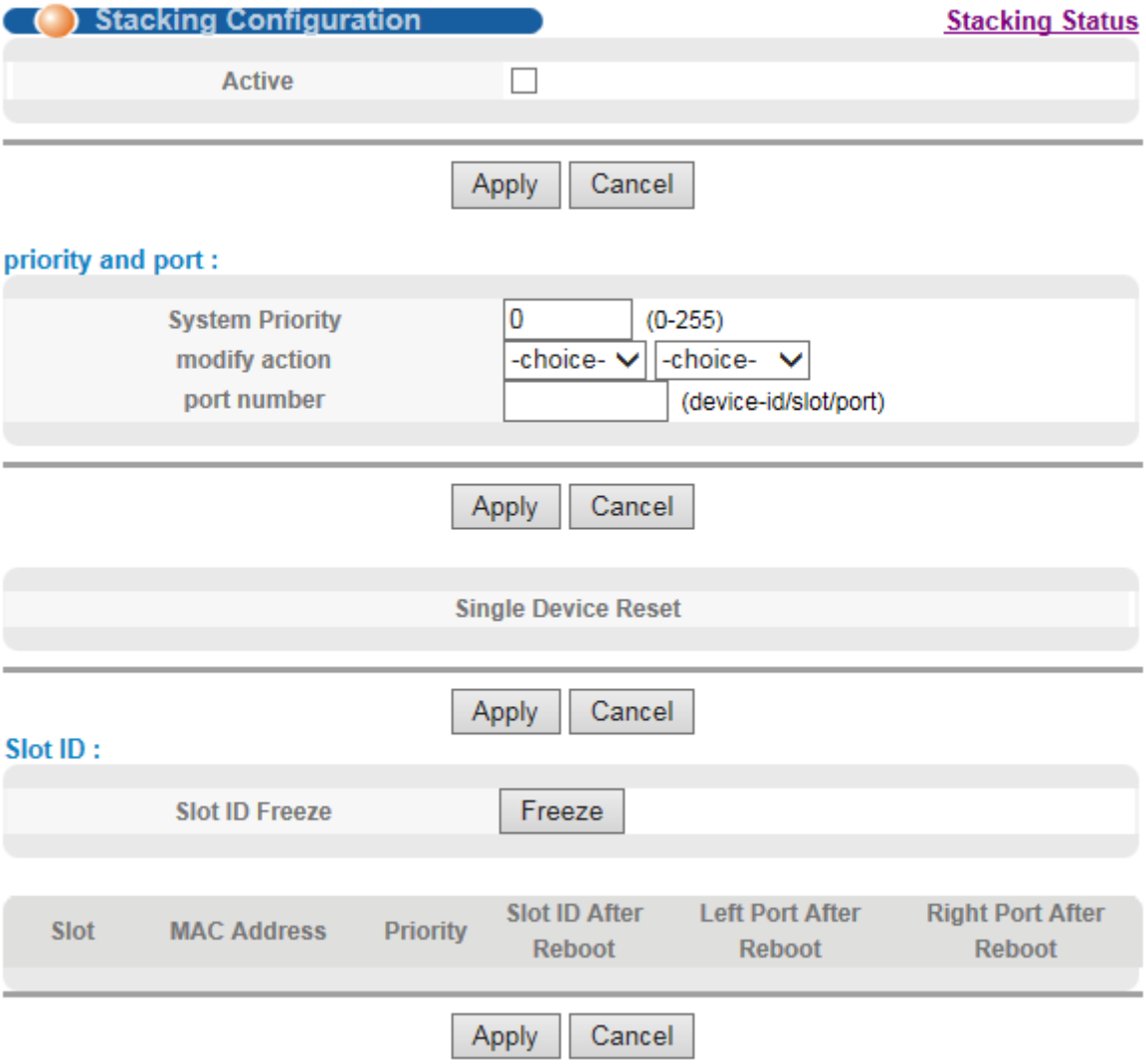
- Low operation and maintenance cost

  Network upgrade does not need to replace existing equipment, just need to add new equipment, multiple equipments to form a logical equipment, reduce maintenance costs.

4.2.8.3 Stacking Configuration

Select **Basic Setting > Stacking > Stacking Configuration** to open stack and set System Priority.

Figure 4-21 Stacking Configuration



Parameter Description

Table 4-8 Stacking Configuration parameter description

Parameter	Description
Active	Select open or close stack.
System Priority	Set system priority, the default is 0.
Slot id Freeze	Freeze slot ID.
Slot id After Reboot	Device number after the device is rebooted.

Instructions

Stacking Configuration

- Device default to stand-alone mode, and to be stacked, you must configure device ID, stack port, and then enable the stacked feature.
- Device priority is optional, which defaults to 0 (lowest priority), and higher priority devices have a greater likelihood of being voted as primary devices. It is generally

necessary to configure the priority of the device where the upstream port is located to a relatively high priority.

- Stacked port LinkDown delayed configuration, which is enabled so that the stacked ports do not immediately age the relevant device members after the occurrence of LinkDown events, but wait for N Hello messages before aging the relevant device members, in order to avoid frequent stack splitting and merging of the stack system due to the instability of the stacked ports. This configuration is turned off by default and is recommended to be turned on.
- Hello datagram timeout configuration, wherein a stacked device member performs heartbeat maintenance with Hello datagram, and when N consecutive Hello datagram no Hello datagram is received from a certain device member, the device member shall be considered to have left the stack and shall be aged.
- A stacked system allows you to reboot a member of a device individually.

Some related configuration only takes effect after restarting the Switch.

4.3 Advanced Application

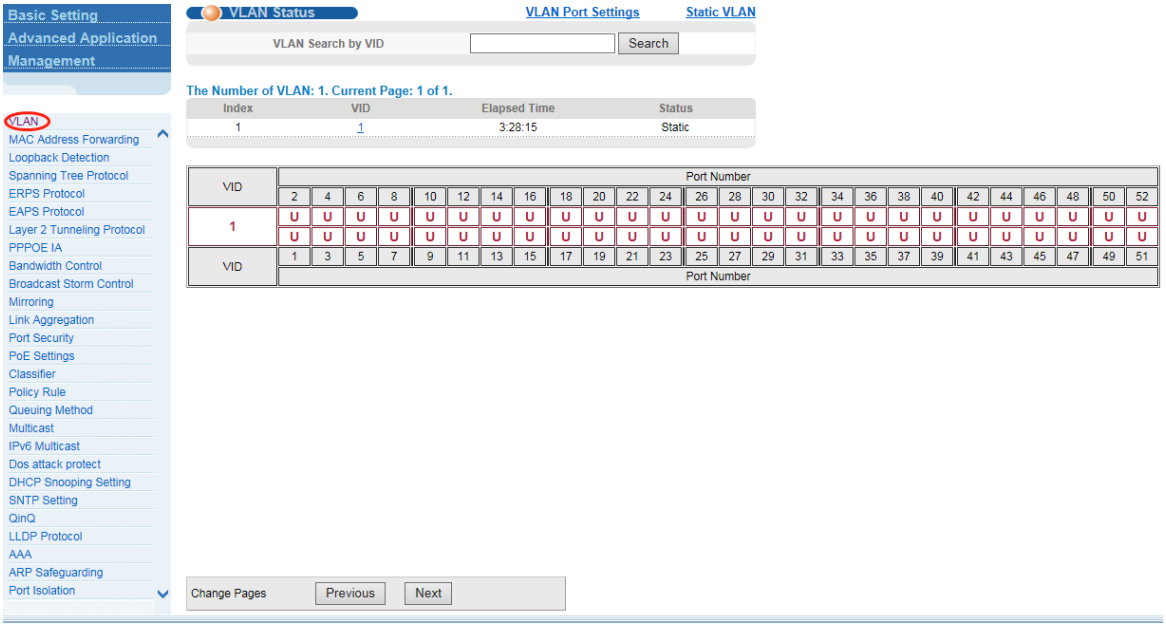
There are "VLAN", "MAC Address Forwarding", "Lookback Detection", "Spanning Tree Protocol", "ERPS Protocol", "EAPS Protocol", "Layer 2 Tunneling Protocol", "PPPOE IA", "Bandwidth Control", "Broadcast Storm Control", "Mirroring", "Link Aggregation", "Port Security", "POE Settings", "Classifier", "Policy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

Figure 4-22 Advanced Application

4.3.2 VLAN

Select Advanced Application >VLAN to configure VLAN.

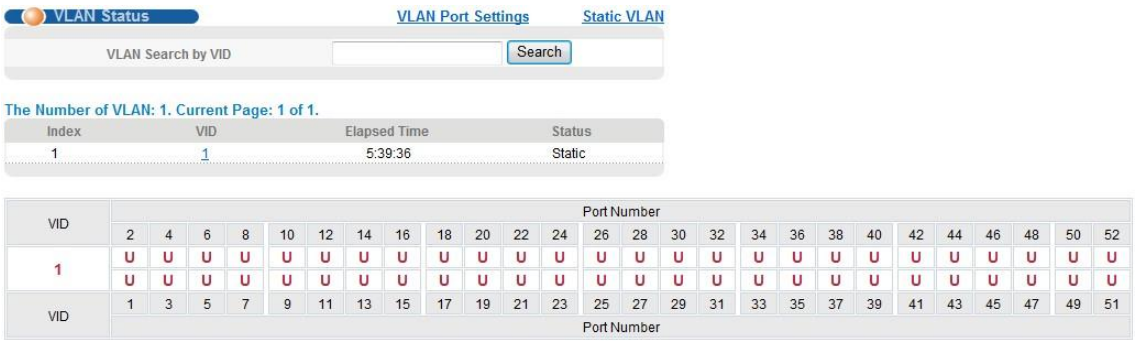
Figure 4-23 VLAN



4.3.2.2 VLAN Status

Select Advanced Application >VLAN>VLAN Status to view VLAN status.

Figure 4-24 VLAN Status(1)



Parameter Description

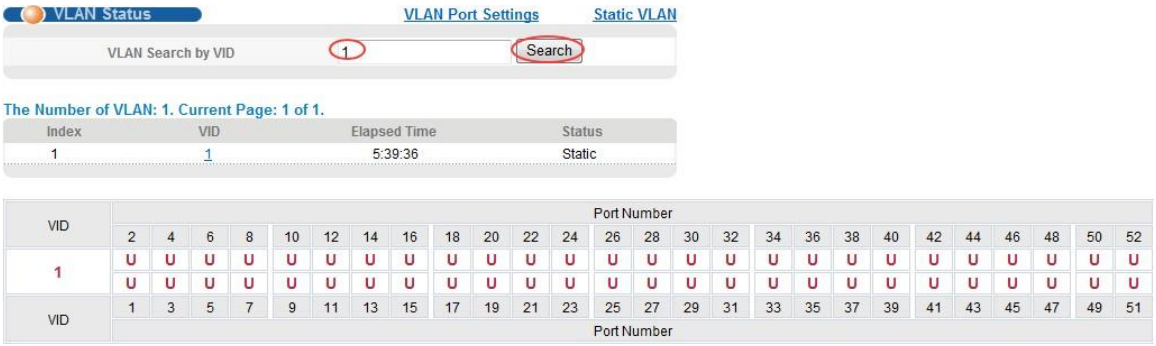
Table 4-9 VLAN Status parameter description

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".

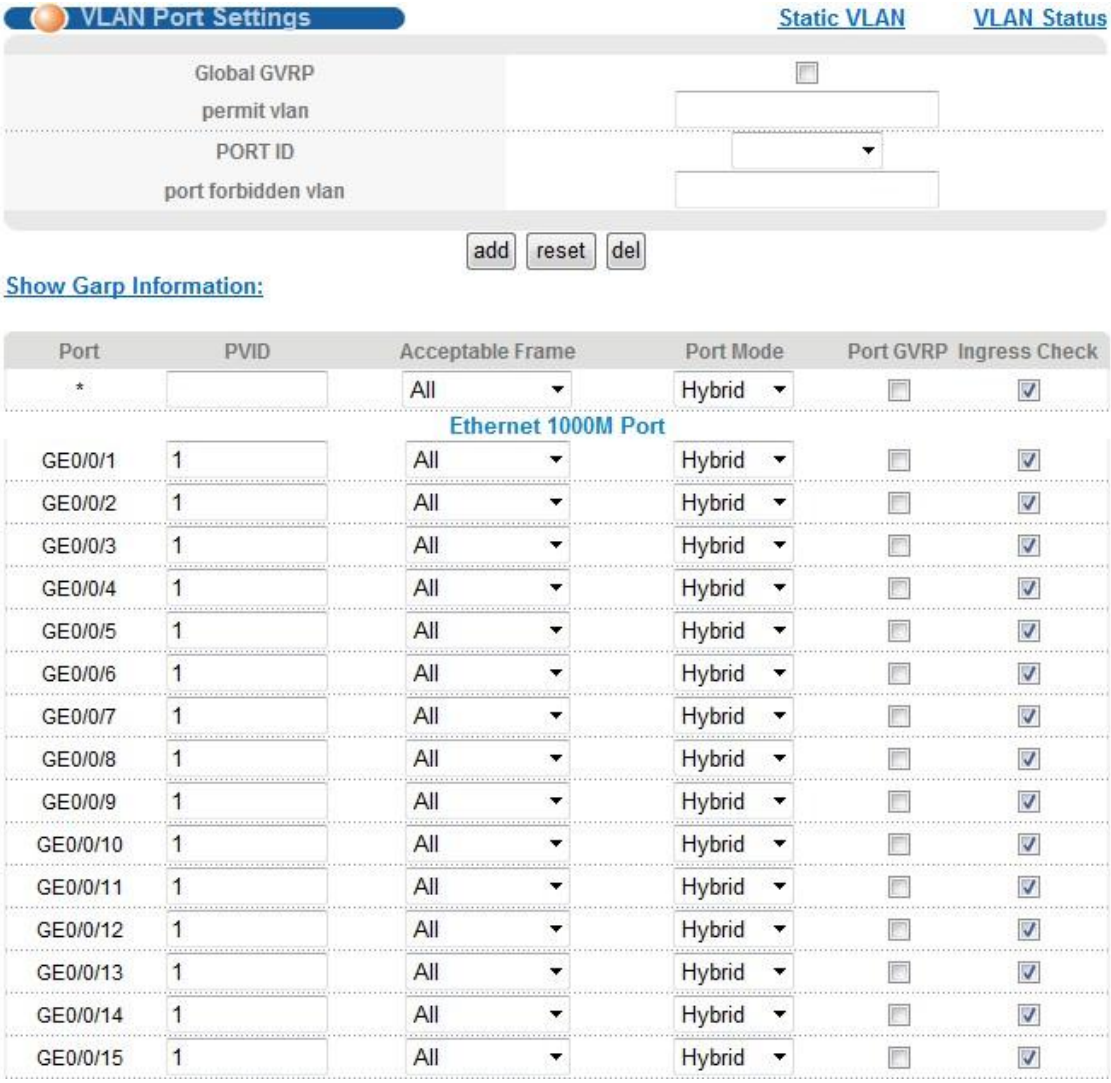
Figure 4-25 VLAN Status(2)



4.3.2.3 VLAN Port Settings

Select Advanced Application >VLAN>VLAN Port Settings to set VLAN port.

Figure 4-26 VLAN Port Settings



Parameter Description

Table 4-10 VLAN Port Settings parameter description

Parameter	Description
PVID	The PVID of the port can be modified. The default port PVID is "1".
Acceptable Frame	Select the following kinds: All, Tagged only, Untagged only.
Port Mode	● 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 filtering function opens.

Instructions

In Access mode, the port can only be a member of a VLAN.

- Hybrid port to packet:

  Receives a packet, judge whether there is 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:

  ✧ Determine the VLAN in this port attributes (disp interface can see the port to which VLAN untag, which VLAN tag).

  ✧ If it is untag stripping VLAN information, send again, if the tag is sent directly.

GVRP (GARP VLAN Registration Protocol) is an application of GARP. It is based on the working mechanism of GARP to maintain VLAN dynamic Registration information that supports GVRP devices and propagate this information to other devices. To agree on VLAN information for all GVRP-enabled devices within the same LAN. The VLAN registrations propagated by GVRP include both static registrations for local manual configuration and dynamic registrations from other switches.

Configuration example

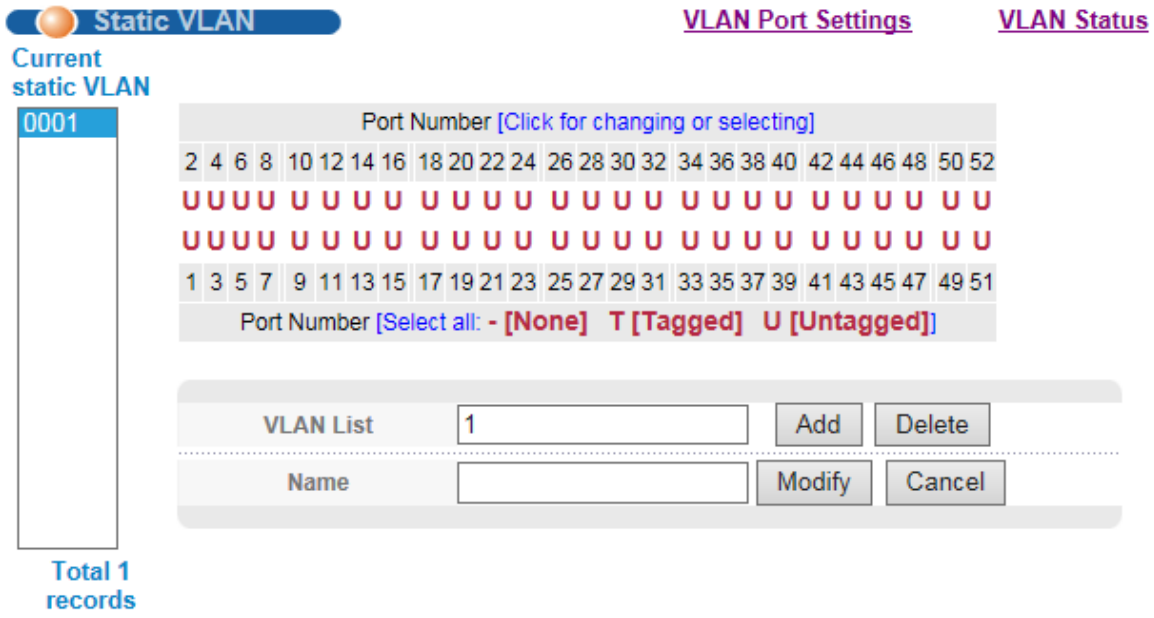
Such as: The PVID of port 1 is set to“1", the frame type is set to “All", the port mode is set to “Hybrid", and the port GVRP is not turned on and the entry inspection function is opened.

Figure 4-27 Configuration example

4.3.2.4 Static VLAN

Select Advanced Application >Static VLAN to configure Static VLAN.

Figure 4-28 Static VLAN



Parameter Description

Table 4-11 Static VLAN parameter description

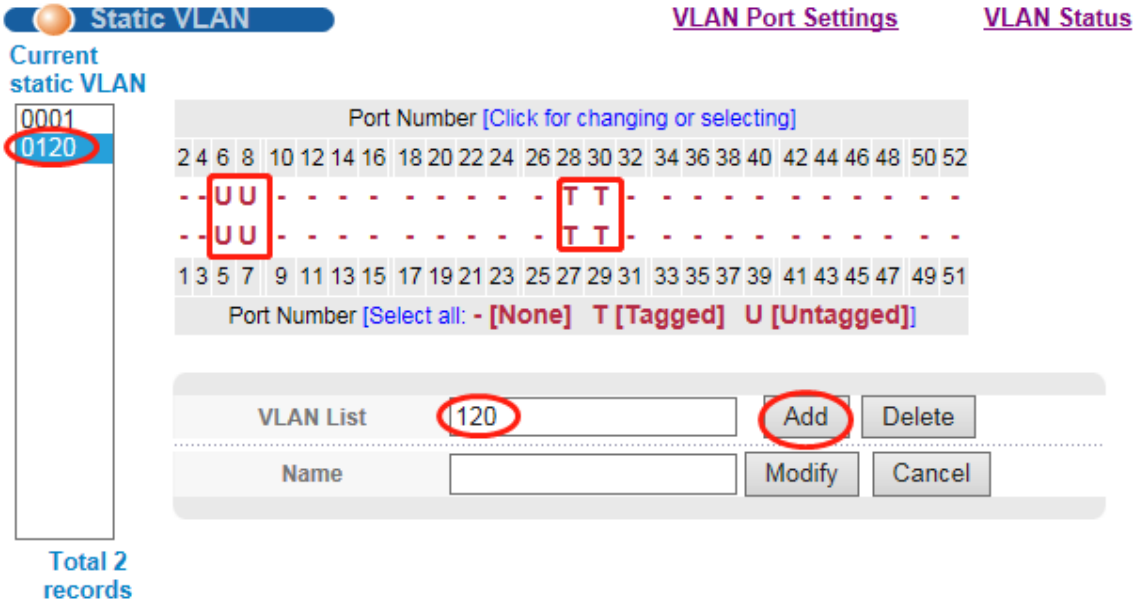
Parameter	Description
VLAN List	VLAN Group ID.
Name	VLAN Group name.

Configuration example

Add and delete VLAN members

Such as: Adding a new VLAN, VLAN Group ID 120 contains non-untag member port 6, 8. Tag member port 11, 12. The user can modify the port member by clicking on the white area below the port number.

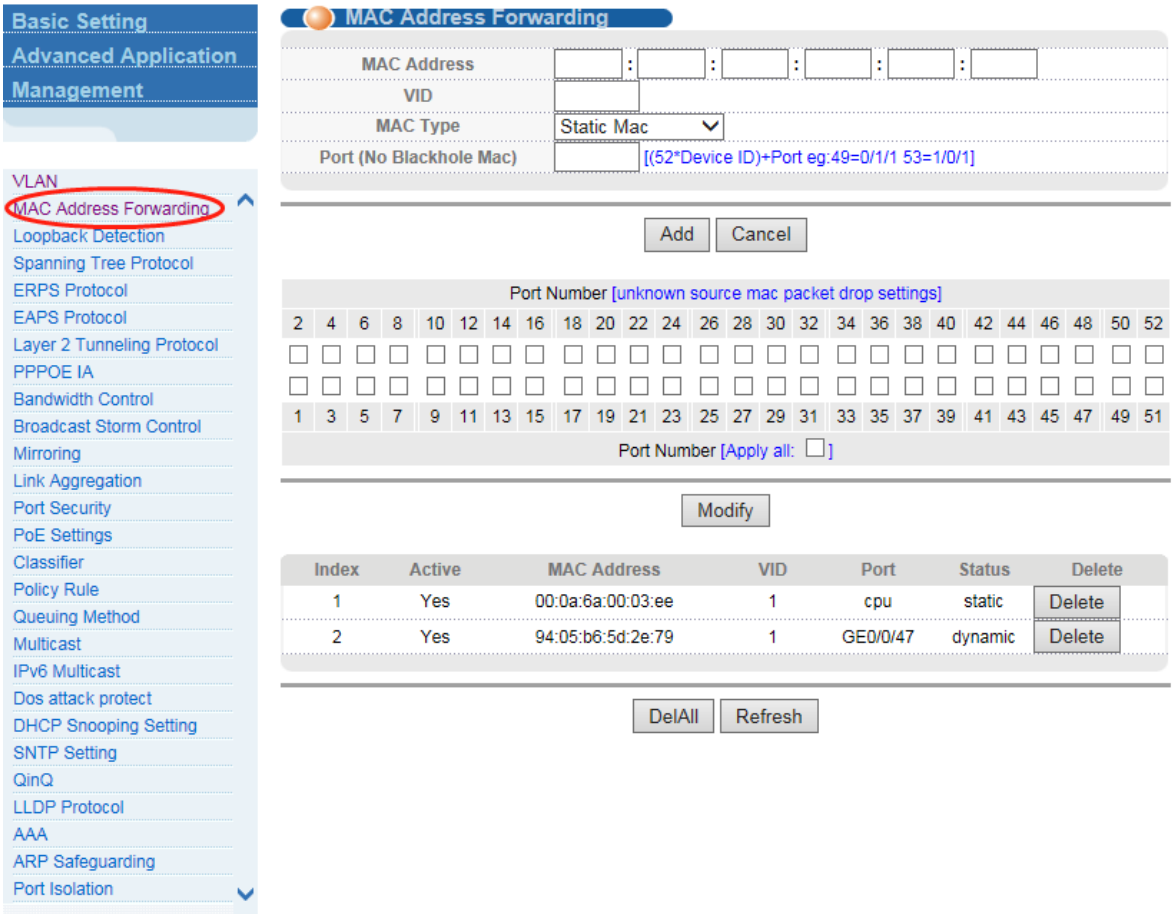
Figure 4-29 Static VLAN Configuration example



4.3.3 MAC Address Forwarding

Select Advanced Application >MAC Address Forwarding to configure MAC Address Forwarding.

Figure 4-30 MAC Address Forwarding



Parameter Description

MAC Type: Static MAC, Dynamic MAC, Blackhole MAC, Permanent MAC

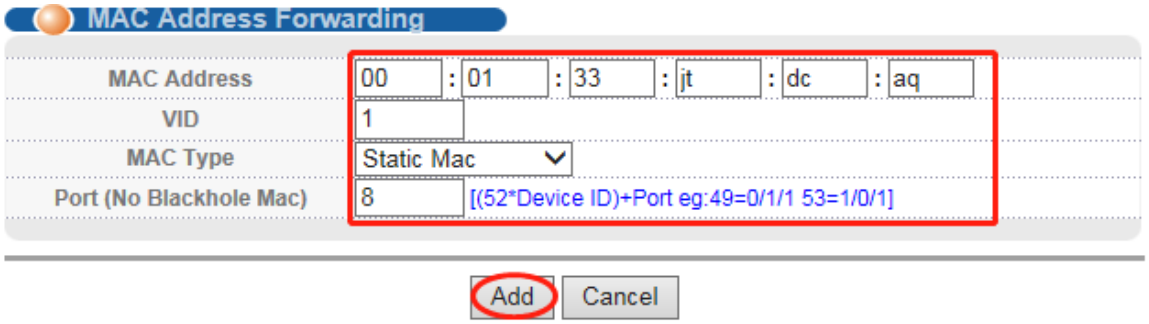
Instructions

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

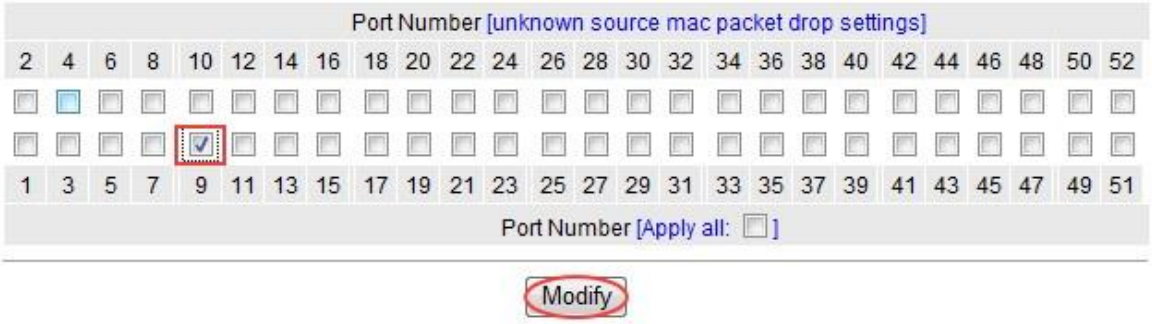
- MAC Address Forwarding

Figure 4-31 MAC Address Forwarding



- Unknown source mac packet drop settings.

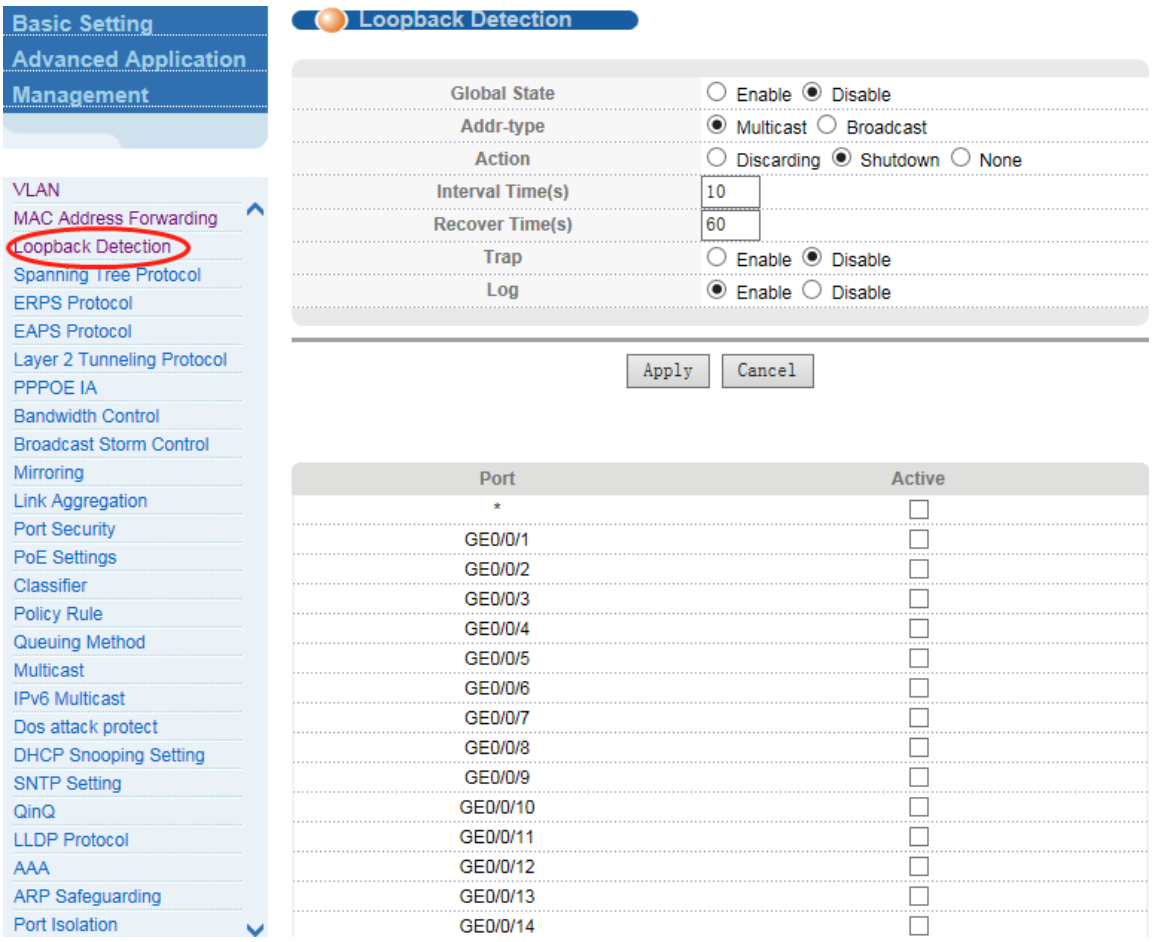
Figure 4-32 Unknown source mac packet drop settings



4.3.4 Loopback Detection

Select Advanced Application >Loopback Detection to configure Loopback Detection.

