Web Smart Managed Switches

User Manual

Models 508834, 560559, 561167, 561198, 561341, 561426, 562003

INTELLINET NETWORK SOLUTIONS

intellinet-network.com

Chapter 1 - Product Introduction

Thank you for purchasing this Intellinet Web Smart Managed Switch. Before you install and use this product, please read this manual carefully to benefit from the full set of features that are available.

1.1 Product Overview

These Layer 2 switches are designed to create a high-security and high-performance network with Self-Healing Network features. They provide from eight to 24 10/100/1000 Mbps auto-sensing RJ45 ports and 100/1000 Mbps SFP optical ports. All ports support wire-speed forwarding and can provide you with larger network flexibility.

Some of our newer features have been labeled as Self-Healing Network (SHN) features. These features are designed to assist in the automated preservation of health on the network. To assist even further, we have partnered with Domotz™ to provide the additional option of Cloud Management, which gives the ability to administer our managed switches from any internet-connected device through an app on your smartphone or web application hosted by Domotz (Cloud Management is subscription-based, and information can be found at the following link: https://www.domotz.com/residential-plan.php.)

1.2 Features

- Compliance with IEEE 802.3i, IEEE 802.3u, IEEE802.3x, IEEE802.3ab, IEEE802.1q, IEEE802.1p standards
- In PoE versions, supports IEEE802.3af, IEEE802.3at standards, management of the PoE ports, PoE port power on/off, and port output power restriction
- Web interface management
- Up to 24 x 10/100/1000 Mbps Auto MDI/MDI-X Ethernet ports, ports Auto MDI/MDIX
- 8K-entry MAC address table of the Switch with auto-learning and auto-aging
- Supports IEEE802.3x flow control for Full-duplex Mode and backpressure for Half-duplex Mode
- Supports QoS (quality of service), port mirroring, link aggregation protocol
- Supports packet length 9,216 bytes jumbo frame packet forwarding at wire speed
- LED indicators for monitoring Link / Activity / Speed and, in PoE versions, PSE monitoring

1.3 External Component Description

1.3.1 Front Panel (Example shown from 560559)

Depending on your model number, the front panel of the Switch consists of up to 24 x 10/100/1000 Mbps RJ45 ports, 4 x 1000 Mbps SFP ports (and 4 x Uplink RJ45 ports), 1 x Console port, 1 x Reset button and a series of LED indicators as shown as below.

A — 10/100/1000 Mbps RJ45 ports (1 – 24):
Designed to connect to a device with a bandwidth of 10 Mbps, 100 Mbps or 1000 Mbps. Each has a corresponding 10/100/1000 Mbps LED (see E — LED indicators below).

B — SFP ports (SFP1, SFP2, 25S, etc.):
Designed to install an SFP module and connect to the device with a bandwidth of 1000 Mbps. Each has a corresponding 1000 Mbps LED.

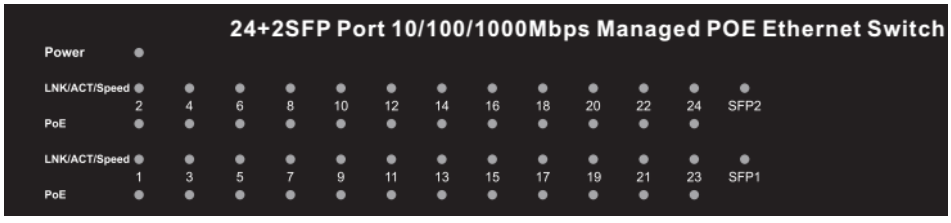
Combo ports (25-28T) on model 561426:

The four SFP receiver slots are shared with four related RJ45 ports (25-28T). An SFP port and a related RJ45 port are called "composite" ports, which means that they can't be used at the same time. Either the SFP port works or the RJ45 port works.

C — Console port (Console):
Designed to connect with the serial port of a computer or terminal for monitoring and configuring the Switch.

D — Reset button (Reset):
With the device powered on, press down the button for about 5 seconds. The system restores the factory default settings.

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



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

LED	COLOR	STATUS	STATUS DESCRIPTION
Power	Green	On	Power On
		Off	Power Off
LINK/ACT/ Speed (1 – 24; 25T – 28T)	Orange (10/100 Mbps)	On	A device is connected to the port
		Off	No device is connected to the port
	Green (1000 Mbps)	Flashing	Sending or receiving data
LINK/ACT/ Speed (SFP1, 2)	Green	On	A device is connected to the port
		Off	No device is connected to the port
		Flashing	Sending or receiving data
PoE (1 – 24) (excluding 508834)	Yellow	On	A Powered Device is connected to the port and is receiving power.
		Off	No Powered Device is connected to the port, or no power is supplied according to the power limits of the port.
		Flashing	The PoE power circuit may be in short or the power current may be overloaded.

1.3.2 Rear Panel (19 Rackmount/Desktop example shown)

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

F — AC Power Connector:
Power is supplied through an external AC power adapter. See specifications for your model.

G — Grounding Terminal:
The Switch already comes with a Lightning Protection Mechanism. You can also ground the Switch through the PE (Protecting Earth) cable of an AC cord or with a Ground Cable.

1.4 Environment

- Operating Temperature: 0°C – 45°C
- Storage Temperature: -40°C – 70°C
- Operating Humidity: 10% – 90% non-condensing
- Storage humidity: 5% – 90% non-condensing

1.5 Package Contents

Before installing the Switch, make sure that the following the packing list matches the items in the packaging. If any part is lost and damaged, please contact your local agent immediately. In addition, make sure that you have the tools to install switches and cables on hand.

- One Managed Ethernet Switch
- Four rubber feet, two mounting ears and eights screws (except for Industrial version 508834, which is for DIN Rail mounting)
- One AC power cord (except for Industrial version 508834, which is designed to receive power from an Industrial power source)
- Quick Install Guide

Chapter 2 - Installing and Connecting the Switch

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

2.1 Installation (19 Rackmount & Desktop version)

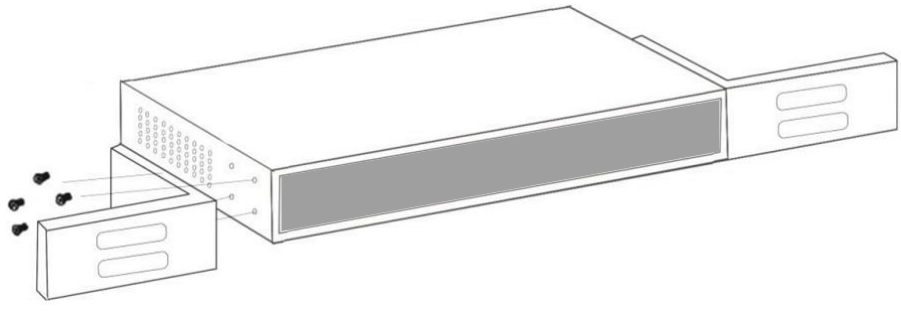
Please follow these instructions to avoid incorrect installation, cause device damage or security threats.

- Put the Switch on stable place or desktop to prevent damage from falling.
- Make sure the Switch works in the proper AC input range and matches the voltage labeled on the Switch.
- To prevent electrical shocks, do not open the Switch's housing, even in power failure or if disconnected from a power source.
- Make sure that there is proper heat dissipation from and adequate ventilation around the Switch.
- Make sure the cabinet can hold the weight of the Switch and its accessories.

2.1.1 Installation in a 19-inch Rack / Cabinet

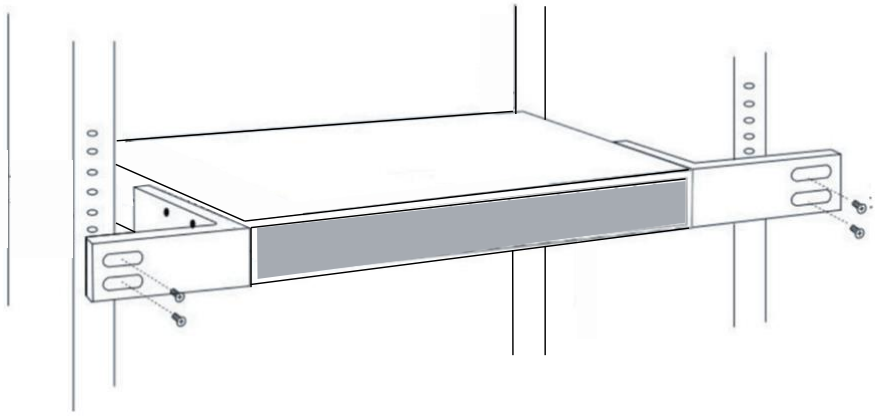
The Switch can be mounted in an EIA standard-sized, 19-inch rack, which can be placed in a wiring closet with other equipment. To install the Switch, follow these steps:

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



Bracket Installation

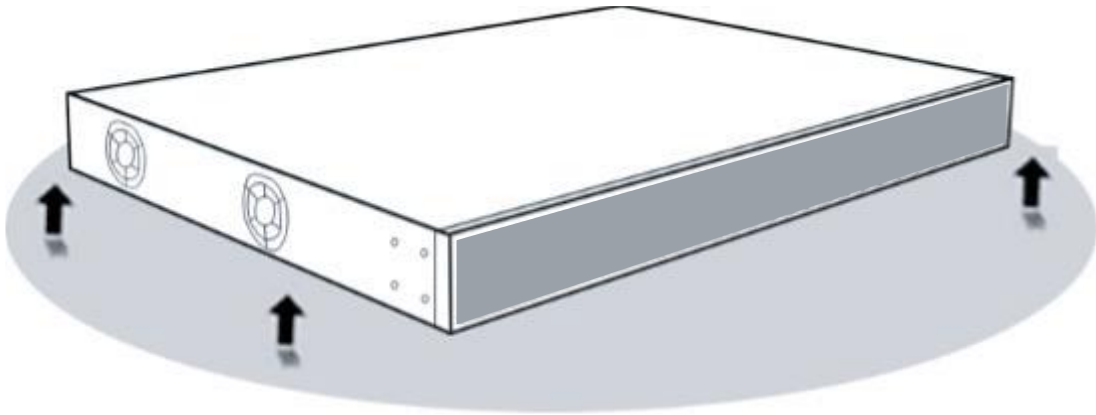
b. Use the screws provided with the equipment rack to mount the Switch on the rack and tighten it.



Rack Installation

2.1.2 Desktop Installation

If users are not equipped with a 19-inch standard cabinet, install the Switch on a desktop. Attach the included rubber feet on the bottom of the Switch at each corner to minimize external vibration. Allow adequate space for ventilation between the device and the objects around it.

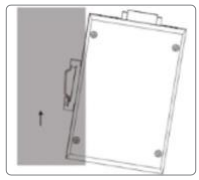


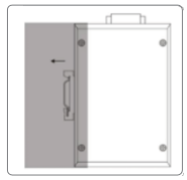
Desktop Installation

2.1.3 DIN Rail Installation

For Industrial Models, the Switch can be installed onto a DIN rail. Follow these instructions:

1. With the DIN-rail bracket attached to the device with screws, angle the bracket onto the DIN rail.
2. Push in the device until it clicks into place.

1. 

2. 

2.1.4 Power on the Switch

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

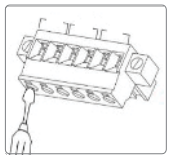
AC Electrical Outlet:
It is recommended to use single-phase three-wire receptacle with neutral outlet or multifunctional computer professional receptacle. Please make sure to connect the metal ground connector to the grounding source on the outlet.

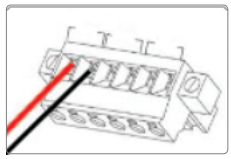
AC Power Cord Connection:
Connect the AC power connector in the back panel of the Switch to external receptacle with the included power cord, and check the power indicator is ON. When it is ON, it indicates the power connection is OK.

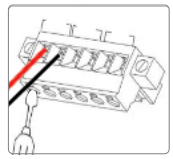
DC Terminal Block Installation (for Industrial models)
NOTE: Ensure all power is off/disconnected before beginning!

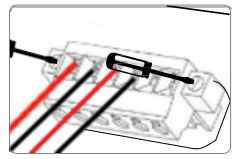
1. Loosen appropriate screws.
2. Insert bare power-supply wires into appropriate terminal slots (positive wire into positive slot; negative wire into negative slot).
3. Tighten appropriate screws to secure wires. (If desired, repeat steps 1 – 3 on second input pair.)
4. Install block into the device and tighten screws.

Example — Your model may be different.

1. 

2. 

3. 

4. 

2.2 Connect Computer (NIC) to the Switch

After installing the network card driver, insert the NIC into the computer. Connect one end of the twisted pair to the RJ45 jack on your computer, and connect the other end to any RJ45 port of the Switch, with a maximum distance of 100 meters between the Switch and the computer. Once the connection is OK and the devices power on normally, the LINK/ACT/Speed status indicator lights, corresponding to ports on the Switch.

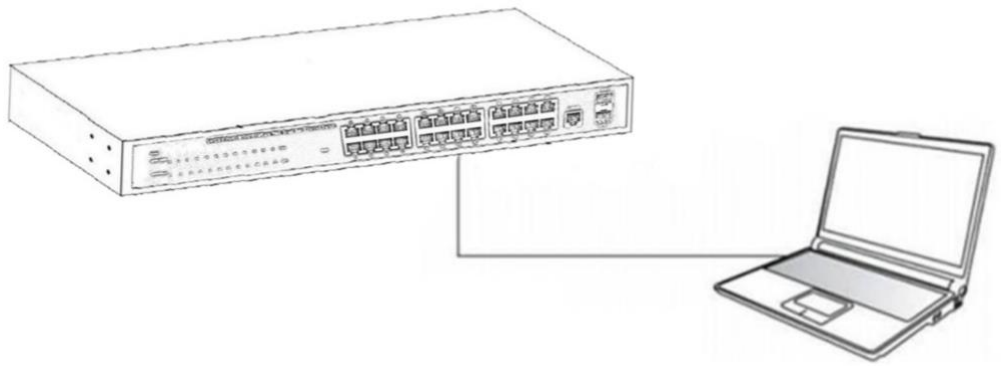
2.3 Switch connection to the PD (excluding 508834)

On PoE models, any ports that have a PoE indicator also have the PoE power supply function, which makes it possible to provide power to PD devices such as VoIP phones, network cameras, wireless access points and more. You only need to connect the Switch PoE port directly to the PD with a network cable.

Chapter 3 - How to Log into the Switch

3.1 Switch to End Node

Use standard Cat5 and higher 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 Indicator table shown above. The LNK/ACT/Speed LEDs for each port lights when the link is available.

3.2 Login Information

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

Parameter	Default Value
Default IP address	192.168.2.1
Default Username	admin
Default Password	SERIAL NUMBER (S/N; found on the bottom of the switch)

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

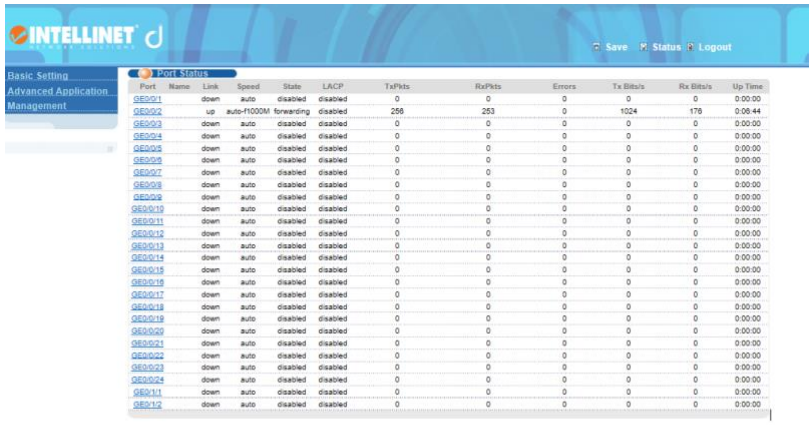
1. Connect the Switch with the computer NIC interface.
2. Power on the Switch.

3. Check whether the IP address of the computer is within this network segment: 192.168.2.xxx (xxx ranges 2 – 254), for example, 192.168.2.100.
4. Open the browser and enter http://192.168.2.1 and then press Enter. The Switch login window appears with the following picture:

Enter the Username and Password. The factory default Username is **admin** and the initial Password is the same as the serial number found on the bottom of the switch. Then click **Login** to log into the Switch configuration window.

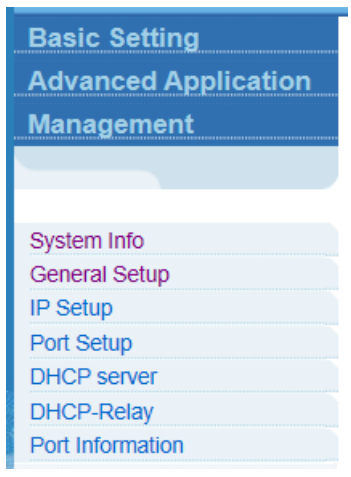
Chapter 4 - Web Configuration Guide

The Switch configuration interface consists of three main areas: the status bar at the top, the left function menu bar, and the main configuration window. Select the different functions in the function menu bar to modify all settings in the main configuration window.



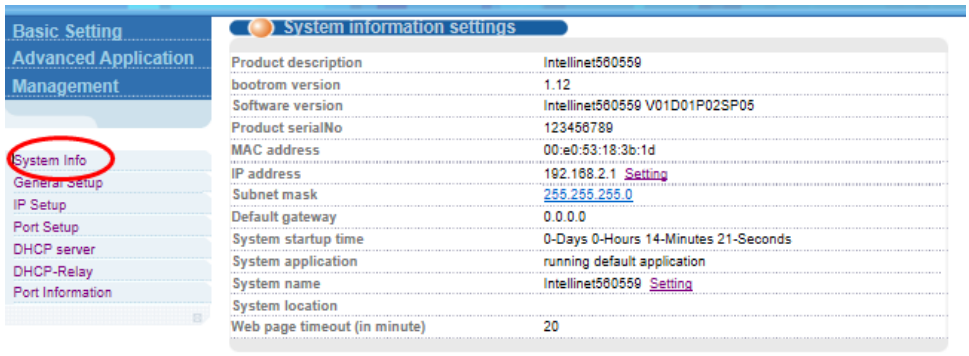
4.1 Basic Setting

Choose Basic Setting, and the following page appears. There are configuration web pages for **System Info**, **General Setup**, **IP Setup**, **Port Setup**, **DHCP server**, **DHCP-Relay**, and **Port Information**.



4.1.1 System Info

To view the basic information of System and configure the IP address and System name, select **Basic Setting**>**System Information settings** in the function menu bar.



【Parameter Description】

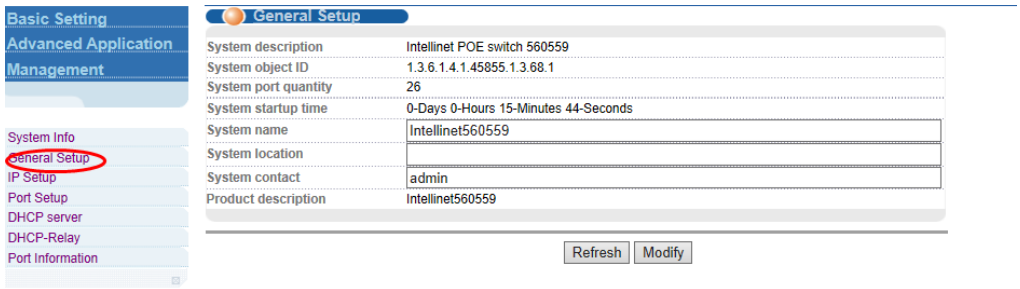
Parameter	Description
Product description	Brief description of device type
Software version	Show switch's current software version.
MAC address	Show switch's physical address.
IP Address	The management IP of Switch
Subnet Mask	Configure the corresponding subnet mask of the IP address specified above. The default is 255.255.255.0.
Default Gateway	Specify a gateway address for the switch.
System name	System name.
System Location	Specify the system location.

【Information】

You can view and configure Running System status.

4.1.2 General Setup

To view the basic information of Switch, such as System Description and so on, select **Basic Setting**>**General Setup** in the function menu bar. You can also modify the System name, System contact and System location.



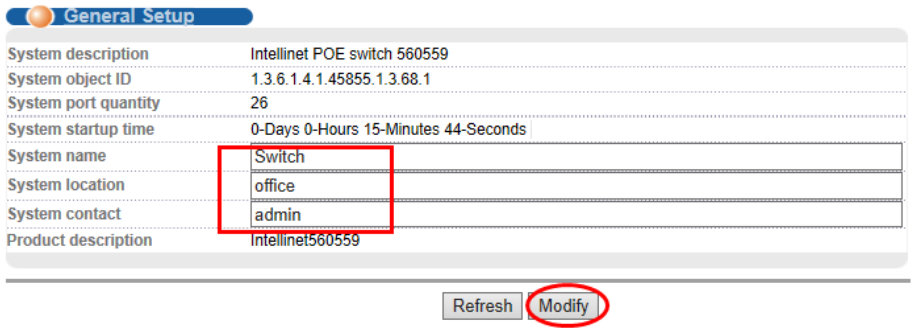
【Parameter Description】

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

【Configuration example】

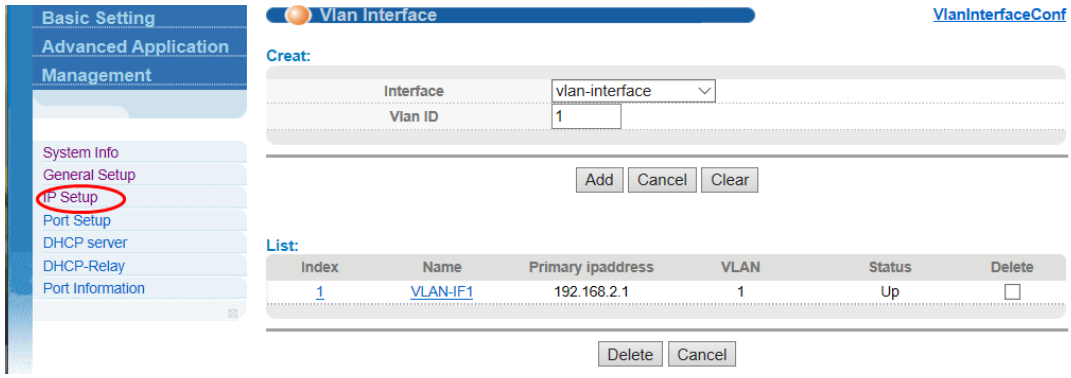
To configure general system information:

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



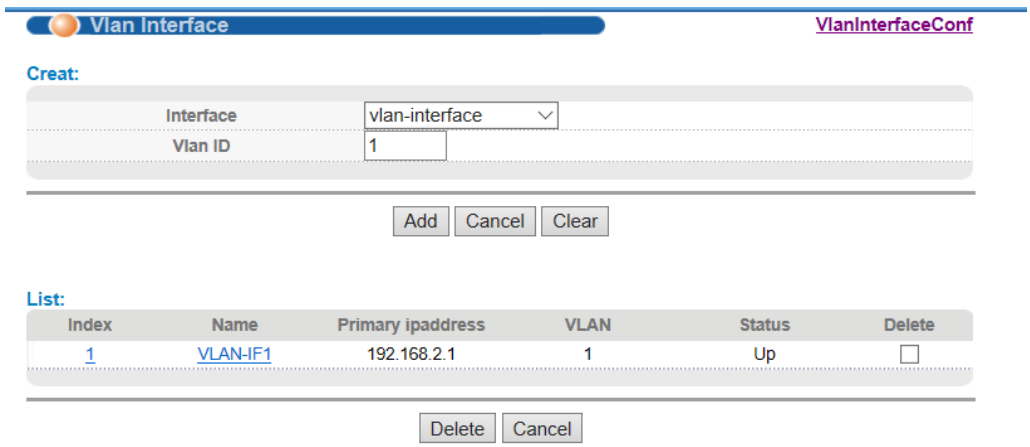
4.1.3 IP Setup

To configure the IP, select **Basic Setting**>**IP Setup** in the function menu bar.



4.1.3.1 VLAN interface

To configure the VLAN Interface, select **Basic Setting**>**IP Setup**>**Vlan interface** in the function menu bar.

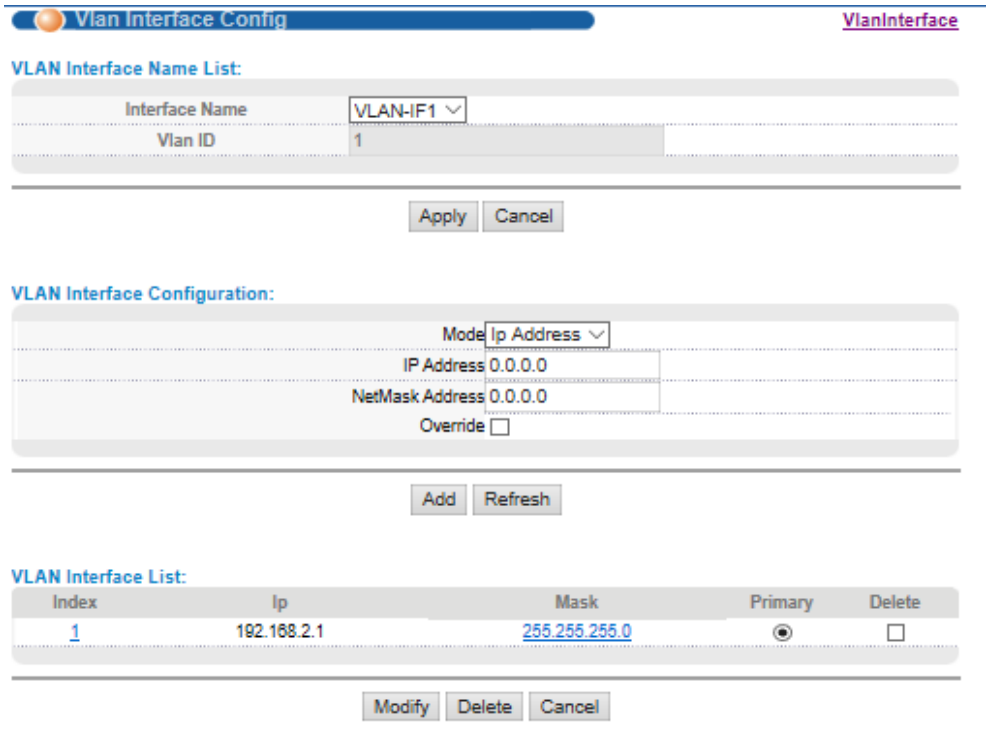


【Parameter Description】

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

4.1.3.2 VLAN Interface Config

To adjust settings to the VLAN Interface Configuration, select **Basic Setting**>**IP Setup**>**Vlan Interface Config** in the function menu bar.



