Web Management Guide

Digital Data Communications GmbH.

http://www.level1.com

Web Management Guide

GTP-2871

28-Port L3 Lite Managed Gigabit PoE Switch

GTP-5271

52-Port L3 Lite Managed Gigabit PoE Switch

How to Use This Guide

This guide includes detailed information on the switch software, including how to operate and use the management functions of the switch. To deploy this switch effectively and ensure trouble-free operation, you should first read the relevant sections in this guide so that you are familiar with all of its software features.

Who Should Read this Guide?

This guide is for network administrators who are responsible for operating and maintaining network equipment. The guide assumes a basic working knowledge of LANs (Local Area Networks), the Internet Protocol (IP), and Simple Network Management Protocol (SNMP).

How this Guide is Organized

This guide provides detailed information about the switch's key features. It also describes the switch's web browser interface. For information on the command line interface refer to the *CLI Reference Guide*.

The guide includes these sections:

- Section I "Web Configuration" — Includes all management options available through the web browser interface.

Related Documentation

This guide focuses on switch software configuration through the web browser.

For information on how to manage the switch through the command line interface, see the following guide: *CLI Reference Guide*

Note: For a description of how to initialize the switch for management access via the CLI, web interface or SNMP, refer to "Initial Switch Configuration" in the *CLI Reference Guide*.

Conventions

The following conventions are used throughout this guide to show information:

Note: Emphasizes important information or calls your attention to related features or instructions.

Revision History

This section summarizes the changes in each revision of this guide.

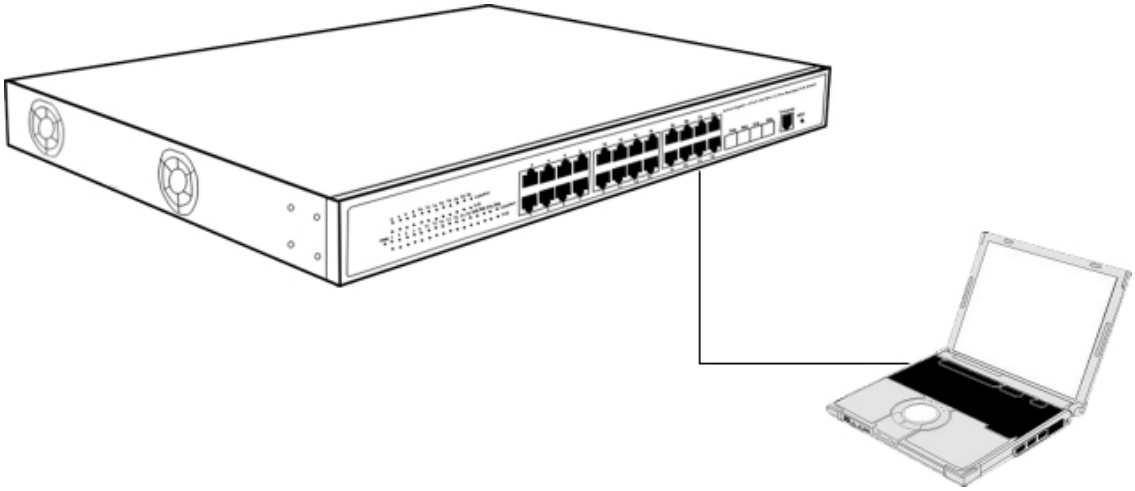
Revision	*Date*	*Change Description*
d19-02-22	02/2019	Initial release

Contents

Connecting to the Web Interface

This switch provides an embedded HTTP web agent. Using a web browser you can configure the switch and view statistics to monitor network activity. The web agent can be accessed by any computer on the network using a standard web browser (Internet Explorer 9, Mozilla Firefox 39, or Google Chrome 44, or more recent versions).

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



⚠ WEB Configuration guide takes GTP-2871/ GTP-5271 as an example.

How to Login the Switch

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

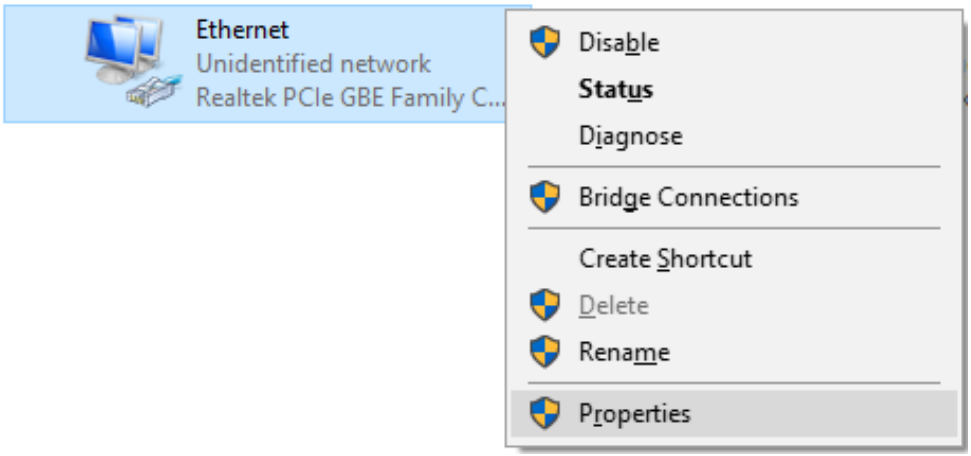
Parameter	Default Value
Default IP address	192.168.1.1
Default user name	admin
Default password	admin

Logging on to the equipment

- Connect the RJ-45 interface cable of a switch with a computer using a network cable.
- Set the TCP/IP properties of the computer.

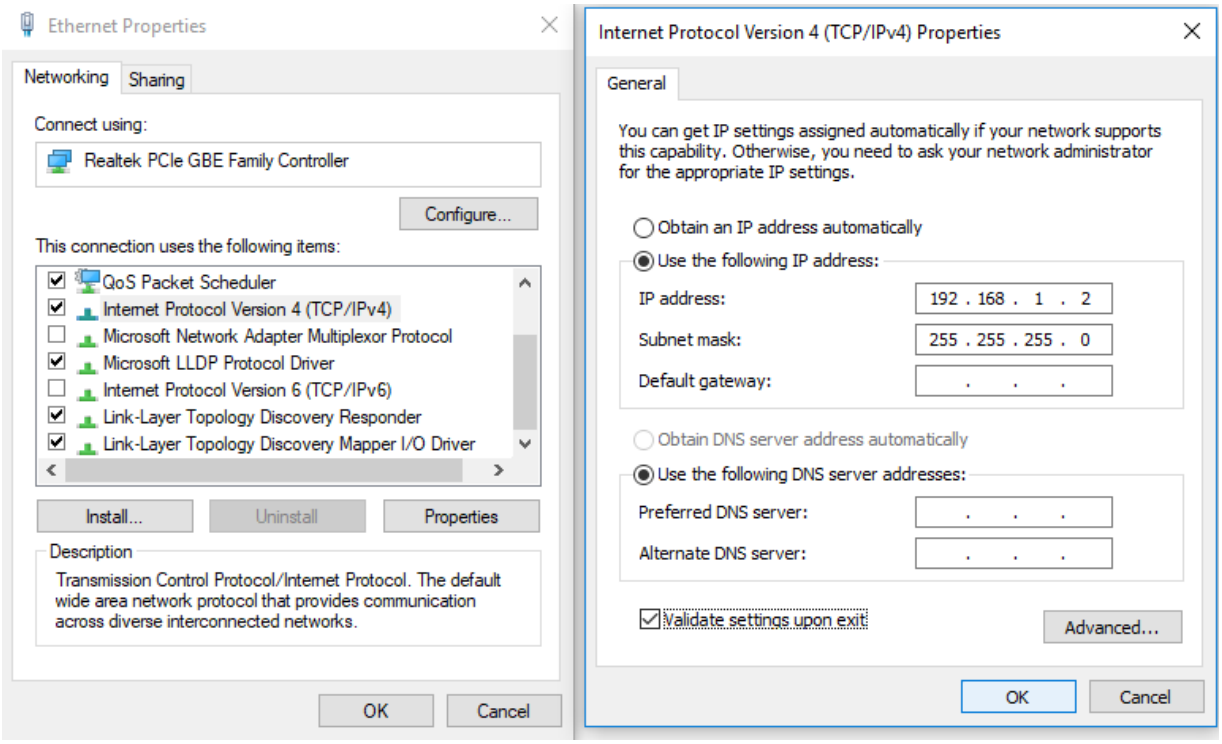
•Windows

1. Click **Start—> Control Panel—> Network and Internet—> Network and Sharing Center—> Change adapter settings**, right click **Local connection** and select **Properties**;

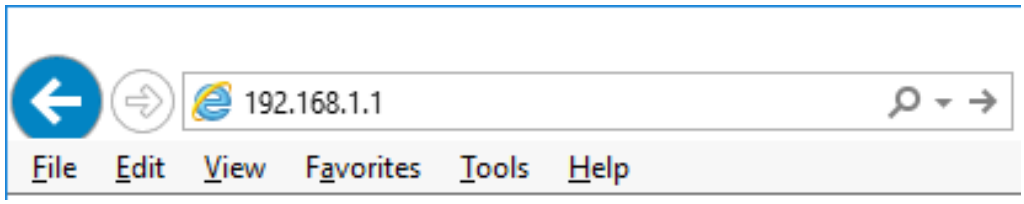


2. Double-click **Internet Protocol 4 (TCP/IPv4)**; Set the computer's IP address:

The computer's IP address should be any one of the following free IP addresses 192.168.1.2 ~ 192.168.1.254, and then click **OK**, to return to the previous page, click **OK**.



- Logging on to the equipment: Open a browser and type 192.168.1.1 in the address bar, and then press Enter; in the pop-up login interface, enter the factory logon **username** "**admin**", **password** "**admin**" and click OK.



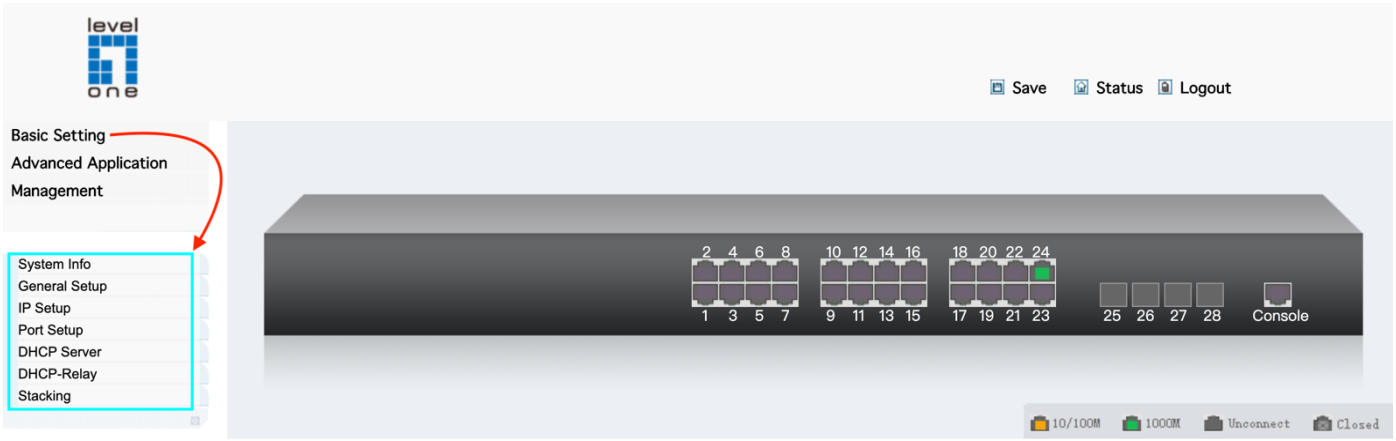
Section I

Basic Setting

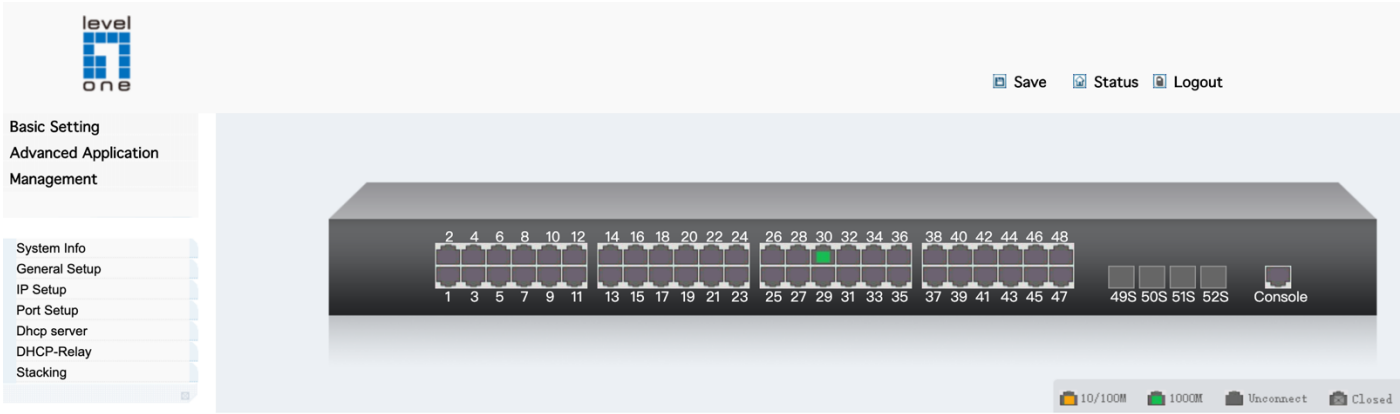
Panel Display

The web agent displays an image of the switch's ports. The Mode can be set to display different information for the ports, including Active (i.e., up or down), Duplex (i.e., half or full duplex), or Flow Control (i.e., with or without flow control)

GTP-2871 (Front Panel Indicators)



GTP-5271 (Front Panel Indicators)



1 System Info

Displaying System Information

Use the System > General page to identify the system by displaying information such as the device name, location and contact information.

Parameters

These parameters are displayed:

- **System Description** – Brief description of device type.

  management subsystem.

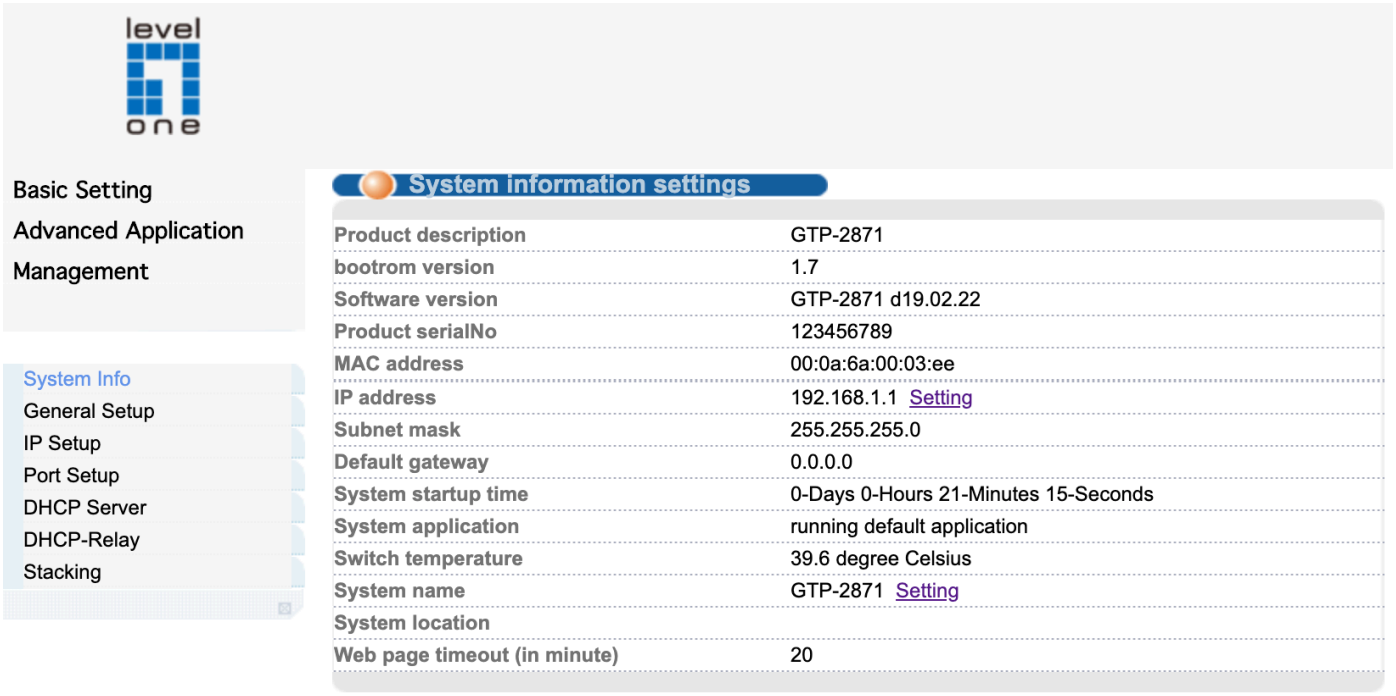
- **System Up Time** – Length of time the management agent has been up.
- **System Name** – Name assigned to the switch system.
- **System Location** – Specifies the system location.
- **System Contact** – Administrator responsible for the system.

Web Interface

To configure general system information:

1. Click System, General.
2. Specify the system name, location, and contact information for the system administrator.
3. Click Apply.

GTP-2871 (System Information)



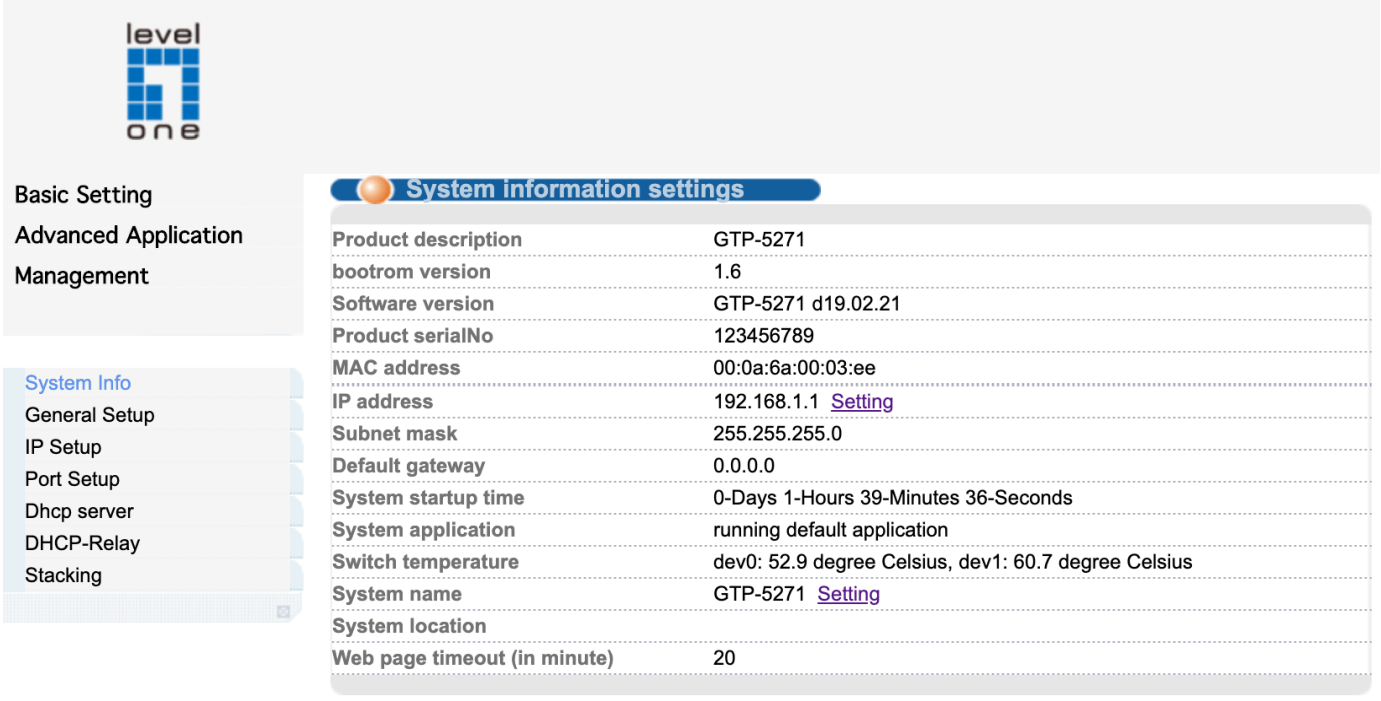
Basic Setting
Advanced Application
Management

System Info
General Setup
IP Setup
Port Setup
DHCP Server
DHCP-Relay
Stacking

System information settings

Product description	GTP-2871
bootrom version	1.7
Software version	GTP-2871 d19.02.22
Product serialNo	123456789
MAC address	00:0a:6a:00:03:ee
IP address	192.168.1.1 Setting
Subnet mask	255.255.255.0
Default gateway	0.0.0.0
System startup time	0-Days 0-Hours 21-Minutes 15-Seconds
System application	running default application
Switch temperature	39.6 degree Celsius
System name	GTP-2871 Setting
System location	
Web page timeout (in minute)	20

GTP-5271 (System Information)



Basic Setting
Advanced Application
Management

System Info
General Setup
IP Setup
Port Setup
Dhcp server
DHCP-Relay
Stacking

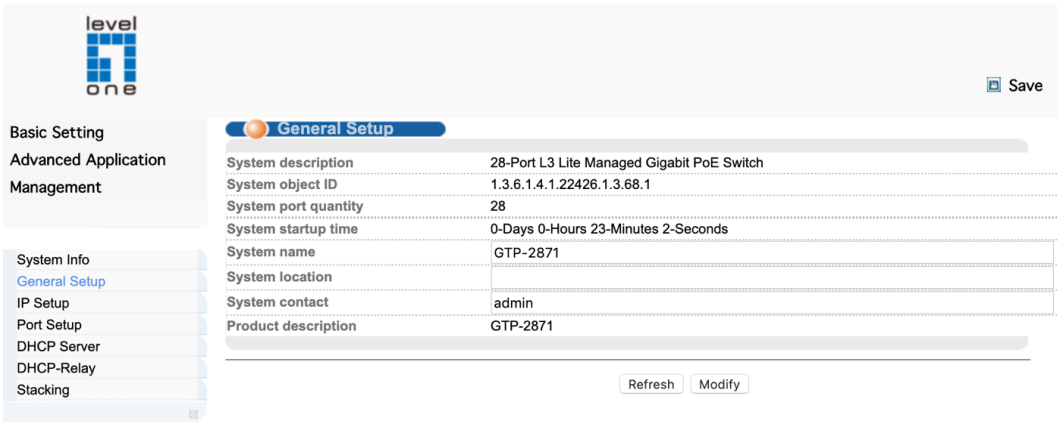
System information settings

Product description	GTP-5271
bootrom version	1.6
Software version	GTP-5271 d19.02.21
Product serialNo	123456789
MAC address	00:0a:6a:00:03:ee
IP address	192.168.1.1 Setting
Subnet mask	255.255.255.0
Default gateway	0.0.0.0
System startup time	0-Days 1-Hours 39-Minutes 36-Seconds
System application	running default application
Switch temperature	dev0: 52.9 degree Celsius, dev1: 60.7 degree Celsius
System name	GTP-5271 Setting
System location	
Web page timeout (in minute)	20

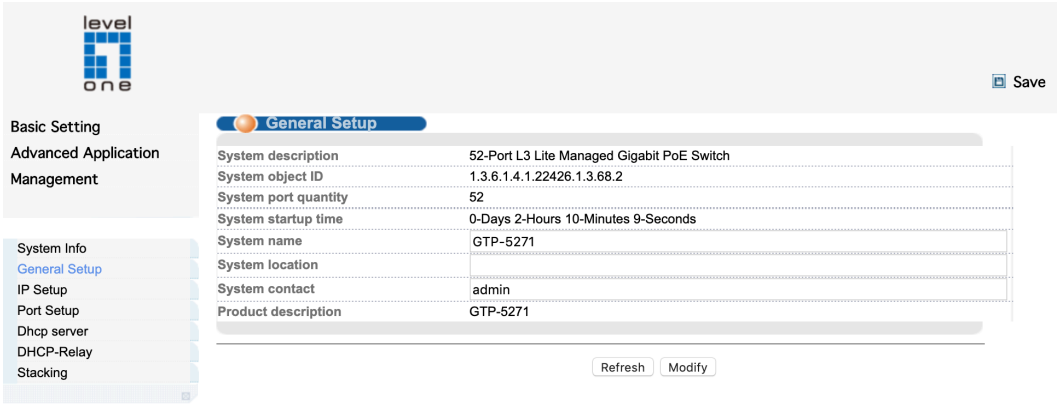
2 General Setup

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

GTP-2871 (General Setup Information)



GTP-5271 (General Setup Information)



【Parameter Description】

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

【Configuration example】

Such as: Setting System name as Switch

3 IP Setup

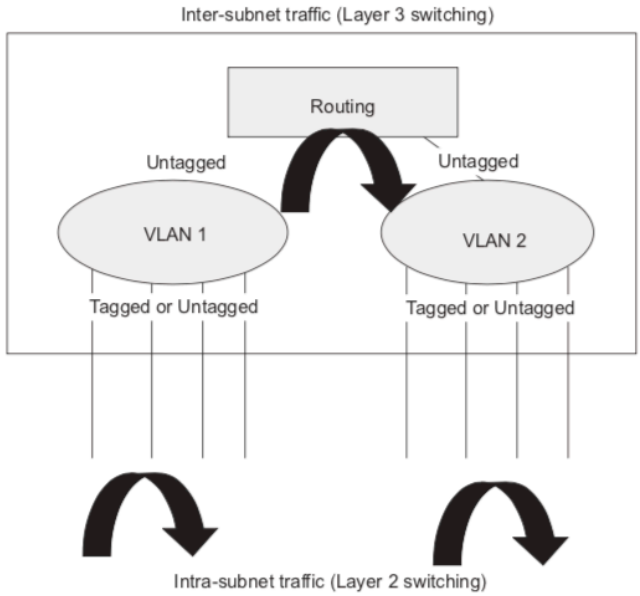
Overview

This switch supports IP routing and routing path management via static routing definitions. When IP routing is functioning, this switch acts as a wire-speed router, passing traffic between VLANs with different IP interfaces, and routing traffic to external IP networks. However, when the switch is first booted, default routing can only forward traffic between local IP interfaces. As with all traditional routers, static routing must first be configured to work.

Initial Configuration

By default, all ports belong to the same VLAN and the switch provides only Layer 2 functionality. To segment the attached network, first create VLANs for each unique user group or application traffic, assign all ports that belong to the same group to these VLANs, and then assign an IP interface to each VLAN. By separating the network into different VLANs, it can be partitioned into subnetworks that are disconnected at Layer 2. Network traffic within the same subnet is still switched using Layer 2 switching. And the VLANs can now be interconnected (as required) with Layer 3 switching.
Each VLAN represents a virtual interface to Layer 3. You just need to provide the network address for each virtual interface, and the traffic between different subnetworks will be routed by Layer 3 switching.