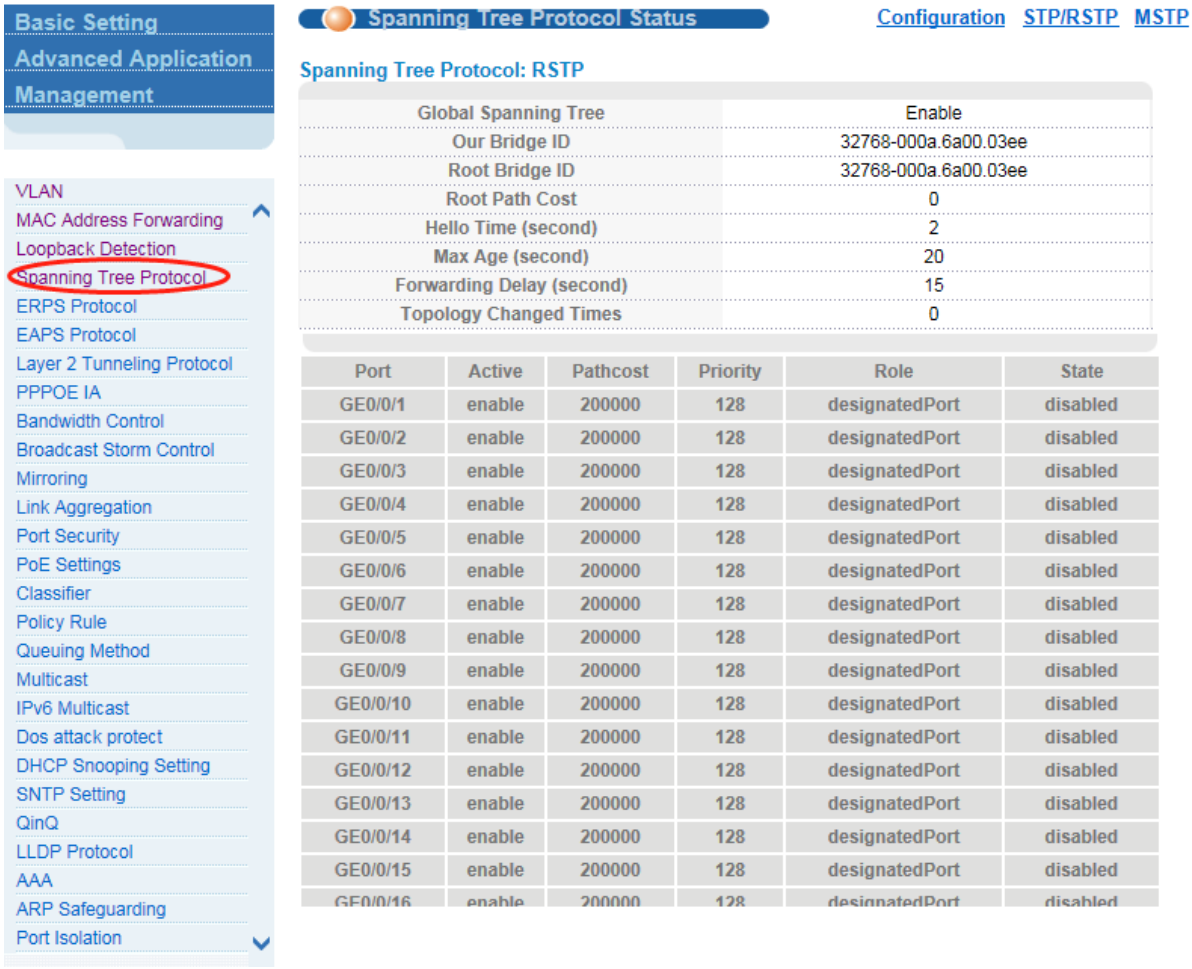
Figure 4-33 Loopback Detection



4.3.5 Spanning Tree Protocol

Select Advanced Application >Spanning Tree Protocol to configure spanning tree protocol.

Figure 4-34 Spanning tree protocol



4.3.5.2 Spanning Tree Protocol Status

Select **Advanced Application > Spanning Tree Protocol > Spanning Tree Protocol Status** to view spanning tree protocol status.

Figure 4-35 Spanning Tree Protocol Status

Parameter Description

Table 4-12 Spanning Tree Protocol Status 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.

Instructions

In the spanning tree, there are 5 types of port states:

- Disabled

  The port does not participate in frame forwarding, MAC address learning, and spanning tree operations. When the port is disabled by management means, the port state becomes the Disabled state. When the port is in the Disabled state, the port can be enabled by the management means, and the port state becomes the Blocking state.

- Blocking

  The port does not forward frames or learn MAC addresses, but receives BPDUs and participates in spanning tree operations. After the bridge is initialized, the port enters the Blocking state, or when the port is in the Disabled state and the port is enabled through management means, the port enters the Blocking state.

  Through the calculation of the spanning tree, the port can enter the Blocking state from the Listening, Learning, or Forwarding state.

- Listening

  The port does not forward frames and does not learn MAC addresses. However, when receiving BPDUs and participating in spanning tree operations, the received BPDUs need to be submitted for transmission. When the spanning tree determines that this port needs to participate in frame forwarding, the port changes from the blocking state to the listening state.

- Learning

  The port does not forward frames, but it learns MAC addresses and receives BPDUs and participates in spanning tree operations. The received BPDUs need to be submitted for transmission. When the protocol timer expires, the port changes from the Listening state to the Learning state.

- Forwarding

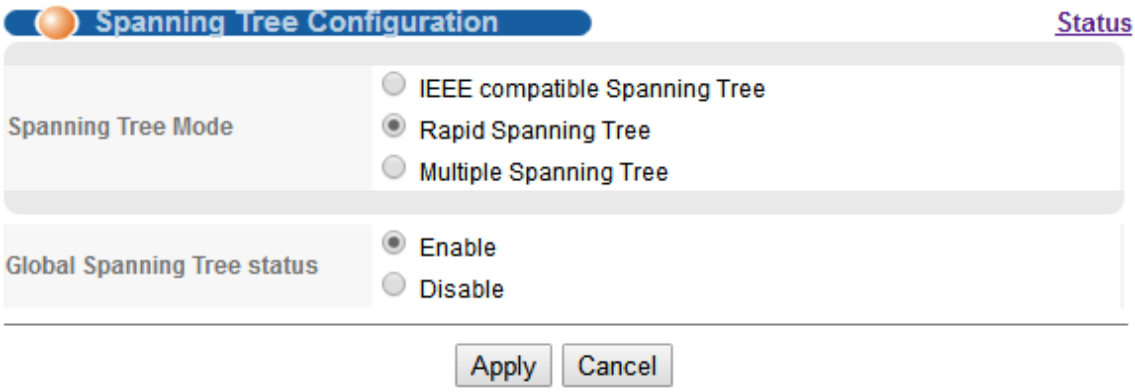
  The port forwards frames, learns the MAC address and receives BPDUs and participates in spanning tree operations. The received BPDUs need to be submitted for transmission. When the protocol timer expires, the port state changes from the Learning state to the Forwarding state.

  In spanning tree, only when the port of the bridge belongs to the root port or designated port, can it participate in the frame forwarding, and the other ports are in the Blocking state.

4.3.5.3 Spanning Tree Configuration

Select **Advanced Application > Spanning Tree Protocol > Spanning Tree Configuration** to configure spanning tree.

Figure 4-36 Spanning Tree Configuration



Parameter Description

Table 4-13 Spanning Tree Configuration 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.

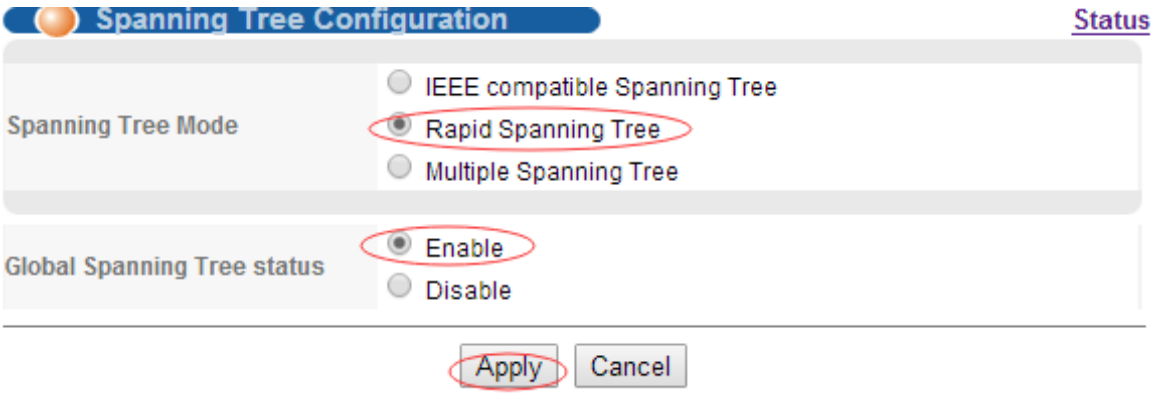
Instructions

After spanning tree is started globally, by default all ports will participate in the calculation of spanning tree topology. If the administrator wants some ports not to participate in the calculation of spanning tree, they can also enter the configuration mode of the specified port and use no spanning-tree to disable the spanning tree function of the port.

Configuration example

Such as: Spanning Tree Mode as “Rapid Spanning Tree", open Global Spanning.

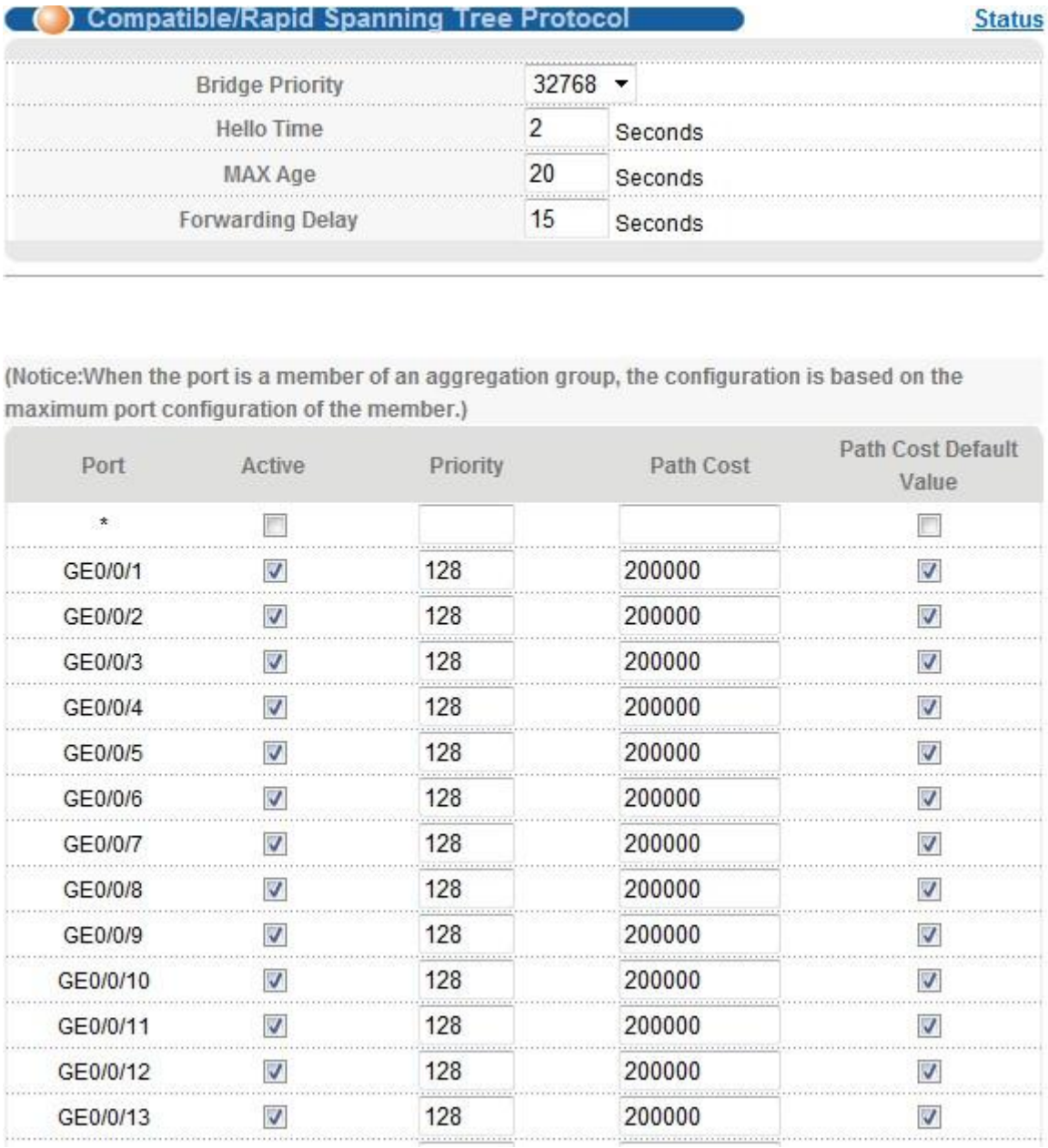
Figure 4-37 Global Spanning



4.3.5.4 Compatible/Rapid Spanning Tree Protocol

Select **Advanced Application > Spanning Tree Protocol > Compatible/Rapid Spanning Tree Protocol** to configure Compatible/Rapid Spanning Tree Protocol.

Figure 4-38 Compatible/Rapid Spanning Tree Protocol



Parameter Description

Table 4-14 Compatible/Rapid Spanning Tree Protocol parameter description

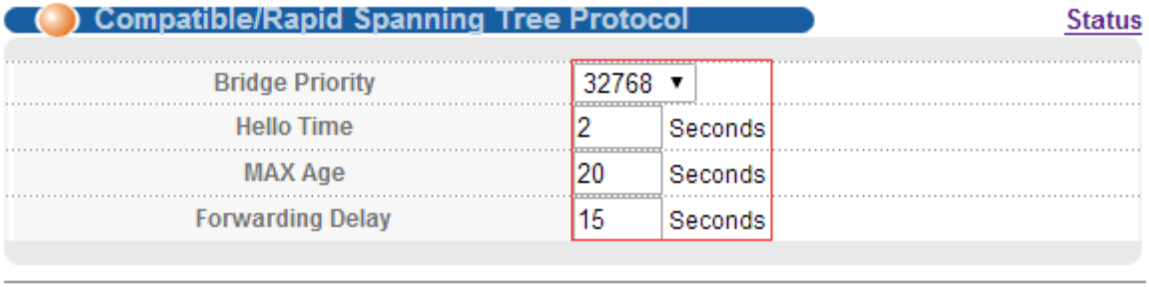
Parameter	Description
Bridge Priority	Set bridge priority, the default instance bridge priority for 32768.
Hello Time	Switches sends bpdu in packet interval.

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

- Configure the bridge priority as 32768, the Hello Time is 2 seconds, the MAX Age is 20 seconds, and the Forwarding Delay is 15 seconds.

Figure 4-39 Configuration example(1)



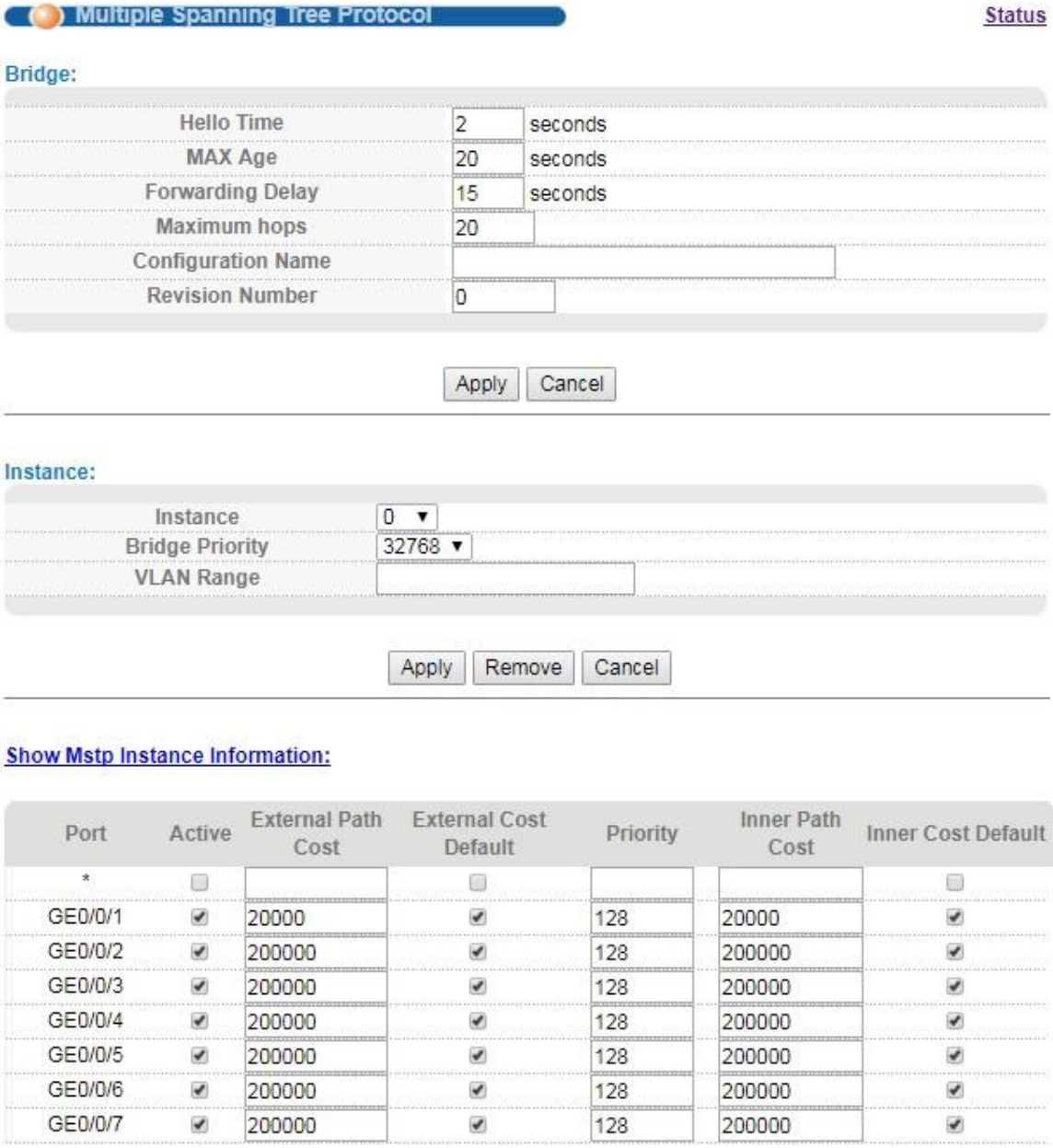
- The priority of port 48 is 64, and the path cost is 200000.

Figure 4-40 Configuration example(2)

4.3.5.5 Multiple Spanning Tree Protocol

Select **Advanced Application > Spanning Tree Protocol > Multiple Spanning Tree Protocol** to configure Multiple Spanning Tree Protocol.

Figure 4-41 Multiple Spanning Tree Protocol



Parameter Description

Table 4-15 Multiple Spanning Tree Protocol parameter description

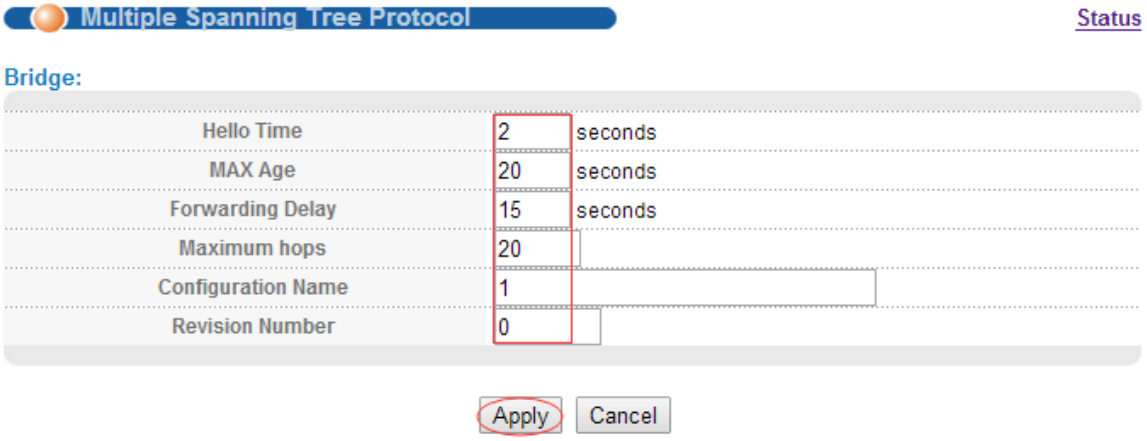
Parameter	Description
Hello Time	Switches sends bpdu in packet interval.
Max age	Ports are not yet received a message in the time, will initiate topology changes.
Forwarding Delay	The state of the port switch time.
Maximum Hops	Set the maximum number of hops that BPDUs can support in the spanning tree.
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.

Configuration example

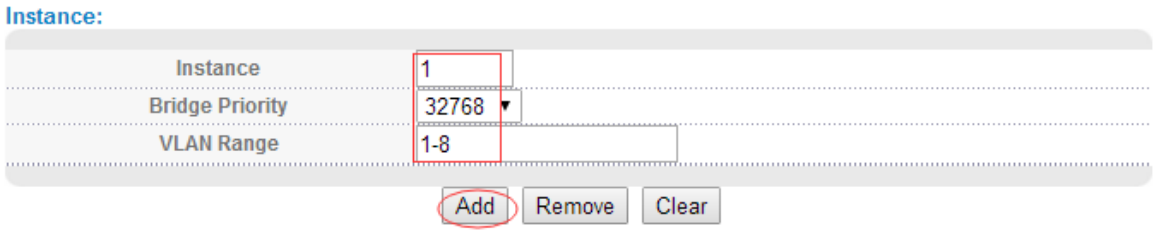
- Bridge

Figure 4-42 Configuration example(1)



- Instance

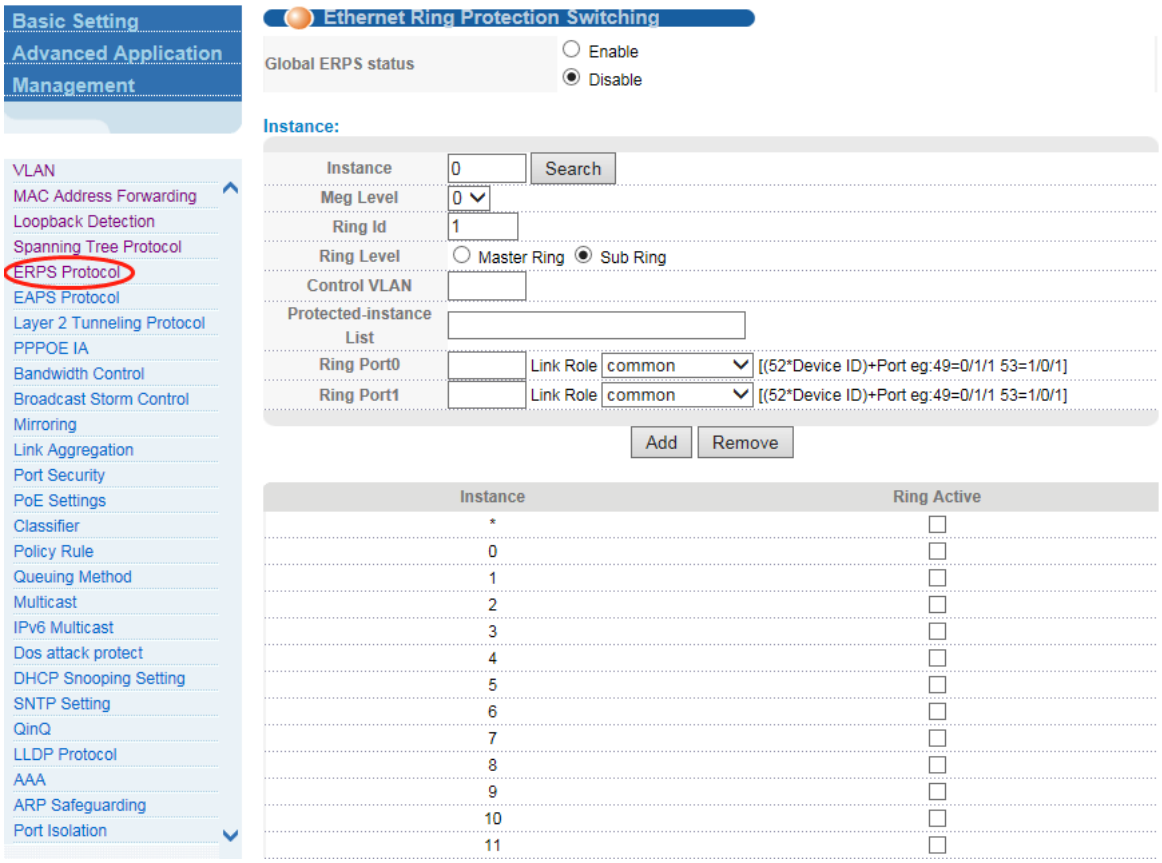
Figure 4-43 Configuration example(1)



4.3.6 ERPS Protocol

Select **Advanced Application > ERPS Protocol** to configure ERPS protocol.

Figure 4-44 ERPS protocol



Parameter Description

Table 4-16 ERPS protocol parameter description

Parameter	Description
Global ERPS status	Select open or close ERPS.
Instance	The range of 0-15, active instance.
Meg level	The range of 0-7.
Ring Id	The range of 1-239.
Ring Level	Main Ring and Sub Ring.
Control VLAN	You must configure the VLAN before configuring the ERRP ring.
Protected-instance List	Application of MST instance.
Ring port1	Configurable ports are common, owner, neighbor, next-neighbor.
Ring port2	Configurable ports are common, owner, neighbor, next-neighbor.

Instructions

ERPS is an Ethernet multi-ring protection technology. It can prevent the broadcast storm caused by the data loop when the Ethernet ring is complete, and can quickly restore the

communication path between each node on the ring network when a link on the Ethernet ring is disconnected, with a high convergence speed.

Control VLAN and data VLAN are relative:

- Control VLAN

  The control VLAN is used to transfer ERRP protocol packets. Each ERRP domain has two control VLANs: the main control VLAN and the sub-control VLAN. The control VLAN of the main ring is called the main control VLAN, and the control VLAN of the sub-ring is called the sub-control VLAN. Only the main control VLAN needs to be specified during configuration, and the system will automatically use the VLAN with a VLAN ID value greater than 1 as the sub-control VLAN.

  Only ports connected to the Ethernet ring (that is, ERRP ports) on the device belong to the control VLAN, and other ports cannot be added to the control VLAN. The ERRP port of the main ring must belong to both the main control VLAN and the sub-control VLAN; the ERRP port of the sub-ring only belongs to the sub-control VLAN.

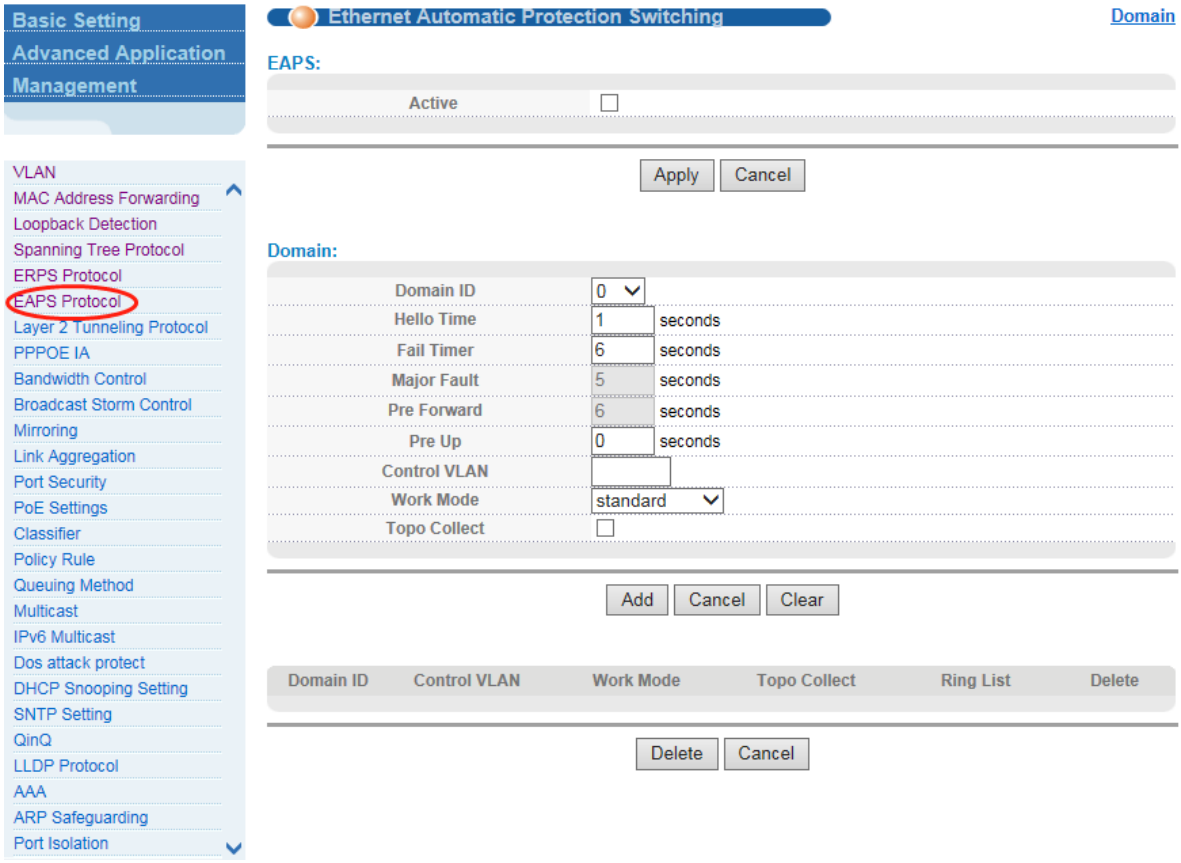
- Data VLAN

  In contrast to the control VLAN, the data VLAN is used to transmit data packets. The data VLAN can contain both ERRP ports and non-ERRP ports.

4.3.7 EAPS Protocol

Select **Advanced Application > EAPS Protocol** to configure EAPS protocol.

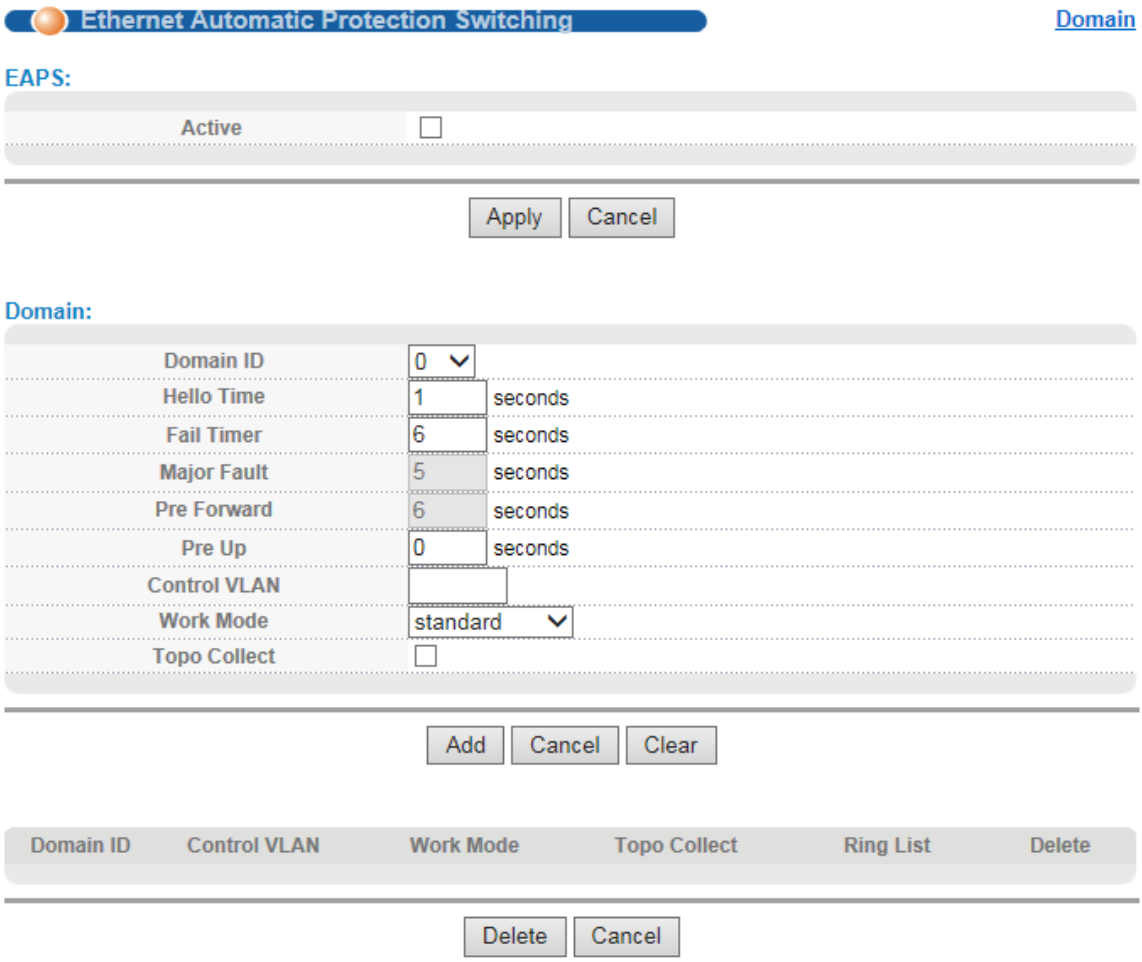
Figure 4-45 EAPS protocol



4.3.7.2 Ethernet Automatic Protection Switching

Select **Advanced Application > EAPS Protocol > Ethernet Automatic Protection Switching** to configure Ethernet automatic protection switching.

