28 ports
Layer 2 Industrial Ethernet Switch
User Manual

Document Version: 01

Issue Date: 12/28/2022

Preface

Layer 2 Industrial Ethernet Switch User Manual has introduced this switch:

- Product features
- Product network management configuration
- Overview of related principles of network management

Audience

This manual applies to the following engineers:

- Network administrators
- Technical support engineers
- Network engineer

Text Format Convention

Format	Description
" "	Words with “” represent the interface words. Such as: “Port No.“.
>	Multi-level path is separated by ">". Such as opening the local connection path description: Open "Control Panel> Network Connection> Local Area Connection".
Light Blue Font	It represents the words clicked to achieve hyperlink. The font color is as follows: ‘Light Blue’.

Symbols

Format	Description
 Notice	Remind the announcements in the operation, improper operation may result in data loss or equipment damage.
 Warning	Pay attention to the notes on the mark, improper operation

Format	Description
	may cause personal injury.
 Note	Conduct a necessary supplements and explanations for the description of operation content.
 Key	Configuration, operation, or tips for device usage.
 Tips	Pay attention to the operation or information to ensure success device configuration or normal working.

Revision Record

Version No.	Date	Revision note
01	12/28/2022	Product release

Contents

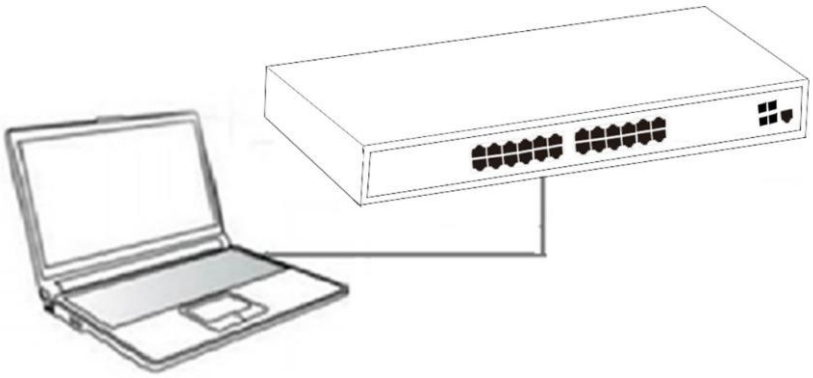
PREFACE 1
CONTENTS I
1 HOW TO LOGIN THE SWITCH 1
1.1 SWITCH TO END NODE 1
1.2 HOW TO LOGIN THE SWITCH 1
2 WEB CONFIGURATION GUIDE 3
2.1 BASIC SETTING 3
2.1.1 System Info 4
2.1.2 General Setup 5
2.1.3 IP Setup 5
2.1.4 Port Setup 8
2.2 ADVANCED APPLICATION 10
2.2.1 VLAN 11
2.2.2 MAC Address Forwarding 17
2.2.3 Loopback Detection 19
2.2.4 Spanning Tree Protocol 20
2.2.5 Bandwidth Control 27
2.2.6 Broadcast Storm Control 29
2.2.7 Mirroring 30
2.2.8 Link Aggregation 32
2.2.9 POE Settings 36
2.2.10 Classifier 38
2.2.11 Policy Rule 39
2.2.12 Queuing Method 40
2.2.13 Multicast 42
2.2.14 IPv6 Multicast 46
2.2.15 Dos attack protect 50
2.2.16 DHCP Snooping Setting 51
2.2.17 SNTP Setting 56
2.2.18 LLDP Protocol 58
2.2.19 AAA 60
2.2.20 EEE 67
2.2.21 ARP Safeguarding 68
2.3 MANAGEMENT 69

2.3.1 Management &Maintenance 70
2.3.2 Access Control 71
2.3.3 Diagnostic 76
2.3.4 Syslog 77

1 How to Login the Switch

1.1 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.



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

1.2 How to Login the Switch

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

Parameter	Default Value
Default IP address	192.168.1.254
Default user name	admin123

Default password	admin123

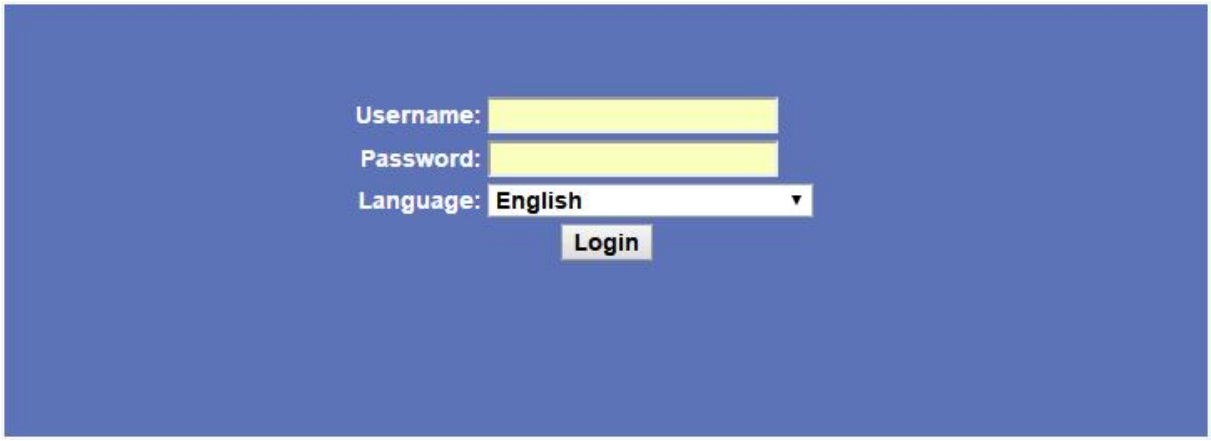
You can log on to the configuration window of the Switch through following steps:

Step 1. .Connect the Switch with the computer NIC interface.

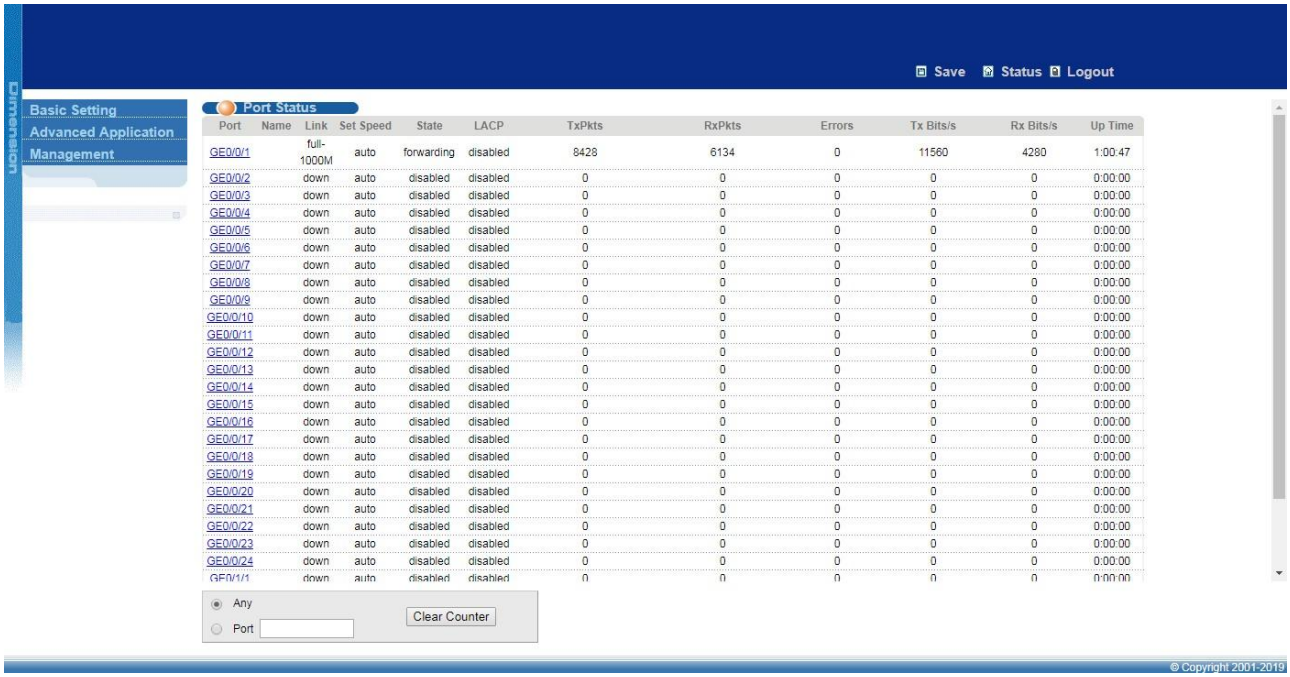
Step 2. Power on the Switch.

Step 3. Check whether the IP address of the computer is within this network segment: 192.168.1.xxx ("xxx" ranges 1~253), for example, 192.168.1.100.

Step 4. Open the browser, and enter http://192.168.1.254 and then press "Enter". The Switch login window appears, as shown below.



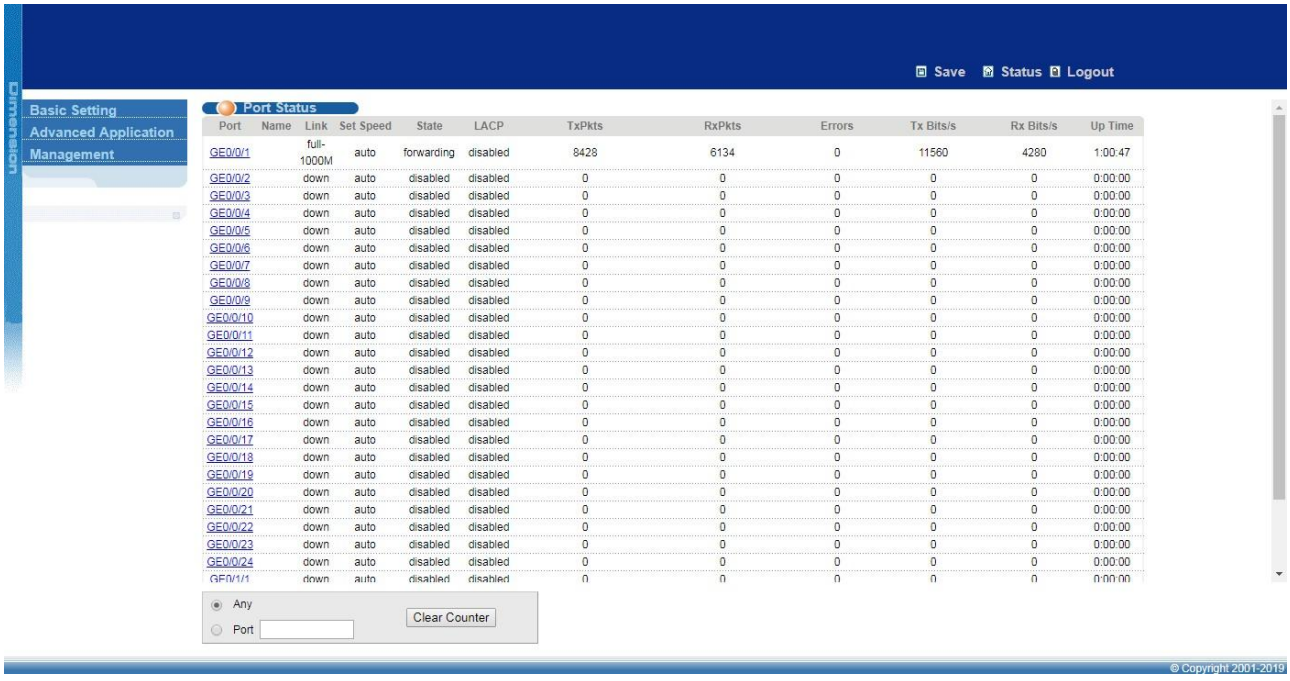
Step 5. Switching language to English .Enter the Username and Password (The factory default Username is admin123 and Password is admin123), and then click "Login" to log in to the Switch configuration window



Step 6. END.

2 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.

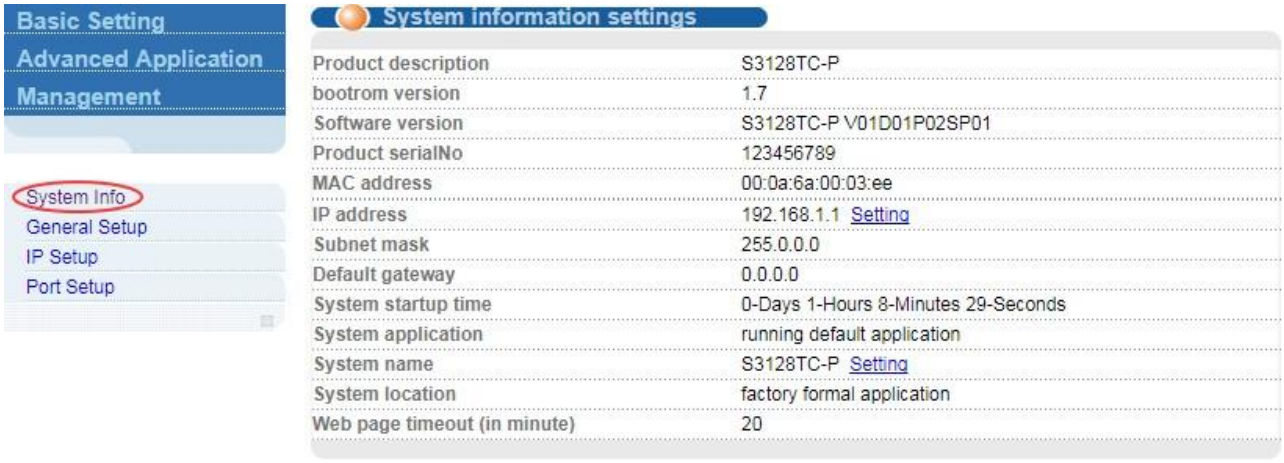


2.1 Basic Setting

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

2.1.1 System Info

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



【Parameter Description】

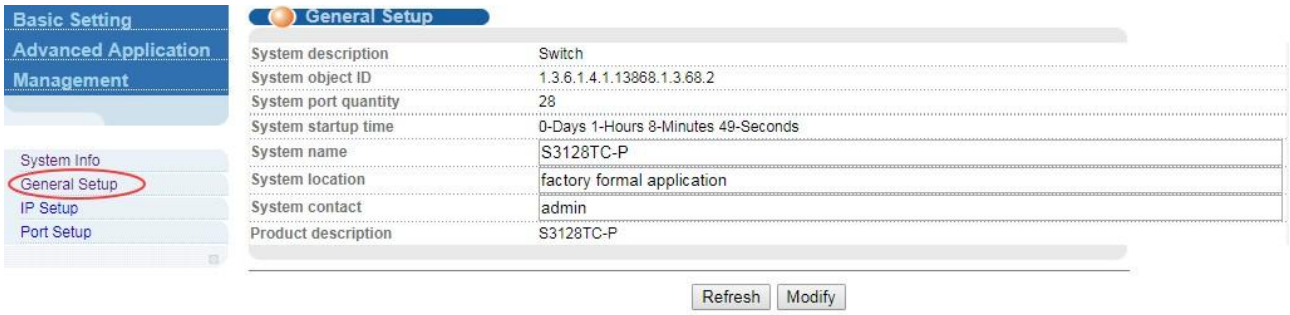
Parameter	Description
IP Address	The management IP of Switch
System name	System name

【Instructions】

You can view and configure Running System status.

2.1.2 General Setup

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

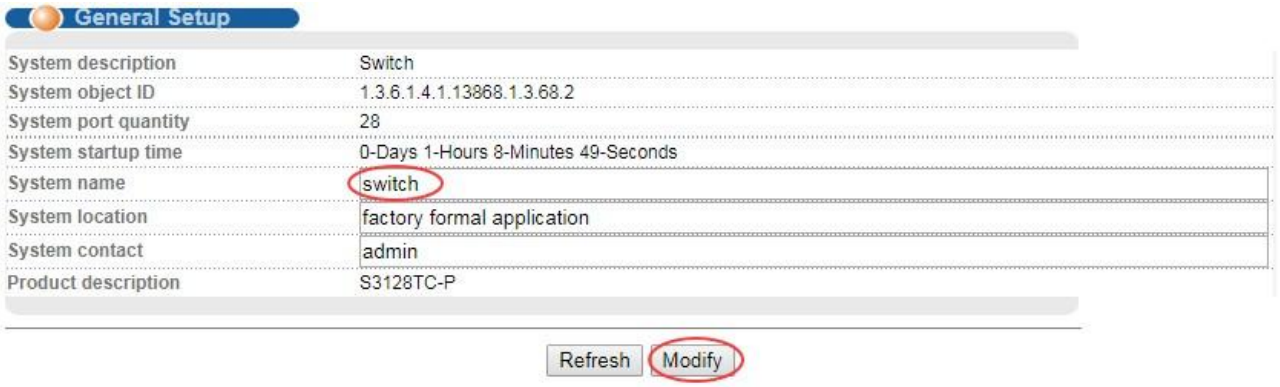


【Parameter Description】

Parameter	Description
System name	System name
System contact	Including company or related URL

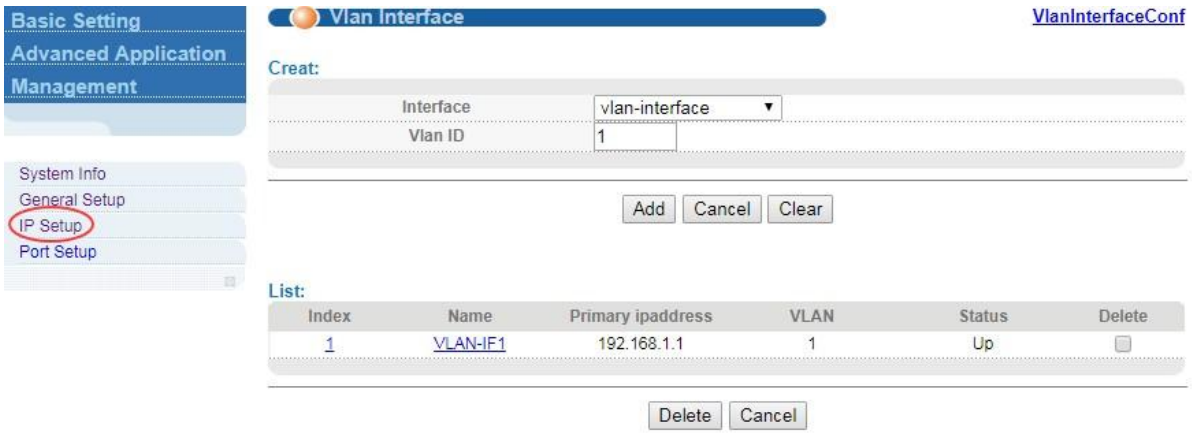
【Configuration example】

Such as: Setting System name as Switch.



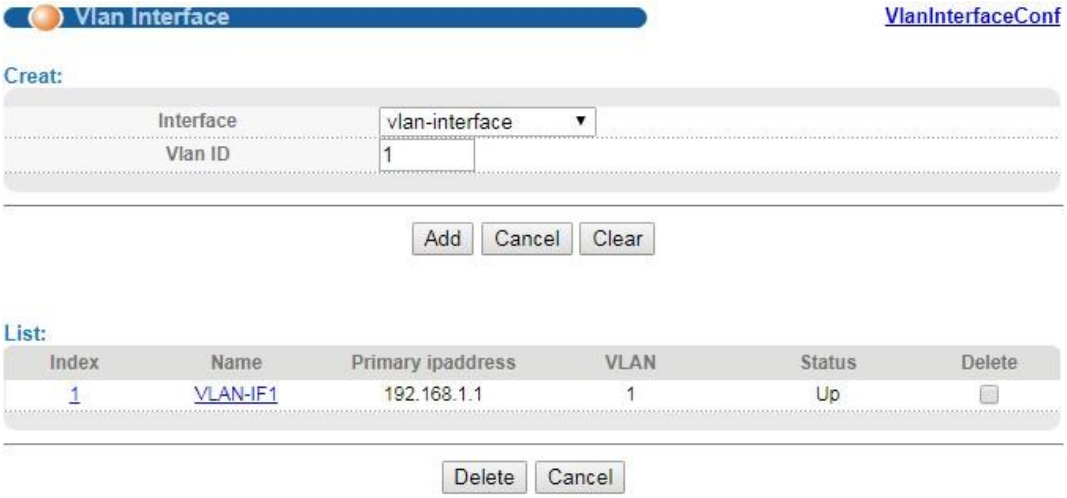
2.1.3 IP Setup

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



2.1.3.1 Vlan interface

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

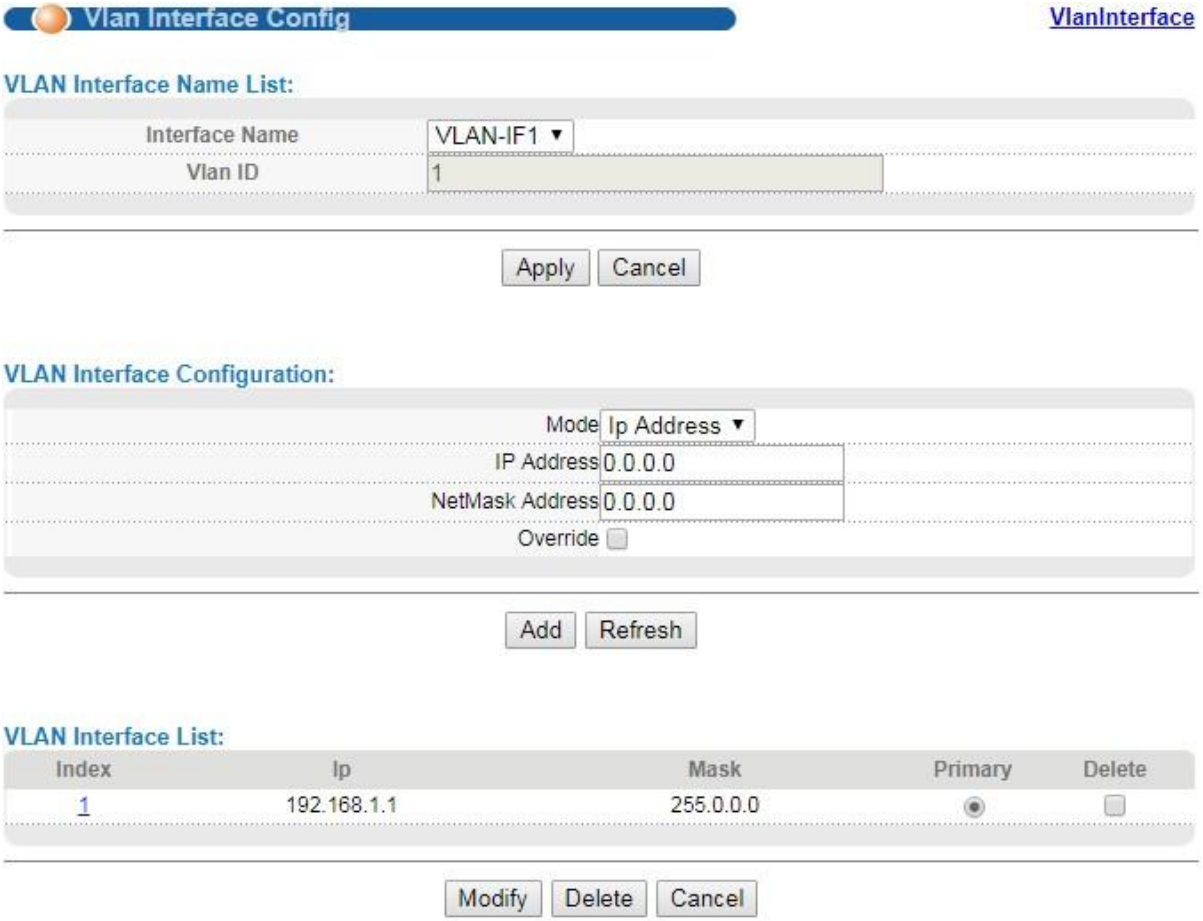


【Parameter Description】

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

2.1.3.2 V lan interface Config

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

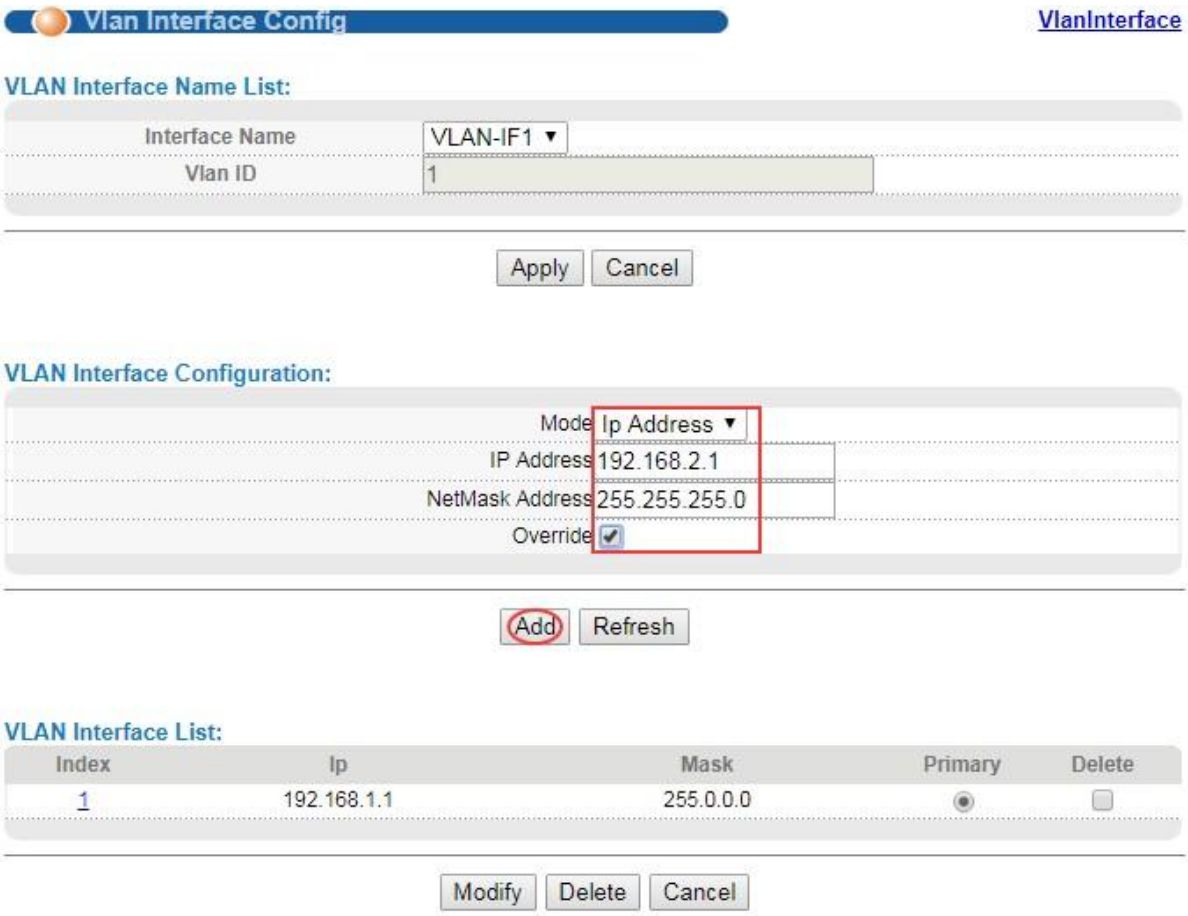


【Parameter Description】

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 former original primary IP or not

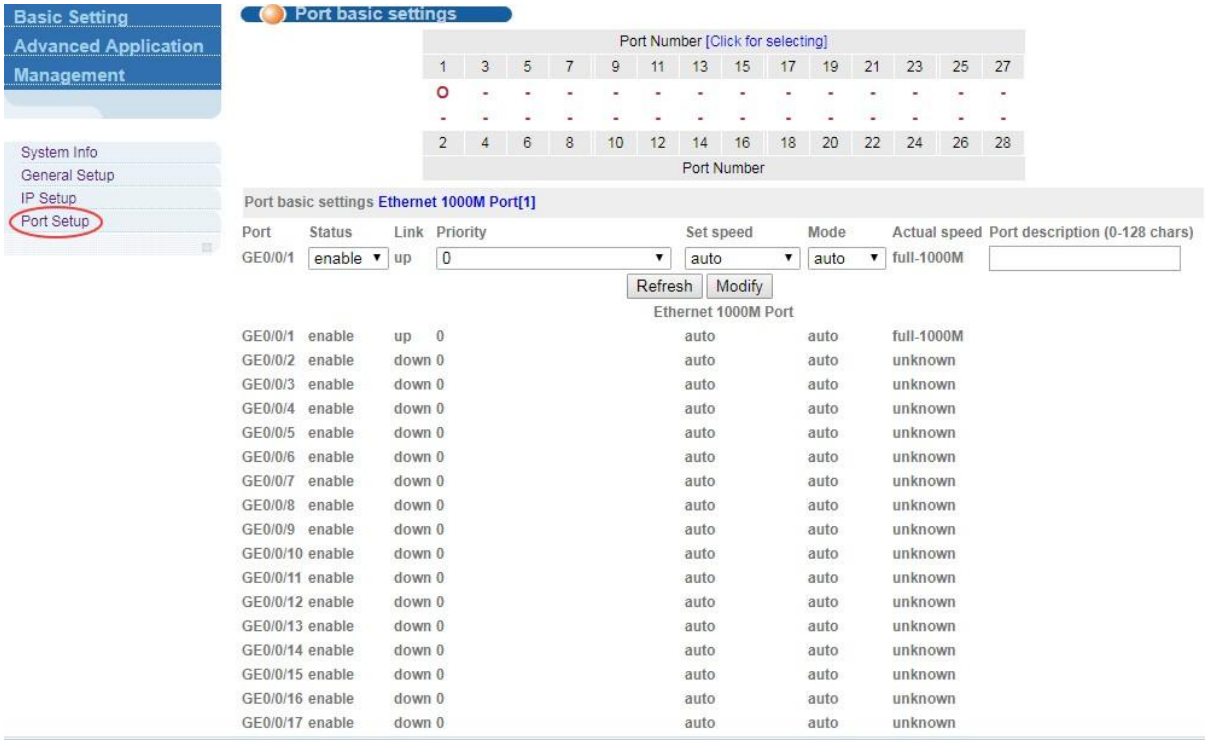
【Configuration example】

Such as: Setting IP address as 192.168.2.1 and mask as 255.255.255.0.And then selecting override.