Figure : Virtual Interfaces and Layer 3 Routing



IP Routing and Switching

IP Switching (or packet forwarding) encompasses tasks required to forward packets for both Layer 2 and Layer 3, as well as traditional routing. These functions include:

- ◆ Layer 2 forwarding (switching) based on the Layer 2 destination MAC address
- ◆ Layer 3 forwarding (routing):
  - • Based on the Layer 3 destination address
  - • Replacing destination/source MAC addresses for each hop
  - • Incrementing the hop count
  - • Decrementing the time-to-live
  - • Verifying and recalculating the Layer 3 checksum

If the destination node is on the same subnetwork as the source network, then the packet can be transmitted directly without the help of a router. However, if the MAC address is not yet known to the switch, an Address Resolution Protocol (ARP) packet with the destination IP address is broadcast to get the destination MAC address from the destination node. The IP packet can then be sent directly with the destination MAC address.

If the destination belongs to a different subnet on this switch, the packet can be routed directly to the destination node. However, if the packet belongs to a subnet not included on this switch, then the packet should be sent to the next hop router (with the MAC address of the router itself used as the destination MAC address, and the destination IP address of the destination node). The router will then forward the packet to the destination node through the correct path. The router can also use the ARP protocol to find out the MAC address of the destination node of the next hop router as necessary.

Note: In order to perform IP switching, the switch should be recognized by other network nodes as an IP router, either by setting it as the default gateway or by redirection from another router via the ICMP process.

When the switch receives an IP packet addressed to its own MAC address, the packet follows the Layer 3 routing process. The destination IP address is checked against the Layer 3 address table. If the address is not already there, the switch broadcasts an ARP packet to all the ports on the destination VLAN to find out the destination MAC address. After the MAC address is discovered, the packet is reformatted and sent out to the destination. The reformat process includes decreasing the Time-To-Live (TTL) field of the IP header, recalculating the IP header checksum, and replacing the destination MAC address with either the MAC address of the destination node or that of the next hop router.

When another packet destined to the same node arrives, the destination MAC can be retrieved directly from the Layer 3 address table; the packet is then reformatted and sent out the destination port. IP switching can be done at wire-speed when the destination address entry is already in the Layer 3 address table.

If the switch determines that a frame must be routed, the route is calculated only during setup. Once the route has been determined, all packets in the current flow are

simply switched or forwarded across the chosen path. This takes advantage of the high throughput and low latency of switching by enabling the traffic to bypass the routing engine once the path calculation has been performed.

Routing Path Management

Routing Path Management involves the determination and updating of all the routing information required for packet forwarding, including:

- Updating the routing table
- Updating the Layer 3 switching database

Configuring Static Routes

You can enter static routes in the routing table using the IP > Static Routes (Add) page. Static routes may be required to force the use of a specific route to a subnet. Static routes do not automatically change in response to changes in network topology, so you should only configure a small number of stable routes to ensure network accessibility.

Command Usage

- If more than one static routes have the same lowest cost, the first route stored in the routing table will be used.

Parameters

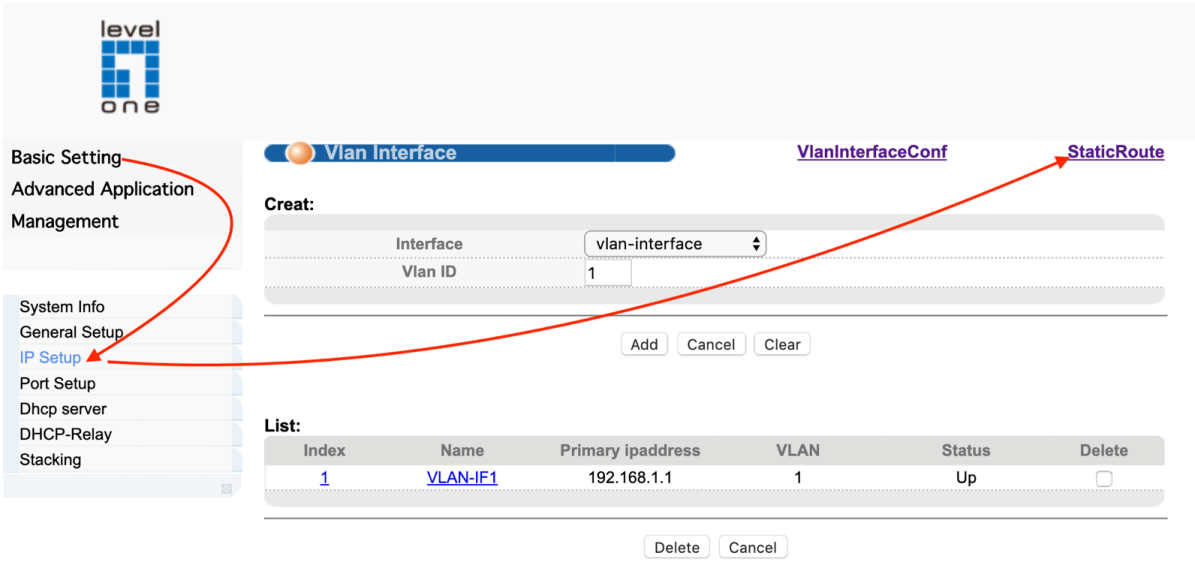
These parameters are displayed:

- **Destination IP Address** – IP address of the destination network, subnetwork, or host.
- **Net Mask** – Network mask for the associated IP subnet. This mask identifies the host address bits used for routing to specific subnets.
- **Next Hop** – IP address of the next router hop used for this route.
- **Distance** – An administrative distance indicating that this route can be overridden by other routing information. (Range: 1-255, Default: 1)

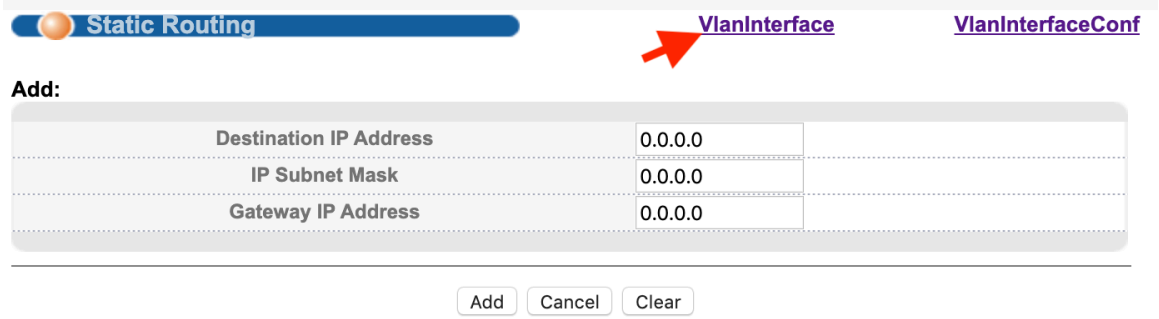
Web Interface to configure static routes

Example: Target network segment IP address and subnet mask (192.168.60.0/255.255.255.0) Next hop router interface IP address (192.168.2.2)

1. Click **Basic Setting** > **IP Setup** > **Static Route**

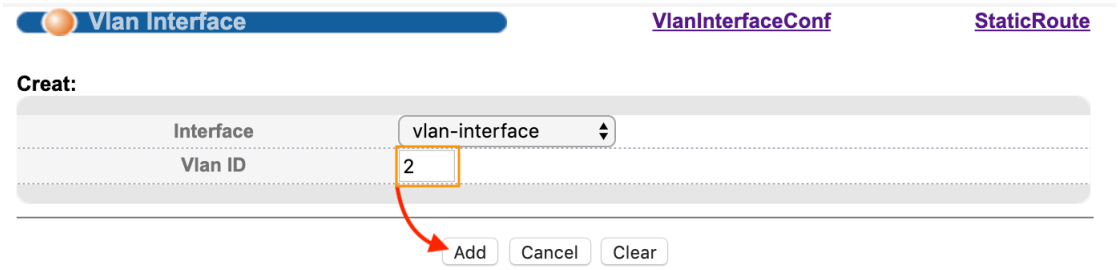


2. Click VlanInterface



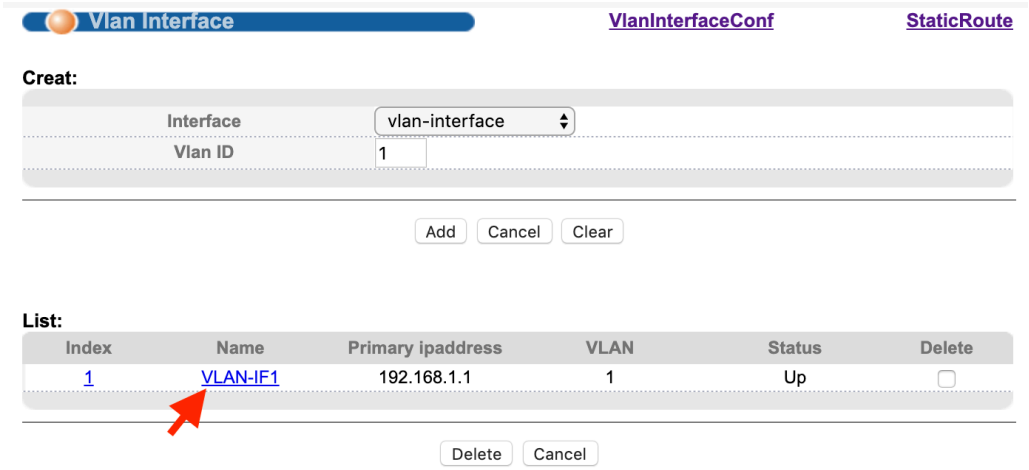
3. Enter Vlan ID: 2

Set default value the VLAN-IF1. You can create a new VLAN port, but before setting a static route, you must first create the corresponding to Advanced Application >> VLAN >> Static VLAN >> VLAN List : add 2)

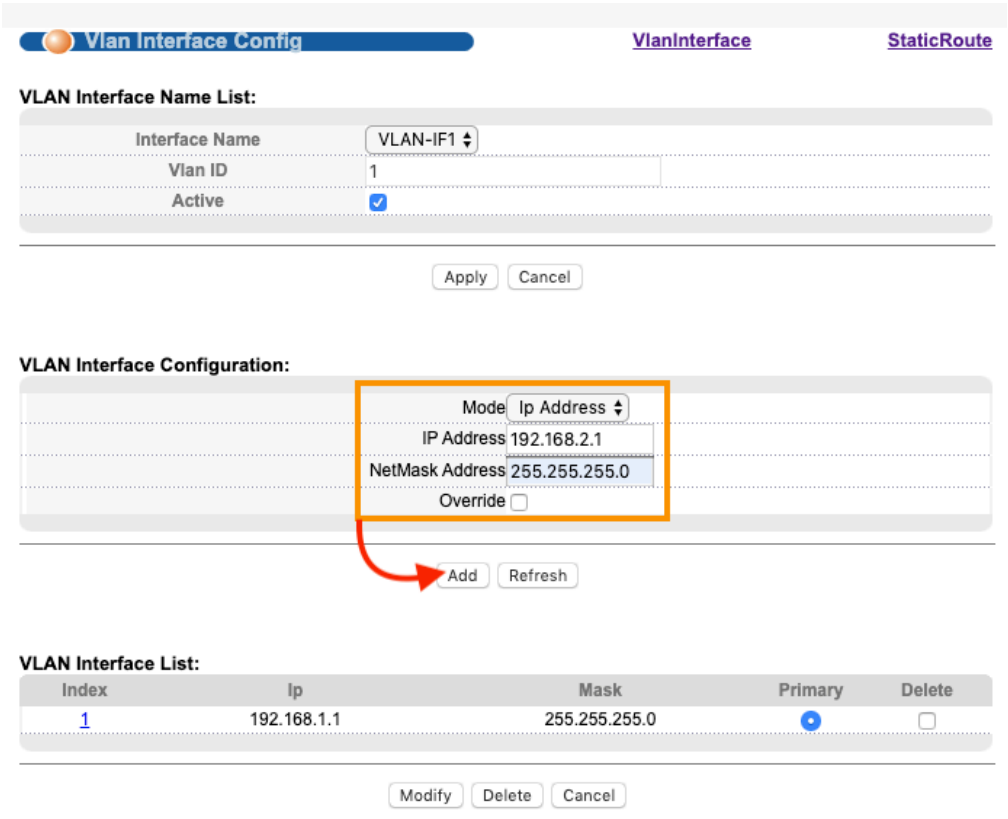


4.Configure an IP address 192.168.2.1/24 on the same network segment as the next hop address (192.168.2.2) in the corresponding VLAN interface (taking VLAN interface 1 as example)

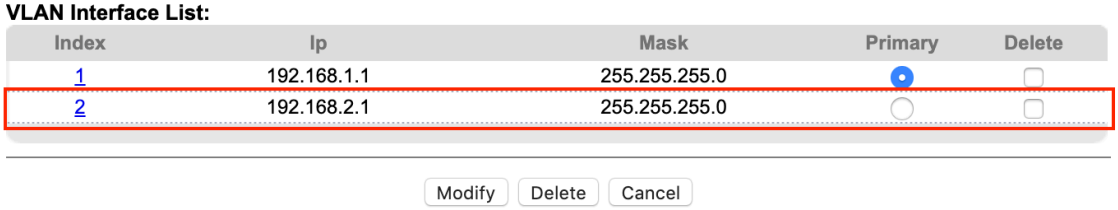
- Click **VLAN-IF1**



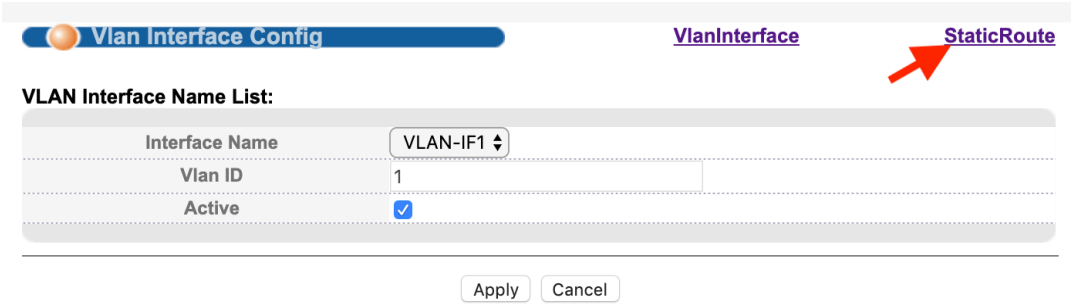
- Enter VLAN Interface Configuration: 192.168.2.1/255.255.255.0, Click Add.



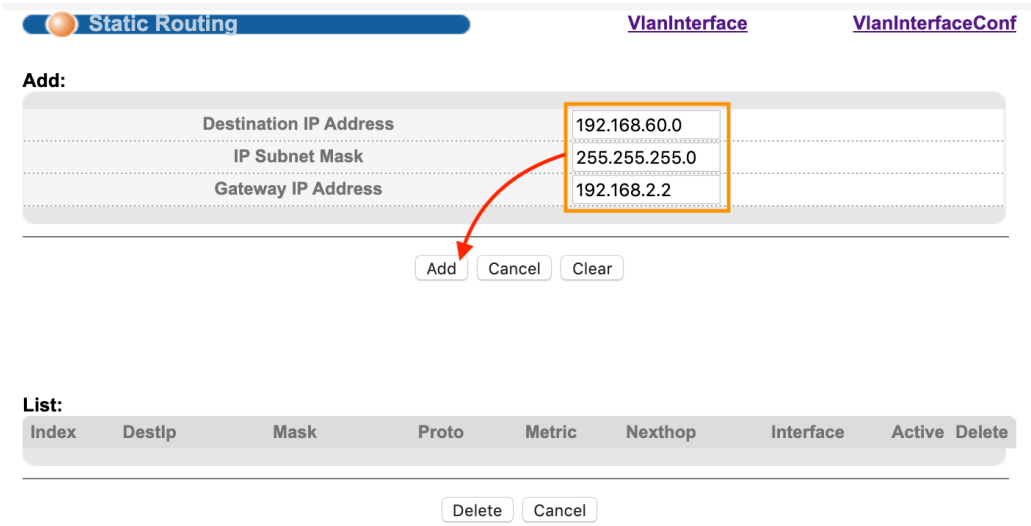
- Check the contents of the VLAN Interface List



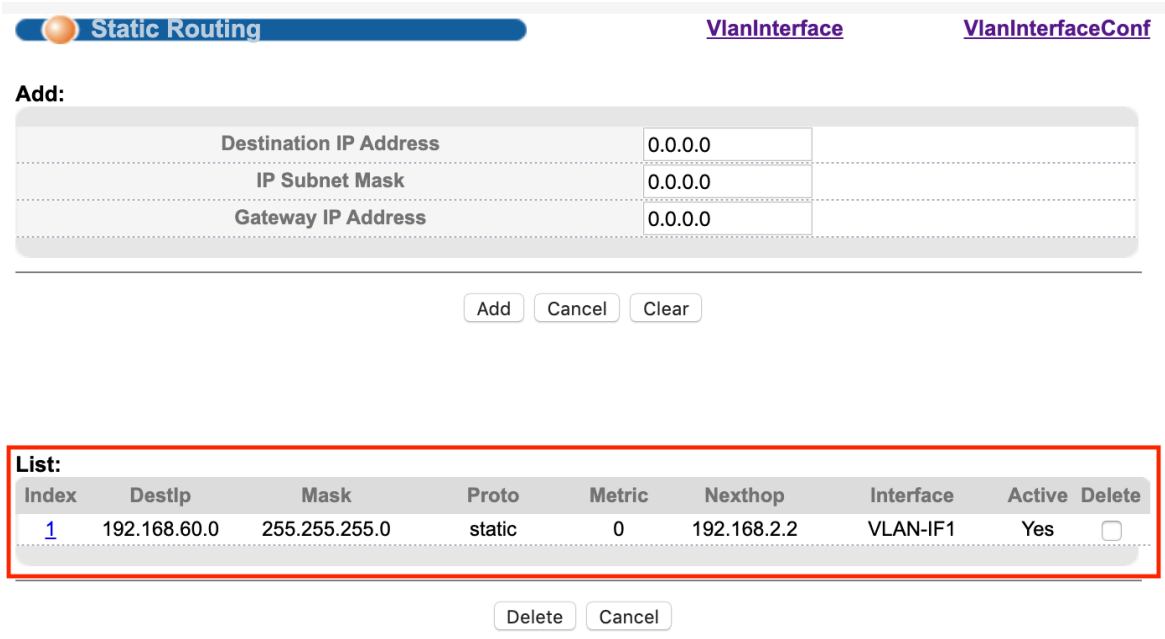
● Click **Static Route**



● Enter Destination IP Address/Mask/Gateway : 192.168.2.1 / 255.255.255.0 / 192.168.2.2 , Click Add.

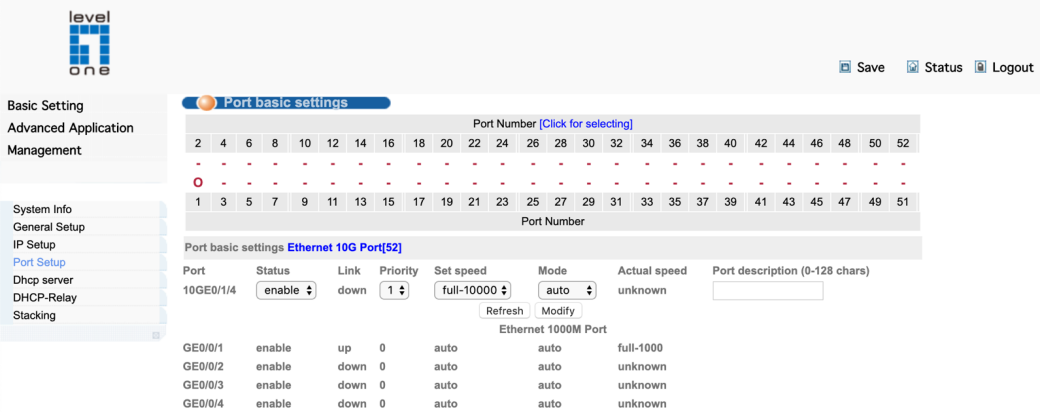


● Confirm Interface: VLAN-IF1 successfully added static route



4 Port Setup

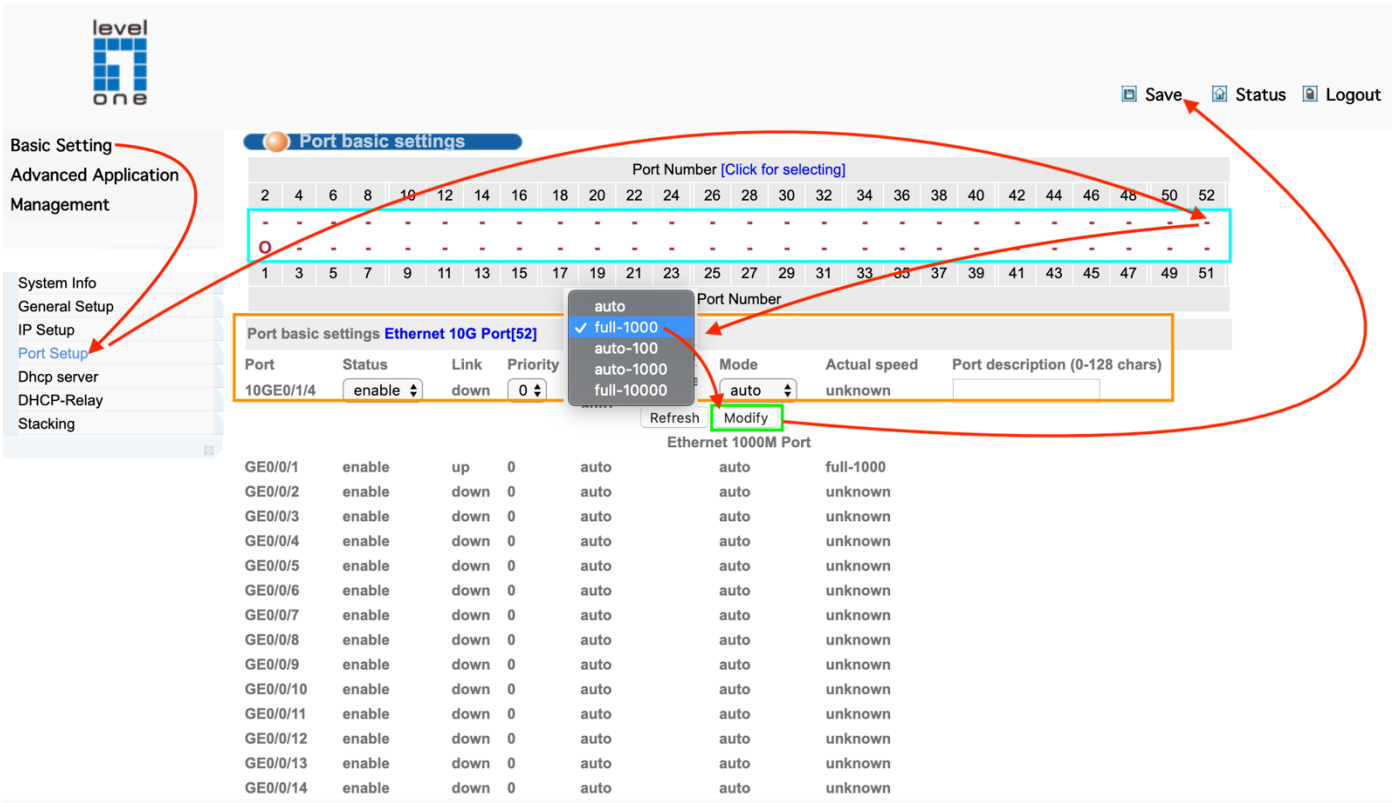
Selecting “**Basic Setting**>**Port Setup**" in the navigation bar, you can configure the related parameter of port.



【Parameter Description】

Parameter	Description
Port	Port number
status	Choose whether to close link port
link	Status: Down up
priority	Set port priority, the range of 0-7
Set speed	Choose the following modes: auto half-100 full-100 half-1000 full-1000 Port 25-28 can choose the following modes(10 Gigabit fiber equipment has this function module): Full-1000 Full-10000
Mode	Choose the following kinds: auto slave master
Actual speed	The actual speed of the port
Port description	The port is described

Figure Example: To insert 1.25Gbps Single-mode SFP Transceiver, you need to modify the input speed status of port 52 to full-1000



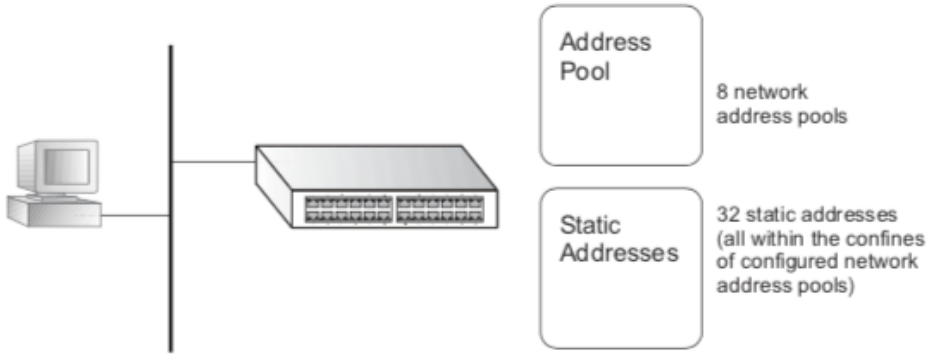
5 DHCP Server

Configuring the DHCP Server

This switch includes a Dynamic Host Configuration Protocol (DHCP) server that can assign temporary IP addresses to any attached host requesting service. It can also provide other network settings such as the domain name, default gateway, Domain Name Servers (DNS), or information on the bootup file for the host device to download.

Addresses can be assigned to clients from a common address pool configured for a specific IP interface on this switch, or fixed addresses can be assigned to hosts based on the client identifier code or MAC address.

Figure : DHCP Server



Command Usage

- First configure any excluded addresses, including the address for this switch.
- Then configure address pools for the network interfaces. You can configure up to 7 network address pools. You can also manually bind an address to a specific client if required. However, any fixed addresses must fall within the range of an existing network address pool.
- If the DHCP server is running, you must disable it and then re-enable it to implement any configuration changes. This can be done on the IP Service > DHCP > Server (Configure Global) page.

Setting Excluded Addresses

Use the DHCP Server (Configure Excluded Addresses – Add) page to specify the IP addresses that should not be assigned to clients.

Parameters

These parameters are displayed:

- Start IP Address – Specifies a single IP address or the first address in a range that the DHCP server should not assign to DHCP clients.
- End IP Address – The last address in a range that the DHCP server should not assign to DHCP clients.