Figure 4-46 Ethernet Automatic Protection Switching



Parameter Description

Table 4-17 Ethernet Automatic Protection Switching Parameter Description

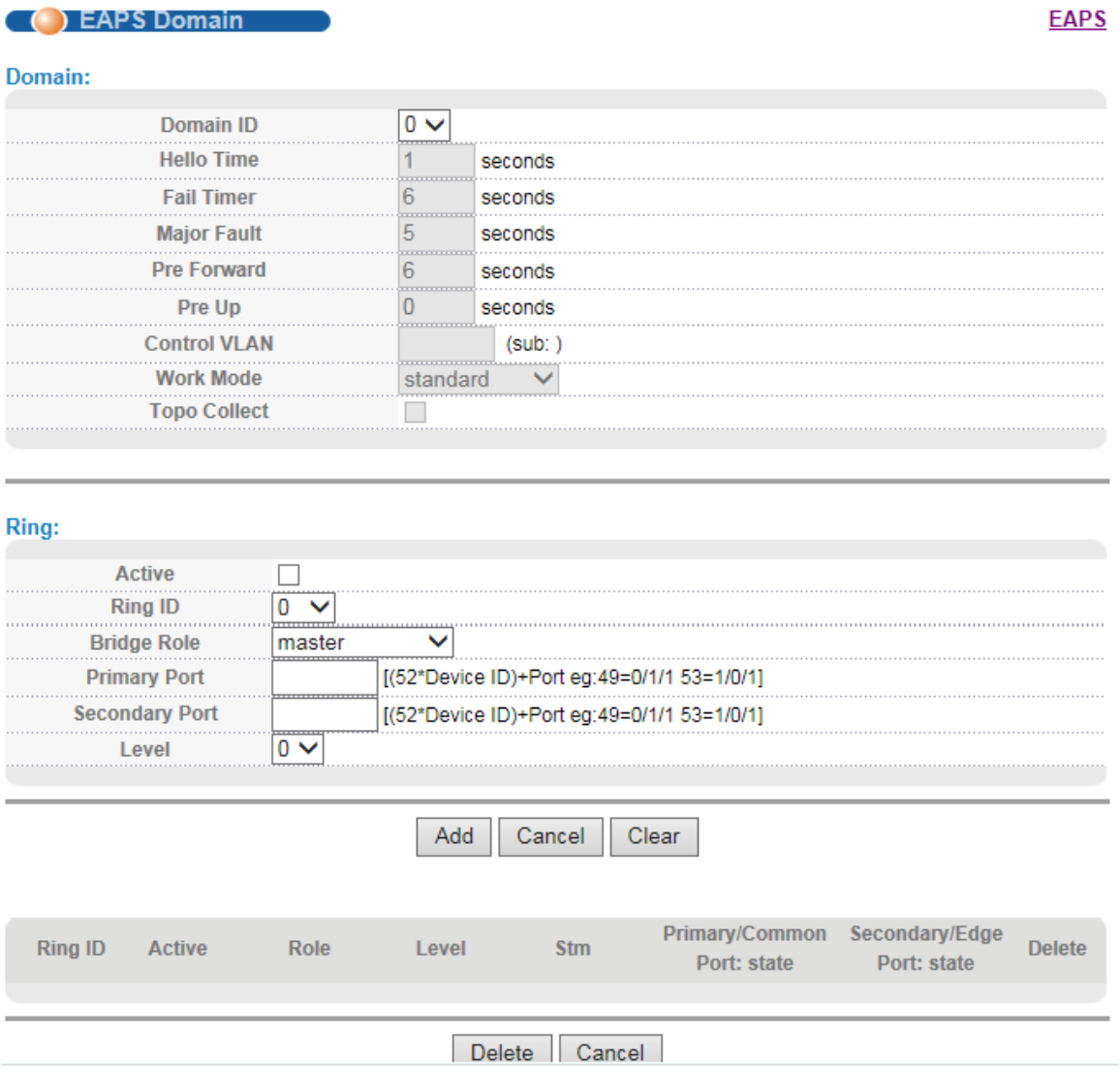
Parameter	Description
Active	Select open or close EAPS
Hello time	Switches sends bpdu in packet interval
Fail Timer	Configure the information timeout
Major Fault	The Major Fault timer will be automatically updated by the system
Pre Forward	The Pre forward timer will be automatically updated by the system
Pre Up	Loop recovery wait time
Domain ID	You need to specify the Domain ID when creating the EAPS Domain
Control VLAN	You must configure the VLAN before configuring the EAPS Ring

Work mode	Such as standard and eips-subring
Topo Collect	Select open or close Topo Collect

4.3.7.3 EAPS Domain

Select **Advanced Application > EAPS Protocol > EAPS Domain** to configure EAPS Domain.

Figure 4-47 EAPS Domain



Parameter Description

Table 4-18 EAPS Domain Parameter Description

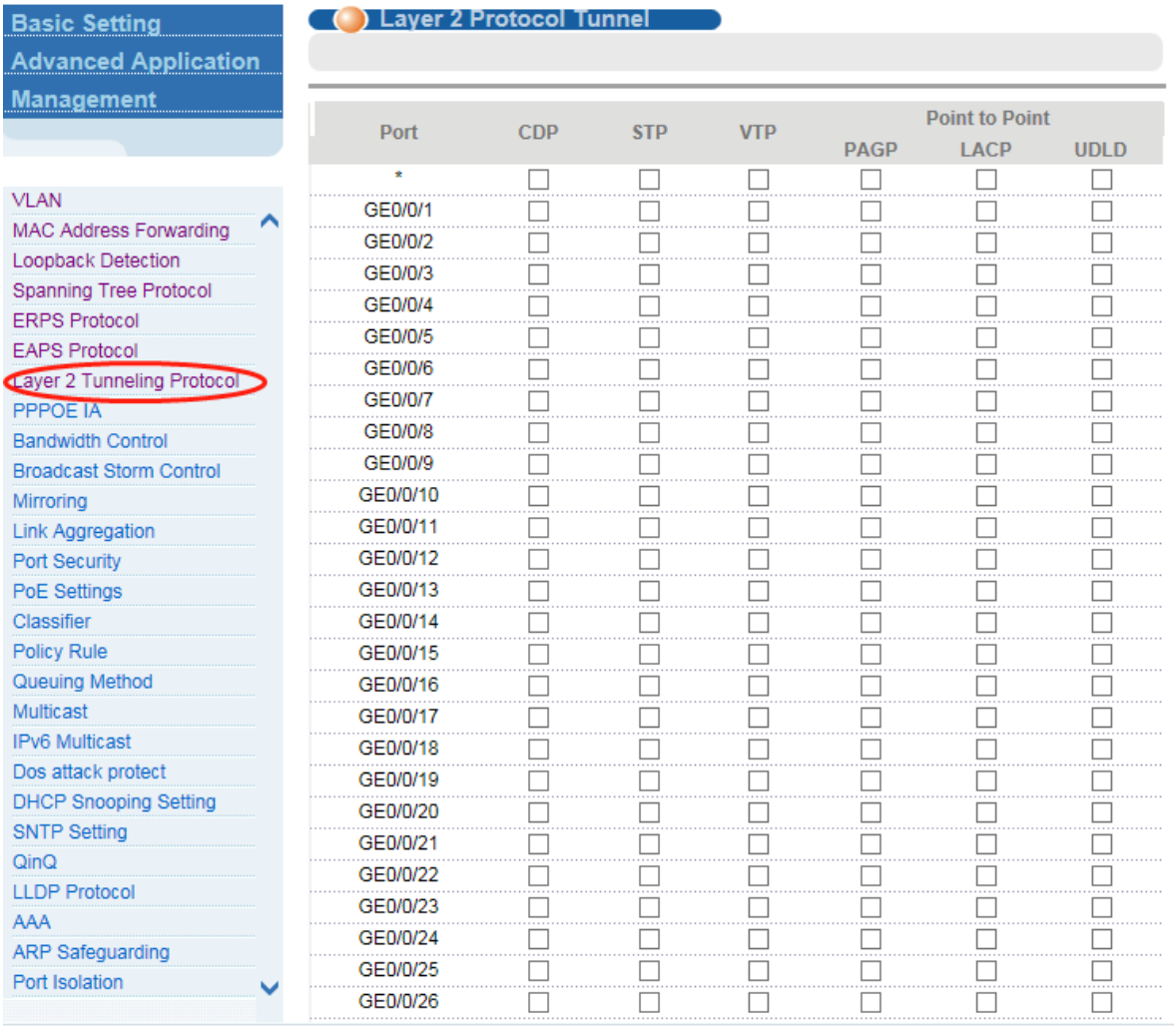
Parameter	Description
Domain ID	Select Domain ID
Control VLAN	You must configure the VLAN before configuring the EAPS Ring
Work mode	Such as standard, and eips-subring
Topo Collect	Select open or close Topo Collect

Active	Select open or close Ring
Ring ID	Select ring ID
Query Solicit	Select open or close Query Solicit
Bridge Role	Bridge Role: main, transit, edge, assistant-edge
Level	Level: 0, 1

4.3.8 Layer 2 Tunneling Protocol

Select **Advanced Application > Layer 2 Tunneling Protocol** to configure the specified protocol message that enters the port to perform a tunnel operation.

Figure 4-48 EAPS protocol



Instructions

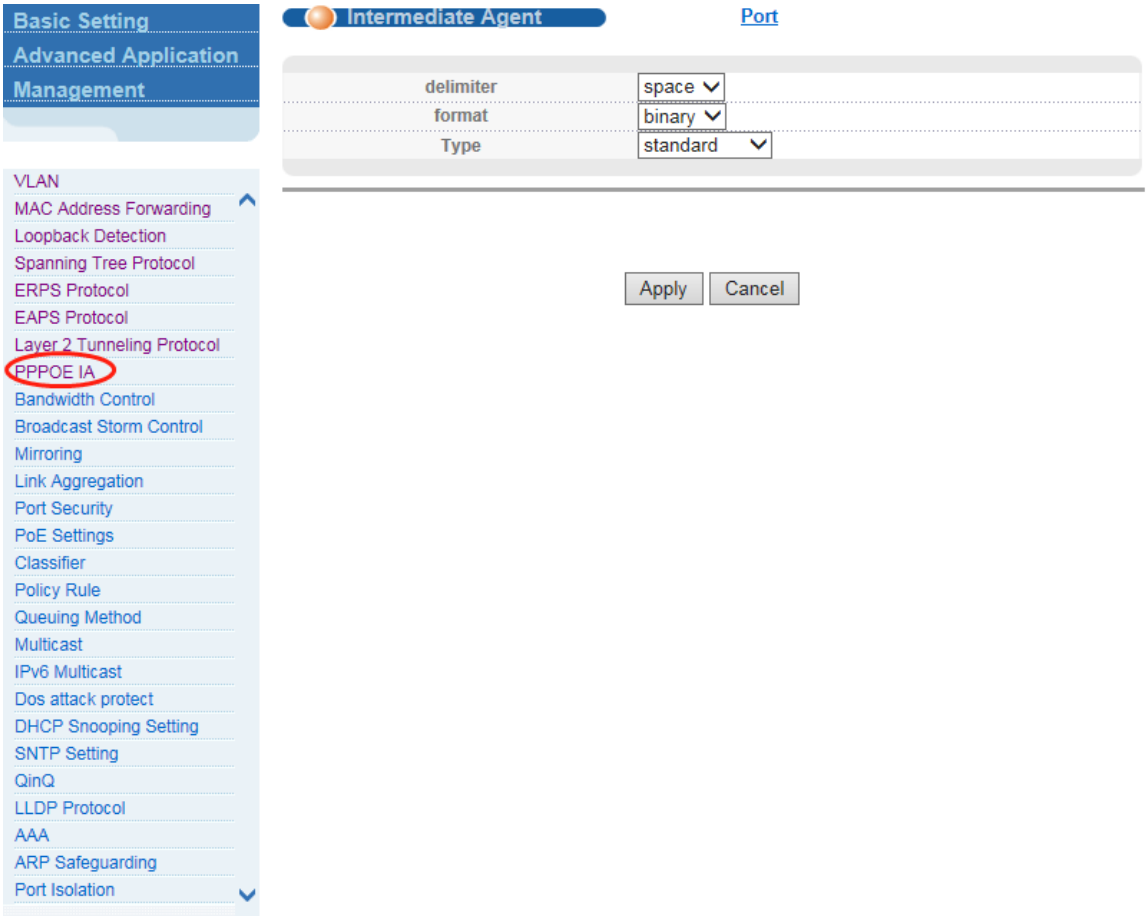
In a VPN network, certain protocol packets received at the edge of the service-provider network need to be encapsulated in a specific format. The internal device of the SP network can recognize this encapsulation and ensure that the packet penetrates the SP network unchanged. The other side of the SP network will decapsulate and restore the message, so that the peer entities connected to the edge of the SP network can communicate normally.

Support 6 types of PDU packets: cdp, lacp, pagp, stp, udld, vtp. When the function is used, it must be combined with Qinq: receive the standard PDU protocol message from the customer, re-encapsulate it into a tunnel message and transfer it from uplink; receive the encapsulated PDU message from uplink and convert it into a standard PDU protocol message After transferring from customer.

4.3.9 PPPOE IA

Select **Advanced Application >PPPOE IA** to configure PPPOE IA.

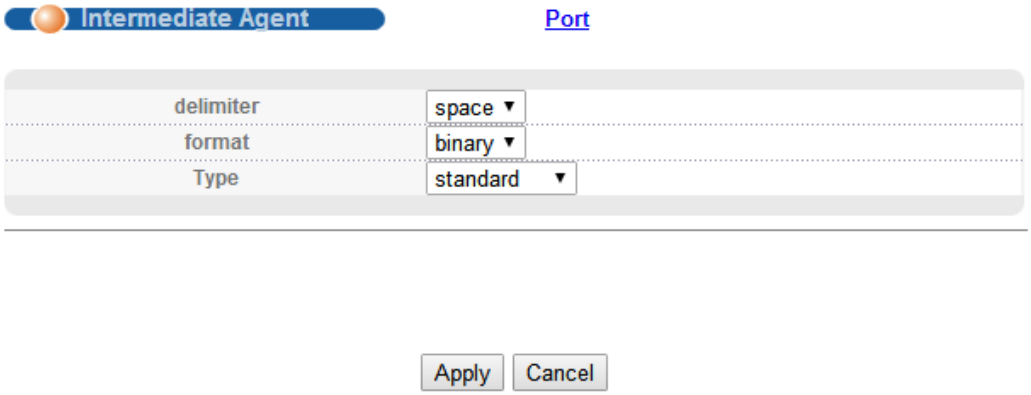
Figure 4-49 PPPOE IA.



4.3.9.2 Intermediate Agent

Select **Advanced Application > PPPOE IA > Intermediate Agent** to configure Intermediate Agent.

Figure 4-50 Intermediate Agent



Parameter Description

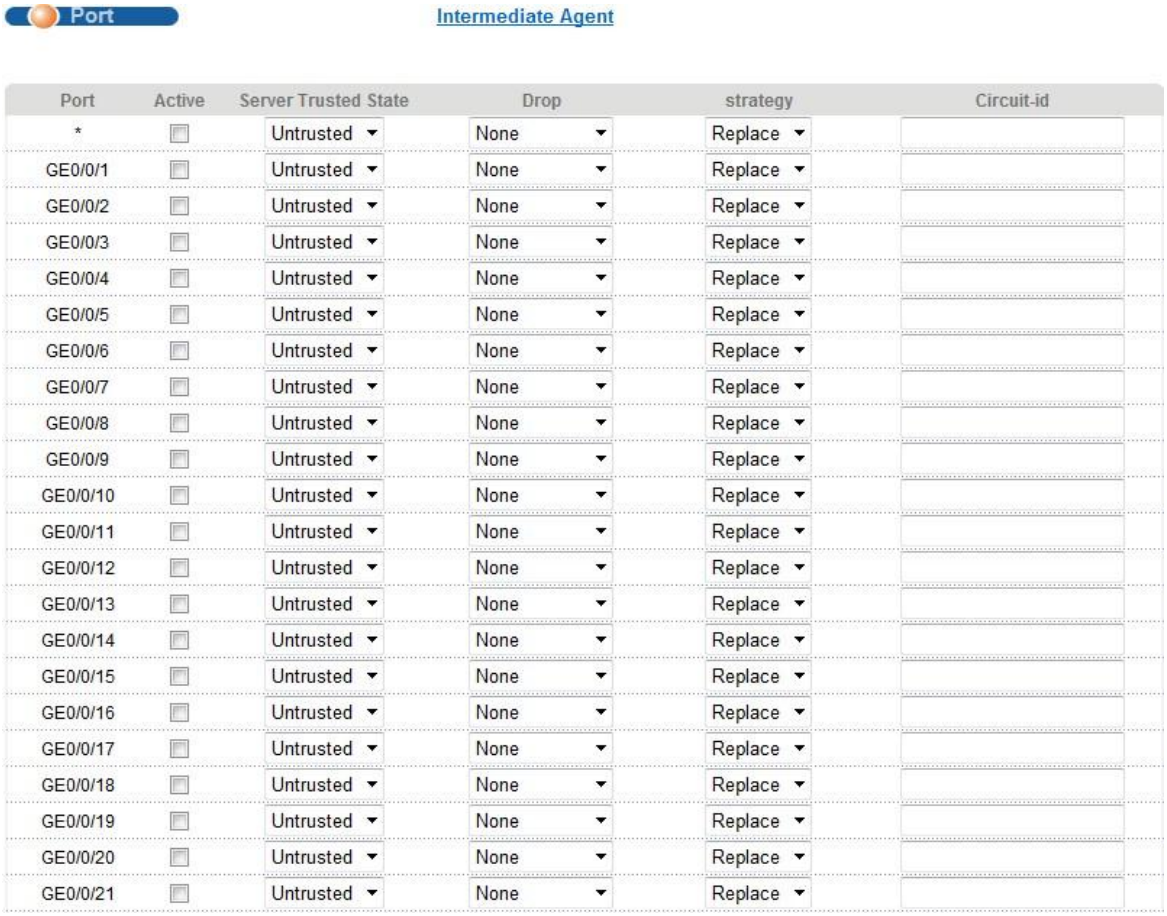
Table 4-19 Intermediate Agent parameter description

Parameter	Description
delimiter	Configure delimiter, choose “space",“:",“.",“#",“/".
format	Configure format, choose binary, ascii.
type	Configure the message type, including standard, and self-defined.

4.3.9.3 Port

Select **Advanced Application > Spanning Tree Protocol > Port** to configure Intermediate Agent.

Figure 4-51 Port



Parameter Description

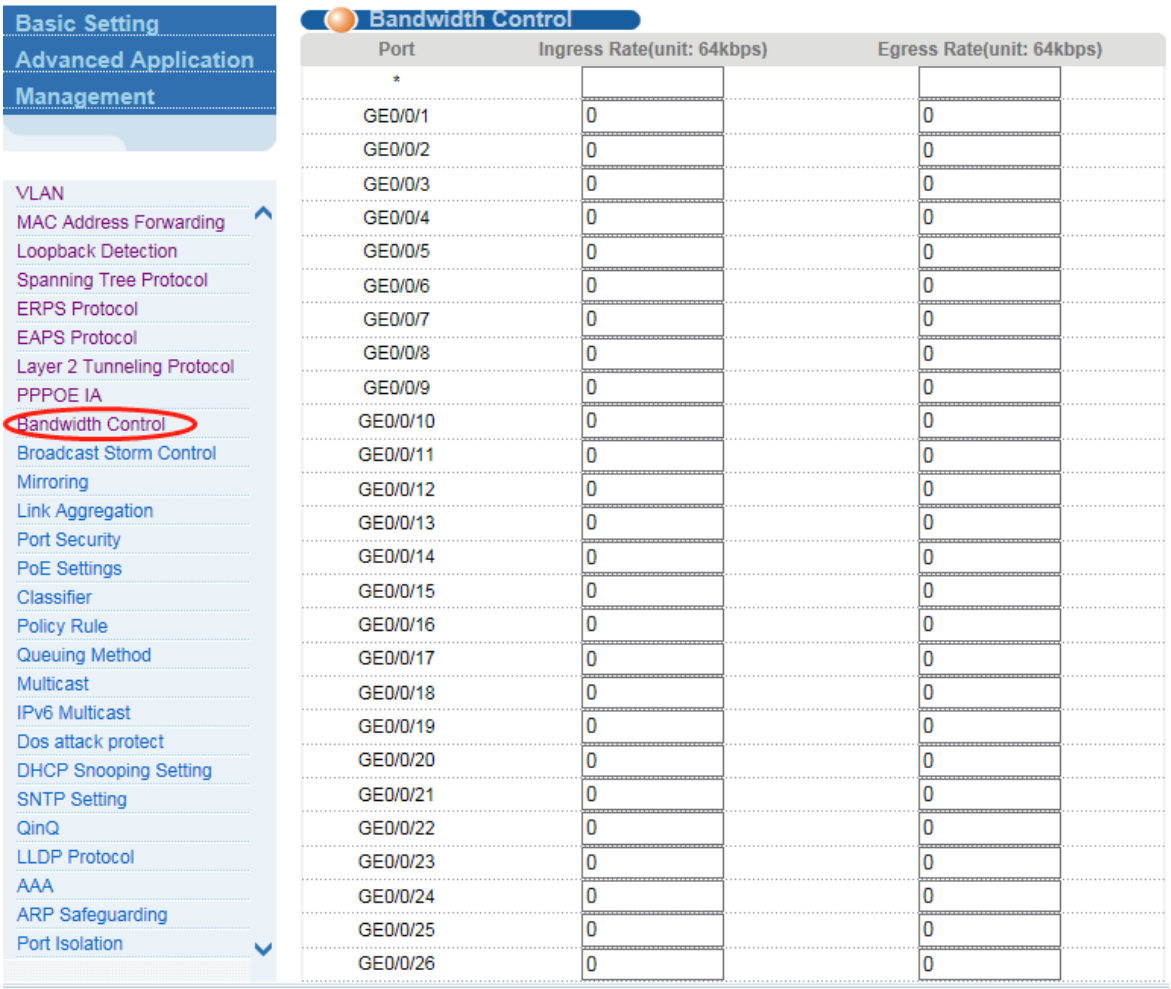
Table 4-20 Port parameter description

Parameter	Description
active	Select open or close port PPPOE IA.
Server Trusted State	Configure the upstream port to be Trusted or Untrusted.
Drop	Configure the pppoe padi/pado packets received by the port.
Strategy	Select Drop, Keep, Replace.

4.3.10 Bandwidth Control

Select **Advanced Application > Bandwidth Control** to configure Bandwidth Control.

Figure 4-52 Bandwidth Control



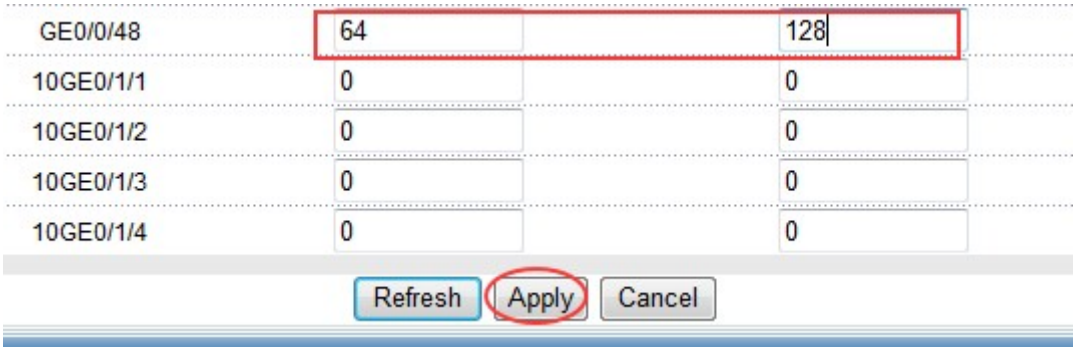
Instructions

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

Such as: Configure port-24 Ingress Rate is 64kbps, Egress Rate is 128kbps.

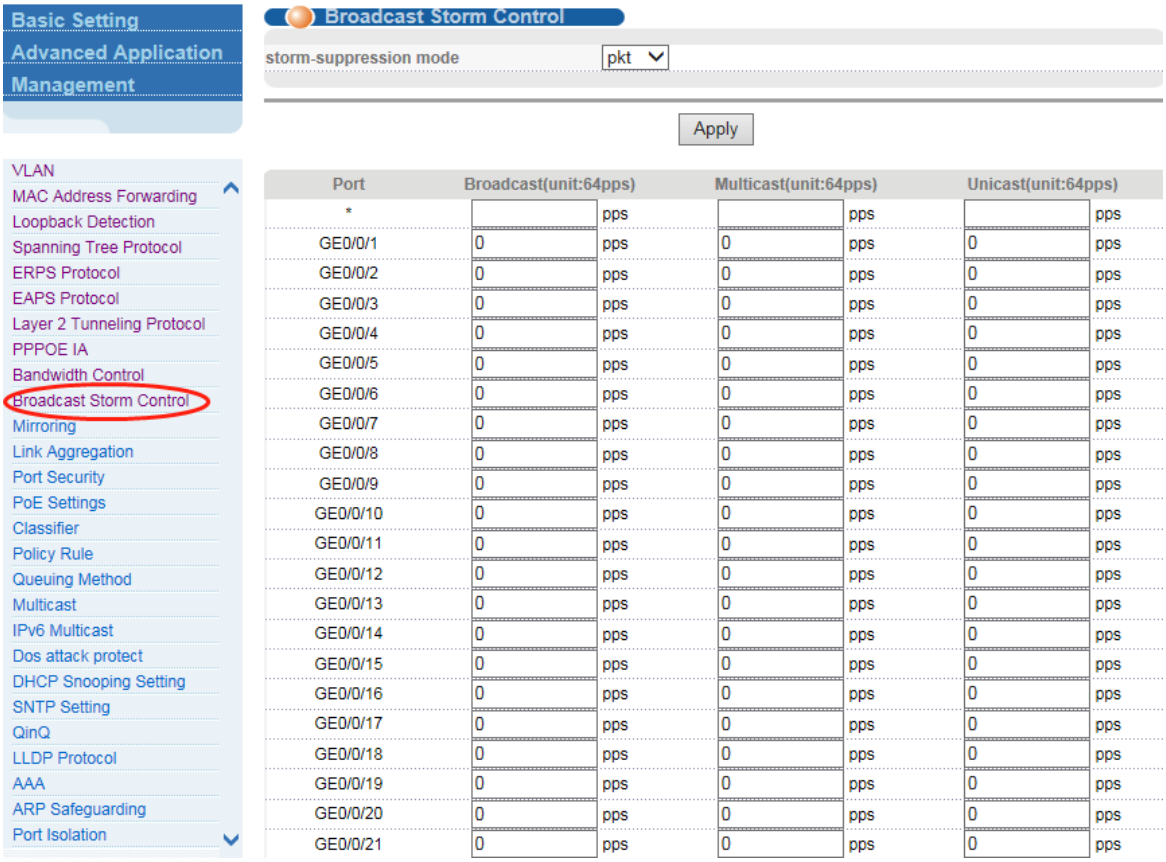
Figure 4-53 Configuration example



4.3.11 Broadcast Storm Control

Select **Advanced Application > Broadcast Storm Control** to configure Broadcast Storm Control.

Figure 4-54 Broadcast Storm Control



Parameter Description

Table 4-21 Broadcast Storm Control 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).

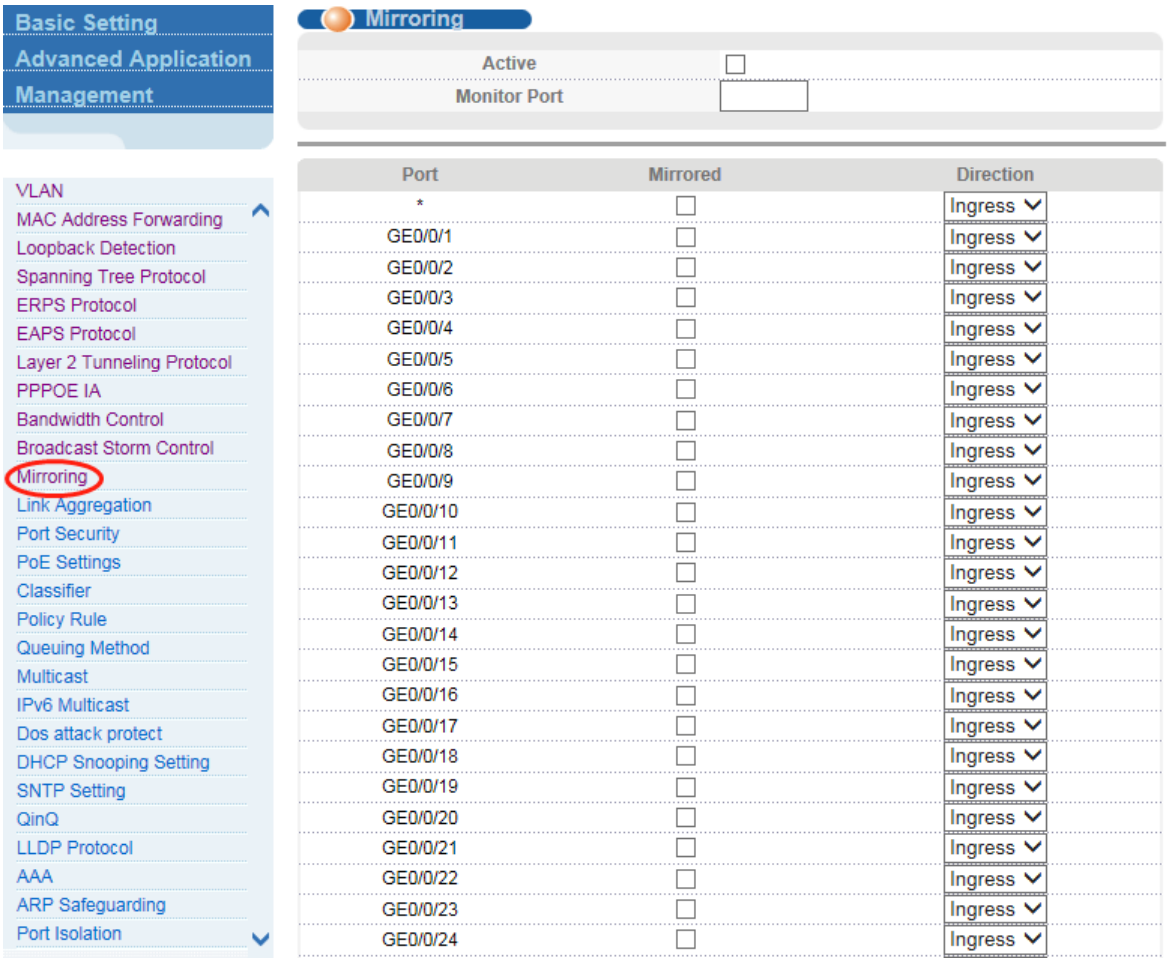
Instructions

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.

4.3.12 Mirroring

Select **Advanced Application > Mirroring** to configure mirroring.

Figure 4-55 Mirroring



Parameter Description

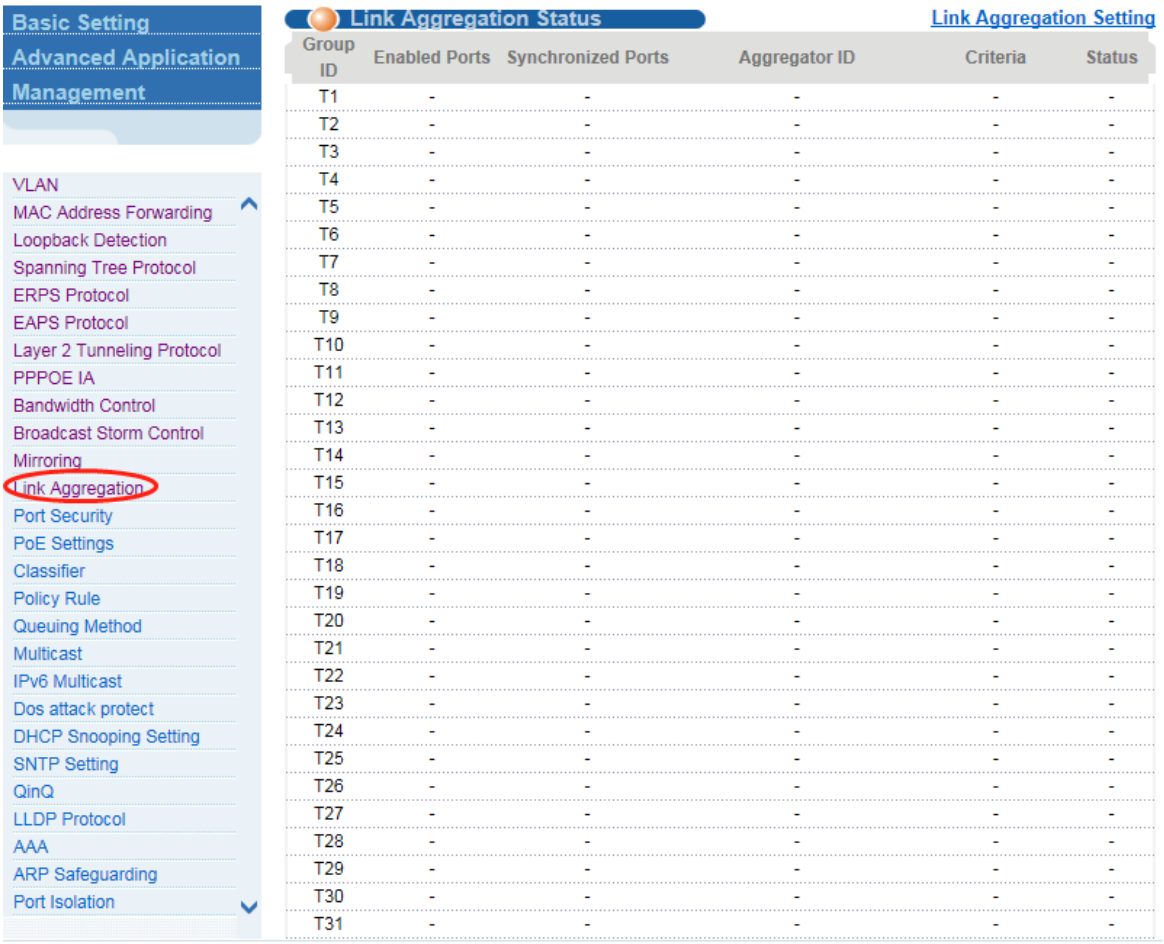
Table 4-22 Mirroring parameter description

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.