2.1.4 Port Setup

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



【Parameter Description】

Parameter	Description
Port	Port number
status	Choose whether to close link port
link	Status: Down up
priority	Set port priority, the range of 0-7
Set speed	Choose the following modes: full-100 half-100 auto-100 auto
Mode	Choose the following kinds: auto slave master
Actual speed	The actual speed of the port

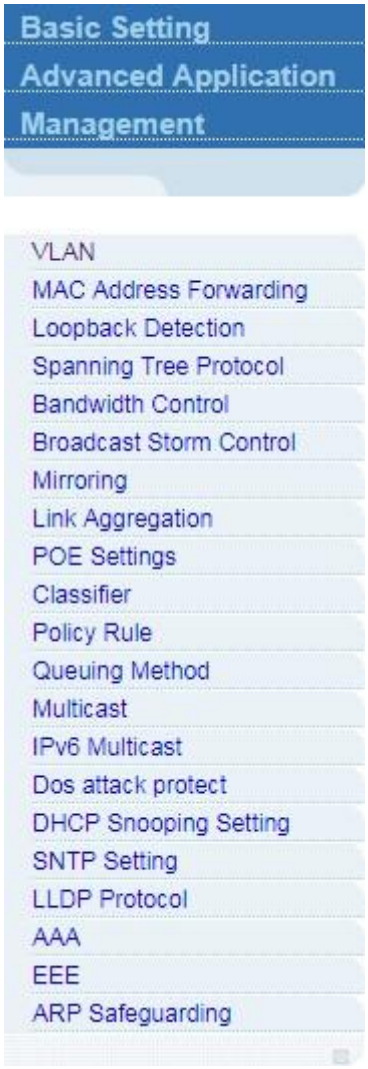
Parameter	Description
Port description	The port is described

【Configuration example】

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

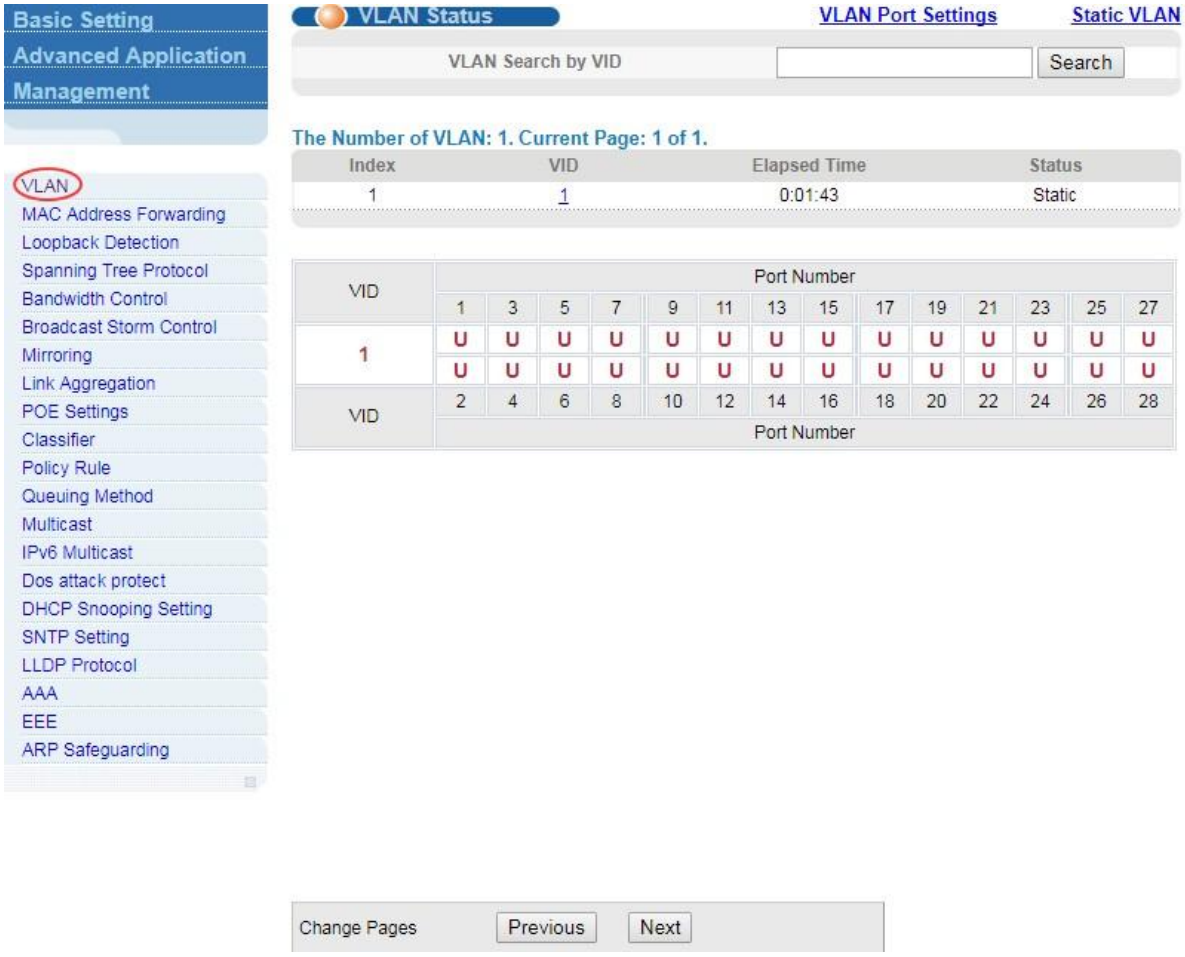
2.2 Advanced Application

Choose Advanced Application, and the following page appears. There are "VLAN", "MAC Address Forwarding", “ Lookback Detection", “Spanning Tree Protocol",“Bandwidth Control", “Broadcast Storm Control", “Mirroring", “Link Aggregation", “POE Settings",“Classifier", “Policy Rule", “Queuing Method", “Multicast", “IPv6 Multicast", “Dos attack protect”, DHCP Snooping Setting" , “SNTP Setting", “LLDP Protocol" , “AAA" ,”EEE” and “ARP Safeguarding” configuration web pages.



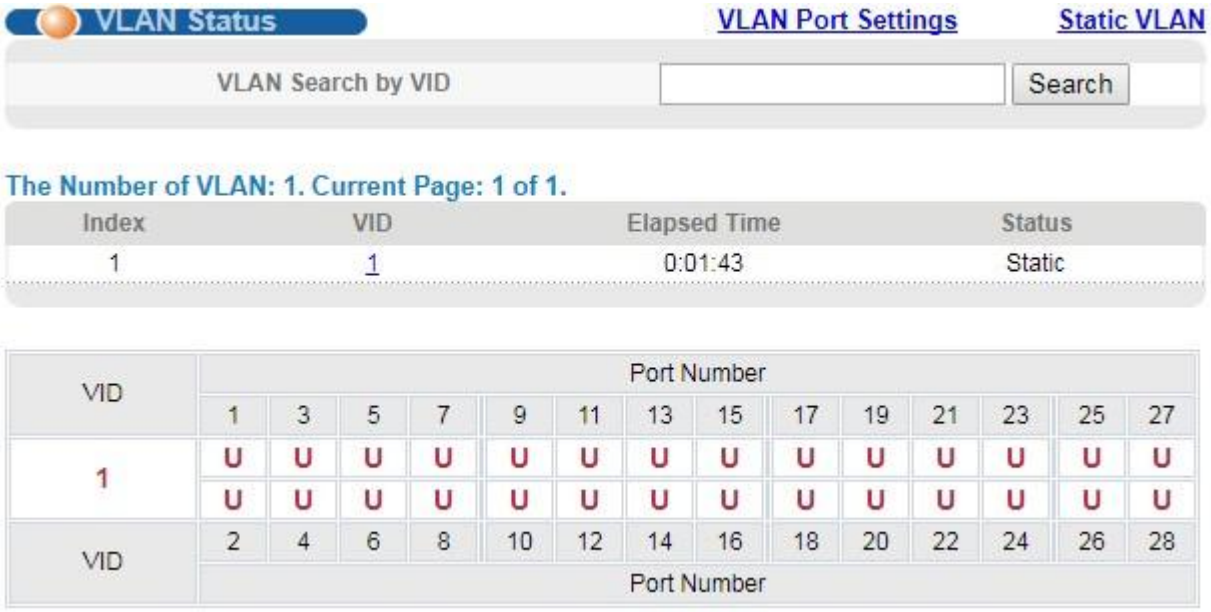
2.2.1 VLAN

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



2.2.1.1 VLAN Status

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

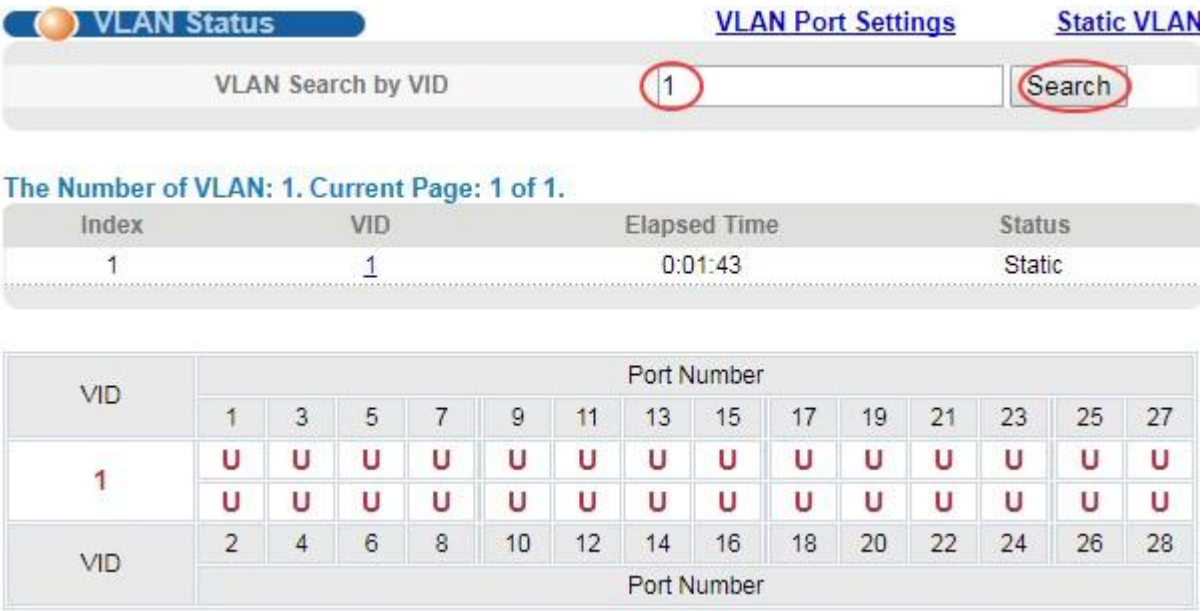


【Parameter Description】

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

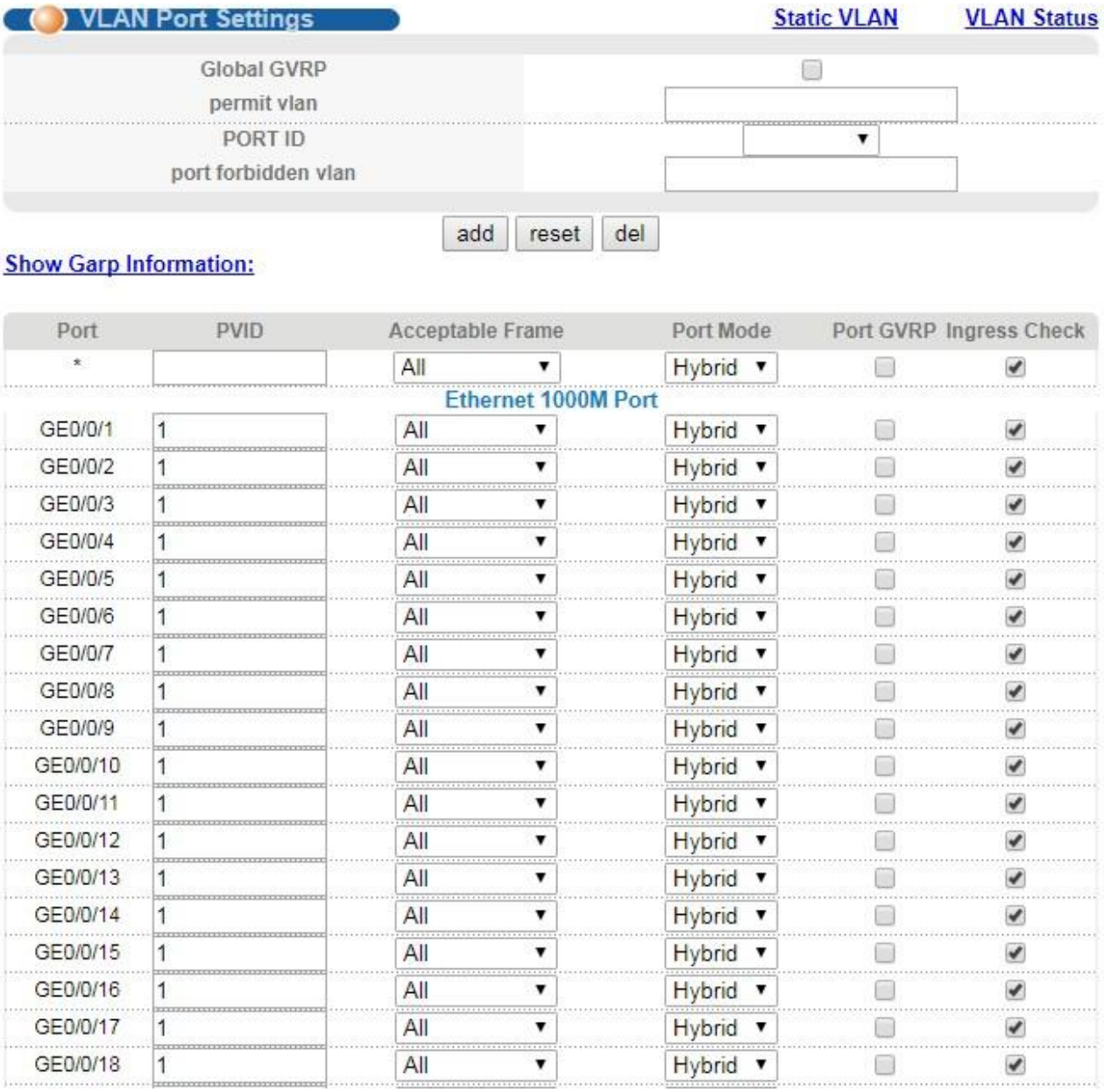
【Configuration example】

Such as: View the VLAN of VID as “1".



2.2.1.2 VLAN Port Settings

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



【Parameter Description】

Parameter	Description
PVID	The PVID of the port can be modified, the default port PVID is "1"

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

【Instructions】

Hybrid port to packet:

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

Hybrid port to send packet:

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

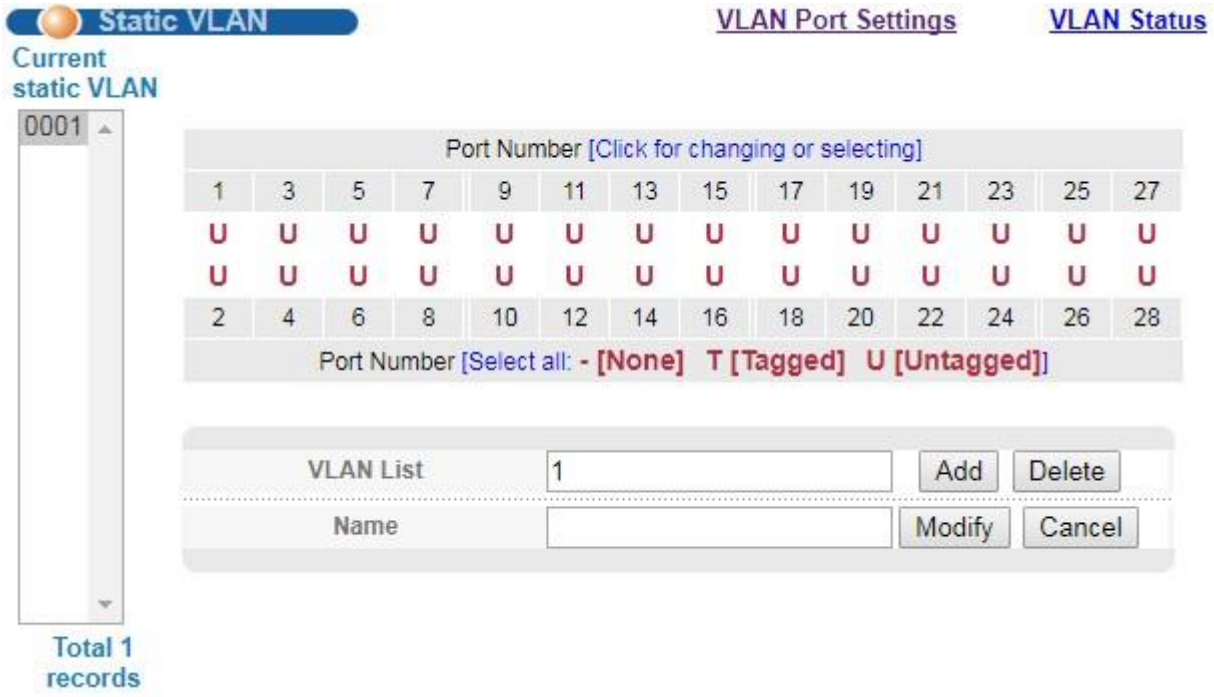
2. If it is untag stripping VLAN information, send again, if the tag is sent directly.

【Configuration example】

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.

2.2.1.3 Static VLAN

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



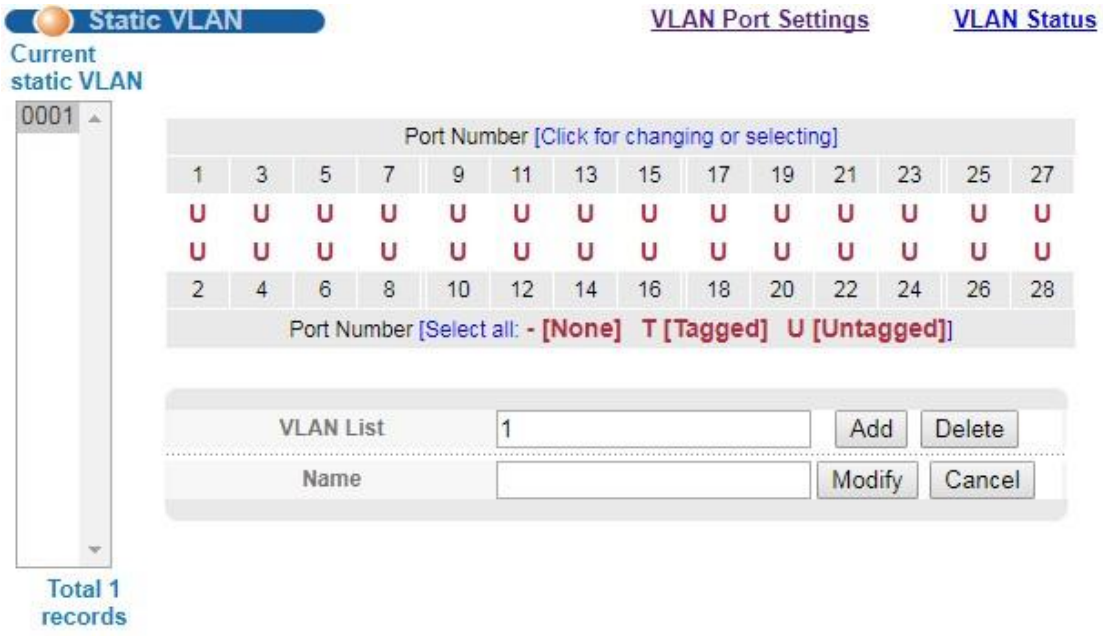
【Parameter Description】

Parameter	Description
VLAN List	VLAN Group ID
Name	VLAN Group name

【Configuration example】

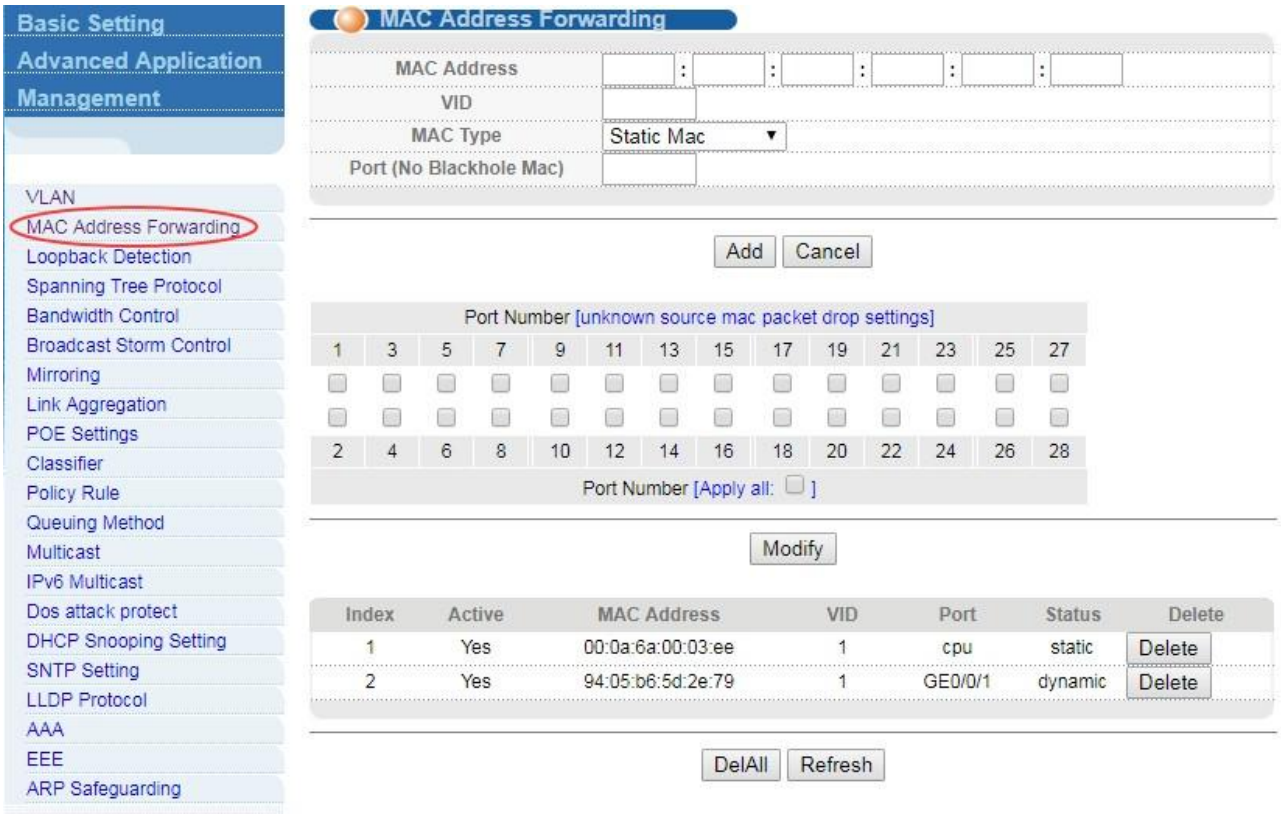
Add and delete VLAN members

Such as: Adding a new VLAN, VLAN Group ID 120 contains non-untag member port 6, 8. Tag member port 18, 20. The user can modify the port member by clicking on the white area below the port number;



2.2.2 MAC Address Forwarding

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



【Parameter Description】

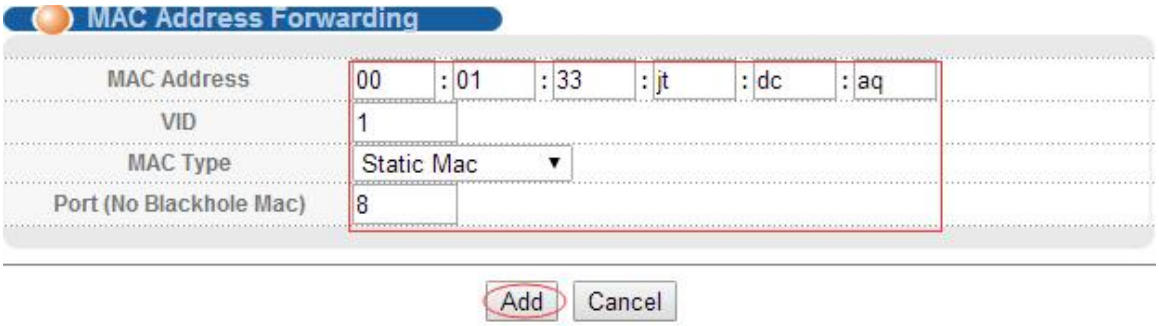
Parameter	Description
MAC Type	MAC Type: Static MAC Dynamic MAC Blackhole MAC Permanent MAC

【Instructions】

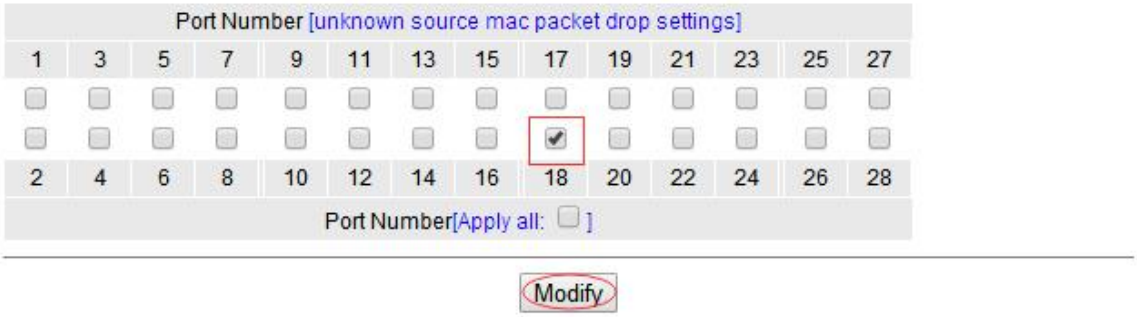
Blackhole MAC: If a PC's MAC address is configured on a switch to be a blackhole MAC, then the PC's package will be discarded by the switch and not forwarded to the network.