 **Note:** Be sure you exclude the address for this switch and other key network devices.

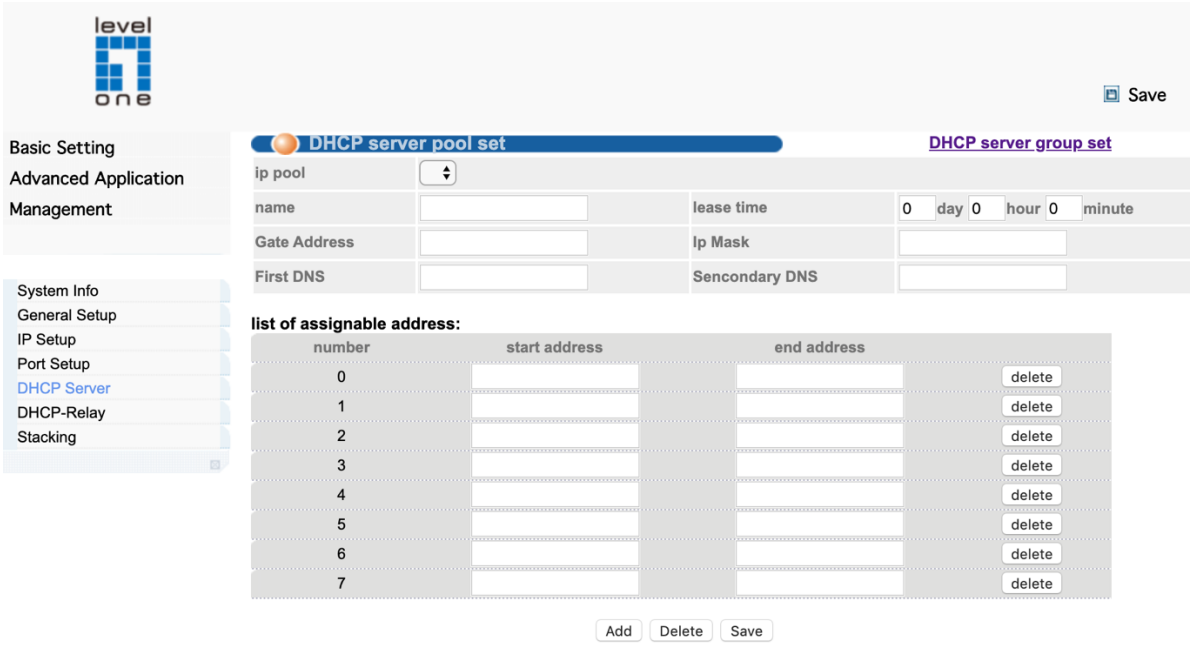
Configuring Address Pools

Use the DHCP Server page configure IP address pools for each IP interface that will provide addresses to attached clients via the DHCP server.

Command Usage

- First configure address pools for the network interfaces. Then you can manually bind an address to a specific client if required. However, note that any static host address must fall within the range of an existing network address pool.
  You can configure up to 8 network address pools, and up to 14 manually bound host address pools (i.e., two address per host pool). Just note that any address specified in a host address pool must fall within the range of a configured network address pool.
- When a client request is received, the switch first checks for a network address pool matching the gateway where the request originated (i.e., if the request was forwarded by a relay server). If there is no gateway in the client request (i.e., the request was not forwarded by a relay server), the switch searches for a network pool matching the interface through which the client request was received. It then searches for a manually configured host address that falls within the matching network pool. If no manually configured host address is found, it assigns an address from the matching network address pool. However, if no matching address pool is found the request is ignored.
- When searching for a manual binding, the switch compares the client identifier and then the hardware address for DHCP clients. Since BOOTP clients cannot transmit a client identifier, you must configure a hardware address for this host type. If no manual binding has been specified for a host entry with a hardware address or client identifier, the switch will assign an address from the first matching network pool.
- If the subnet mask is not specified for network or host address pools, the class A, B, or C natural mask is used. The DHCP server assumes that all host addresses are available.

Figure : Configuring DHCP Server Address Pools (Network)

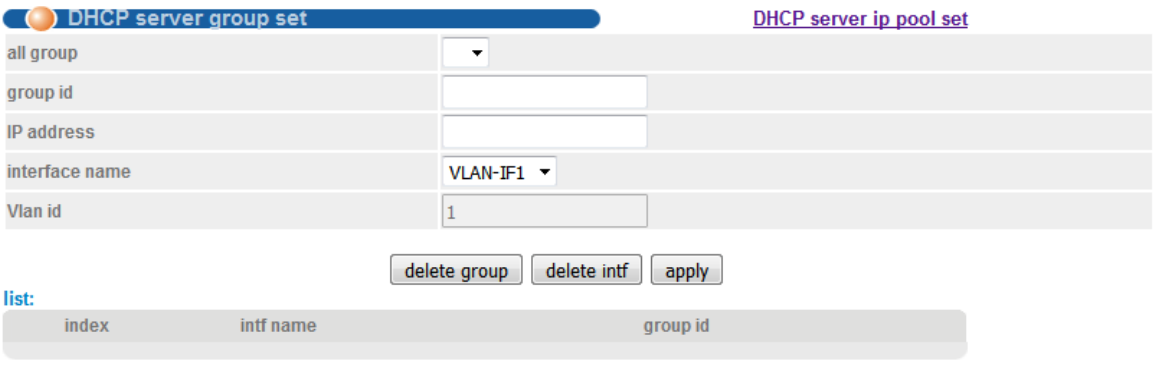


【Parameter Description】

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

DHCP Server Group Set

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



【Parameter Description】

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

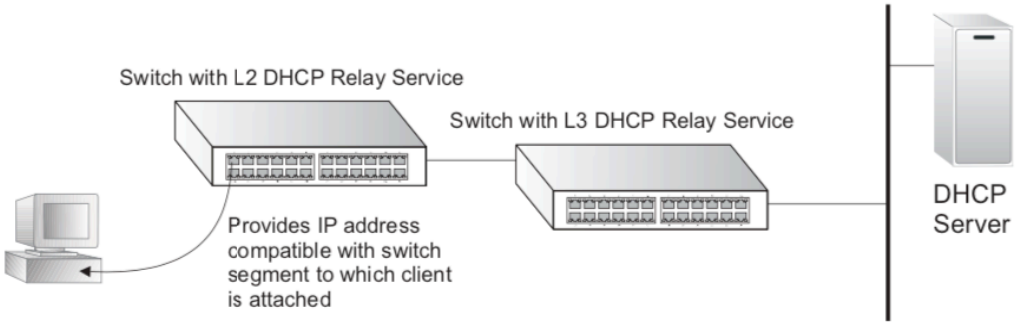
6 DHCP-Relay

Configuring DHCP L2 Relay Service

If the switch is configured to provide L2 DHCP Relay service use the second IP Service > DHCP > Relay page to configure the L2 DHCP relay service for attached host devices. To configure L2 or L3 DHCP relay service refer to the CLI Reference Guide DHCP Relay settings of the CLI Reference Guide - specifically the command: ip dhcp l2/l3 relay.

If L2 DHCP relay is enabled, and this switch sees a DHCP request broadcast, it will unicast the request towards the configured server(s). Further Option 82 RID and CID information can be configured to be included with the unicast DHCP Request packet. When Option 82 information is configured the switch's policy can be configured to drop, keep or replace and the extra sub-options sub-types can be included or excluded. When the server receives the DHCP request, it allocates a free IP address for the DHCP client from its defined scope for the DHCP client's subnet, and sends a DHCP response back to the network segment where this switch is situated. The switch will then eventually pass the DHCP response received from the server to the client.

Figure : Layer 2 DHCP Relay Service (DHCP server on a separate network segment)



Command Usage

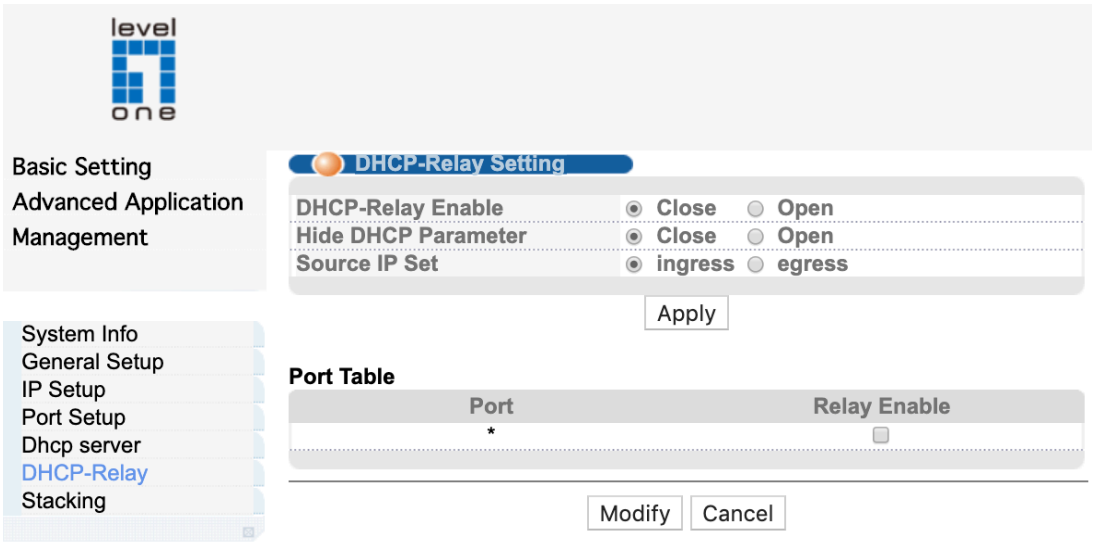
- You must specify the IP address for at least one active DHCP server.

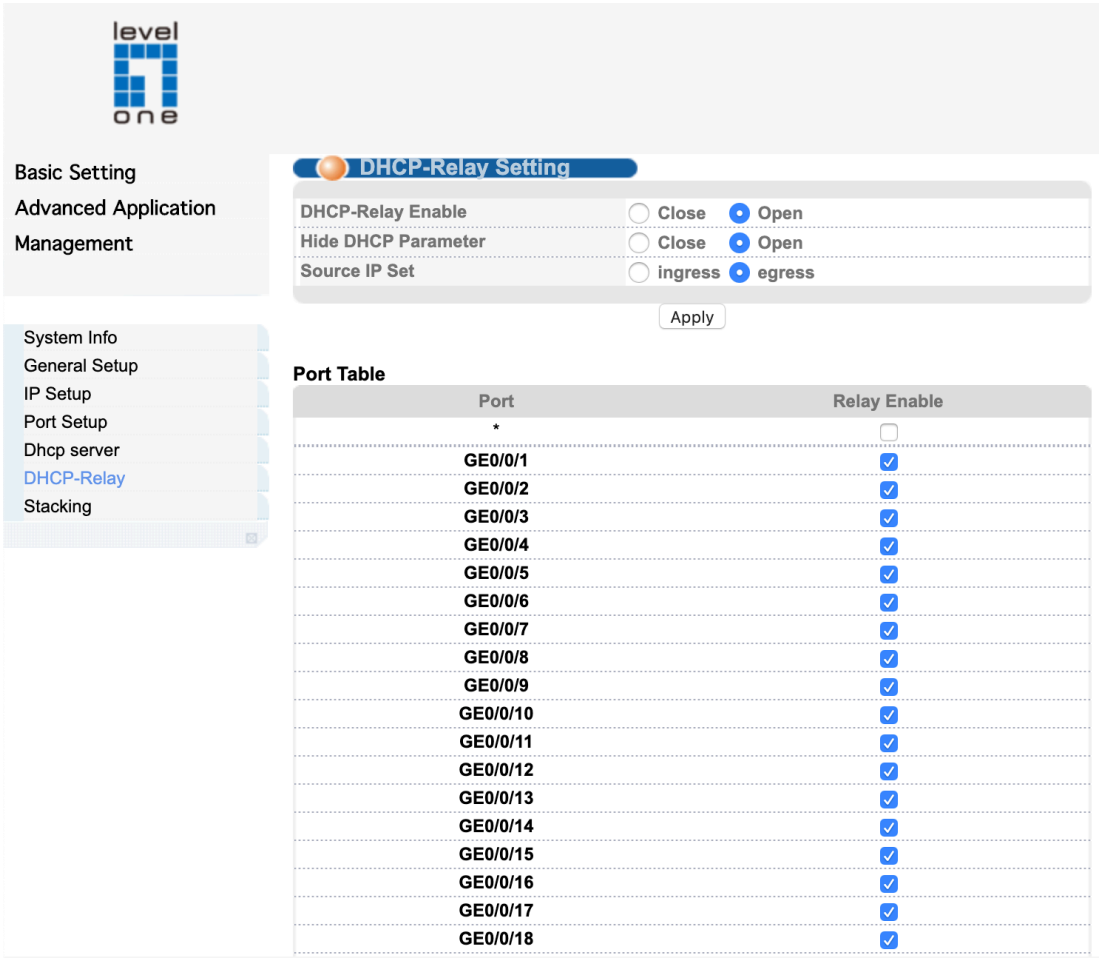
  Otherwise, the switch's DHCP relay agent will not be able to forward client requests to a DHCP server.

- You can exclude sending the extra subtypes when the Type and Length

  fields are not required to be included with the CID and RID of the option 82 information.

Selecting “**Basic Setting**>**DHCP-Relay**" in the navigation bar, you can You can turn on the DHCP relay function, Hidden DHCP Server. Set the source IP used.



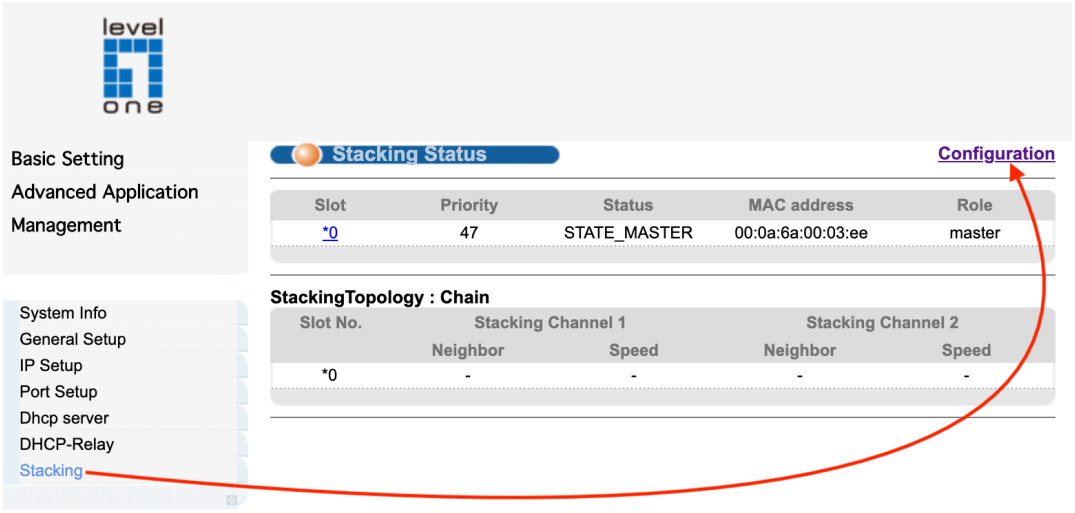


7 Stacking (Virtual Stacking)

Before configuring the stack, we highly recommend you to prepare the configuration planning with a clear set of the role and function of each member device. Some configuration needs device reboot to take effect, so you are kindly recommended to configure the stack at first, next connect the devices physically after powering off them, then you can power them on and the devices will join the stack automatically. After stack is established, users can log in the stack system through any member devices to configure and manage it.

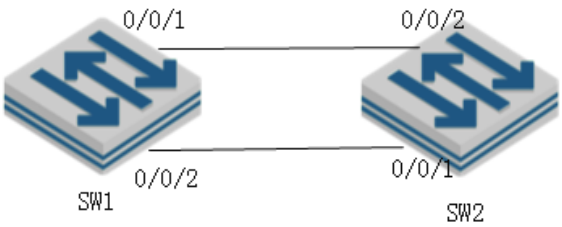
Note: Virtual stacking supports up to 4 switches in a single logical stack for unified management, monitoring and configuration, Only the same model can use Virtual stacking(ex: GTP-2871 to GTP-2871 Or GTP-5271 to GTP-5271)

Selecting “Basic Setting>IP Setup>Stacking Status" in the navigation bar, you can view the stack interface information, neighbor interface information.



【Configuration example】

As shown in the figure, configure SW1 as Master and SW2 as Slave.



SW1

1.Enable Stack function.

2.Configure device-id as 0.

3.Configure left port of SW1.

4.Configure System priority as 200.

SW2:

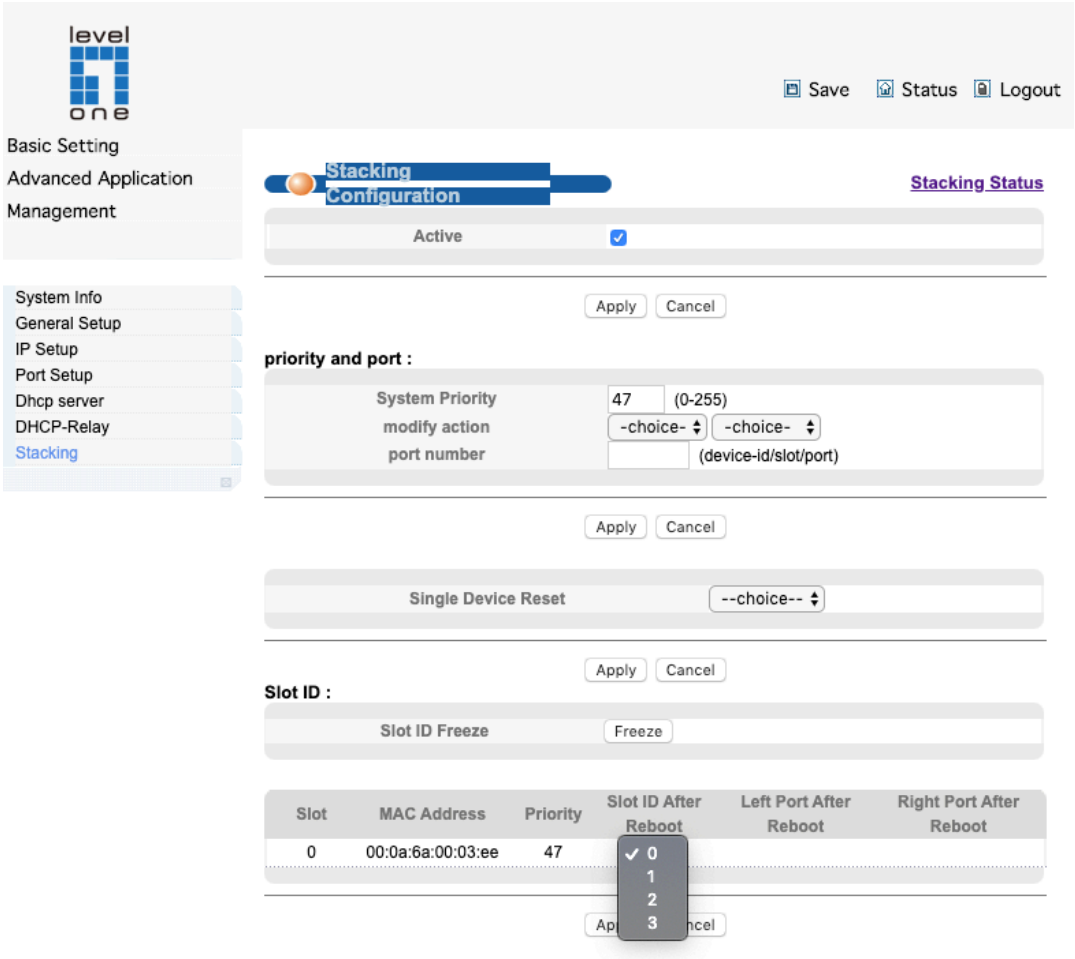
1.Enable Stack function.

2.Configure device-id as 0.

3.Configure left port of SW2.

4.Configure System priority as 100.

After restarting the two devices, connect two devices according to Figure.



【Parameter Description】

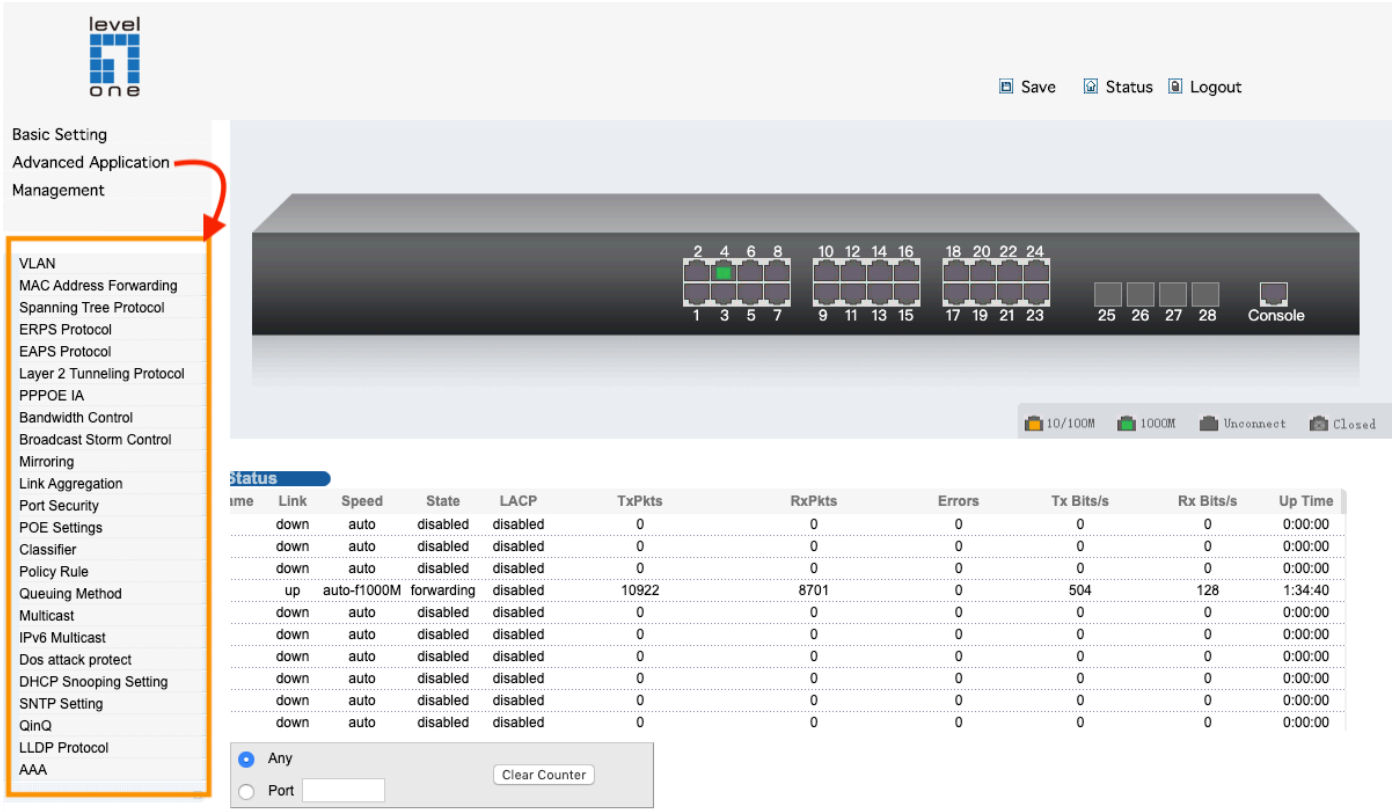
Parameter	Description
Active	Select open or close stack
System Priority	Set system priority, the default is 0
Slot id Freeze	Freeze slot ID
Slot id After Reboot	Device number after the device is rebooted

Note: Some related configuration, only to restart equipment ,can take effect;

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

Section II

Advanced Application



1. VLAN Configuration

IEEE 802.1Q VLANs

In large networks, routers are used to isolate broadcast traffic for each subnet into separate domains. This switch provides a similar service at Layer 2 by using VLANs to organize any group of network nodes into separate broadcast domains. VLANs confine broadcast traffic to the originating group, and can eliminate broadcast storms in large networks. This also provides a more secure and cleaner network environment.

An IEEE 802.1Q VLAN is a group of ports that can be located anywhere in the network, but communicate as though they belong to the same physical segment.

VLANs help to simplify network management by allowing you to move devices to a new VLAN without having to change any physical connections. VLANs can be easily organized to reflect departmental groups (such as Marketing or R&D), usagegroups (such as e-mail), or multicast groups (used for multimedia applications such as video conferencing).

If a packet matches the rules defined by more than one of these functions, only one of them is applied, with the precedence being MAC-based, IP subnet-based, protocol-based, and then native port-based.
groups (such as e-mail), or multicast groups (used for multimedia applications such as video conferencing).
VLANs provide greater network efficiency by reducing broadcast traffic, and allow you to make network changes without having to update IP addresses or IP subnets. VLANs inherently provide a high level of network security since traffic must pass through a configured Layer 3 link to reach a different VLAN.

This switch supports the following VLAN features:

- Up to 4094 VLANs based on the IEEE 802.1Q standard
- Distributed VLAN learning across multiple switches using explicit or implicit tagging and GVRP protocol
- Port overlapping, allowing a port to participate in multiple VLANs
- End stations can belong to multiple VLANs
- Passing traffic between VLAN-aware and VLAN-unaware devices

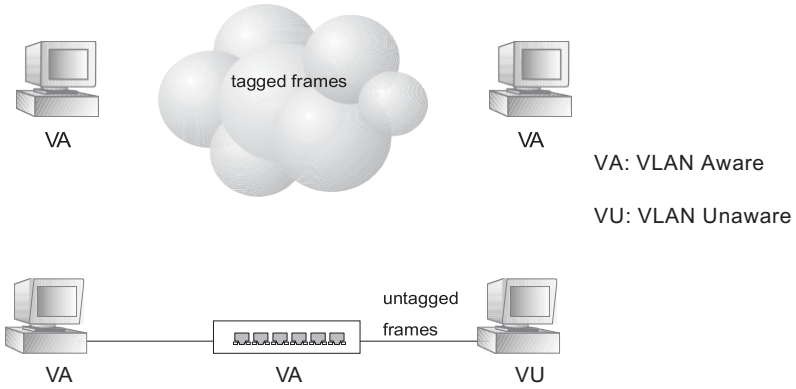
◆ Priority tagging

Assigning Ports to VLANs

Before enabling VLANs for the switch, you must first assign each port to the VLAN group(s) in which it will participate. By default all ports are assigned to VLAN 1 as untagged ports. Add a port as a tagged port if you want it to carry traffic for one or more VLANs, and any intermediate network devices or the host at the other end of the connection supports VLANs. Then assign ports on the other VLAN-aware network devices along the path that will carry this traffic to the same VLAN(s), either manually or dynamically using GVRP. However, if you want a port on this switch to participate in one or more VLANs, but none of the intermediate network devices nor the host at the other end of the connection supports VLANs, then you should add this port to the VLAN as an untagged port.

Note: VLAN-tagged frames can pass through VLAN-aware or VLAN-unaware network interconnection devices, but the VLAN tags should be stripped off before passing it on to any end-node host that does not support VLAN tagging.