4.3.13 Link Aggregation

Select **Advanced Application > Link Aggregation** to configure link aggregation.

Figure 4-56 Link Aggregation



4.3.13.2 Link Aggregation status

Select **Advanced Application > Link Aggregation > Link Aggregation Status** to view link aggregation status, you can view Group ID, Enabled Ports, Synchronized Ports, Aggregator ID, Criteria, Status.

Figure 4-57 Link Aggregation status

Link Aggregation Status

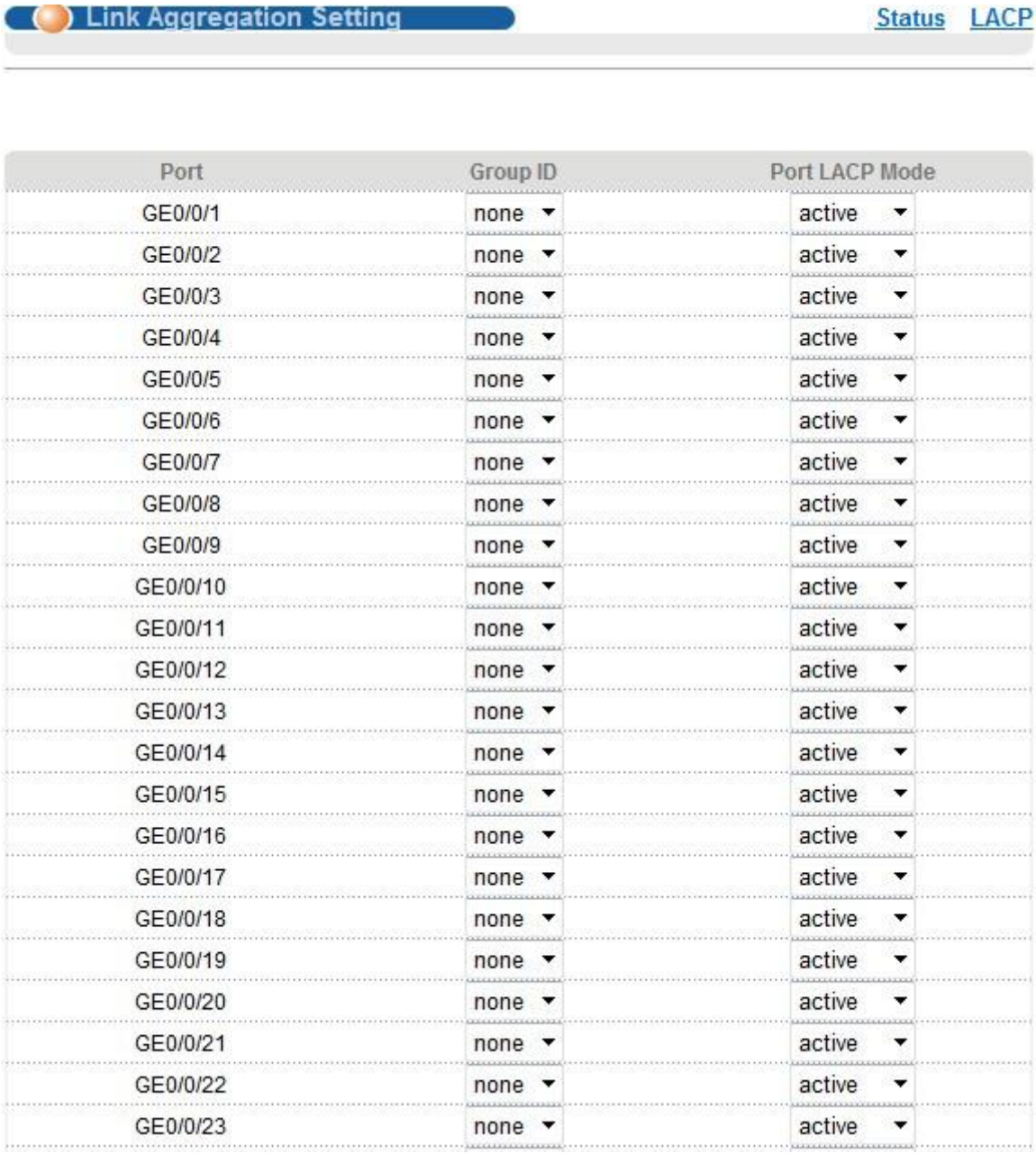
Link Aggregation Setting

Group ID	Enabled Ports	Synchronized Ports	Aggregator ID	Criteria	Status
T1	-	-	-	-	-
T2	-	-	-	-	-
T3	-	-	-	-	-
T4	-	-	-	-	-
T5	-	-	-	-	-
T6	-	-	-	-	-
T7	-	-	-	-	-
T8	-	-	-	-	-
T9	-	-	-	-	-
T10	-	-	-	-	-
T11	-	-	-	-	-
T12	-	-	-	-	-
T13	-	-	-	-	-
T14	-	-	-	-	-
T15	-	-	-	-	-
T16	-	-	-	-	-
T17	-	-	-	-	-
T18	-	-	-	-	-
T19	-	-	-	-	-
T20	-	-	-	-	-
T21	-	-	-	-	-
T22	-	-	-	-	-
T23	-	-	-	-	-
T24	-	-	-	-	-
T25	-	-	-	-	-
T26	-	-	-	-	-
T27	-	-	-	-	-
T28	-	-	-	-	-
T29	-	-	-	-	-
T30	-	-	-	-	-
T31	-	-	-	-	-

4.3.13.3 Link Aggregation Setting

Select **Advanced Application > Link Aggregation > Link Aggregation Setting** to set Link Aggregation.

Figure 4-58 Link Aggregation setting



Parameter Description

Table 4-23 Link Aggregation parameter description

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

Instructions

Port aggregation is the aggregation of multiple physical ports to form an aggregation group to achieve load balancing of traffic and redundant backup of links.

The basic configuration of ports in the same aggregation group must be consistent. The basic configuration mainly includes related configurations such as STP, QoS, VLAN, and port attributes.

On the same switch, if these characteristics of a port in an aggregation group are modified, the remaining ports in the same aggregation group are automatically modified synchronously.

According to different aggregation methods, port aggregation can be divided into static aggregation and dynamic LACP aggregation.

There are three LACP protocol modes for ports:

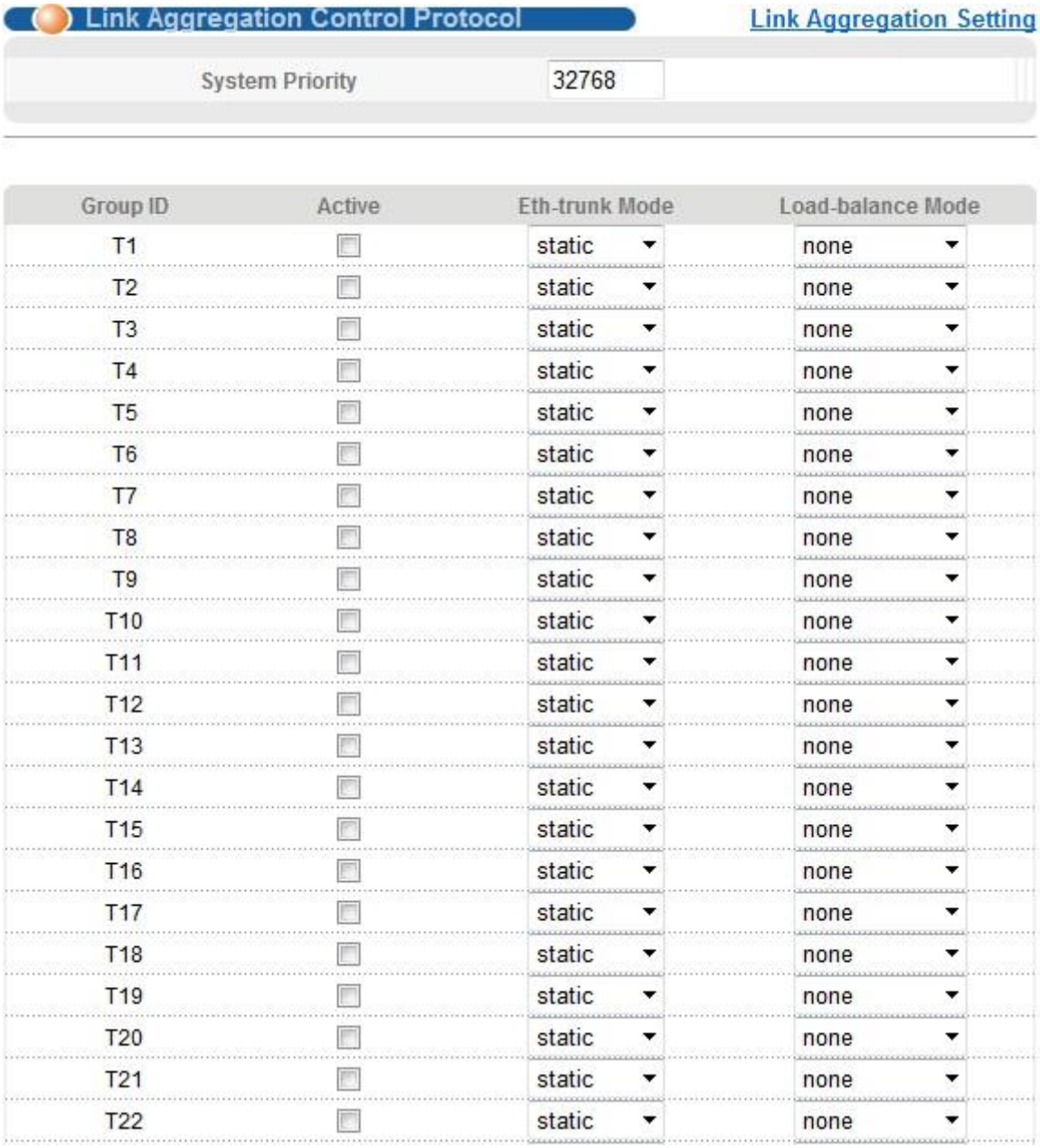
- Static mode (on): Does not run LACP protocol.
- Active mode: In active mode, the port actively initiates LACP negotiation.
- Passive mode: In passive mode, the port only responds to LACP negotiation.

When docking with another device, it can only be docked statically and statically, active can be docked with active or passive, and Passive can only be docked with active.

4.3.13.4 Link Aggregation Control Protocol

Select **Advanced Application > Link Aggregation > Link Aggregation Control Protocol** to configure Link Aggregation Control Protocol.

Figure 4-59 Link Aggregation Control Protocol



Parameter Description

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

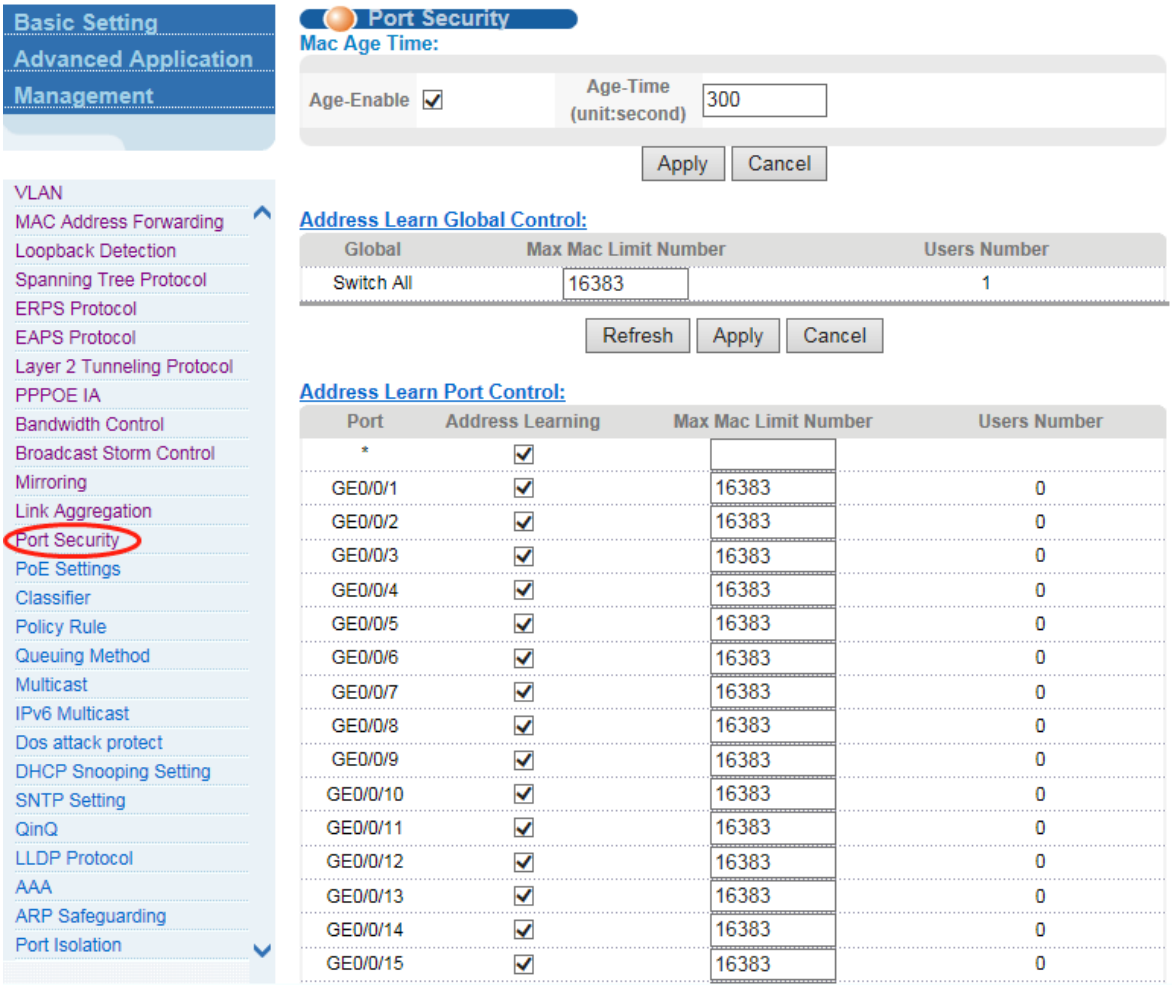
Instructions

In the dynamic LACP mode, the main and subordinate switches are selected according to the system ID. The system ID is composed of the system priority and the local MAC address.

4.3.14 Port Security

Select **Advanced Application > Port Security** to configure port address learn control.

Figure 4-60 Port Security



Parameter Description

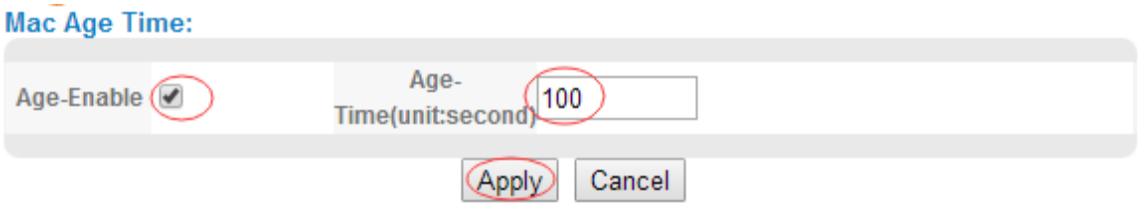
Table 4-24 Port Security parameter description

Parameter	Description
Age-Enable	Open age-enable.
Age-Time	Set Age Time (the range of 10-1000000, unit: second).
Max Mac Limit Number (Global)	Set the global Max MAC Limit Number (0-16384).
Address Learning	The MAC address learning function of port enables the power switch (the default port MAC learning function opens).
Max Mac Limit Number (Port)	Set the port Max MAC Limit Number (0-16384).

Configuration example

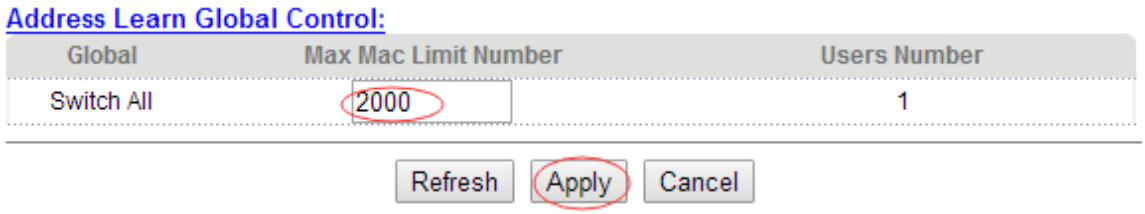
- Configure mac Age Time, open Age-Time, Age-Time (second) is 100.

Figure 4-61 Configuration example(1)



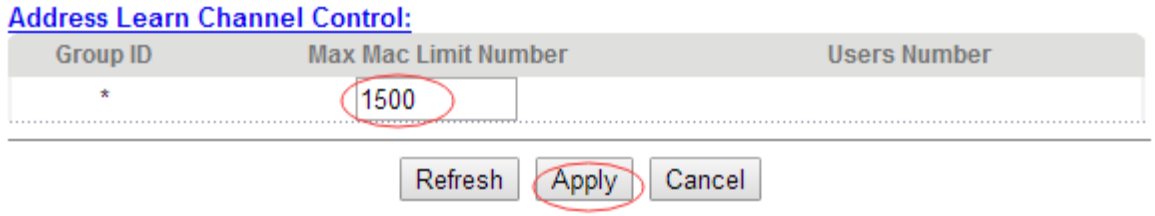
- Configure Address Learn Global Control, set max mac limit number is 2000.

Figure 4-62 Configuration example(2)



- Configure Address Learn Channel Control, set max mac limit number (channel) is 1500.

Figure 4-63 Configuration example(3)



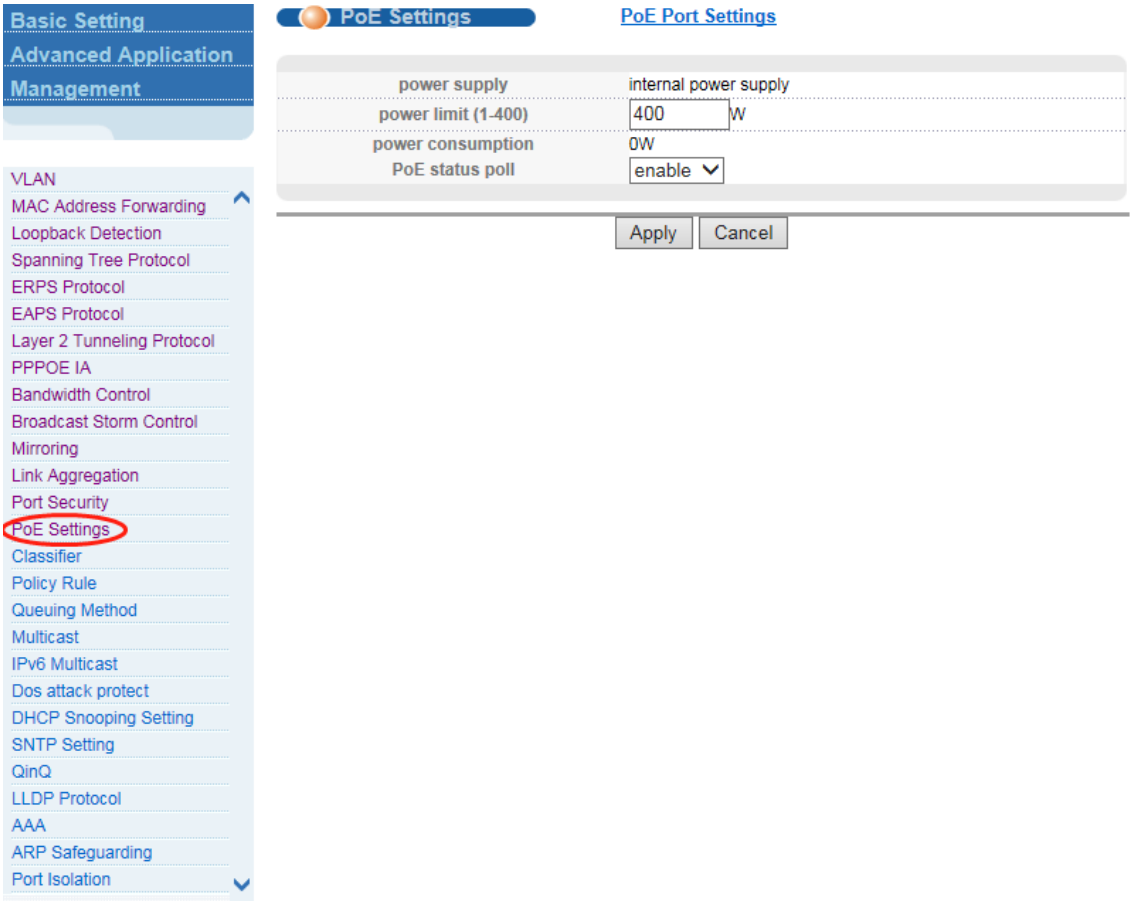
- Configure Address Learn Vlan Control, set Max Mac Limit Number (Vlan) is 1900.

Figure 4-64 Configuration example(3)

4.3.15 POE Settings

Select **Advanced Application > POE Settings** to configure POE.

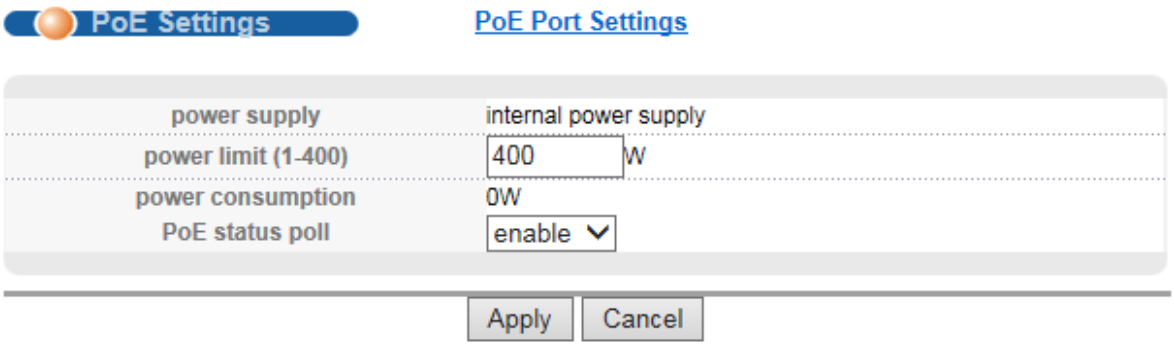
Figure 4-65 POE Settings



4.3.15.2 POE Settings

Select **Advanced Application > POE Settings** to configure POE.

Figure 4-66 POE Settings



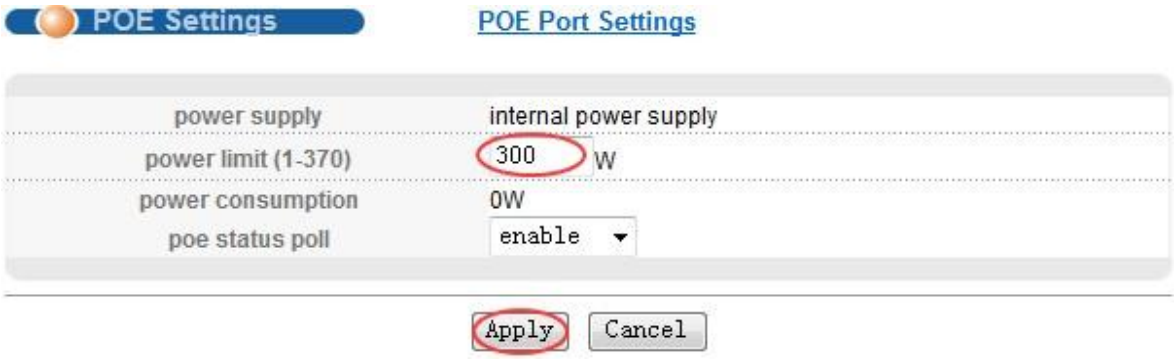
Parameter Description

Power Limit: The power of switch POE can be limited.

Configuration example

Such as: set power limit is 300W.

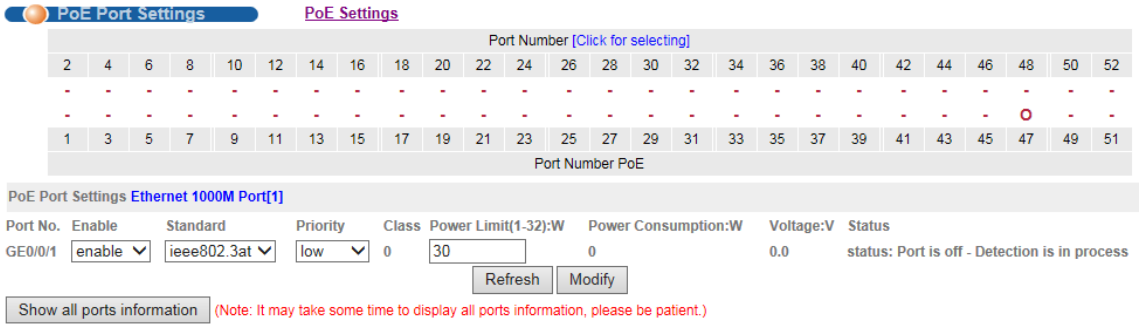
Figure 4-67 Configuration example



4.3.15.3 POE Port Settings

Select **Advanced Application > POE Port Settings** to configure POE Port.

Figure 4-68 POE Port Settings



Parameter Description

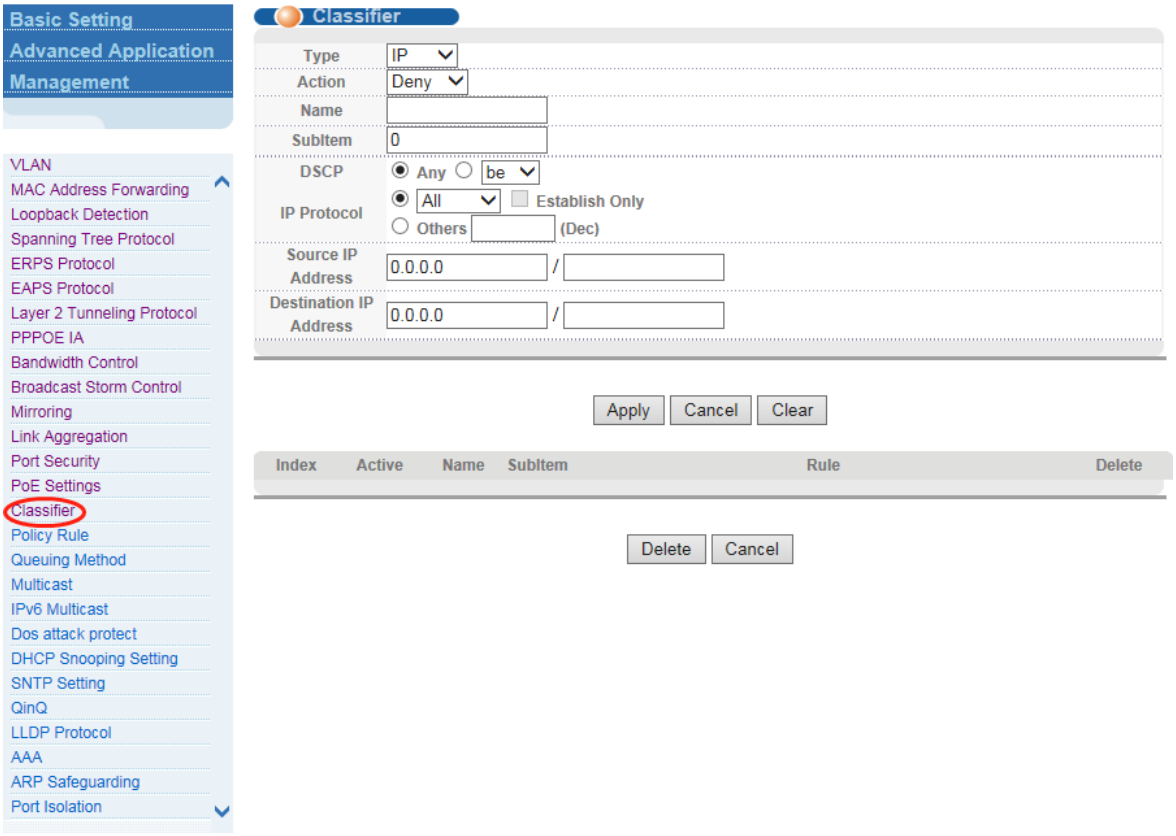
Table 4-25 PoE Port Settings parameter description

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.

4.3.16 Classifier

Select **Advanced Application > Classifier** to configure Classifier.

Figure 4-69 Classifier



Parameter Description

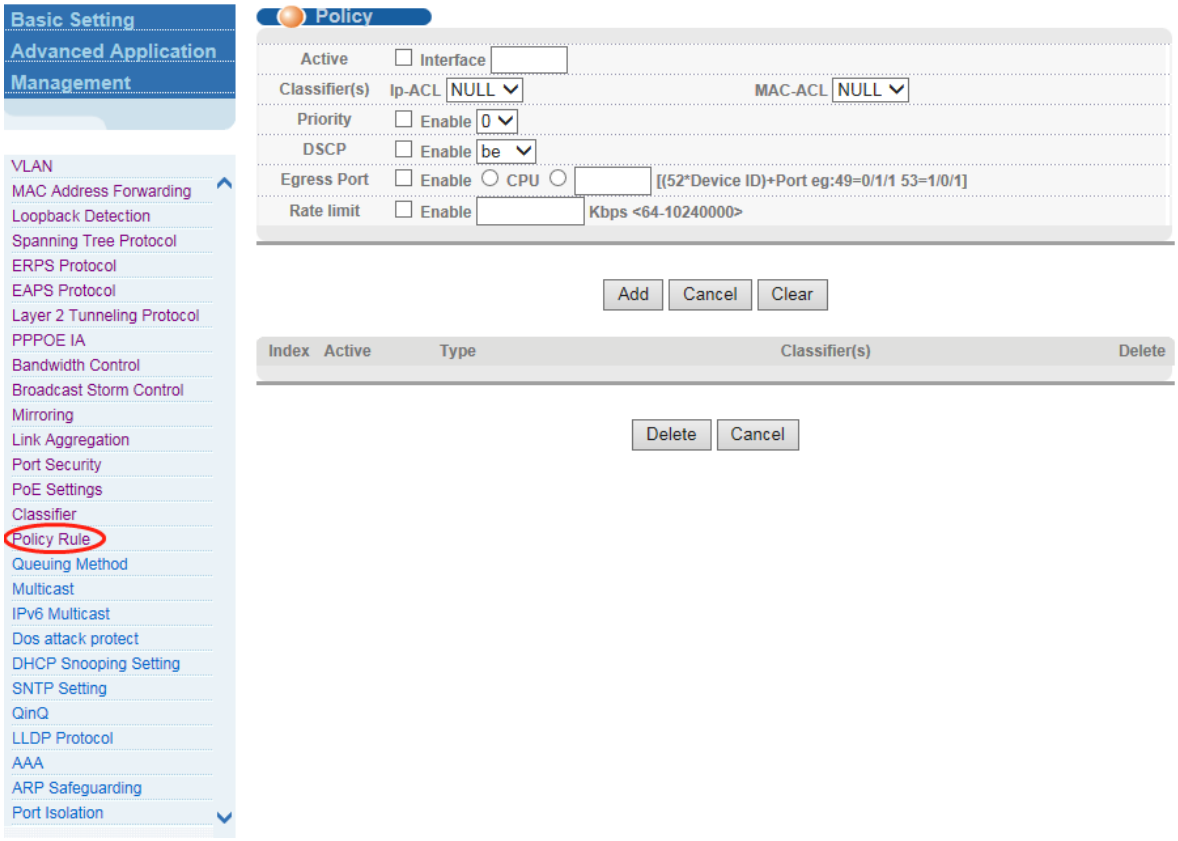
Table 4-26 Classifier parameter description

Parameter	Description
Active	Active Classifier.
Layer2	Set VLAN, Priority, Ethernet type, Source Mac Address, DSCP, IP Protocol.
Layer3	Set Source IP.

4.3.17 Policy Rule

Select **Advanced Application > Policy Rule** to configure Policy Rule.