【Configuration example】

1. MAC Address Forwarding

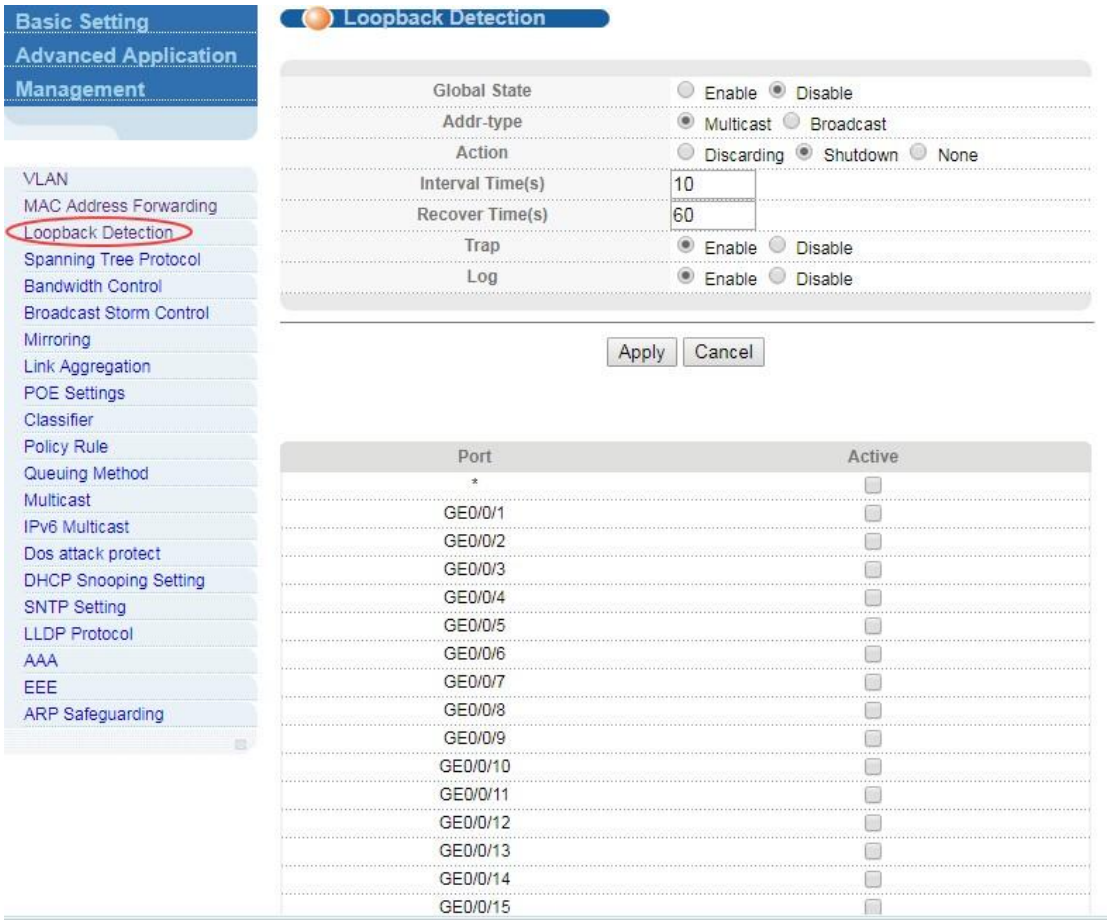


2. Unknown source mac packet drop settings.



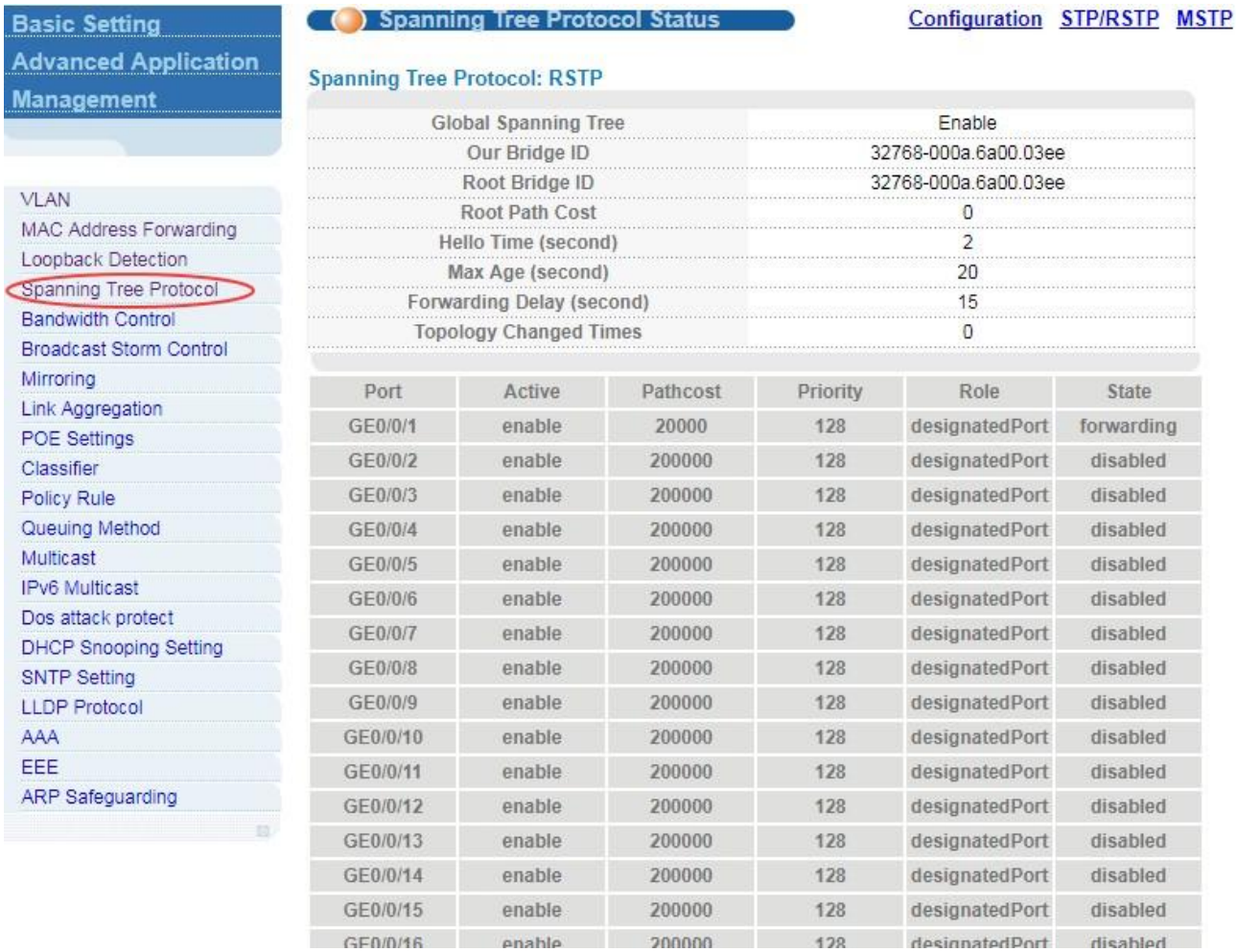
2.2.3 Loopback Detection

Selecting “**Advanced Application**>**Lookback Detection**", in the navigation bar, you can configure lookback detection.



2.2.4 Spanning Tree Protocol

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



2.2.4.1 Spanning Tree Protocol Status

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

Spanning Tree Protocol Status Configuration STP/RSTP MSTP

Spanning Tree Protocol: RSTP

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

Port	Active	Pathcost	Priority	Role	State
GE0/0/1	enable	20000	128	designatedPort	forwarding
GE0/0/2	enable	200000	128	designatedPort	disabled
GE0/0/3	enable	200000	128	designatedPort	disabled
GE0/0/4	enable	200000	128	designatedPort	disabled
GE0/0/5	enable	200000	128	designatedPort	disabled
GE0/0/6	enable	200000	128	designatedPort	disabled
GE0/0/7	enable	200000	128	designatedPort	disabled
GE0/0/8	enable	200000	128	designatedPort	disabled
GE0/0/9	enable	200000	128	designatedPort	disabled
GE0/0/10	enable	200000	128	designatedPort	disabled
GE0/0/11	enable	200000	128	designatedPort	disabled
GE0/0/12	enable	200000	128	designatedPort	disabled
GE0/0/13	enable	200000	128	designatedPort	disabled
GE0/0/14	enable	200000	128	designatedPort	disabled
GE0/0/15	enable	200000	128	designatedPort	disabled

【Parameter Description】

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

2.2.4.2 Spanning Tree Configuration

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

【Parameter Description】

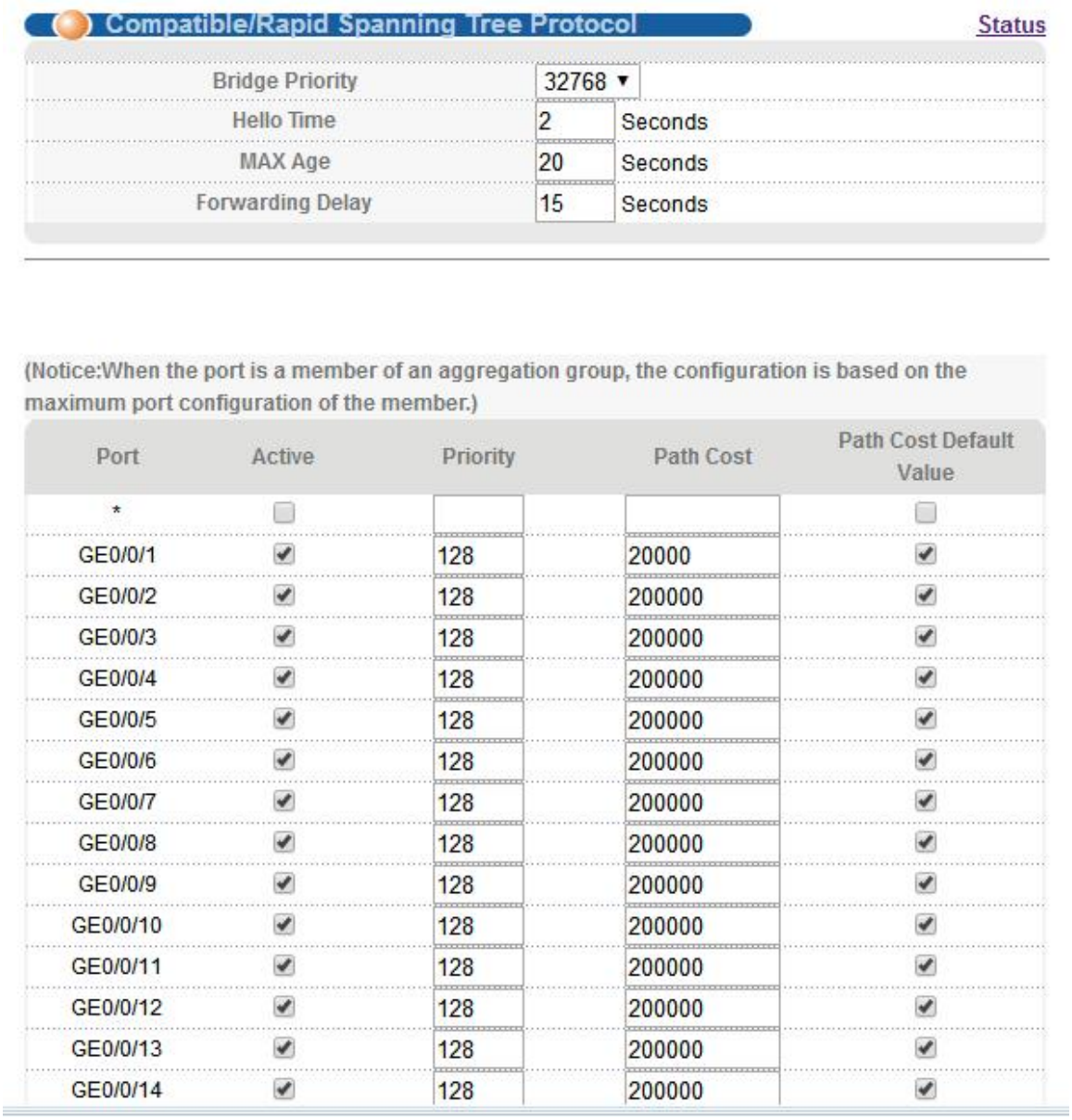
Parameter	Description
Spanning Tree Mode	Spanning tree mode: IEEE Compatible Spanning Tree Rapid Spanning Tree Multiple Spanning Tree
Global Spanning Tree Status	Select open or close Global Spanning

【Configuration example】

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

2.2.4.3 Compatible/Rapid Spanning Tree Protocol

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



【Parameter Description】

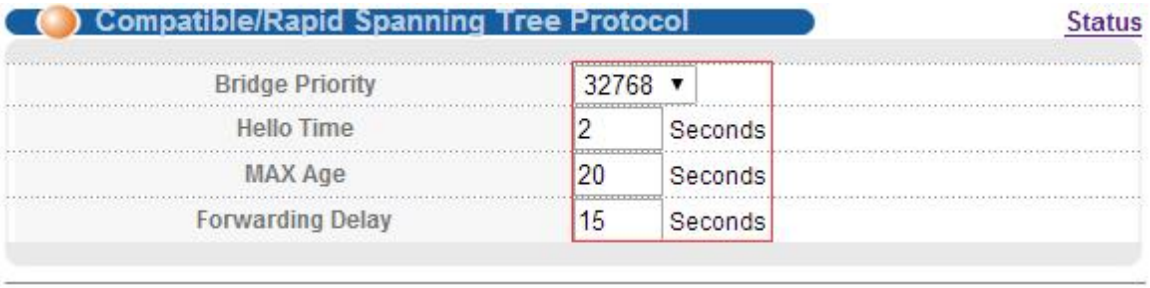
Parameter	Description
Bridge Priority	Set bridge priority, the default instance bridge priority for 32768

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
Port Priority	Set port instance priority, defaults to 128
Path Cost	Configure port costs

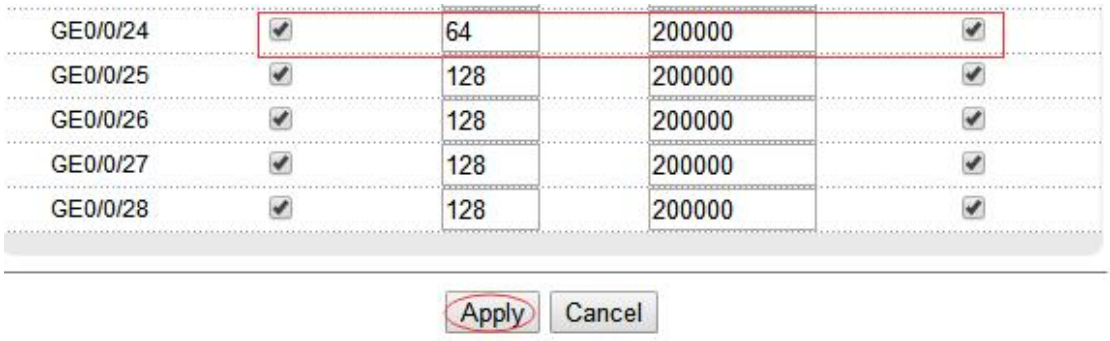
【Configuration example】

Such as:

1. 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.

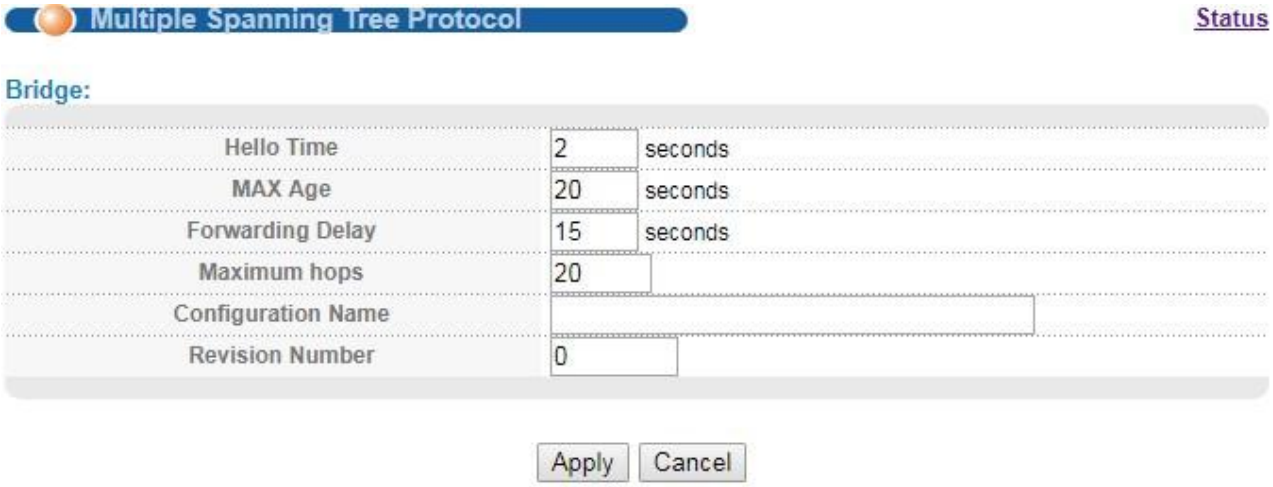


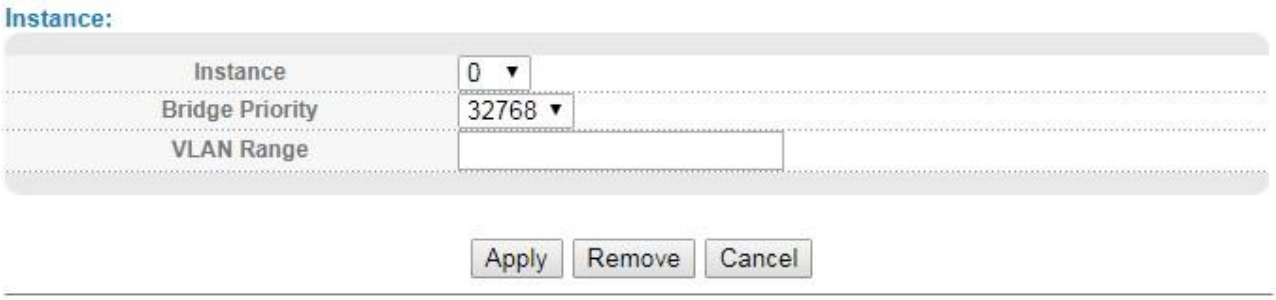
2. The priority of port 24 is 64, and the path cost is 200000.



2.2.4.4 Multiple Spanning Tree Protocol

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





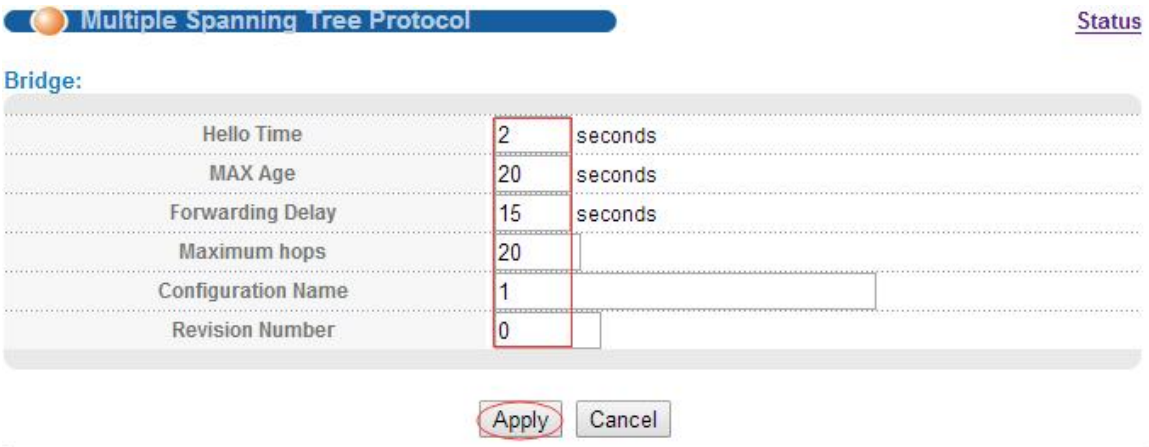
【Parameter Description】

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

Parameter	Description
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】

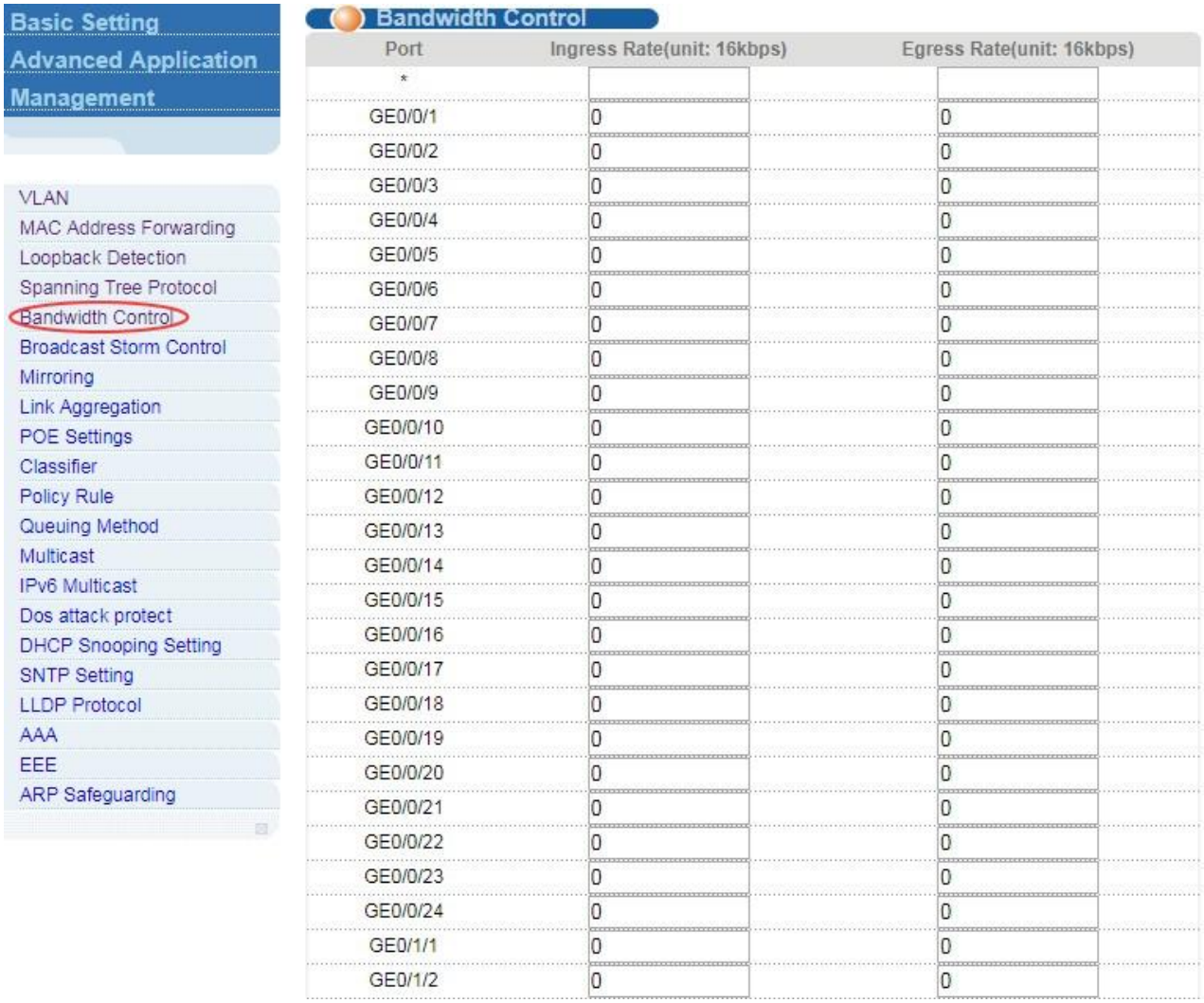
1. Bridge



2. Instance

2.2.5 Bandwidth Control

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

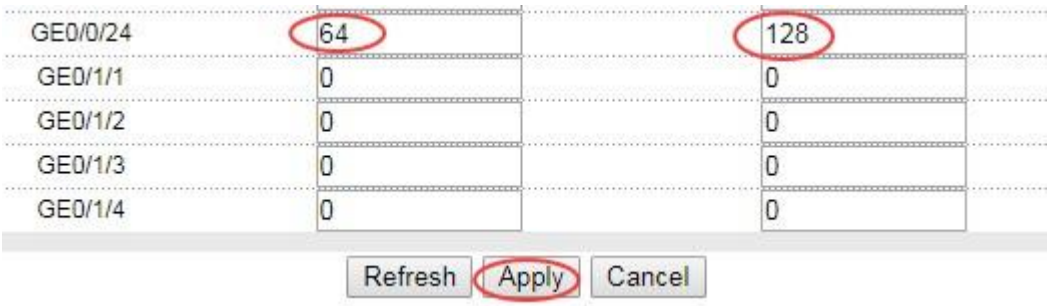


【Instructions】

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.

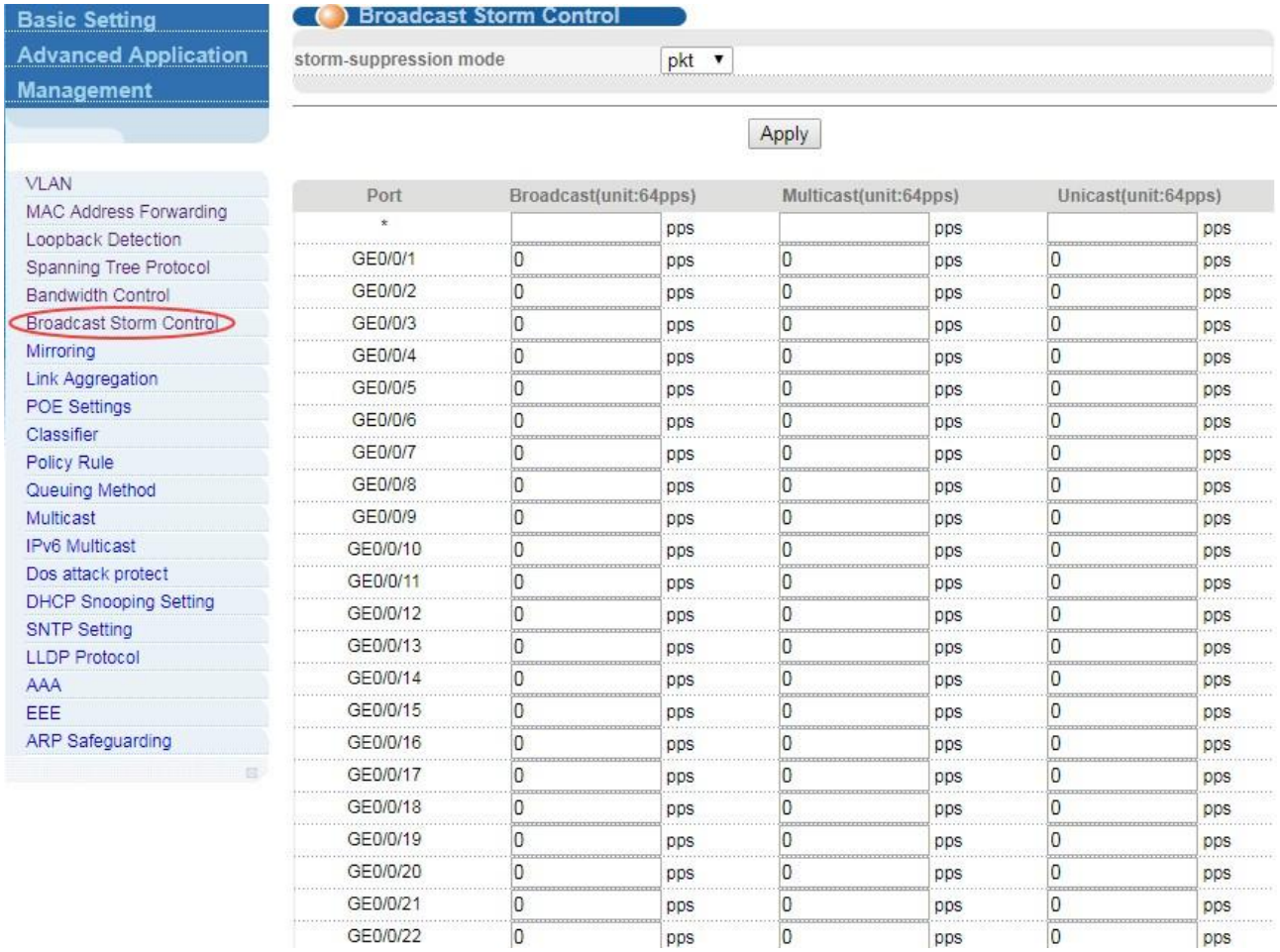
【Configuration example】

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



2.2.6 Broadcast Storm Control

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

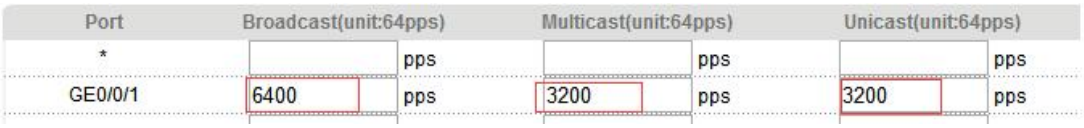
	unit: pps, you must enter multiple of 64, default to 49984)

【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.