VLAN Compliant and VLAN Non-compliant Devices



VLAN Classification – When the switch receives a frame, it classifies the frame in one of two ways. If the frame is untagged, the switch assigns the frame to an associated VLAN (based on the default VLAN ID of the receiving port). But if the frame is tagged, the switch uses the tagged VLAN ID to identify the port broadcast domain of the frame.

Port Overlapping – Port overlapping can be used to allow access to commonly shared network resources among different VLAN groups, such as file servers or printers. Note that if you implement VLANs which do not overlap, but still need to communicate, you can connect them by enabled routing on this switch.

Untagged VLANs – Untagged VLANs are typically used to reduce broadcast traffic and to increase security. A group of network users assigned to a VLAN form a broadcast domain that is separate from other VLANs configured on the switch.

Packets are forwarded only between ports that are designated for the same VLAN. Untagged VLANs can be used to manually isolate user groups or subnets. However, you should use IEEE 802.3 tagged VLANs with GVRP whenever possible to fully automate VLAN registration.

Automatic VLAN Registration – GVRP (GARP VLAN Registration Protocol) defines a system whereby the switch can automatically learn the VLANs to which each end station should be assigned. If an end station (or its network adapter) supports the IEEE 802.1Q VLAN protocol, it can be configured to broadcast a message to your network indicating the VLAN groups it wants to join. When this switch receives these messages, it will automatically place the receiving port in the specified VLANs, and then forward the message to all other ports. When the message arrives at another switch that supports GVRP, it will also place the receiving port in the specified VLANs, and pass the message on to all other ports. VLAN requirements are propagated in this way throughout the network. This allows GVRP-compliant devices to be automatically configured for VLAN groups based solely on end station requests.

disable GVRP on the boundary ports to prevent advertisements from being propagated, or forbid those ports from joining restricted VLANs.

Note: If you have host devices that do not support GVRP, you should configure static or untagged VLANs for the switch ports connected to these devices. But you can still enable GVRP on these edge switches, as well as on the core switches in the network.

Forwarding Tagged/Untagged Frames

If you want to create a small port-based VLAN for devices attached directly to a single switch, you can assign ports to the same untagged VLAN. However, to participate in a VLAN group that crosses several switches, you should create a VLAN for that group and enable tagging on all ports.

Ports can be assigned to multiple tagged or untagged VLANs. Each port on the switch is therefore capable of passing tagged or untagged frames. When forwarding a frame from this switch along a path that contains any VLAN-aware devices, the switch should include VLAN tags. When forwarding a frame from this switch along a path that does not contain any VLAN-aware devices (including the destination host), the switch must first strip off the VLAN tag before forwarding the frame. When the switch receives a tagged frame, it will pass this frame onto the VLAN(s) indicated by the frame tag. However, when this switch receives an untagged frame from a VLAN-unaware device, it first decides where to forward the frame, and then inserts a VLAN tag reflecting the ingress port's default VID.

Configuring VLAN Groups

Use the VLAN > Static (Add) page to create or remove VLAN groups, set administrative status, or specify Remote VLAN type. To propagate information about

VLAN groups used on this switch to external network devices, you must specify a VLAN ID for each of these groups.

Parameters

These parameters are displayed:

Add

- **VLAN ID** – ID of VLAN or range of VLANs (1-4094).
  VLAN 1 is the default untagged VLAN.
  VLAN 4093 is dedicated for Switch Clustering. Configuring this VLAN for other purposes may cause problems in the Clustering operation.

- **Status** – Enables or disables the specified VLAN.

- **Remote VLAN** – Reserves this VLAN for RSPAN

Modify

- **VLAN ID** – ID of configured VLAN (1-4094).

- **VLAN Name** – Name of the VLAN (1 to 32 characters).

- **Status** – Enables or disables the specified VLAN.

- **L3 Interface** – Sets the interface to support Layer 3 configuration, and reserves memory space required to maintain additional information about this interface type. This parameter must be enabled before you can assign an IP address to a VLAN.

Show

- **VLAN ID** – ID of configured VLAN.

- **VLAN Name** – Name of the VLAN.

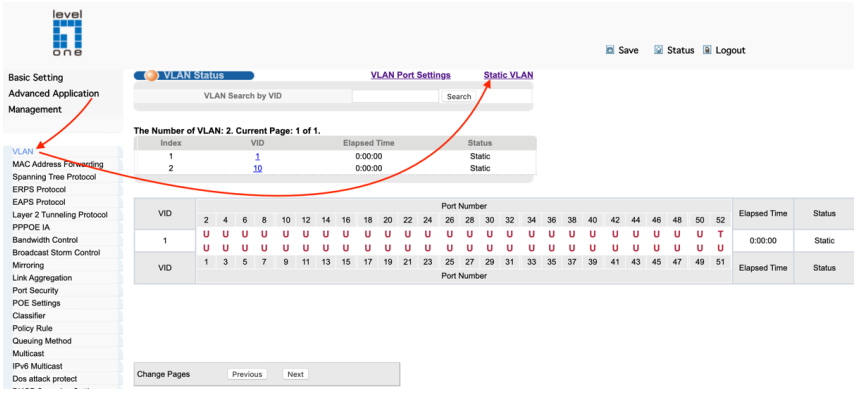
- **Status** – Operational status of configured VLAN.

- **Remote VLAN** – Shows if RSPAN is enabled on this VLAN.

- **L3 Interface** – Shows if the interface supports Layer 3 configuration.

Status VLAN

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

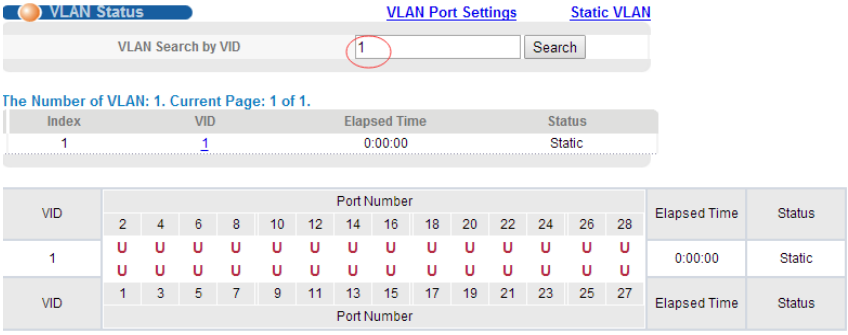


【Parameter Description】

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

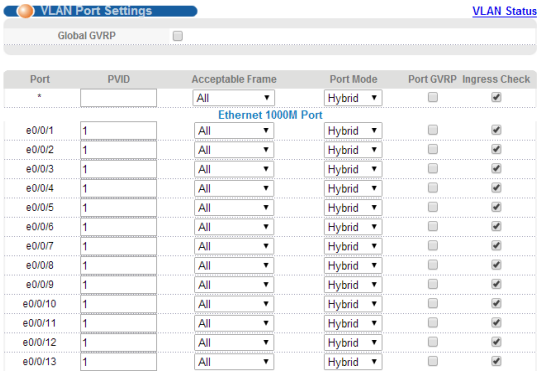
【Configuration example】

Such as: View the VLAN of VID as “1".



VLAN Port Settings

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



Parameter	Description
PVID	The PVID of the port can be modified, the default port PVID is "1"
Acceptable Frame	Choose the following kinds: All Tagged only Untagged only
Port Mode	Choose the following modes: Hybrid: The port can be either a tag member or untag member in a VLAN and can be a member port for multiple vlans. Trunk: The port can only be an tag member in a VLAN and can be a member port for multiple vlans Access: The port can only be a member of untag in VLAN and the port can only be in a VLAN.
Port GVRP	Select open or close GVRP, dynamic VLAN learning function, port mode must be Trunk mode. ● Using GVRP Forwarding Tagged/Untagged Frames If you want to create a small port-based VLAN for devices attached directly to a single switch, you can assign ports to the same untagged VLAN. However, to participate in a VLAN group that crosses several switches, you should create a VLAN for that group and enable tagging on all ports. Ports can be assigned to multiple tagged or untagged VLANs. Each port on the switch is therefore capable of passing tagged or untagged frames. When forwarding a frame from this switch along a path that contains any VLAN-aware devices, the switch should include VLAN tags. When forwarding a frame from this switch along a path that does not contain any VLAN-aware devices (including the destination host), the switch must first strip off the VLAN tag before forwarding the frame. When the switch receives a tagged frame, it will pass this frame onto the VLAN(s) indicated by the frame tag. However, when this switch receives an untagged frame from a VLAN-unaware device, it first decides where to forward the frame, and then inserts a VLAN tag reflecting the ingress port’s default VID.
Ingress Check	Open port filtering function. If the port settings only receive the Tagged type of message, if the Ingress Check function is opened, the Untagged type of message will be discarded when the port receives the message of the untagged type of message, otherwise it can be forwarded. The default port filtering function opens.

【Instructions】

Hybrid port to packet:

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

Hybrid port to send packet:

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

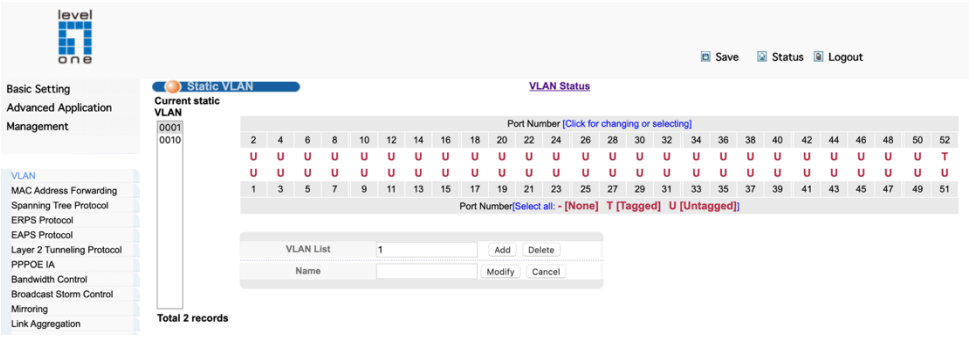
2. If it is untag stripping VLAN information, send again, if the tag is sent directly.

【Configuration example】

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

Static VLAN

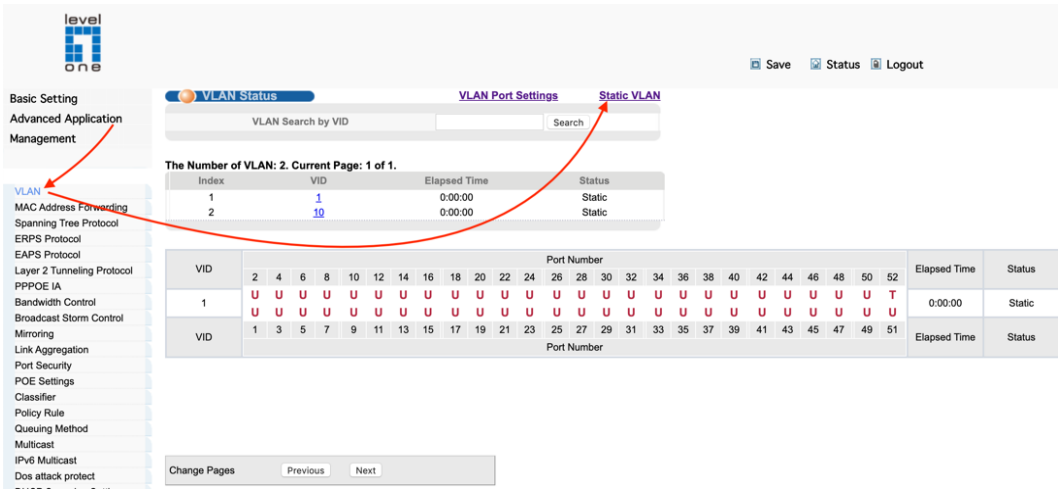
Selecting “**Advanced Application**>**Static VLAN**" in the navigation bar, you can configure Static VLAN.

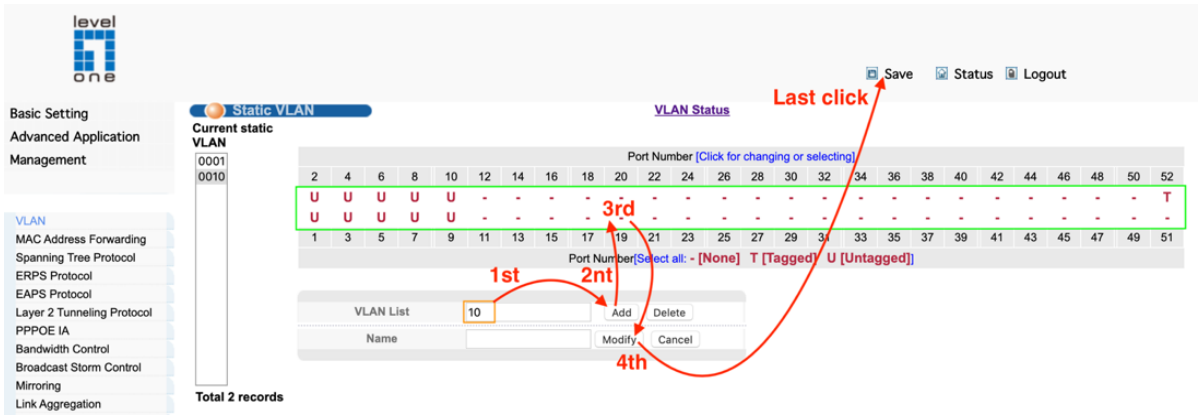


【Configuration example】

Add and delete VLAN members

Such as: Adding a new VLAN, VLAN Group ID 10 contains non-untag member port 1 to 10 . Tag member port 52(“Connection between switch and switch” on 52 port.). The user can modify the port member by clicking on the white area below the port number.




Save
Status
Logout
Basic Setting
Advanced Application
Management
VLAN
MAC Address Forwarding
Spanning Tree Protocol
ERPS Protocol
EAPS Protocol
Layer 2 Tunneling Protocol
PPPOE IA
Bandwidth Control
Broadcast Storm Control
Mirroring
Link Aggregation
Static VLAN
VLAN Status
Current static VLAN
0001
0010
Total 2 records
Port Number [Click for changing or selecting]
Port Number[Select all: - [None] T [Tagged] U [Untagged]]
VLAN List
10
Add
Delete
Name
Modify
Cancel
1st
2nt
3rd
4th
Last click

2. MAC Address Forwarding

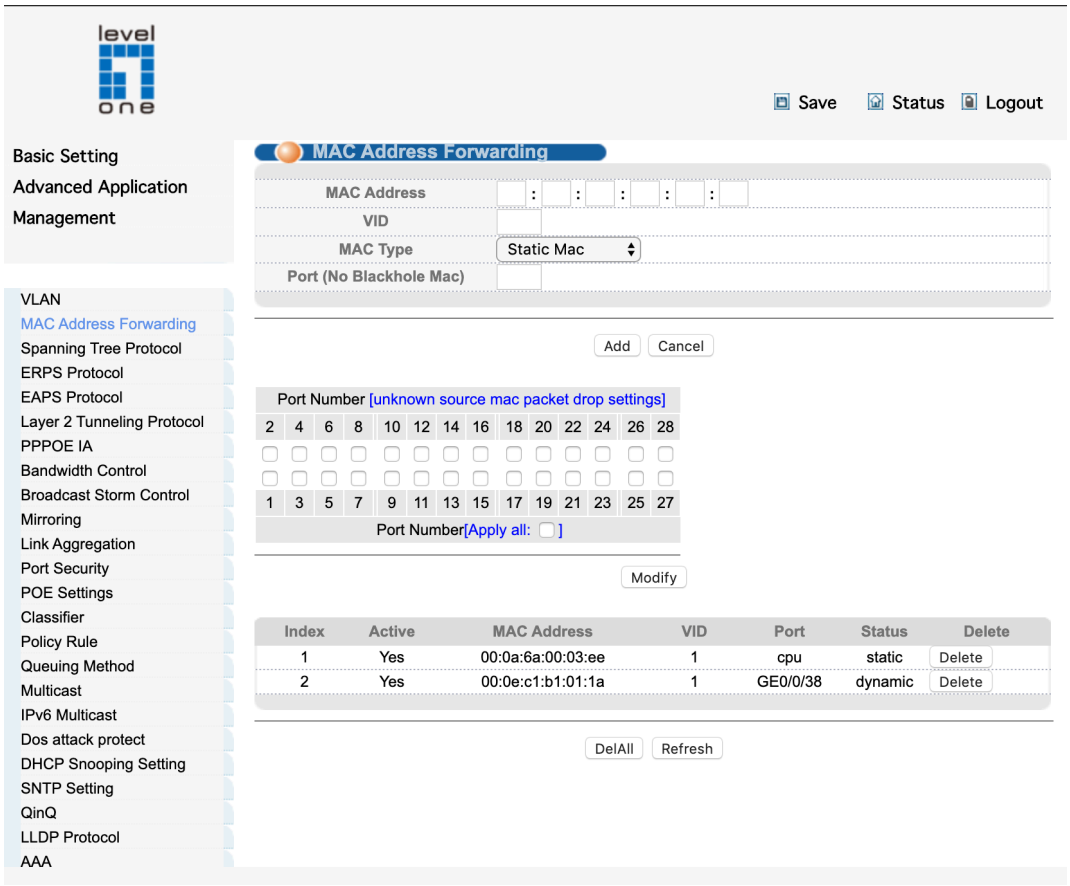
MAC-Based page to configure VLAN based on MAC addresses. The MAC-based VLAN feature assigns VLAN IDs to ingress untagged frames according to source MAC addresses.

When MAC-based VLAN classification is enabled, untagged frames received by a port are assigned to the VLAN which is mapped to the frame's source MAC address. When no MAC address is matched, untagged frames are assigned to the receiving port's native VLAN ID (PVID).

Command Usage

- The MAC-to-VLAN mapping applies to all ports on the switch.
- Source MAC addresses can be mapped to only one VLAN ID.
- Configured MAC addresses cannot be broadcast or multicast addresses.

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



【Parameter Description】

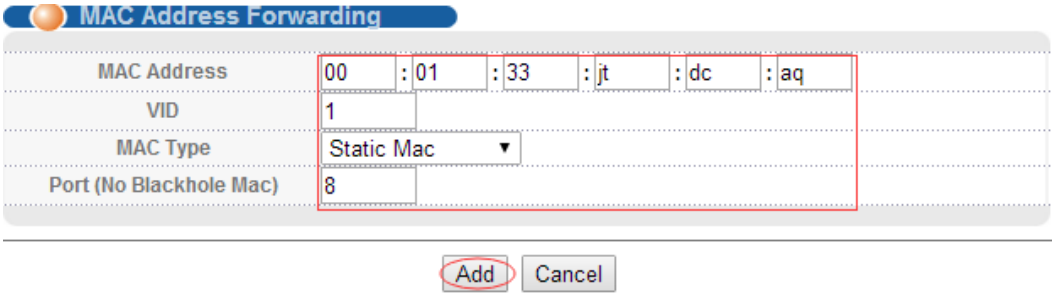
Parameter	Description
MAC Type	MAC Type: Static MAC Dynamic MAC Blackhole MAC Permanent MAC

【Instructions】

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

【Configuration example】

1. MAC Address Forwarding



2. Unknown source mac packet drop settings.

3. Spanning Tree Protocol

This chapter describes the following basic topics:

- Loopback Detection – Configures detection and response to loopback BPDUs.
- Global Settings for STA – Configures global bridge settings for STP, RSTP and MSTP.
- Interface Settings for STA – Configures interface settings for STA, including priority, path cost, link type, and designation as an edge port.
- Global Settings for MSTP – Sets the VLANs and associated priority assigned to an MST instance
- Interface Settings for MSTP – Configures interface settings for MSTP, including priority and path cost.

Overview

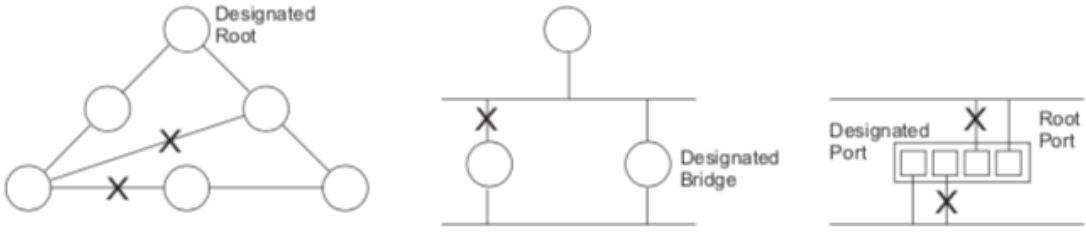
The Spanning Tree Algorithm (STA) can be used to detect and disable network loops, and to provide backup links between switches, bridges or routers. This allows the switch to interact with other bridging devices (that is, an STA-compliant switch, bridge or router) in your network to ensure that only one route exists between any two stations on the network, and provide backup links which automatically take over when a primary link goes down.

The spanning tree algorithms supported by this switch include these versions:

- STP – Spanning Tree Protocol (IEEE 802.1D)
- RSTP – Rapid Spanning Tree Protocol (IEEE 802.1w)
- MSTP – Multiple Spanning Tree Protocol (IEEE 802.1s)

STP – STP uses a distributed algorithm to select a bridging device (STP-compliant switch, bridge or router) that serves as the root of the spanning tree network. It selects a root port on each bridging device (except for the root device) which incurs the lowest path cost when forwarding a packet from that device to the root device. Then it selects a designated bridging device from each LAN which incurs the lowest path cost when forwarding a packet from that LAN to the root device. All ports connected to designated bridging devices are assigned as designated ports. After determining the lowest cost spanning tree, it enables all root ports and designated ports, and disables all other ports. Network packets are therefore only forwarded between root ports and designated ports, eliminating any possible network loops.

Figure : STP Root Ports and Designated Ports

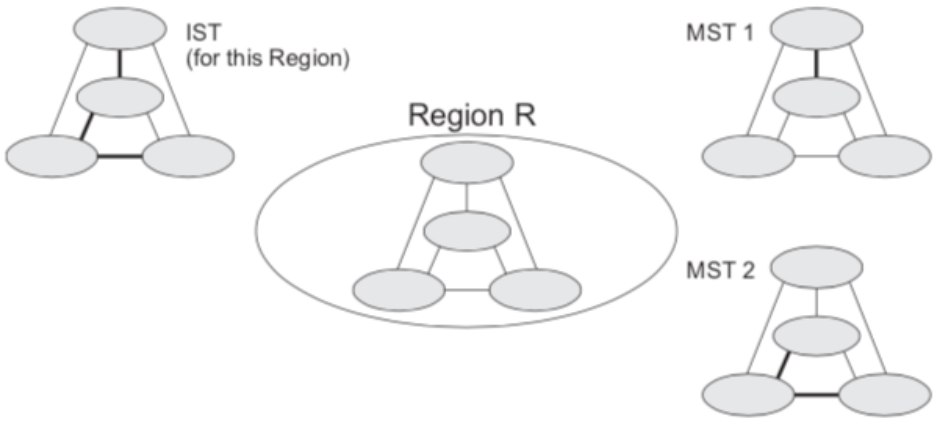


Once a stable network topology has been established, all bridges listen for Hello BPDUs (Bridge Protocol Data Units) transmitted from the Root Bridge. If a bridge does not get a Hello BPDU after a predefined interval (Maximum Age), the bridge assumes that the link to the Root Bridge is down. This bridge will then initiate negotiations with other bridges to reconfigure the network to reestablish a valid network topology.

RSTP – RSTP is designed as a general replacement for the slower, legacy STP. RSTP is also incorporated into MSTP. RSTP achieves much faster reconfiguration (i.e., around 1 to 3 seconds, compared to 30 seconds or more for STP) by reducing the number of state changes before active ports start learning, predefining an alternate route that can be used when a node or port fails, and retaining the forwarding database for ports insensitive to changes in the tree structure when reconfiguration occurs.

MSTP – When using STP or RSTP, it may be difficult to maintain a stable path between all VLAN members. Frequent changes in the tree structure can easily isolate some of the group members. MSTP (which is based on RSTP for fast convergence) is designed to support independent spanning trees based on VLAN groups. Using multiple spanning trees can provide multiple forwarding paths and enable load balancing. One or more VLANs can be grouped into a Multiple Spanning Tree Instance (MSTI). MSTP builds a separate Multiple Spanning Tree (MST) for each instance to maintain connectivity among each of the assigned VLAN groups. MSTP then builds a Internal Spanning Tree (IST) for the Region containing all commonly configured MSTP bridges.

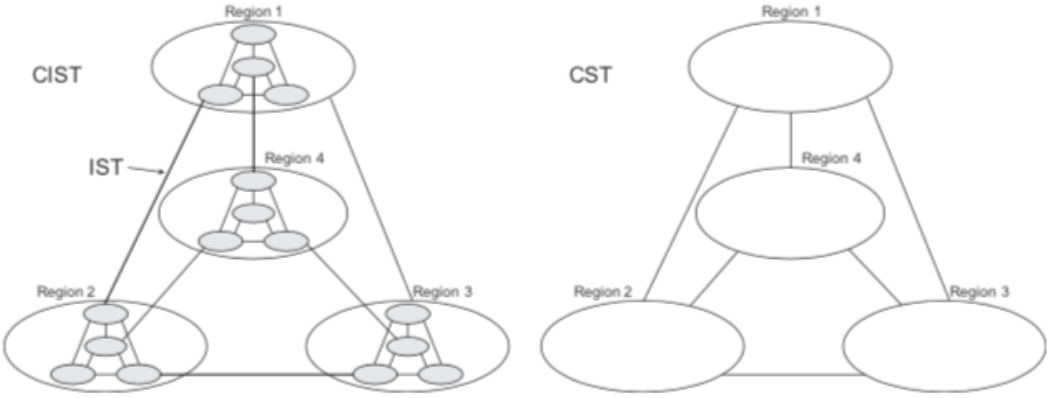
Figure : MSTP Region, Internal Spanning Tree, Multiple Spanning Tree



An MST Region consists of a group of interconnected bridges that have the same MST Configuration Identifiers. An MST Region may contain multiple MSTP Instances. An

Internal Spanning Tree (IST) is used to connect all the MSTP switches within an MST region. A Common Spanning Tree (CST) interconnects all adjacent MST Regions, and acts as a virtual bridge node for communications with STP or RSTP nodes in the global network.

Figure : Spanning Tree – Common Internal, Common, Internal



MSTP connects all bridges and LAN segments with a single Common and Internal Spanning Tree (CIST). The CIST is formed as a result of the running spanning tree algorithm between switches that support the STP, RSTP, MSTP protocols.

Once you specify the VLANs to include in a Multiple Spanning Tree Instance (MSTI), the protocol will automatically build an MSTI tree to maintain connectivity among each of the VLANs. MSTP maintains contact with the global network because each instance is treated as an RSTP node in the Common Spanning Tree (CST).