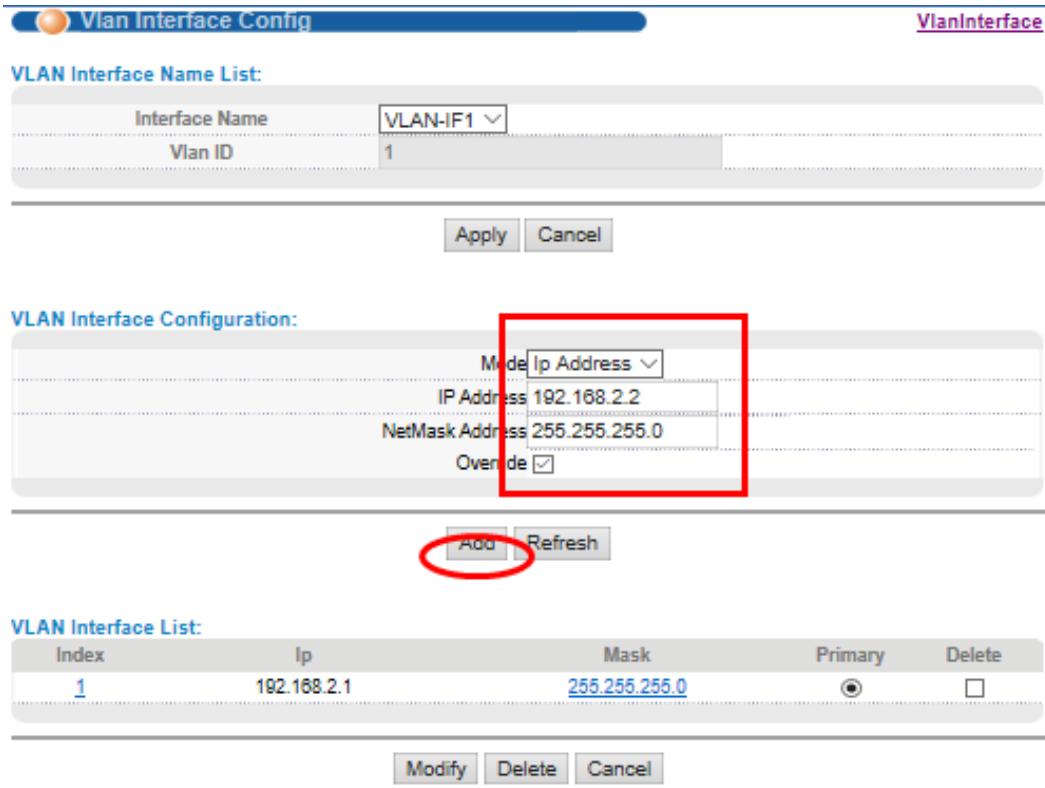
【Parameter Description】

Parameter	Description
Interface name	Name of interface
Vlan ID	Specify the VLAN ID
IP Address	The IP address to log into the Switch
Override	You can override former original primary IP or not

【Configuration example】

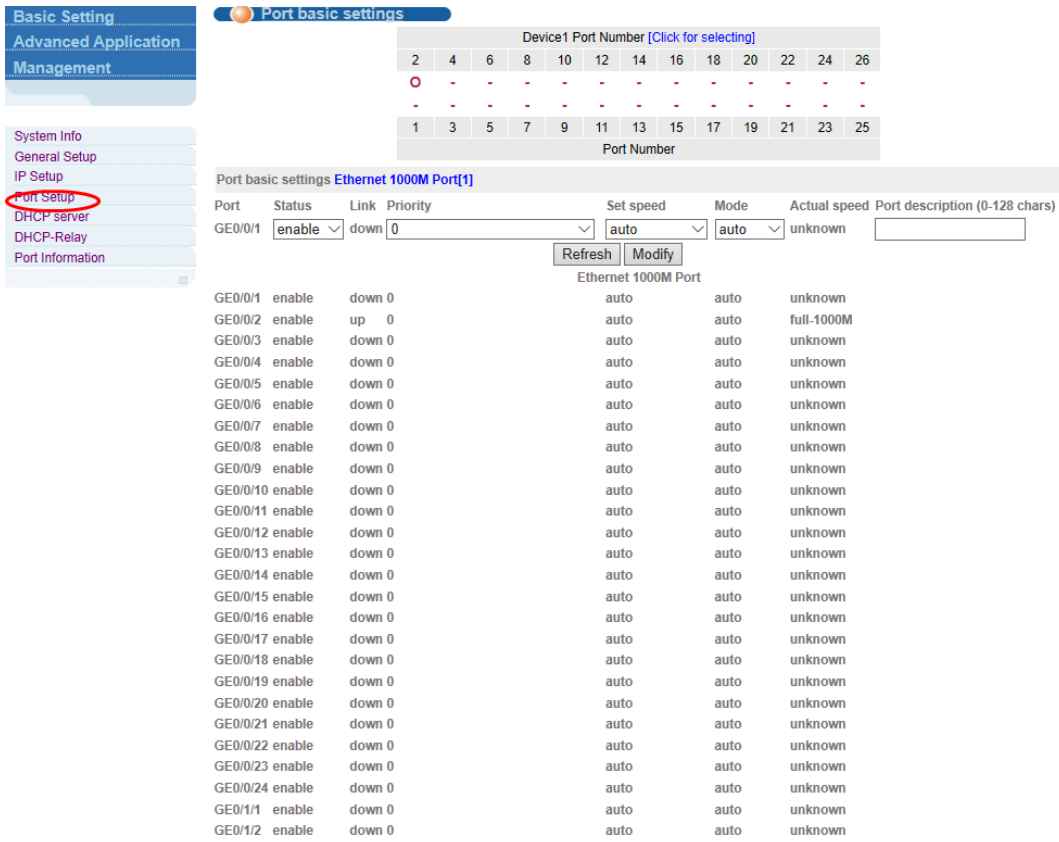
To configure general system information:

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


Vlan Interface Config
VlanInterface
VLAN Interface Name List:
Interface Name
VLAN-IF1
Vlan ID
1
Apply
Cancel
VLAN Interface Configuration:
Mode
Ip Address
IP Address
192.168.2.2
NetMask Address
255.255.255.0
Override
Add
Refresh
VLAN Interface List:
Index
Ip
Mask
Primary
Delete
1
192.168.2.1
255.255.255.0
Modify
Delete
Cancel

4.1.4 Port Setup

To configure the related parameters of a port, select **Basic Setting**>**Port Setup** in the function menu bar.



【Parameter Description】

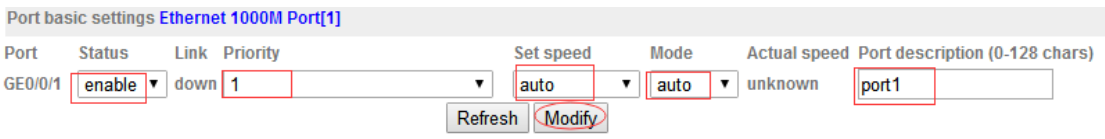
Parameter	Description
Port	Port number
Status	Choose whether to enable or disable the link port
Link	Status: down up
Priority	Set port priority in the range of 0 – 7
Set speed	Choose the following modes: 10/100 Mbps ports: full-10 half-10 auto-10 full-100 half-100

Parameter	Description
	auto-100 10/100/1000 Mbps ports: full-10 half-10 auto-10 full-100 half-100 auto-100 full-1000 half-1000 auto-1000 auto
Mode	Choose the following kinds: auto slave master
Actual speed	Displays the actual speed of the port
Port description	Describe the port.

【Configuration example】

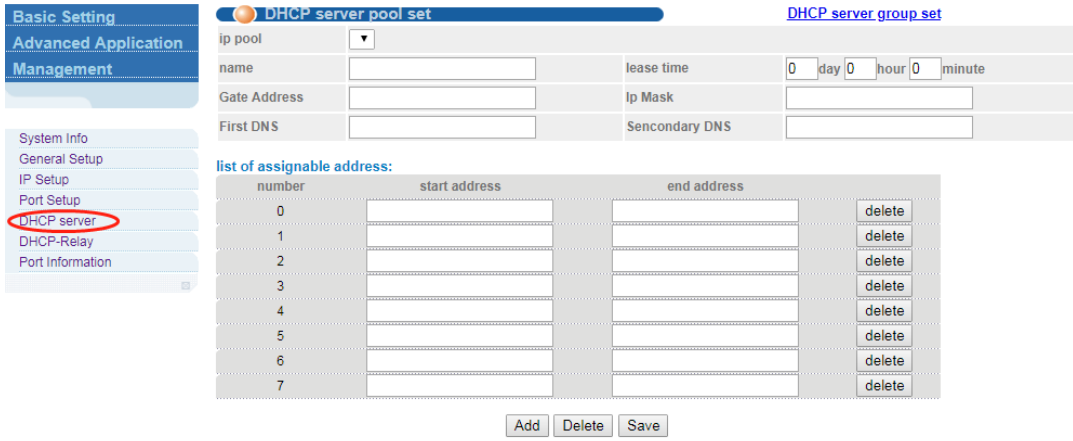
To configure static routes:

1. Click Basic Setting > Port Setup.
2. Configure the related parameters for port 1: Status is enable, Priority is 1, Set speed is auto, Mode is auto, Port description is port 1.
3. Click Modify.



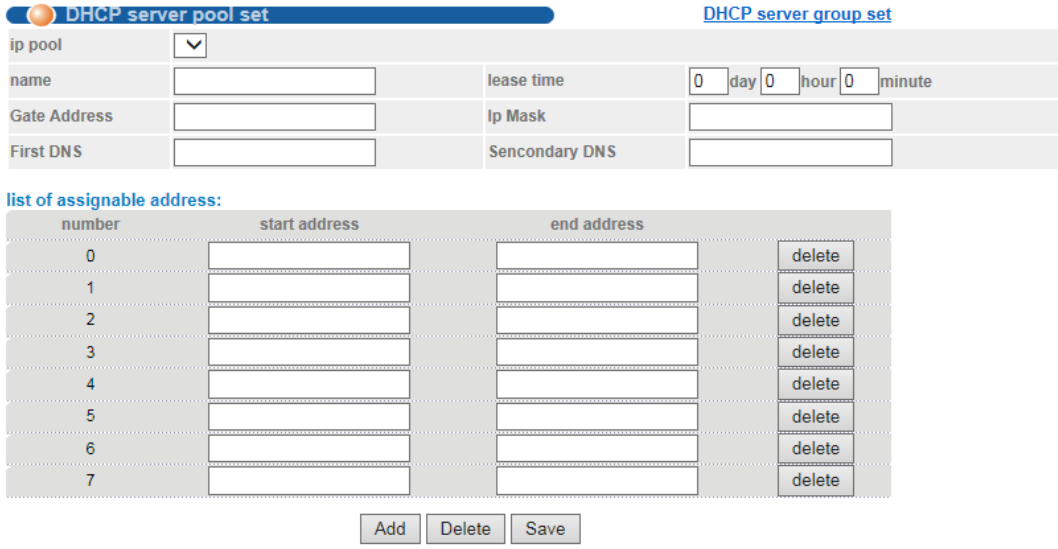
4.1.5 DHCP Server

To configure the DHCP server pool and DHCP server group, select **Basic Setting**>**DHCP Server** in the function menu bar.



4.1.5.1 DHCP server pool set

To configure DHCP Server pool set, select **Basic Setting**>**DHCP server**>**DHCP server pool set** in the function menu bar.

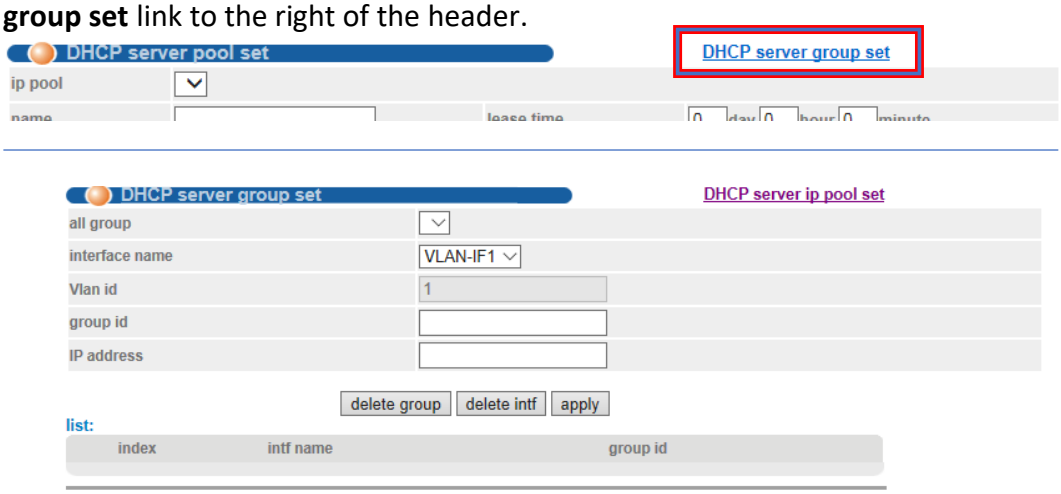


【Parameter Description】

Parameter	Description
ip pool	IP pool ID
name	Set the name of IP pool
lease time	Set lease time
Gate Address	Set gate address
Ip Mask	Set IP mask
First DNS	Set first DNS
Secondary DNS	Set secondary DNS
Start address	Set start address range
End address	Set end address range

4.1.5.2 DHCP server group set

To configure the DHCP Server group, select **Basic Setting**>**DHCP server**>**DHCP server group set** link to the right of the header.

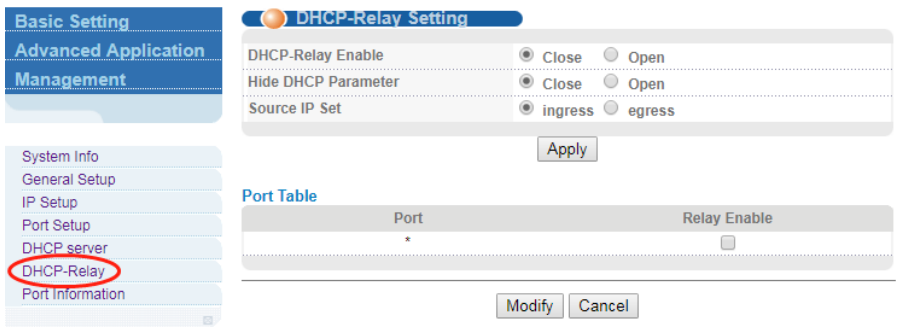


【Parameter Description】

Parameter	Description
group id	Provide the DHCP server group ID
IP address	Provide the DHCP server IP address

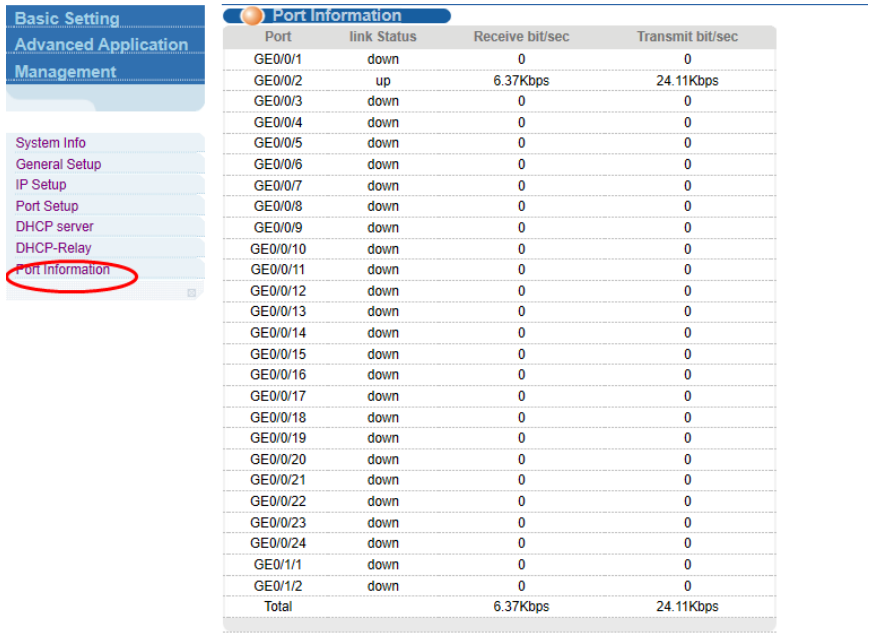
4.1.6 DHCP-Relay

To turn on the DHCP relay function, hide DHCP Server, and set the source IP used, select **Basic Setting**>**DHCP-Relay** in the function menu bar.



4.1.7 Port Information

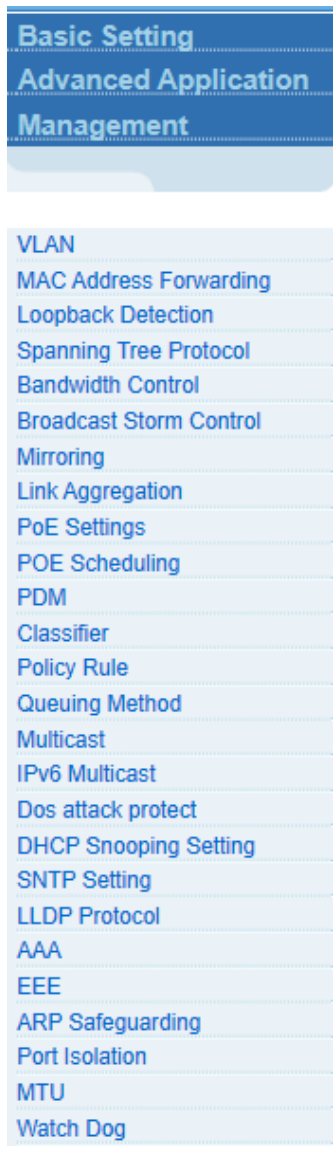
To view port information, select **Basic Setting**>**Port Information** in the function menu bar.



Port	link Status	Receive bit/sec	Transmit bit/sec
GE0/0/1	down	0	0
GE0/0/2	up	6.37Kbps	24.11Kbps
GE0/0/3	down	0	0
GE0/0/4	down	0	0
GE0/0/5	down	0	0
GE0/0/6	down	0	0
GE0/0/7	down	0	0
GE0/0/8	down	0	0
GE0/0/9	down	0	0
GE0/0/10	down	0	0
GE0/0/11	down	0	0
GE0/0/12	down	0	0
GE0/0/13	down	0	0
GE0/0/14	down	0	0
GE0/0/15	down	0	0
GE0/0/16	down	0	0
GE0/0/17	down	0	0
GE0/0/18	down	0	0
GE0/0/19	down	0	0
GE0/0/20	down	0	0
GE0/0/21	down	0	0
GE0/0/22	down	0	0
GE0/0/23	down	0	0
GE0/0/24	down	0	0
GE0/1/1	down	0	0
GE0/1/2	down	0	0
Total		6.37Kbps	24.11Kbps

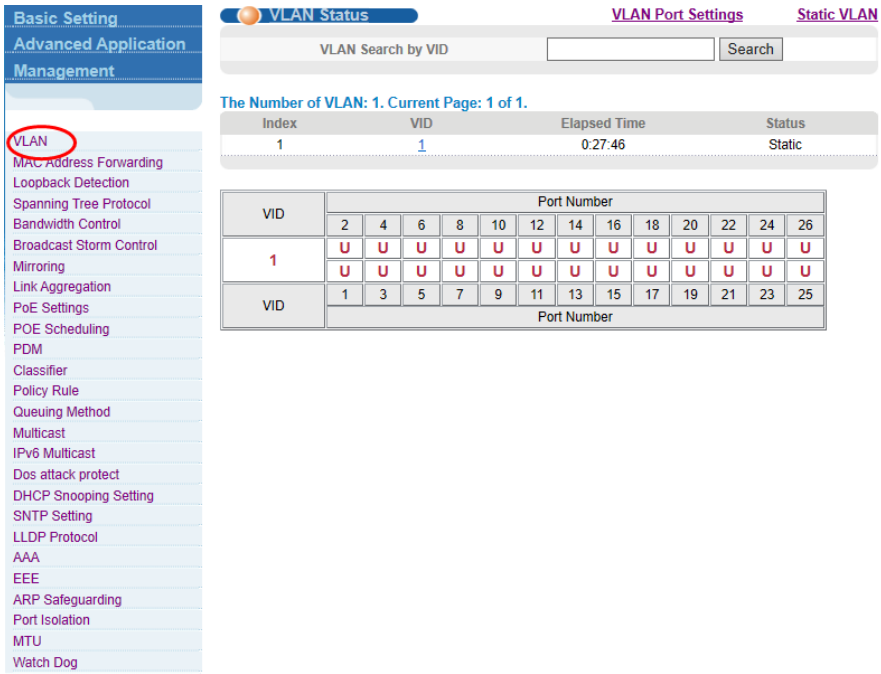
4.2 Advanced Application

Choose Advanced Application, and the function menu bar shows configuration web pages for **VLAN**, **MAC Address Forwarding**, **Loopback Detection**, **Spanning Tree Protocol**, **Bandwidth Control**, **Broadcast Storm Control**, **Mirroring**, **Link Aggregation**, **PoE Settings**, **PoE Scheduling**, **PDM, Classifier**, **Policy Rule**, **Queuing Method**, **Multicast**, **IPv6 Multicast**, **Dos attack protect**, **DHCP Snooping Setting**, **SNTP Setting**, **LLDP Protocol**, **AAA**, **EEE**, **ARP Safeguarding**, **Port Isolation**, **MTU**, and **Watch Dog**.



4.2.1 VLAN

To configure VLAN, select **Advanced Application**>**VLAN** in the function menu bar.



【Information】

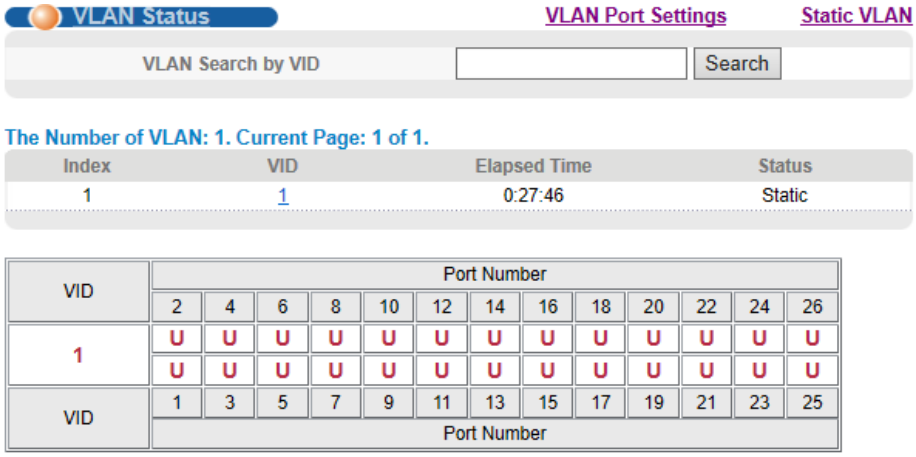
Traditional Ethernet uses a common communication medium and is based on Carrier Sense Multiple Access/Collision Detect (CSMA/CD) data network communication protocol. Overloaded hosts in a LAN will cause major collisions, flooding broadcasts, subpar performance, or even the collapse of the Internet using standard Ethernet. While substantial collisions can be avoided by connecting LANs through switches, flooding broadcasts cannot be avoided because they consume a lot of bandwidth resources and could result in significant security issues.

A network topology called a Virtual Local Area Network (VLAN) is set up using a logical plan rather than a physical one. Switches use VLAN technology to manage broadcast in LANs. You can divide a physical LAN into several logical LANs, each with its own broadcast domain, by implementing VLANs. The communication between hosts on the same VLAN is similar to that of a LAN. However, hosts in separate VLANs are unable to directly connect with one another.

VLANs therefore restrict broadcast packets. Standard Ethernet is how hosts in the same VLAN communicate, while Layer 3 switches, routers, and other Internet-connected devices are the method of communication for hosts in separate VLANs.

4.2.1.1 VLAN Status

To view VLAN status, select **Advanced Application**>**VLAN**>**VLAN Status** in the function menu bar.