Figure 4-70 Policy Rule



Parameter Description

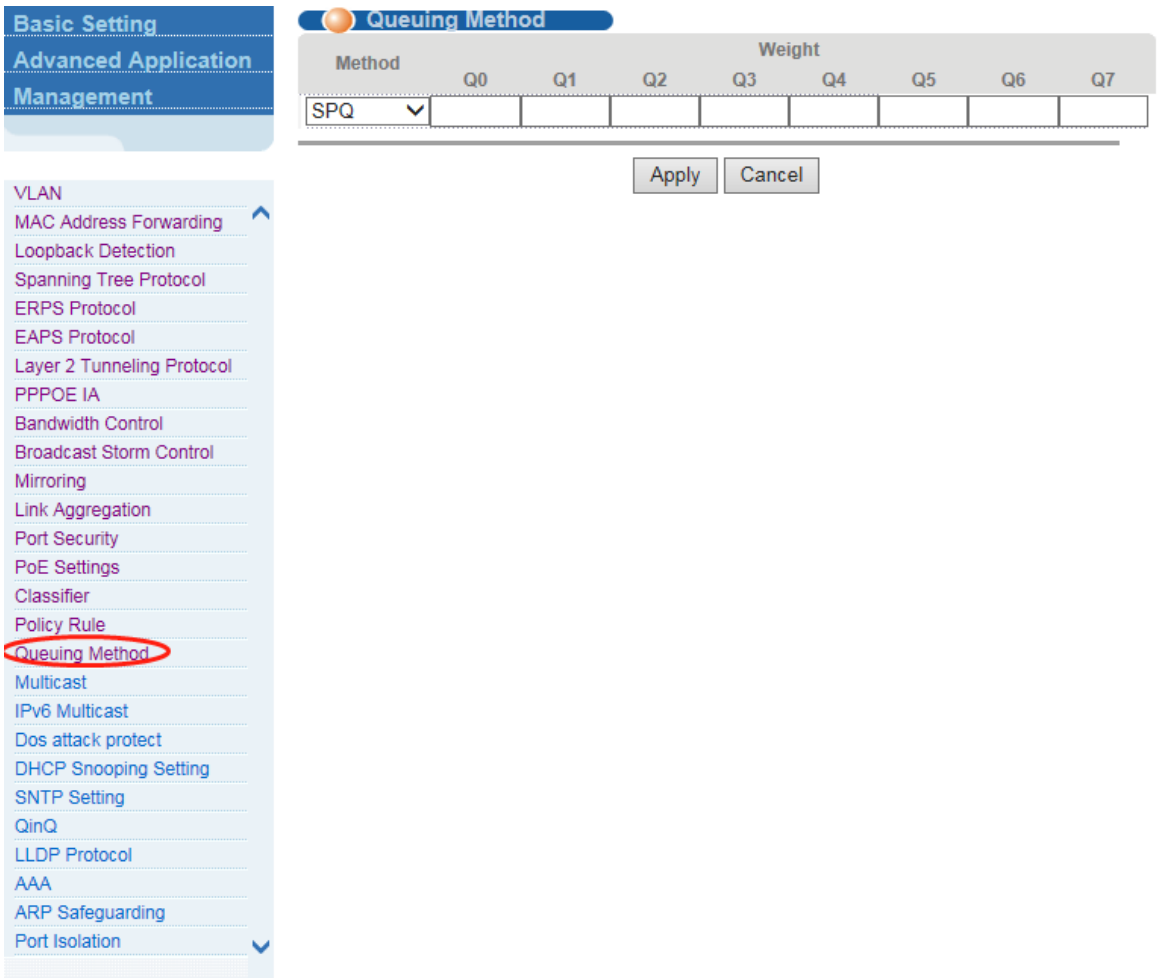
Table 4-27 Policy Rule parameter description

Parameter	Description
Active	Active Classifier.
Classifier(s)	You need to match the set of classification rules.
Parameter	Set Bandwidth, Egress Port, Priority, DSCP, TOS.

4.3.18 Queuing Method

Select **Advanced Application > Queuing Method** to configure queuing method.

Figure 4-71 Queuing Method

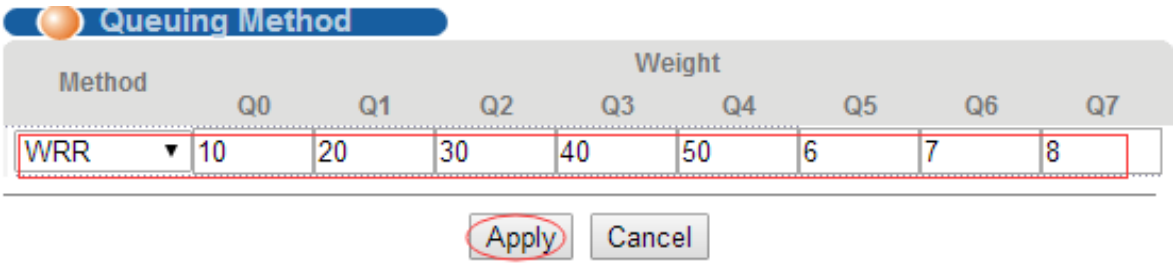


Parameter Description

Method: SPQ, WRR, SP+WRR, WFQ, SP+WFQ.

Configuration example

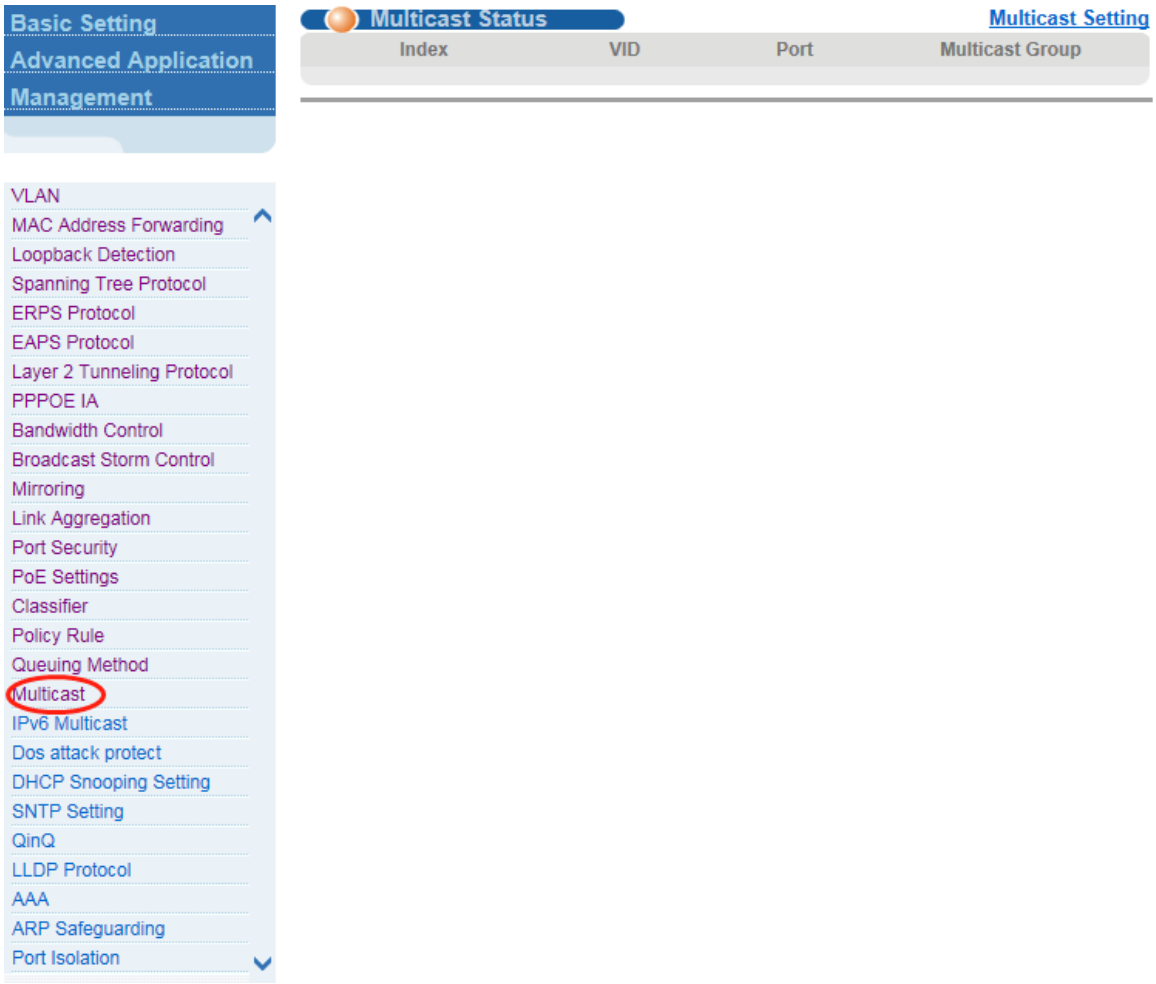
Figure 4-72 Configuration example



4.3.19 Multicast

Select **Advanced Application > Multicast** to configure Multicast.

Figure 4-73 Multicast



4.3.19.2 Multicast Status

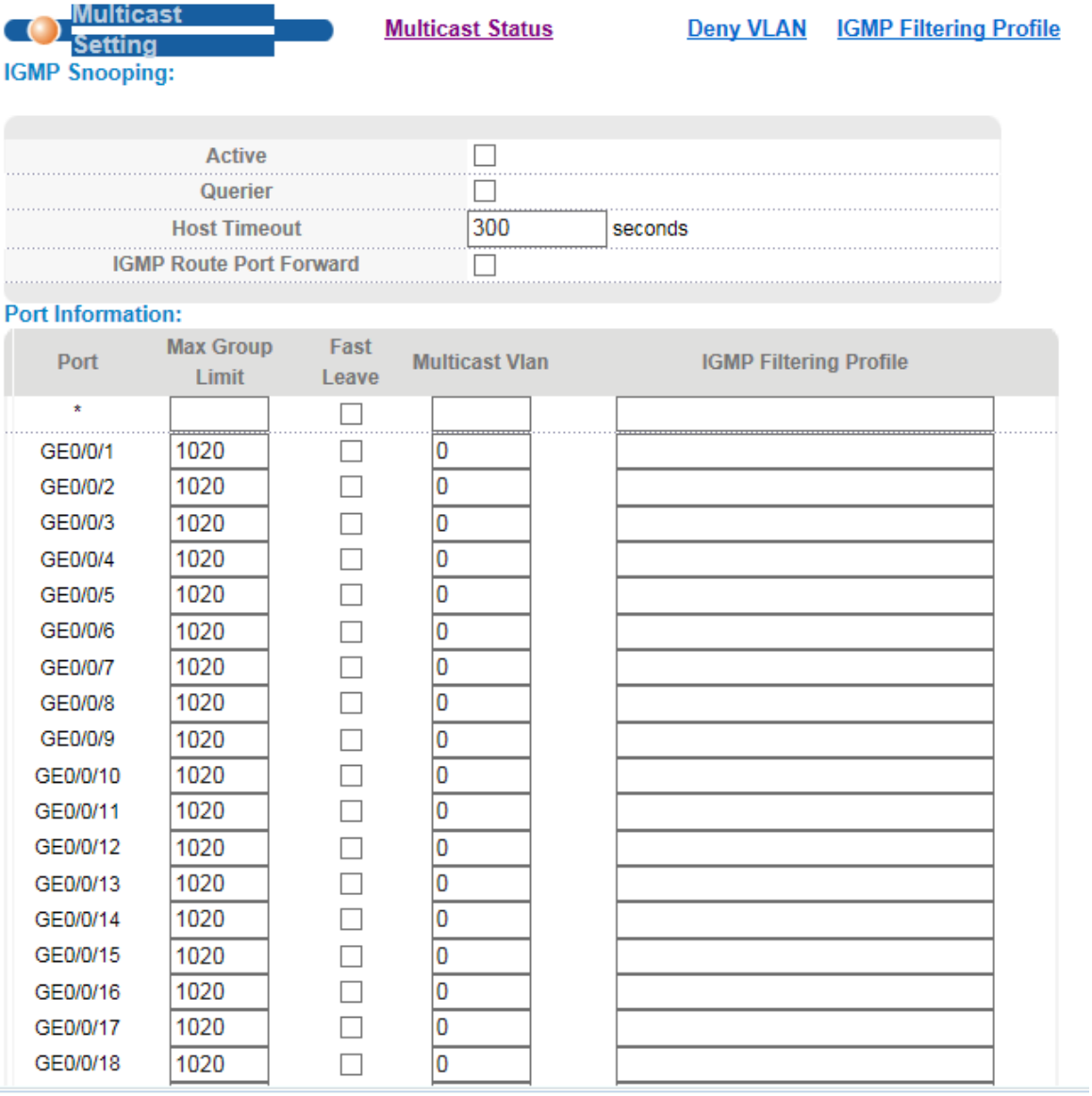
Select **Advanced Application > Multicast > Multicast Status** to view all multicast. This includes the static configuration and the multicast that is learned through the IGMP-Snooping protocol.

Figure 4-74 Multicast Status

4.3.19.3 Multicast Settings

Select **Advanced Application > Multicast > Multicast Settings** to set multicast.

Figure 4-75 Multicast Settings



Parameter Description

Table 4-28 Multicast Settings parameter description

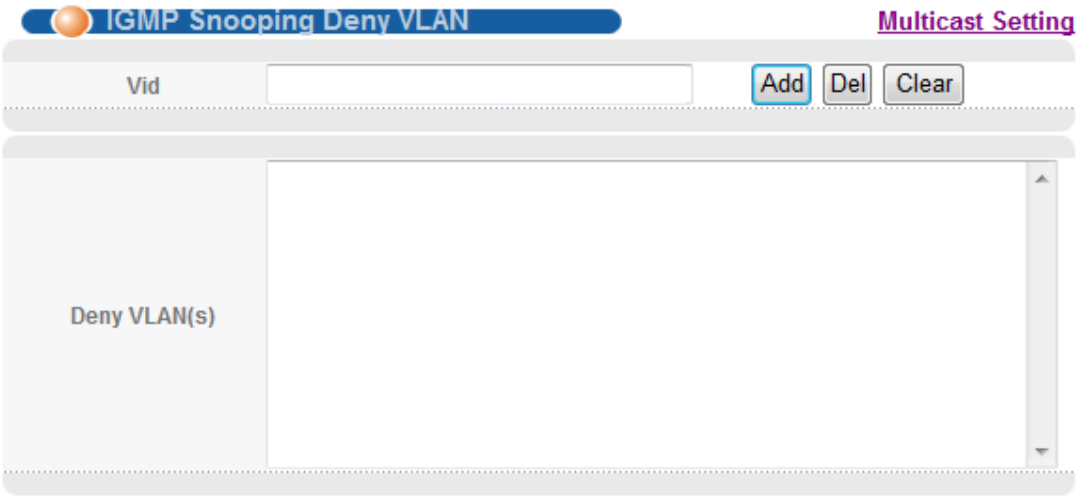
Parameter	Description
Active	Open IGMP-snooping.
Querier	Open IGMP-snooping timed query function.
Host Timeout	Configure the dynamic group sowing time (default 300s).
IGMP Route Port Forward	Open IGMP Route Port Forward.
Max Group Limit	Max learning group of configuration port (default 1020).
Fast Leave	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.

4.3.19.4 IGMP Snooping Dney VLAN

Select **Advanced Application > Multicast > IGMP Snooping Dney VLAN** to preview the banned group broadcast group, unable to teach the multicast group that is prohibited by the group preview.

Figure 4-76 IGMP Snooping Dney VLAN



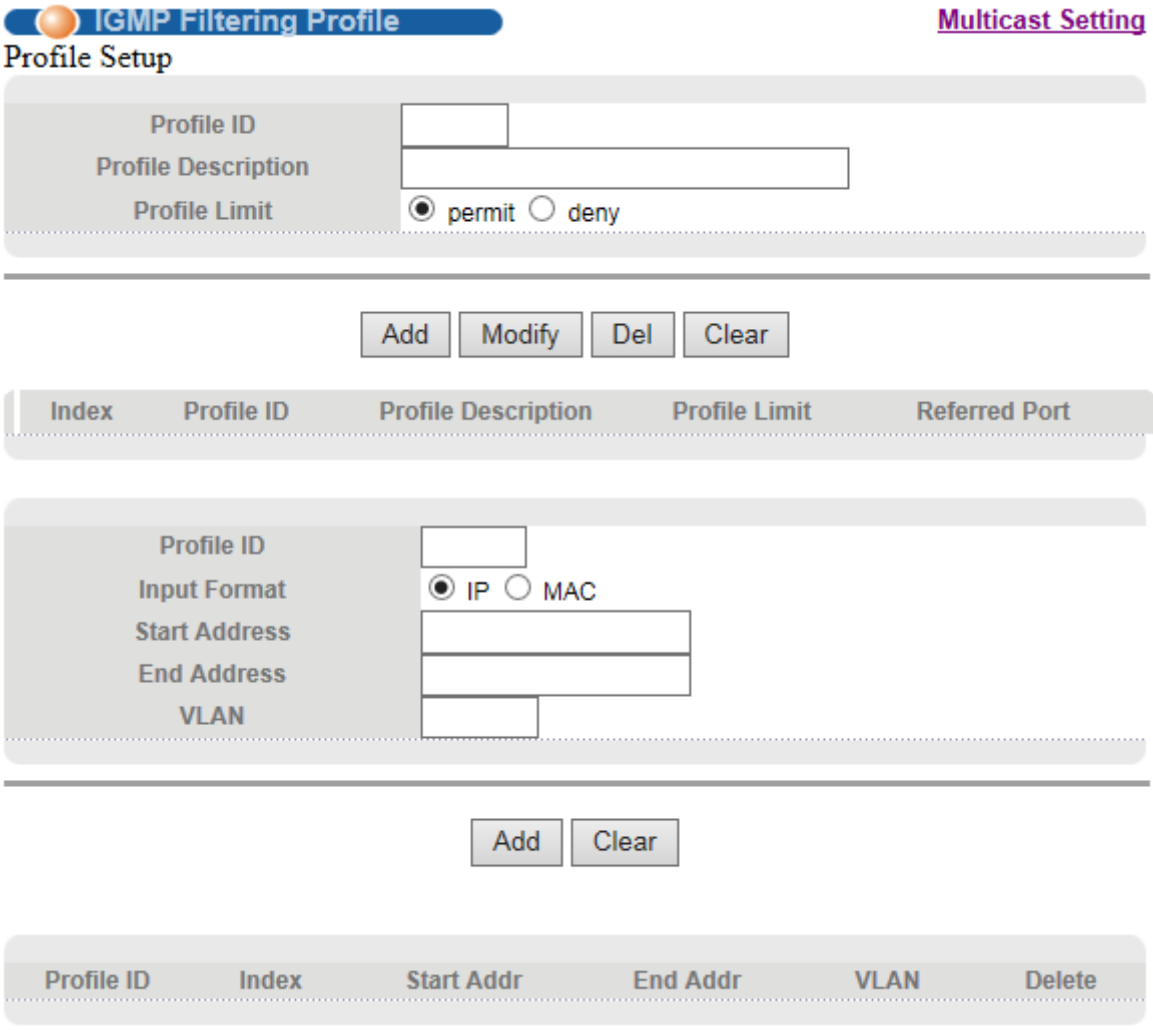
Parameter Description

Vid: Vlan’s ID.

4.3.19.5 IGMP Filtering Profile

Select **Advanced Application > Multicast > IGMP Filtering Profile** to add and remove the preview feature of the modified group.

Figure 4-77 IGMP Filtering Profile



Parameter Description

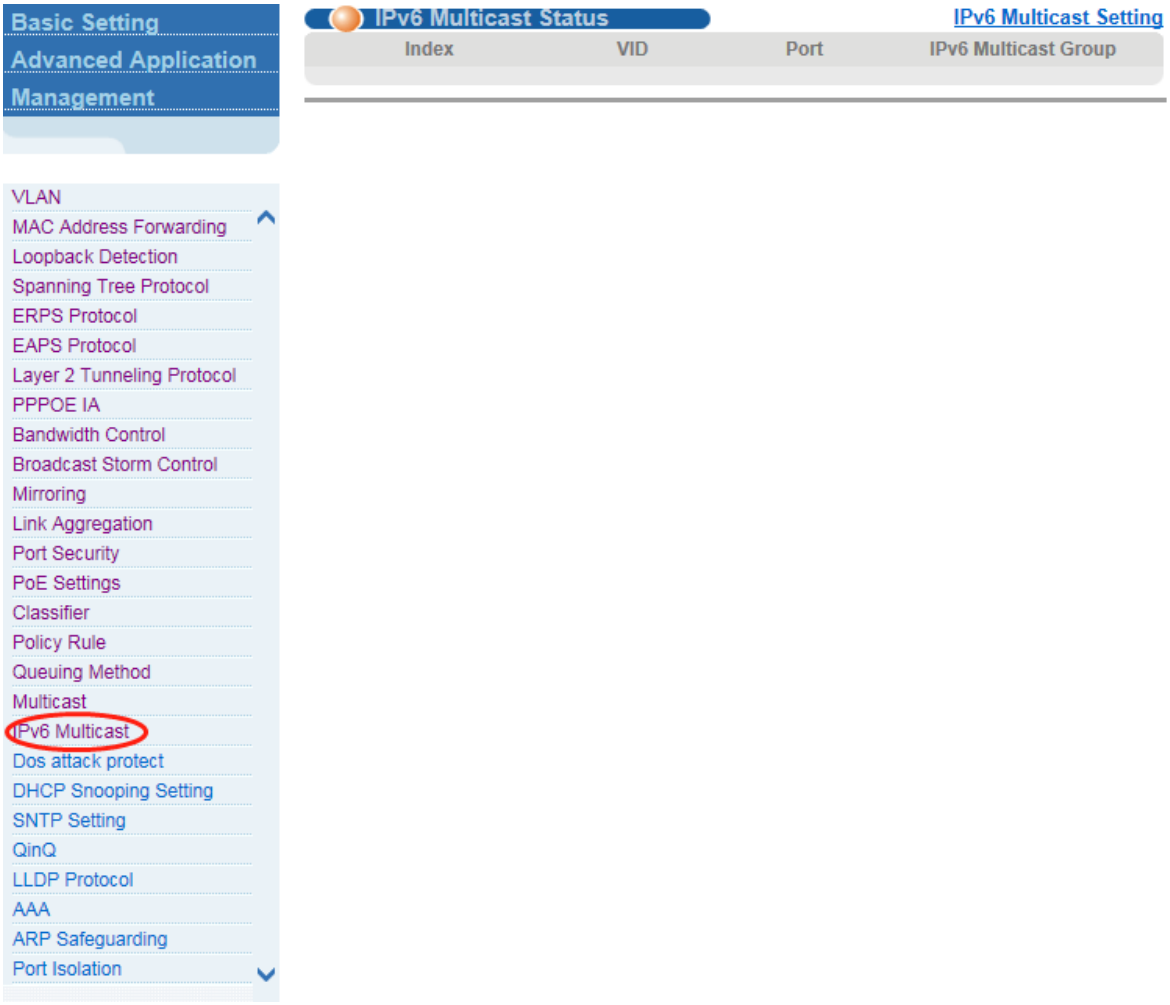
Table 4-29 IGMP Filtering Profile parameter description

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.

4.3.20 IPv6 Multicast

Select **Advanced Application > IPv6 Multicast** to configure IPv6 Multicast.

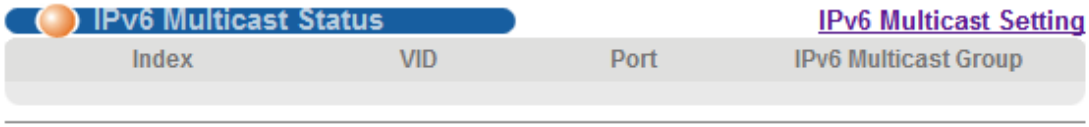
Figure 4-78 IPv6 Multicast



4.3.20.2 IPv6 Multicast Status

Select **Advanced Application > IPv6 Multicast > IPv6 Multicast Status** to view all IPv6 Multicast groups.

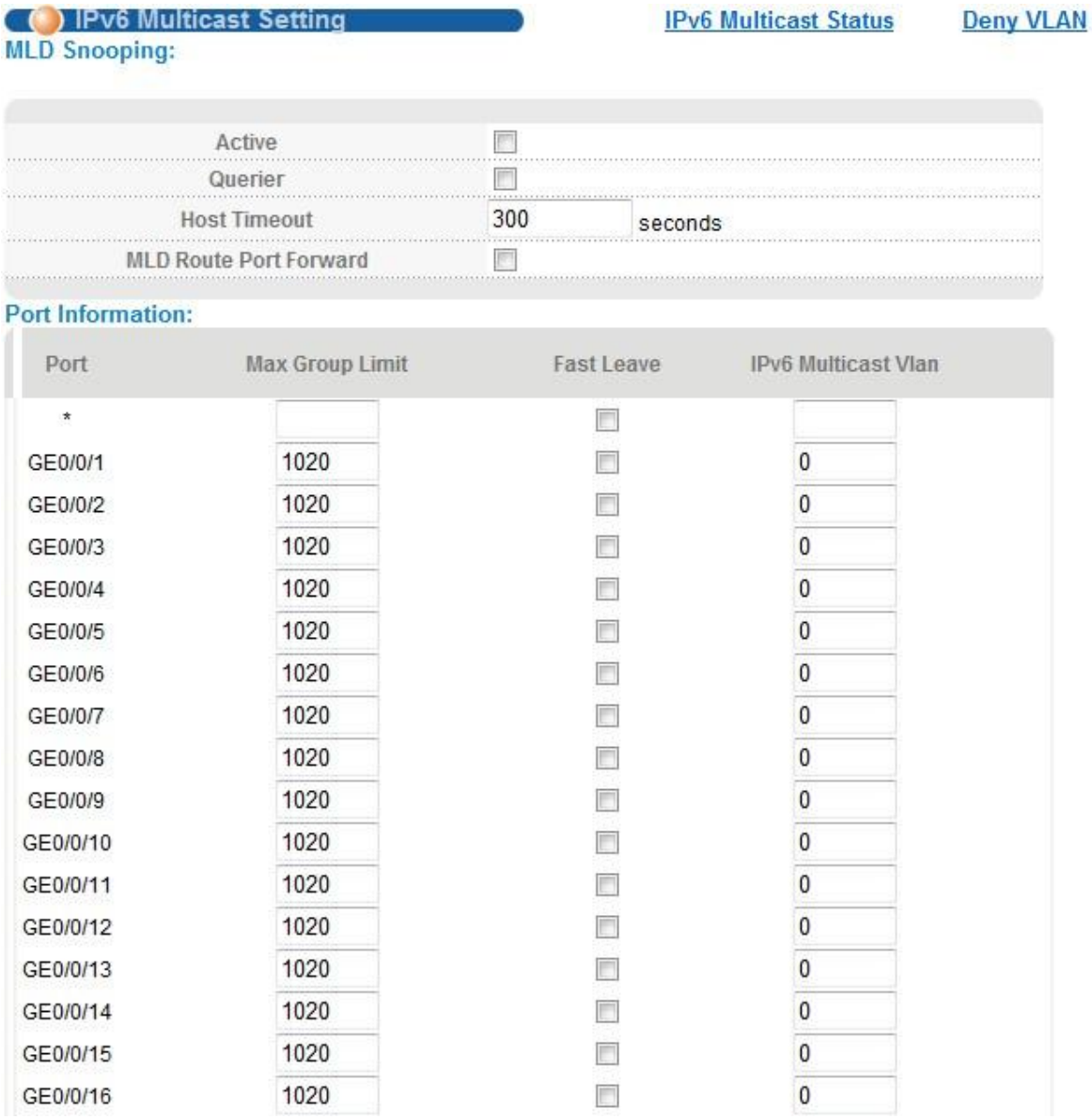
Figure 4-79 IPv6 Multicast Status



4.3.20.3 IPv6 Multicast Setting

Select **Advanced Application > IPv6 Multicast > IPv6 Multicast Setting** to configure IPv6 Multicast.

Figure 4-80 IPv6 Multicast Setting



Parameter Description

Table 4-30 IPv6 Multicast Setting parameter description

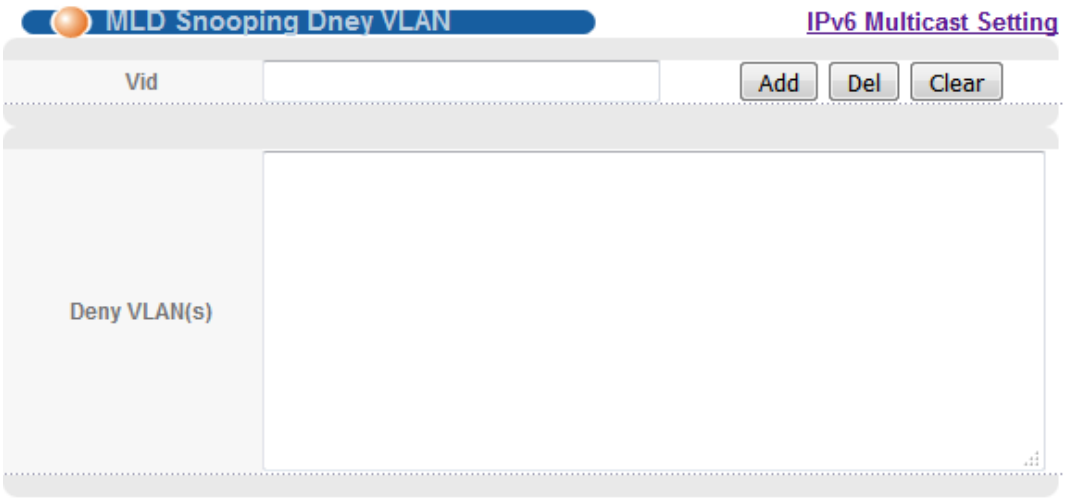
Parameter	Description
Active	Enable or disable MLD snooping.
Querier	Enable or disable MLD snooping timed Querier.
Host Timeout	Configure Dynamic IPv6 multicast aging time (default 300s).
MLD Route Port Forward	Enable or disable MLD Route Port Forward.
Max Group Limit	Configure maximum learning IPv6 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.

4.3.20.4 MLD Snooping Dney VLAN

Select **Advanced Application > IPv6 Multicast > MLD Snooping Dney VLAN** to configure MLD Snooping Dney VLAN.

Figure 4-81 MLD Snooping Dney VLAN



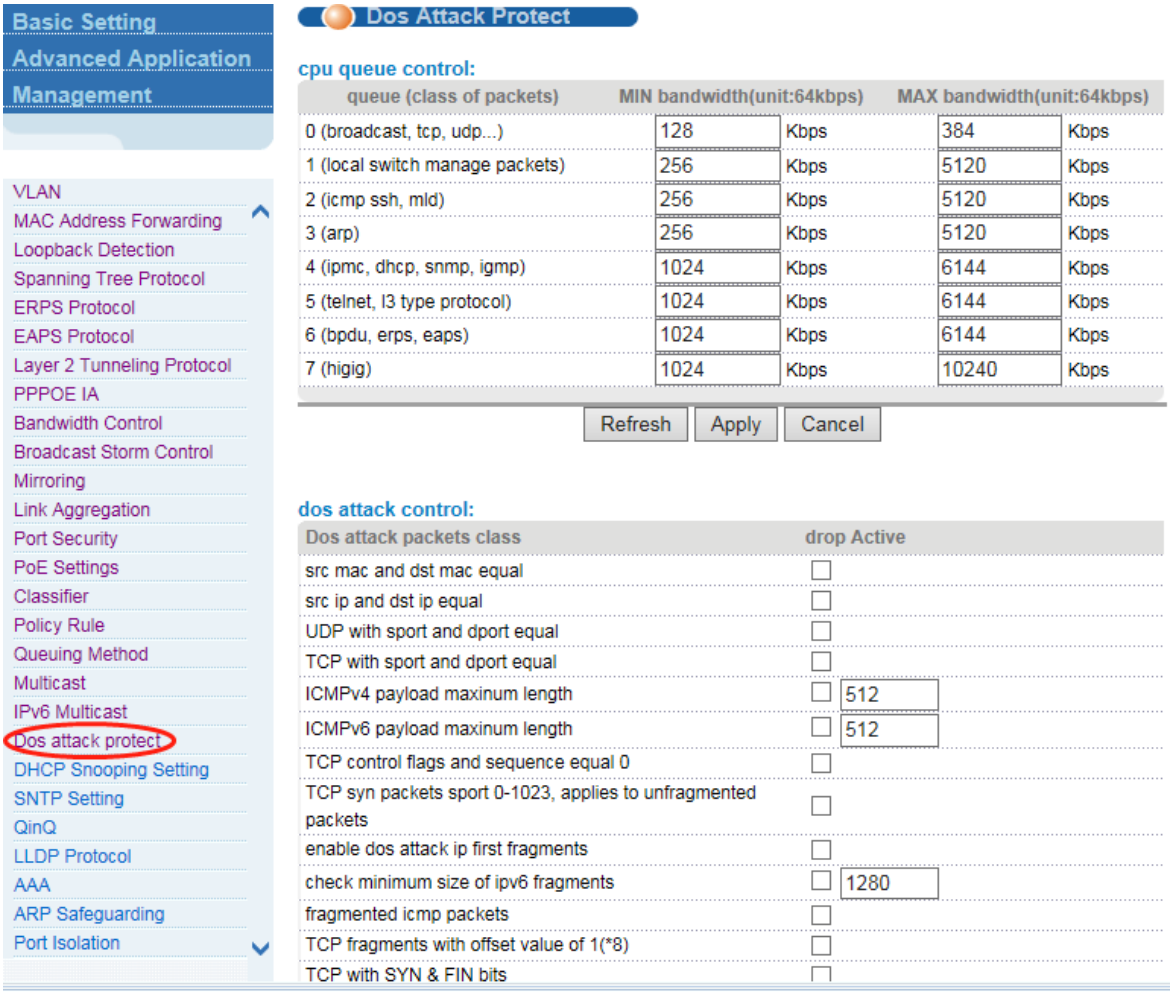
Parameter Description

Vid: Vlan ID

4.3.21 Dos attack protect

Select **Advanced Application > Dos attack protect** to configure dos attack protect.