Configuring Loopback Detection

Use the Spanning Tree > Loopback Detection page to configure loopback detection on an interface. When loopback detection is enabled and a port or trunk receives it's own BPDU, the detection agent drops the loopback BPDU, sends an SNMP trap, and places the interface in discarding mode. This loopback state can be released manually or automatically. If the interface is configured for automatic loopback release, then the port will only be returned to the forwarding state if one of the following conditions is satisfied:

- The interface receives any other BPDU except for it's own, or;
- The interfaces's link status changes to link down and then link up again, or;
- The interface ceases to receive it's own BPDUs in a forward delay interval.

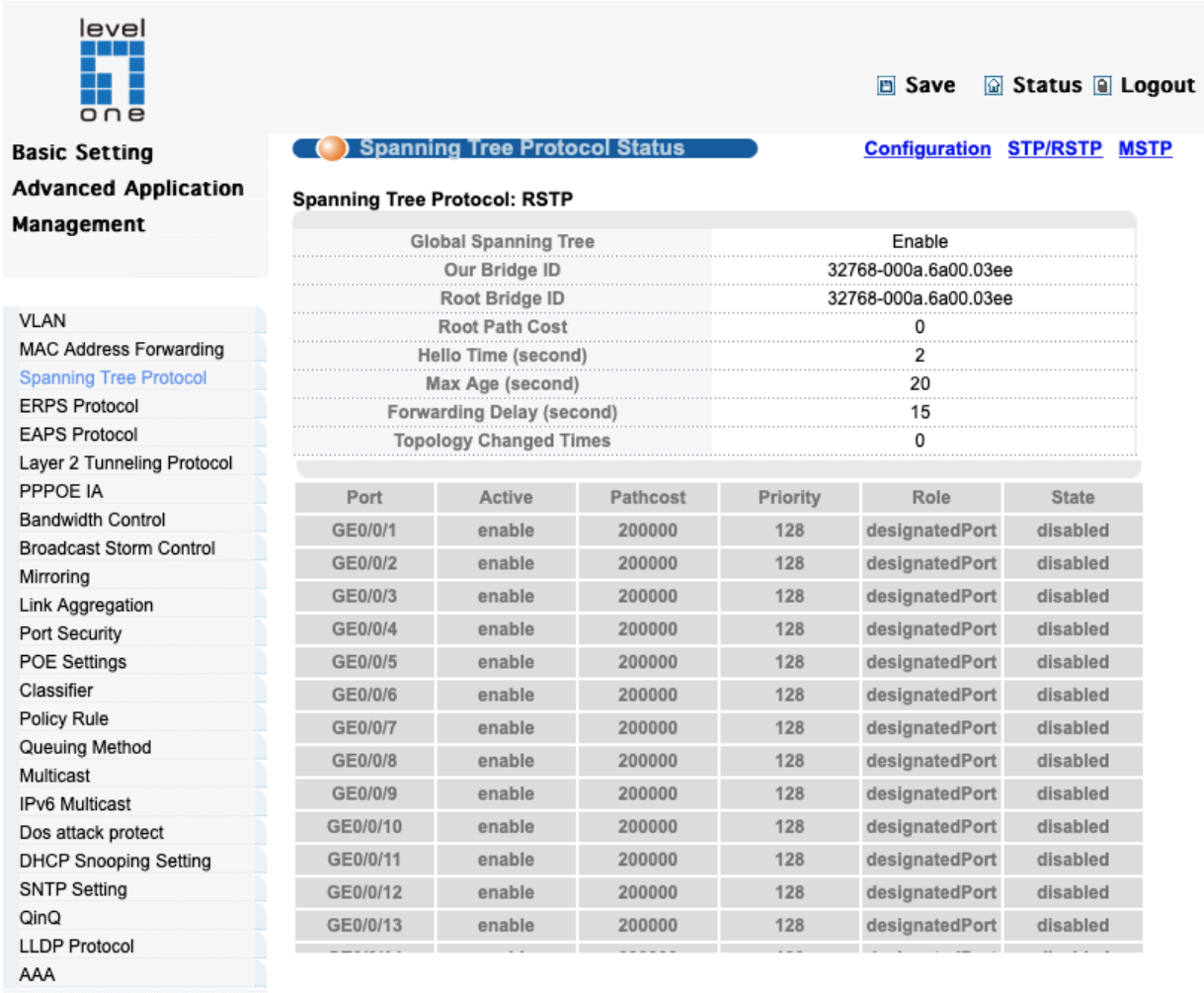
Note: If loopback detection is not enabled and an interface receives it's own BPDU, then the interface will drop the loopback BPDU according to IEEE Standard 802.1w- 2001 9.3.4 (Note 1).

Note: Loopback detection will not be active if Spanning Tree is disabled on the switch.

Note: When configured for manual release mode, then a link down/up event will not release the port from the discarding state.

Spanning Tree Protocol Status

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

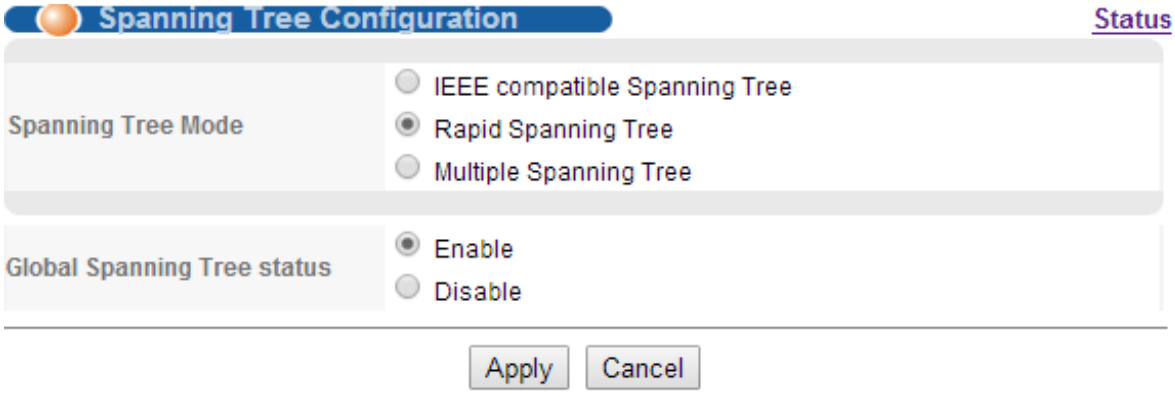


【Parameter Description】

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

Spanning Tree Configuration

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

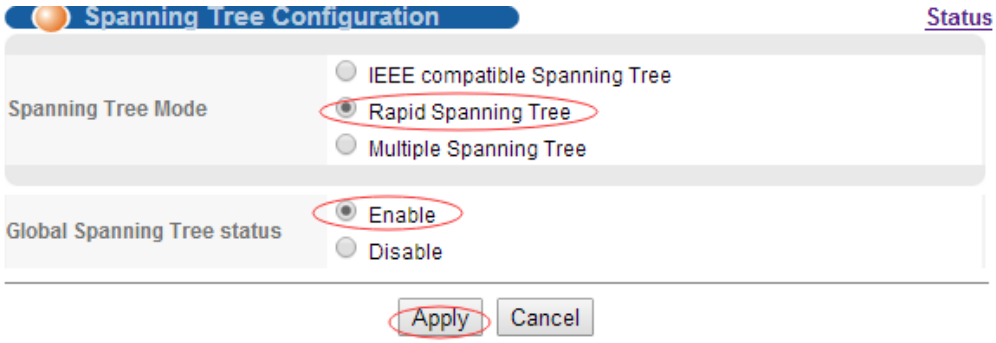


【Parameter Description】

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

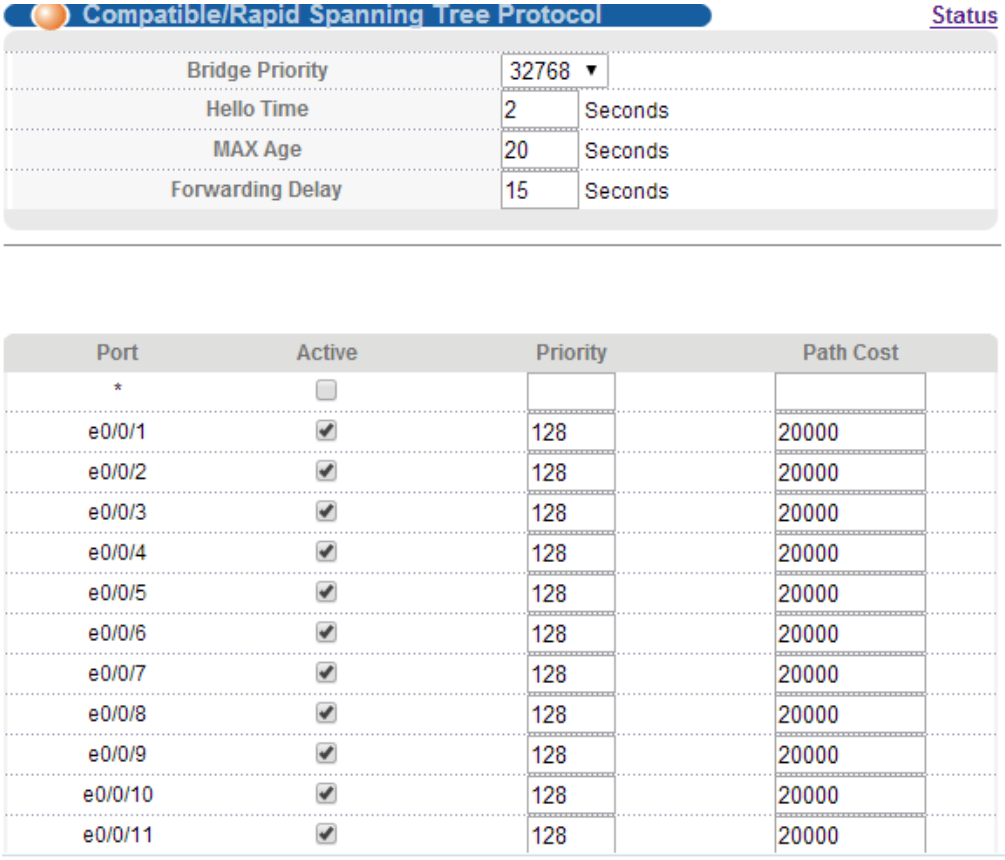
【Configuration example】

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



Compatible/Rapid Spanning Tree Protocol

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



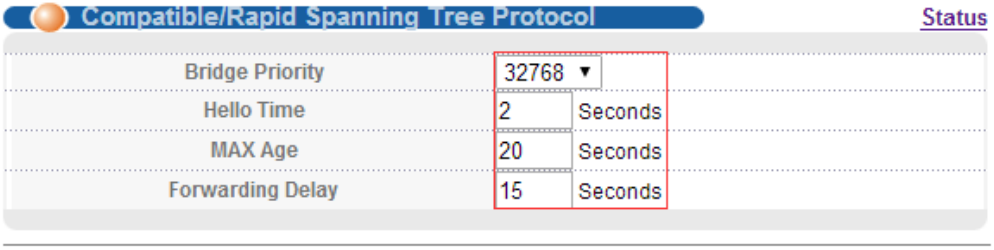
【Parameter Description】

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

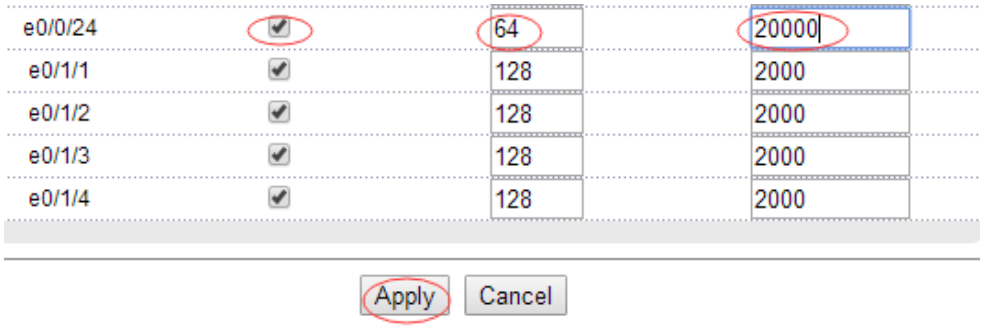
【Configuration example】

Such as:

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

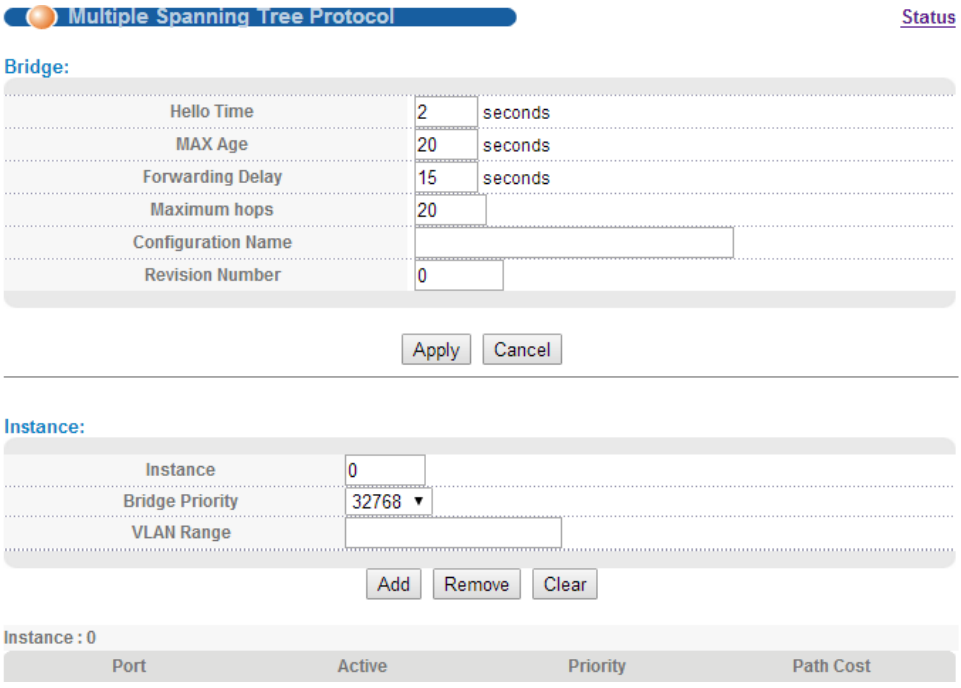


2. The priority of port 24 is 64, and the path cost is 20000.



Multiple Spanning Tree Protocol

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

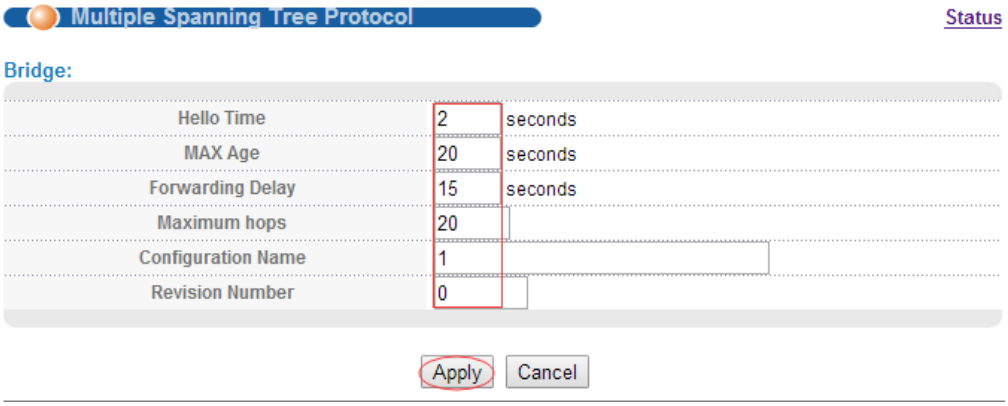


【Parameter Description】

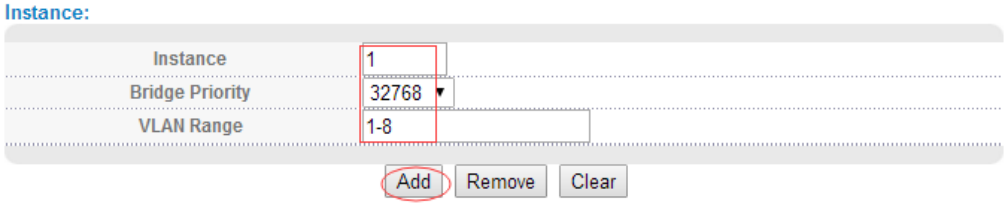
Parameter	Description
Hello Time	Switches sends bpdu in packet interval
Max age	Ports are not yet received a message in the time, will initiate topology changes
Forwarding Delay	The state of the port switch time
Maximum Hops	Set the maximum number of hops that BPDUs can support in the spanning tree
Configuration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

【Configuration example】

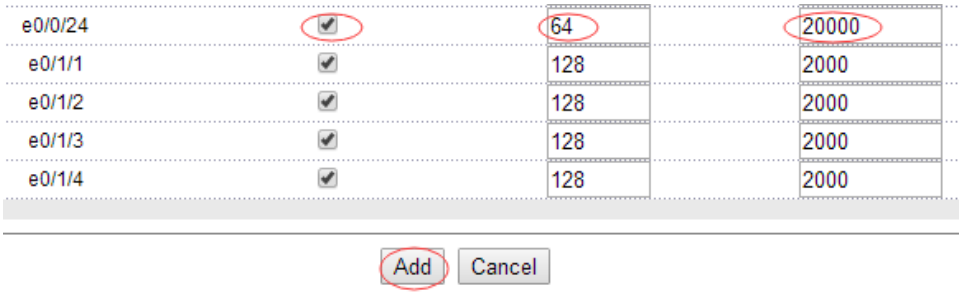
1. Bridge



2. Instance



3. The priority of port 24 is 64, and the path cost is 20000.



4. ERPS Protocol (Ethernet Ring Protection Switching)

Note: Information in this section is based on ITU-T G.8032/Y.1344.

The ITU G.8032 recommendation specifies a protection switching mechanism and protocol for Ethernet layer network rings. Ethernet rings can provide wide-area multipoint connectivity more economically due to their reduced number of links. The mechanisms and protocol defined in G.8032 achieve highly reliable and stable protection; and never form loops, which would fatally affect network operation and service availability.

The G.8032 recommendation, also referred to as Ethernet Ring Protection Switching (ERPS), can be used to increase the availability and robustness of Ethernet rings. An Ethernet ring built using ERPS can provide resilience at a lower cost and than that provided by SONET or EAPS rings.

ERPS is more economical than EAPS in that only one physical link is required between each node in the ring. However, since it can tolerate only one break in the ring, it is not as robust as EAPS. ERPS supports up to 255 nodes in the ring structure. ERPS requires a higher convergence time when more that 16 nodes are used, but should always run under than 500 ms.

Operational Concept

Loop avoidance in the ring is achieved by guaranteeing that, at any time, traffic may flow on all but one of the ring links. This particular link is called the ring protection link (RPL), and under normal conditions this link is blocked to traffic. One designated node, the RPL owner, is responsible for blocking traffic over the RPL. When a ring failure occurs, the RPL owner is responsible for unblocking the RPL, allowing this link to be used for traffic.

Ring nodes may be in one of two states:

Idle – normal operation, no link/node faults detected in ring

Protection – Protection switching in effect after identifying a signal fault

In Idle state, the physical topology has all nodes connected in a ring. The logical topology guarantees that all nodes are connected without a loop by blocking the RPL. Each link is monitored by its two adjacent nodes using Connectivity Fault Management (CFM) protocol messages.

Protection switching (opening the RPL to traffic) occurs when a signal failure message generated by the Connectivity Fault Management (CFM) protocol is

declared on one of the ring links, and the detected failure has a higher priority than any other request; or a Ring – Automatic Protection Switching protocol request

(R-APS, as defined in Y.1731) is received which has a higher priority than any other local request.

A link / node failure is detected by the nodes adjacent to the failure. These nodes block the failed link and report the failure to the ring using R-APS (SF) messages. This message triggers the RPL owner to unblock the RPL, and all nodes to flush their forwarding database. The ring is now in protection state, but it remains connected in a logical topology.

When the failed link recovers, the traffic is kept blocked on the nodes adjacent to the recovered link. The nodes adjacent to the recovered link transmit R-APS (NR - no request) message indicating they have no local request. When the RPL owner receives an R-APS (NR) message it starts the Wait-To-Recover (WTR) timer. Once WTR timer expires, the RPL owner blocks the RPL and transmits an R-APS (NR, RB - ring blocked) message. Nodes receiving this message flush the forwarding database and unblock their previously blocked ports. The ring is now returned to Idle state.

Multi-ring/Ladder Network – ERPSv2 also supports multipoint-to-multipoint connectivity within interconnected rings, called a “multi-ring/ladder network” topology. This arrangement consists of conjoined rings connected by one or more interconnection points, and is based on the following criteria:

- The R-APS channels are not shared across Ethernet Ring interconnections.
- On each ring port, each traffic channel and each R-APS channel are controlled (e.g., for blocking or flushing) by the Ethernet Ring Protection Control Process (ERP Control Process) of only one ring.
- Each Major Ring or Sub-Ring must have its own RPL.

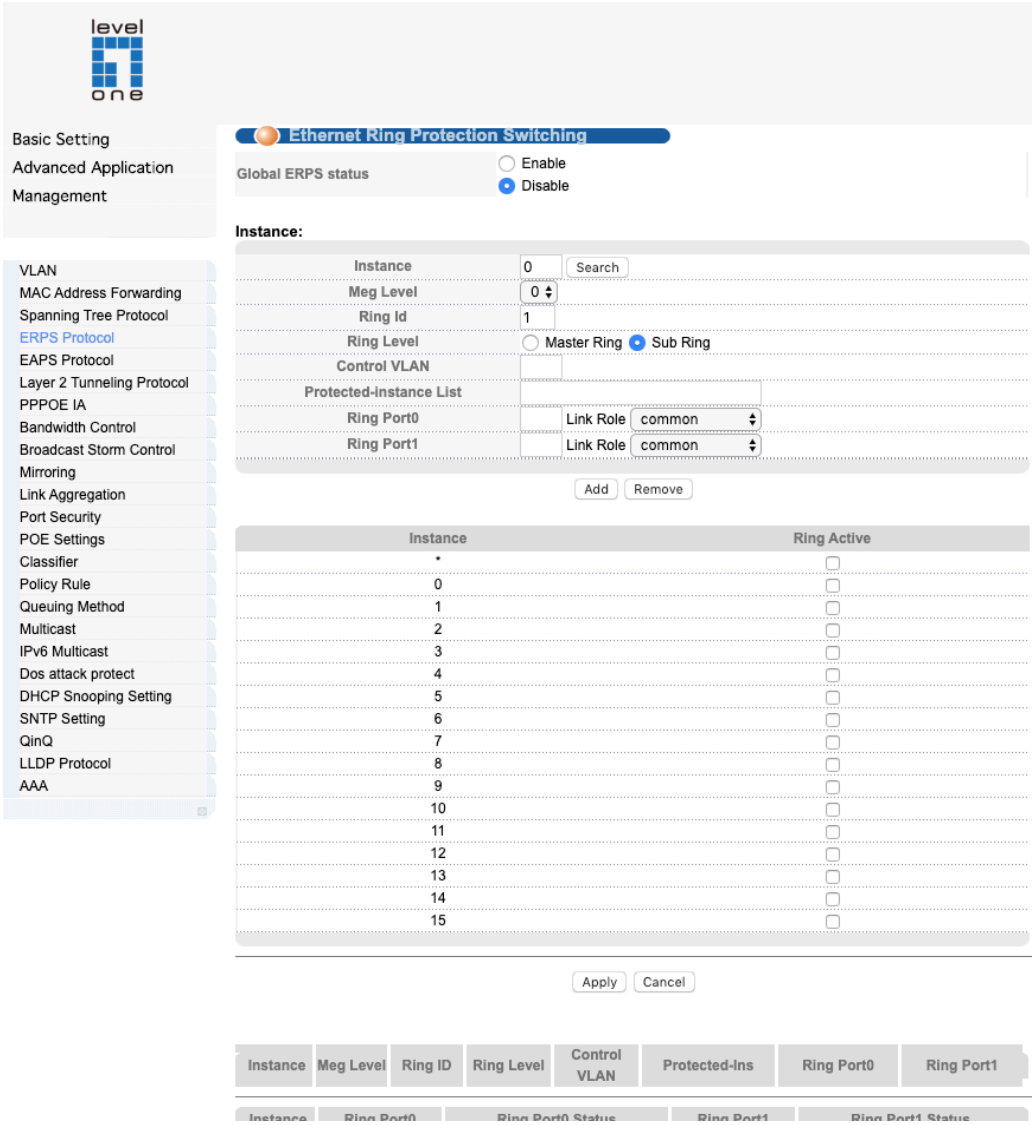
formed by the ring links of ERP2 and the ring link between the interconnection nodes that is controlled by ERP1. ERP2 is a sub-ring. Ring node A is the RPL owner node for ERP1, and ring node E is the RPL owner node for ERP2. These ring nodes (A and E) are responsible for blocking the traffic channel on the RPL for ERP1 and ERP2 respectively. There is no restriction on which ring link on an ring may be set as the RPL. For example the RPL of ERP1 could be set as the link between ring node C and D .

Ring nodes C and D, that are common to both ERP1 and ERP2, are called interconnection nodes. The ring link between the interconnection nodes are controlled and protected by the ring it belongs to. In the example for the Normal Condition, the ring link between ring nodes C and D is part of ERP1, and, as such, are controlled and protected by ERP1. Ethernet characteristic information traffic corresponding to the traffic channel may be transferred over a common Ethernet connection for ERP1 and ERP2 through the interconnection nodes C and D. Interconnection nodes C and D have separate ERP Control Processes for each

Ethernet Ring.

(Signal Fail Condition) illustrates a situation where protection switching has occurred due to an SF condition on the ring link between interconnection nodes C and D. The failure of this ring link triggers protection only on the ring to which it belongs, in this case ERP1. The traffic and R-APS channels are blocked bi-directionally on the ports where the failure is detected and bi-directionally unblocked at the RPL connection point on ERP1. The traffic channels remain bi-directionally blocked at the RPL connection point on ERP2. This prevents the formation of a loop.

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



【Parameter Description】

Parameter	Description
Global ERPS status	Select open or close ERPS
Instance	The range of 0-15, active instance.