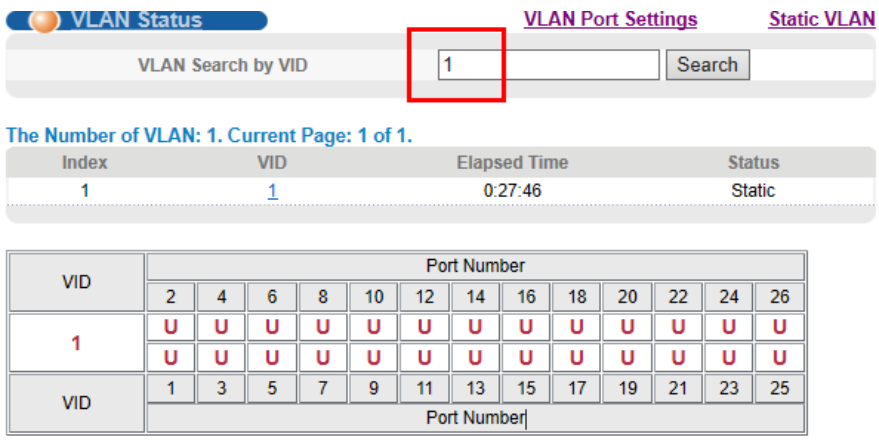


【Parameter Description】

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

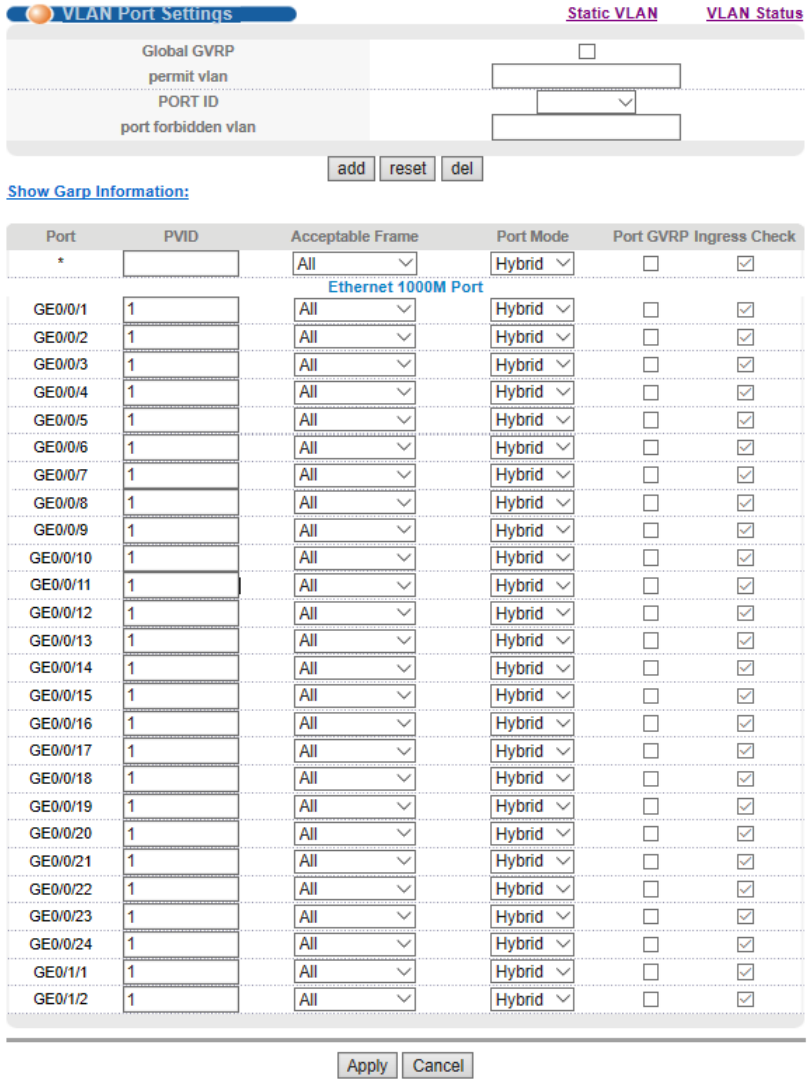
【Configuration example】

View the VLAN of VID as 1.



4.2.1.2 VLAN Port Settings

To configure or adjust settings related to a VLAN port, select **Advanced Application**>**VLAN**>**VLAN Port Settings** in the function menu bar.



【Parameter Description】

Parameter	Description
PVID (Port VLAN ID)	The PVID of the port can be modified, the default port PVID is 1
Acceptable Frame	Choose the following kinds: All Tagged only Untagged only
Port Mode	Choose the following modes:

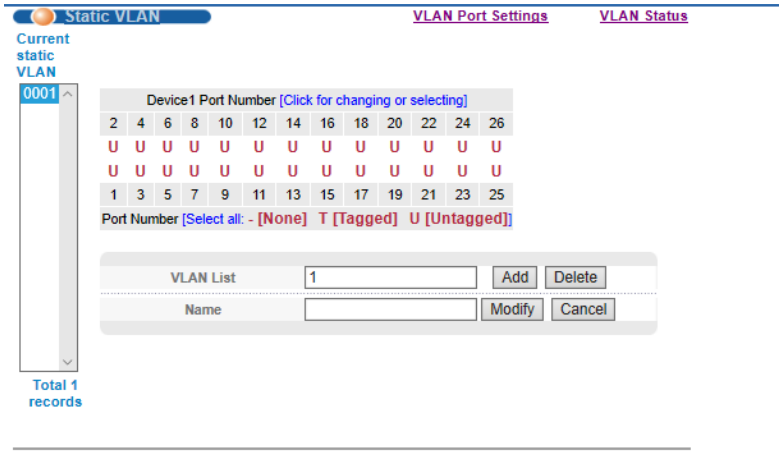
Parameter	Description
	Hybrid: The port can be either a tagged member or untagged member in the VLAN and can be a member port for multiple VLANs. Used to connect switches to each other and to computers. **Trunk**: The port can only be a tagged member in the VLAN and can be a member port for multiple VLANs. Typically used to connect switches to each other. **Access**: port belongs to one VLAN. Common use is to connect computer ports. The port can only be an untagged member in the VLAN and the port can only be in one VLAN, not multiple.
Port GVRP	Select enable or disable GVRP (a dynamic VLAN learning function); port mode must be Trunk mode.
Ingress Check	Enable port filtering function. If enabled, the port checks for a tagged message. If the message is untagged, it is disregarded. If disabled, all messages are allowed through.

【Configuration example】

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

4.2.1.3 Static VLAN

To configure a Static VLAN, select **Advanced Application**>**VLAN**>**Static VLAN** in the function menu bar.



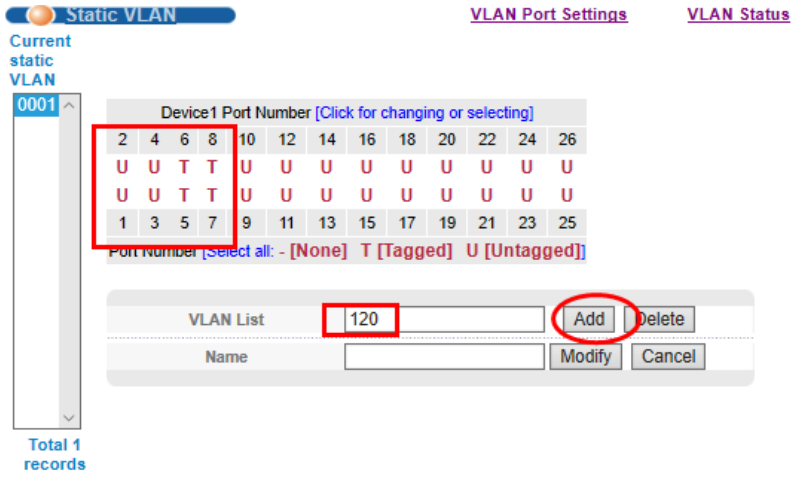
【Parameter Description】

Parameter	Description
VLAN List	VLAN group ID
Name	VLAN group name

【Configuration example】

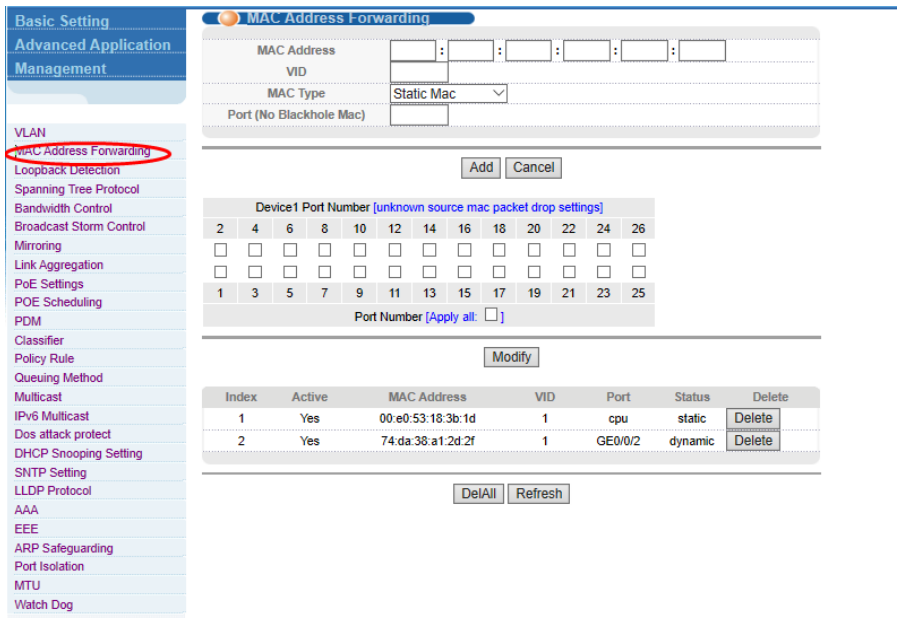
To add and delete VLAN members:

1. Click Advanced Application > VLAN> Static VLAN.
2. Add a new VLAN with VLAN Group ID (VLAN List) 120, which contains untagged member ports 1 – 4 and Tagged member ports 5 - 8. The user can modify the port member by clicking on the white area below the port number.
3. Click Apply.



4.2.2 MAC Address Forwarding

To configure MAC Address Forwarding, select **Advanced Application**>**MAC Address Forwarding** in the function menu bar.



【Parameter Description】

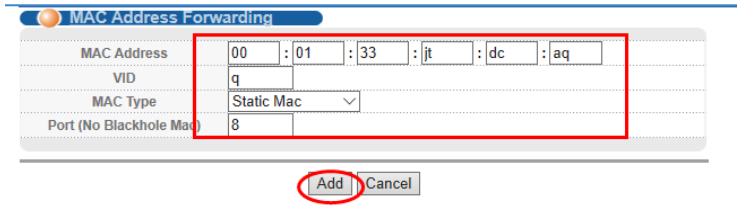
Parameter	Description
MAC Type	MAC Type: Static MAC Dynamic MAC Blackhole MAC Permanent MAC

【Information】

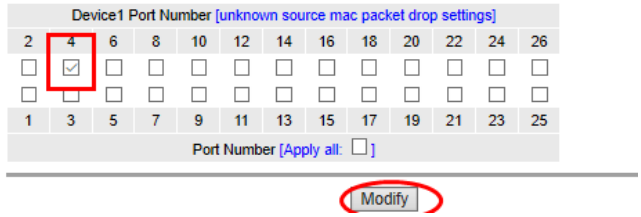
Example to Create a Blackhole MAC: If a PC's MAC address is configured on a switch to be a blackhole MAC, then the PC's packets will be discarded by the switch and not forwarded to the network.

【Configuration example】

1. Click Advanced Application > MAC Address Forwarding.
2. Provide the MAC address, VID, choose the MAC Type and enter port number for the blackhole MAC:



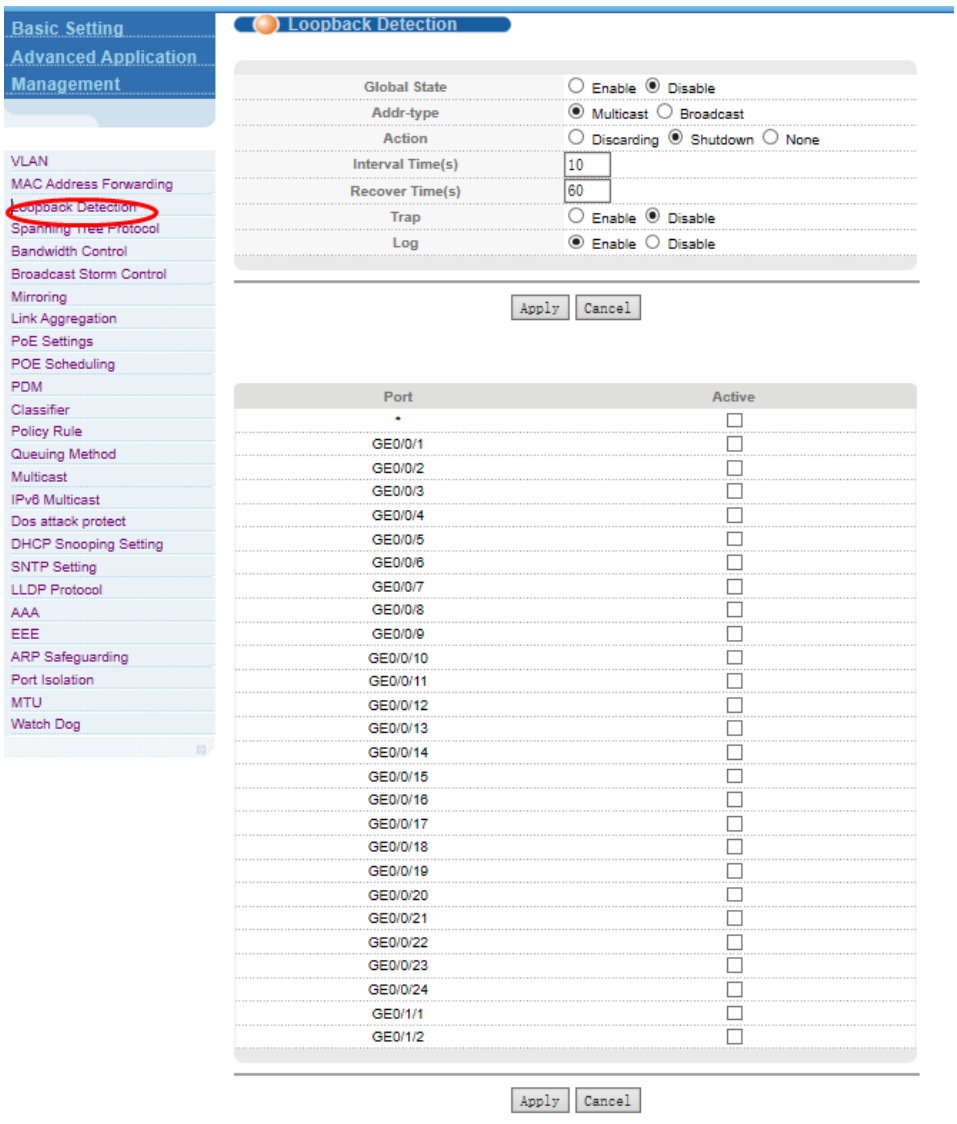
3. Unknown source MAC packet drop settings.



4. Click Modify.

4.2.3 Loopback Detection (Part of our Self-Healing Network Suite of Features)

To configure Loopback Detection, select **Advanced Application**>**Loopback Detection** in the function menu bar. Loopback Detection allows the switch to detect loops in the network. When a loop is detected on a port, the switch will display an alert on the management interface and further block the corresponding port according to your configurations.

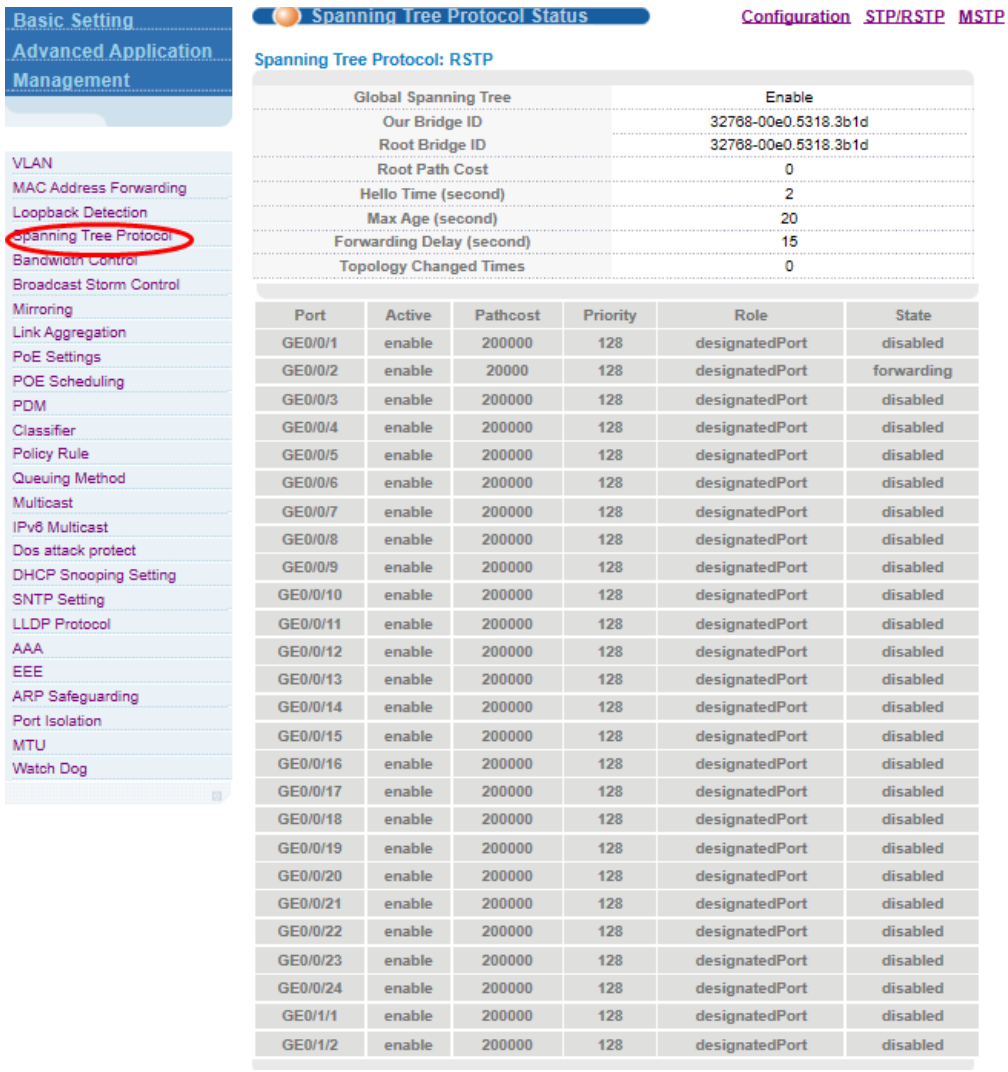


【Parameter Description】

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

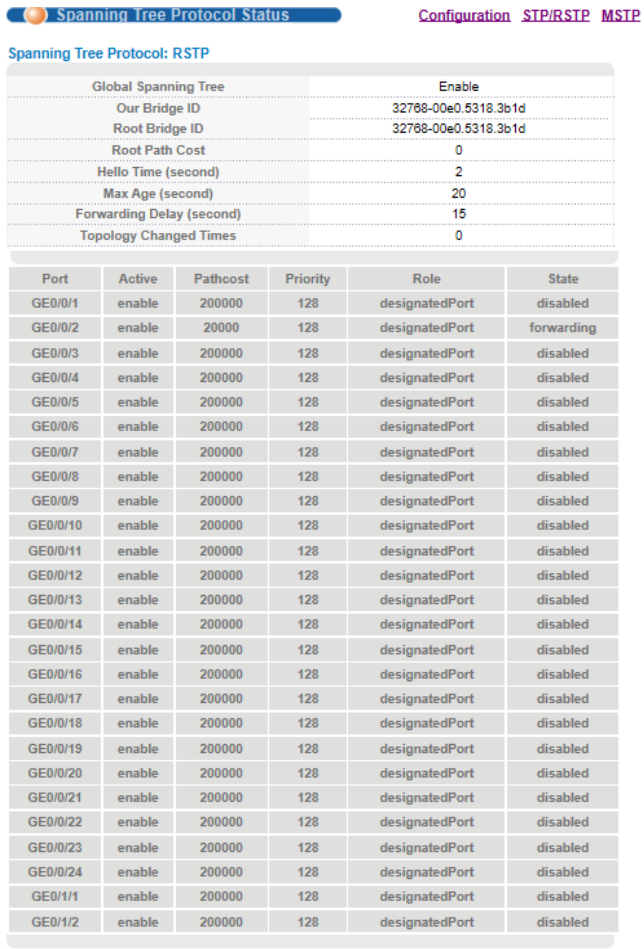
4.2.4 Spanning Tree Protocol (Part of our Self-Healing Network Suite of Features)

To configure Spanning Tree Protocol (STP), select **Advanced Application**>**Spanning Tree Protocol** in the function menu bar. According to the IEEE 802.1D standard, STP is used to create ring-free networks on the Data Link layer in a local network. A ring network can be separated from the network by using STP-enabled devices that identify loops and block ports from endlessly repeating and forwarding packets.



4.2.4.1 Spanning Tree Protocol Status

To view Spanning Tree Protocol status, select **Advanced Application**>**Spanning Tree Protocol**>**Spanning Tree Protocol Status** in the function menu bar.

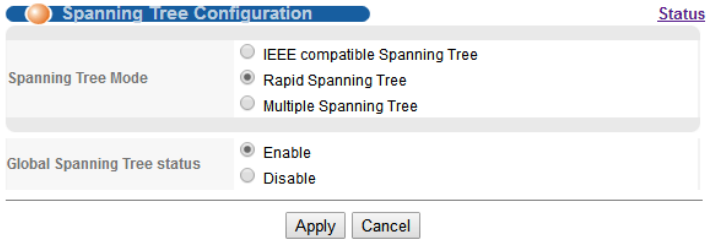


【Parameter Description】

Parameter	Description
Root Path Cost	Configure Root Path Cost
Hello time (second)	Send Bridge Protocol Data Unit (BPDU) in packet interval
Max age (second)	Topology changes are initiated for ports that have not received a message in the time specified
Forwarding delay (second)	The state of the port switch time
Topology changed times	The number of topology changes

4.2.4.2 Spanning Tree Configuration

To configure Spanning Tree, select **Advanced Application**>**Spanning Tree Protocol**>**Spanning Tree configuration** in the function menu bar.

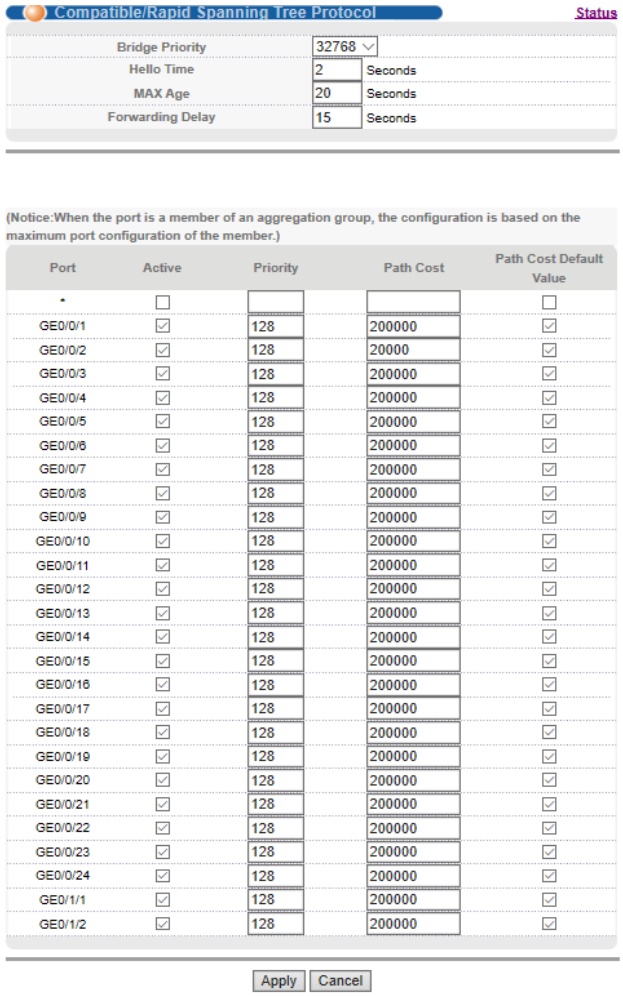


【Parameter Description】

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

4.2.4.3 Compatible/Rapid Spanning Tree Protocol

To configure Compatible/Rapid Spanning Tree Protocol, select **Advanced Application**>**Spanning Tree Protocol**>**Compatible/Rapid Spanning Tree Protocol** in the function menu bar.



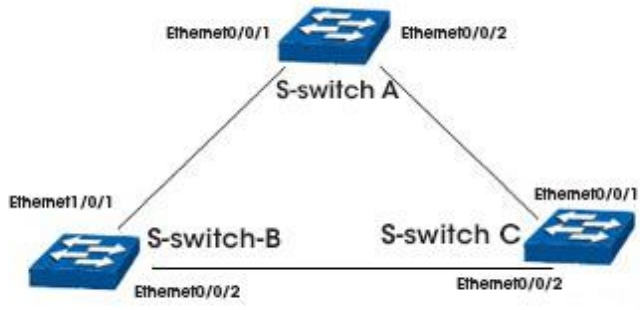
【Parameter Description】

Parameter	Description
Bridge Priority	Set bridge priority, the default instance bridge priority for 32768
Hello Time	Send Bridge Protocol Data Unit (BPDU) in packet interval
Max Age	The time the switch will wait before initiating topology changes for ports that have not received a message
Forwarding Delay	The state of the port switch time
Priority	Set port instance priority, defaults to 128
Path Cost	Configure port costs

【Configuration example】

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

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



S-switch-A Configuration：

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

S-switch-B Configuration：

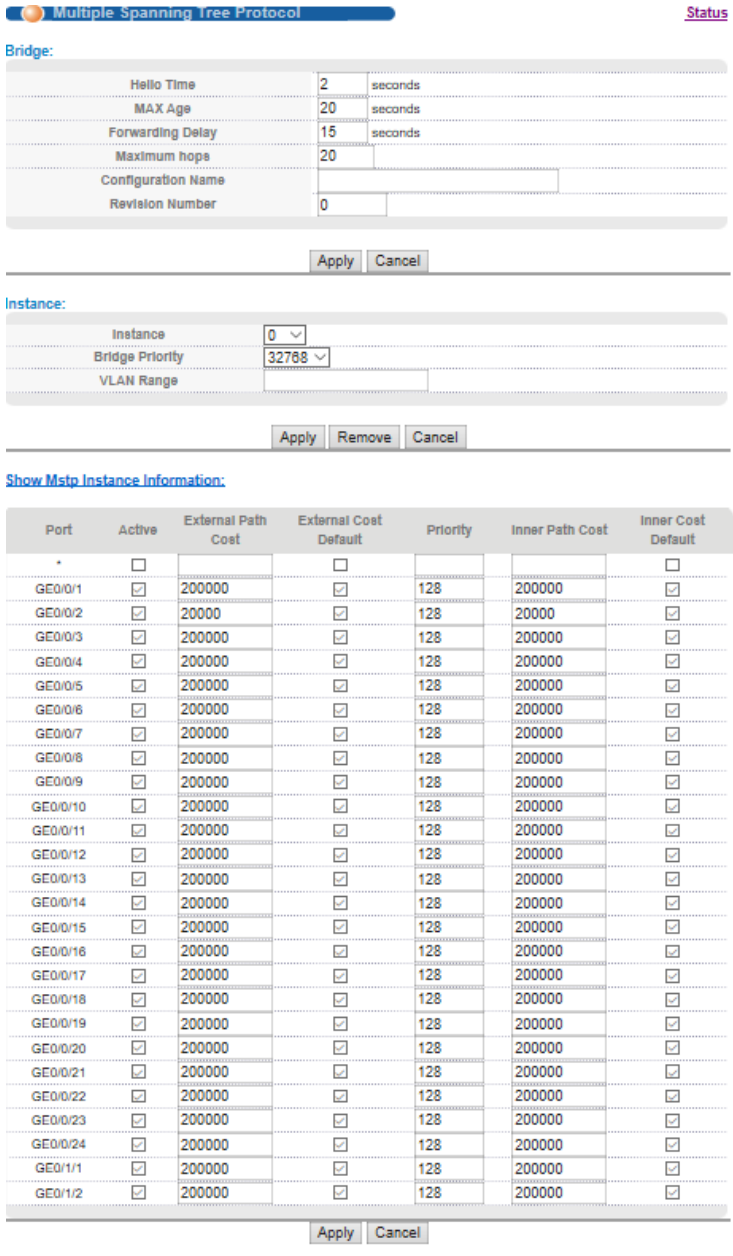
1. Configure Ethernet0/0/1 and Ethernet0/0/2 as a trunk port.
2. Configure spanning-tree priority as 4096, and configure the Ethernet0/0/1 port path cost and the Ethernet0/0/2 port path cost as 10.
3. Enable RSTP globally.