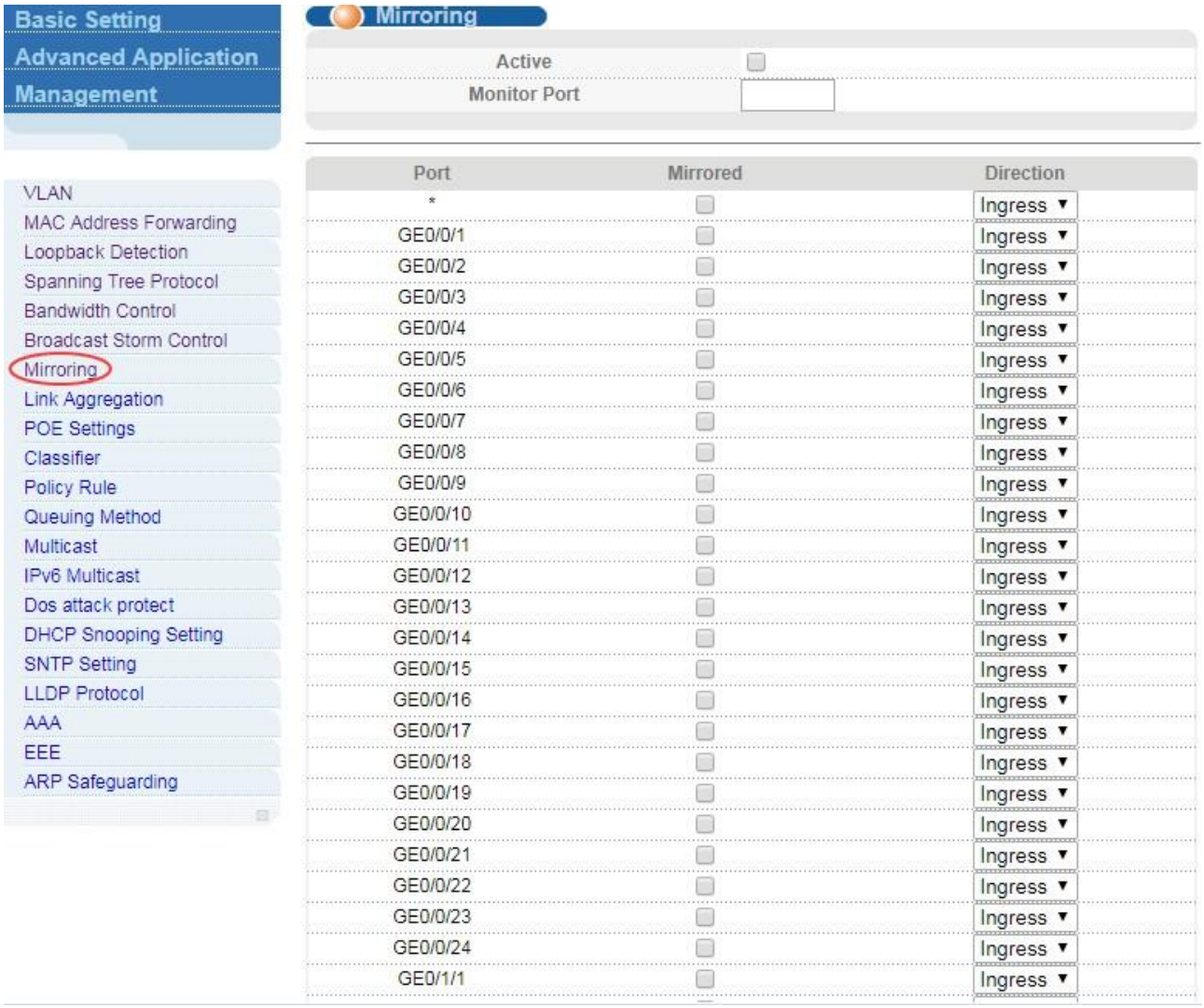
【Configuration example】

Such as: Set Port1 broadcast as 6400 pps, multicast as 3200 pps, unicast as 3200 pps.



2.2.7 Mirroring

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

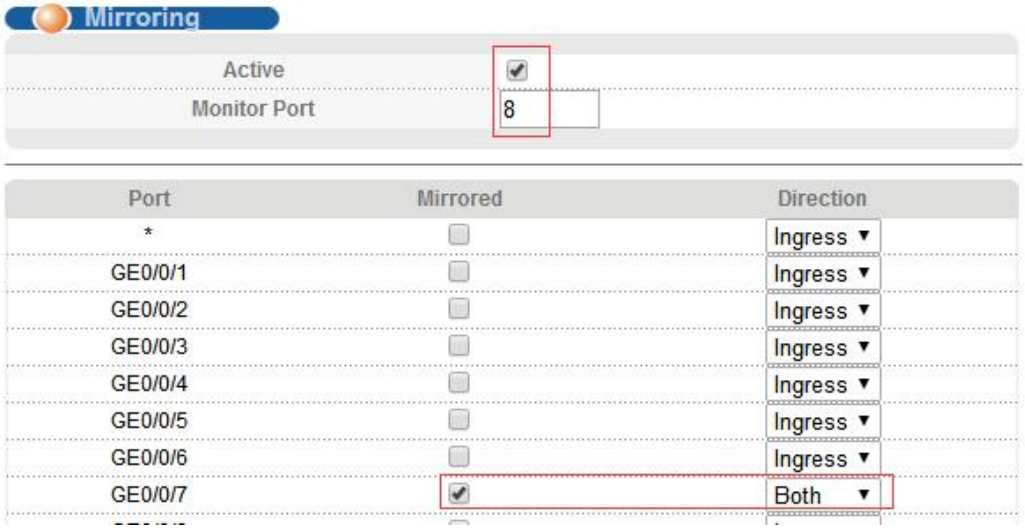


【Parameter Description】

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

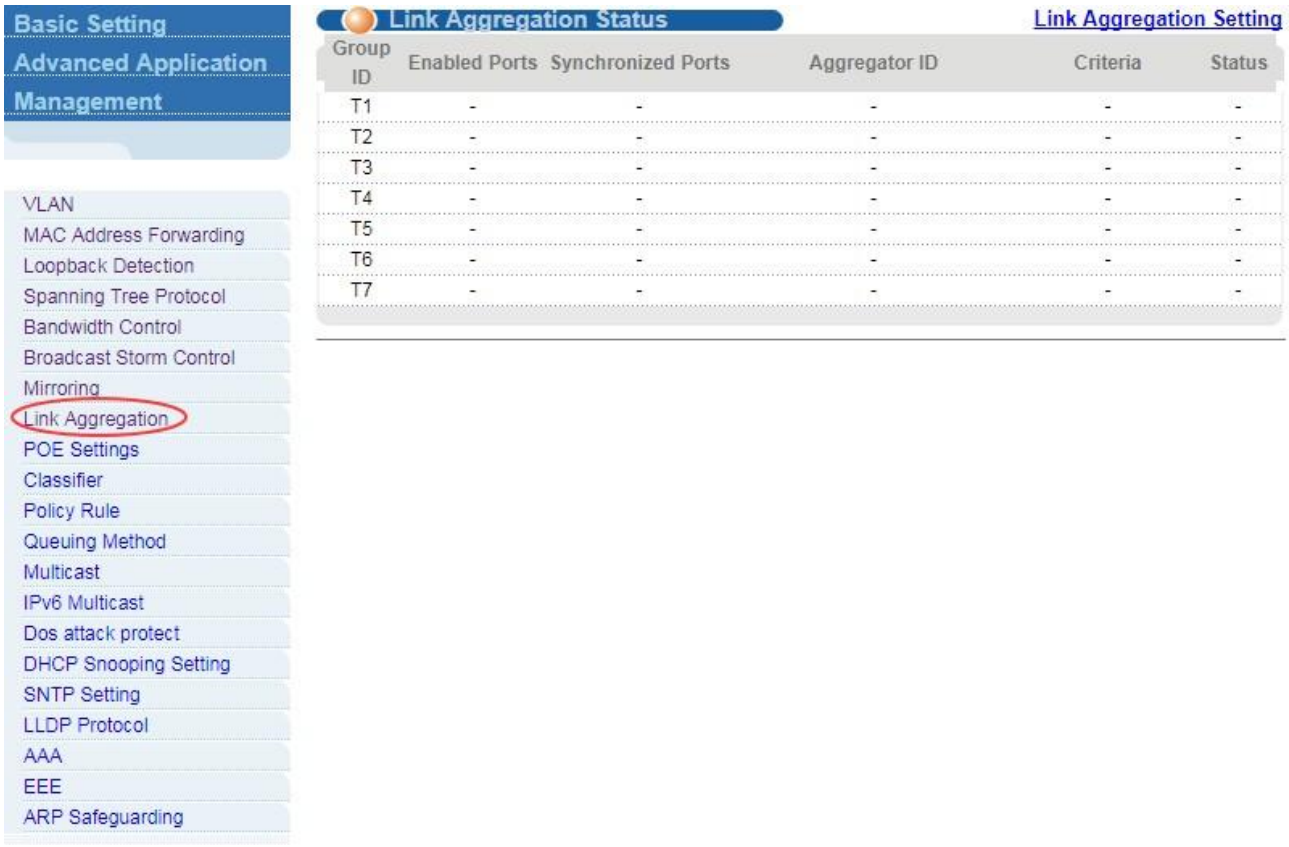
【Configuration example】

Such as: Open mirroring, configure monitoring port is port 8, the source port is port 7, and the mirror message is in both direction.



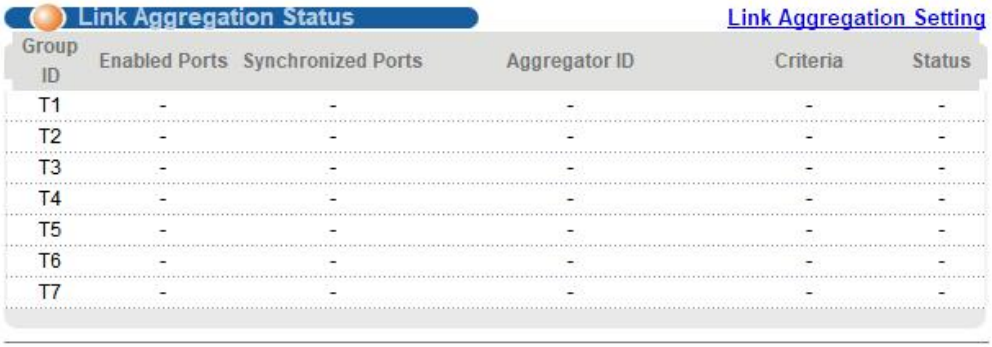
2.2.8 Link Aggregation

Selecting “**Advanced Application**>**Link Aggregation**", in the navigation bar, you can configure link aggregation.



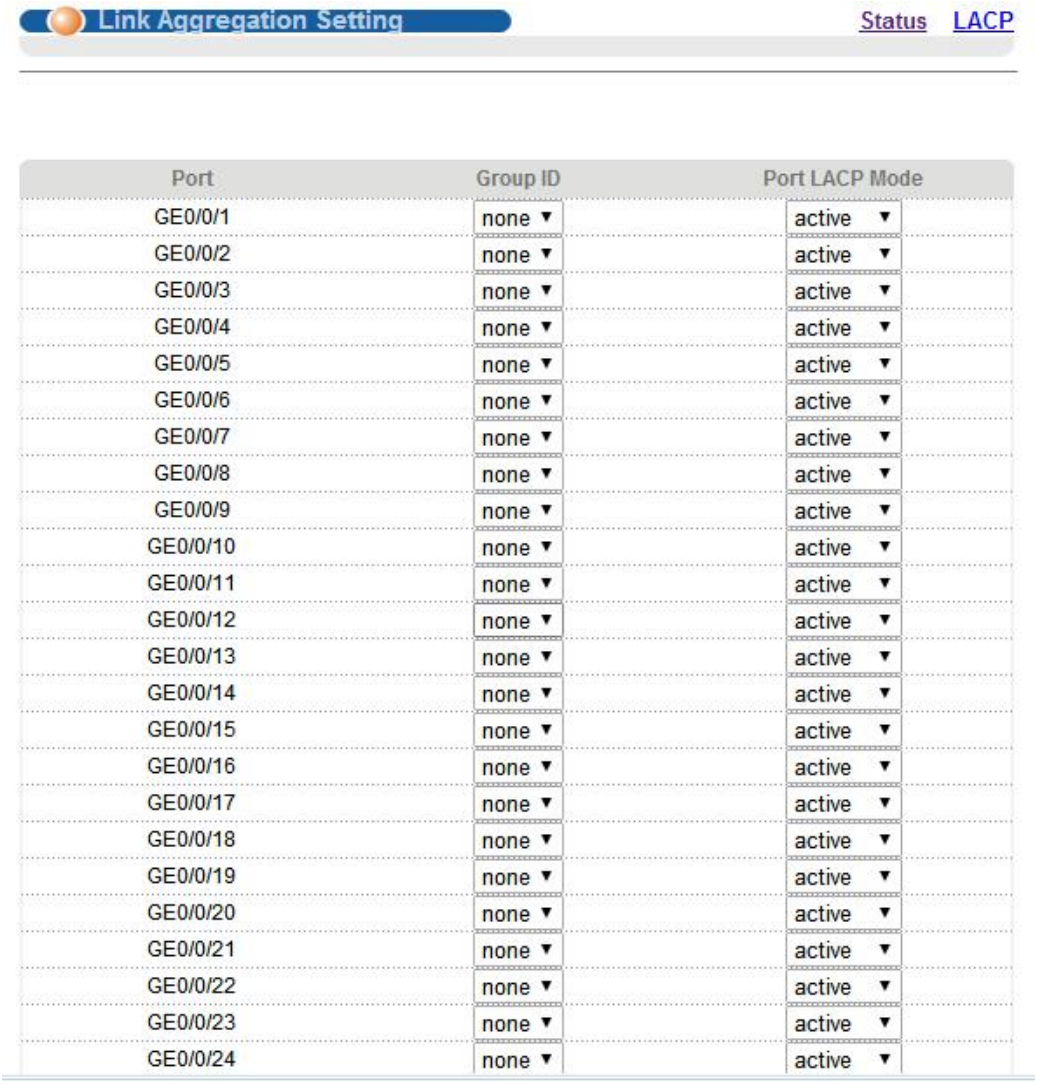
2.2.8.1 Link Aggregation status

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



2.2.8.2 Link Aggregation Setting

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

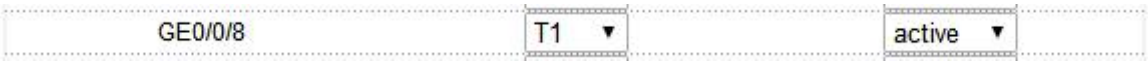


【Parameter Description】

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)

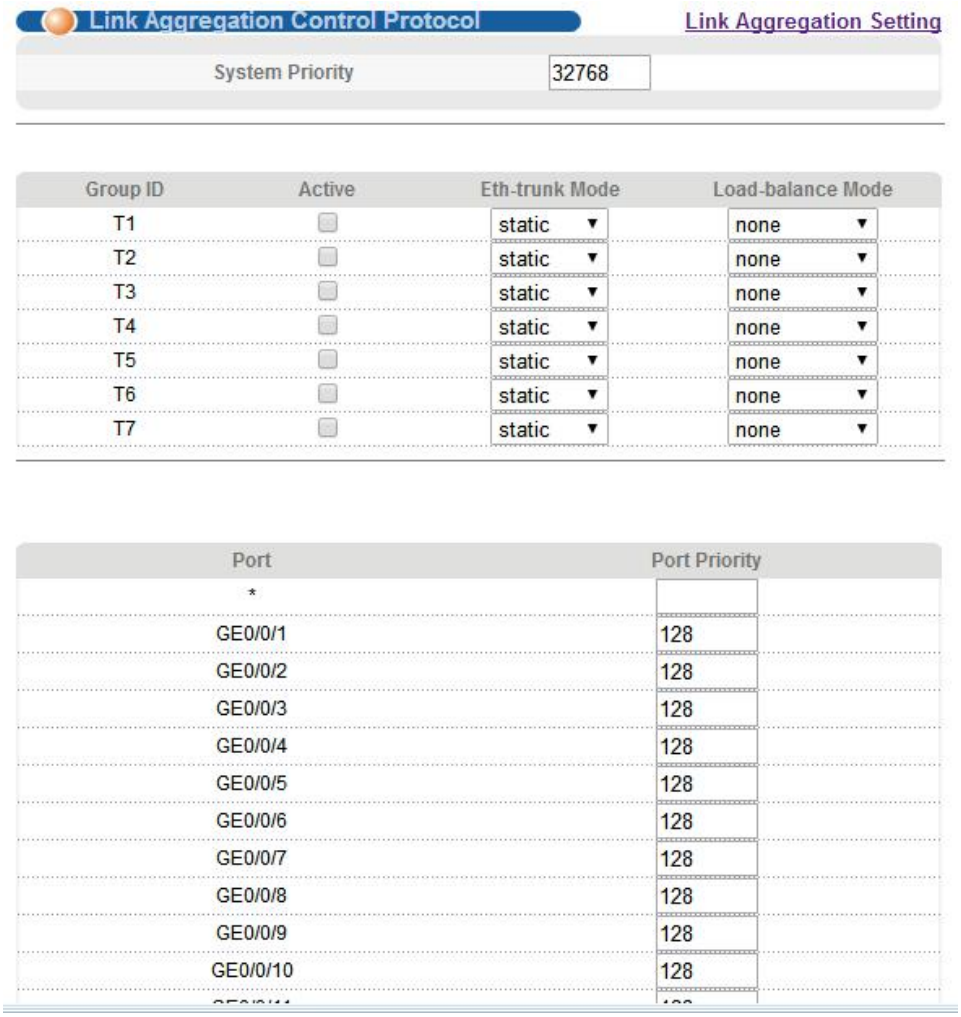
【Configuration example】

Such as: configure parameter of Aggregation Group port-8.



2.2.8.3 Link Aggregation Control Protocol

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



【Parameter Description】

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

【Configuration example】

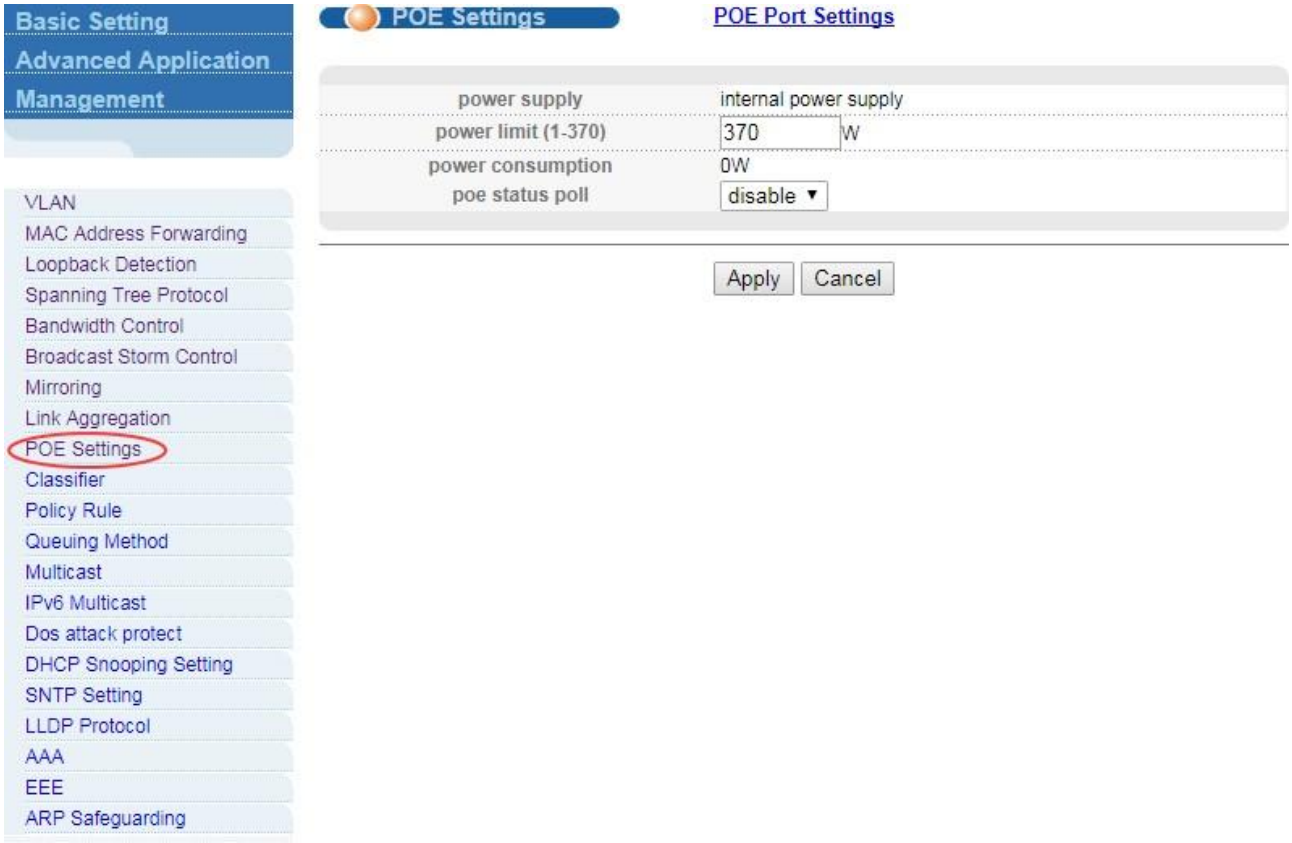
Such as:

1.Open aggregation group T1 LACP.

2.The priority for configuring port 8 is 64.

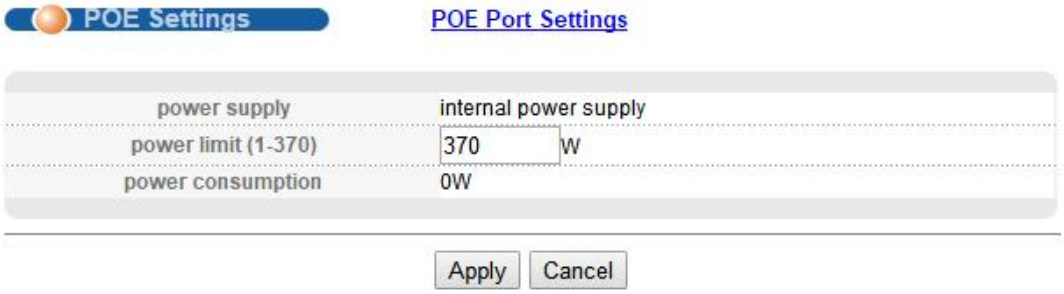
2.2.9 POE Settings

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



2.2.9.1 POE Settings

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

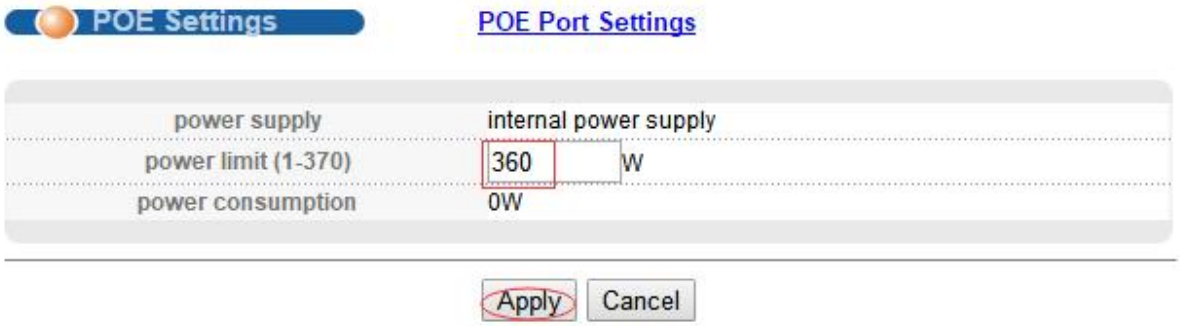


【Parameter Description】

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

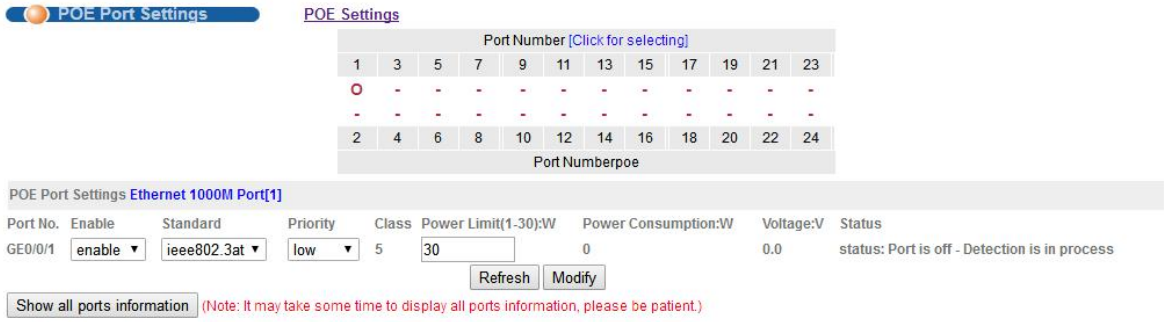
【Configuration example】

Such as: set power limit is 360 W.



2.2.9.2 POE Port Settings

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



【Parameter Description】

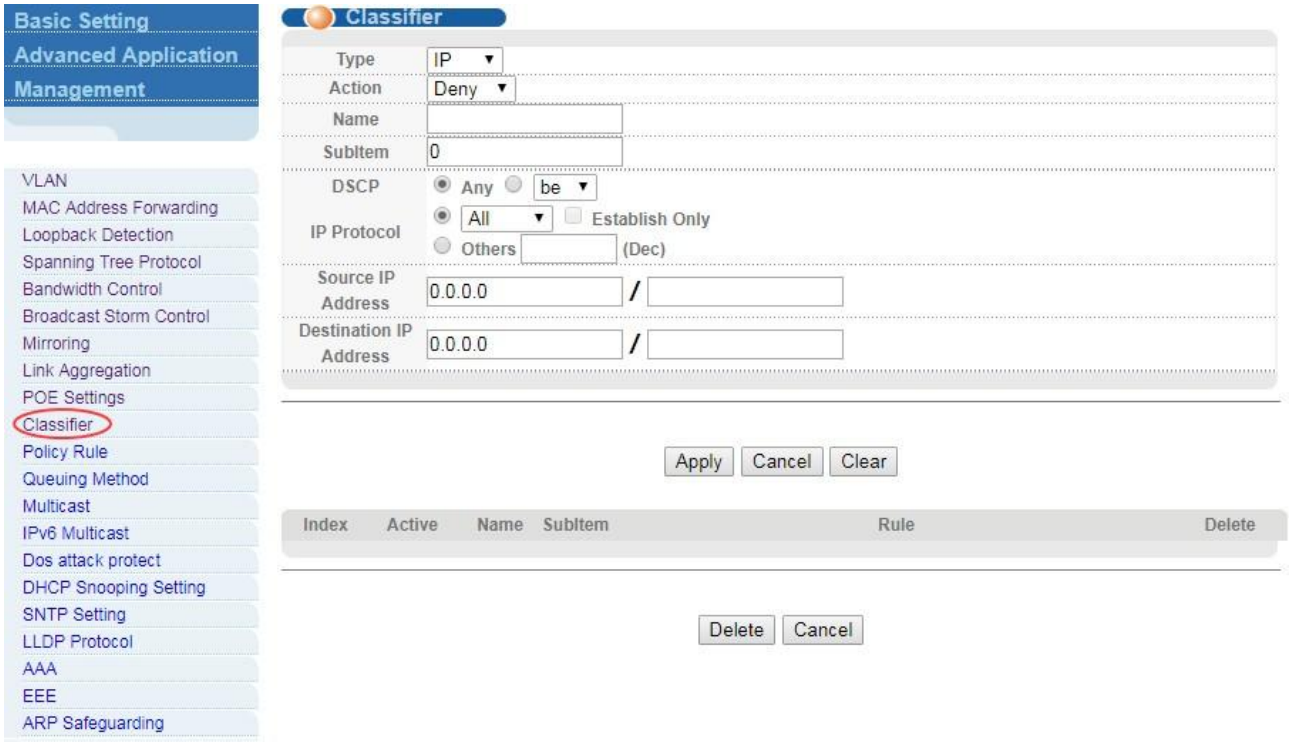
Parameter	Description
Enable	Turn the port POE power on and off and the default is open
Standard	Configure ieee802.3af, ieee802.3at mode, default to ieee802.3at
Priority	Configure port Priority low, critical, high, the default priority is low
Power limit	The power of switch POE can be limited

【Configuration example】

Such as: Configure the POE for port 1.