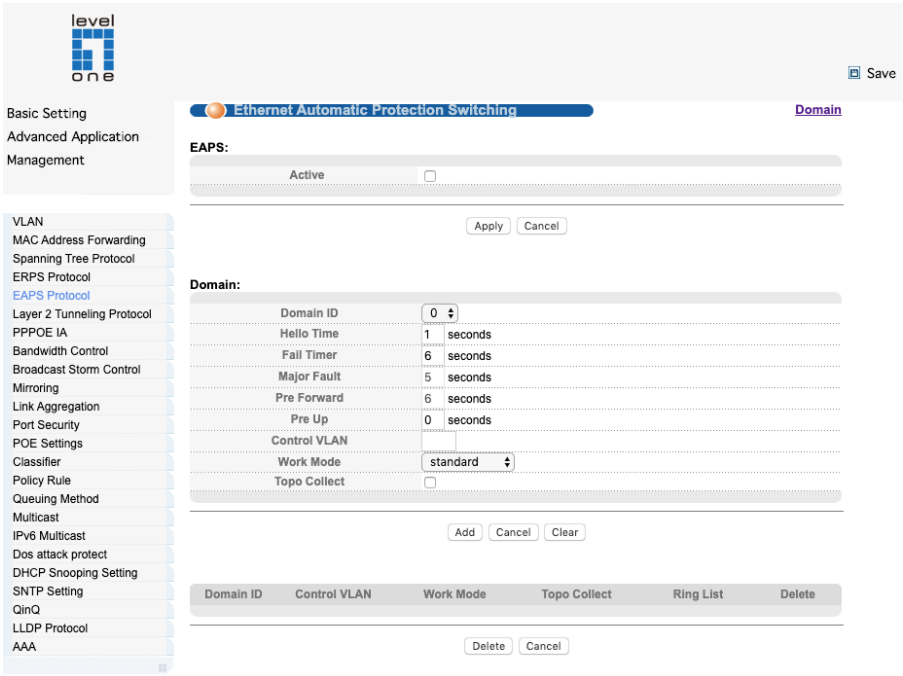
Parameter	Description
Meg level	The range of 0-7
Ring Id	The range of 1-239
Ring Level	Master Ring and Sub Ring
Control VLAN	You must configure the VLAN before configuring the ERRP ring
Protected-instance List	Application of MST instance
Ring port1	Configurable ports are common, owner, neighbor, next-neighbor
Ring port2	Configurable ports are common, owner, neighbor, next-neighbor

【Configuration example】

Such as: Open Global ERPS

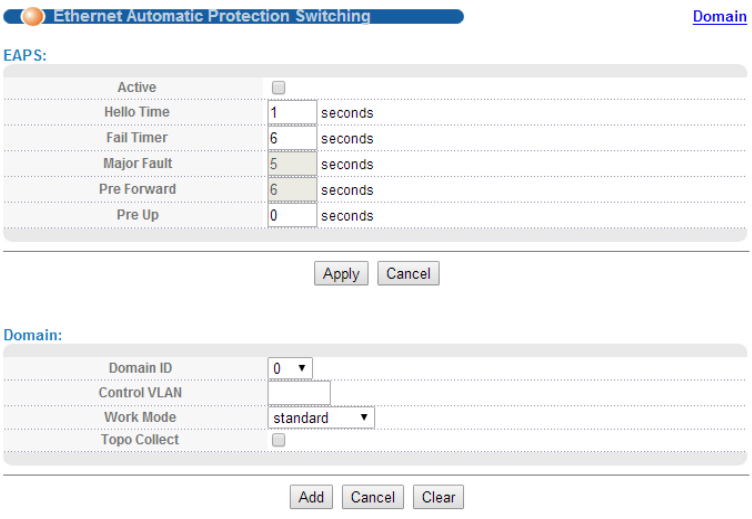
5. EAPS Protocol

Selecting “**Advanced Application**>**EAPS Protocol**>**Domain**, in the navigation bar, you can configure EAPS protocol.



Ethernet Automatic Protection Switching

Selecting “**Advanced Application**>**EAPS Protocol**>**Ethernet automatic protection switching**", in the navigation bar, you can configure Ethernet automatic protection switching.

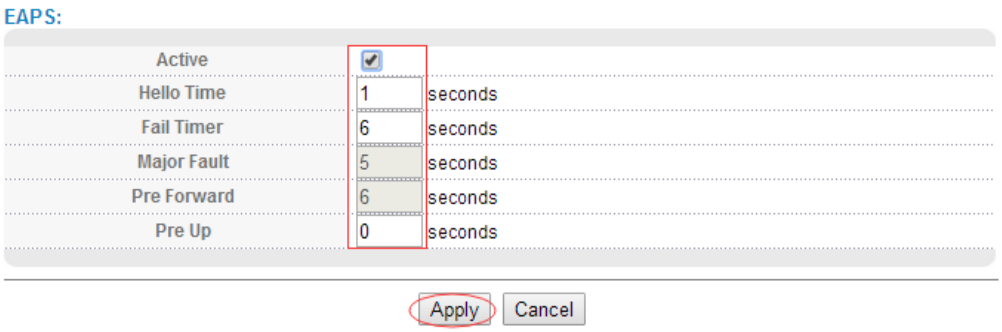


【Parameter Description】

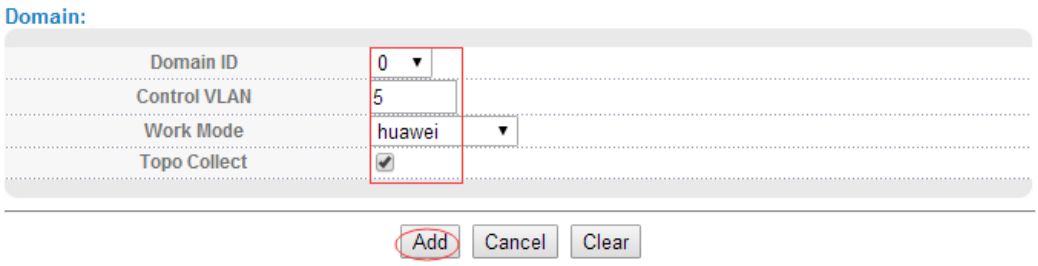
Parameter	Description
Active	Select open or close EAPS
Hello time	Switches sends bpdu in packet interval
Fail Timer	Configure the information timeout
Major Fault	The Major Fault timer will be automatically updated by the system
Pre Forward	The Pre forward timer will be automatically updated by the system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

【Configuration example】

1.EAPS

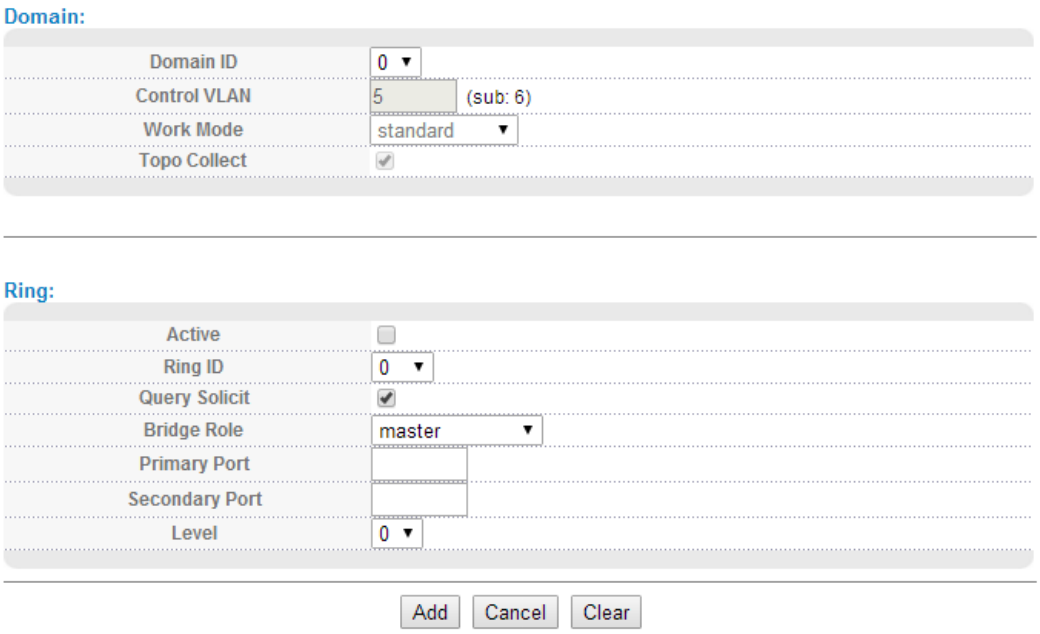


2.Domain



EAPS Domain

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

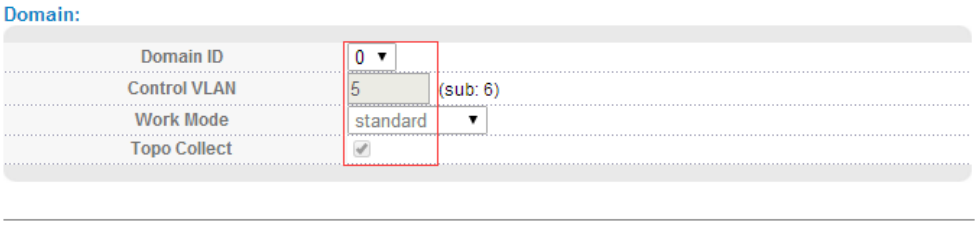


【Parameter Description】

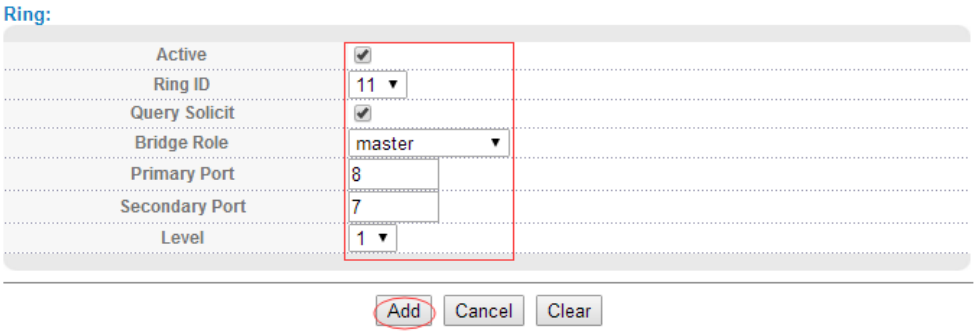
Parameter	Description
Domain ID	Select Domain ID
Control VLAN	You must configure the VLAN before configuring the EAPS Ring
Work mode	Work mode: standard huawei eips-subring
Topo Collect	Select open or close Topo Collect
Active	Select open or close Ring
Ring ID	Select ring ID
Query Solicit	Select open or close Query Solicit
Bridge Role	Bridge Role: mastesr transit edge assistant-edge
Level	Level: 0, 1

【Configuration example】

1. Configure Domain



2. Configure Ring

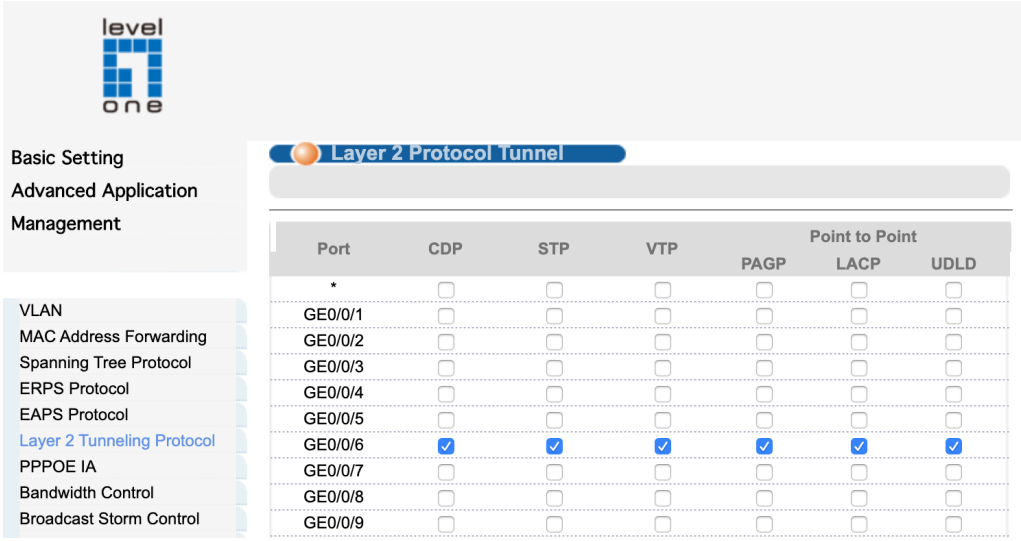


6. Layer 2 Tunneling Protocol

Use Layer 2 Tunneling Protocol > Application Filter page to forward CDP/STP/VTP/PAGP/LACP/UDLD packets.

Command Usage

If this feature is not enabled, the switch will handle CDP/STP/VTP/PAGP/LACP/UDLD packets as normal packets. In other words, they are forwarded to other ports in the same VLAN that are also configured to forward the specified packet type.



Parameters

These parameters are displayed:

- Port – Port identifier (GTP-2871 Range: 1-28 / GTP-5271 Range: 1-52)
- CDP – Cisco Discovery Protocol
- STP – Spanning Tree Protocol (STP, IEEE 802.1D-2004)
- VTP – Cisco VLAN Trunking Protocol
- LACP – Link Aggreation Control Protocol
- UDLD (UniDirectional Link Detection) – Detects general loopback conditions caused by hardware problems or faulty protocol settings.

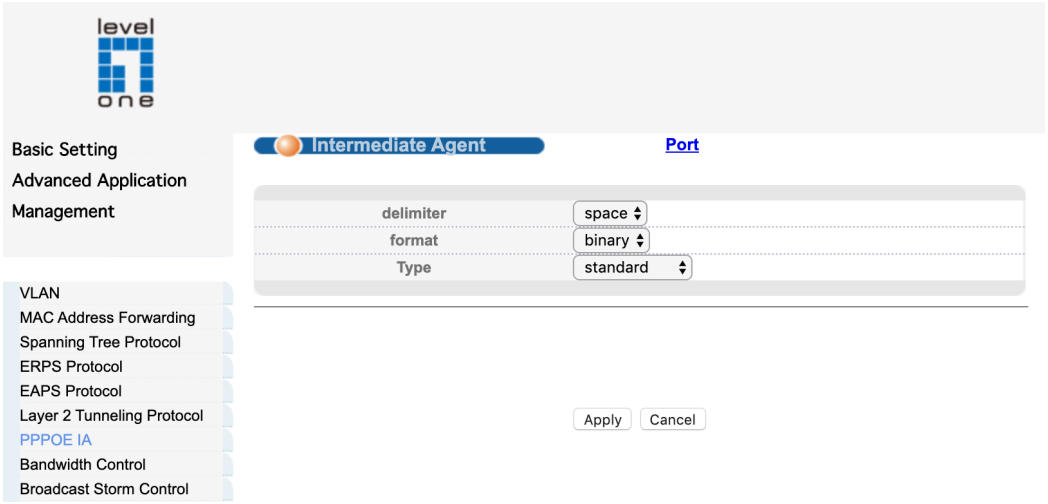
Web Interface

To discard or forward CDP/STP/VTP/PAGP/LACP/UDLD packets:

1. Set the packet type to be discarded or forwarded as required.
2. Click Apply.

7. PPPoE IA

PPPoE Intermediate Agent – Configures PPPoE Intermediate Agent (PPPoE IA) relay parameters required for passing authentication messages between a client and broadband remote access servers.



Command Usage

When PPPoE IA is enabled, the switch inserts a tag identifying itself as a PPPoE IA residing between the attached client requesting network access and the ports connected to broadband remote access servers (BRAS). The switch extracts access-loop information from the client's PPPoE Active Discovery Request, and forwards this information to all trusted ports (designated on the Configure Interface page). The BRAS detects the presence of the subscriber's circuit-ID tag inserted by the switch during the PPPoE discovery phase, and sends this tag as a NAS-port-ID attribute in PPP authentication and AAA accounting requests to a RADIUS server.

【Parameter Description】

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

PPPoE IA Global Status – Enables the PPPoE Intermediate Agent globally on the switch. (Default: Disabled)

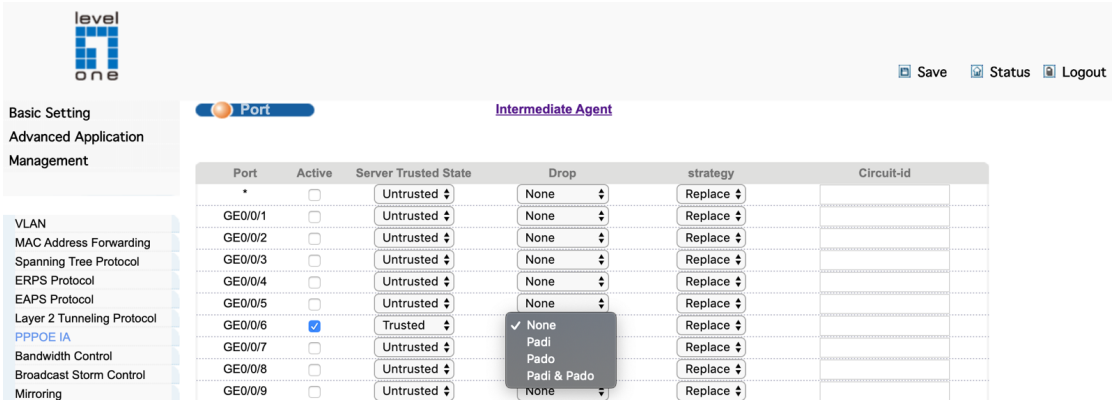
Note that PPPoE IA must be enabled globally before it can be enabled on an interface.

Access Node Identifier – String identifying this switch as an PPPoE IA to the PPPoE server. (Range: 1-48 ASCII characters: Default: IP address of first IPv4 interface on the switch.)

The switch uses the access-node-identifier to generate the circuit-id for PPPoE discovery stage packets sent to the BRAS, but does not modify the source or destination MAC address of these PPPoE discovery packets. These messages are forwarded to all trusted ports designated on the Configure Interface page.

Port

Selecting "**Advanced Application**>**PPPoE IA**>**Port**", in the navigation bar, you can configure port.



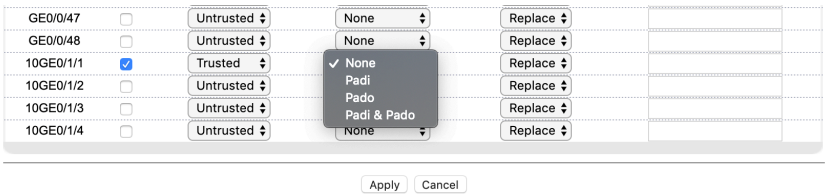
【Parameter Description】

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

Web Interface (Example : GTP-5271)

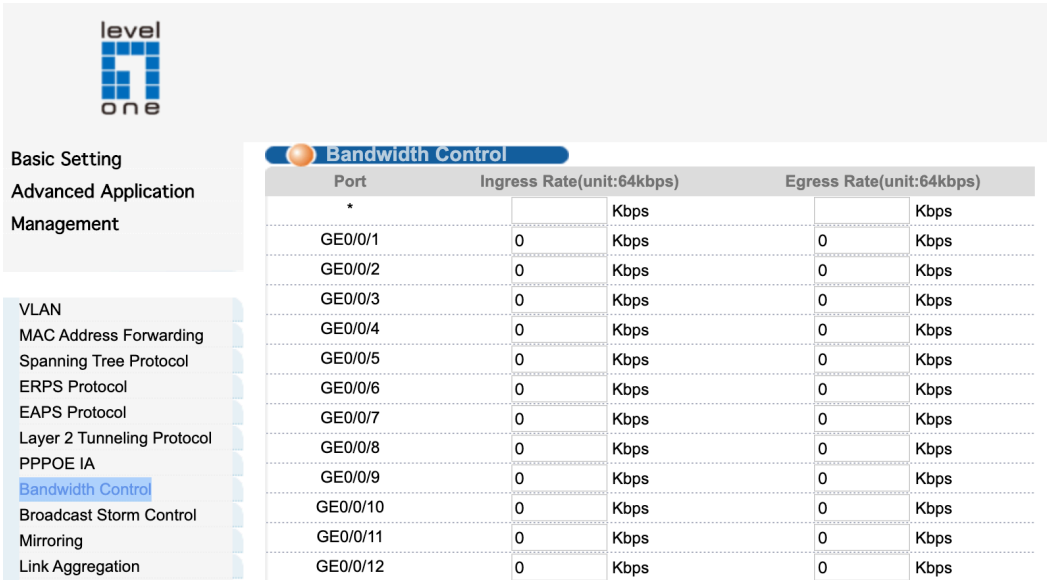
To configure global settings for PPPoE IA:

1. Select Configure Global from the Step list.
2. Enable the PPPoE IA on the switch, set the access node identifier, and set the generic error message.
3. Click Apply.



8. Bandwidth Control

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

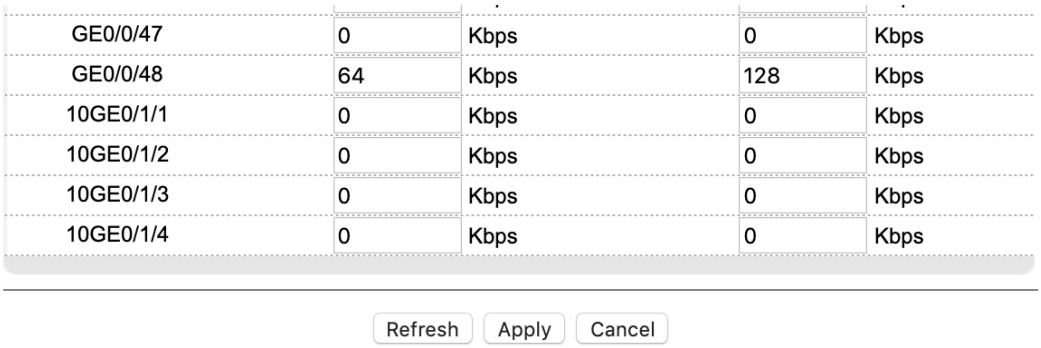


【Instructions】

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

【Configuration example】

Such as: Configure port-48 Ingress Rate is 64kbps, Egress Rate is 128kbps.
(Example : GTP-5271)



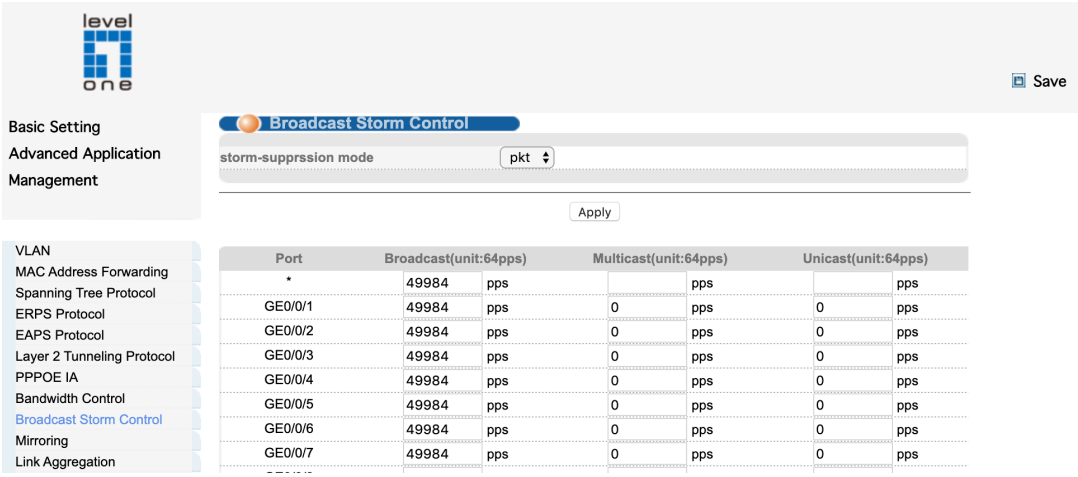
9. Broadcast Storm Control

Use the Broadcast Storm Control page to configure broadcast, multicast, and unknown unicast storm control thresholds. Traffic storms may occur when a device on your network is malfunctioning, or if application programs are not well designed or properly configured. If there is too much traffic on your network, performance can be severely degraded or everything can come to complete halt.
You can protect your network from traffic storms by setting a threshold for broadcast, multicast or unknown unicast traffic. Any packets exceeding the specified threshold will then be dropped.

Command Usage
When traffic exceeds the threshold specified for broadcast and multicast or unknown unicast traffic, packets exceeding the threshold are dropped until the rate falls back down beneath the threshold.

Rate limits set by the storm control function are also used by automatic storm control when the control response is set to rate control on the Auto Traffic Control (Configure Interface) page.

◆ Using both rate limiting and storm control on the same interface may lead to unexpected results.
It is therefore not advisable to use both of these features on the same interface.



【Parameter Description】

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

【Instructions】

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

Parameters

These parameters are displayed:

- Interface – Displays a list of ports or trunks.
- Broadcast – Specifies storm control for broadcast traffic.
- Multicast – Specifies storm control for multicast traffic.
- Unicast – Specifies storm control for unknown unicast traffic.
- Status – Enables or disables storm control. (Default: disabled for broadcast, multicast and unknown unicast storm control)

【Configuration example】

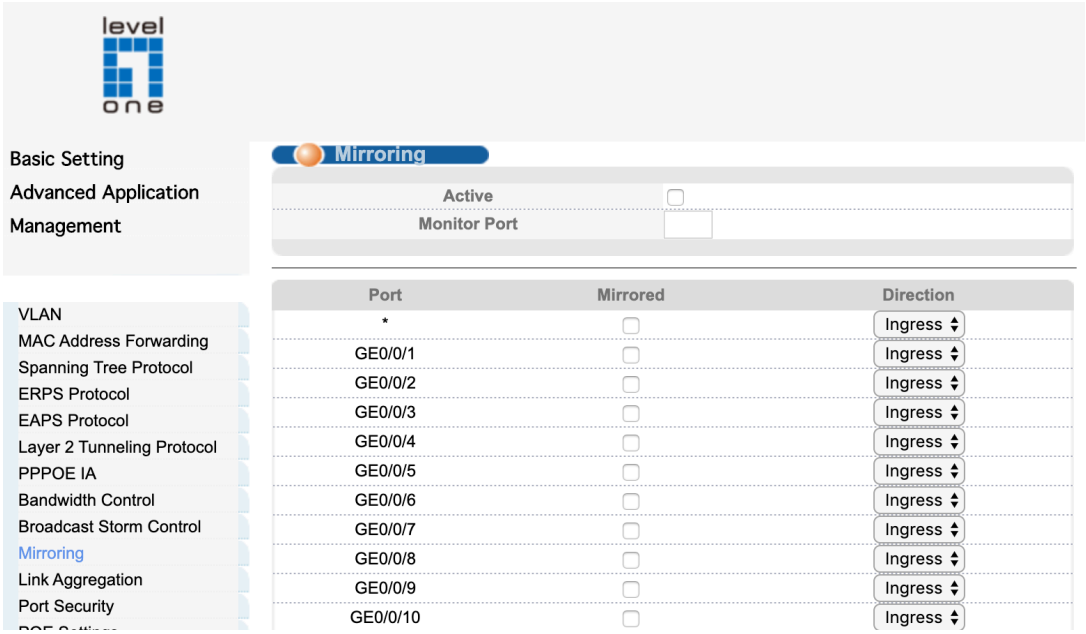
Such as: Set Port1 broadcast as 6400 pps, multicast as 3200 pps, unicast as 3200 pps.