S-switch-C Configuration：

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

4.2.4.4 Multiple Spanning Tree Protocol

To configure Multiple Spanning Tree Protocol, select **Advanced Application**>**Spanning Tree Protocol**>**Multiple Spanning Tree Protocol** in the function menu bar.



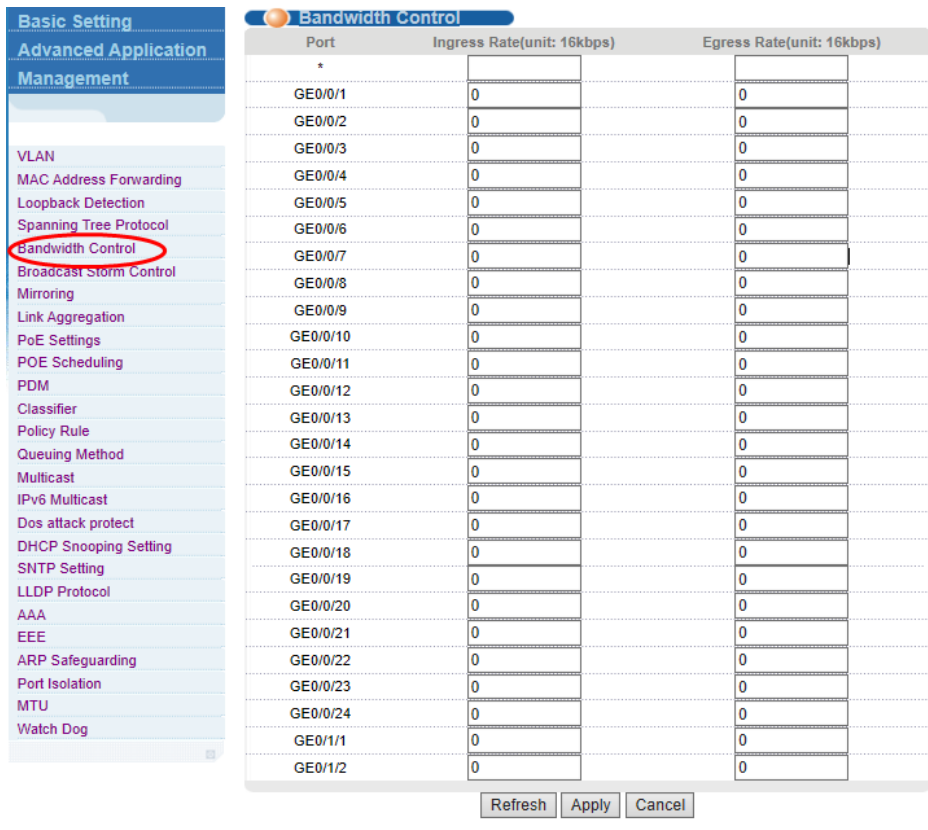
【Parameter Description】

Parameter	Description
Hello Time	Send BPDU in packet interval
Max age	The time the switch will wait before initiating topology changes for ports that have not received a message
Forwarding Delay	The state of the port switch time

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

4.2.5 Bandwidth Control

To configure Bandwidth Control, select **Advanced Application**>**Bandwidth Control** in the function menu bar.



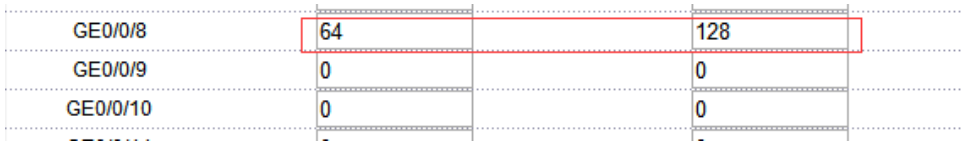
【Information】

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】

Configure bandwidth control for port 8.

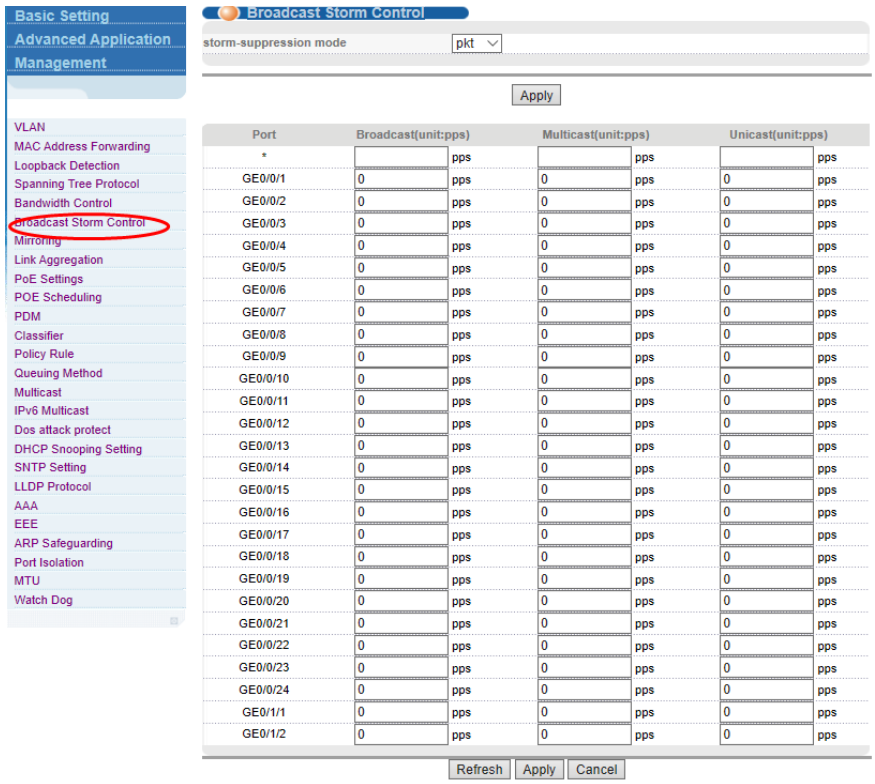
1. Click Basic Setting > Bandwidth Control.
2. Configure port-8 Ingress Rate as 64 kbps and the Egress Rate as 128 kbps.



3. Click Apply.

4.2.6 Broadcast Storm Control

To configure Broadcast Storm Control, select **Advanced Application**>**Broadcast Storm Contro**l in the function menu bar.



【Parameter Description】

Parameter	Description
Broadcast	Broadcast rate limitation (the range of 64 - 32000000, unit: pps; you must enter a multiple of 64, default is 49984)

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

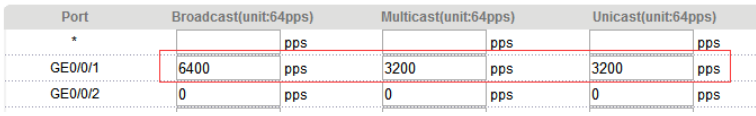
【Information】

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

【Configuration example】

To configure broadcast storm control for port 1.

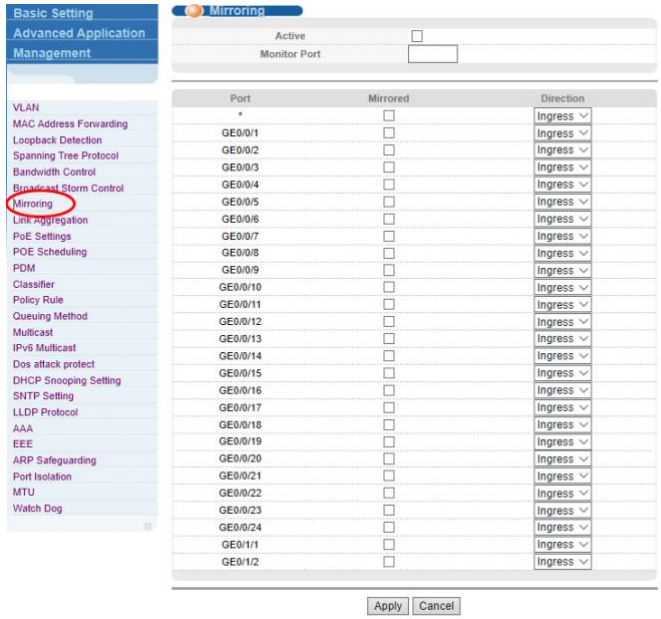
1. Click Basic Setting > Broadcast Storm Control.
2. Set port 1 broadcast as 6400 pps, multicast as 3200 pps, and unicast as 3200 pps.



3. Click Apply.

4.2.7 Mirroring

To configure mirroring, select **Advanced Application**>**Mirroring** in the function menu bar.

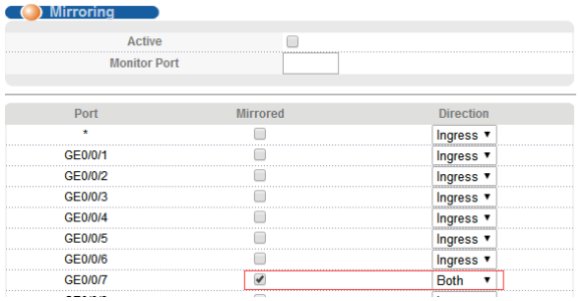


【Parameter Description】

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

【Configuration example】

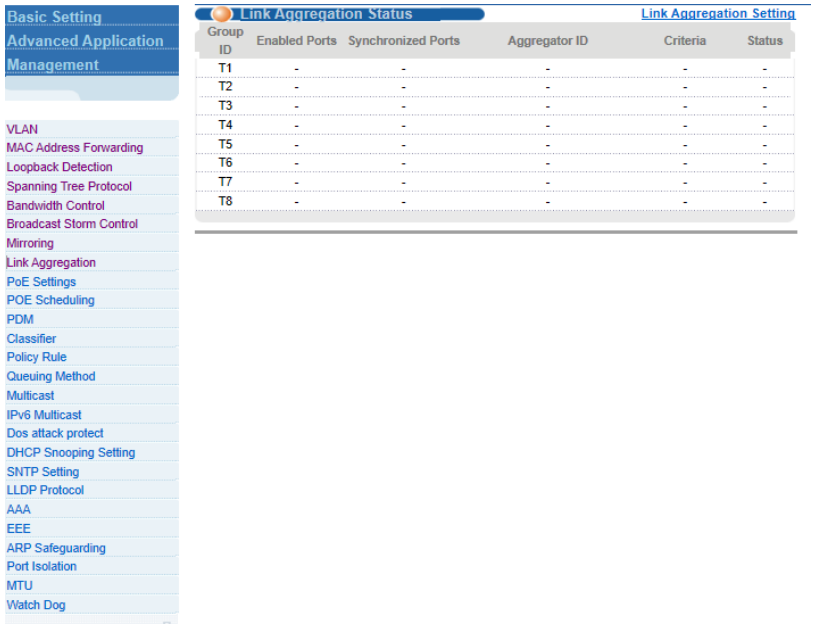
1. Click Advanced Application > Mirroring.
2. Enable mirroring; the monitoring port is port 8, the source port is port 7, and the mirror message is in both directions.
3. Click Apply.


Mirroring
Active
Monitor Port
Port
Mirrored
Direction
*
GE0/0/1
GE0/0/2
GE0/0/3
GE0/0/4
GE0/0/5
GE0/0/6
GE0/0/7
Ingress
Ingress
Ingress
Ingress
Ingress
Ingress
Ingress
Both

4.2.8 Link Aggregation

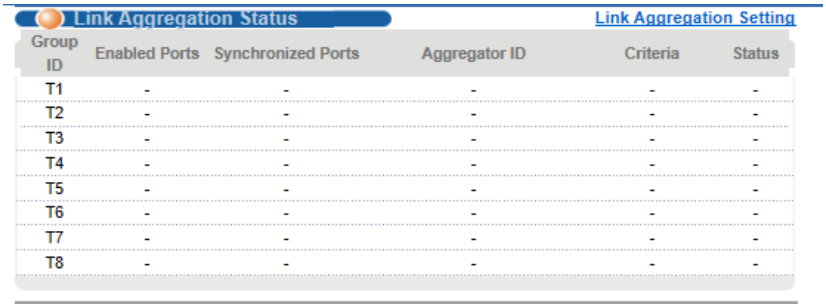
To configure link aggregation, select **Advanced Application**>**Link Aggregation** in the function menu bar. With the LAG (Link Aggregation Group) function enabled, you can aggregate multiple physical ports into a logical interface to increase link bandwidth and configure the backup ports to enhance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

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



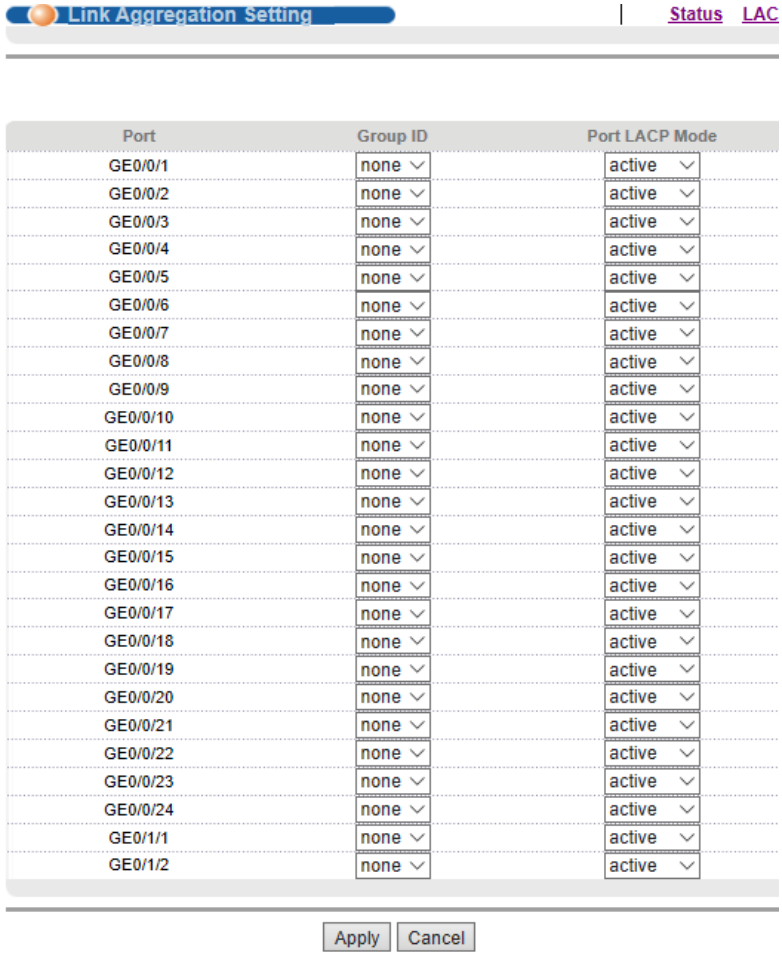
4.2.8.1 Link Aggregation status

To view link aggregation status, Group ID, Enabled Ports, Synchronized Ports, Aggregator ID, Criteria, and overall Status, select **Advanced Application**>**Link Aggregation**>**Link Aggregation Status** in the function menu bar.



4.2.8.2 Link Aggregation Setting

To set Link Aggregation, select **Advanced Application**>**Link Aggregation**>**Link Aggregation Setting** in the function menu bar.

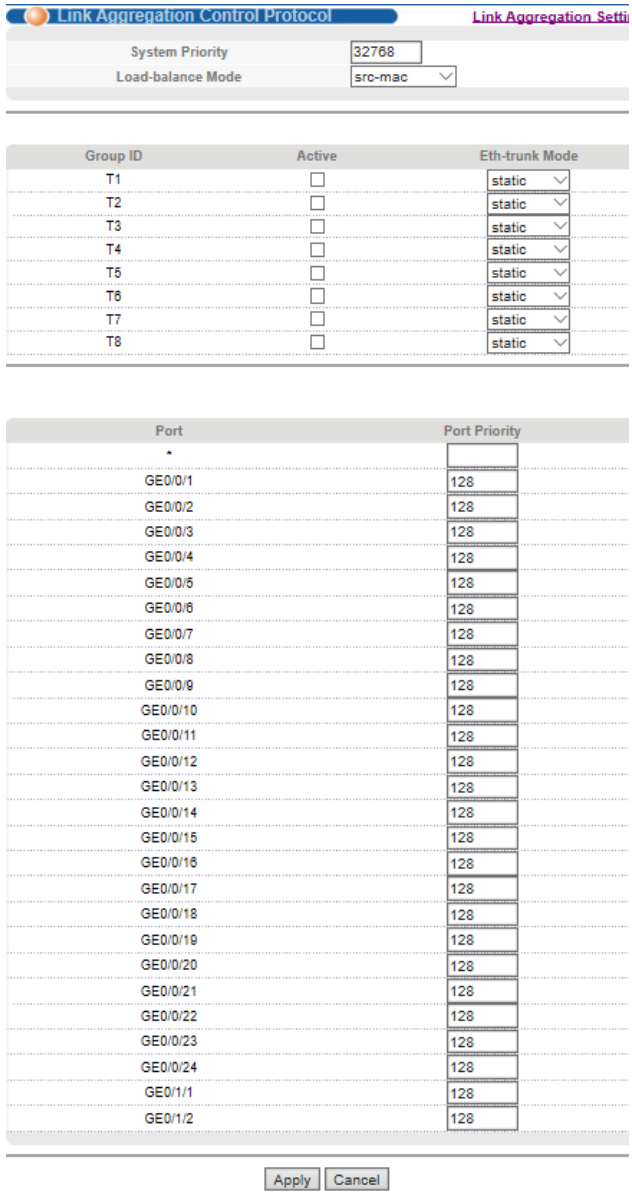


【Parameter Description】

Parameter	Description
Group ID	Add the port to the specified Aggregation Group ID
Port LACP mode	Configure port aggregation (active/passive)

4.2.8.3 Link Aggregation Control Protocol

To configure Link Aggregation Control Protocol, select **Advanced Application**>**Link Aggregation**>**Link Aggregation Control Protocol** in the function menu bar.

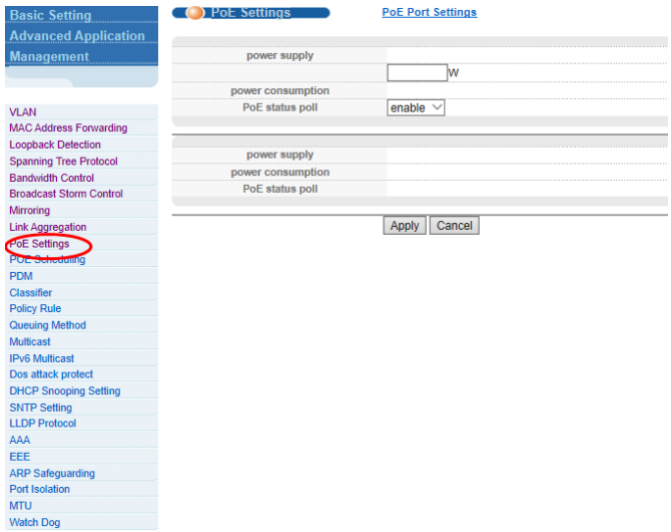


【Parameter Description】

Parameter	Description
System priority	Aggregation group system priority, the default is 32768 (the range is 1 - 65535)
Load-balance Mode	Configure the Aggregation Group load balancing (src-mac/dst-mac/src-dst-mac/src-ip/dst-ip/src-dst-ip)

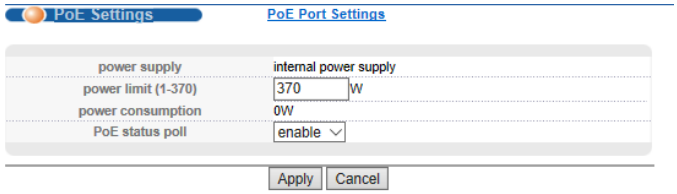
4.2.9 PoE Settings (excludes 508834, where PoE is not supported)

To adjust settings for PoE, select **Advanced Application**>**PoE Settings**.



4.2.9.1 PoE Settings

To configure PoE, select **Advanced Application**>**PoE Settings**.

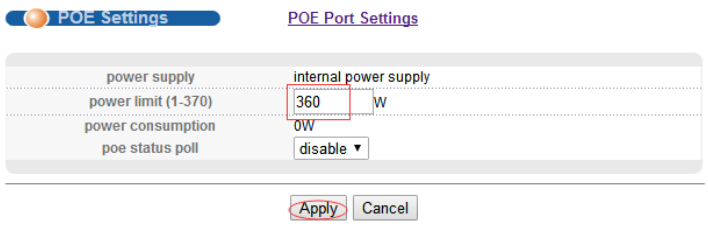


【Parameter Description】

Parameter	Description
power limit	Set the limit for the overall power of PoE switch

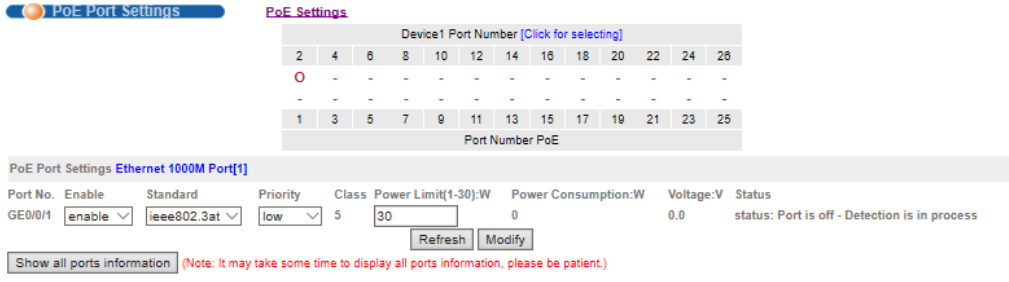
【Configuration example】

Set the power limit to 360 W.



4.2.9.2 PoE Port Settings

To configure settings for a PoE Port, select **Advanced Application**>**PoE Settings**>**PoE Port Settings** in the function menu bar.

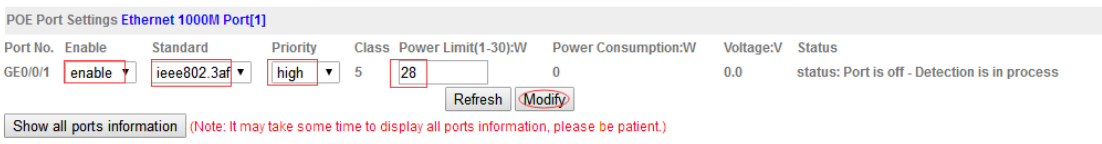


【Parameter Description】

Parameter	Description
Enable	Turn the port PoE power on and off; the default is enabled
Standard	Configure IEEE 802.3af or IEEE 802.3at mode; the default is IEEE 802.3at
Priority	Configure port priority as low, critical, high; the default priority is low
Power limit	Set the power limit of PoE port

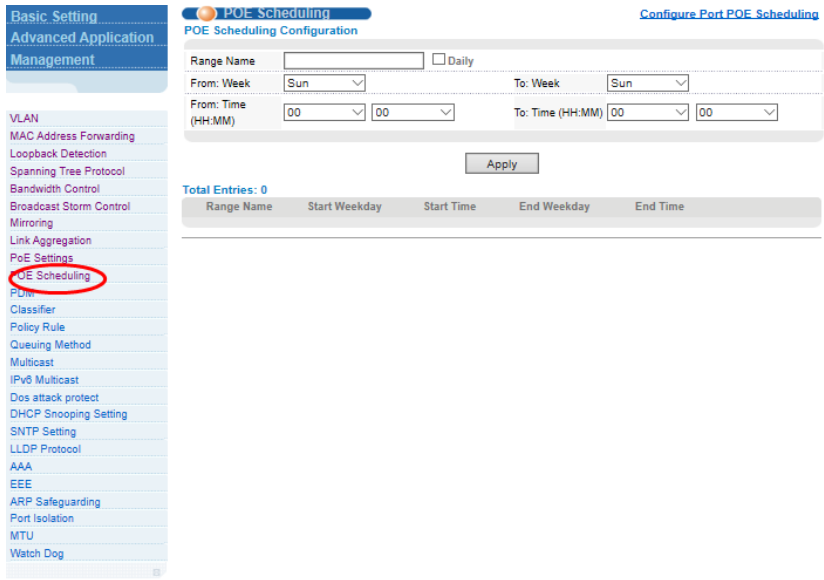
【Configuration example】

Configure the PoE for port 1.