2.2.10 Classifier

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

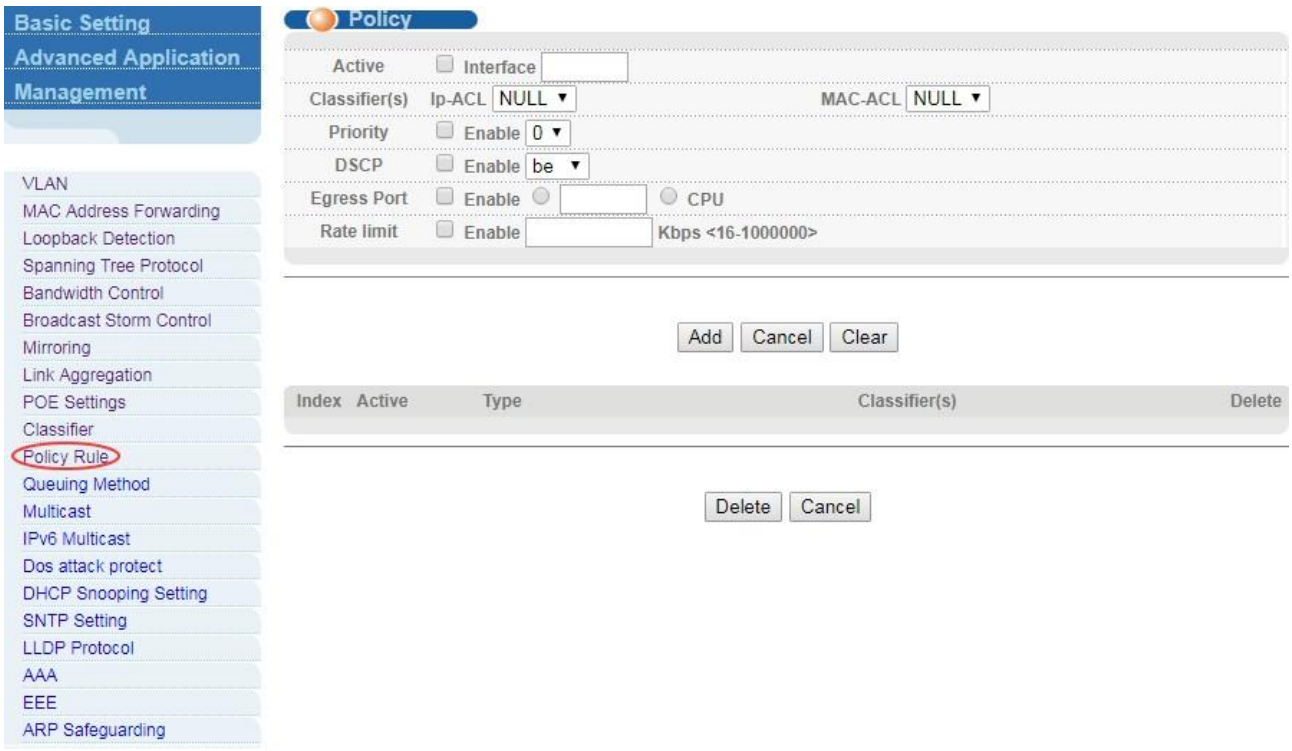


【Parameter Description】

Parameter	Description
Active	Active Classifier

2.2.11 Policy Rule

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

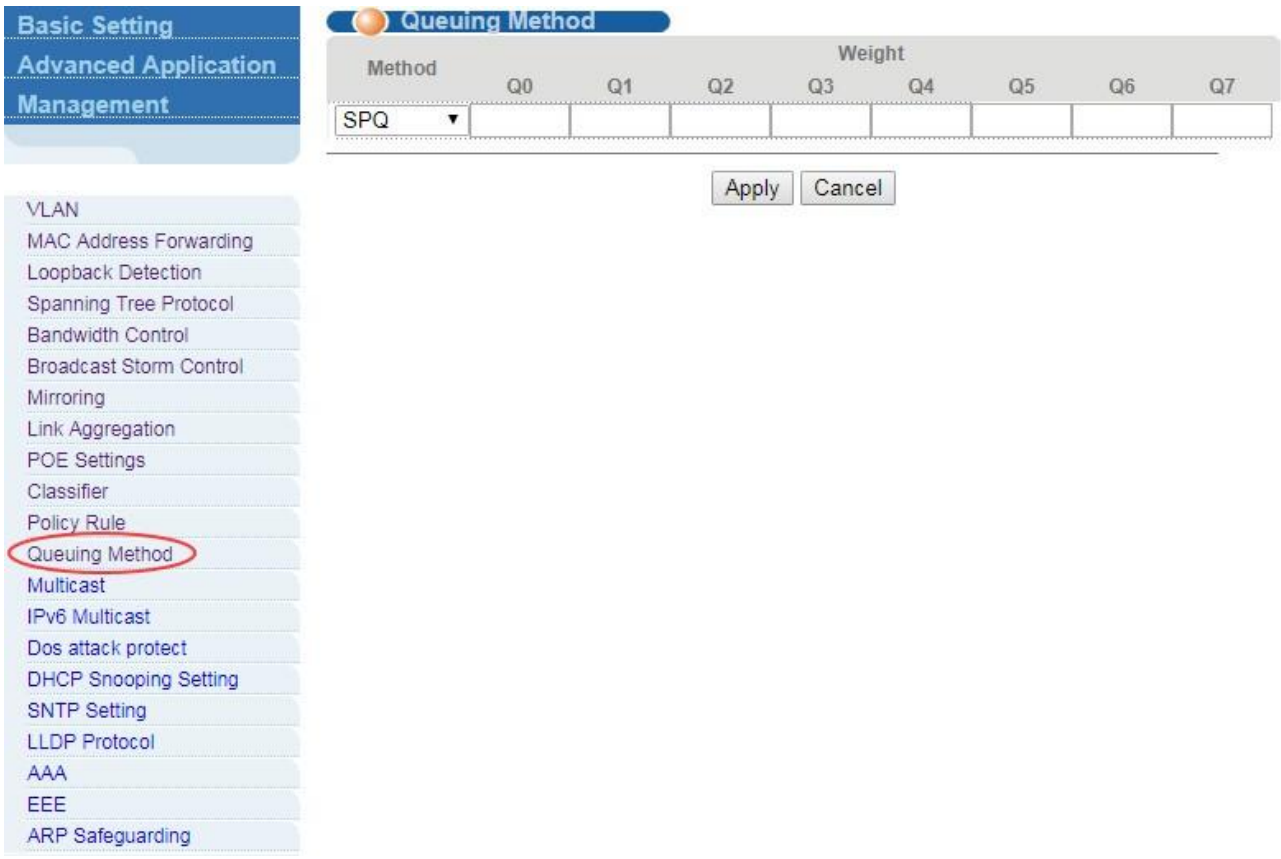


【Parameter Description】

Parameter	Description
Active	Active Classifier

2.2.12 Queuing Method

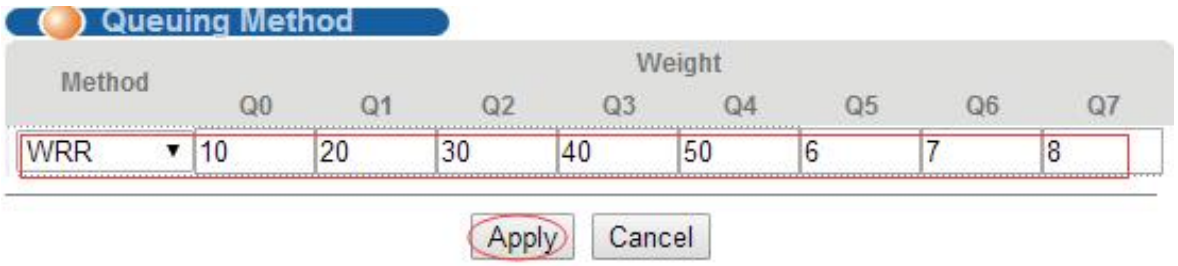
Selecting “**Advanced Application**>**Queuing Method**", in the navigation bar, you can configure queuing method.



【Parameter Description】

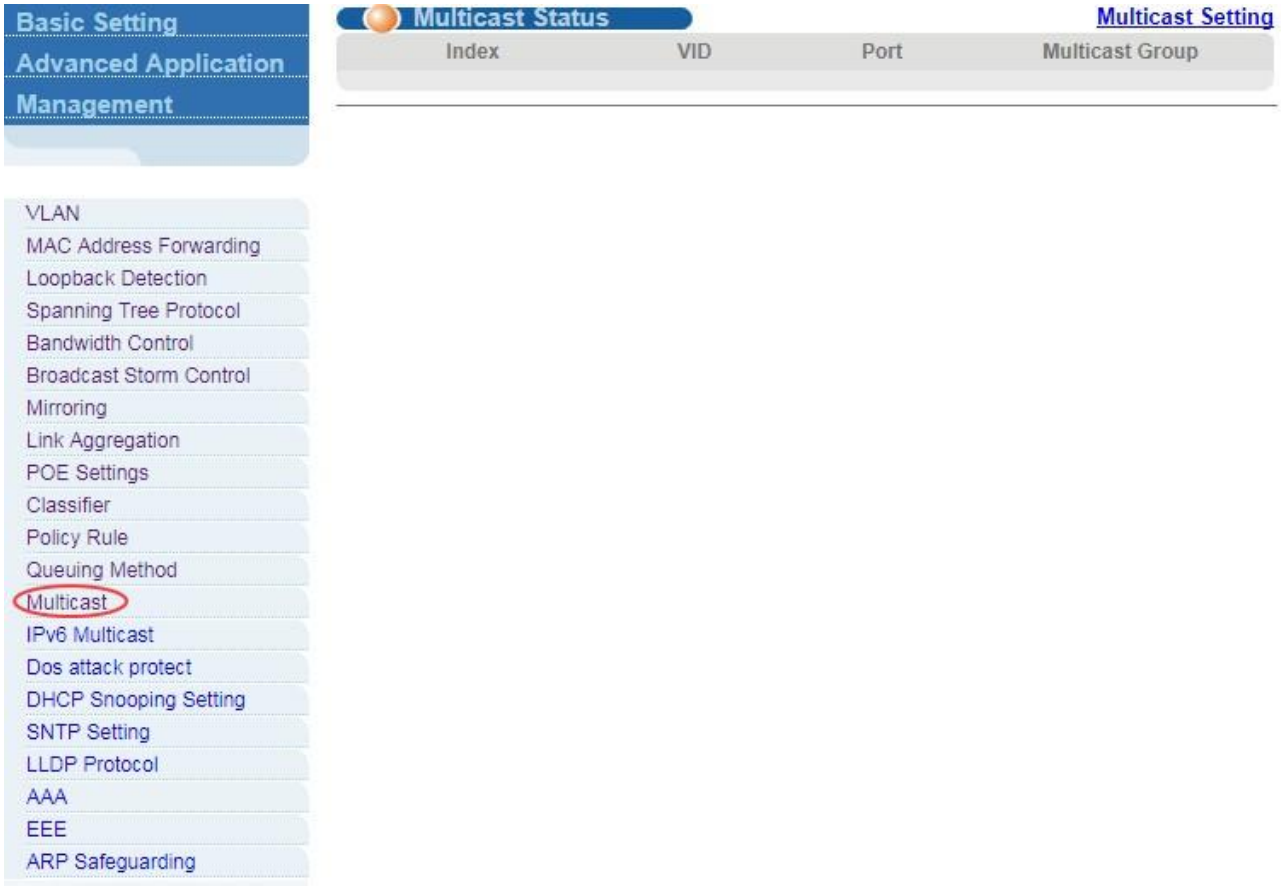
Parameter	Description
Method	Five method: SPQ,WRR,SP+WRR,WFQ,SP+WFQ

【Configuration Example】



2.2.13 Multicast

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

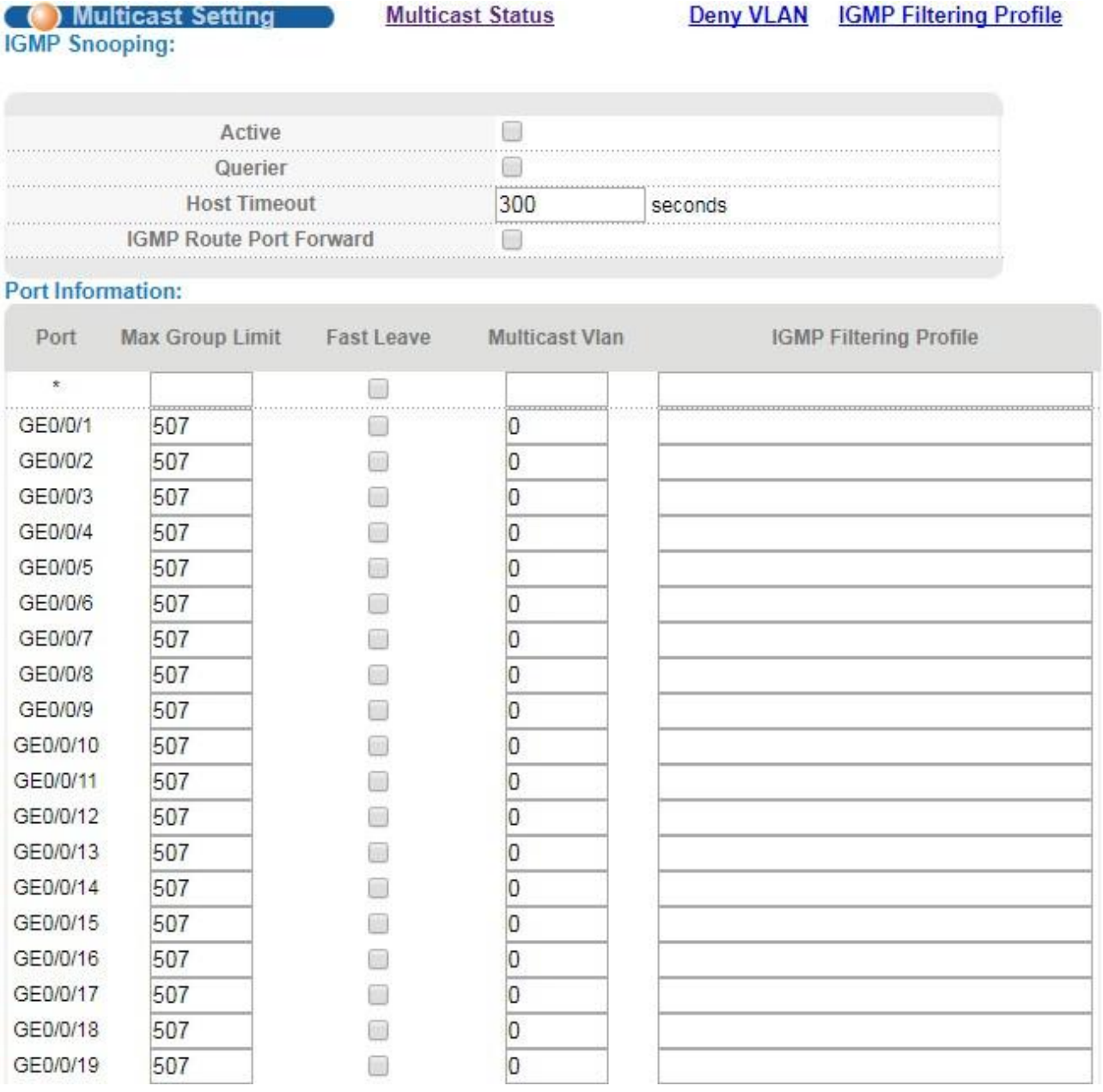


2.2.13.1 Multicast Status

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

2.2.13.2 Multicast Settings

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



【Parameter Description】

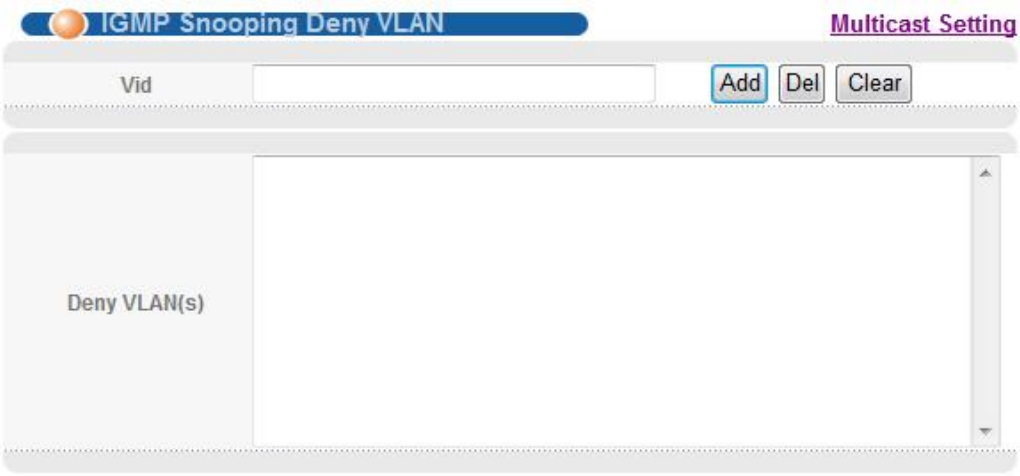
Parameter	Description
Active	Open IGMP-snooping
Querier	Open IGMP-snooping timed query function