Port	Broadcast(unit:64pps)		Multicast(unit:64pps)		Unicast(unit:64pps)	
*	6400	pps	3200	pps	3200	pps
GE0/0/1	6400	pps	3200	pps	3200	pps
GE0/0/2	6400	pps	3200	pps	3200	pps
GE0/0/3	6400	pps	3200	pps	3200	pps

10. Mirroring

Configuring Local Port Mirroring

Use the Mirroring page to mirror traffic from any source port to a target port for real-time analysis. You can then attach a logic analyzer or RMON probe to the target port and study the traffic crossing the source port in a completely unobtrusive manner.



When traffic matches the rules for both port mirroring, and for mirroring of VLAN traffic or packets based on a MAC address, the matching packets will not be sent to target port specified for port mirroring.

The destination port cannot be a trunk or trunk member port.

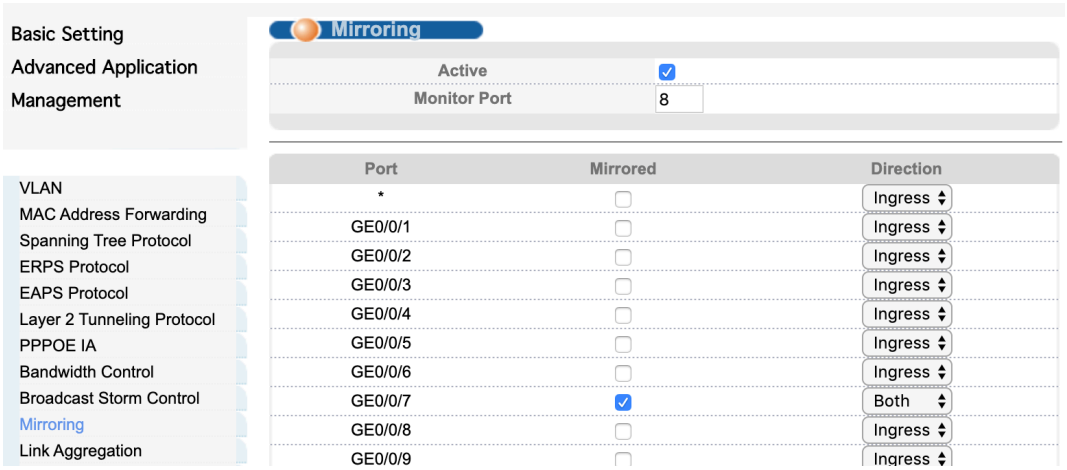
Note that Spanning Tree BPDU packets are not mirrored to the target port.

【Parameter Description】

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

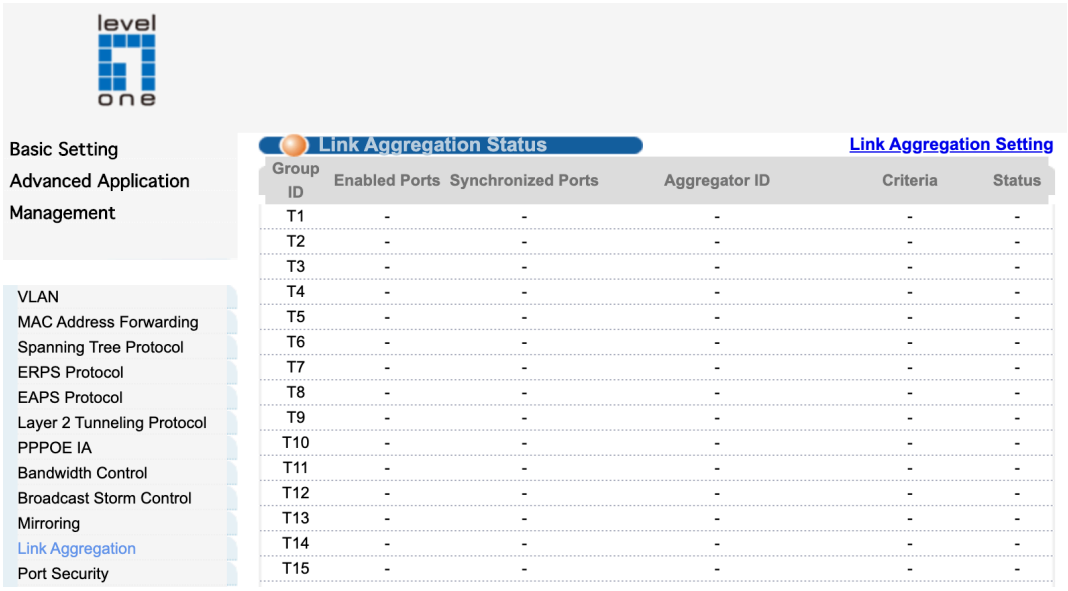
【Configuration example】

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



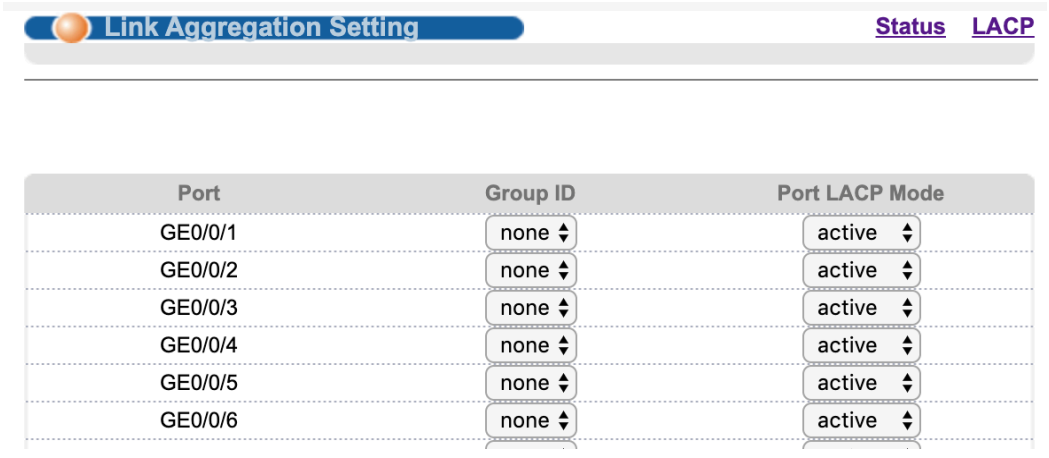
11. Link Aggregation

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



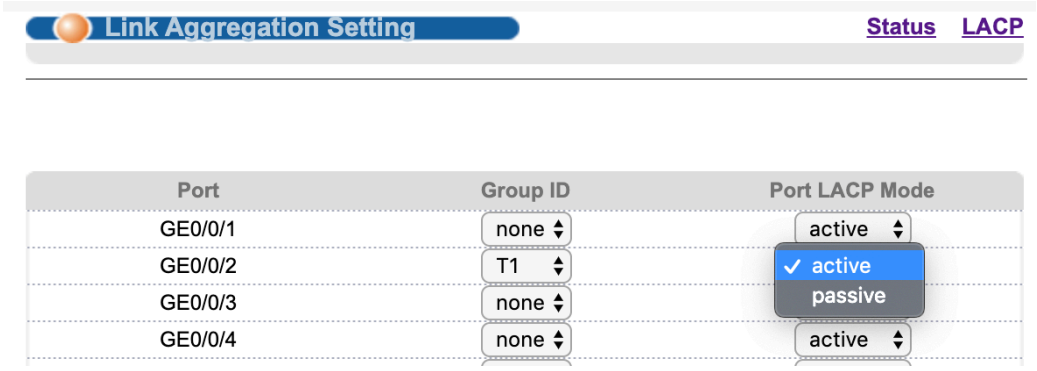
Link Aggregation status

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



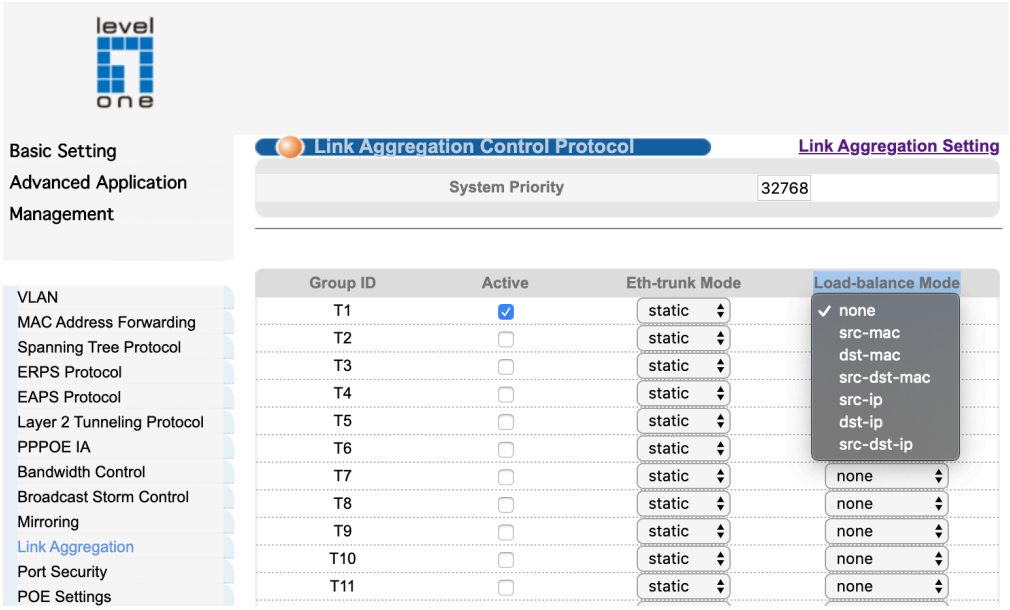
【Configuration example】

Such as: configure parameter of Aggregation Group port-2.



Link Aggregation Control Protocol

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



【Parameter Description】

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

【Parameter Description】

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

Command Usage

To avoid creating a loop in the network, be sure you enable LACP before connecting the ports, and also disconnect the ports before disabling LACP.

If the target switch has also enabled LACP on the connected ports, the trunk will be activated automatically.

A trunk formed with another switch using LACP will automatically be assigned the next available trunk ID.

If more than eight ports attached to the same target switch have LACP enabled, the additional ports will be placed in standby mode, and will only be enabled if one of the active links fails.

All ports on both ends of an LACP trunk must be configured for full duplex, and auto-negotiation.

This command applies to all static and dynamic trunks on the switch.

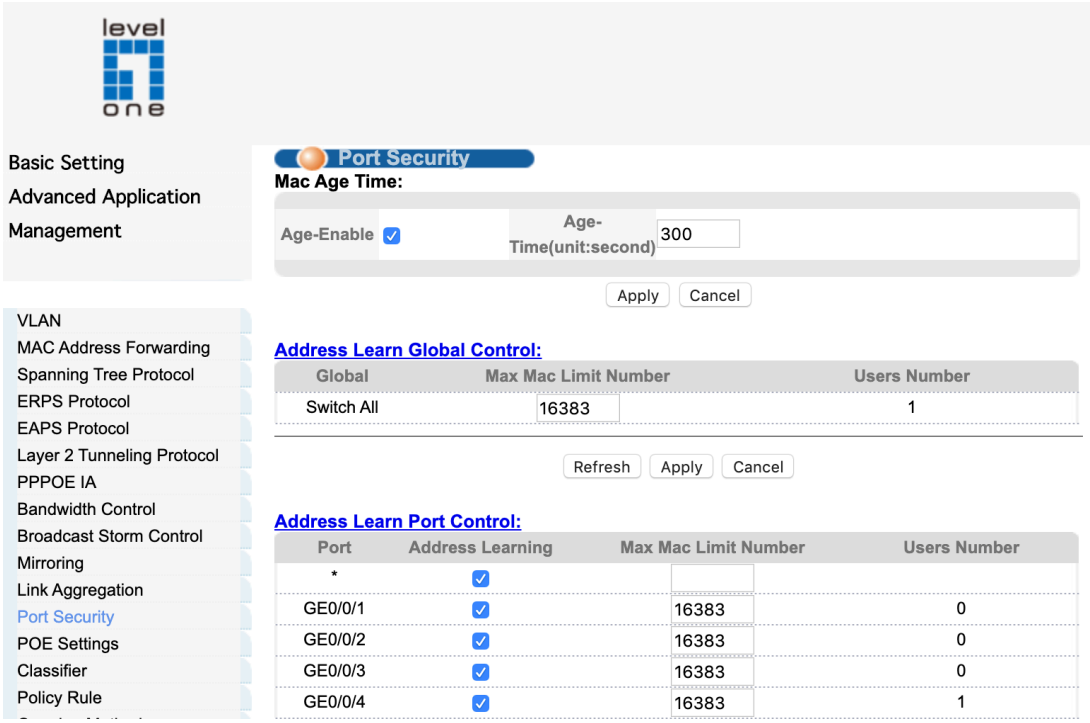
To ensure that the switch traffic load is distributed evenly across all links in a trunk, select the source and destination addresses used in the load-balance calculation to provide the best result for trunk connections:

◆ Destination IP Address : All traffic with the same destination IP address is output on the same link in a trunk. This mode works best for switch-to- router trunk links where traffic through the switch is destined for many different hosts. Do not use this mode for switch-to-server trunk links where the destination IP address is the same for all traffic.

◆ Destination MAC Address : All traffic with the same destination MAC address is output on the same link in a trunk. This mode works best for switch-to-switch trunk links where traffic through the switch is destined for many different hosts. Do not use this mode for switch-to-router trunk links where the destination MAC address is the same for all traffic.

12. Port Security

Selecting “**Advanced Application>Port Security**", in the navigation bar, you can configure port address learn control.

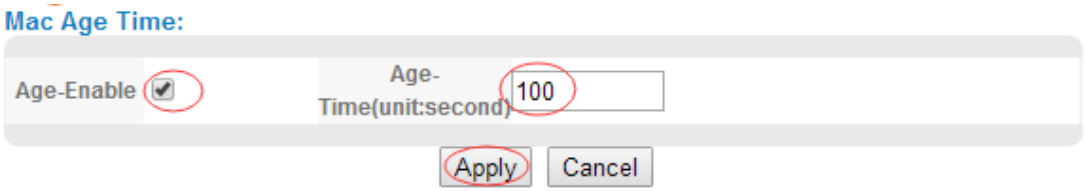


【Parameter Description】

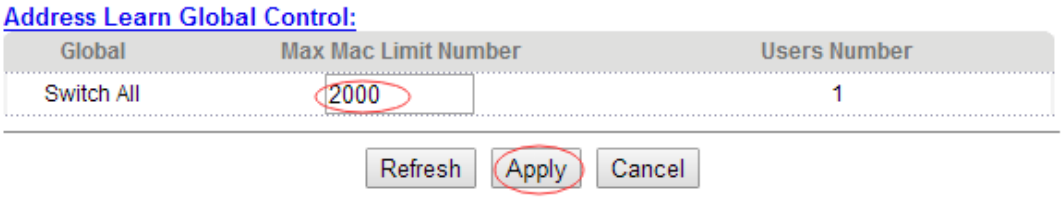
Parameter	Description
Age-Enable	Open age-enable
Age-Time	Set Age Time(the range of 10-1000000, unit: second)
Max Mac Limit Number (Global)	Set the global Max MAC Limit Number(0-16384)
Address Learning	The MAC address learning function of port enables the power switch (the default port MAC learning function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

【Configuration example】

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

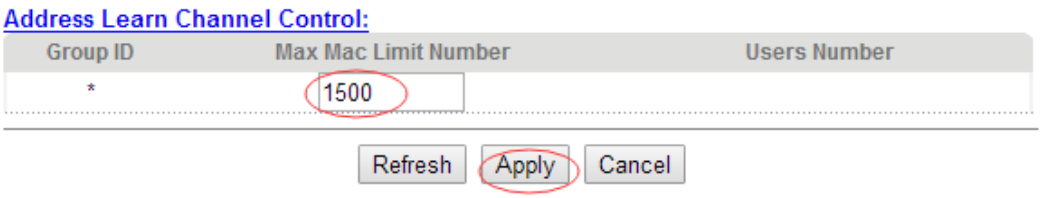


2.Configure Address Learn Global Control, set max mac limit number is 2000.

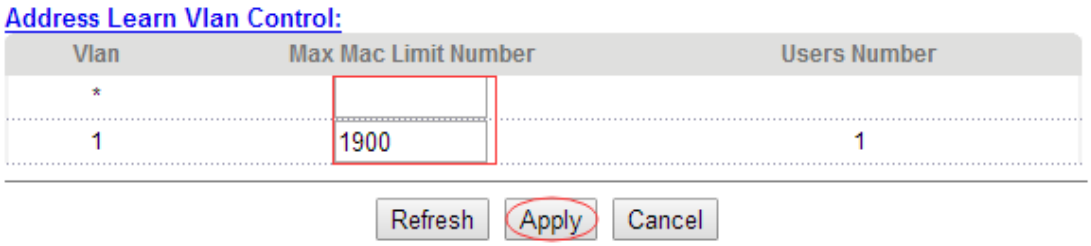


3.Port 8 address learn control, Max Mac Limit Number is 1800.

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

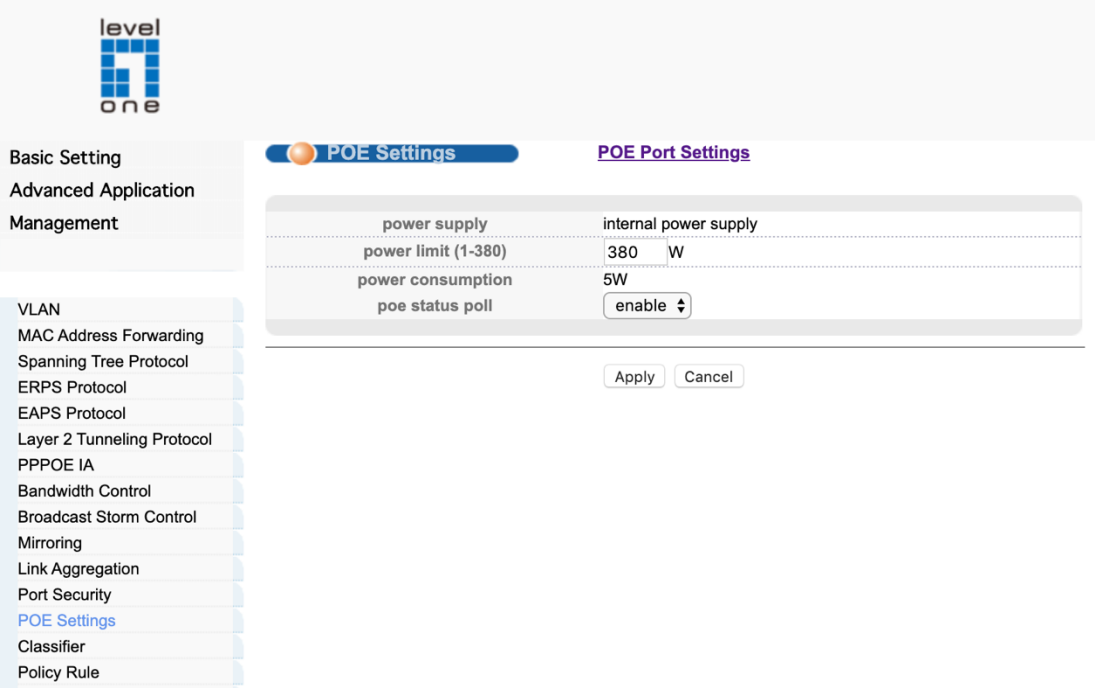


5.Configure Address Learn Vlan Control, set Max Mac Limit Number (Vlan) is 1900.



13. POE Settings

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



PoE Budget

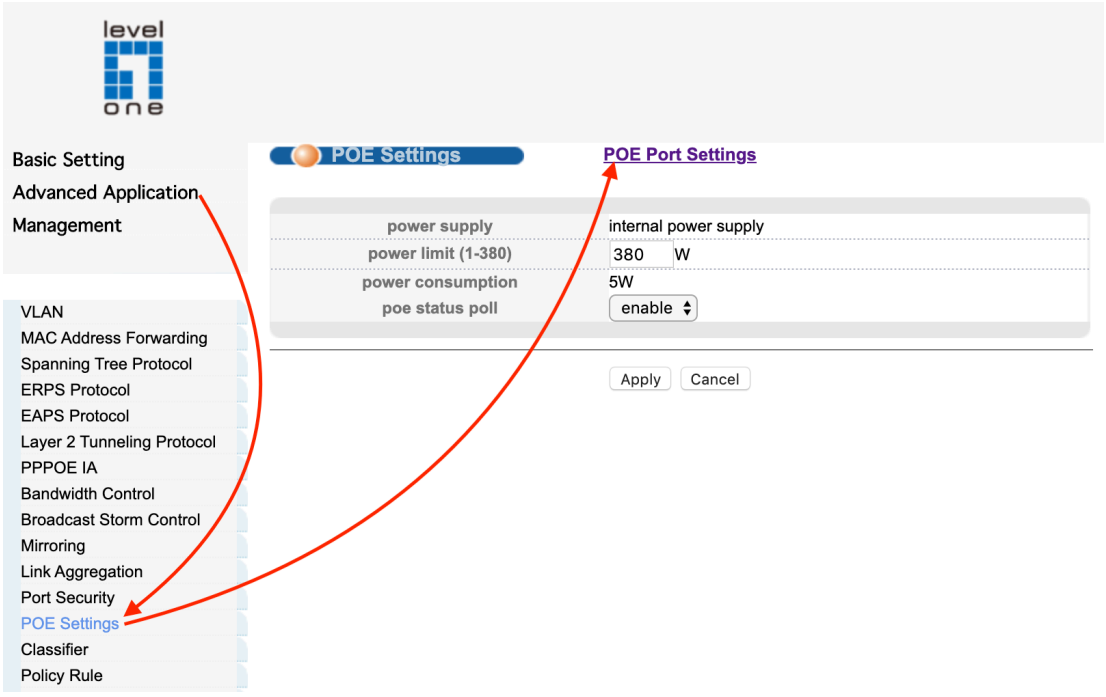
- 320W@100~160VAC,50/60HZ
- 400W@200~240VAC,50/60HZ
- Power Budget: Max. 400W (Recommended Max use 380W)
- Power Output: Up to 30W per port
- Protection: Circuit protection to prevent power interference between ports

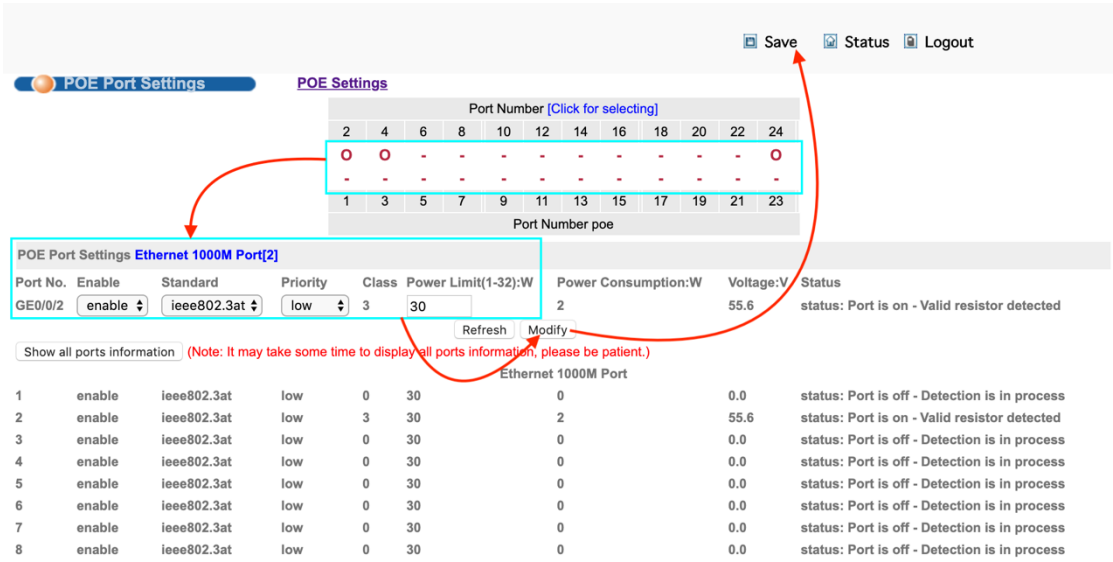
【Parameter Description】

Parameter	Description
power limit (1-380)	The power of switch POE can be limited

POE Port Settings

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



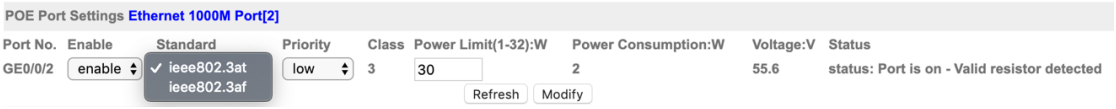


【Parameter Description】

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

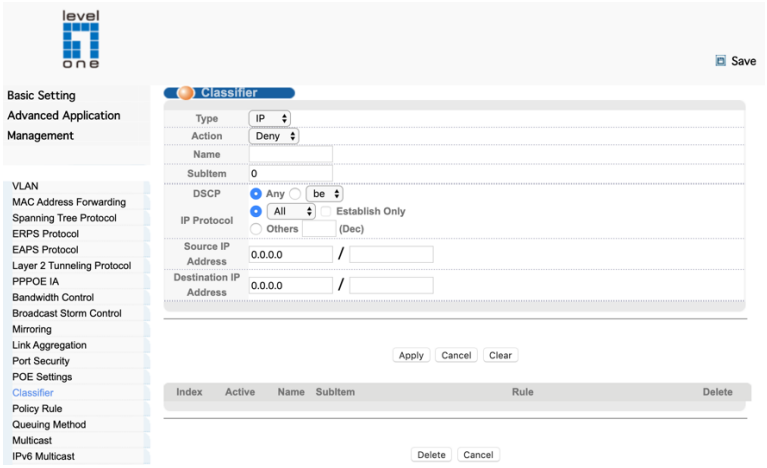
【Configuration example】

Such as: Configure the POE for port 1.



14. Classifier

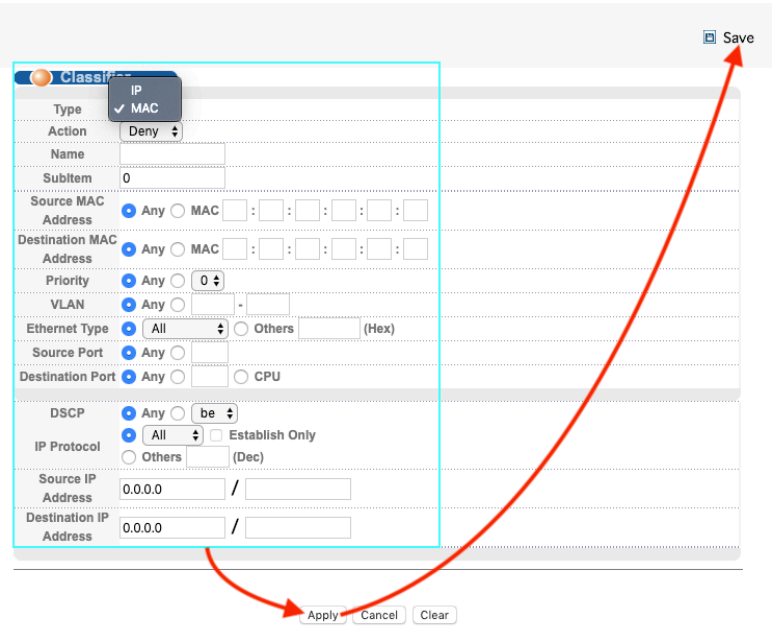
Selecting “**Advanced Application**>**Classifier**", in the navigation bar, you can configure Classifier.