Figure 4-82 Dos Attack Protect



Parameter Description

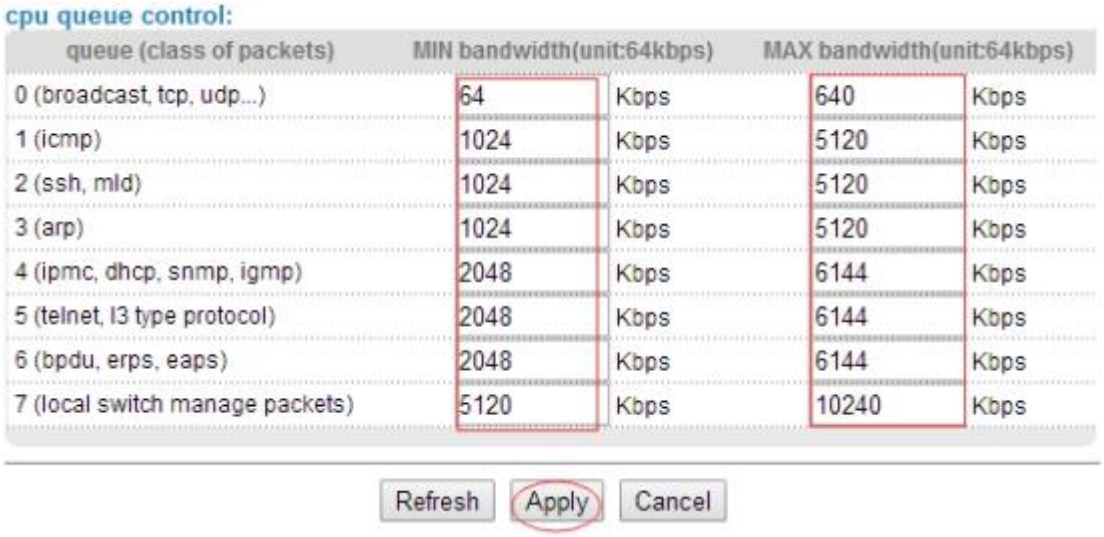
Table 4-31 DOS Attack Protect parameter description

Parameter	Description
cpu queue control	The CPU queue is controlled by setting minimum bandwidth and maximum bandwidth (minimum value is 64 kbps).
dos attack control	The DOS attack is controlled by the discarding behavior of the corresponding message.

Configuration example

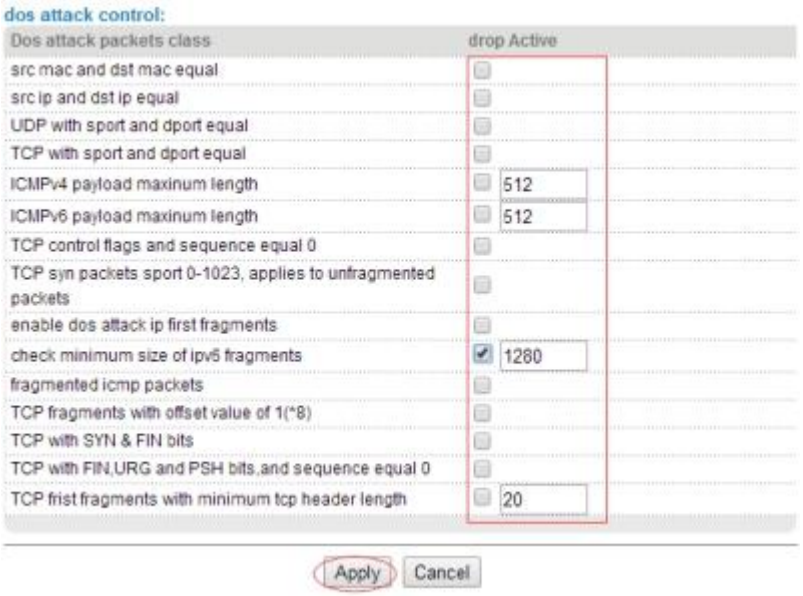
- cpu queue control

Figure 4-83 Configuration example(1)



- dos attack control

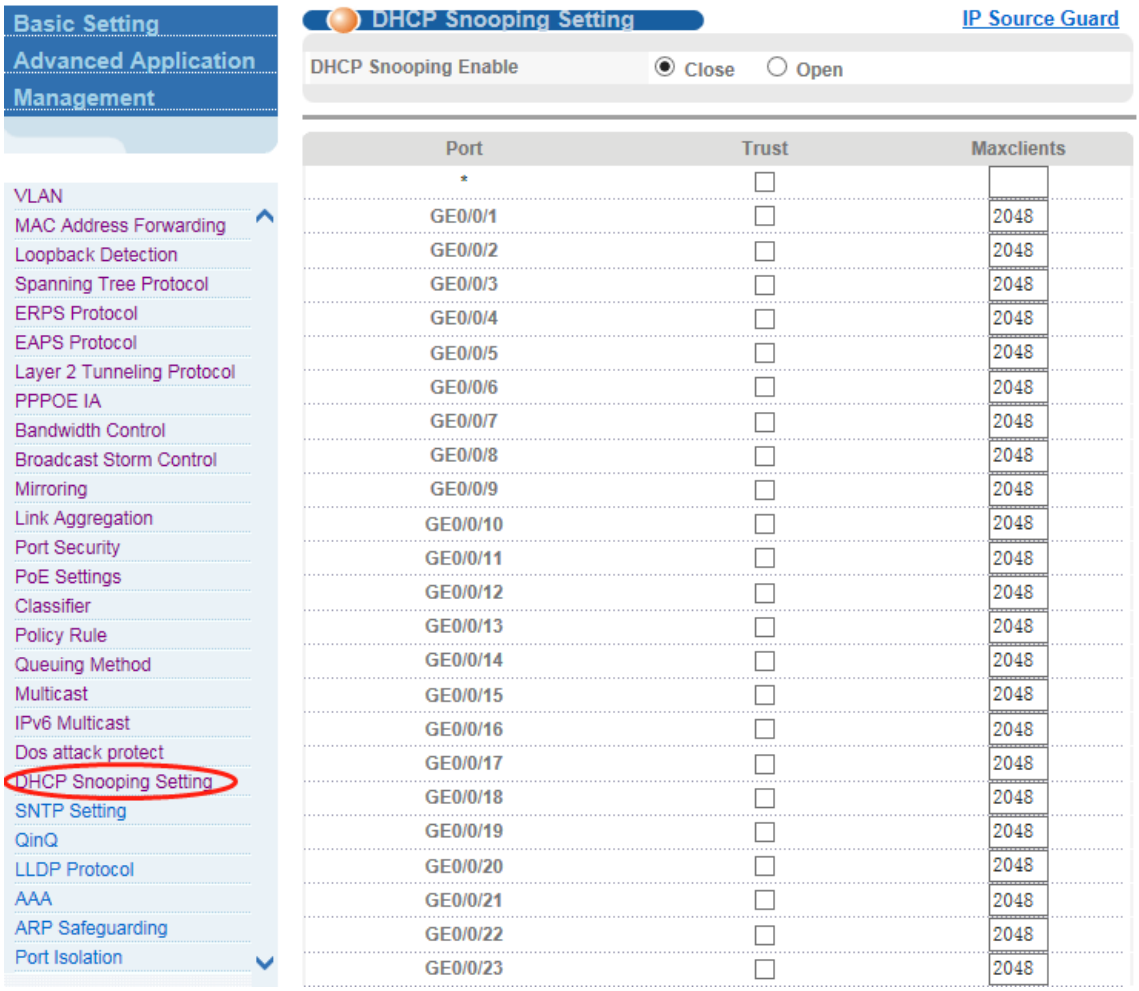
Figure 4-84 Configuration example(2)



4.3.22 DHCP Snooping Setting

Select **Advanced Application > DHCP Snooping Setting** to configure DHCP Snooping.

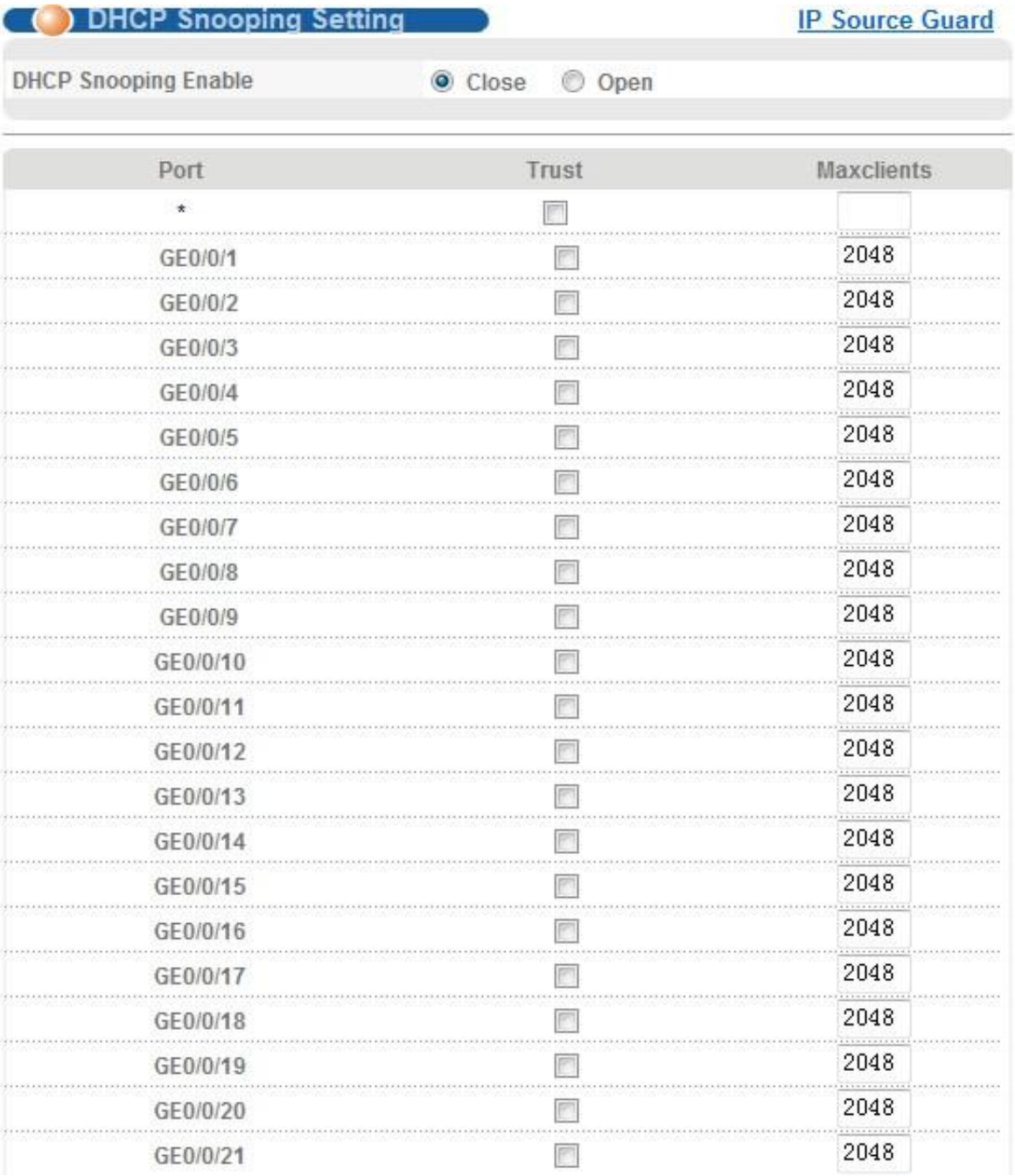
Figure 4-85 DHCP Snooping Setting



4.3.22.2 DHCP Snooping Setting

Select **Advanced Application > DHCP Snooping Setting > DHCP Snooping Setting** to configure DHCP Snooping.

Figure 4-86 DHCP Snooping Setting



Parameter Description

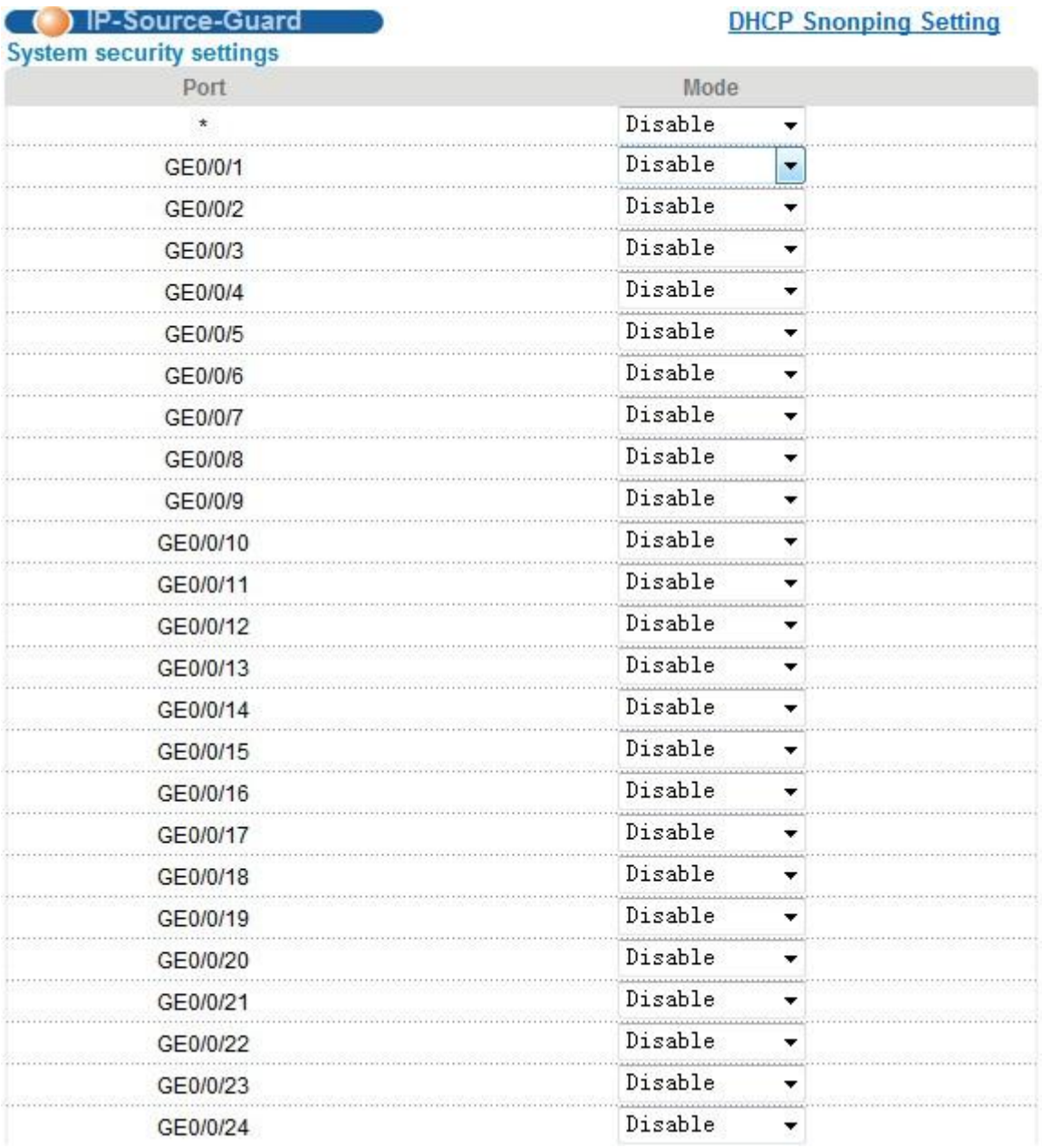
Table 4-32 DHCP Snooping Setting parameter description

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.

4.3.22.3 IP Source Guard

Select **Advanced Application >DHCP Snooping Setting > IP Source Guard** to configure IP Source Guard.

Figure 4-87 IP Source Guard



Parameter Description

Disable unbinding entry to access network: Enable or Disable unbinding entry to access network.

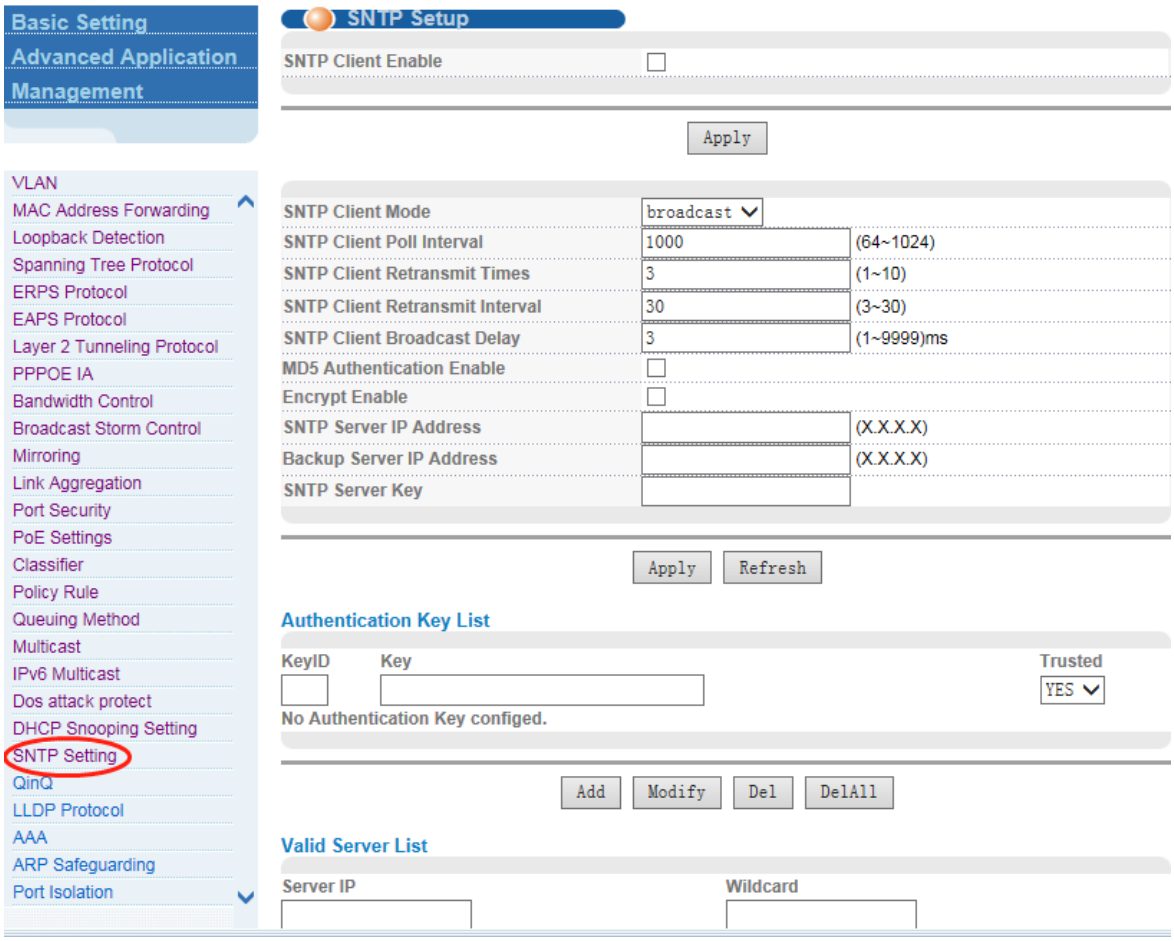
Instructions

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

4.3.23 SNTP Setting

Select **Advanced Application > SNTP Setting** to configure SNTP.

Figure 4-88 SNTP Setting



Parameter Description

Table 4-33 SNTP Setting 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.

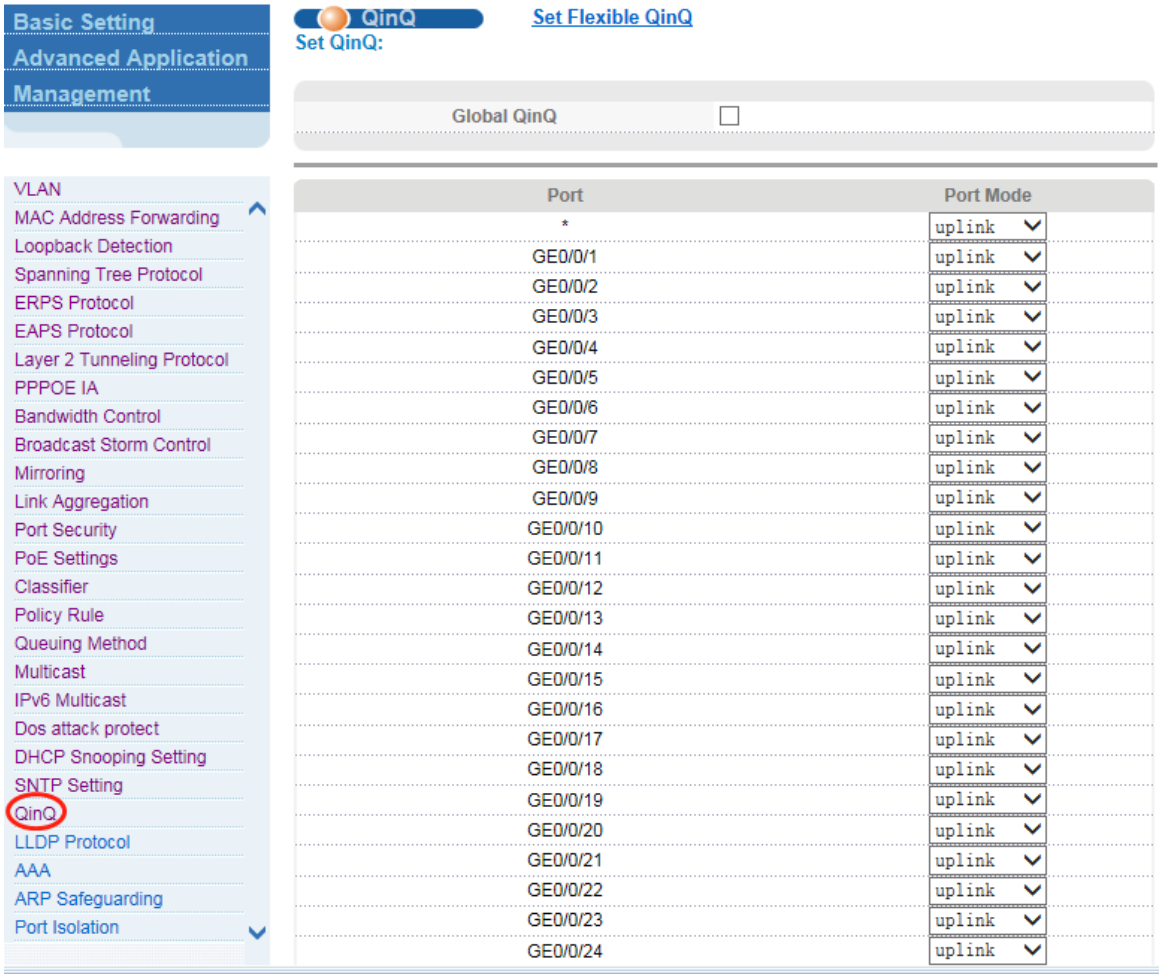
Instructions

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).

4.3.24 QinQ

Select **Advanced Application > QinQ** to configure QinQ.

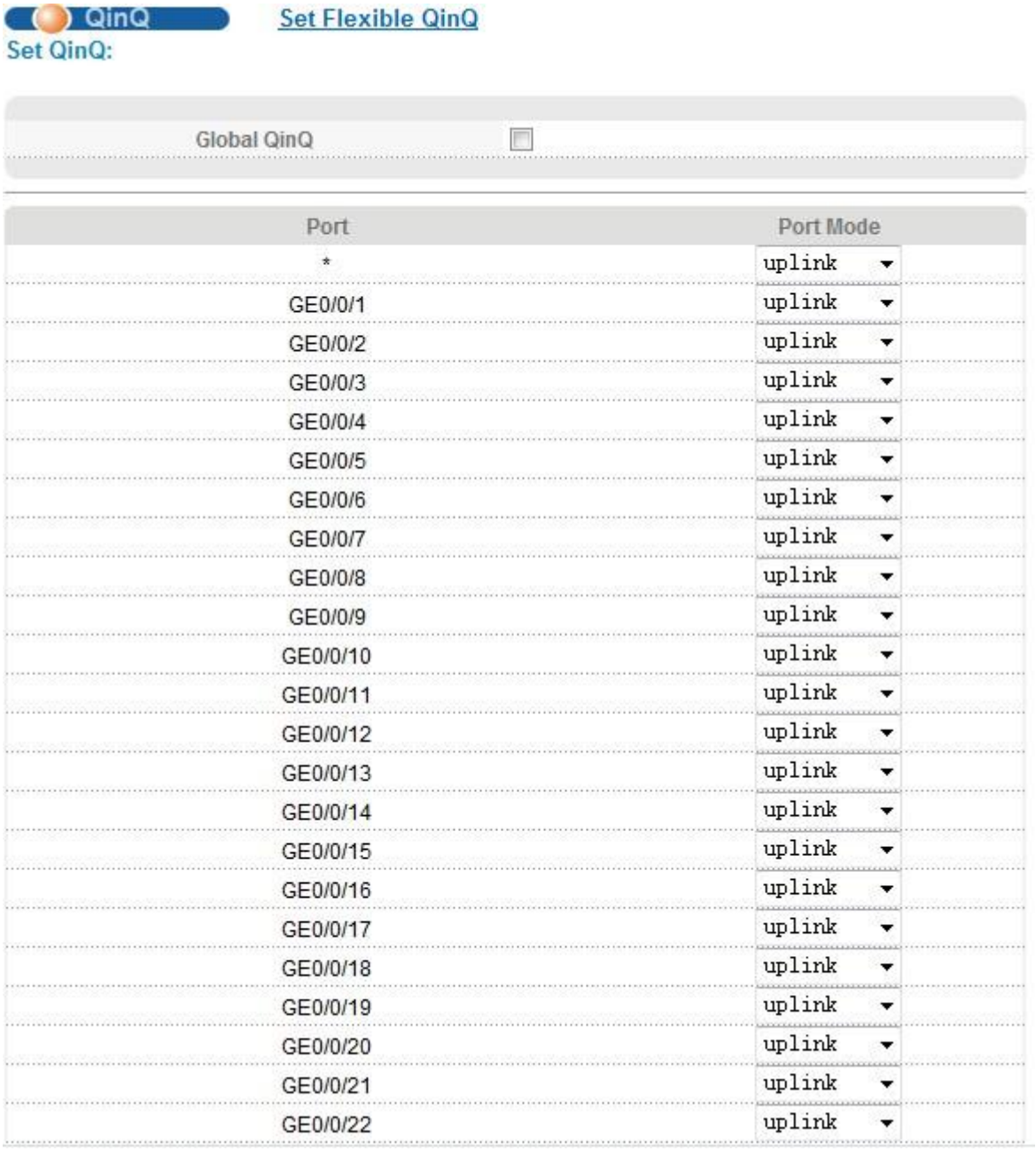
Figure 4-89 QinQ



4.3.24.2 Set QinQ

Select **Advanced Application > QinQ > Set QinQ** to configure QinQ.

Figure 4-90 Set QinQ



Parameter Description

Table 4-34 Set QINQ parameter description

Parameter	Description
Active	Enable or disable global QinQ.
QinQ	Enable or disable QinQ of ports.
Port Mode	Port Mode: uplink, customer.

Instructions

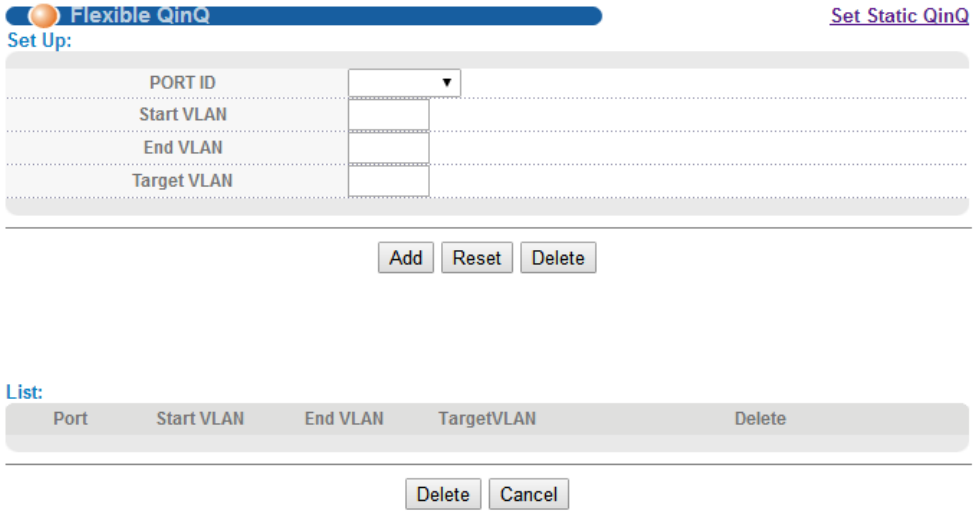
Customer, the port in this mode and the port in uplink mode form a static QinQ application, and the packets entering this port will be considered as not containing the outer VLAN tag and inner

VLAN tag, so that the packet will use the PVID of the port or the VLAN ID specified by other rules as The outer VLAN ID of the packet; the packets sent from this port will be stripped of the outer VLAN tag, regardless of the configuration of the outer VLAN.
The customer port needs to be connected to the port of the device on the user's network side. A single VLAN tag message entered from this port can carry 2 VLAN tags when sent from the uplink port.
Uplink, the port in this mode is connected to the port of the network device on the carrier side, the packets entering this port will try to identify the outer VLAN tag; the packets sent from the port will always carry the inner VLAN tag, and the outer VLAN tag is based on Whether the configuration of the outer VLAN is stripped. The Uplink port judges whether the packet is tagged or not based on whether the packet's vlan protocol number is the same as the globally configured outer-tpid value. If it is the same, it is considered to be tagged, and if it is different, it is not tagged.

4.3.24.3 Flexible QinQ

Select **Advanced Application > QinQ > Set QinQ to QinQ**.

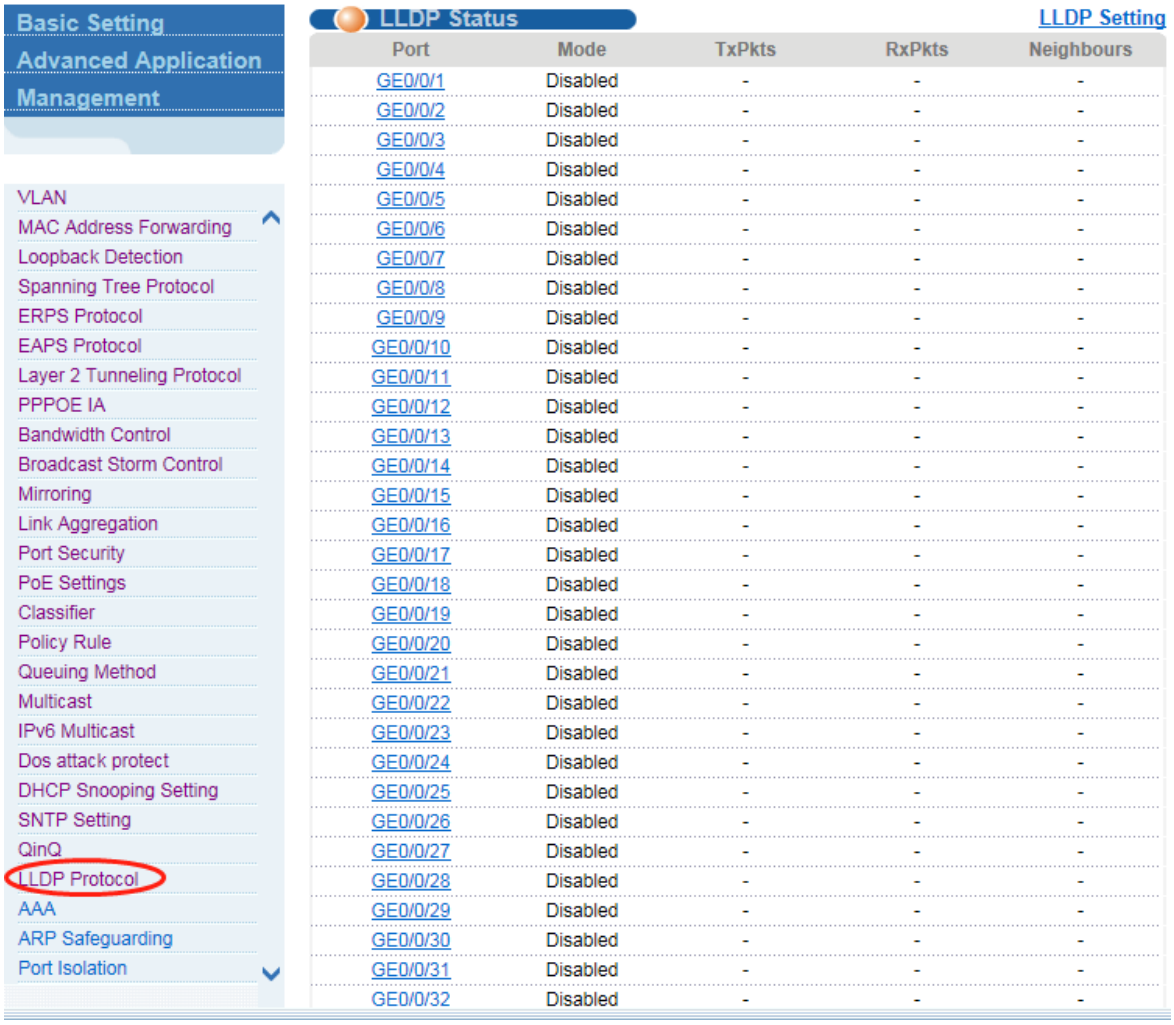
Figure 4-91 Flexible QinQ



4.3.25 LLDP Protocol

Select **Advanced Application > LLDP Protocol** to configure LLDP.