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

【Configuration Example】

2.2.13.3 IGMPSnooping Dney VLAN

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

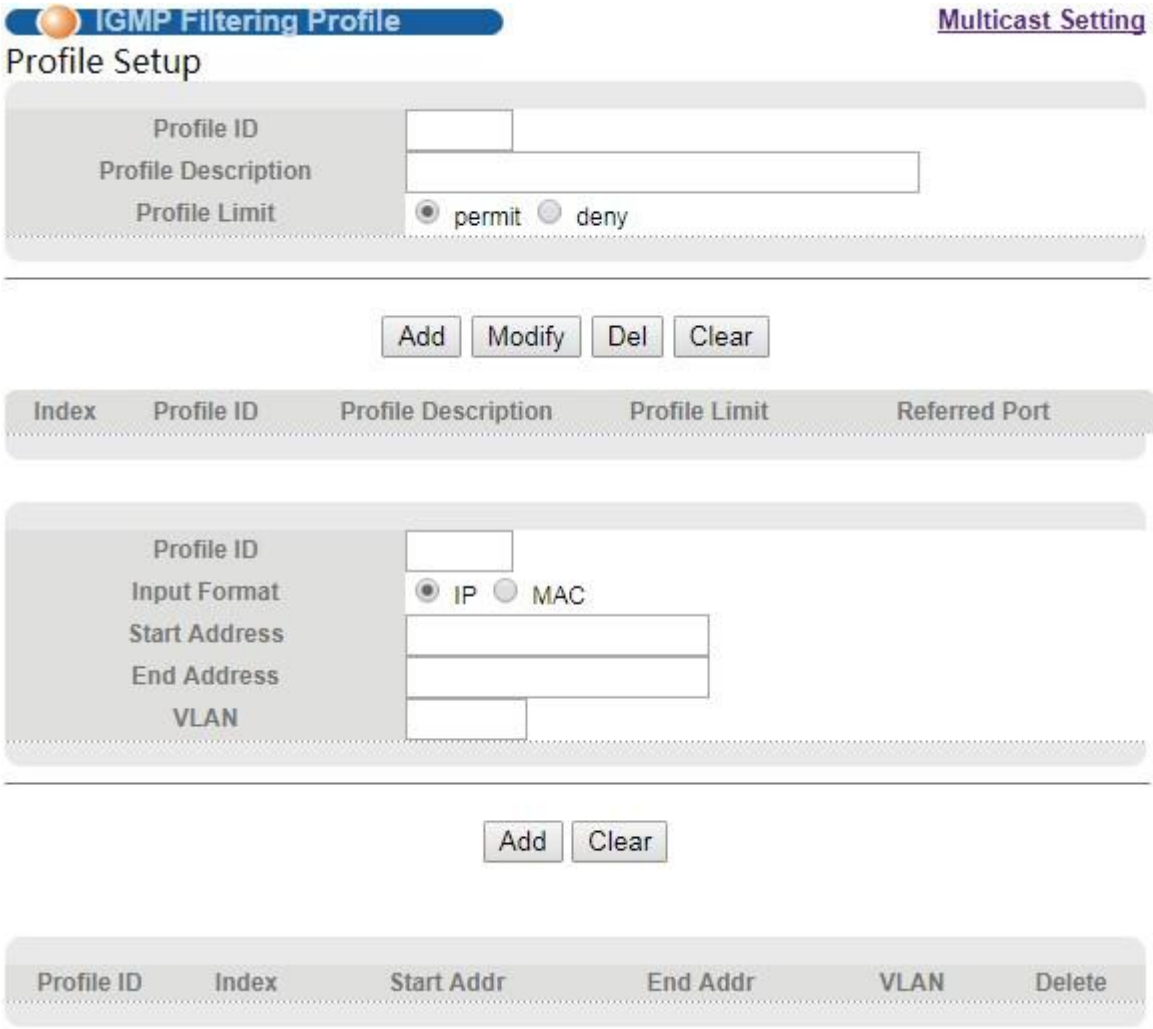


【Parameter Description】

Parameter	Description
Vid	Vlan's ID

2.2.13.4 IGMP Filtering Profile

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

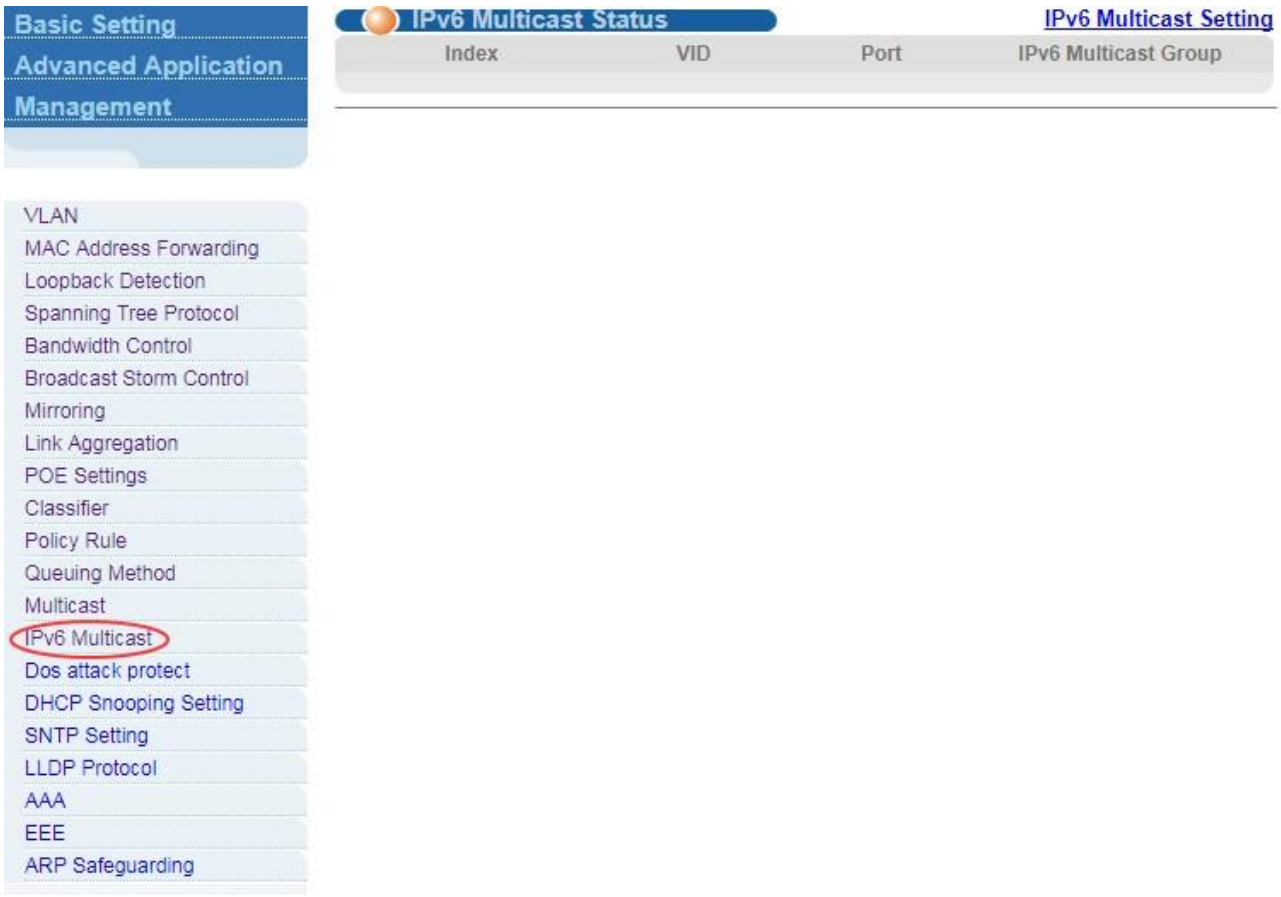


【Parameter Description】

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

2.2.14 IPv6 Multicast

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

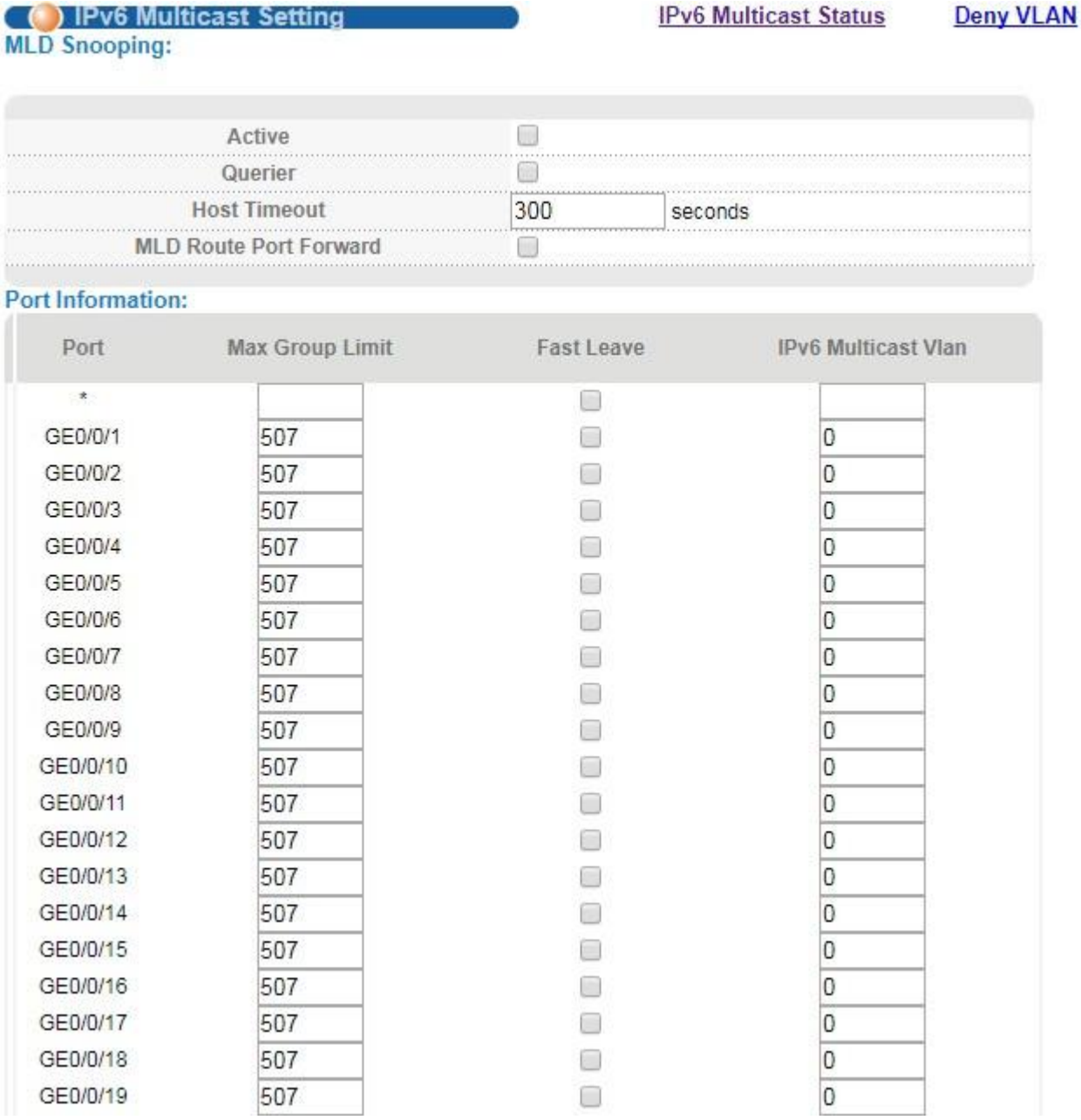


2.2.14.1 IPv6 Multicast Status

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

2.2.14.2 IPv6 Multicast Setting

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

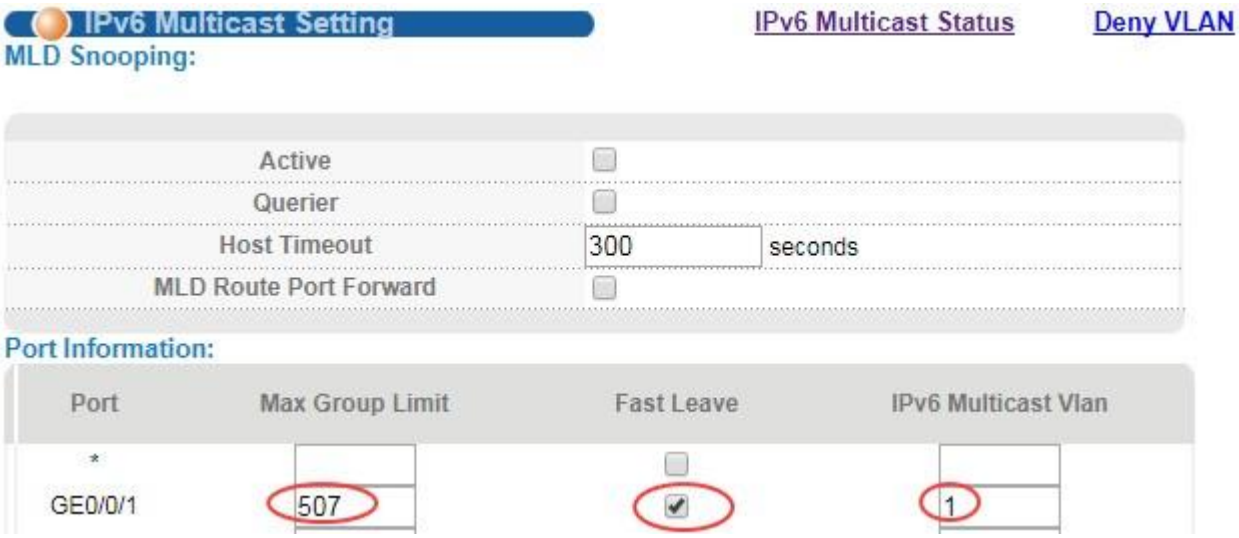


【Parameter Description】

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

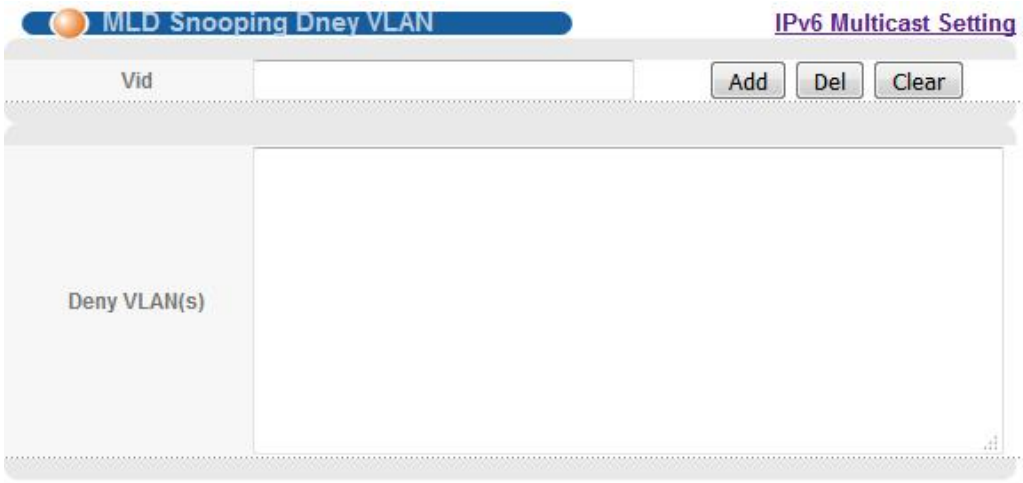
	Forward
Max Group Limit	Configure maximum learning IPv6 Multicast message of port(default 1020)
Fast Leave	Enable or disable Fast Leave (That is, when the port receives IGMP leave message, the port is deleted immediately from the IPv6 multicast group)
IPv6 Multicast VLAN	Configure IPv6 multicast default VLAN

【Configuration Example】



2.2.14.3 MLD Snooping Dney VLAN

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

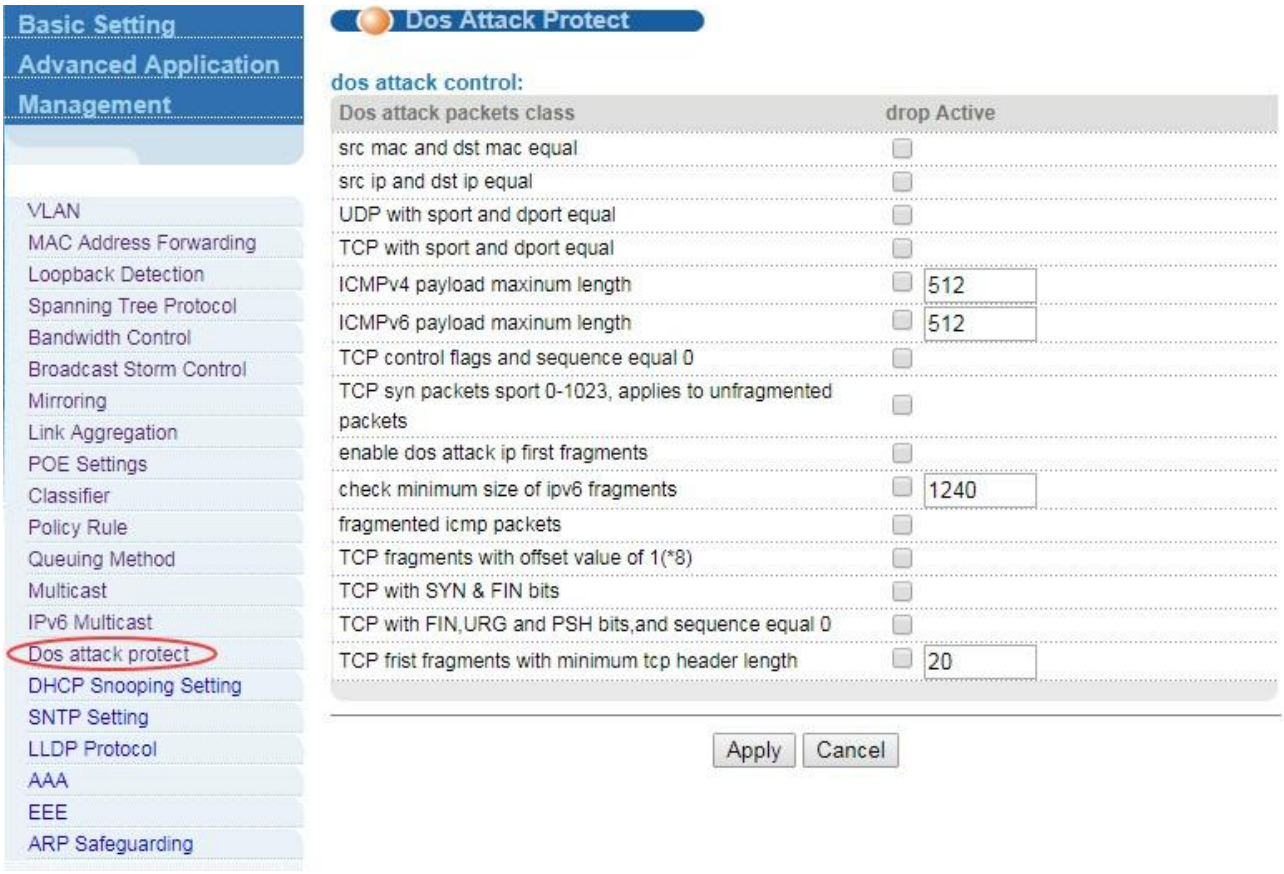


【Parameter Description】

Parameter	Description
Vid	Vlan ID

2.2.15 Dos attack protect

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

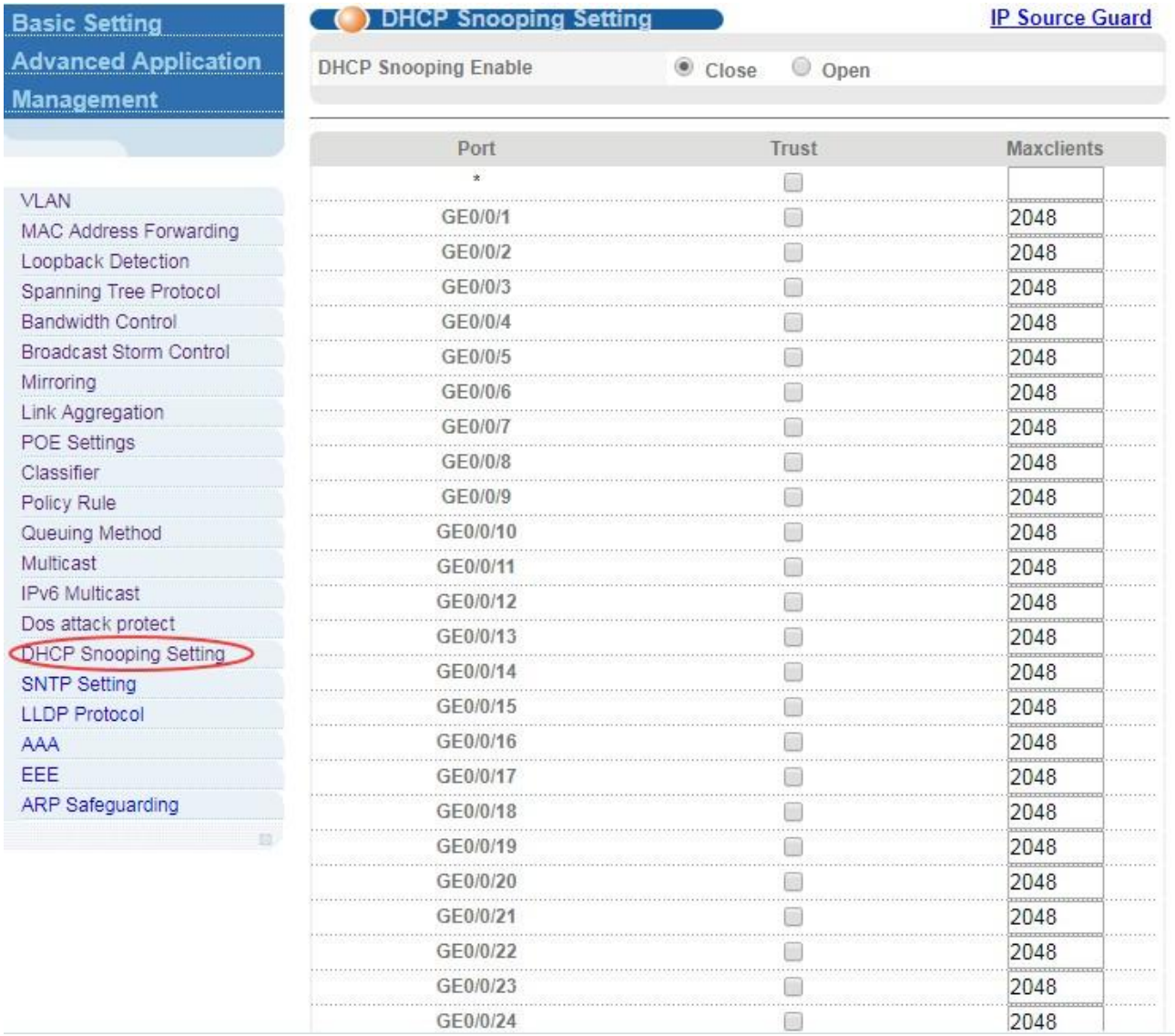


【Parameter Description】

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

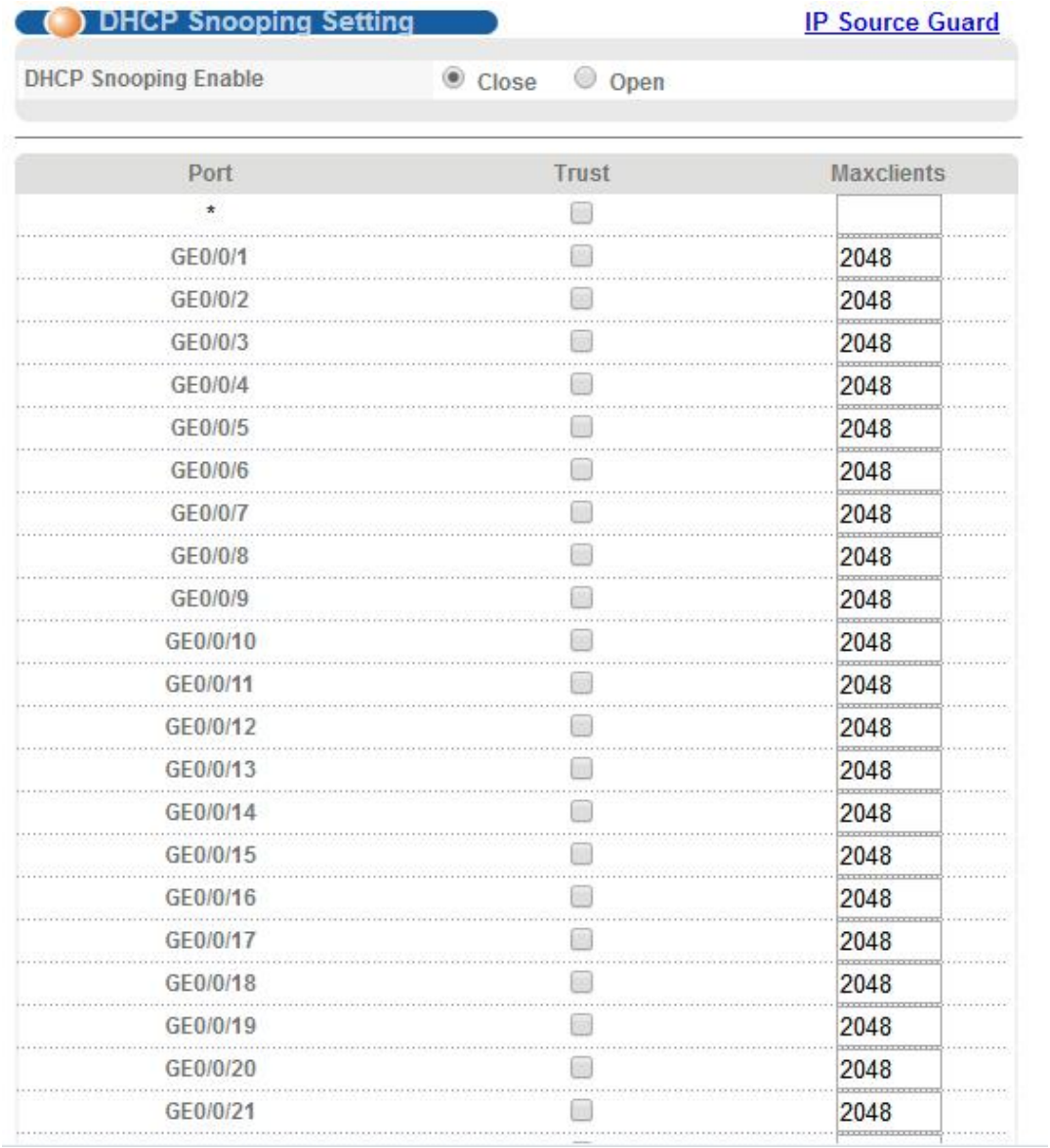
2.2.16 DHCP Snooping Setting

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



2.2.16.1 DHCP Snooping Setting

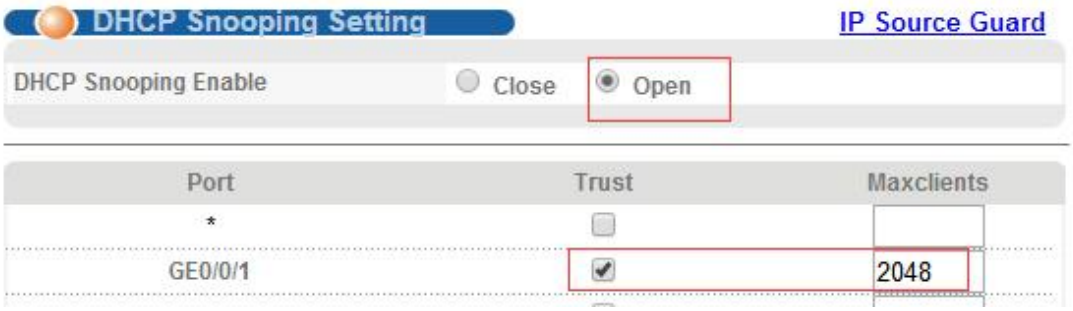
Selecting "**Advanced Application>DHCP Snooping Setting>DHCP Snooping Setting**", in the navigation bar, you can configure DHCP Snooping.



【Parameter Description】

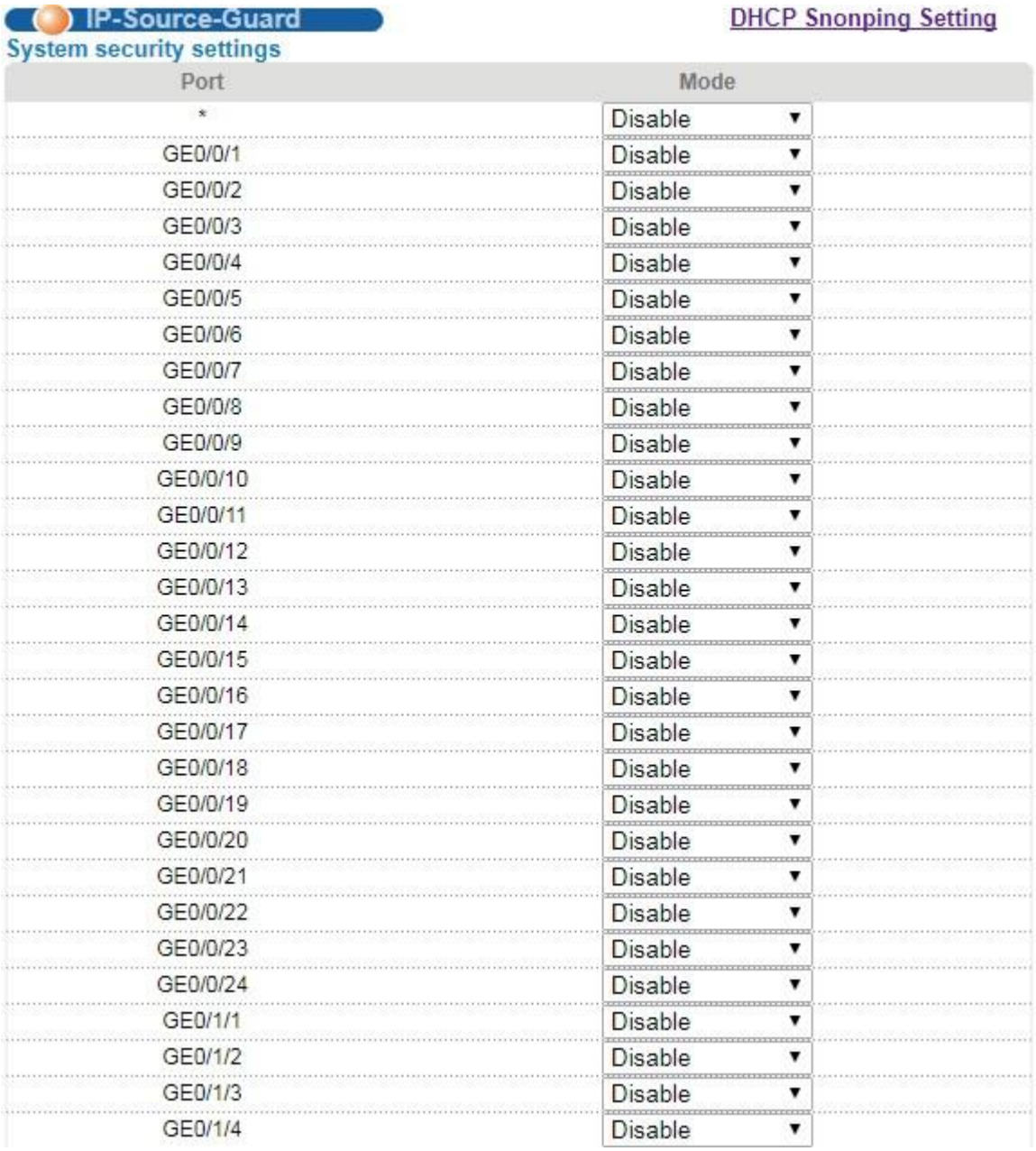
Parameter	Description
DHCP Snooping Enable	Enable or disable DHCP Snooping serve
Trust	Enable or disable the DHCP Snooping port trust property state
Maxclients	Set Maxclients

【Configuration Example】



2.2.16.2 IP Source Guard

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



【Parameter Description】

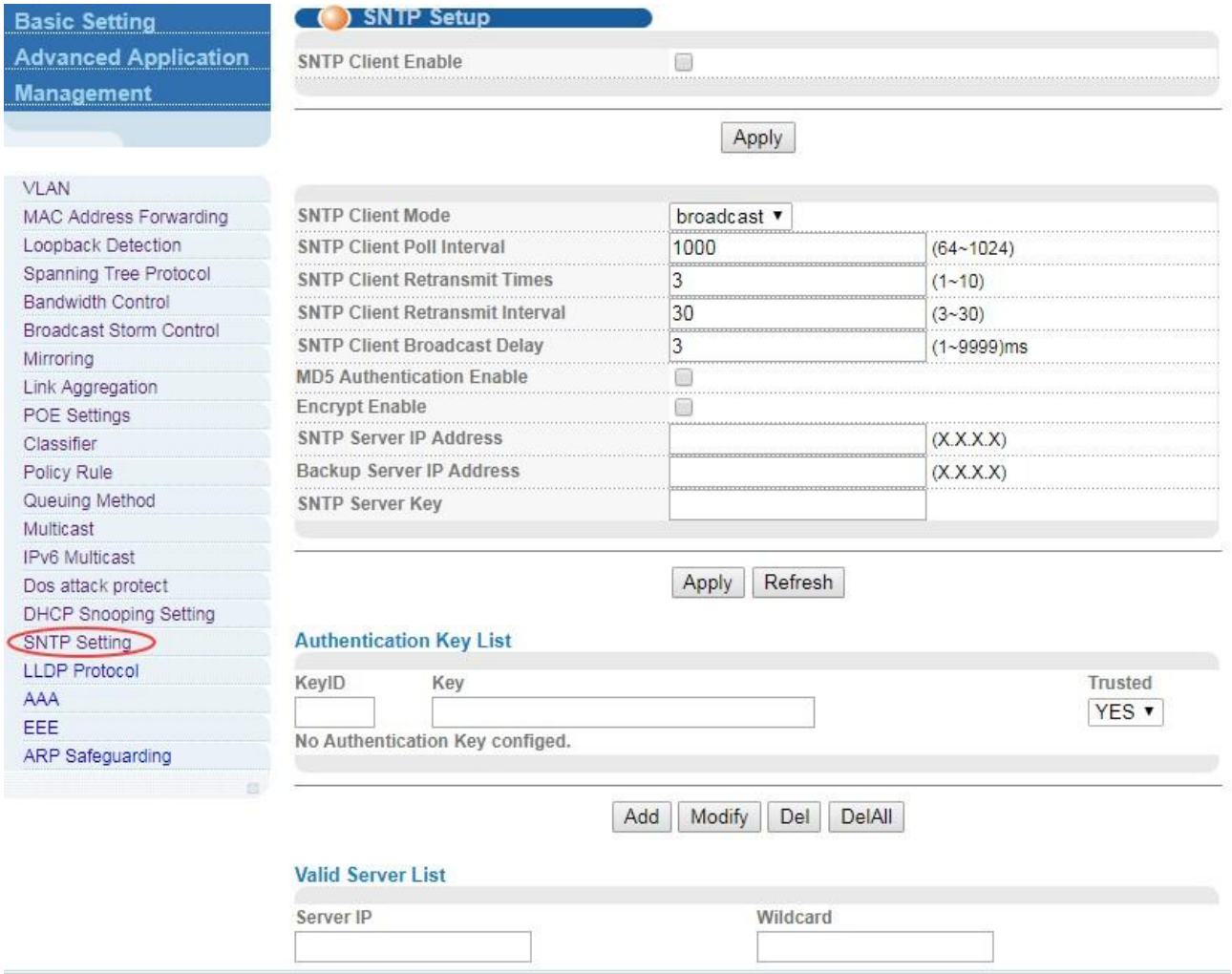
Parameter	Description
Disable unbinding entry to access network	Enable or Disable unbinding entry to access network

【Instructions】

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

2.2.17 SNTP Setting

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



【Parameter Description】

Parameter	Description
SNTP Client Enable	Enable or disable SNTP Client
SNTP Client Mode	SNTP Client Mode: broadcast, anycast