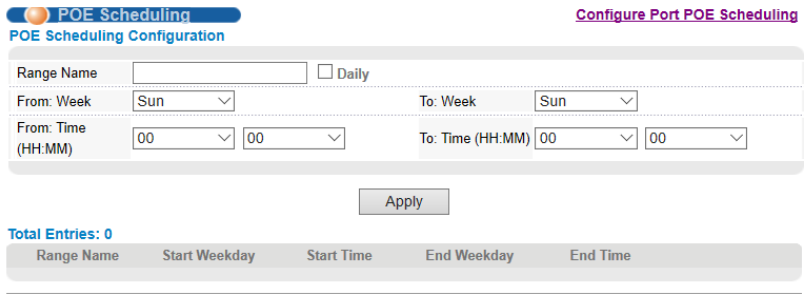
4.2.10 PoE Scheduling (Part of our Self-Healing Network Suite of Features)

To configure PoE Scheduling, select **Advanced Application**>**PoE Scheduling**.



4.2.10.1 PoE Scheduling

To configure PoE Scheduling, select **Advanced Application**>**PoE Scheduling**.

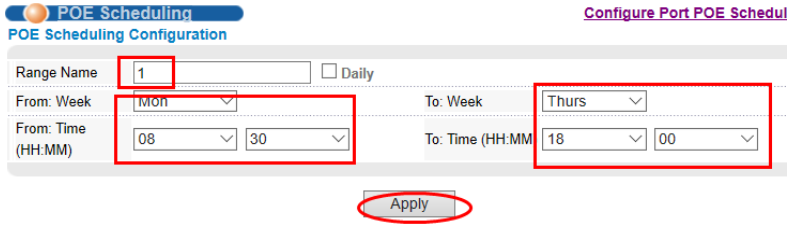


【Parameter Description】

Parameter	Description
Range Name	Set the name for the schedule
From: Week	Set the start day
To: Week	Set the end day
From: Time (HH:MM)	Set the start time
To: Time (HH:MM)	Set the end time

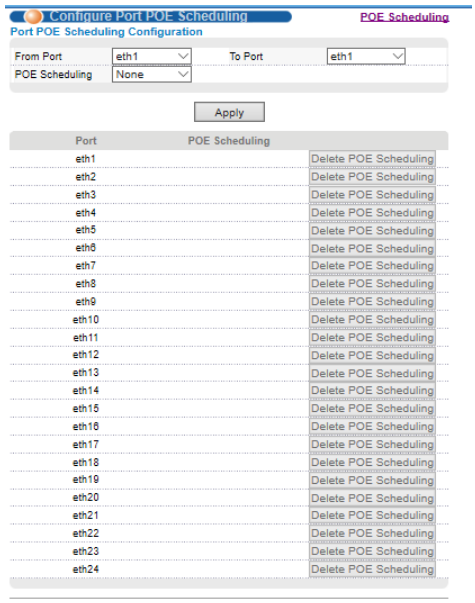
【Configuration example】

Set Range Name 1 with the values shown.



4.2.10.2 Configure Port PoE Scheduling

To configure Port PoE Scheduling, select **Advanced Application**>**PoE Scheduling**>**Configure Port PoE Scheduling** in the function menu bar.

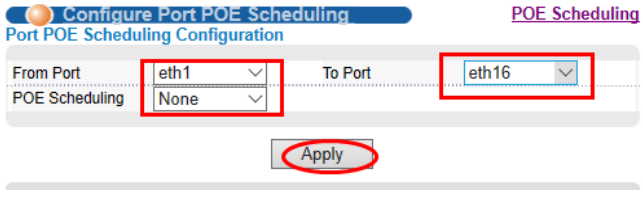


【Parameter Description】

Parameter	Description
From Port	Set the start port
To Port	Set the end port

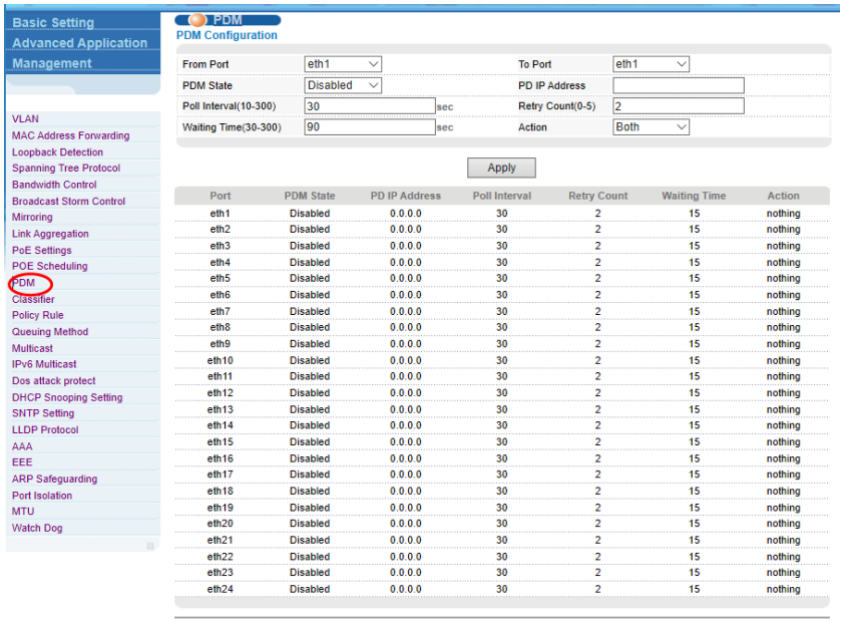
【Configuration example】

Configure PoE from Port 1 to Port 16.



4.2.11 PDM (Part of our Self-Healing Network Suite of Features)

To configure the Powered Device Monitor (PDM) which restarts “down” devices, select **Advanced Application**>**PDM**.

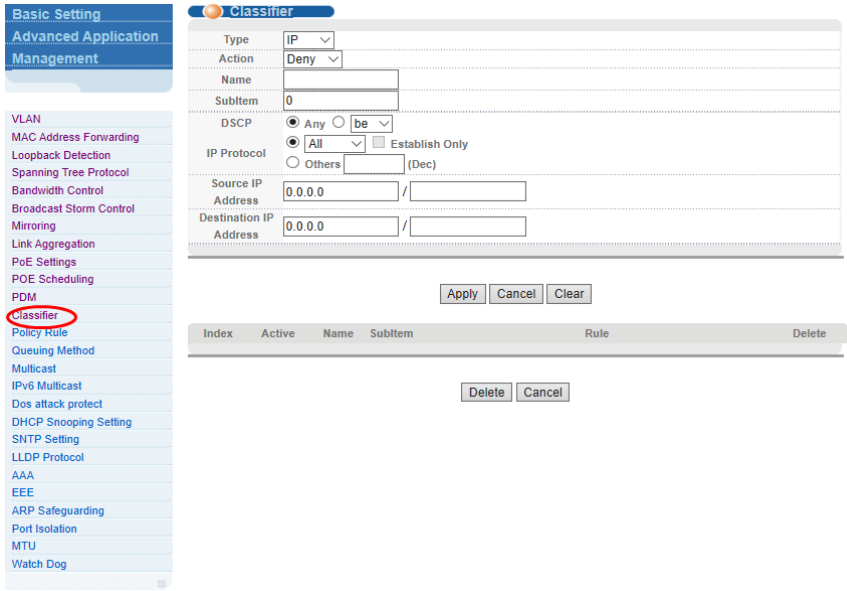


【Parameter Description】

Parameter	Description
From Port	Set the start port
To Port	Set the end port
PDM State	Set the PDM State (disabled and enabled)
Poll Interval	Set the poll interval, range 10 - 300 s
Retry Count	Set the retry count, range 0 - 5
Waiting Time	Set the waiting time, range 30 - 300 s
Action	Set the Action (Reset/Notify/Both)

4.2.12 Classifier

To configure Classifier, select **Advanced Application**>**Classifier** in the function menu bar.

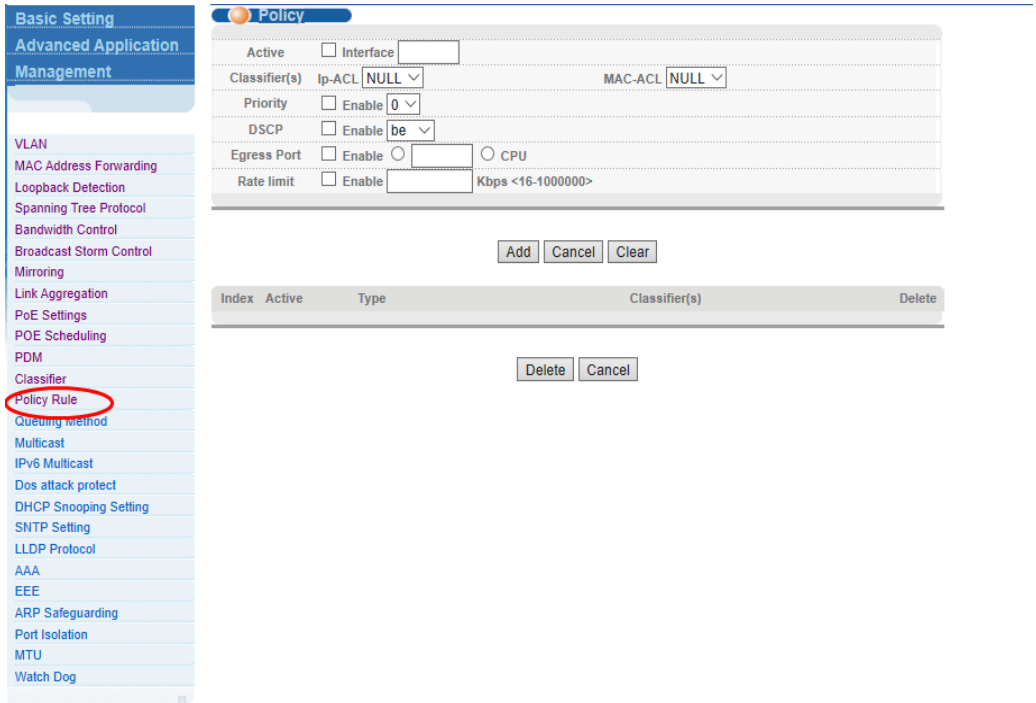


【Parameter Description】

Parameter	Description
Action	Deny or Permit
Type	IP or MAC
Action	Permit or Deny

4.2.13 Policy Rule

To configure Policy Rule, select **Advanced Application**>**Policy Rule** in the function menu bar.

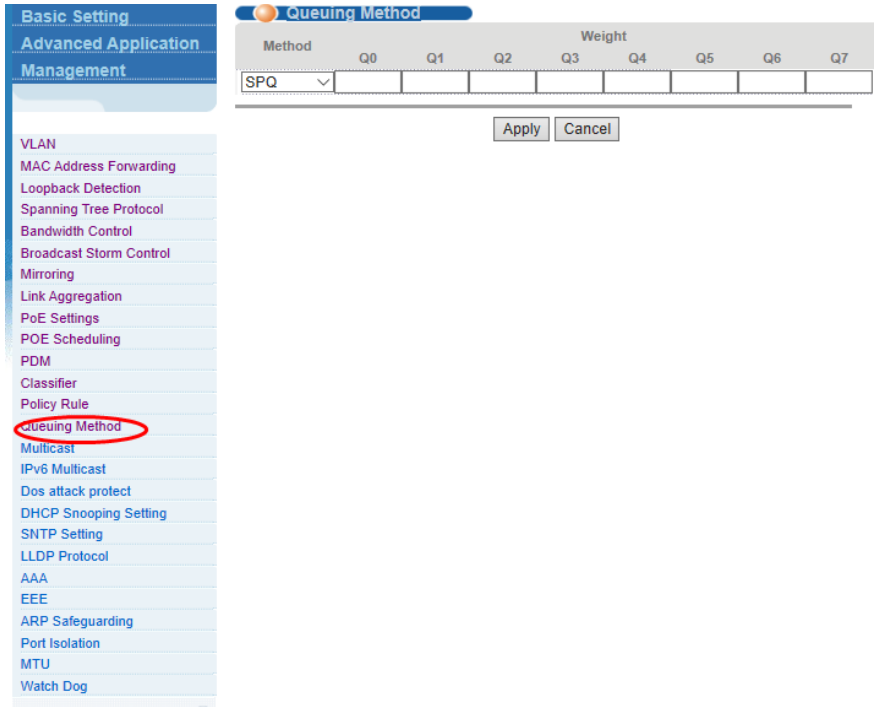


【Parameter Description】

Parameter	Description
Active	Activate Classifier
Classifier(s)	Note: Classification rules must match
Priority	Choose whether to enable priority and set priority
DSCP	Choose whether to enable DSCP
Egress Port	Choose whether to enable an egress port and set
Rate limit	Choose whether to enable a rate limt and set

4.2.14 Queuing Method

To configure queuing method, select **Advanced Application**>**Queuing Method** in the function menu bar.



【Parameter Description】

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

【Information】

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

1. Strict Priority Queueing

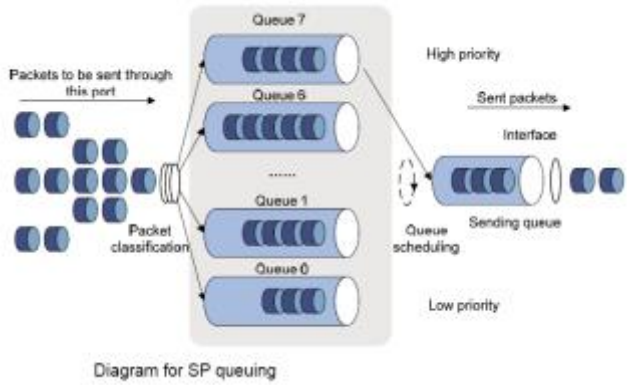
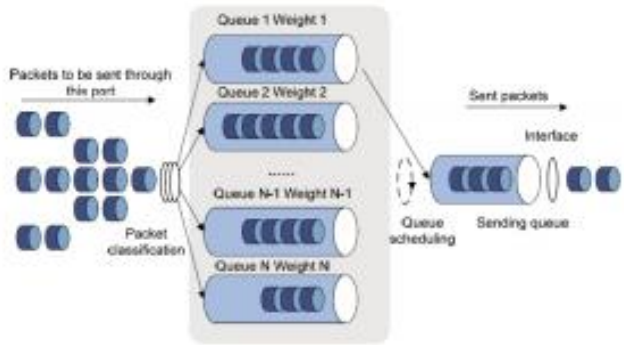


Diagram for SP queuing

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

2. Weighted Round Robin



The WRR queue-scheduling algorithm ensures every queue receives guaranteed service time by taking turns according to a schedule determined by weighted values. Assume a 100-M port has four egress queues with four weight values w3, w2, w1 and w0 and the corresponding values 25, 15, 5 and 5 that reflect the proportion of resources assigned to those four queues. The queue with the lowest priority can be assured of receiving at least 10 Mbps bandwidth, which avoids the disadvantage of the SP algorithm where packets in low-priority queues may not be served for long periods of time. Another advantage of the WRR algorithm is that, though the queues are scheduled in turn, the service time for each queue is not fixed. That is, when a queue is emptied, the next queue is scheduled for service. Therefore, bandwidth resources are more fully utilized.

4.2.15 Multicast

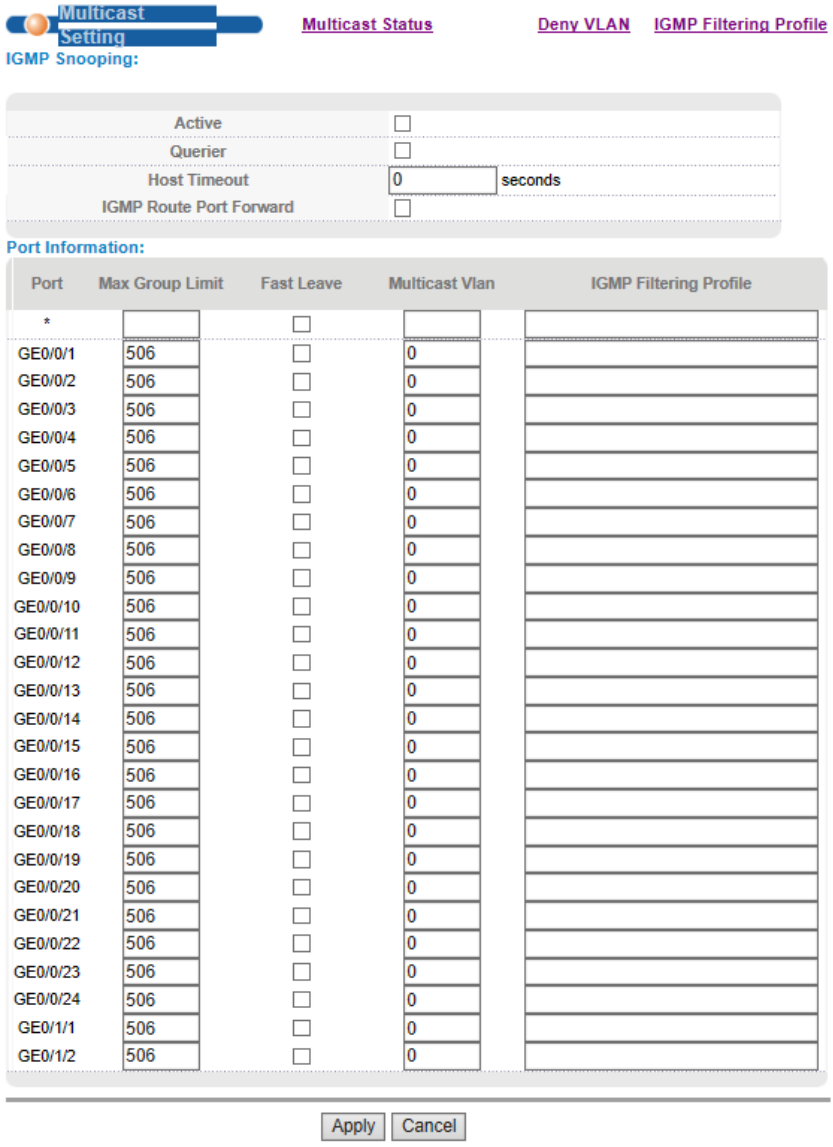
To configure Multicast, select **Advanced Application**>**Multicast** in the function menu bar.

4.2.15.1 Multicast Status

To view all multicast, including the static configuration and the multicast that is learned through the IGMP-Snooping protocol, select **Advanced Application**>**Multicast**>**Multicast Status** in the function menu bar.

4.2.15.2 Multicast Settings

To set multicast, select **Advanced Application**>**Multicast**>**Multicast Settings** in the function menu bar.



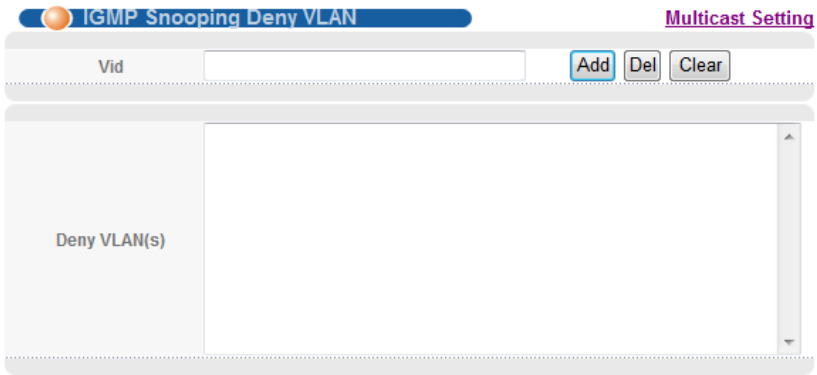
【Parameter Description】

Parameter	Description
Active	Enable IGMP snooping
Querier	Enable IGMP snooping timed query function
Host Timeout	Configure the dynamic group sowing time (default 300 s)
IGMP Route Port Forward	Enable IGMP Route Port Forward

Parameter	Description
Max Group Limit	Max learning group of configuration port (default 1020)
Fast Leave	Enable 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 by the broadcast group that is allowed in the group broadcast preview and cannot be learned by the multicast group, which is forbidden by the group broadcast preview

4.2.15.3 IGMP Snooping Deny VLAN

To preview the banned group broadcast group that is unable to learn the multicast group which is prohibited by the group preview, select **Advanced Application**>**Multicast**>**IGMP Snooping Deny VLAN** in the function menu bar.

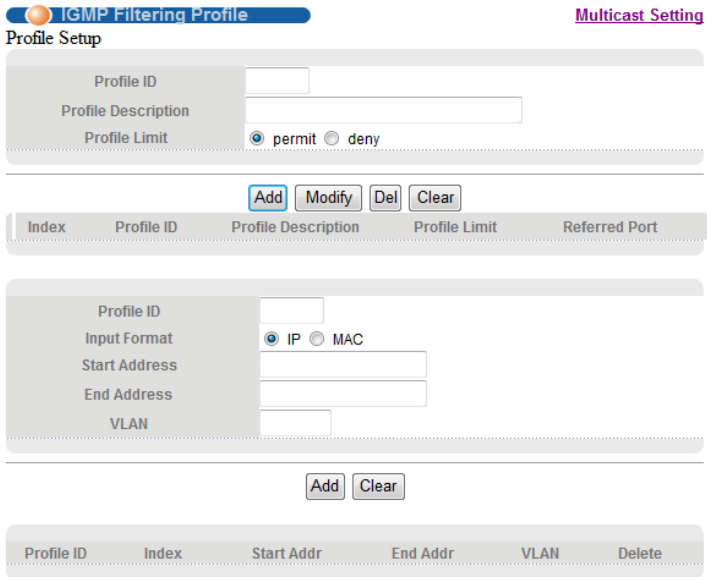


【Parameter Description】

Parameter	Description
Vid	VLAN ID

4.2.15.4 IGMP Filtering Profile

To add and remove the preview feature of the modified group, select **Advanced Application**>**Multicast**>**IGMP Filtering Profile** in the function menu bar.

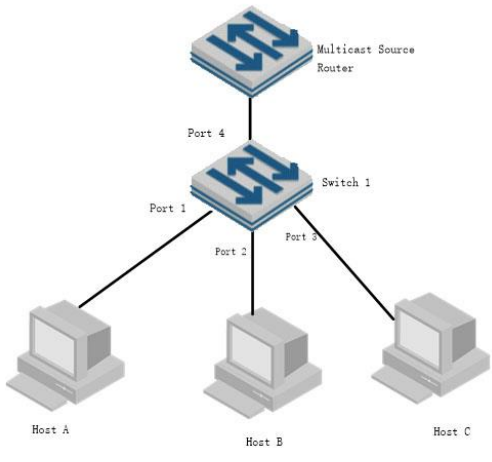


【Parameter Description】

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

【Configuration example】

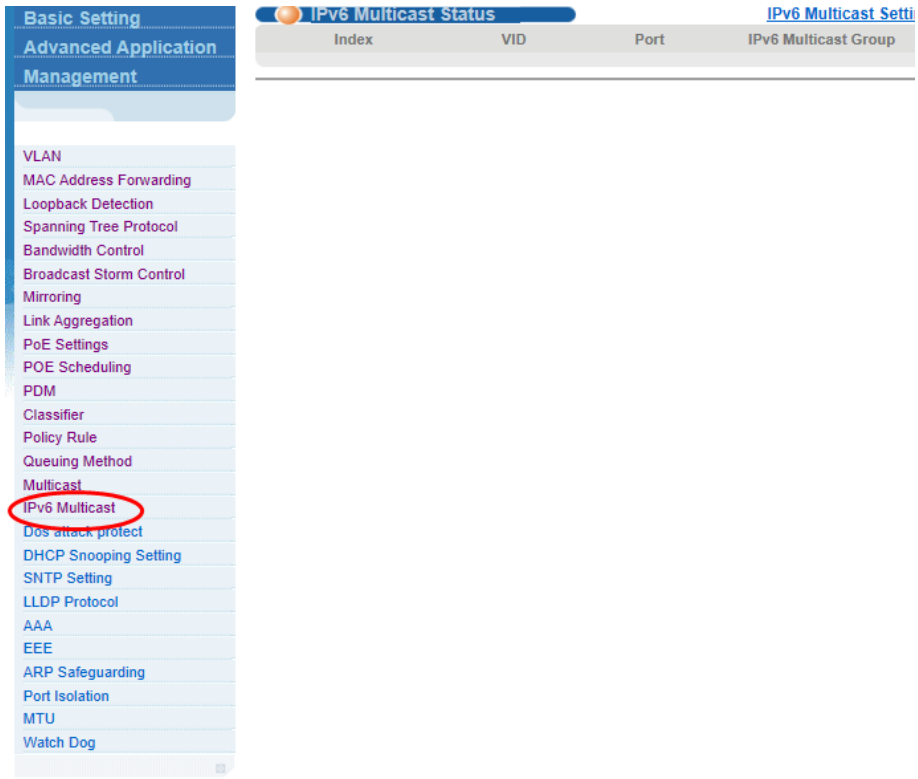
As shown in the figure, host-A, host-B and host-C belong to VLAN2, VLAN3 and VLAN4, respectively. The configuration enables the three hosts to receive the data of the multicast group with the group address of 224.0.1.1 – 224.0.1.3.



1. Enable IGMP Snooping.
2. Add different ports to different VLANs.
3. The host sends the report message to the switch, and the switch learns the multicast group.
4. The multicast source router sends a query message to the switch, which will learn the routing port table entry.
5. The multicast source router sends a multicast traffic stream to the switch and the switch distributes it to the hosts.