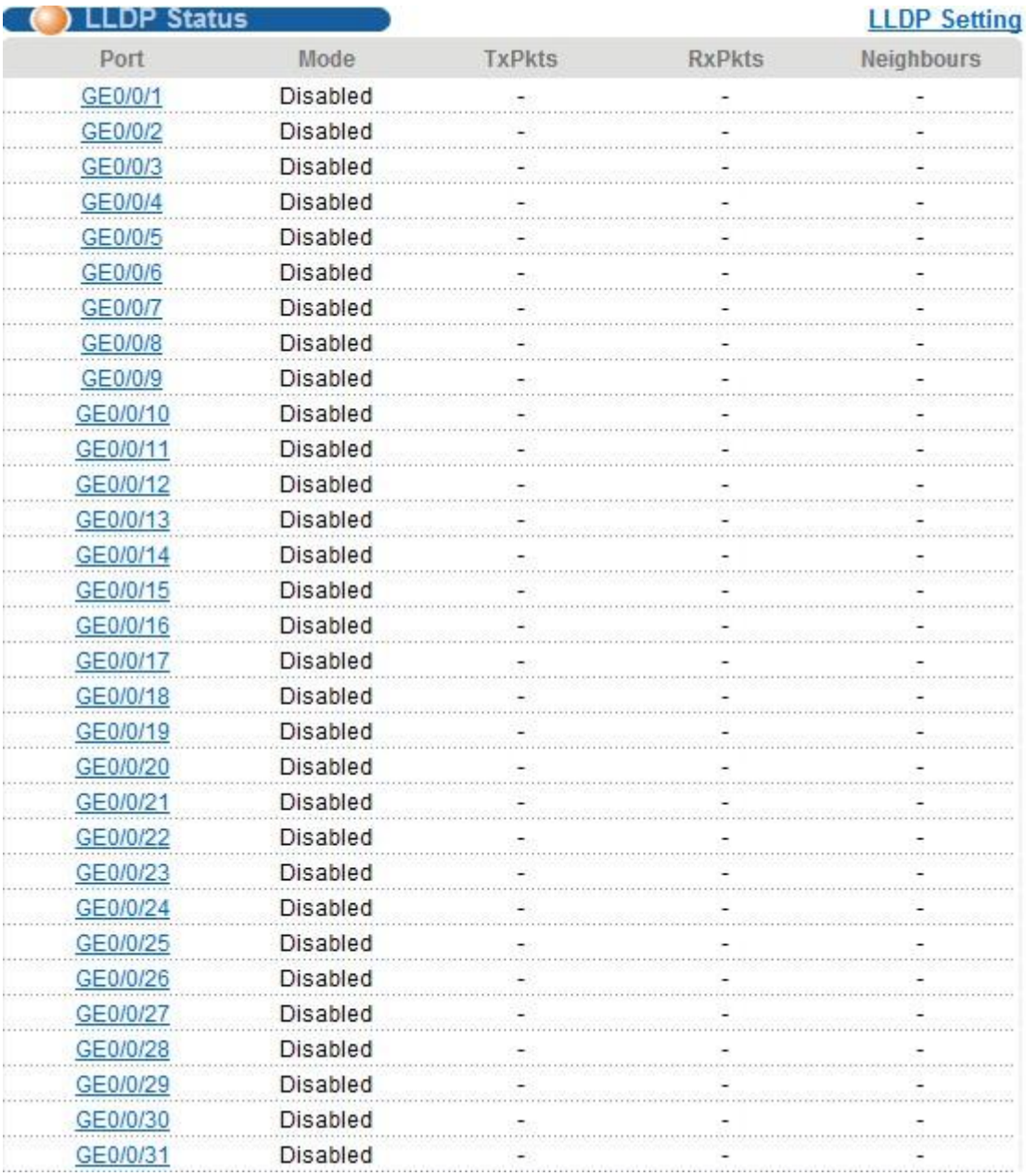
Figure 4-92 LLDP Protocol



4.3.25.2 LLDP Status

Select **Advanced Application > LLDP Protocol > LLDP Status** to view LLDP status.

Figure 4-93 LLDP Status

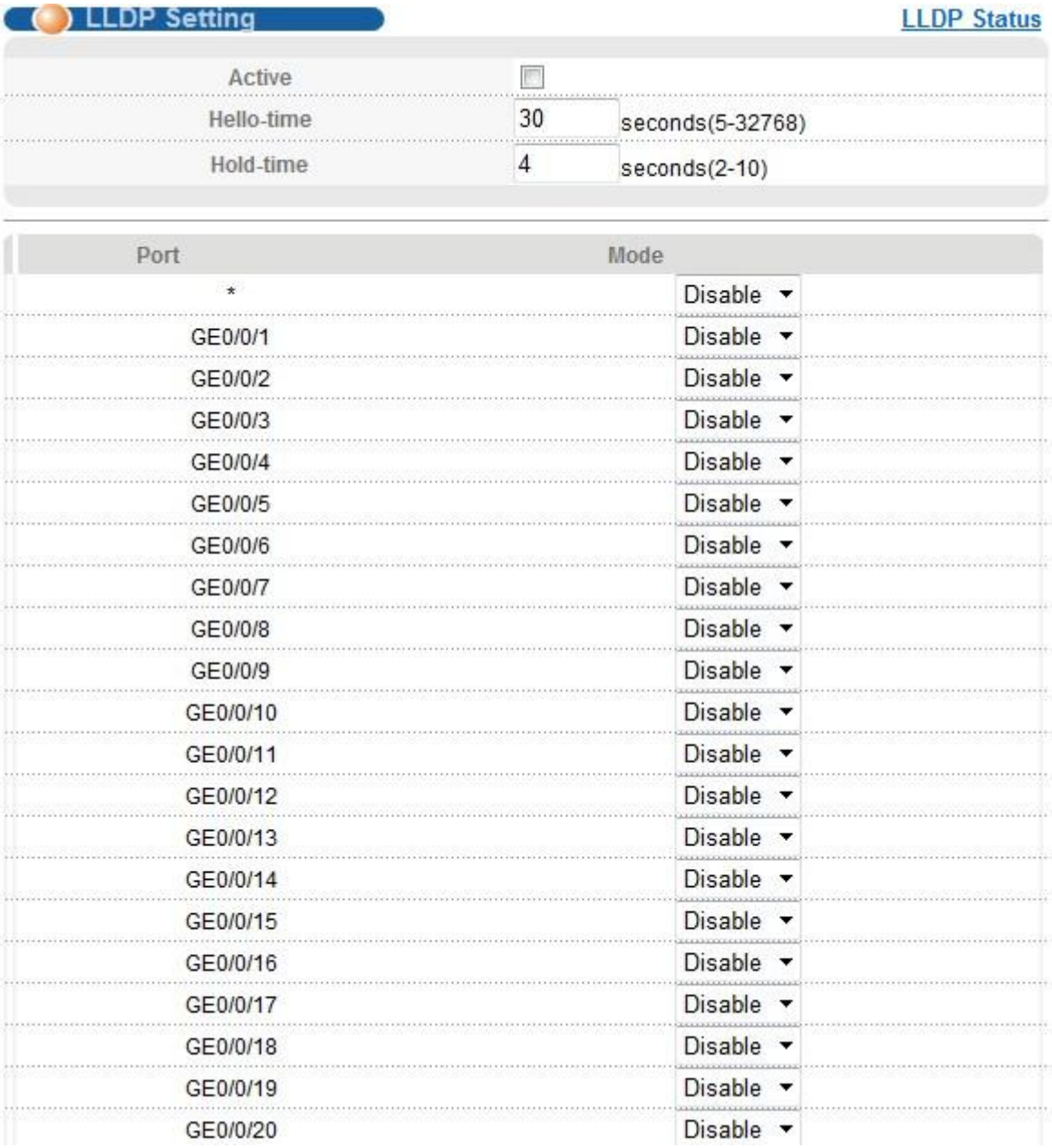


Port	Mode	TxPkts	RxPkts	Neighbours
GE0/0/1	Disabled	-	-	-
GE0/0/2	Disabled	-	-	-
GE0/0/3	Disabled	-	-	-
GE0/0/4	Disabled	-	-	-
GE0/0/5	Disabled	-	-	-
GE0/0/6	Disabled	-	-	-
GE0/0/7	Disabled	-	-	-
GE0/0/8	Disabled	-	-	-
GE0/0/9	Disabled	-	-	-
GE0/0/10	Disabled	-	-	-
GE0/0/11	Disabled	-	-	-
GE0/0/12	Disabled	-	-	-
GE0/0/13	Disabled	-	-	-
GE0/0/14	Disabled	-	-	-
GE0/0/15	Disabled	-	-	-
GE0/0/16	Disabled	-	-	-
GE0/0/17	Disabled	-	-	-
GE0/0/18	Disabled	-	-	-
GE0/0/19	Disabled	-	-	-
GE0/0/20	Disabled	-	-	-
GE0/0/21	Disabled	-	-	-
GE0/0/22	Disabled	-	-	-
GE0/0/23	Disabled	-	-	-
GE0/0/24	Disabled	-	-	-
GE0/0/25	Disabled	-	-	-
GE0/0/26	Disabled	-	-	-
GE0/0/27	Disabled	-	-	-
GE0/0/28	Disabled	-	-	-
GE0/0/29	Disabled	-	-	-
GE0/0/30	Disabled	-	-	-
GE0/0/31	Disabled	-	-	-

4.3.25.3 LLDP Setting

Select **Advanced Application > LLDP Protocol > LLDP Setting** to configure LLDP.

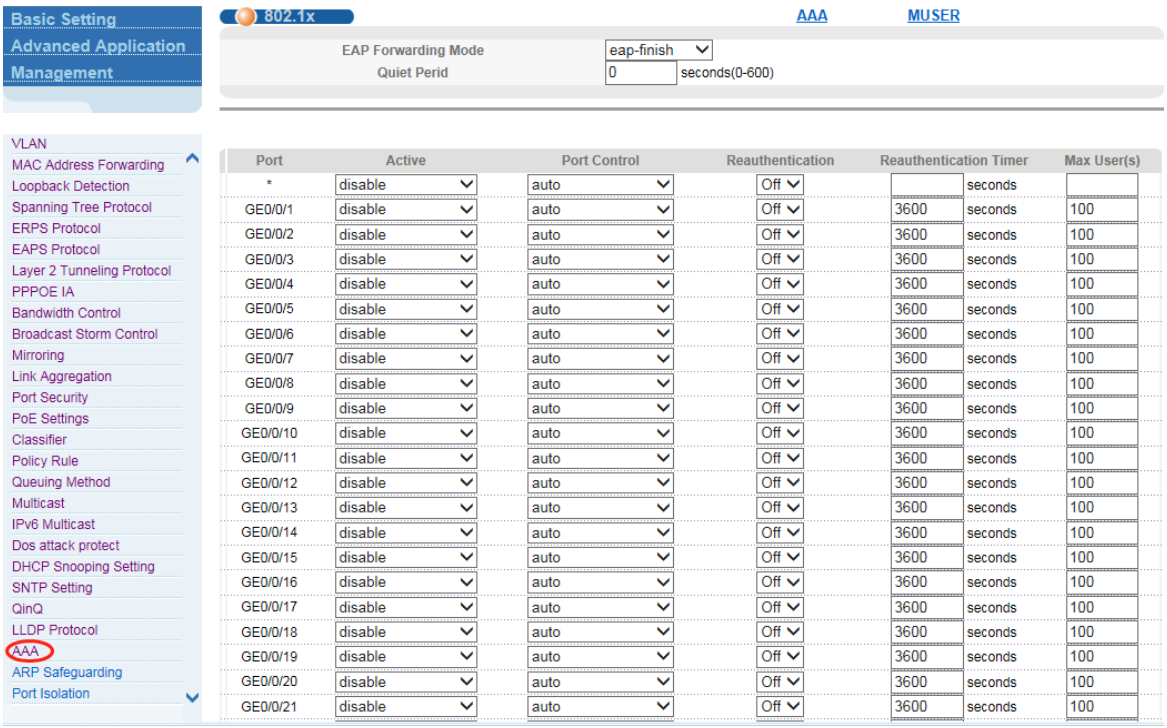
Figure 4-94 LLDP Setting



4.3.26 AAA

Select **Advanced Application > AAA** to configure AAA.

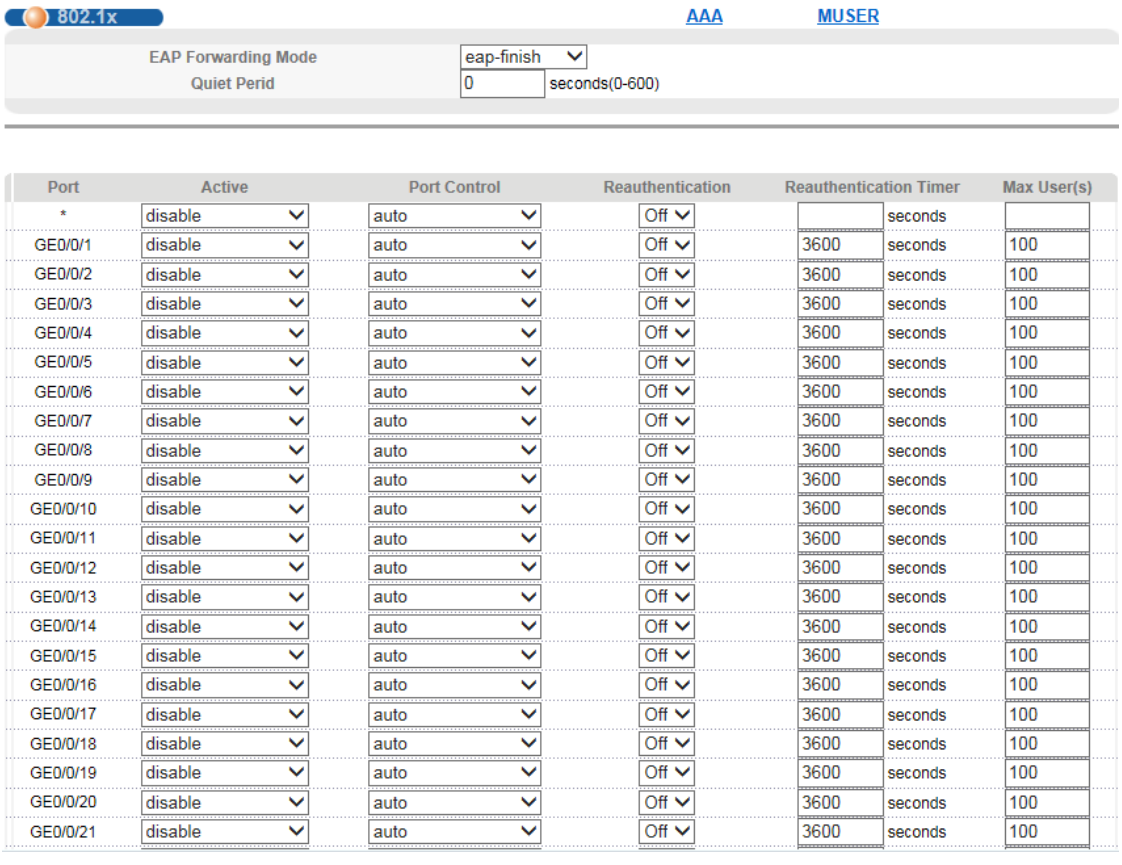
Figure 4-95 AAA



4.3.26.2 802.1x

Select **Advanced Application > AAA > 802.1x** to configure 802.1x.

Figure 4-96 802.1X



Parameter Description

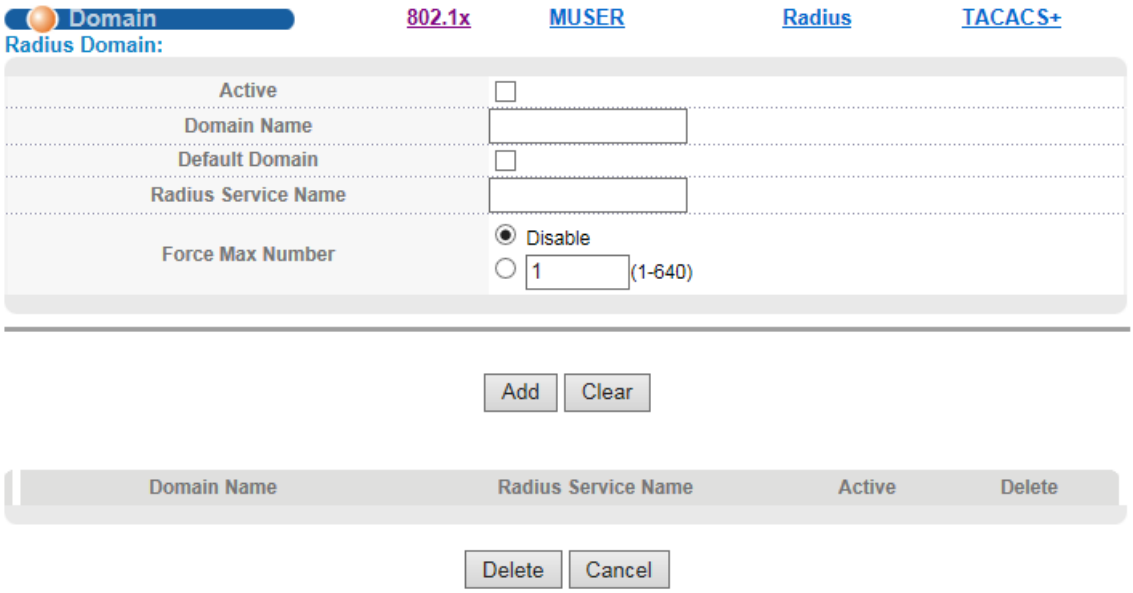
Table 4-35 802.1X parameter description

Parameter	Description
EAP Forwarding Mode	EAP Forwarding Mode : eap-finish, Eap-tansfer.
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.

4.3.26.3 Radius Domain

Select **Advanced Application > AAA > Radius Domain** to configure Radius Domain.

Figure 4-97 Radius Domain



Parameter Description

Table 4-36 Radius

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.

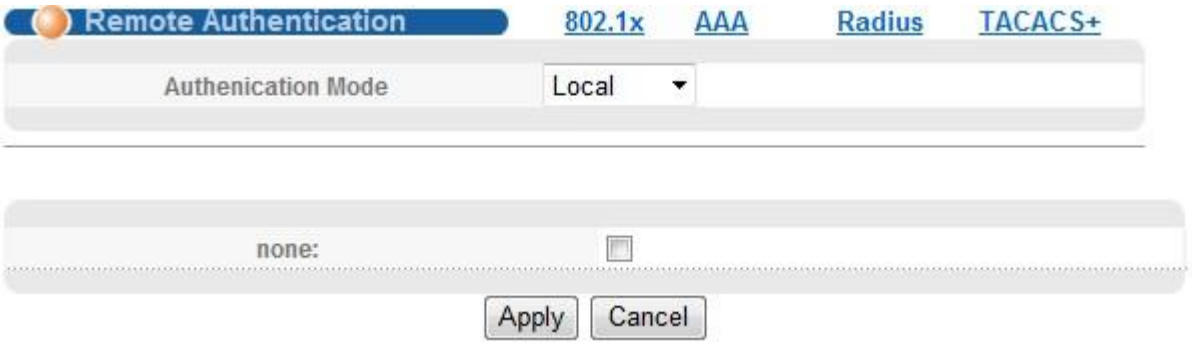
Instructions

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.

4.3.26.4 Remote Authentication

Select **Advanced Application > AAA > Remote Authentication** to configure Remote Authentication.

Figure 4-98 Remote Authentication



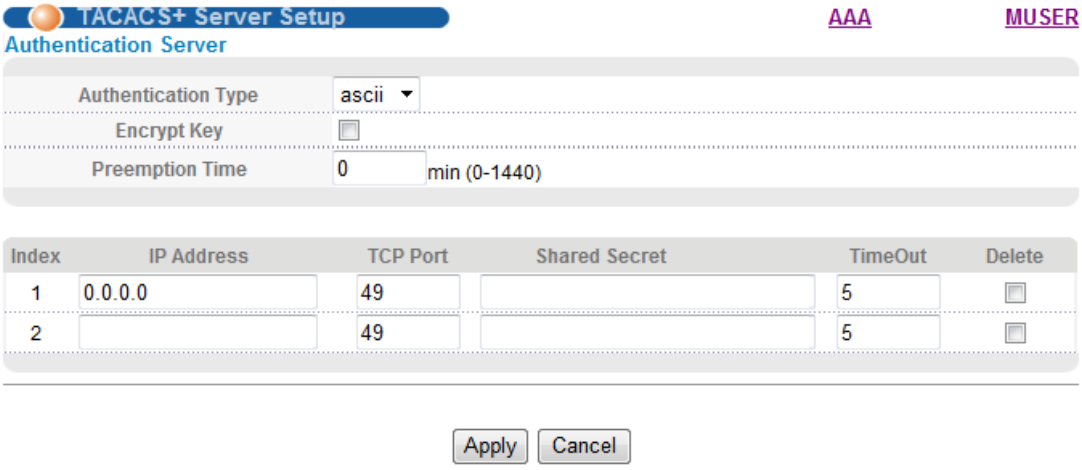
Parameter Description

Authentication Mode: Local, Radius, Tacacs+.

4.3.26.5 TACACS+ Server Setup

Select **Advanced Application > AAA > TACACS+ Server Setup** to configure TACACS+ Server Setup.

Figure 4-99 TACACS+ Server Setup



Parameter Description

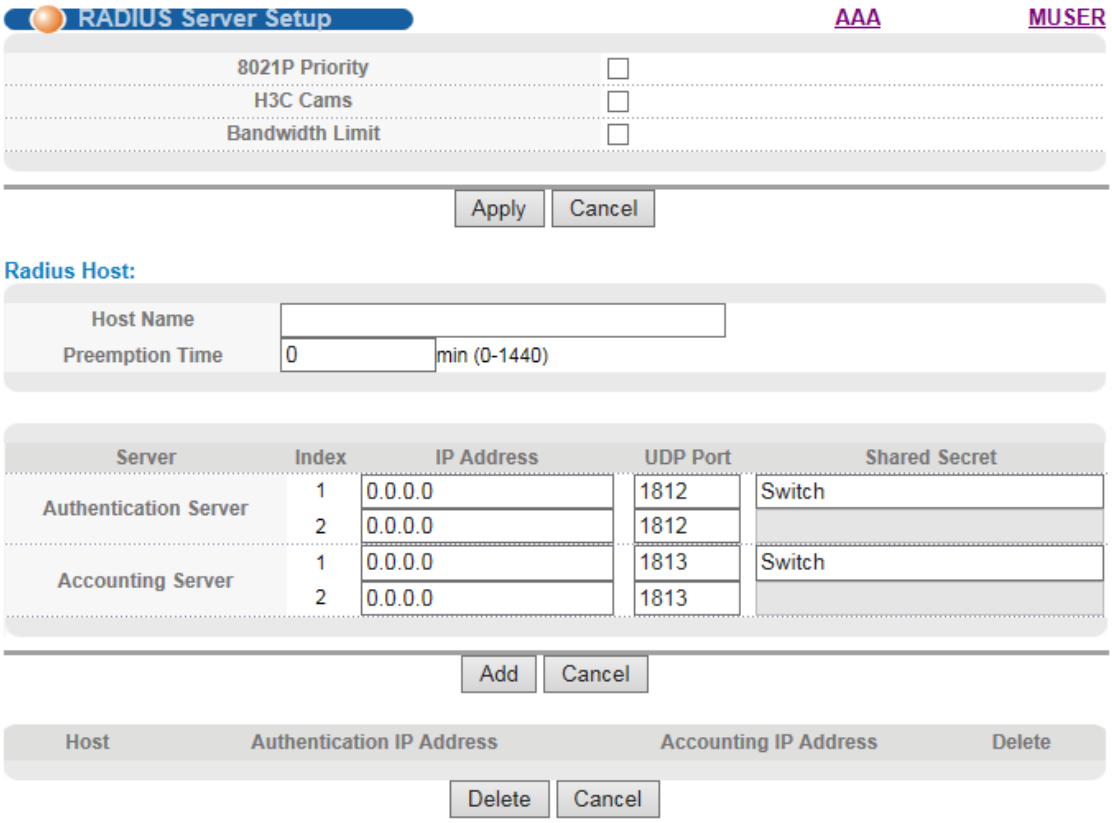
Table 4-37 TACACS+ Server Setup parameter description

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

4.3.26.6 Radius Server Setup

Select **Advanced Application > AAA > Radius Server Setup** to configure Radius Server Setup.

Figure 4-100 Radius Server Setup



Parameter Description

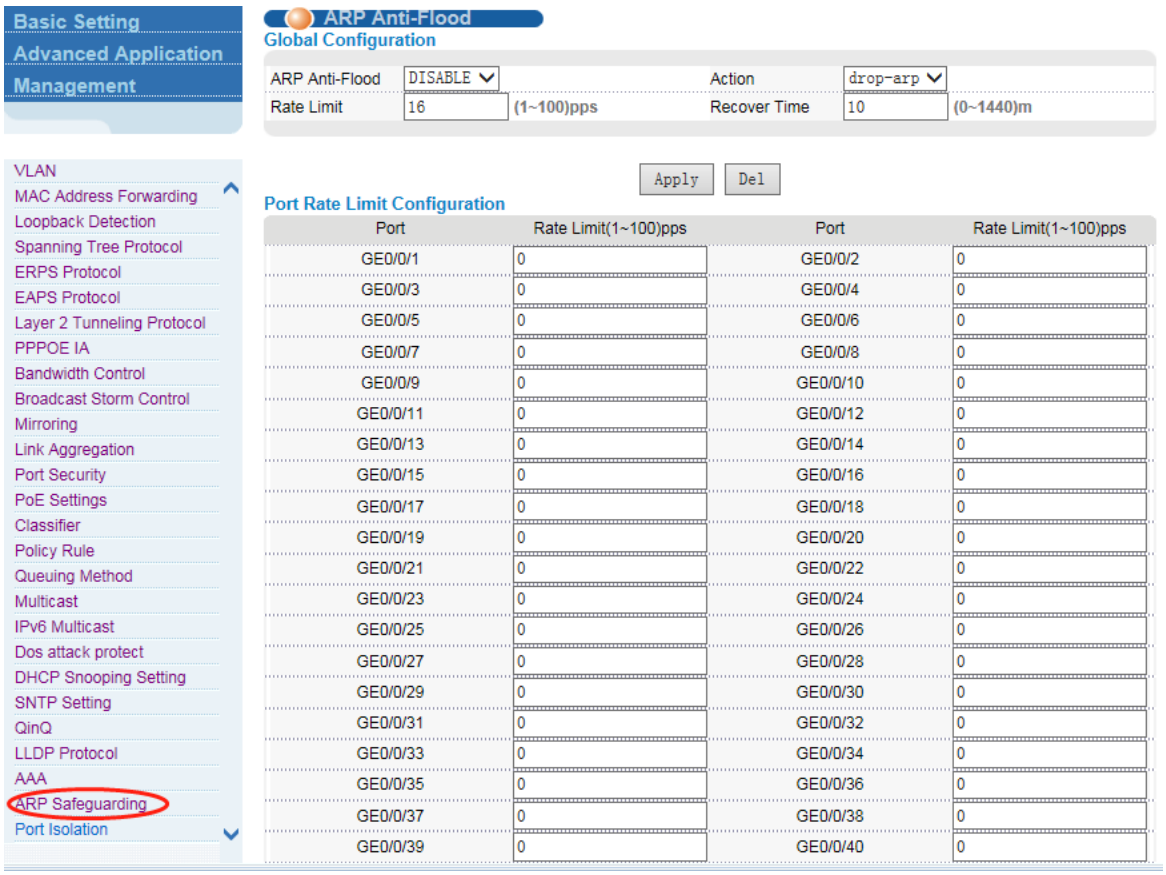
Table 4-38 RADIUS Server Setup parameter description

Parameter	Description
8021P Priority	After this function is turned on, if the user is authenticated, 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 is authenticated, it will modify the Bandwidth of the user's port.

4.3.27 ARP Safeguarding

Select **Advanced Application > ARP Safeguarding** to configured to prevent arp flooding.

Figure 4-101 ARP Safeguarding



Parameter Description

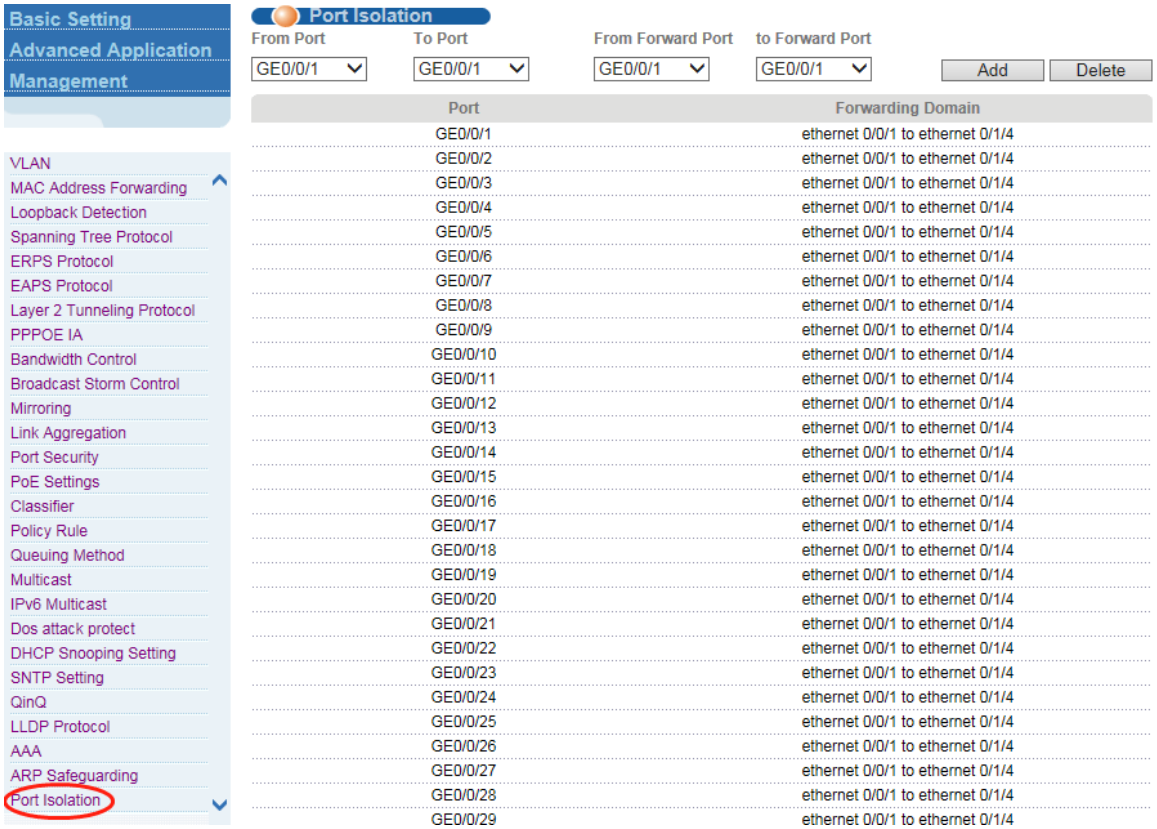
Table 4-39 ARP Safeguarding parameter description

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.