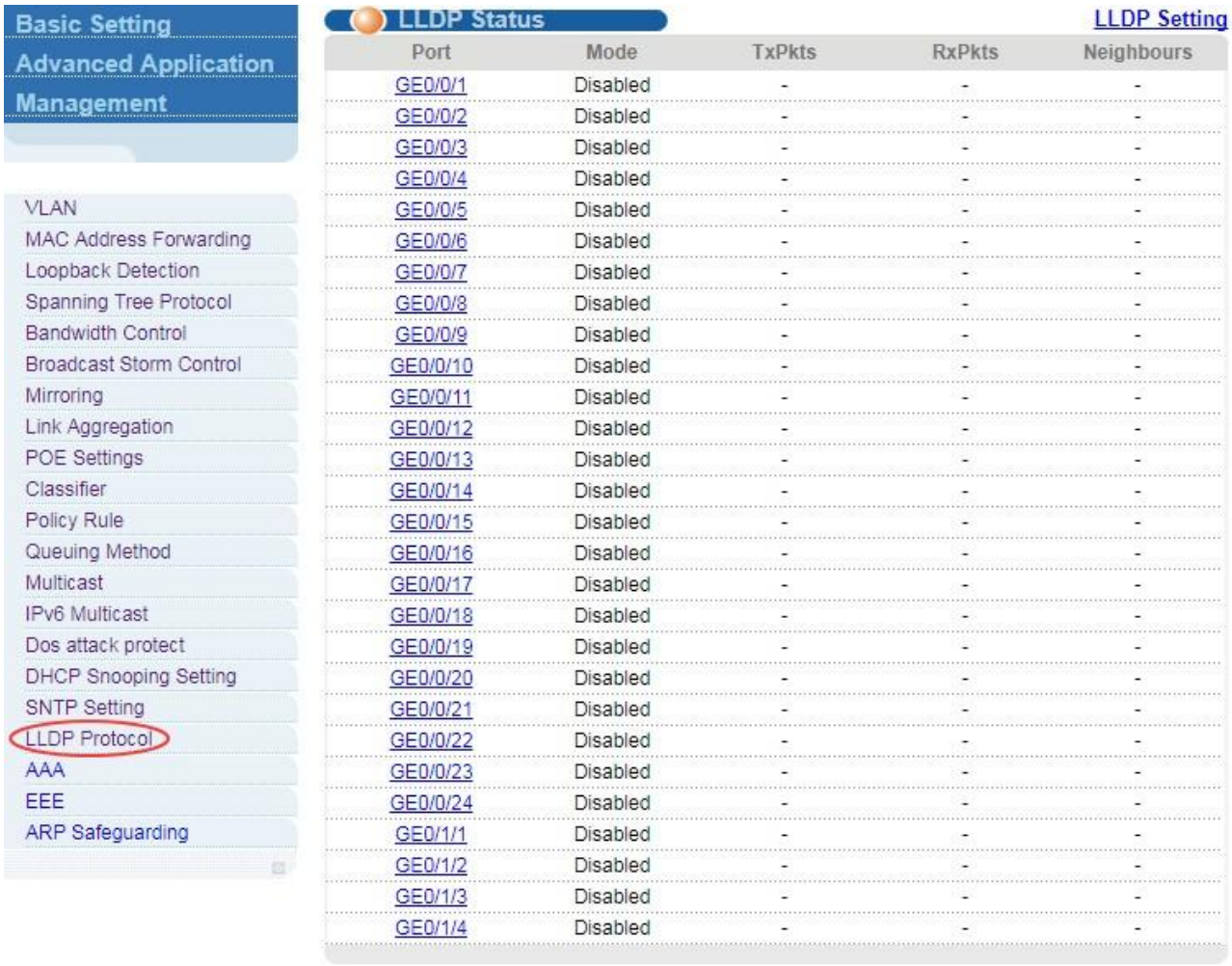
	multicast unicast
SNTP Client Poll Interval	It's interval that SNTP Client sends requests to SNTP Server
SNTP Client Retransmit Times	If SNTP Client does not receive a response within a certain period of time after sending a request,it will resend the request until the number of retransmissions exceeds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

【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)

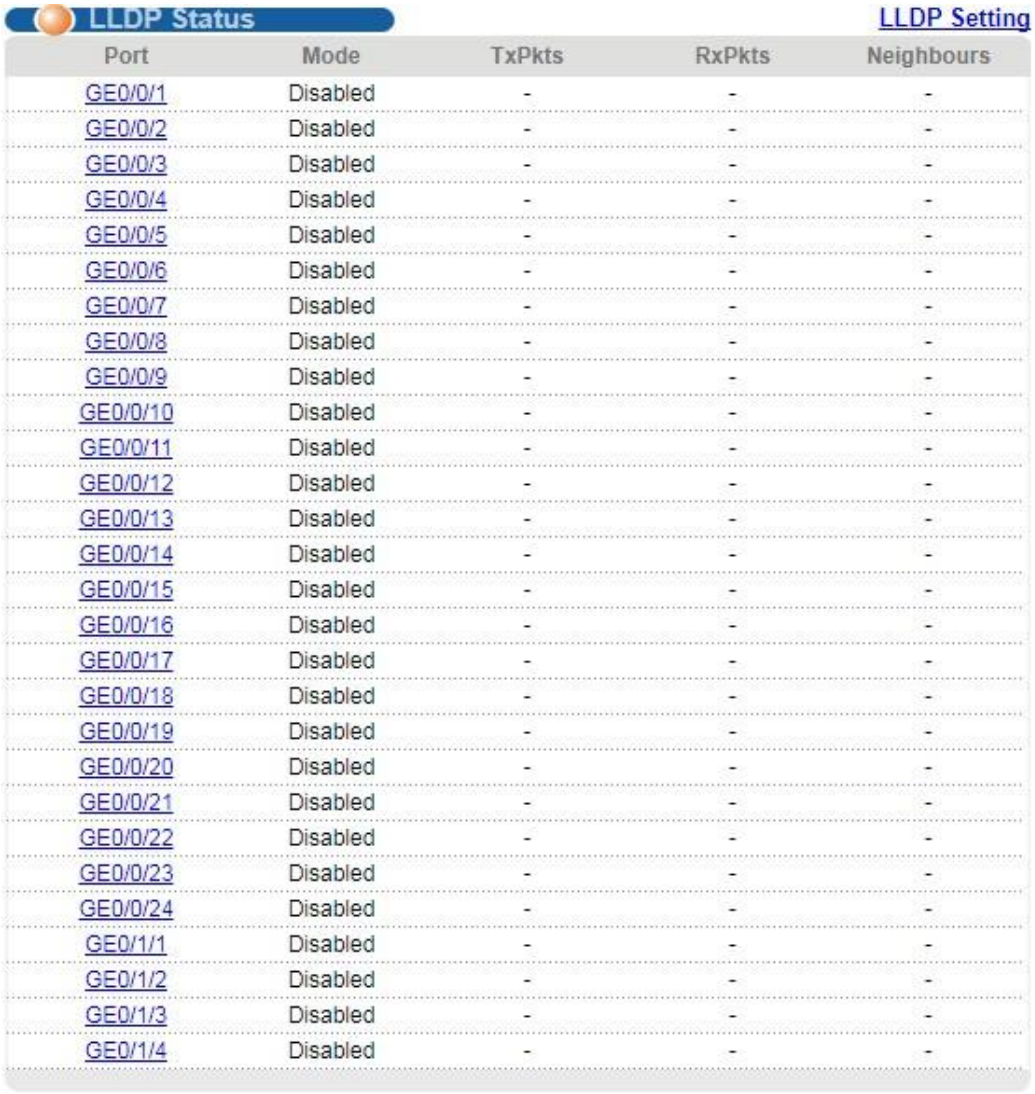
2.2.18 LLDP Protocol

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



2.2.18.1 LLDP Status

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



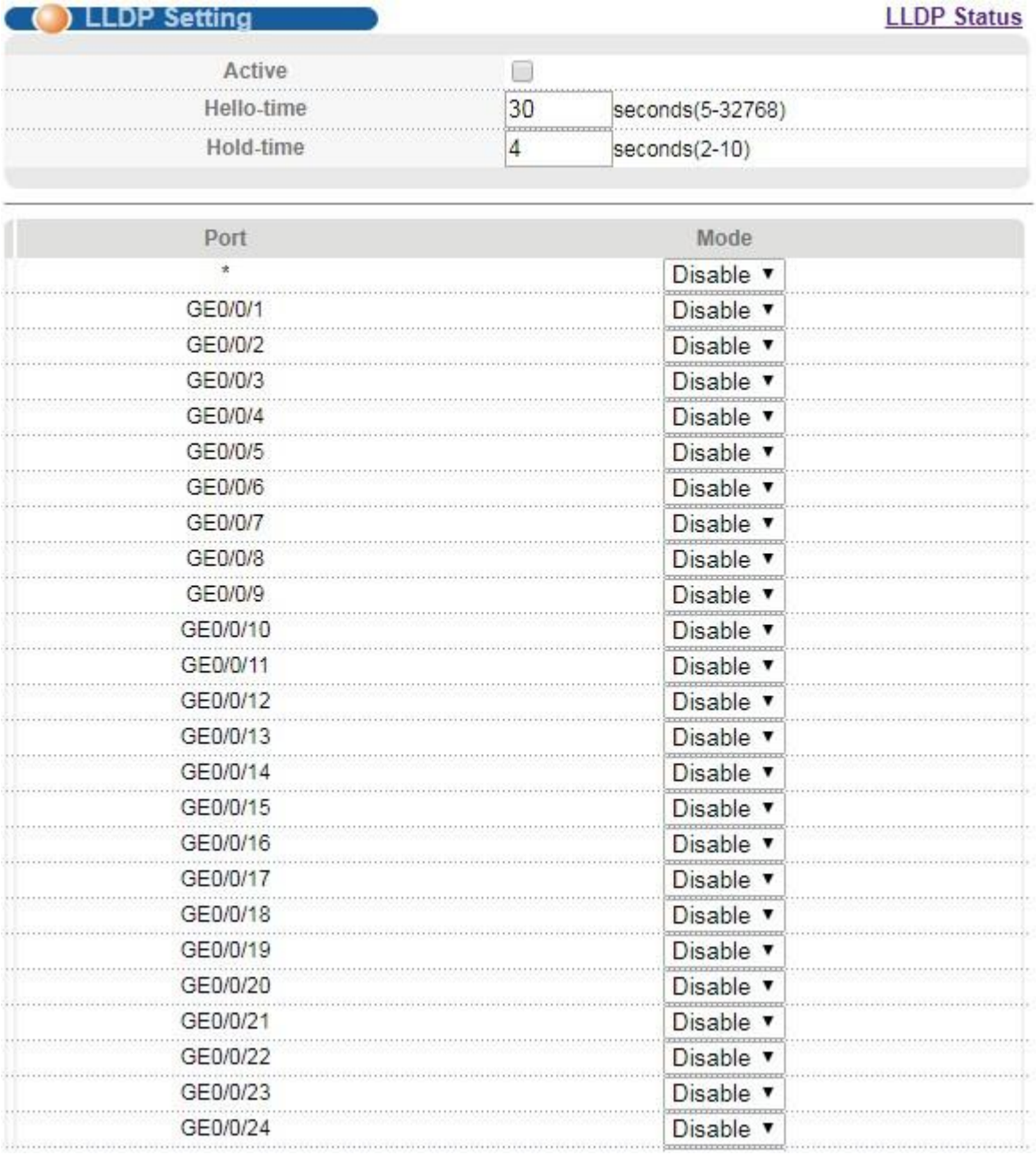
LLDP Status

LLDP Setting

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	-	-	-
GE0/1/1	Disabled	-	-	-
GE0/1/2	Disabled	-	-	-
GE0/1/3	Disabled	-	-	-
GE0/1/4	Disabled	-	-	-

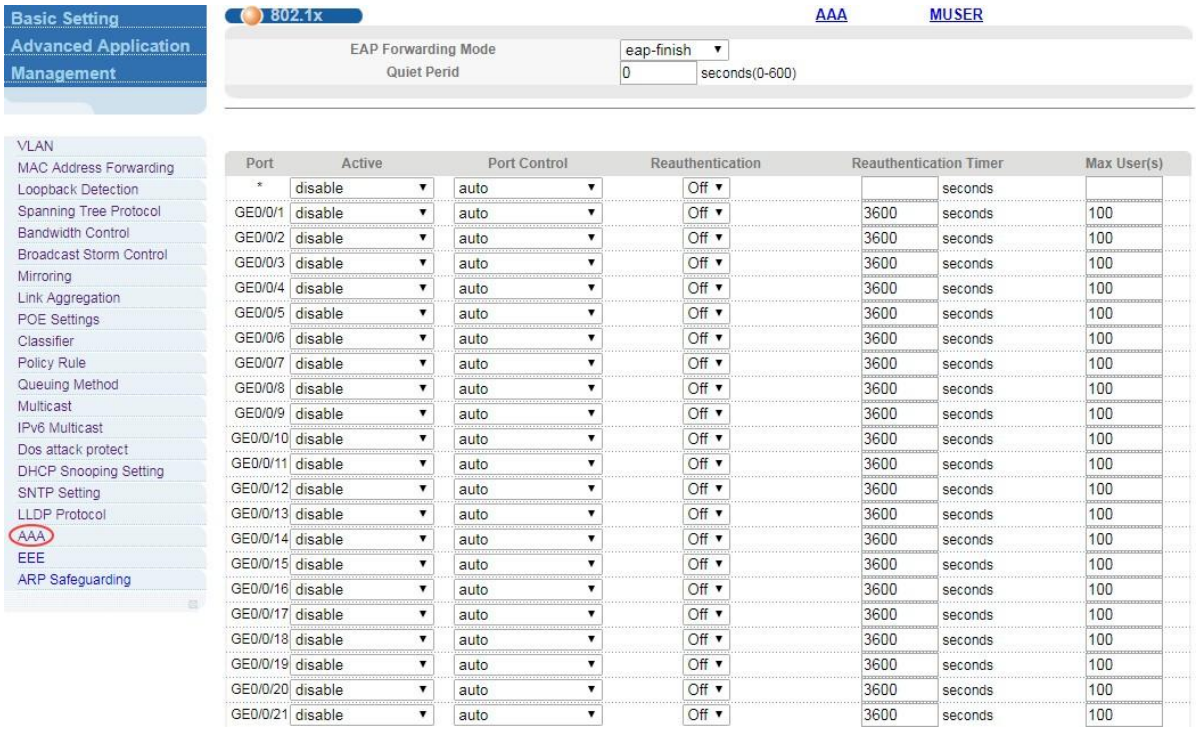
2.2.18.2 LLDP Setting

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



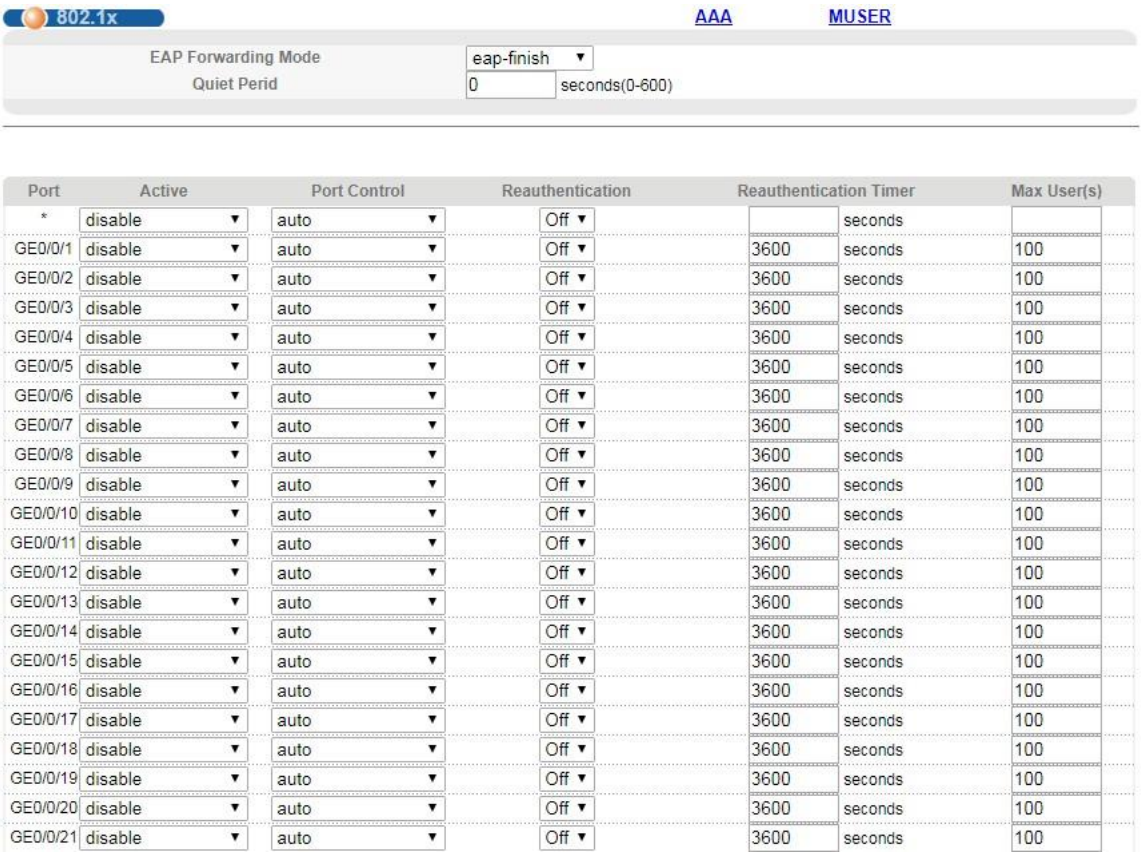
2.2.19 AAA

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



2.2.19.1 802.1x

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



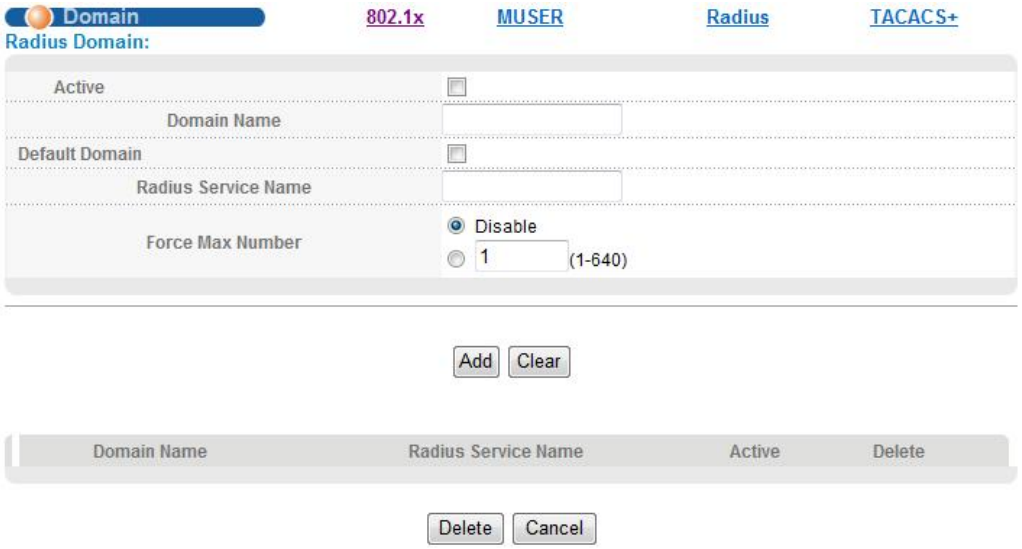
【Parameter Description】

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

2.2.19.2 Radius Domain

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



【Parameter Description】

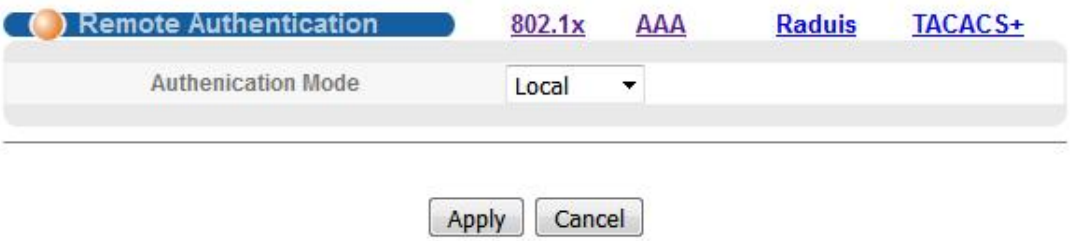
Parameter	Description
Active	Enable or disable radius domain
Domain Name	Set domain name
Radius Server Name	Set Radius Server name
Force Max Number	Maximum number of user connections range: 1-640

【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.

2.2.19.3 Remote Authentication

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

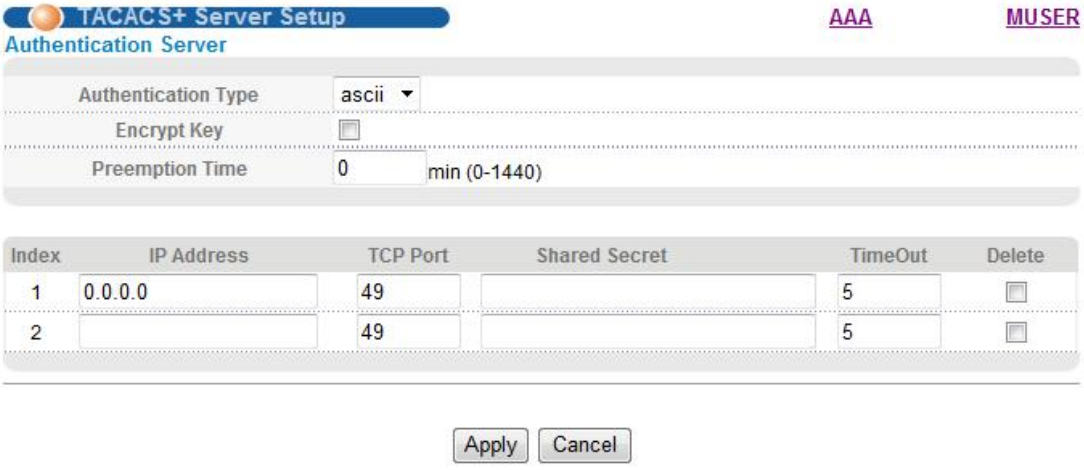


【Parameter Description】

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

2.2.19.4 TACACS+ Server Setup

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



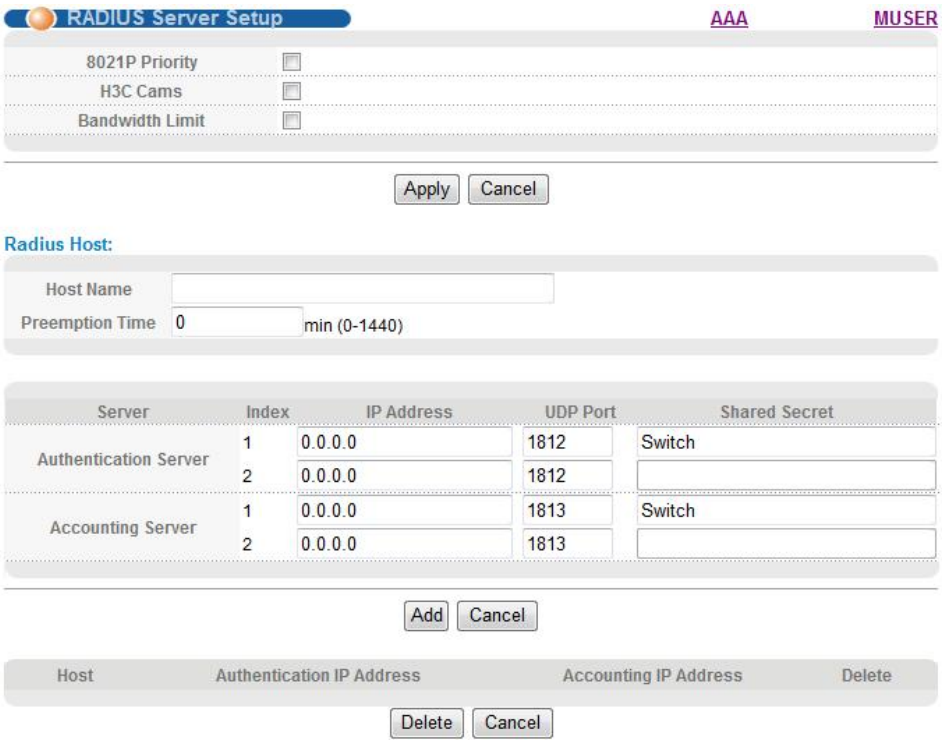
【Parameter Description】

Parameter	Description
Authenication Type	Authenication Mode: ascii, Chap, pap

Preemption Time	The time range of Preemption Time: 0-1440 minutes

2.2.19.5 Radius Server Setup

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



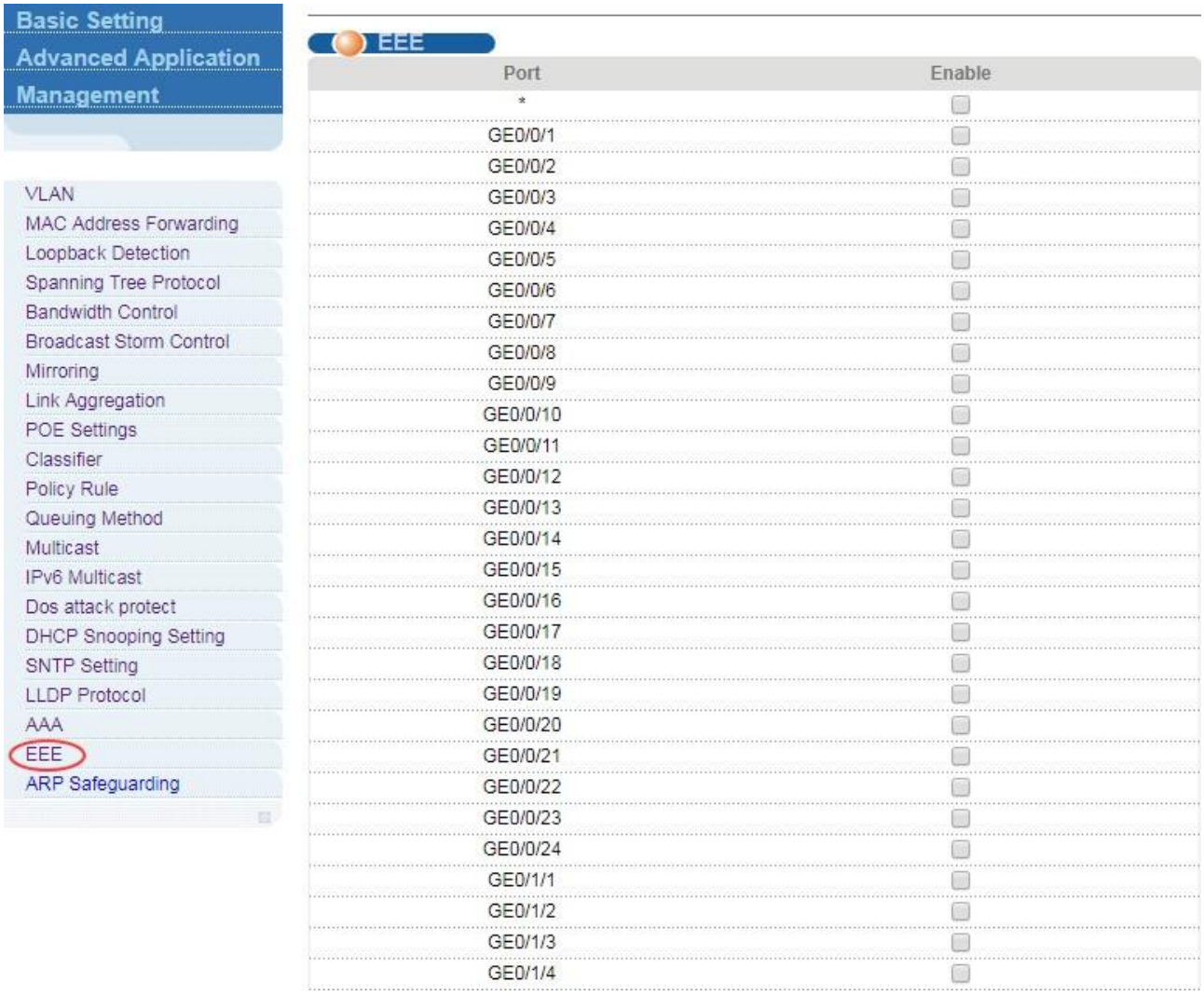
【Parameter Description】

Parameter	Description
8021P Priority	After this function is turned on, if the user authentication is pass, it will modify the PVID of the user's port.
H3C Cams	In this feature, you can configure the version

	information of transmitting clients to the radius server through the radius attribute client-version.
Bandwidth limit	After this function is turned on, if the user authentication is pass, it will modify the Bandwidth of the user's port.