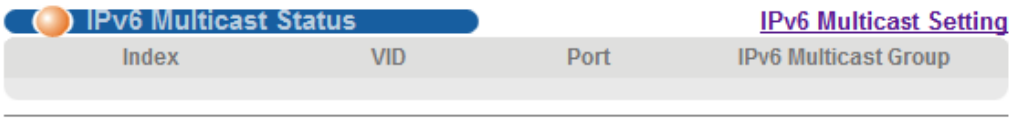
4.2.16 IPv6 Multicast

To configure IPv6 Multicast, select **Advanced Application**>**IPv6 Multicast** in the function menu bar.



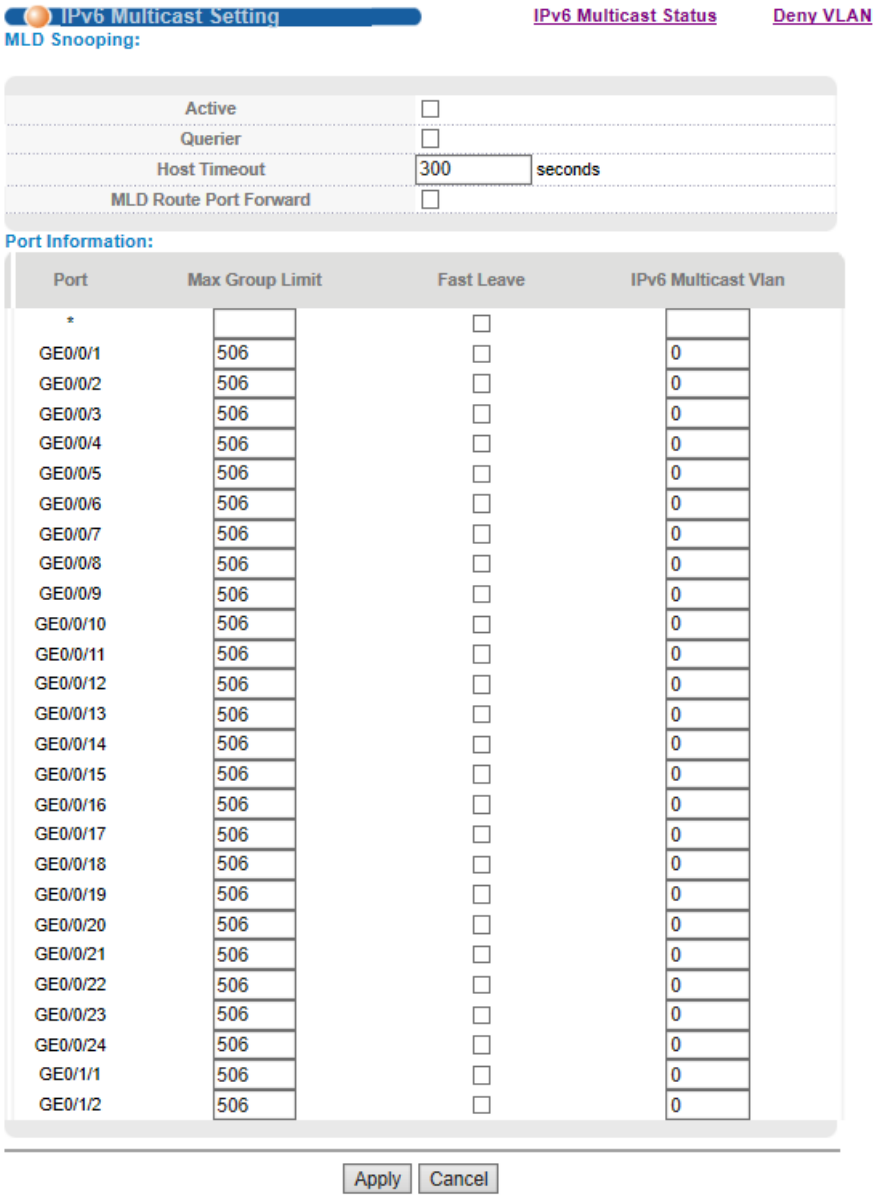
4.2.16.1 IPv6 Multicast Status

To view all IPv6 multicast groups, select **Advanced Application**>**IPv6 Multicast**>**IPv6 Multicast Status** in the function menu bar.



4.2.16.2 IPv6 Multicast Setting

To configure IPv6 Multicast, select **Advanced Application**>**IPv6 Multicast**>**IPv6 Multicast Setting** in the function menu bar.

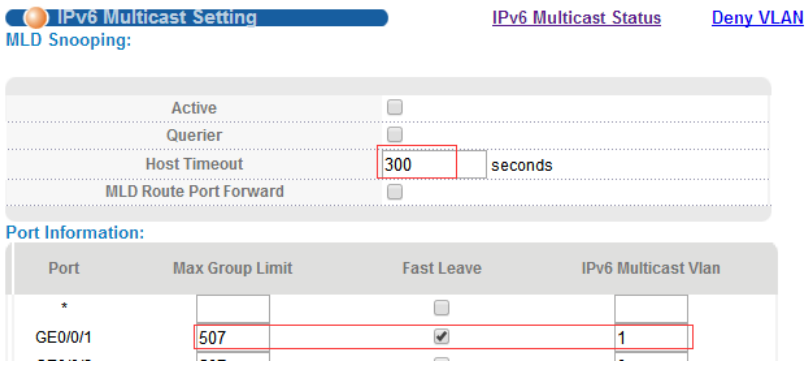


【Parameter Description】

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)

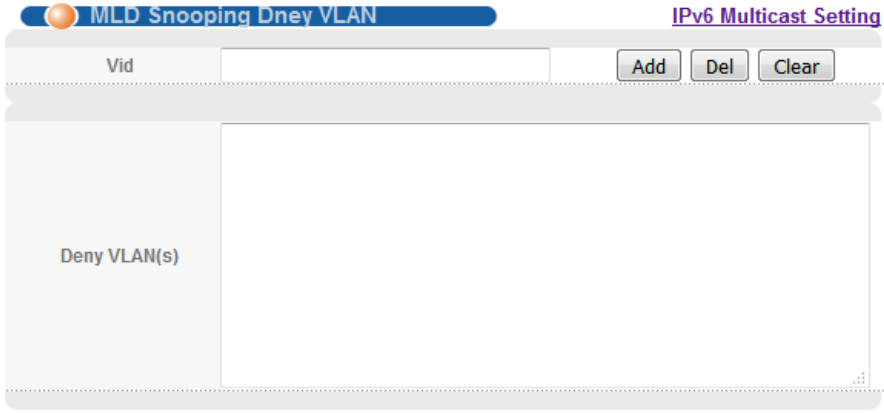
Parameter	Description
MLD Route Port Forward	Enable or disable MLD Route Port Forward
Max Group Limit	Configure maximum learning IPv6 Multicast message of port (default 1020)
Fast Leave	Enable or disable Fast Leave (That is, when the port receives IGMP leave message, the port is deleted immediately from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

【Configuration Example】



4.2.16.3 MLD Snooping Deny VLAN

To configure MLD Snooping Deny VLAN, select **Advanced Application**>**IPv6 Multicast**>**MLD Snooping Deny VLAN** in the function menu bar.

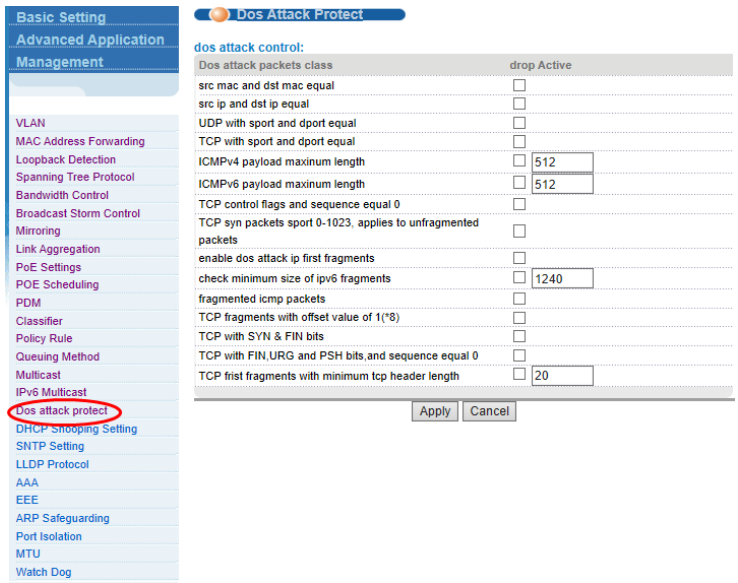


【Parameter Description】

Parameter	Description
Vid	VLAN ID

4.2.17 DoS Attack Protect

To configure DoS Attack Protect, select **Advanced Application**>**Dos Attack Protect** in the function menu bar.

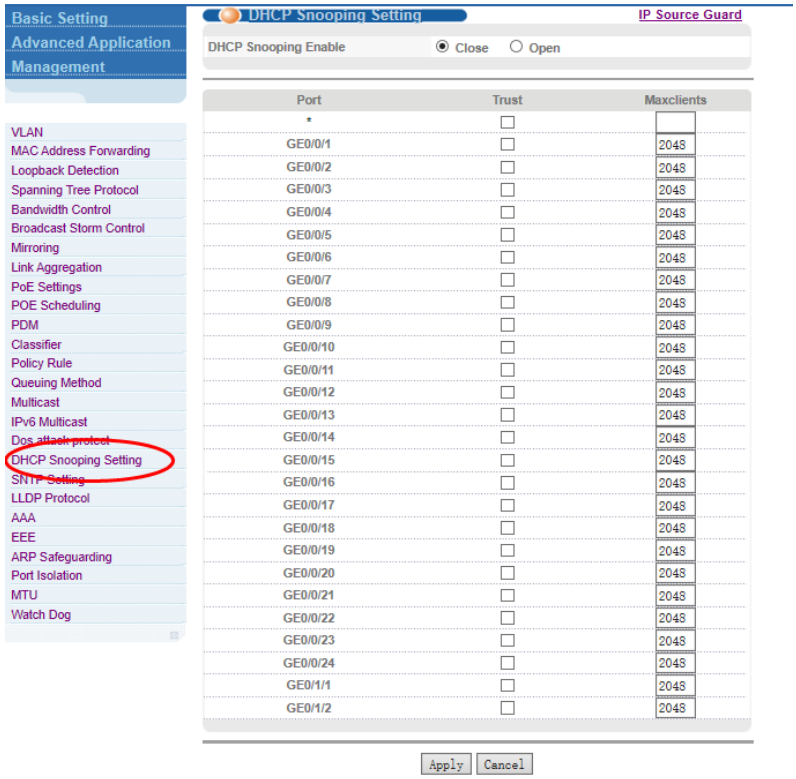


【Parameter Description】

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

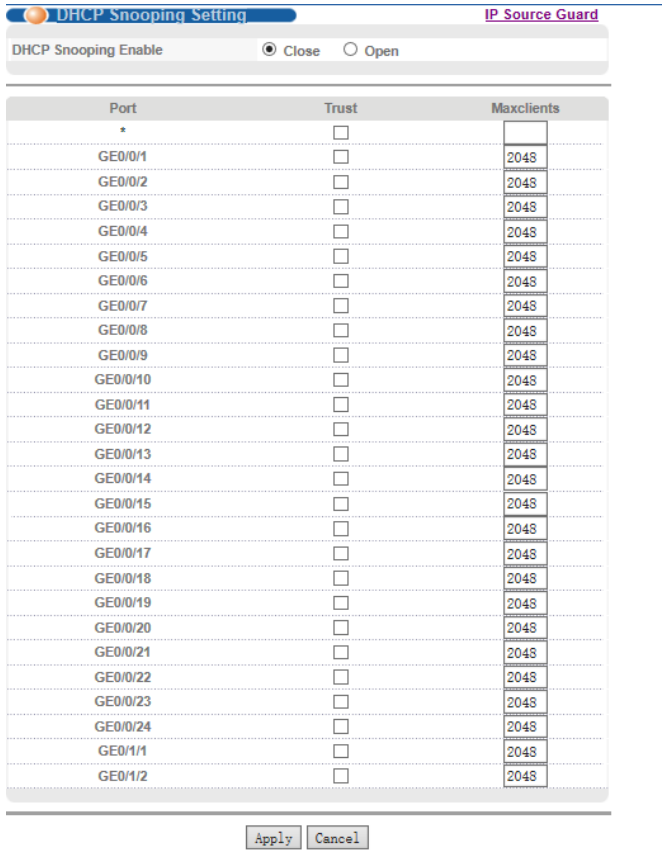
4.2.18 DHCP Snooping Setting

To configure DHCP Snooping, select **Advanced Application**>**DHCP Snooping Setting** in the function menu bar.



4.2.18.1 DHCP Snooping Setting

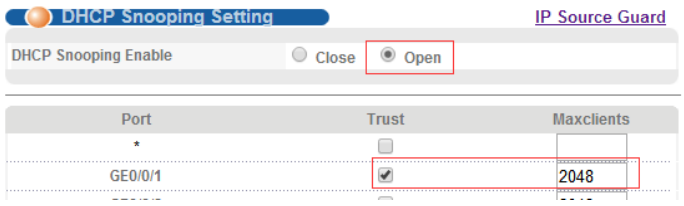
To configure DHCP Snooping, select **Advanced Application**>**DHCP Snooping Setting**>**DHCP Snooping Setting** in the function menu bar. Today's networks can be large and complicated. If the number of wireless network devices exceeds the number of assigned or available IP addresses or if a wireless device's location changes, it becomes necessary to update the corresponding IP address. One way to do this is through Dynamic Host Configuration Protocol (DHCP), the network configuration protocol optimized and developed based on BOOTP.



【Parameter Description】

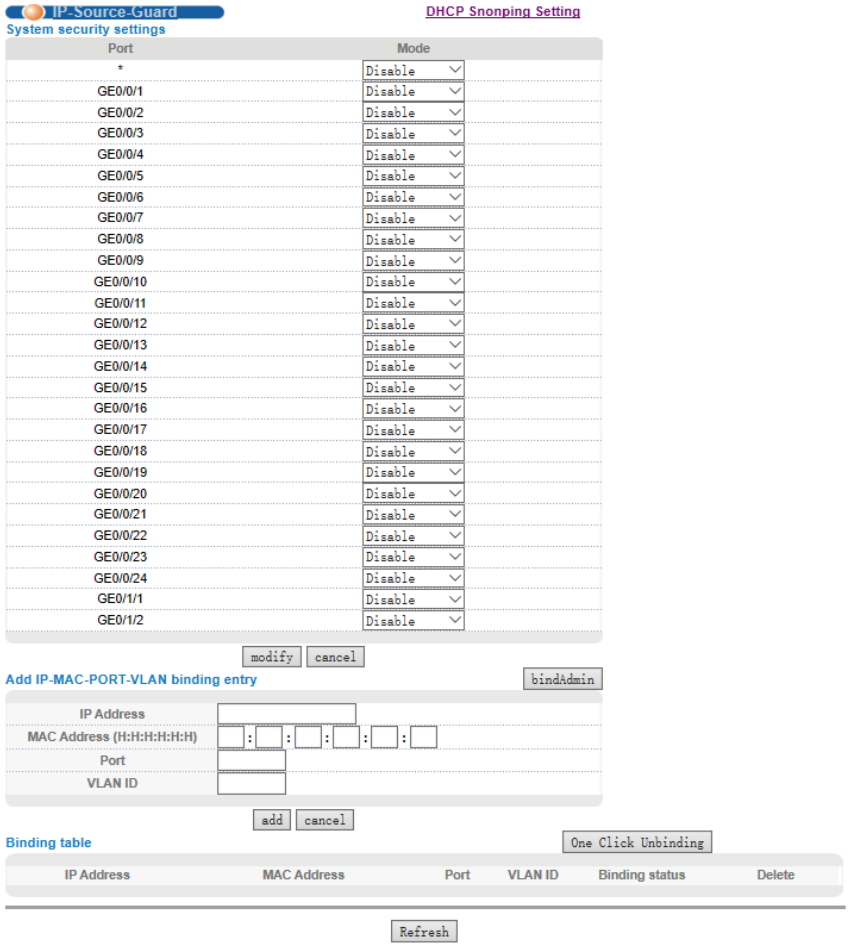
Parameter	Description
DHCP Snooping Enable	Enable or disable DHCP Snooping
Trust	Enable or disable the DHCP Snooping port trust property state
Maxclients	Set Maxclients

【Configuration Example】



4.2.18.2 IP Source Guard

To configure IP Source Guard, select **Advanced Application**>**DHCP Snooping Setting**>**IP Source Guard** in the function menu bar.

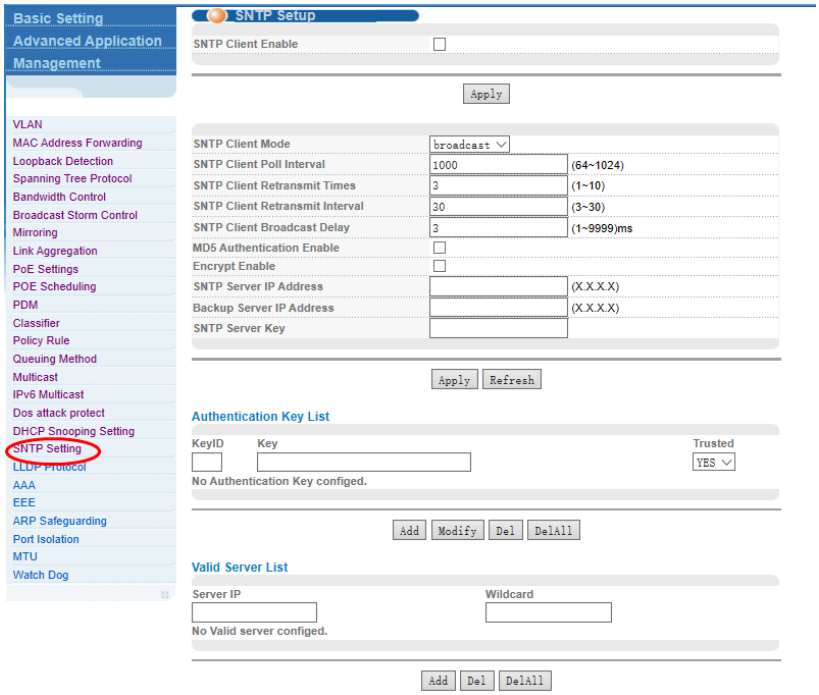


【Parameter Description】

Parameter	Description
Mode	Setting the Mode (Disable, IP, IP+MAC, IP+MAC+VLAN)

4.2.19 SNTP Setting

To configure SNTP, select **Advanced Application**>**SNTP Setting** in the function menu bar.



【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	The interval that SNTP Client sends requests to the SNTP Server
SNTP Client Retransmit Times	If SNTP Client does not receive a response within a certain period after sending a request, it will resend the request until the number of retransmissions exceeds the set value
SNTP Client Retransmit Interval	The interval that SNTP Client resends requests to the SNTP Server
SNTP Client Broadcast Delay	Set SNTP Client Broadcast Delay times
MD5 Authentication Enable	Enable or disable MD5 Authentication
Encrypt Enable	Enable or disable Encrypt
SNTP Server IP Address	Set SNTP Server IP Address
Backup Server IP Address	Set Backup Server IP Address

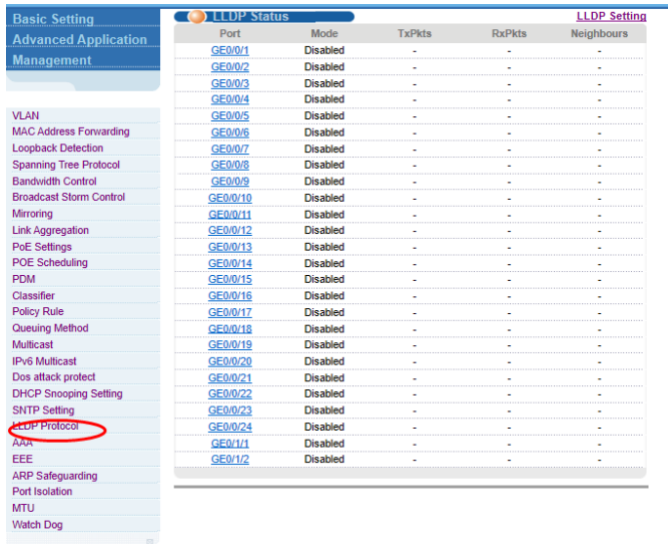
Parameter	Description
SNTP Server Key	Set SNTP Server Key

【Information】

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

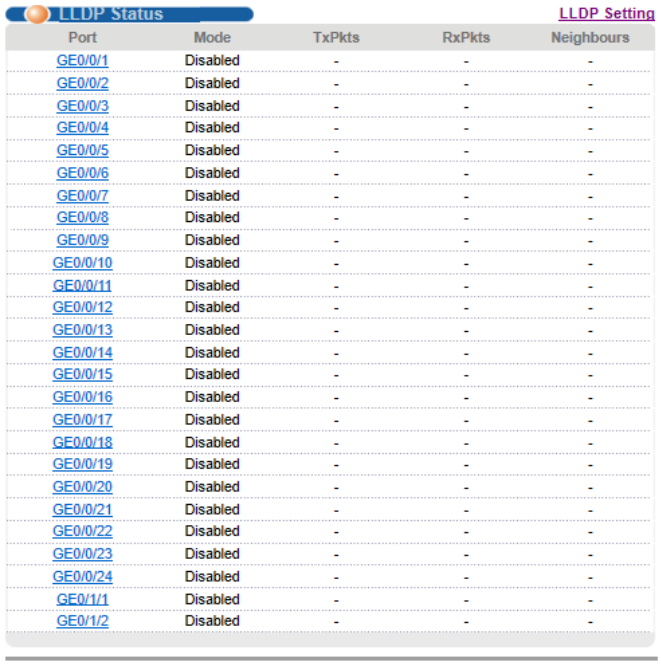
4.2.20 LLDP Protocol

To configure LLDP, select **Advanced Application**>**LLDP Protocol** in the function menu bar.



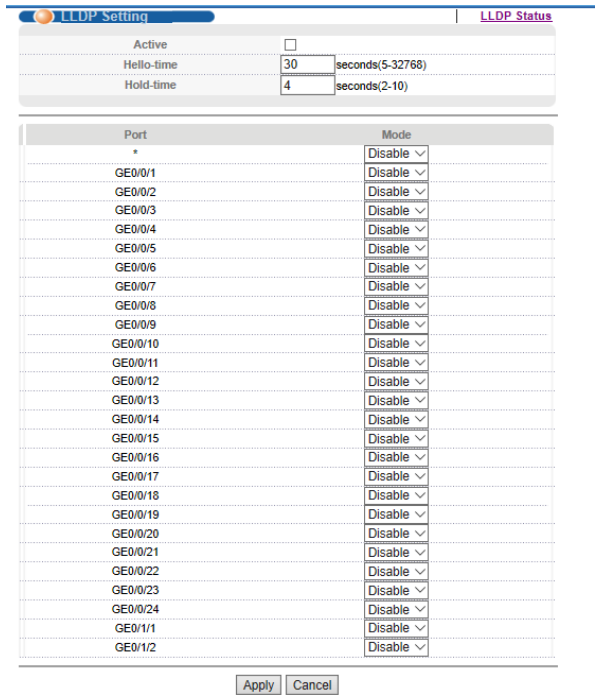
4.2.20.1 LLDP Status

To view LLDP status, select **Advanced Application**>**LLDP Protocol**>**LLDP Status** in the function menu bar.



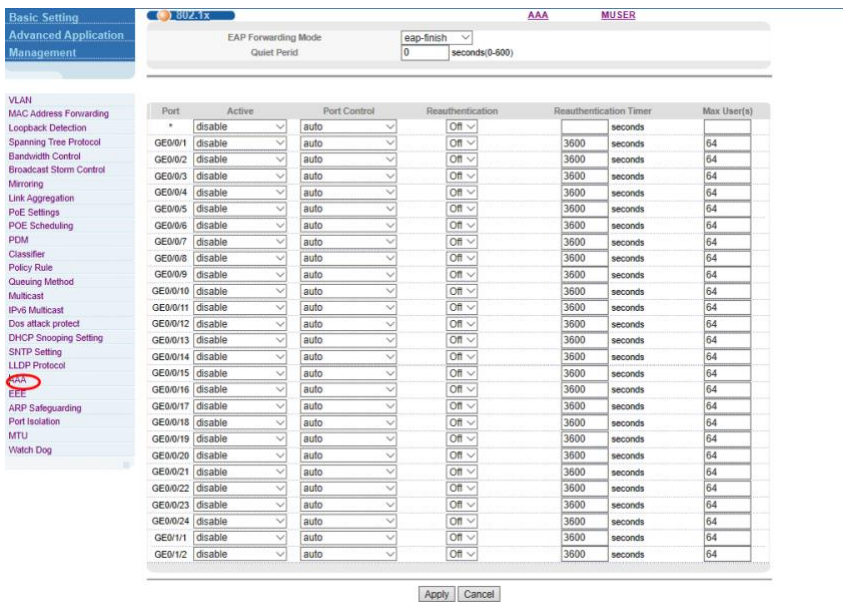
4.2.20.2 LLDP Setting

To configure LLDP, select **Advanced Application**>**LLDP Protocol**>**LLDP Setting** in the function menu bar.



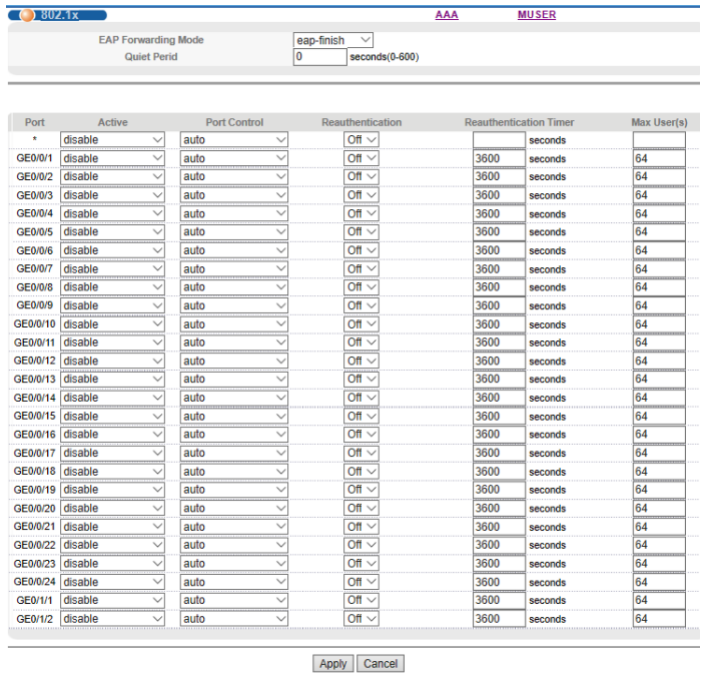
4.2.21 AAA

To configure AAA, select **Advanced Application**>**AAA** in the function menu bar.