4.3.28 Port Isolation

Select **Advanced Application > Port Isolation** to configured to port isolation.

Figure 4-102 Port Isolation



4.4 Management

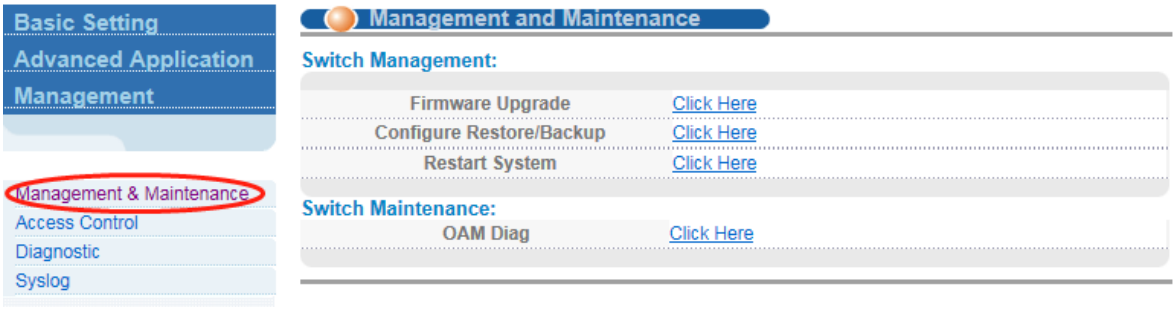
Select **Management**, and the following page appears. There are "Management & Maintenance", "Access Control ", "Diagnostic", "Syslog", configuration web pages.

Figure 4-103 Management

4.4.2 Management &Maintenance

Select **Management > Management & Maintenance** to upgrade firmware, restart and maintenance switch.

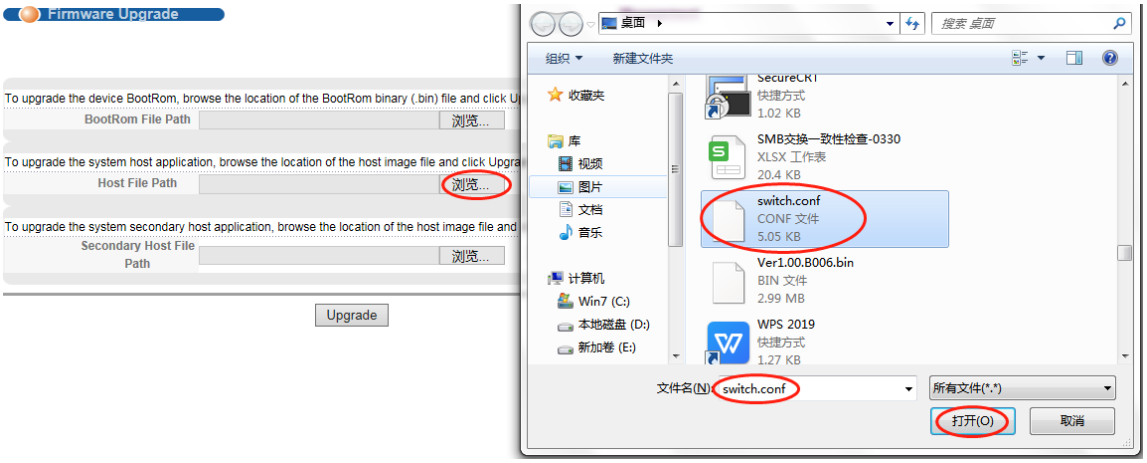
Figure 4-104 Management & Maintenance



Configuration example

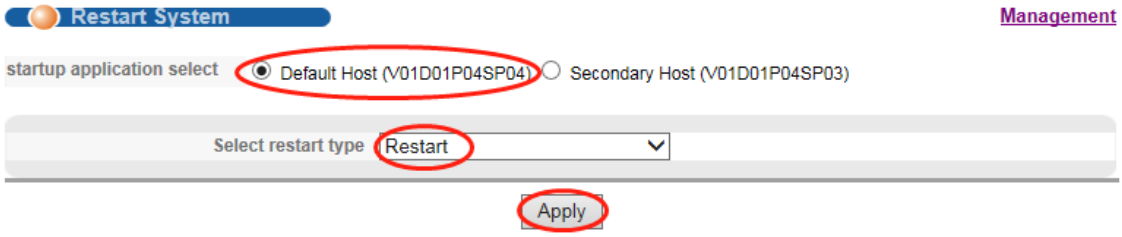
- Firmware Upgrade

Figure 4-103 Configuration example(1)



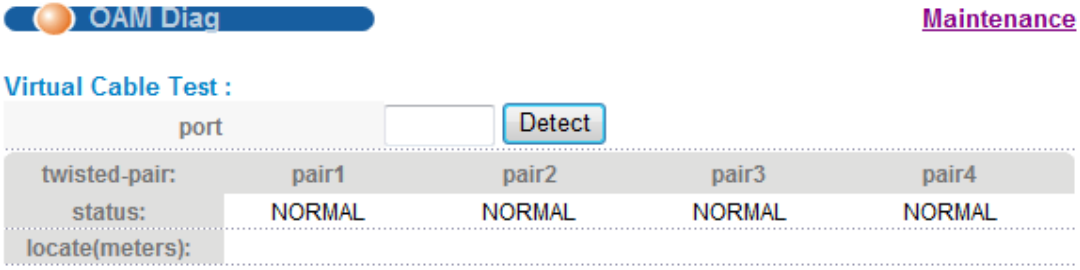
- Restart system. Restart type: Restart, Restart with Factory Defaults.

Figure 4-104 Configuration example(2)



- OAM Diag, Virtual cable can be tested.

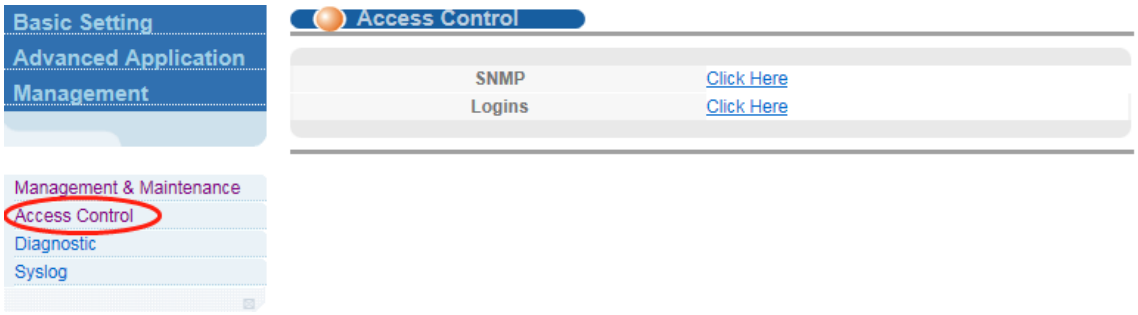
Figure 4-105 Configuration example(3)



4.4.3 Access Control

Select **Management > Access Control** to set SNMP and Logins.

Figure 4-106 Access Control



4.4.3.1 SNMP

Select **Management > Access Control > SNMP** to configure SNMP.

Figure 4-107 SNMP

Parameter Description

Table 4-40 SNMP 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.

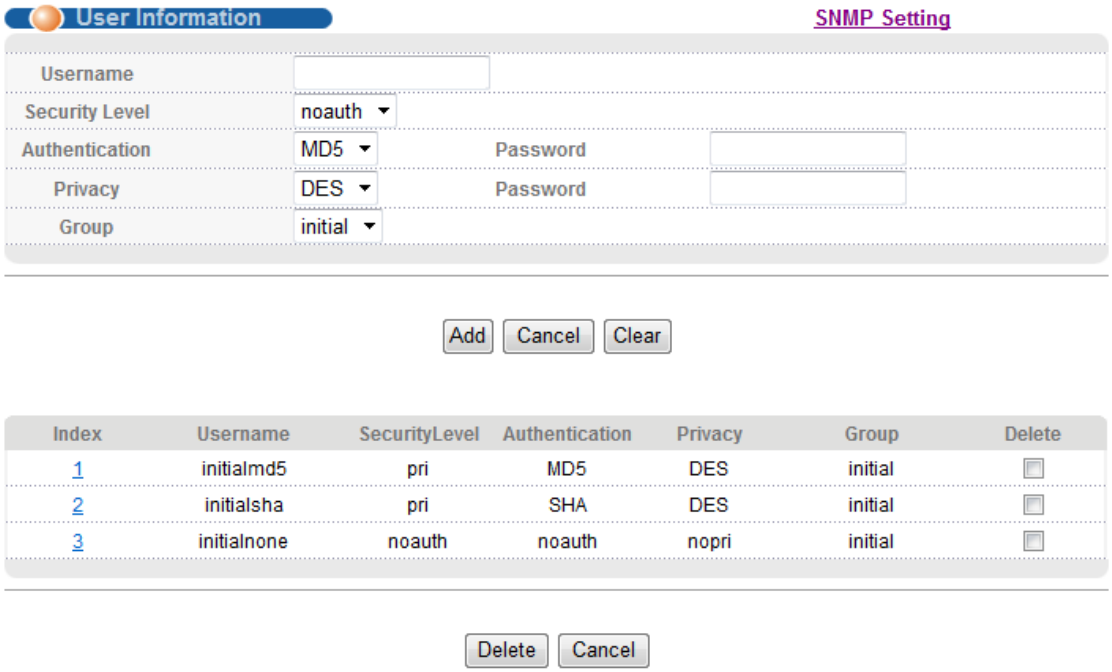
Instructions

Multiple different SNMP hosts can be configured to receive trap messages. The time to trigger the trap message is: Linkup/LinkDown of the port, cold-start (warm restart)/warm-start (warm restart) of the device.

4.4.3.2 User Information

Select **Management > Access Control > User Information** to add user, set Security Level, Authentication, Privacy, Group, Password.

Figure 4-108 User Information



Parameter Description

Table 4-41 User Information parameter description

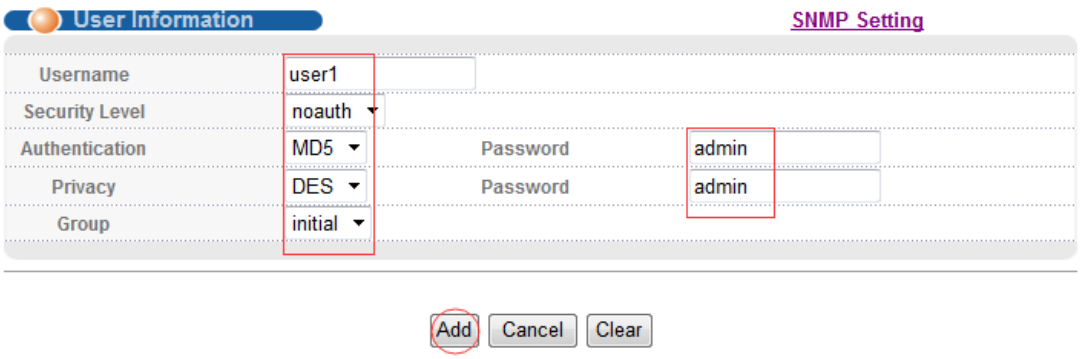
Parameter	Description
Username	SNMP username.
Security Level	Noauth, auth, pri.
Authentication	MD5, SHA.
Privacy	DES Privacy.

Group	User group name.
Password	Encrypted password.

Configuration example

Such as: Add group initial, add username user1.

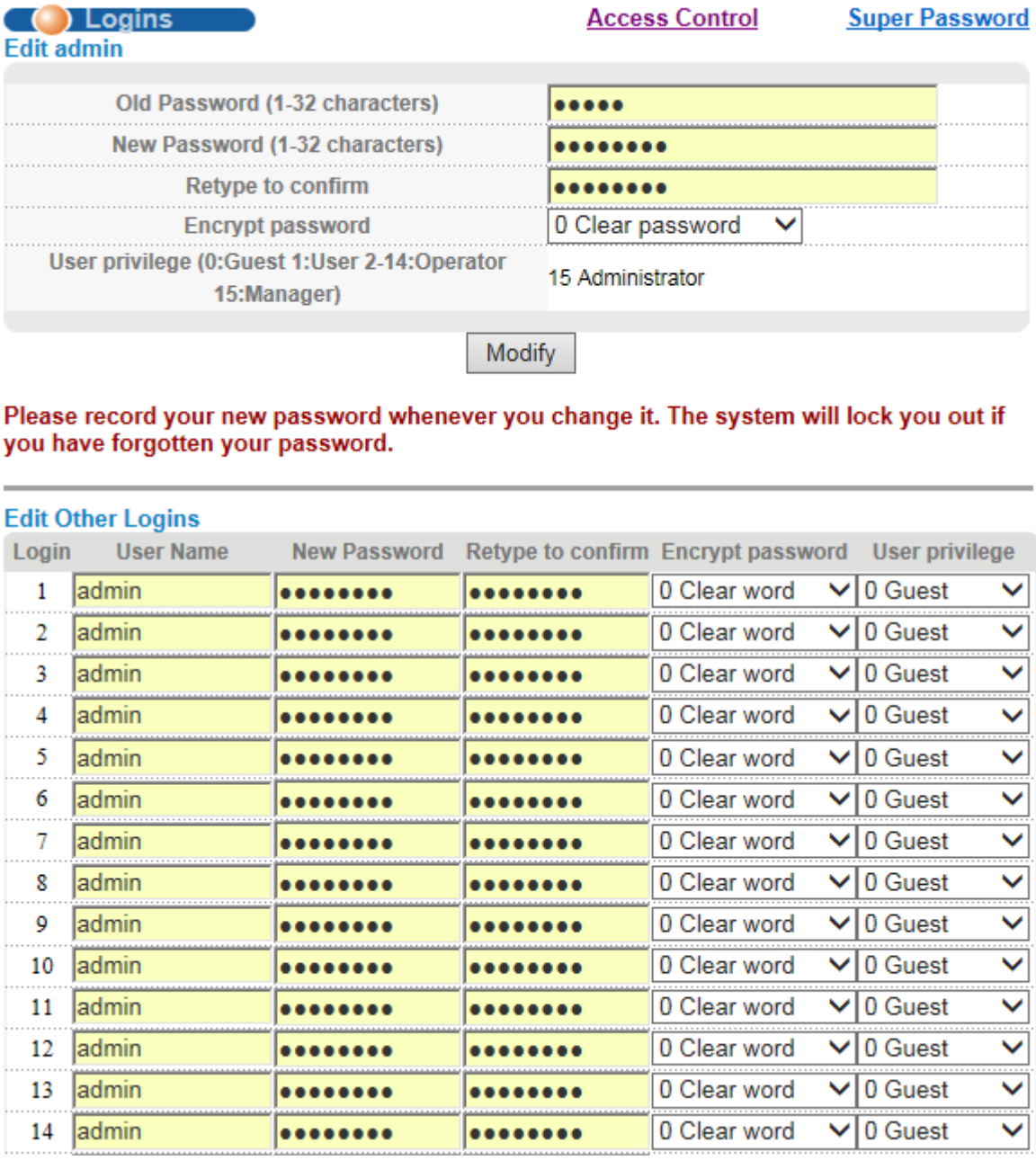
Figure 4-109 Configuration example



4.4.3.3 Logins

Select **Management > Access Control > Logins** to modify admin password, configurable ordinary users.

Figure 4-110 Logins



Parameter Description

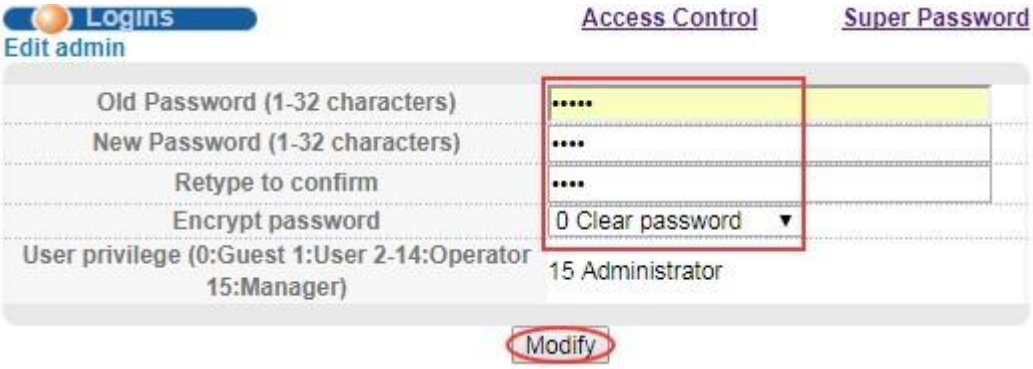
User privilege:

- 0~1: Normal
- 2~14: administrator

Configuration example

Change the password of the administrator "admin" to "1234".

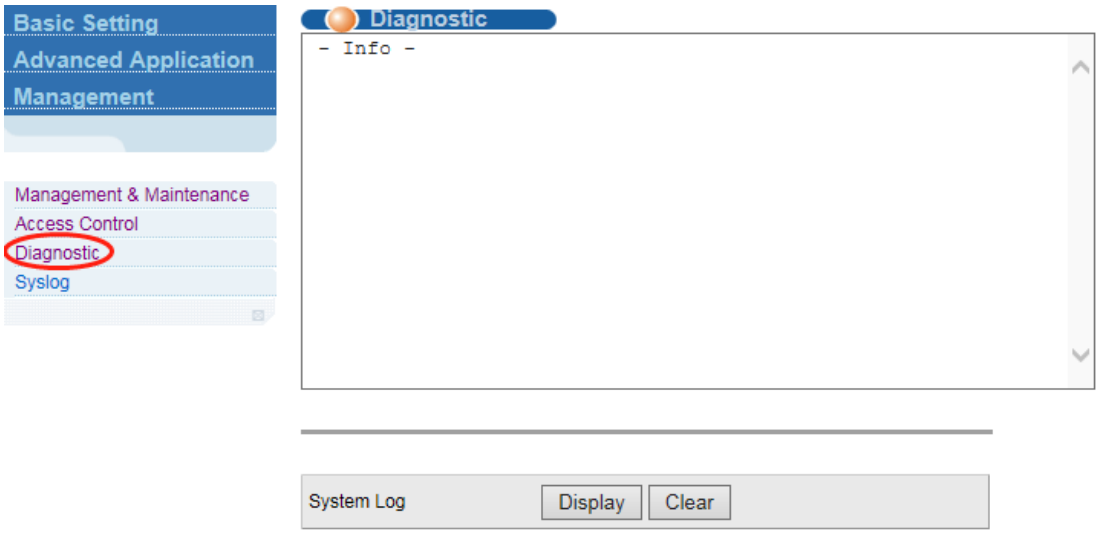
Figure 4-111 Configuration example



4.4.4 Diagnostic

Select **Management > Diagnostic** to display or clear system log.

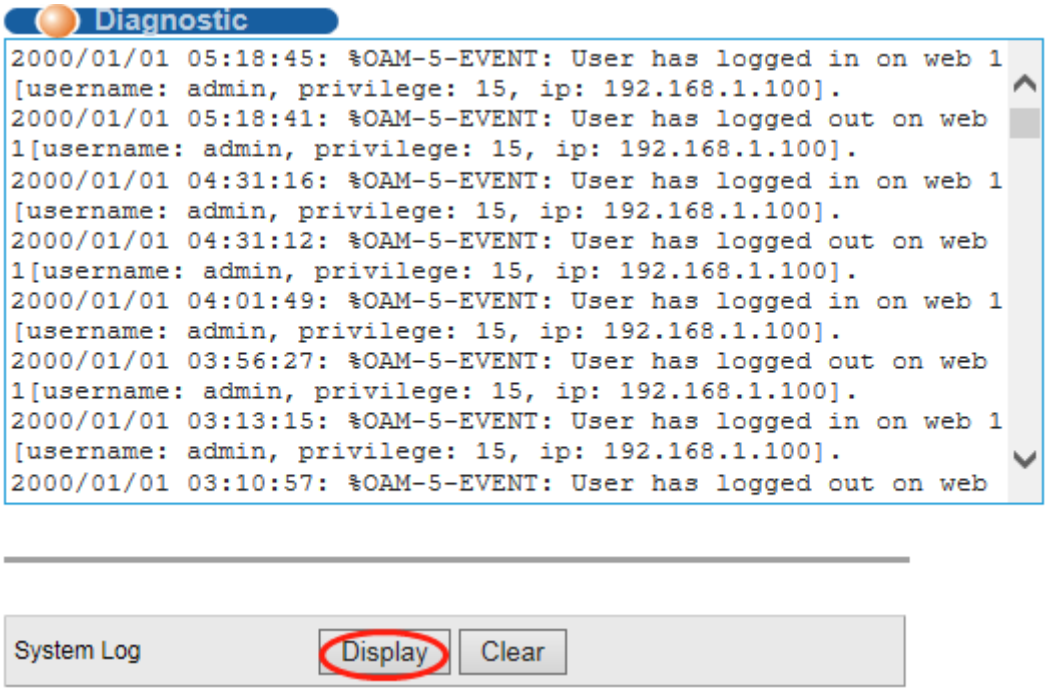
Figure 4-112 Diagnostic



Configuration example

Such as: Display System Log.

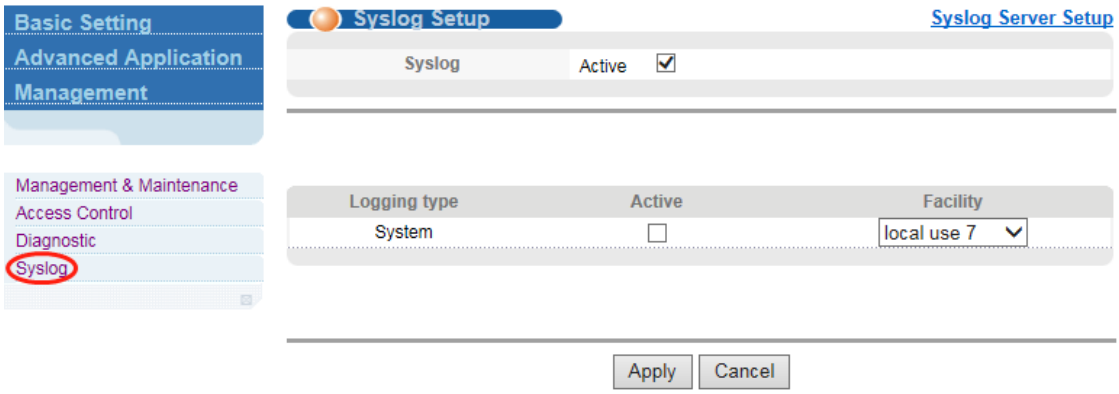
Figure 4-113 Configuration example



4.4.5 Syslog

Select **Management > Syslog** to configure syslog.

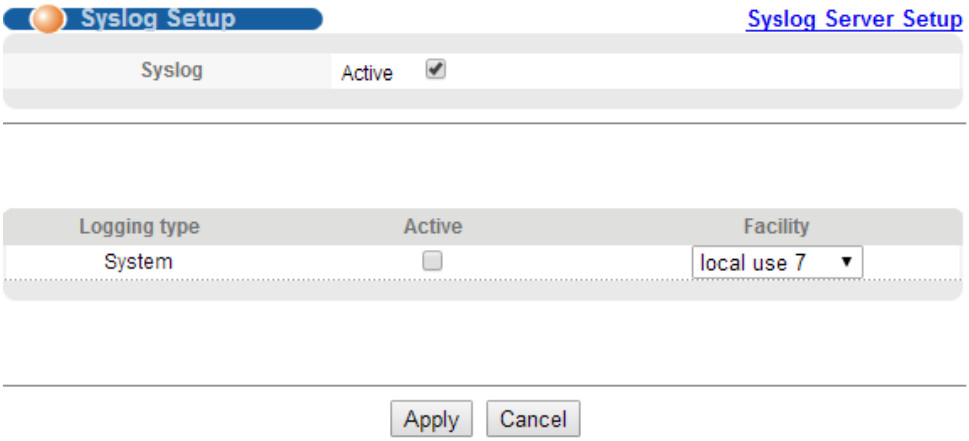
Figure 4-105 Syslog



4.4.5.2 Syslog Setup

Select **Management > Syslog > Syslog Setup** to start the logging function globally and the logging function of the corresponding module.

Figure 4-114 Syslog Setup



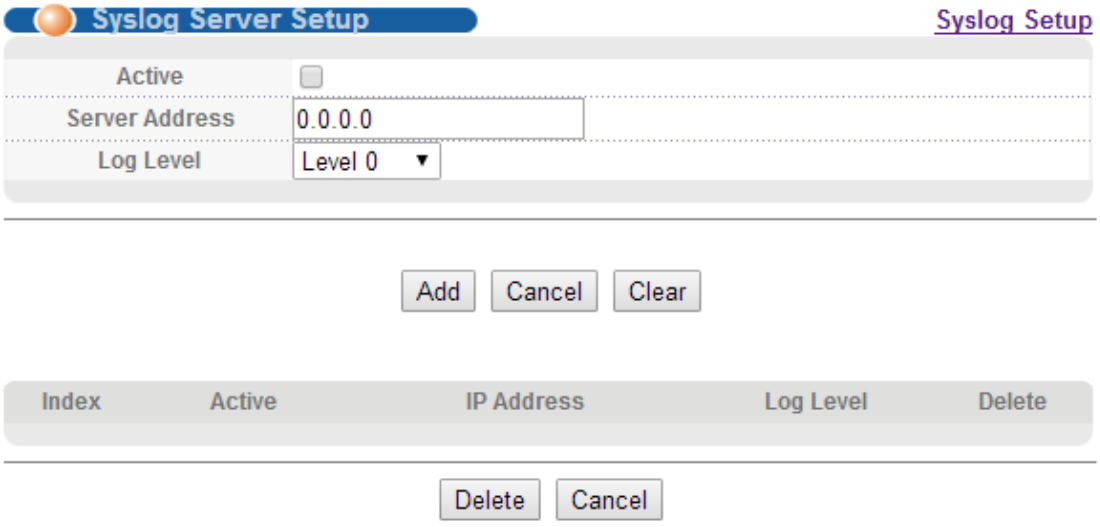
Parameter Description

Facility: local use 0-7, kernel, userlevel, mail, system, sercurity_1-2, sysogd, lineprinter, Networknews, uucp, clock_1-2, ftp, logaudit, logalert.

4.4.5.3 Syslog Server Setup

Select **Management > Syslog > Syslog Server Setup** to set syslog server.

Figure 4-115 Syslog Server Setup



Parameter Description

Table 4-42 Syslog Server Setup 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.

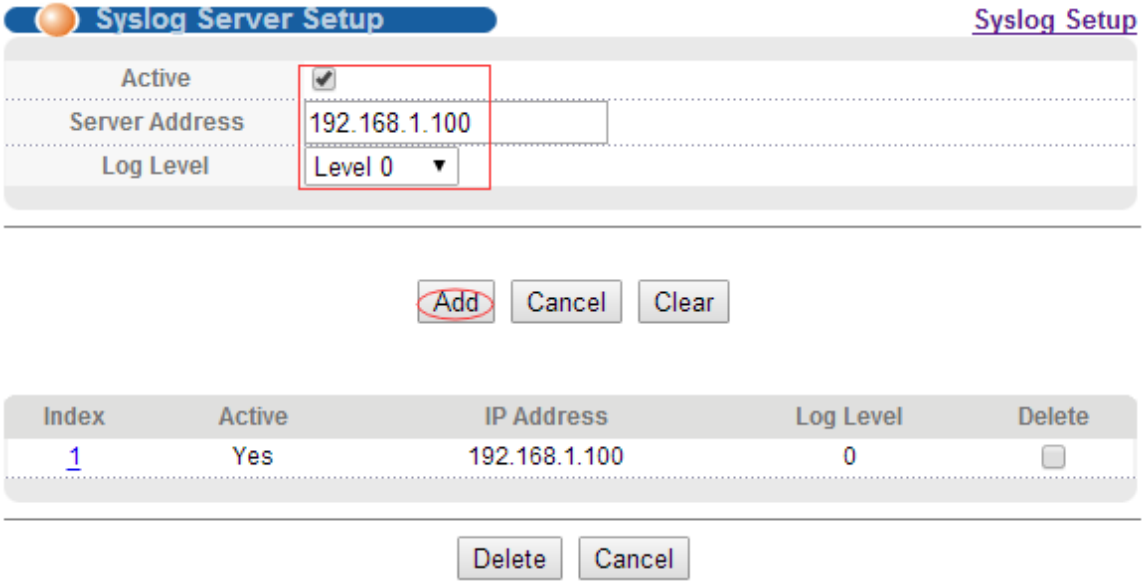
Instructions

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.

Figure 4-116 Configuration example



Appendix 1 Cybersecurity Recommendations

Cybersecurity is more than just a buzzword: it's something that pertains to every device that is connected to the internet. IP video surveillance is not immune to cyber risks, but taking basic steps toward protecting and strengthening networks and networked appliances will make them less susceptible to attacks. Below are some tips and recommendations on how to create a more secured security system.

Mandatory actions to be taken for basic device network security:

1. **Use Strong Passwords**

   Please refer to the following suggestions to set passwords:

   - The length should not be less than 8 characters;
   - Include at least two types of characters; character types include upper and lower case letters, numbers and symbols;
   - Do not contain the account name or the account name in reverse order;
   - Do not use continuous characters, such as 123, abc, etc.;
   - Do not use overlapped characters, such as 111, aaa, etc.;

2. **Update Firmware and Client Software in Time**

   - According to the standard procedure in Tech-industry, we recommend to keep your device (such as NVR, DVR, IP camera, etc.) firmware up-to-date to ensure the system is equipped with the latest security patches and fixes. When the device is connected to the public network, it is recommended to enable the "auto-check for updates" function to obtain timely information of firmware updates released by the manufacturer.
   - We suggest that you download and use the latest version of client software.

"Nice to have" recommendations to improve your device network security:

1. **Physical Protection**

   We suggest that you perform physical protection to device, especially storage devices. For example, place the device in a special computer room and cabinet, and implement well-done access control permission and key management to prevent unauthorized personnel from carrying out physical contacts such as damaging hardware, unauthorized connection of removable device (such as USB flash disk, serial port), etc.

2. **Change Passwords Regularly**

   We suggest that you change passwords regularly to reduce the risk of being guessed or cracked.

3. **Set and Update Passwords Reset Information Timely**

   The device supports password reset function. Please set up related information for password reset in time, including the end user's mailbox and password protection questions. If the

information changes, please modify it in time. When setting password protection questions, it is suggested not to use those that can be easily guessed.

4. **Enable Account Lock**

   The account lock feature is enabled by default, and we recommend you to keep it on to guarantee the account security. If an attacker attempts to log in with the wrong password several times, the corresponding account and the source IP address will be locked.

5. **Change Default HTTP and Other Service Ports**

   We suggest you to change default HTTP and other service ports into any set of numbers between 1024~65535, reducing the risk of outsiders being able to guess which ports you are using.

6. **Enable HTTPS**

   We suggest you to enable HTTPS, so that you visit Web service through a secure communication channel.

7. **MAC Address Binding**

   We recommend you to bind the IP and MAC address of the gateway to the device, thus reducing the risk of ARP spoofing.

8. **Assign Accounts and Privileges Reasonably**

   According to business and management requirements, reasonably add users and assign a minimum set of permissions to them.

9. **Disable Unnecessary Services and Choose Secure Modes**

   If not needed, it is recommended to turn off some services such as SNMP, SMTP, UPnP, etc., to reduce risks.

   If necessary, it is highly recommended that you use safe modes, including but not limited to the following services:

   - SNMP: Choose SNMP v3, and set up strong encryption passwords and authentication passwords.
   - SMTP: Choose TLS to access mailbox server.
   - FTP: Choose SFTP, and set up strong passwords.
   - AP hotspot: Choose WPA2-PSK encryption mode, and set up strong passwords.

10. **Audio and Video Encrypted Transmission**

    If your audio and video data contents are very important or sensitive, we recommend that you use encrypted transmission function, to reduce the risk of audio and video data being stolen during transmission.

    Reminder: encrypted transmission will cause some loss in transmission efficiency.

11. **Secure Auditing**

    - Check online users: we suggest that you check online users regularly to see if the device is logged in without authorization.

- Check device log: By viewing the logs, you can know the IP addresses that were used to log in to your devices and their key operations.

12. **Network Log**

    Due to the limited storage capacity of the device, the stored log is limited. If you need to save the log for a long time, it is recommended that you enable the network log function to ensure that the critical logs are synchronized to the network log server for tracing.

13. **Construct a Safe Network Environment**

    In order to better ensure the safety of device and reduce potential cyber risks, we recommend:

    - Disable the port mapping function of the router to avoid direct access to the intranet devices from external network.
    - The network should be partitioned and isolated according to the actual network needs. If there are no communication requirements between two sub networks, it is suggested to use VLAN, network GAP and other technologies to partition the network, so as to achieve the network isolation effect.
    - Establish the 802.1x access authentication system to reduce the risk of unauthorized access to private networks.
    - Enable IP/MAC address filtering function to limit the range of hosts allowed to access the device.