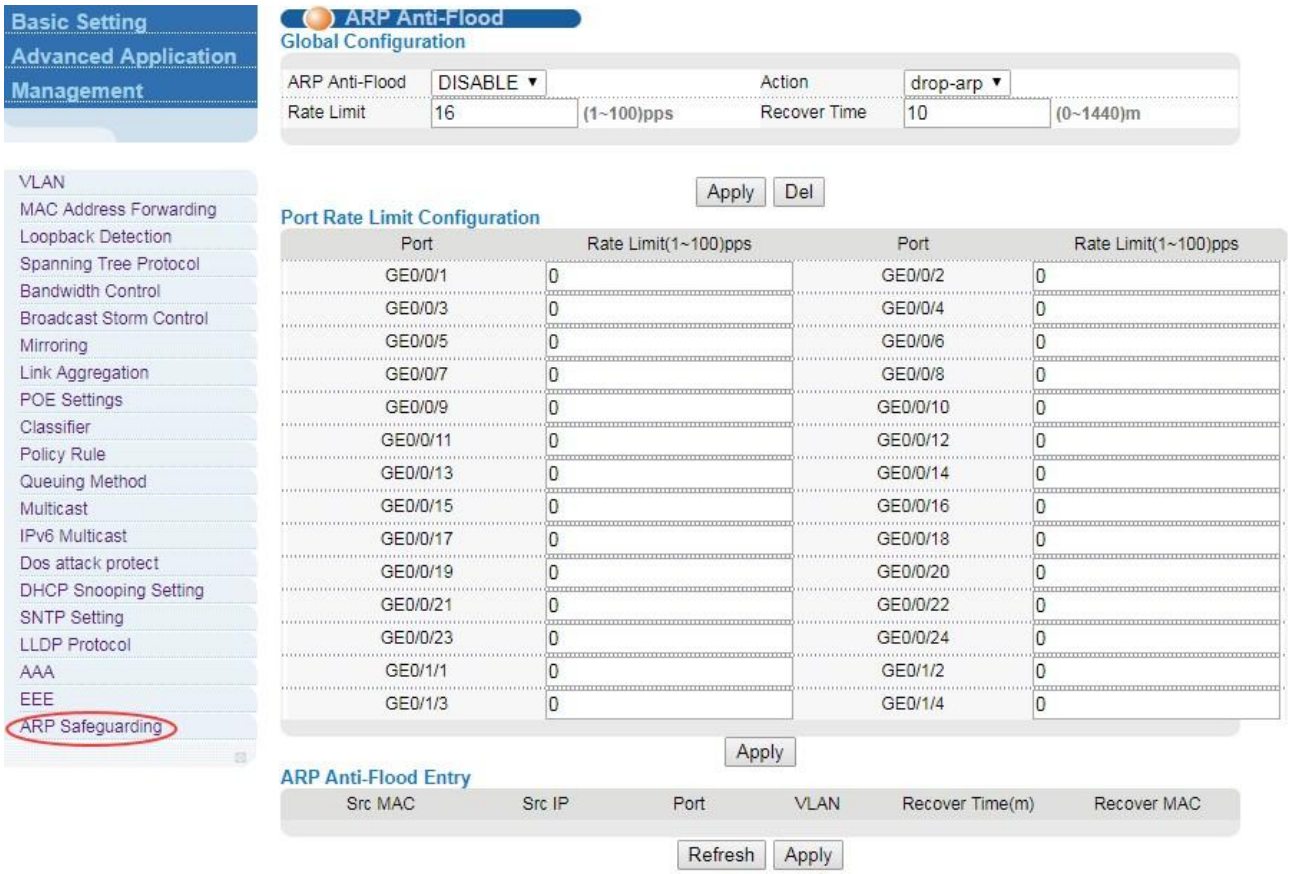
2.2.20 EEE

Selecting “**Advanced Application**>**EEE**", The page can be configured to EEE.



2.2.21 ARP Safeguarding

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



【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.

2.3 Management

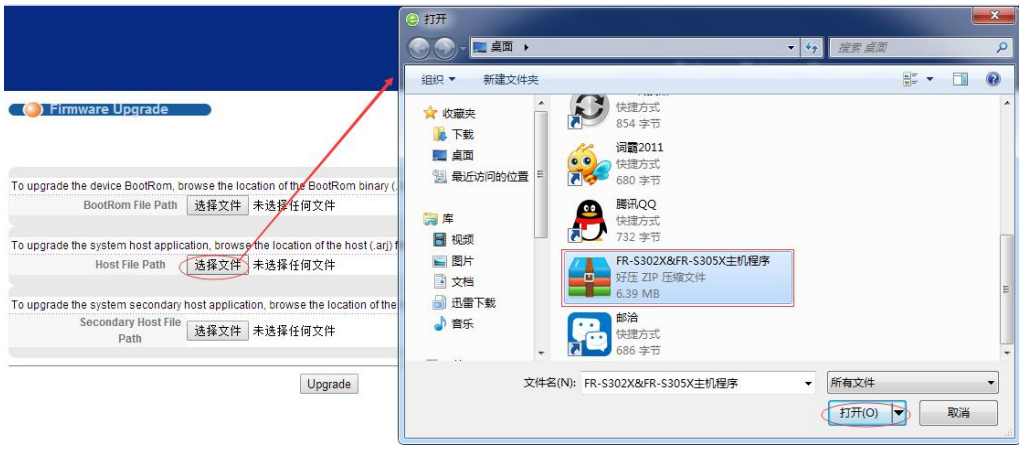
Choose Management, and the following page appears. There are "**Management & Maintenance**", "**Access Control** ", "**Diagnostic**", "**Syslog**", configuration web pages.

2.3.1 Management &Maintenance

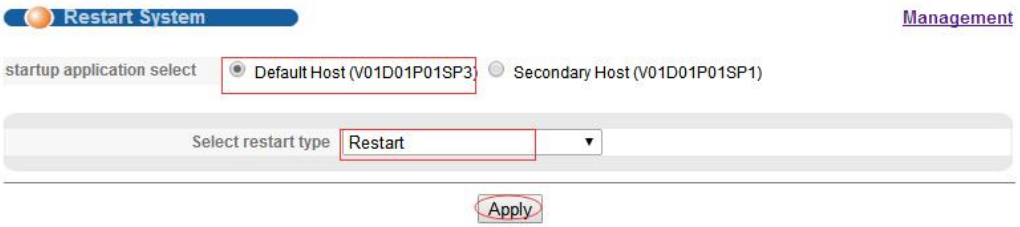
Selecting “**Management**> **Management & Maintenance**", in the navigation bar, you can Upgrade Firmware , Restart System and Maintenance switch.

【Configuration Example】

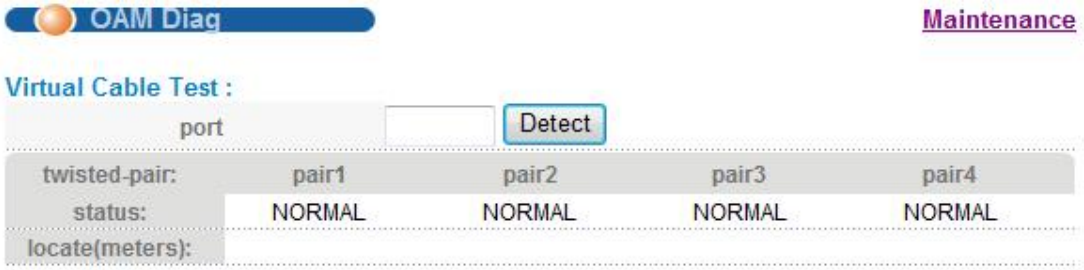
1.Firmware Upgrade



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



3.OAM Diag, Virtual cable can be tested.

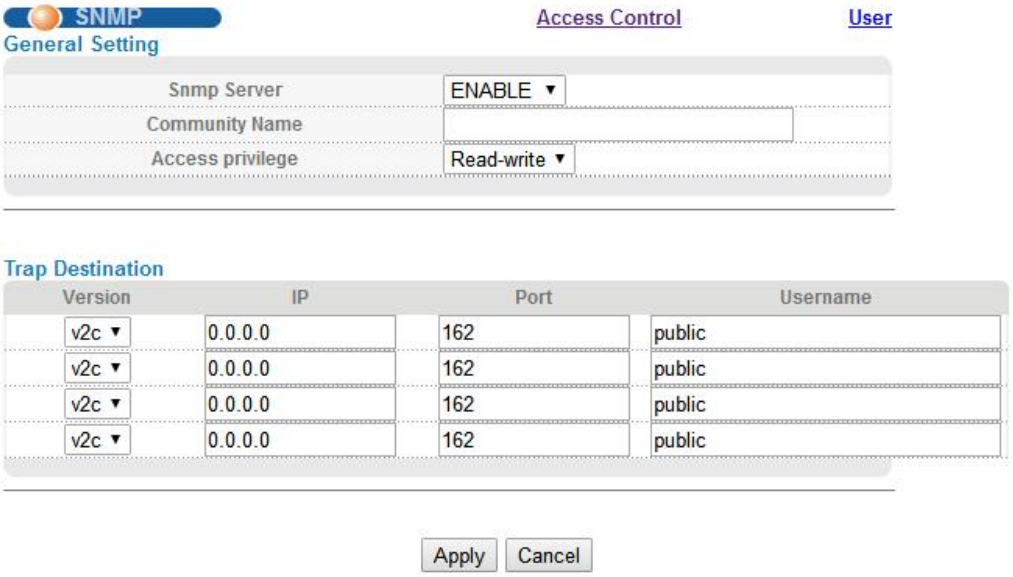


2.3.2 Access Control

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

2.3.2.1 SNMP

Selecting "**Management**> **Access Control**>**SNMP**", in the navigation bar, you can configure SNMP.

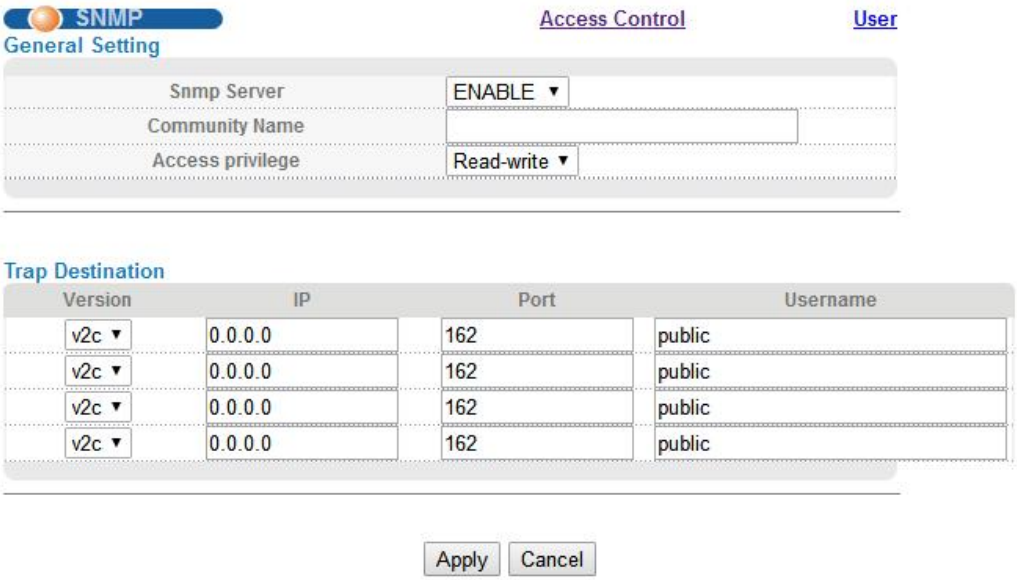


【Parameter Description】

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

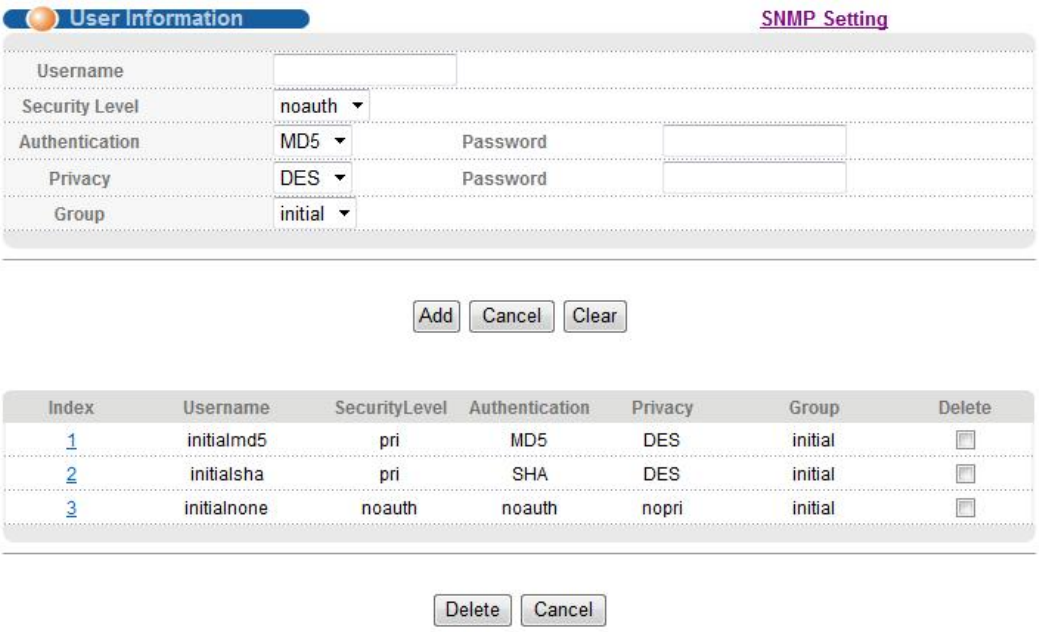
【Configuration Example】

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



2.3.2.2 User Information

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



【Parameter Description】

Parameter	Description
Username	Snmp username
Security Level	noauth

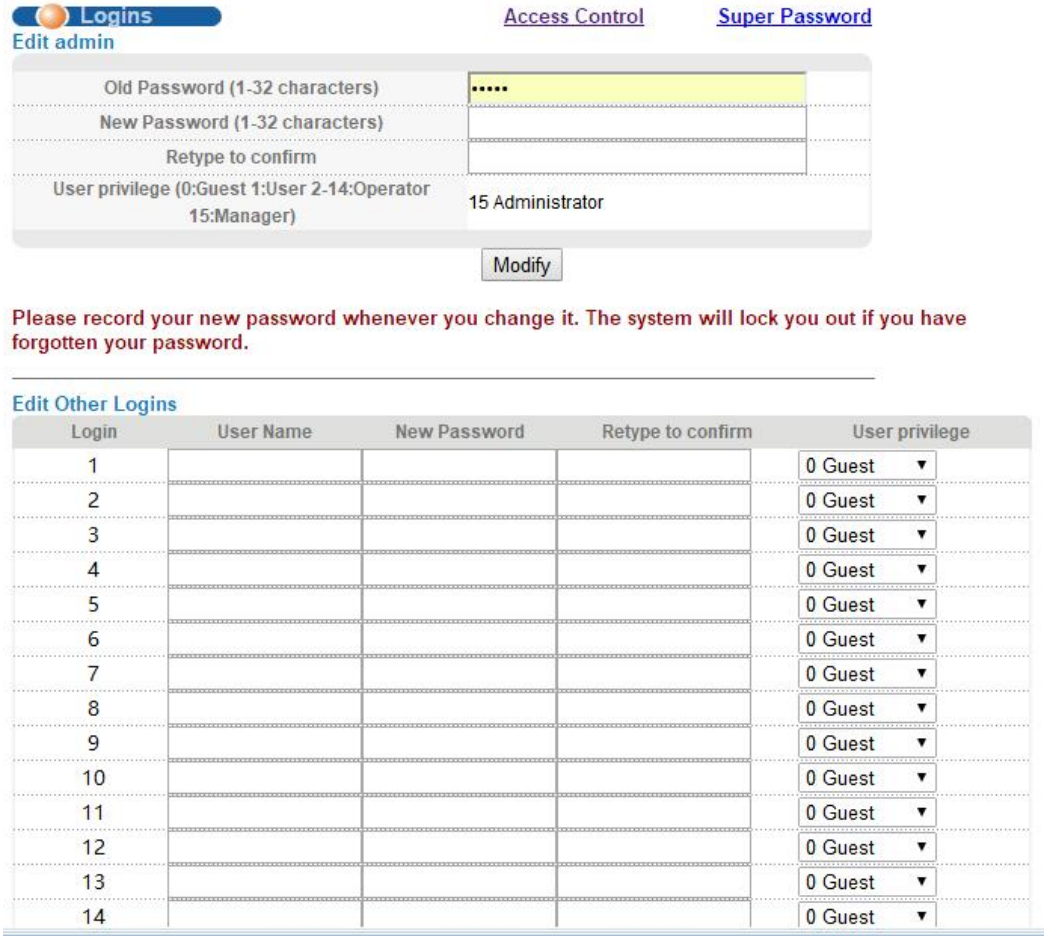
	auth pri
Authentication	MD5 SHA
Privacy	DES Privacy
Group	User group name
Password	Encrypted password

【Configuration Example】

Such as: Add group initial, add username user1.

2.3.2.3 Logins

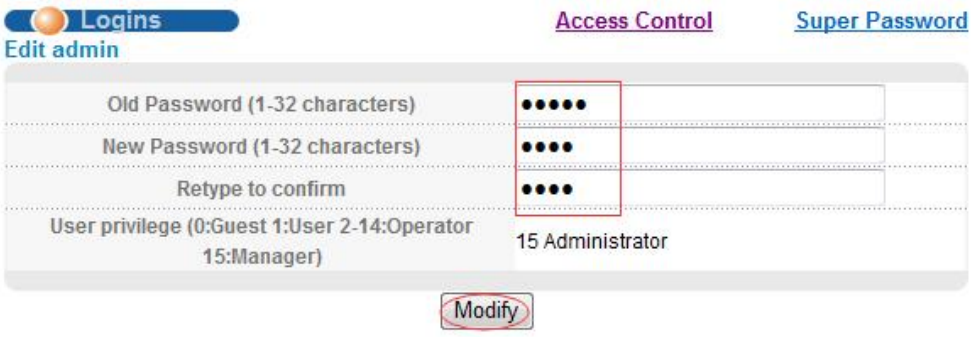
Selecting "**Management>Access Control>Logins**", in the navigation bar, you can modify admin password, configurable ordinary users.

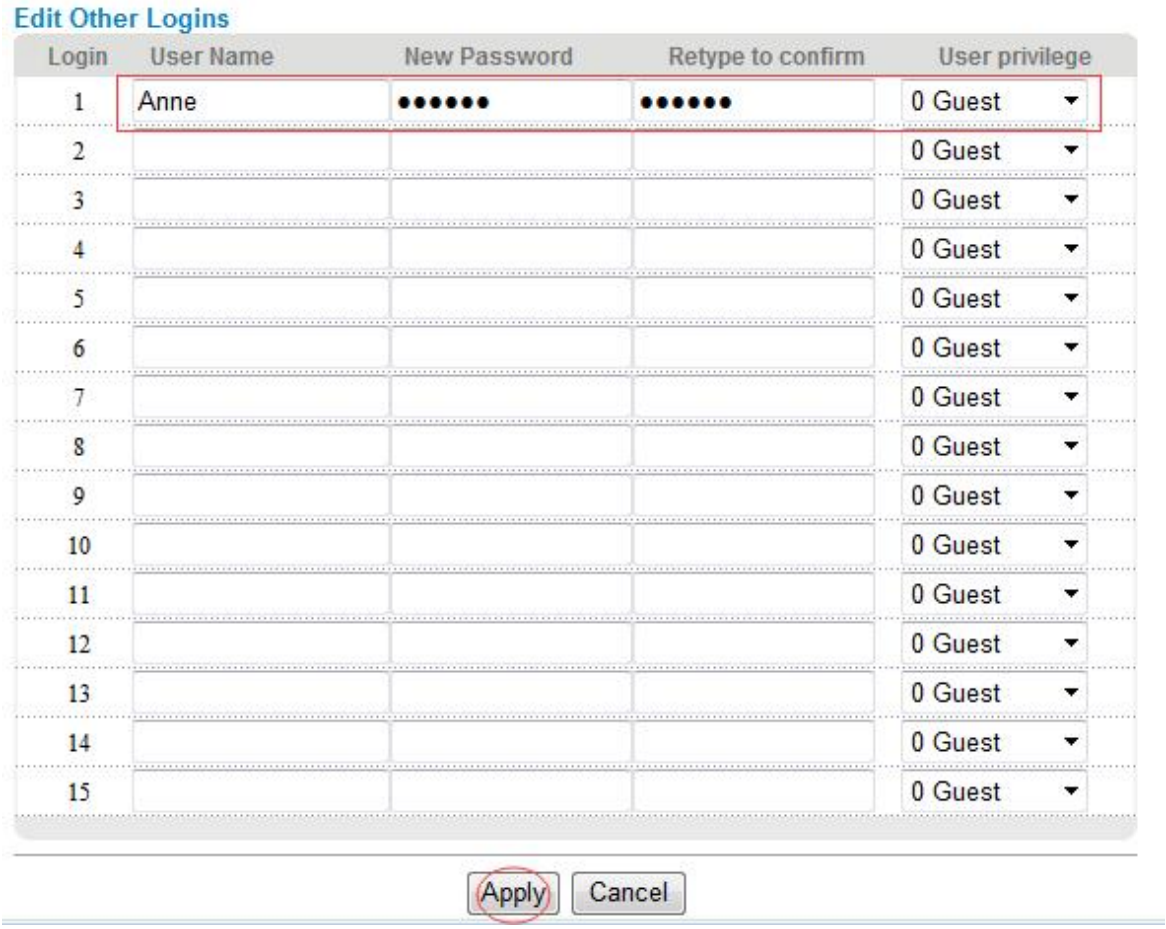


【Parameter Description】

Parameter	Description
User privilege	0: Guest 1:User 2-14: Operator 15:Manager

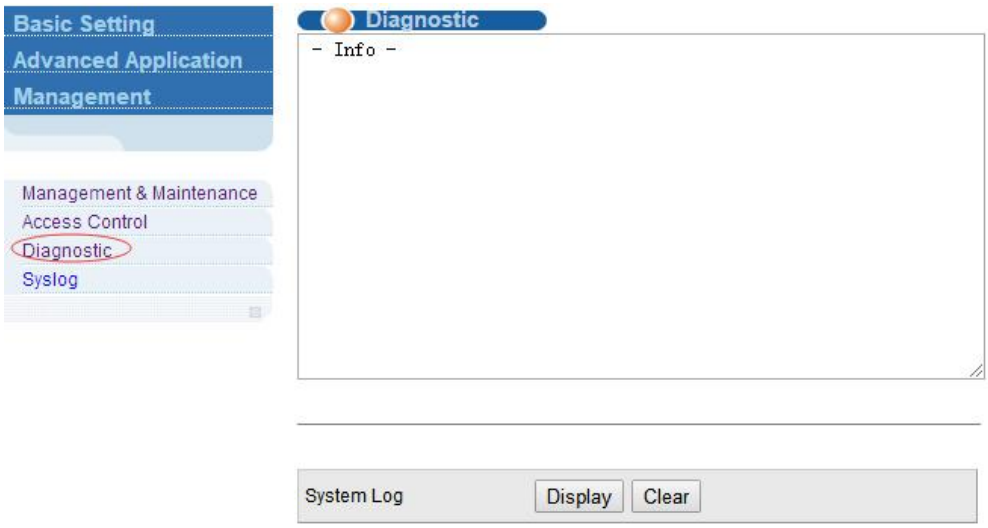
【Configuration Example】





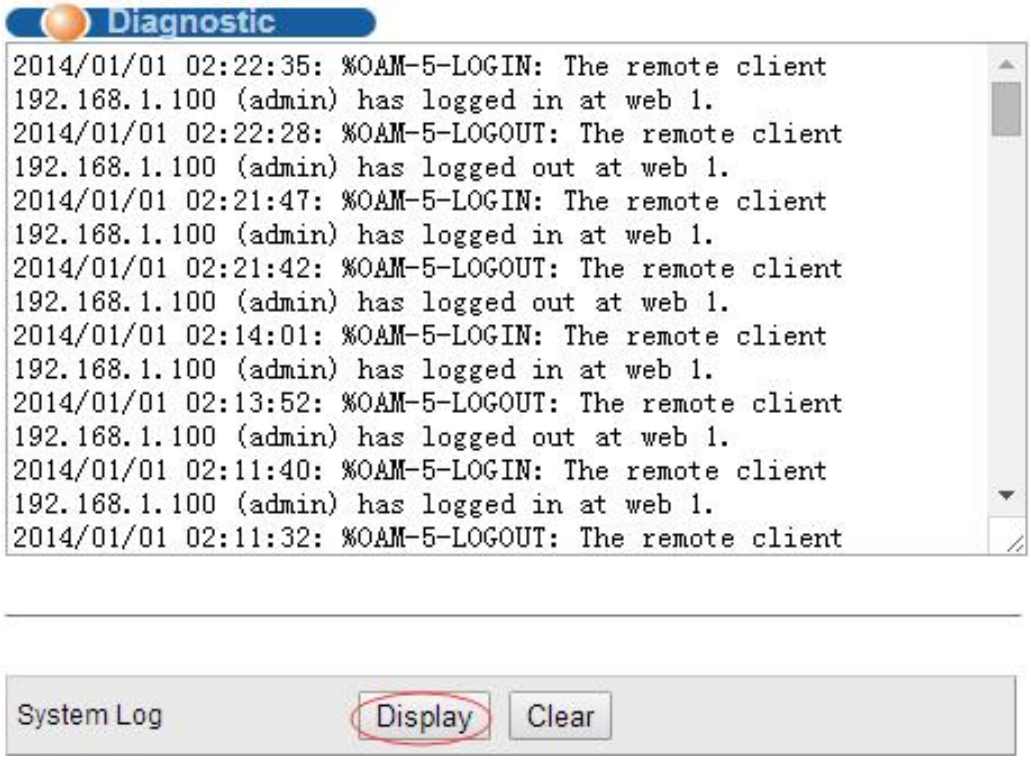
2.3.3 Diagnostic

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



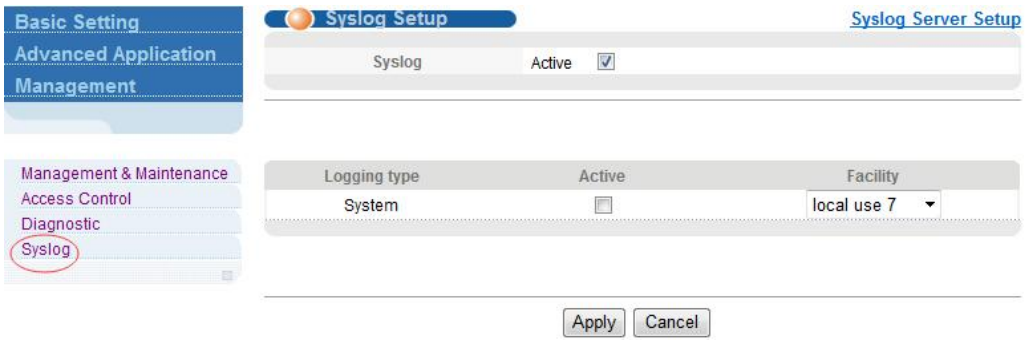
【Configuration Example】

Such as: Display System Log.



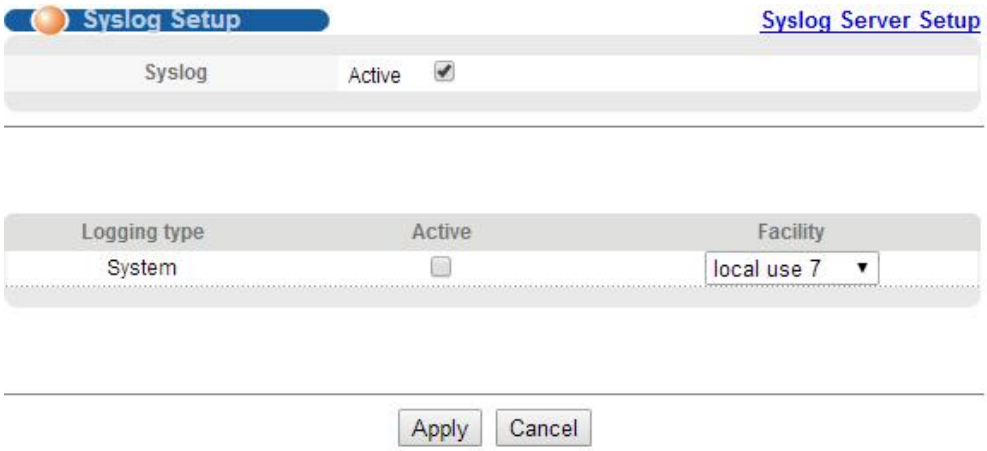
2.3.4 Syslog

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



2.3.4.1 Syslog Setup

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


Syslog Setup
Syslog Server Setup
Syslog
Active
Logging type
Active
Facility
System
local use 7
Apply
Cancel