4.2.21.1 802.1x

To configure 802.1x, select **Advanced Application**>**AAA**>**802.1x** in the function menu bar.

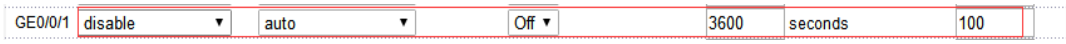


【Parameter Description】

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 until a certain time
Active	Active: disable portbased (multi) portbased (single) macbased
Port Control	Port Control: auto forceauthorized forceunauthorized

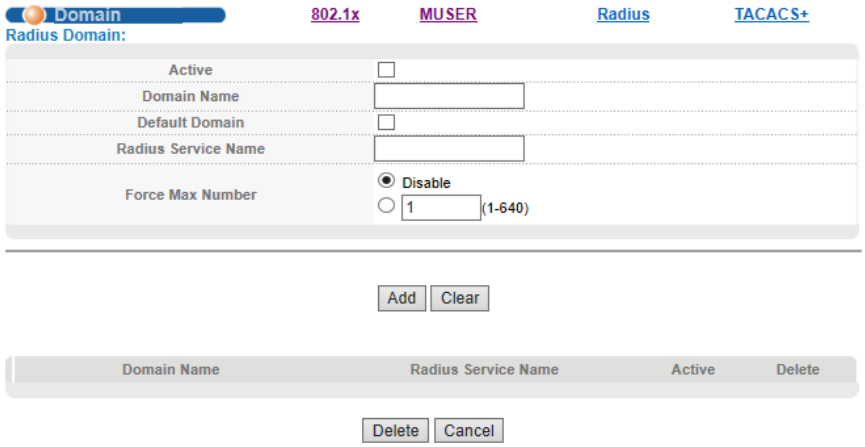
Parameter	Description
Reauthentication	After user authentication is passed, the port can be configured to require reauthentication or to periodically re-authenticate
Reauthentication Timer	Time range: 10 - 3600 seconds
Max user(s)	The maximum number of users: 1 - 100

【Configuration Example】



4.2.21.2 Domain

To configure RADIUS Domain, select **Advanced Application**>**AAA**> **Domain** in the function menu bar.



【Parameter Description】

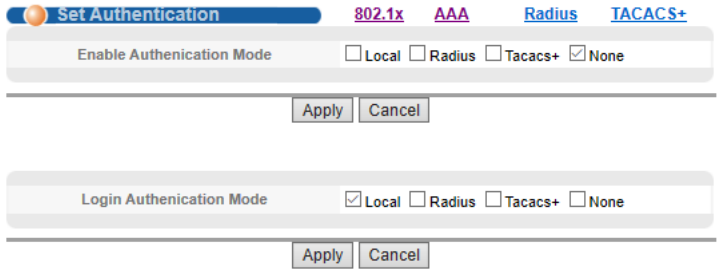
Parameter	Description
Active	Enable or disable RADIUS domain
Domain Name	Set domain name
Default Domain	Enable or disable Default Domain
Radius Server Name	Set RADIUS Server name
Force Max Number	Maximum number of user connections range: 1 - 640

【Information】

This function requires a username and password to authenticate a client. The username information generally includes the user's ISP information, the domain and one-to-one correspondence with the ISP. The main information domain is the domain of the user that is authenticated and accounted for by the RADIUS server.

4.2.21.3 Set Authentication

To configure Remote Authentication, select **Advanced Application**>**AAA**>**Set Authentication** in the function menu bar.

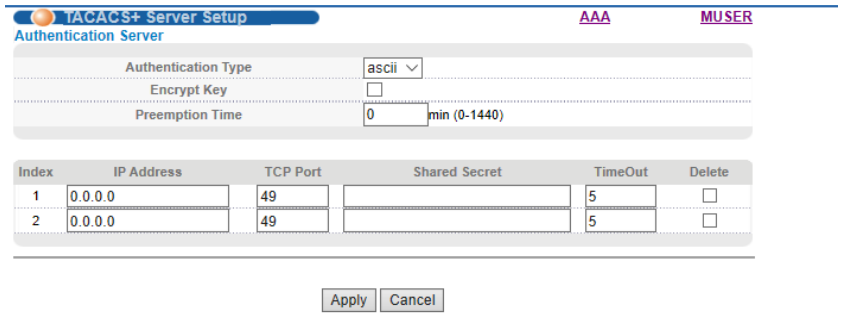


【Parameter Description】

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

4.2.21.4 TACACS+ Server Setup

To configure TACACS+ Server Setup, select **Advanced Application**>**AAA**>**TACACS+ Server Setup** in the function menu bar.

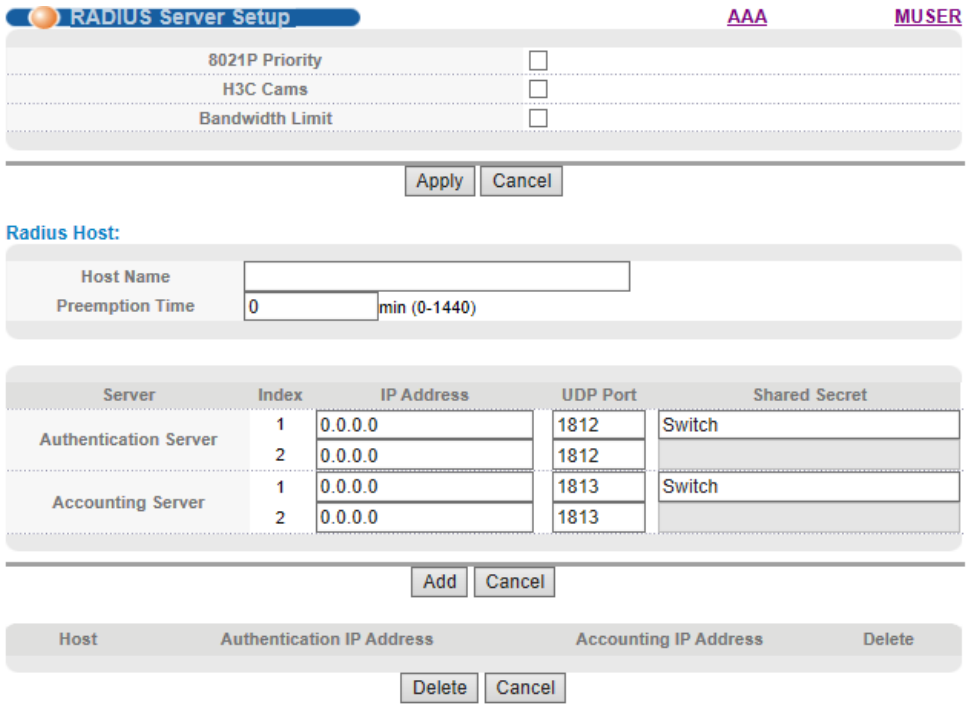


【Parameter Description】

Parameter	Description
Authenication Type	Authenication Mode: ascii, chap, pap
Preemption Time	The time range: 0 - 1440 minutes

4.2.21.5 Radius Server Setup

To configure RADIUS Server Setup, select **Advanced Application**>**AAA**>**Radius Server Setup** in the function menu bar.

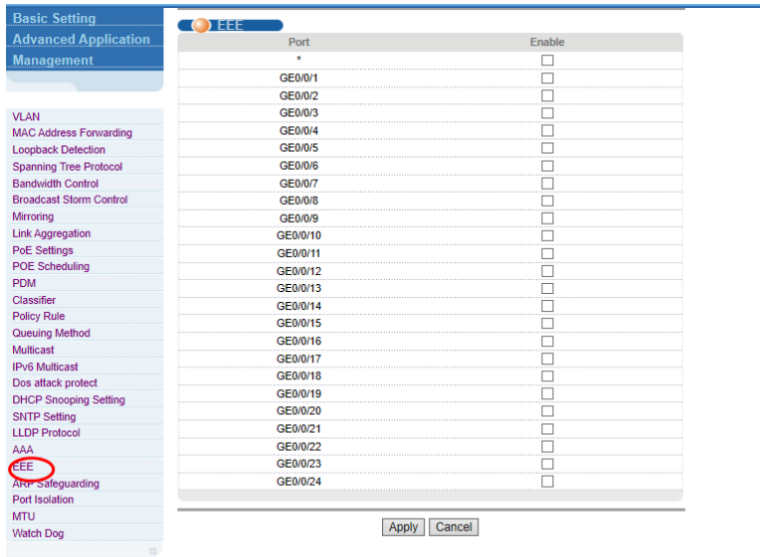


【Parameter Description】

Parameter	Description
8021P Priority	If activated and user authentication is successful, this function will modify the PVID of the user's port.
H3C Cams	If activated, this function configures the version information of transmitting clients to the RADIUS server through the RADIUS attribute client-version.
Bandwidth limit	If activated and user authentication is successful, this function will modify the bandwidth of the user's port.

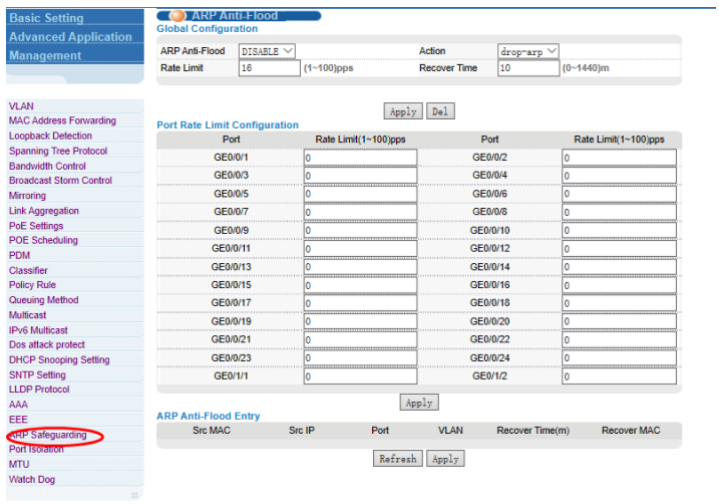
4.2.22 EEE (Part of our Self-Healing Network Suite of Features)

To enable or disable the function for Energy Efficient Ethernet, select **Advanced Application>EEE** in the function menu bar.



4.2.23 ARP Safeguarding

To prevent ARP flooding, select **Advanced Application**>**ARP Safeguarding**.

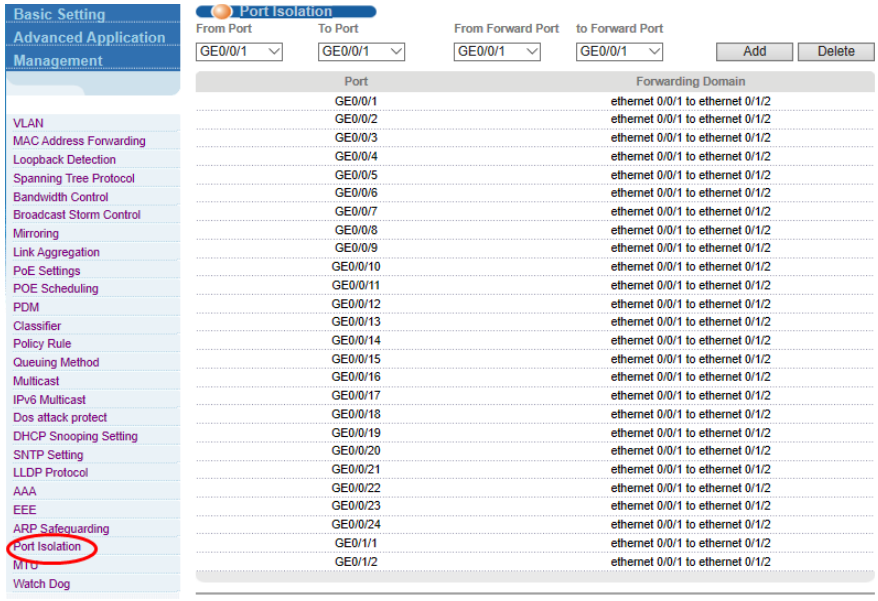


【Parameter Description】

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

4.2.24 Port Isolation

To configure Port Isolation, select **Advanced Application**>**Port Isolation**.



4.2.25 MTU

To configure to MTU, select **Advanced Application**>**MTU**.

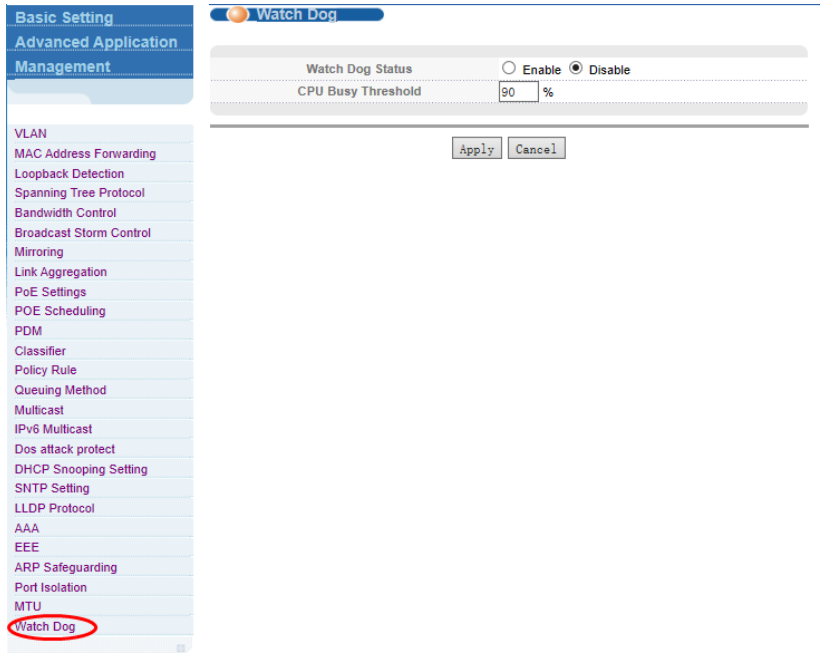
【Parameter Description】

Parameter	Description
MTU	Set MTU, range 1522 – 10240

4.2.26

4.2.26 Watch Dog (Part of our Self-Healing Network Suite of Features)

To configure Watch Dog, select **Advanced Application**>**Watch Dog**.

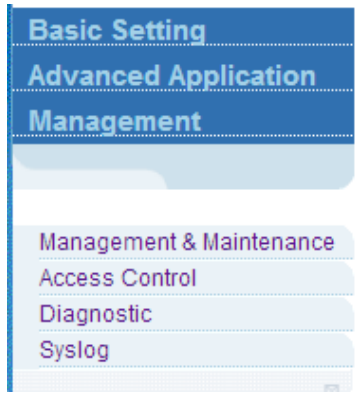


【Parameter Description】

Parameter	Description
Watch Dog Status	Enable or disable Watch Dog Status
CPU Busy Threshold	Set the CPU Busy Threshold

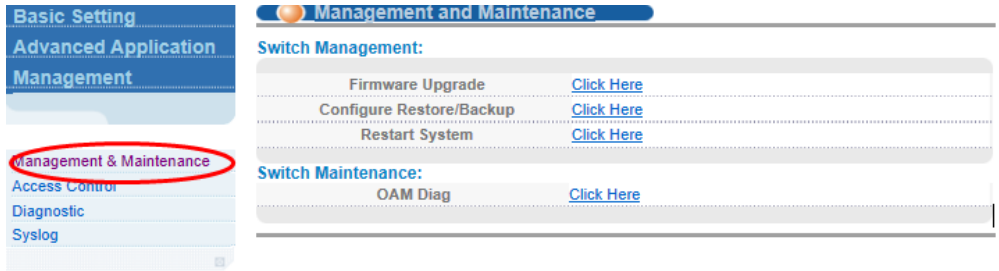
4.3 Management

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



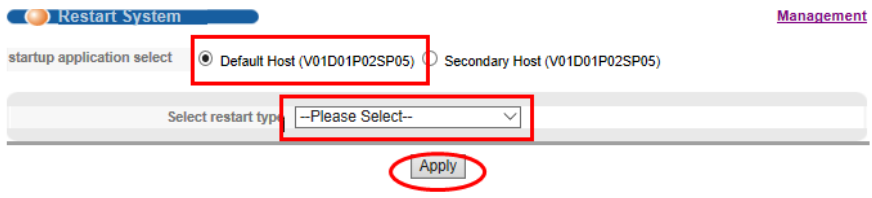
4.3.1 Management and Maintenance

To upgrade firmware, restart the system and perform switch maintenance, select **Management**> **Management & Maintenance** in the function menu bar.

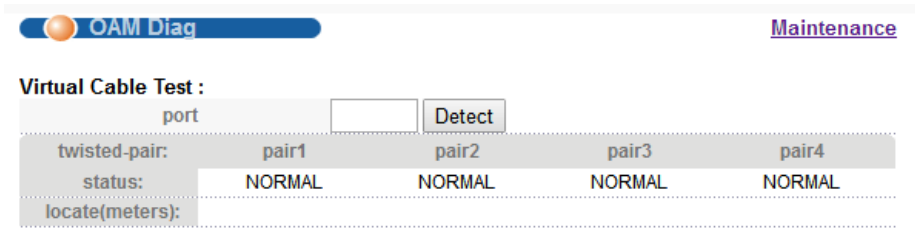


【Configuration Example】

1. Firmware Upgrade.
2. Restart system. Restart type: Restart, Restart with Factory Defaults.

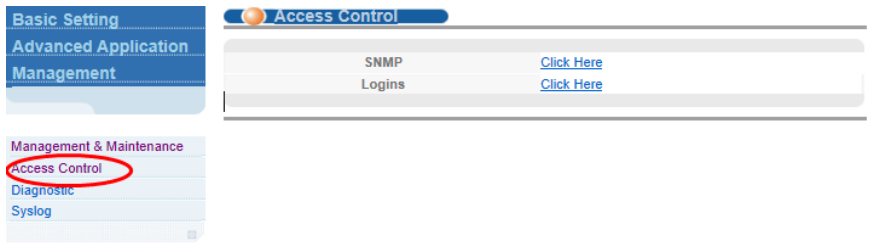


3. OAM Diag, Virtual cable can be tested.



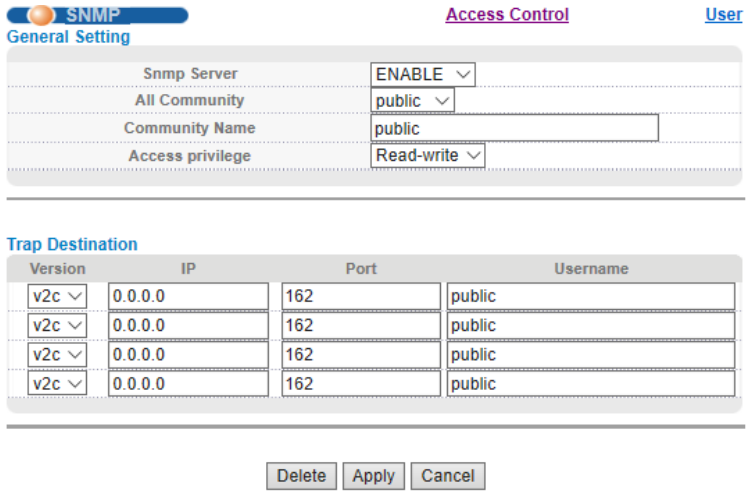
4.3.2 Access Control

To set SNMP and Logins, select **Management**>**Access Control** in the function menu bar.



4.3.2.1 SNMP

To configure SNMP, select **Management**> **Access Control**>**SNMP** in the function menu bar.

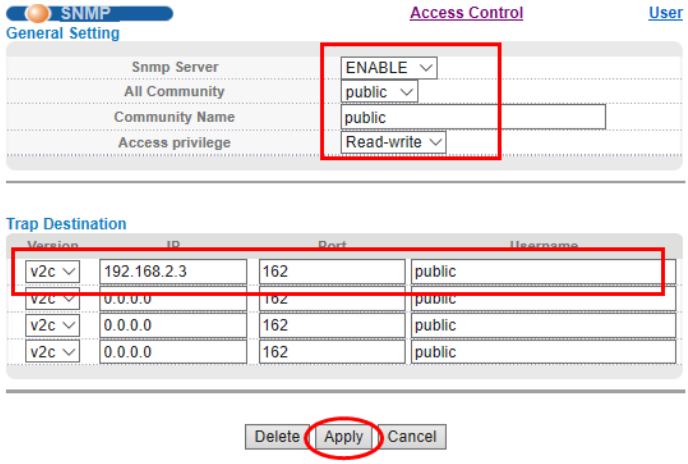


【Parameter Description】

Parameter	Description
All Community	Set All Community
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 read and also be modified
Version	Set version: v1, v2c, v3
IP	Set the IP address of the trap host

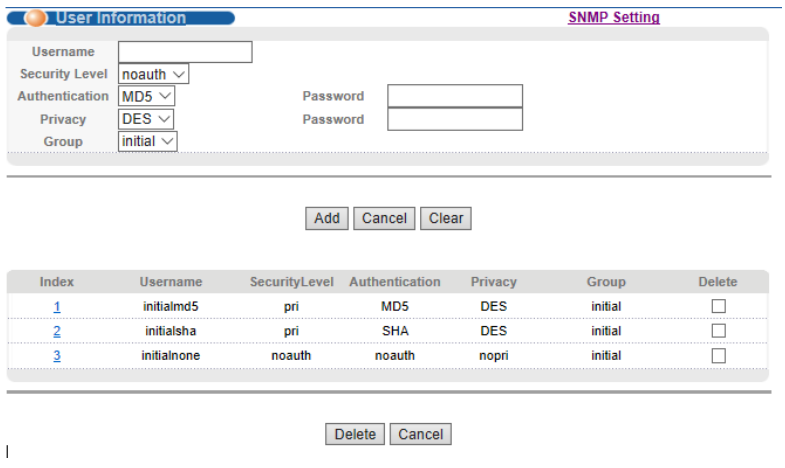
【Configuration Example】

Add a group name public community, set access to Read-Write. Set host 192.168.2.3 to receive trap messages. The specified version is v2c.



4.3.2.2 User Information

To add a user, set a Security Level, Authentication, Privacy, Group and Password, select **Management**> **Access Control**>**User Information** in the function menu bar.

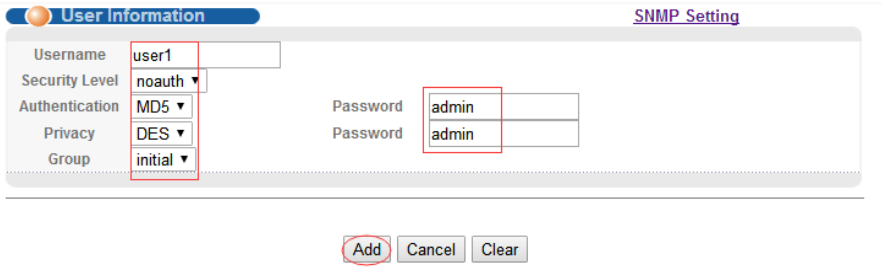


【Parameter Description】

Parameter	Description
Username	SNMP username
Security Level	Noauth, auth, pri
Authentication	MD5, SHA
Privacy	DES Privacy
Group	User group name
Password	Encrypted password

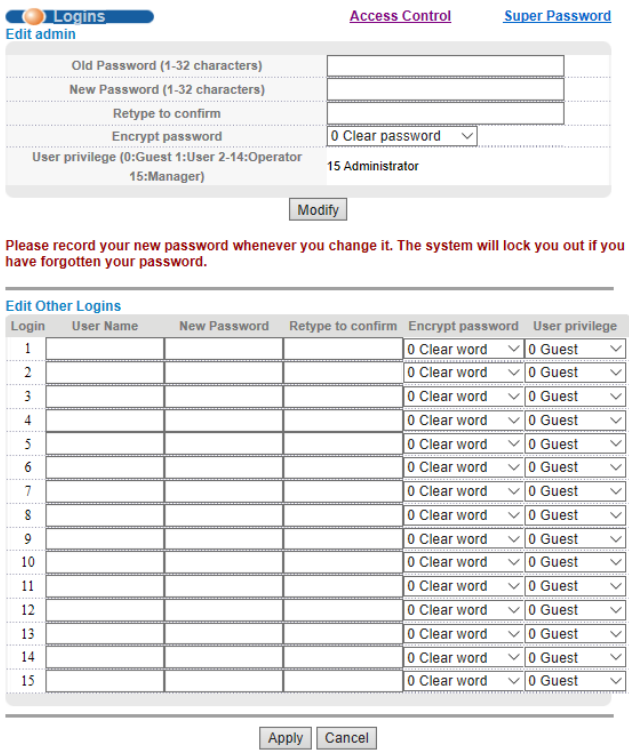
【Configuration Example】

Add group initial, add username user1.



4.3.2.3 Logins

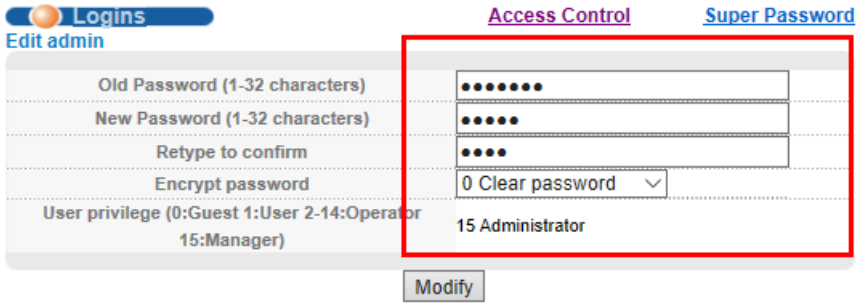
To modify the admin password and configure ordinary users, select **Management**>**Access Control**>**Logins** in the function menu bar.

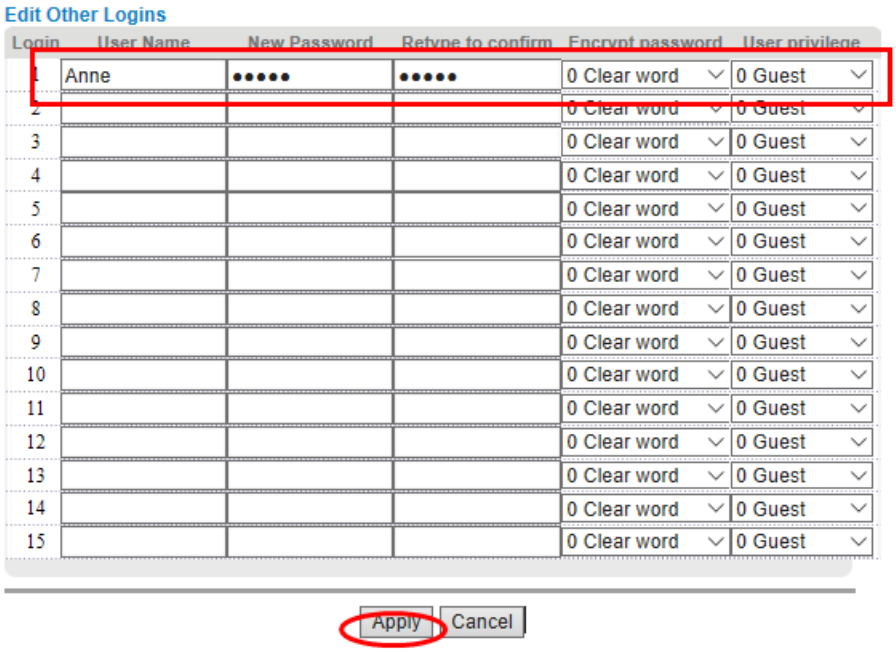


【Parameter Description】

Parameter	Description
User privilege	0 - 1: normal; 2 - 15: administrator

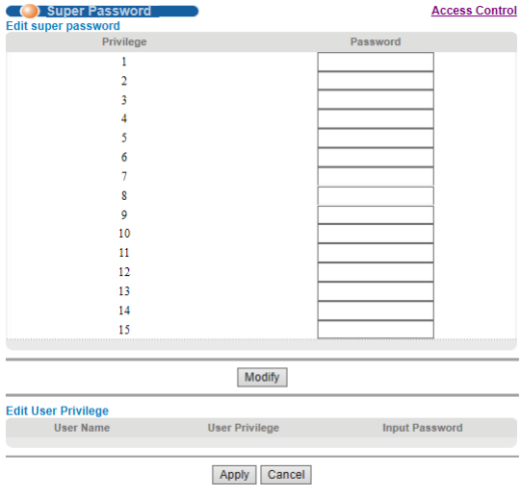
【Configuration Example】





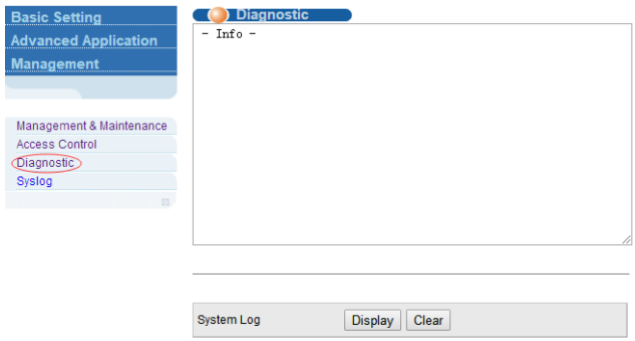
4.3.2.4 Super Password

To set a Super Password, select **Management**>**Access Control**>**Super Password** in the function menu bar.



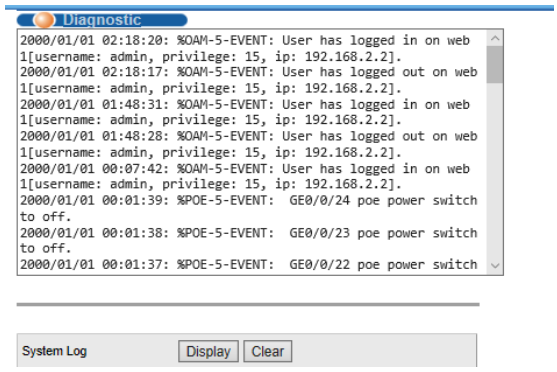
4.3.3 Diagnostic

To display or clear the System Log, select **Management**> **Diagnostic** in the function menu bar.



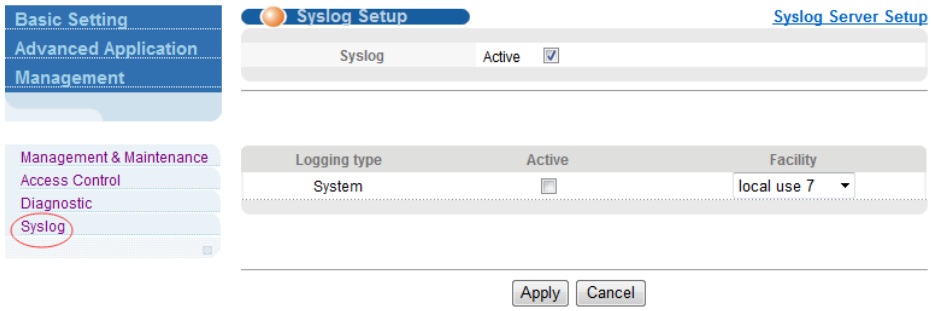
【Configuration Example】

Display System Log.



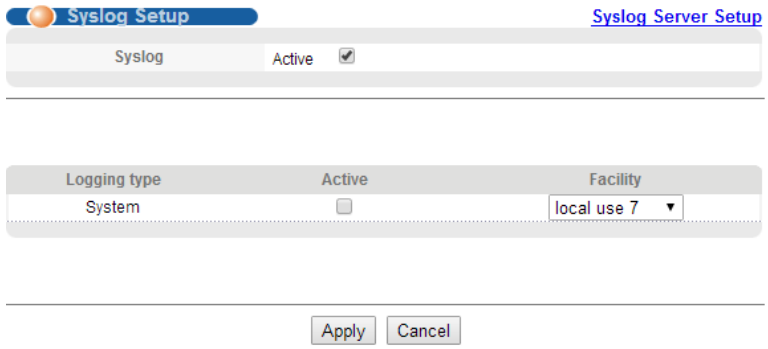
4.3.4 Syslog

To configure the Syslog, select **Management**> **Syslog** in the function menu bar.



4.3.4.1 Syslog Setup

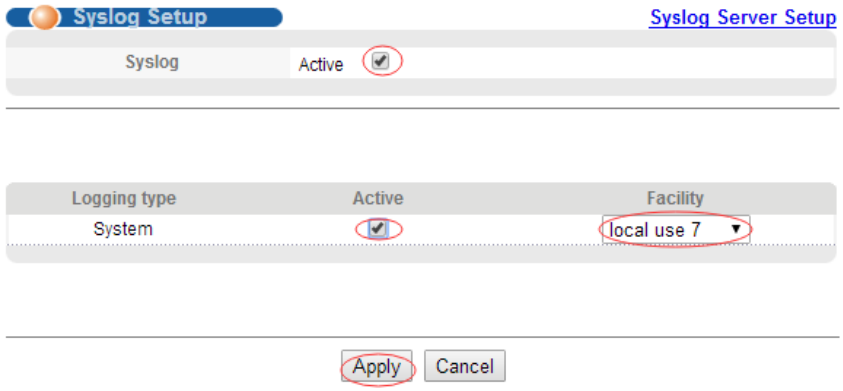
To start the logging function globally and the logging function of the corresponding module, select **Management**>**Syslog**>**Syslog Setup** in the function menu bar.



【Parameter Description】

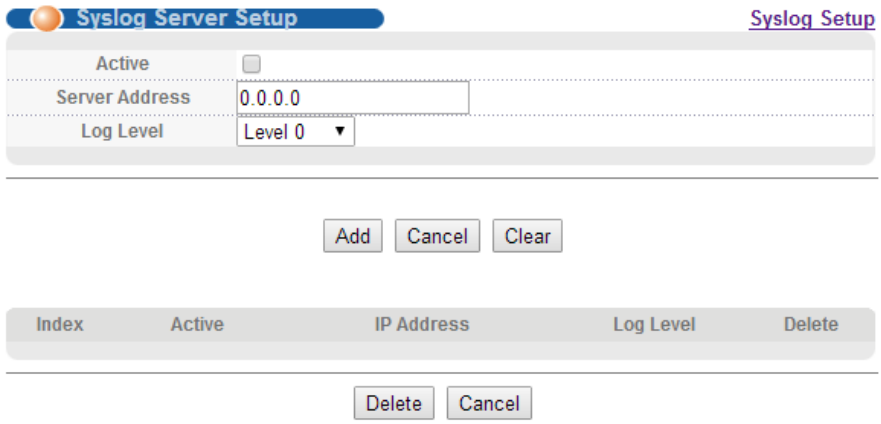
Parameter	Description
Facility	local use 0 - 7 kernel userlevel mail system sercurity_1-2 sysogd lineprinter Networknews uucp clock_1-2 ftp logaudit logalert

【Configuration Example】



4.3.4.2 Syslog Server Setup

To set the syslog server, select **Management**>**Syslog**>**Syslog Server Setup** in the function menu bar.



【Parameter Description】

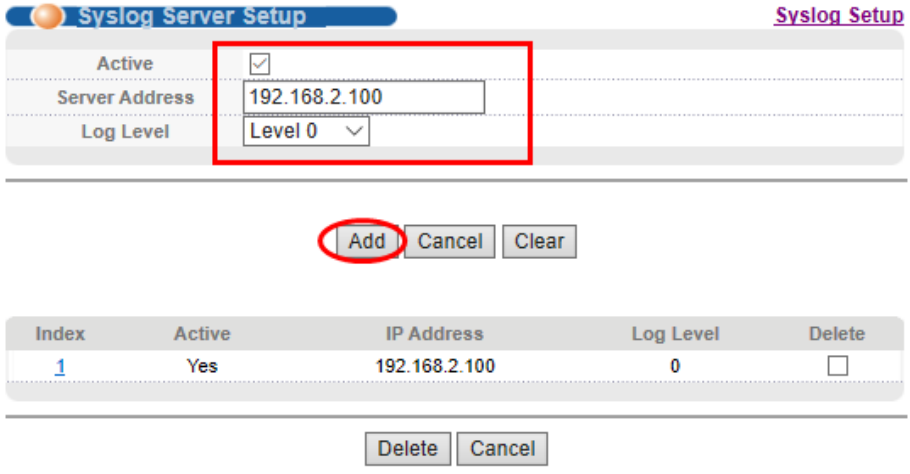
Parameter	Description
Server Address	Syslog Server Address
Log Level	Level 0 Level 0-1 Level 0-2 Level 0-3 Level 0-4 Level 0-5 Level 0-6 Level 0-7
Server Address	Syslog Server Address

【Information】

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

【Configuration Example】

Set server address to 192.168.2.100.



Chapter 5 - Appendix

5.1 Technical Specifications

5.1.1 Hardware Specifications	
Standards	IEEE 802.3i, IEEE 802.3u, IEEE 802.3ab, IEEE 802.3x, IEEE 802.3z, IEEE 802.3at (excluding 508834), IEEE 802.3af (excluding 508834), IEEE 802.1q, IEEE 802.1p
Network Media (Cable)	10Base-T: UTP category 3, 4, 5 cable (maximum 100 m) 100Base-Tx: UTP category 5, 5e cable (maximum 100 m) 1000Base-T: UTP category 5e, 6 cable (maximum 100 m) 1000Base-SX:62.5µm/50µm MMF (2 m – 550 m) 1000Base-LX:62.5µm/50µm MMF (2 m – 550 m) or 10µm SMF (2 m – 5000 m)
Number of Ports (Total)	• 560559: 26 (24 RJ45, 2 SFP) • 561167: 10 (8 RJ45, 2 SFP) • 561198: 18 (16 RJ45, 2 SFP) • 561341: 18 (16 RJ45, 2 SFP) • 561426: 28 (24 RJ45, 4 Combo [4 SFP, 4 RJ45 Uplinks]) • 508834: 10 (8 RJ45, 2 SFP) • 562003: 10 (8 RJ45, 2 SFP)
Transfer Method	Store-and-Forward
Switching Capacity	• 560559: 52 Gbps • 561167: 20 Gbps • 561198: 36 Gbps • 561341: 36 Gbps • 561426: 56 Gbps • 508834: 20 Gbps • 562003: 20 Gbps
MAC Address Learning	8,192
Packet Forwarding Rate	• 1,488,000 pps (1000 Mbps), 148,800 pps (100 Mbps), 14,880 pps (10 Mbps)
Packet Buffer	• 560559, 561167, 561198, 561341: 512 kBytes • 561426, 508834, 562003: 4.1 Mbit
Jumbo Frame	Up to 9,216
PoE Ports (RJ45)	• 560559: 24

		• 561167: 8 • 561198: 16 • 561341: 16 • 561426: 24 • 508834: not applicable • 562003: 8
PoE Budget		• 560559: 240 W • 561167: 140 W • 561198: 374 W • 561341: 220 W • 561426: 370 W • 508834: not applicable • 562003: 242 W
Power Pin Assignment		1/2(+),3/6(-) (excluding 508834)
Indicators	Per Device	**Standard Switches** System Power **Industrial Switch 508834** PWR1, PWR2, System Power
	Per Port	Link/Activity/Speed, PoE (excluding 508834)
Frame Filtering and Forward Rate		10 Mbps: 14880pps 100 Mbps: 148800pps 1000 Mbps: 1488000pps
Dimensions (W x L × H)		• 560559: 440 (W) x 208 (L) x 44 (H) mm (17.3 x 8.19 x 1.7 in.) • 561167: 280 (W) x 180 (L) x 44 (H) mm (11.02 x 7.09 x 1.73 in.) • 561198: 440 (W) x 208 (L) x 44 (H) mm (17.32 x 8.19 x 1.73 in.) • 561341: 440 (W) x 208 (L) x 44 (H) mm (17.32 x 8.19 x 1.73 in.) • 561426: 440 (W) x 208 (L) x 44 (H) mm (17.32 x 8.19 x 1.73 in.) • 508834: 140 (W) x 175 (L) x 55 (H) mm (5.51 x 6.89 x 2.17 in.) • 562003: 230 (W) x 280 (L) x 44 (H) mm (9.06 x 11.02 x 1.73 in.)
Power Supply		• 560559: 90 – 260 V AC, 50 – 60 Hz • 561167, 561198, 561341, 562003: 100.0 – 240.0 VAC, 50 – 60 Hz • 561426: 90 – 240 V AC, 50 – 60 Hz • 508834: 44.0 - 57.0 VDC
Power consumption		• 560559: 260 watts (max.) • 561167: 163.2 watts (max.) • 561198: 410 watts (max.) • 561341: 260 watts (max.) • 561426: 431.7 watts (max.) • 508834: 8.76 watts (max.) • 562003 : 252 watts (max.)

Environment	**Standard Switches** Operating Temperature: 0°C – 45°C Storage Temperature: -40°C – 70°C Operating Humidity: 10% – 90% non-condensing Storage humidity: 5% – 90% non-condensing **Industrial Version 508834** Operating Temperature: -40 °C – 85°C Storage Temperature: -40°C – 85°C Operating Humidity: 5% – 95% RH non-condensing Storage humidity: 5% – 95% RH non-condensing

5.1.2 Software Specification

Basic function	Ethernet Setup STP/RSTP/MSTP Storm-control Port Monitor Port rate-limit MAC filtering
Three layers of functional	ARP deception, network cheating Filtering the IP port Static binding IP and MAC ARP trust port Static routing capacity Ping and Traceroute
The security policy	ACE capacity ACL QoS DAI
VLAN	Port based VLAN 802.1Q VLAN
Safety features	RADIUS TACACS+ Preventing DoS attacks dot1x Gateway ARP deception
Application protocol	DHCP Relay DHCP Snooping DHCP Client FTP/TFTP

Management	HTTP WEB Telnet SSH Console
Other function	LLDP IGMP Snooping SNMPV1, V2c, V3 RMON (1, 2, 3, 9)
PoE Management	PoE Status Power supply management mode(auto/energy/static) The port priority

5.2 Features and Terms Explained

VLAN
A Virtual Local Area Network, this allows network admins to maintain a virtual network to optimize devices attached to the switch for better overall performance.

MAC Address Forwarding
The ability in Layer 2 networking to control network traffic based on MAC address within VLANs.

Loopback Detection
Loopback Detection allows the switch to detect loops in the network (multiple connections from one device to another). When a loop is detected on a port, the switch will display an alert on the management interface and block the traffic on the corresponding port.

Spanning Tree Protocol (STP)
Another form of loopback discovery and protection based upon the IEEE802.1D standard.

Bandwidth Control
The ability to limit network traffic on a specific port of the switch on an inbound and/or outbound basis.

Broadcast Storm Control
Storm control and equivalent protocols allow you to rate-limit broadcast packets.

Broadcast storm control is a feature of many managed switches in which the switch intentionally ceases to forward all broadcast traffic if the bandwidth consumed by incoming broadcast frames exceeds a designated configurable threshold.

Mirroring
The ability to duplicate network traffic from one port to another, on an inbound and/or outbound basis.

Link Aggregation
The ability to link multiple ports into one logical interface to increase bandwidth.

PoE
Power over Ethernet, a technique for delivering DC power to devices over copper Ethernet cabling, eliminating the need for separate power supplies and outlets. Current standards are IEEE802.3af/at and bt.

PoE Scheduling
The ability to schedule the availability of PoE on each port of the switch on a day/time basis.

PDM
Powered Device Monitoring, a function that restarts any connected PoE device that fails to respond or send out network traffic. (Configurable on Intellinet Network Solutions Managed Switches).

Chapter 6 - Additional Information

6.1 WASTE ELECTRICAL & ELECTRONIC EQUIPMENT

DISPOSAL OF ELECTRIC AND ELECTRONIC EQUIPMENT

(Applicable In the E.U. and Other European Countries With Separate Collection Systems)

ENGLISH: This symbol on the product or its packaging means that this product must not be treated as unsorted household waste. In accordance with EU Directive 2012/19/EU on Waste Electrical and Electronic Equipment (WEEE), this electrical product must be disposed of in accordance with the user's local regulations for electrical or electronic waste. Please dispose of this product by returning it to your local point of sale or recycling pickup point in your municipality.

DEUTSCH: Dieses auf dem Produkt oder der Verpackung angebrachte Symbol zeigt an, dass dieses Produkt nicht mit dem Hausmüll entsorgtwerden darf. In Übereinstimmung mit der Richtlinie 2012/19/EU des Europäischen Parlaments und des Rates über Elektro- und Elektronik-Altgeräte (WEEE) darf dieses Elektrogerät nicht im normalen Hausmüll oder dem Gelben Sack entsorgt werden. Wenn Sie dieses Produkt entsorgen möchten, bringen Sie es bitte zur Verkaufsstelle zurück oder zum Recycling-Sammelpunkt Ihrer Gemeinde.

ESPAÑOL: Este símbolo en el producto o su embalaje indica que el producto no debe tratarse como residuo doméstico. De conformidad con la Directiva 2012/19/EU de la UE sobre residuos de aparatos eléctricos y electrónicos (RAEE), este producto eléctrico no puede desecharse se con el resto de residuos no clasificados. Deshágase de este producto devolviéndolo a su punto de venta o a un punto de recolección municipal para su reciclaje.

FRANÇAIS: Ce symbole sur le produit ou son emballage signifie que ce produit ne doit pas être traité comme un déchet ménager. Conformément à la Directive 2012/19/EU sur les déchets d'équipements électriques et électroniques (DEEE), ce produit électrique ne doit en aucun cas être mis au rebut sous forme de déchet municipal non trié. Veuillez vous débarrasser de ce produit en le renvoyant à son point de vente ou au point de ramassage local dans votre municipalité, à des fins de recyclage.

POLSKI: Jeśli na produkcie lub jego opakowaniu umieszczono ten symbol, wówczas w czasie utylizacji nie wolno wyrzucać tego produktu wraz z odpadami komunalnymi. Zgodnie z Dyrektywą Nr 2012/19/EU w sprawie zużytego sprzętu elektrycznego i elektronicznego (WEEE), niniejszego produktu elektrycznego nie wolno usuwać jako nie posortowanego odpadu komunalnego. Prosimy o usuniecie niniejszego produktu poprzez jego zwrot do punktu zakupu lub oddanie do miejscowego komunalnego punktu zbiórki odpadów przeznaczonych do recyklingu.

ITALIANO: Questo simbolo sui prodotto o sulla relativa confezione indica che il prodotto non va trattato come un rifiuto domestico. In ottemperanza alla Direttiva UE 2012/19/EU sui rifiuti di apparecchiature elettriche ed elettroniche (RAEE), questa prodotto elettrico non deve essere smaltito come rifiuto municipale misto. Si prega di smaltire il prodotto riportandolo al punto vendita o al punto di raccolta municipale locale per un opportuno riciclaggio.

6.2 WARRANTY

Go to **Intellinet-network.com**

EN MÉXICO: Póliza de Garantía Intellinet Network Solutions — Datos del importador y responsable ante el consumidor • IC Intracom México, S.A.P.I. de C.V. • Av. Interceptor Poniente # 73, Col. Parque Industrial La Joya, Cuautitlán Izcalli, Estado de México, C.P. 54730, México. • Tel. (55)1500-4500 • La presente garantía cubre los siguientes productos contra cualquier defecto de fabricación en sus materiales y mano de obra. A. Garantizamos los productos de limpieza, aire comprimido y consumibles, por 60 dias a partir de la fecha de entrega, o por el tiempo en que se agote totalmente su contenido por su propia función de uso, lo que suceda primero. B. Garantizamos los productos con partes móviles por 3 años. C. Garantizamos los demás productos por 5 años (productos sin partes móviles), bajo las siguientes condiciones: 1. Todos los productos a que se refiere esta garantía, ampara su cambio físico, sin ningún cargo para el consumidor. 2. El comercializador no tiene talleres de servicio, debido a que los productos que se garantizan no cuentan con reparaciones, ni refacciones, ya que su garantía es de cambio físico. 3. La garantía cubre exclusivamente aquellas partes, equipos o sub-ensambles que hayan sido instaladas de fábrica y no incluye en ningún caso el equipo adicional o cualesquiera que hayan sido adicionados al mismo por el usuario o distribuidor. • Para hacer efectiva esta garantía bastará con presentar el producto al distribuidor en el domicilio donde fue adquirido o en el domicilio de IC Intracom México, S.A.P.I. de C.V., junto con los accesorios contenidos en su empaque, acompañado de su póliza debidamente llenada y sellada por la casa vendedora (indispensable el sello y fecha de compra) donde lo adquirió, o bien, la factura o ticket de compra original donde se mencione claramente el modelo, número de serie (cuando aplique) y fecha de adquisición. Esta garantía no es válida en los siguientes casos: Si el producto se hubiese utilizado en condiciones distintas a las normales; si el producto no ha sido operado conforme a los instructivos de uso; o si el producto ha sido alterado o tratado de ser reparado por el consumidor o terceras personas.

6.3 REGULATORY STATEMENTS

FCC Class A

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the Federal Communications Commission (FCC) Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses and can radiate radio frequency energy, and if not installed and used in accordance with the instruction manual may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at his own expense. Any changes or modifications made to this equipment without the approval of the manufacturer could result in the product not meeting the Class A limits, in which case the FCC could void the user's authority to operate the equipment.

CE

ENGLISH : This device complies with the requirements of CE 2014/30/EU (UKCA Electromagnetic Compatibility Regulations 2016) and / or 2014/35/EU (UKCA Electrical Equipment [Safety] Regulations 2016). The Declaration of Conformity for is available at:

DEUTSCH : Dieses Gerät enspricht der CE 2014/30/EU und / oder 2014/35/EU. Die Konformitätserklärung für dieses Produkt finden Sie unter:

ESPAÑOL : Este dispositivo cumple con los requerimientos de CE 2014/30/EU y / o 2014/35/EU. La declaración de conformidad esta disponible en:

FRANÇAIS: Cet appareil satisfait aux exigences de CE 2014/30/EU et / ou 2014/35/EU. La Déclaration de Conformité est disponible à:

POLSKI : Urządzenie spełnia wymagania CE 2014/30/EU I / lub 2014/35/EU. Deklaracja zgodności dostępna jest na stronie internetowej producenta:

ITALIANO : Questo dispositivo è conforme alla CE 2014/30/EU e / o 2014/35/EU. La dichiarazione di conformità è disponibile al:

support.intellinet-network.com/barcode/560559
support.intellinet-network.com/barcode/561167
support.intellinet-network.com/barcode/561198
support.intellinet-network.com/barcode/561341
support.intellinet-network.com/barcode/561426
support.intellinet-network.com/barcode/508834
support.intellinet-network.com/barcode/562003

North America	Asia & Africa	Europe
IC Intracom America	IC Intracom Asia	IC Intracom Europe
550 Commerce Blvd.	4-F, No. 77, Sec. 1, Xintai 5th Rd.	Löhbacher Str. 7, D-58553
Oldsmar, FL 34677 USA	Xizhi Dist., New Taipei City 221, Taiwan	Halver, Germany

All trademarks and trade names are the property of their respective owners. © IC Intracom. All rights reserved.
Intellinet Network Solutions is a trademark of IC Intracom, registered in the U.S. and other countries.