【Parameter Description】

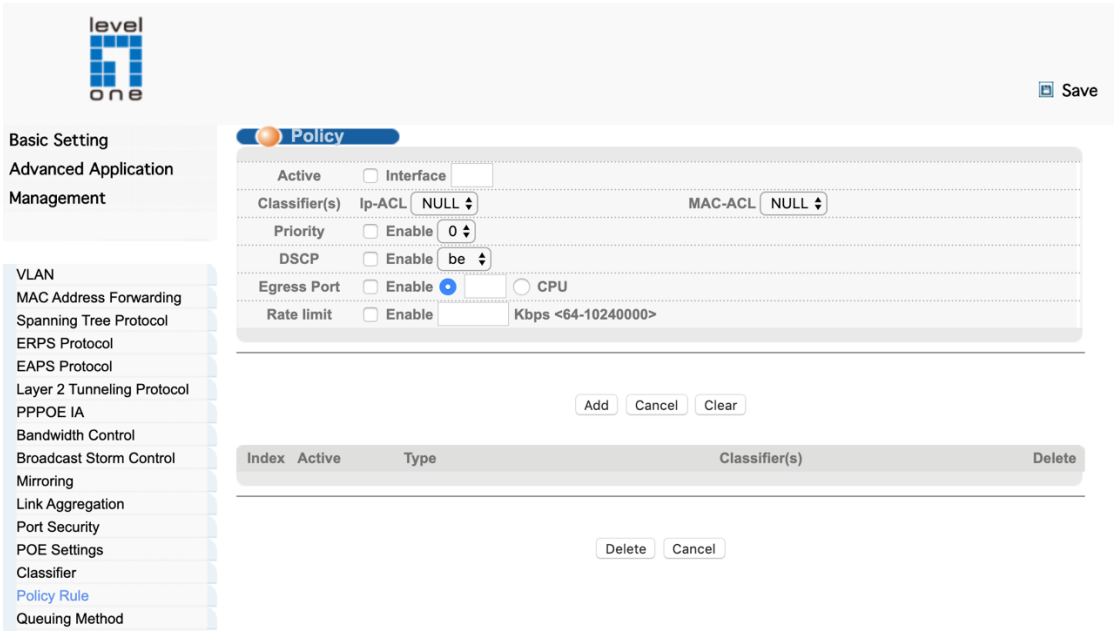
Parameter	Description
Active	Active Classifier
Layer2	Set VLAN, Priority, Ethernet type, Source Mac Address, DSCP, IP Protocol
Layer3	Set Source IP

【Configuration example】



15. Policy Rule

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

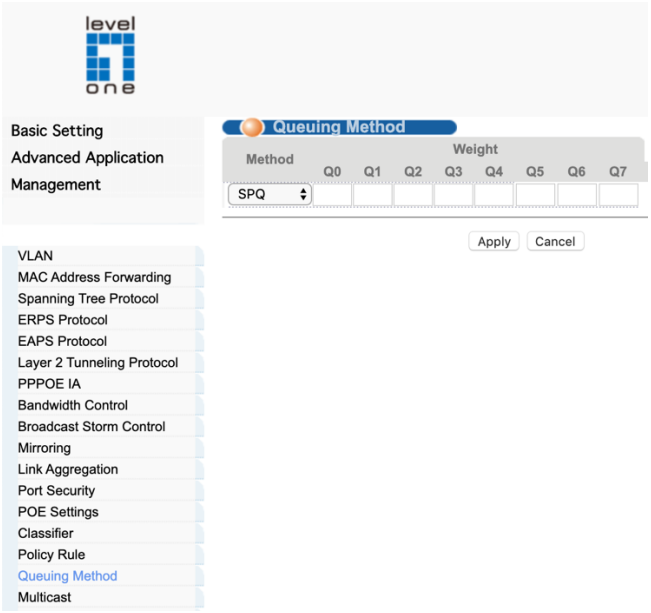


【Parameter Description】

Parameter	Description
Active	Active Policy Rule
Classifier(s)	You need to match the set of classification rules
Priority	Ingress Port Priority (0-7)
DSCP	Default port priority, traffic class map, queue scheduling, IP Precedence, or Differentiated Services Code Point (DSCP)
Egress Port	The switch sends the packet to the proper egress port.
Rate limit	Rate – Sets the rate limit level. (Range: 64 - 1,000,000 kbits per second for Gigabit Ethernet ports; 64 - 10,024,000 kbits per second for 10 Gigabit Ethernet ports)

16. Queuing Method

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



Parameters

These parameters are displayed:

◆ **Queuing Method**

- **Strict** – Services the egress queues in sequential order, transmitting all traffic in the higher priority queues before servicing lower priority queues. This ensures that the highest priority packets are always serviced first, ahead of all other traffic.
- **WRR** – Weighted Round-Robin shares bandwidth at the egress ports by using scheduling weights, and servicing each queue in a round-robin fashion. (This is the default setting.)
- **Strict and WRR** – Uses strict priority on the high-priority queues and WRR on the remaining queues.

◆ **Queue ID** – The ID of the priority queue. (Range: 0-7)

◆ **Strict Mode** – If “Strict and WRR” mode is selected, then a combination of strict service is used for the high priority queues and weighted service for the remaining queues. Use

this parameter to specify the queues assigned to use strict priority when using the strict-weighted queuing mode.

(Default: Disabled)

- **Weight** – Sets a weight for each queue which is used by the WRR scheduler. (Range: 1-127; Default: Weights 1, 2, 4, 6, 8, 10, 12 and 14 are assigned to queues 0 - 7 respectively)

Web Interface

To configure the queue mode:

1. Click Traffic, Priority, Queue.
2. Set the queue mode for the port selected.
3. If the weighted queue mode is selected, the queue weight can be modified if required.
4. If the queue mode that uses a combination of strict and weighted queueing is selected, the queues which are serviced first must be specified by enabling strict mode parameter in the table.
5. Click Apply.
6. Click Save.

Figure : Setting the Queue Mode (WRR)

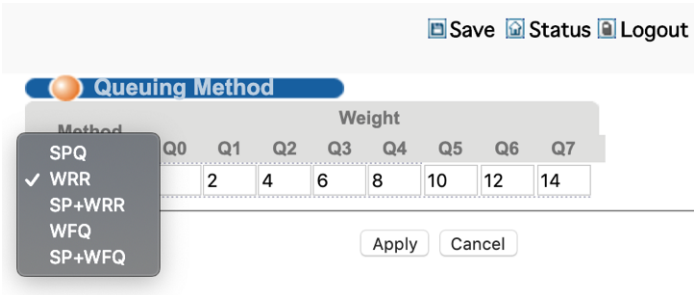
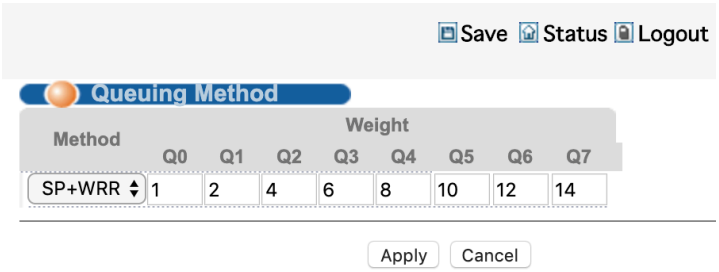


Figure : Setting the Queue Mode (Strict and WRR)



17. Multicast

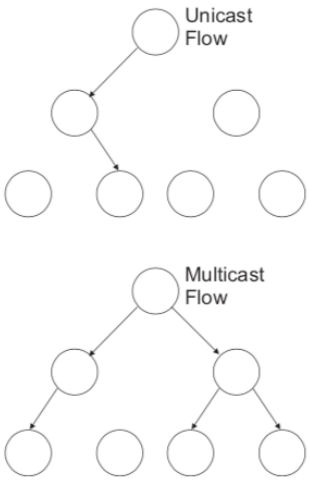
This chapter describes how to configure the following multicast services:

- IGMP Snooping – Configures snooping and query parameters.
- IGMP Filtering and Throttling – Filters specified multicast service, or throttles the maximum of multicast groups allowed on an interface.
- MLD Snooping – Configures snooping and query parameters for IPv6.
- MLD Filtering and Throttling – Filters specified multicast service, or throttles the maximum of multicast groups allowed on an interface.
- Filtering MLD Query Packets on an Interface – Configures the interface to drop MLD query packets.
- Multicast VLAN Registration for IPv4 – Configures a single network-wide multicast VLAN shared by hosts residing in other standard or private VLAN groups, preserving security and data isolation.
- Multicast VLAN Registration for IPv6 – Configures a single network-wide multicast VLAN shared by hosts residing in other standard or private VLAN groups, preserving security and data isolation.

Overview

Multicasting is used to support real-time applications such as video conferencing or streaming audio. A multicast server does not have to establish a separate connection with each client. It merely broadcasts its service to the network, and any hosts that want to receive the multicast register with their local multicast switch/router. Although this approach reduces the network overhead required by a multicast server, the broadcast traffic must be carefully pruned at every multicast switch/router it passes through to ensure that traffic is only passed on to the hosts which subscribed to this service.

Figure : Multicast Filtering Concept



This switch can use Internet Group Management Protocol (IGMP) to filter multicast traffic. IGMP Snooping can be used to passively monitor or “snoop” on exchanges between attached hosts and an IGMP-enabled device, most commonly a multicast router. In this way, the switch can discover the ports that want to join a multicast group, and set its filters accordingly.

If there is no multicast router attached to the local subnet, multicast traffic and query messages may not be received by the switch. In this case (Layer 2) IGMP Query can be used to actively ask the attached hosts if they want to receive a specific multicast service. IGMP Query thereby identifies the ports containing hosts requesting to join the service and sends data out to those ports only. It then propagates the service request up to any neighboring multicast switch/router to ensure that it will continue to receive the multicast service.

The purpose of IP multicast filtering is to optimize a switched network’s performance, so multicast packets will only be forwarded to those ports containing multicast group hosts or multicast routers/switches, instead of flooding traffic to all ports in the subnet (VLAN).

Layer 2 IGMP (Snooping and Query for IPv4)

IGMP Snooping and Query – If multicast routing is not supported on other switches in your network, you can use IGMP Snooping and IGMP Query to monitor IGMP service requests passing between multicast clients and servers, and dynamically configure the switch ports which need to forward multicast traffic. IGMP Snooping conserves bandwidth on network segments where no node has expressed interest in receiving a specific multicast service. For switches that do not support multicast routing, or where multicast routing is already enabled on other switches in the local network segment, IGMP Snooping is the only service required to support multicast filtering.

When using IGMPv3 snooping, service requests from IGMP Version 1, 2 or 3 hosts are all forwarded to the upstream router as IGMPv3 reports. The primary enhancement provided by IGMPv3 snooping is in keeping track of information about the specific multicast sources which downstream IGMPv3 hosts have requested or refused. The switch maintains information about both multicast groups and channels, where a group indicates a multicast flow for which the hosts have not requested a specific source (the only option for IGMPv1 and v2 hosts unless statically configured on the switch), and a channel indicates a flow for which the hosts have requested service from a specific source. For IGMPv1/v2 hosts, the source address of a channel is always null (indicating that any source is acceptable), but for IGMPv3 hosts, it may include a specific address when requested.
Only IGMPv3 hosts can request service from a specific multicast source. When downstream hosts request service from a specific source for a multicast service, these sources are all placed in the Include list, and traffic is forwarded to the hosts from each of these sources. IGMPv3 hosts may also request that service be

forwarded from any source except for those specified. In this case, traffic is filtered from sources in the Exclude list, and forwarded from all other available sources.

Note: When the switch is configured to use IGMPv3 snooping, the snooping version may be downgraded to version 2 or version 1, depending on the version of the IGMP query packets detected on each VLAN.
Note: IGMP snooping will not function unless a multicast router port is enabled on the switch. This can accomplished in one of two ways. A static router port can be manually configured. Using this method, the router port is never timed out, and will continue to function until explicitly removed. The other method relies on the switch to dynamically create multicast routing ports whenever multicast routing protocol packets or IGMP query packets are detected on a port.
Note: A maximum of up to 1023 multicast entries can be maintained for IGMP snooping. Once the table is full, no new entries are learned. Any subsequent multicast traffic not found in the table is dropped if unregistered-flooding is disabled (default behavior) and no router port is configured in the attached VLAN, or flooded throughout the VLAN if unregistered-flooding is enabled

Static IGMP Router Interface – If IGMP snooping cannot locate the IGMP querier, you can manually designate a known IGMP querier (i.e., a multicast router/switch) connected over the network to an interface on your switch. This interface will then join all the current multicast groups supported by the attached router/switch to ensure that multicast traffic is passed to all appropriate interfaces within the switch.
Static IGMP Host Interface – For multicast applications that you need to control more carefully, you can manually assign a multicast service to specific interfaces on the switch.

IGMP Snooping with Proxy Reporting – The switch supports last leave, and query suppression (as defined in DSL Forum TR-101, April 2006):

- When proxy reporting is disabled, all IGMP reports received by the switch are forwarded natively to the upstream multicast routers.
- Last Leave: Intercepts, absorbs and summarizes IGMP leaves coming from IGMP hosts. IGMP leaves are relayed upstream only when necessary, that is, when the last user leaves a multicast group.
- Query Suppression: Intercepts and processes IGMP queries in such a way that IGMP specific queries are never sent to client ports.

The only deviation from TR-101 is that the marking of IGMP traffic initiated by the switch with priority bits as defined in R-250 is not supported.

Based on the IGMP query and report messages, the switch forwards multicast traffic only to the ports that request it. This prevents the switch from broadcasting the traffic to all ports and possibly disrupting network performance.
Command Usage

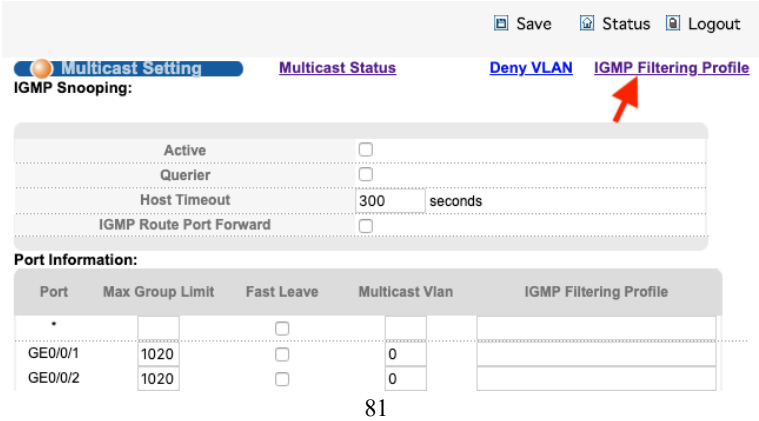
◆ **IGMP Snooping** – This switch can passively snoop on IGMP Query and Report packets transferred between IP multicast routers/switches and IP multicast host groups to identify the IP multicast group members. It simply monitors the IGMP packets passing through it, picks out the group registration information, and configures the multicast filters accordingly.
Note: If unknown multicast traffic enters a VLAN which has been configured with a router port, the traffic is forwarded to that port. However, if no router port exists on the VLAN, the traffic is dropped if unregistered data flooding is disabled (default behavior), or flooded throughout the VLAN if unregistered data flooding is enabled.

◆ **IGMP Querier** – A router, or multicast-enabled switch, can periodically ask their hosts if they want to receive multicast traffic. If there is more than one router/ switch on the LAN performing IP multicasting, one of these devices is elected "querier" and assumes the role of querying the LAN for group members. It then propagates the service requests on to any upstream multicast switch/router to ensure that it will continue to receive the multicast service.
Note: Multicast routers use this information from IGMP snooping and query reports, along with a multicast routing protocol such as DVMRP or PIM, to support IP multicasting across the Internet.

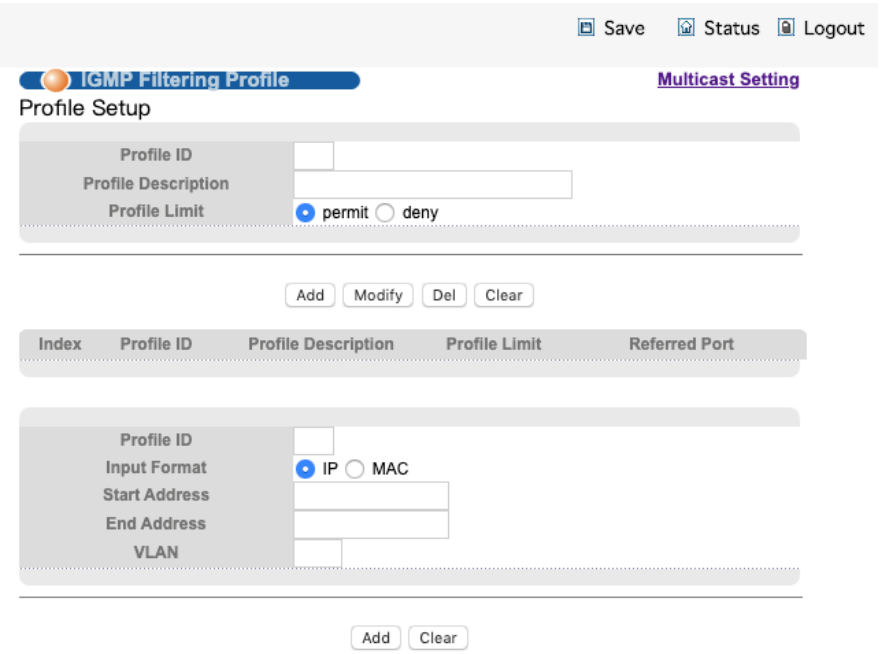
Web Interface

To create an IGMP filter profile and set its access mode:
1. Click Multicast, Multicast Statting.

2. Click IGMP Filtering Profile.



3. Set IGMP Filtering Profile



Parameters

These parameters are displayed:

Add

- Profile ID – Creates an IGMP profile. (Range: 1-999)
- Profile Limit – Sets the access mode of the profile; either permit or deny. (Default: Deny)

When the access mode is set to permit, IGMP join reports are processed when a multicast group falls within the controlled range. When the access mode is set to deny, IGMP join reports are only processed when the multicast group is not in the controlled range.

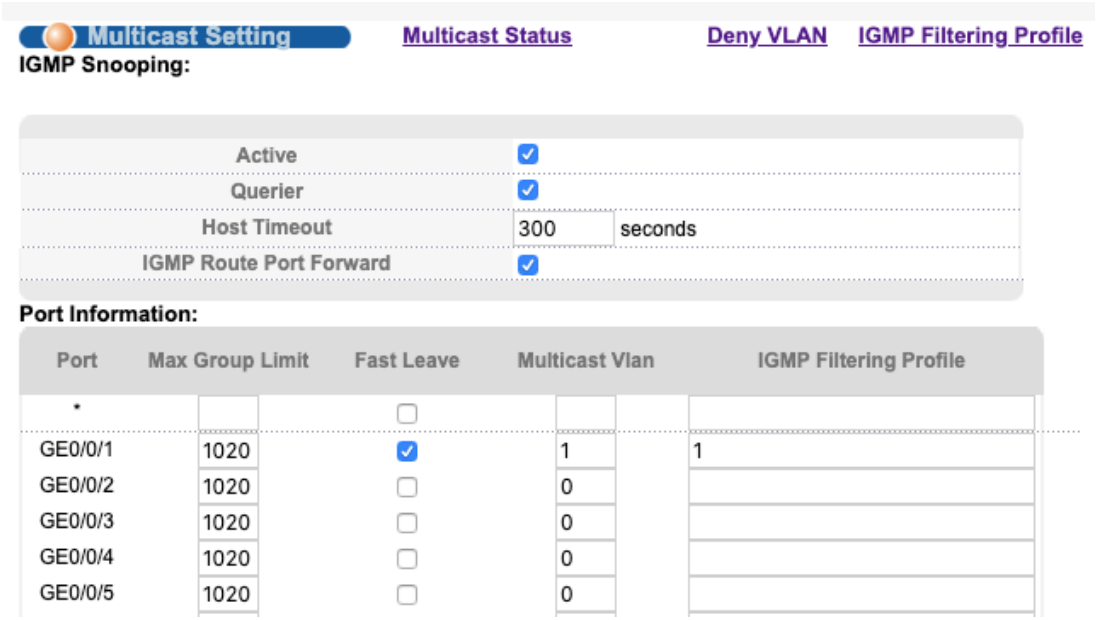
Add Multicast Group Range

- Profile ID – Selects an IGMP profile to configure.
- Start Address (Start Multicast IP Address) – Specifies the starting address of a range of multicast groups.
- End Address (End Multicast IP Address) – Specifies the ending address of a range of multicast groups.
- VLAN – Specifies the VLAN ID of a range of multicast groups.

4. Select Add from the Action list.
5. Enter the number for a profile, and set its access mode.
6. Click Apply.
7. Click Save.

Multicast Settings

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

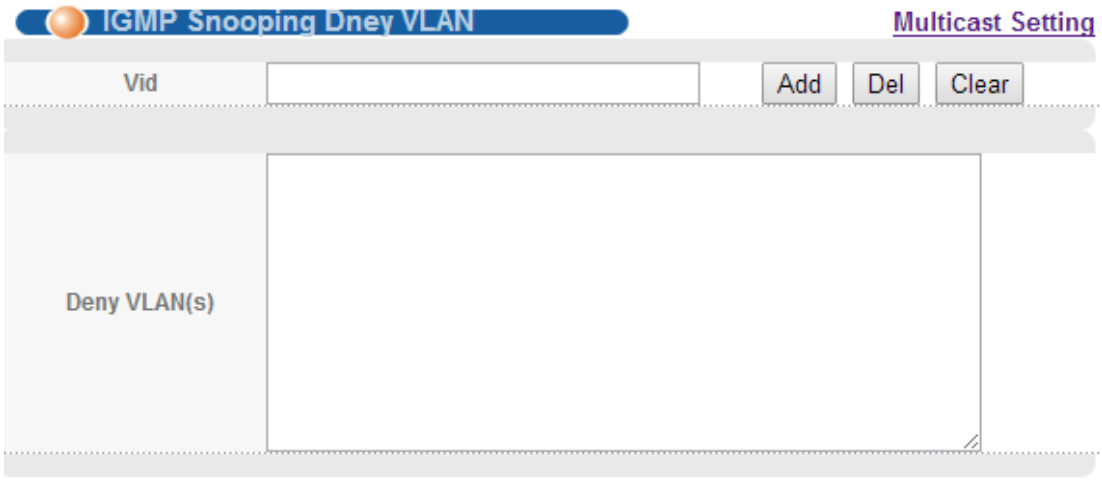


【Parameter Description】

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

IGMP Snooping Dney VLAN

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

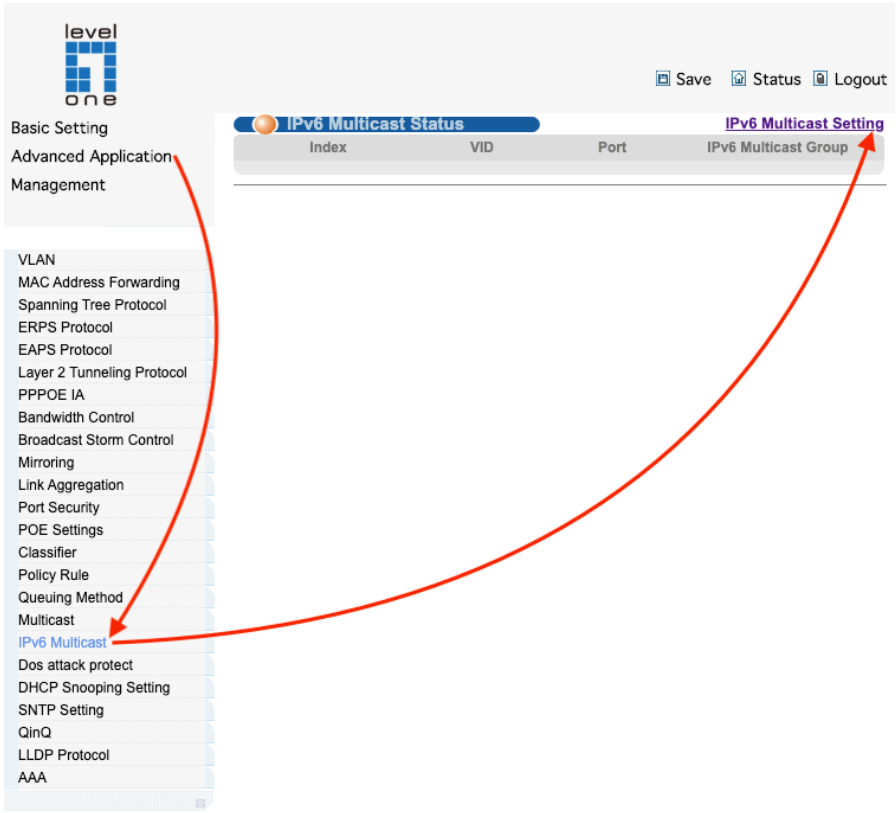


【Parameter Description】

Parameter	Description
Vid	Vlan’s ID

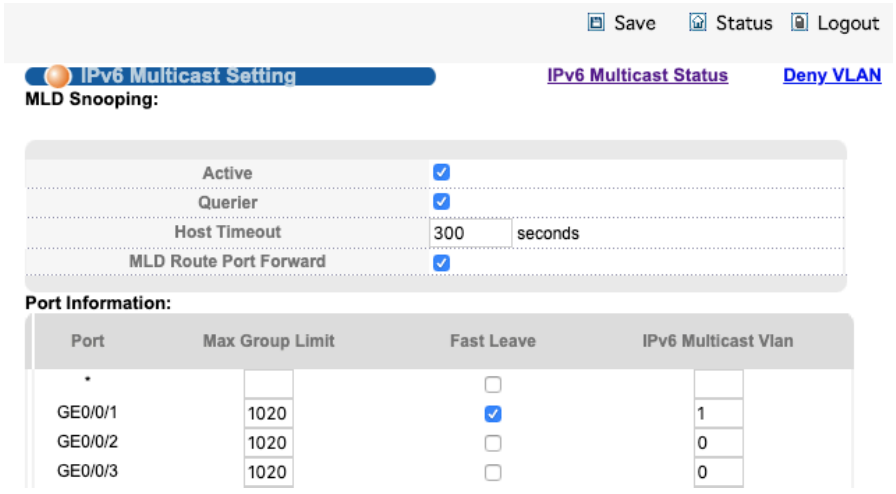
18. IPv6 Multicast

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



IPv6 Multicast Setting

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

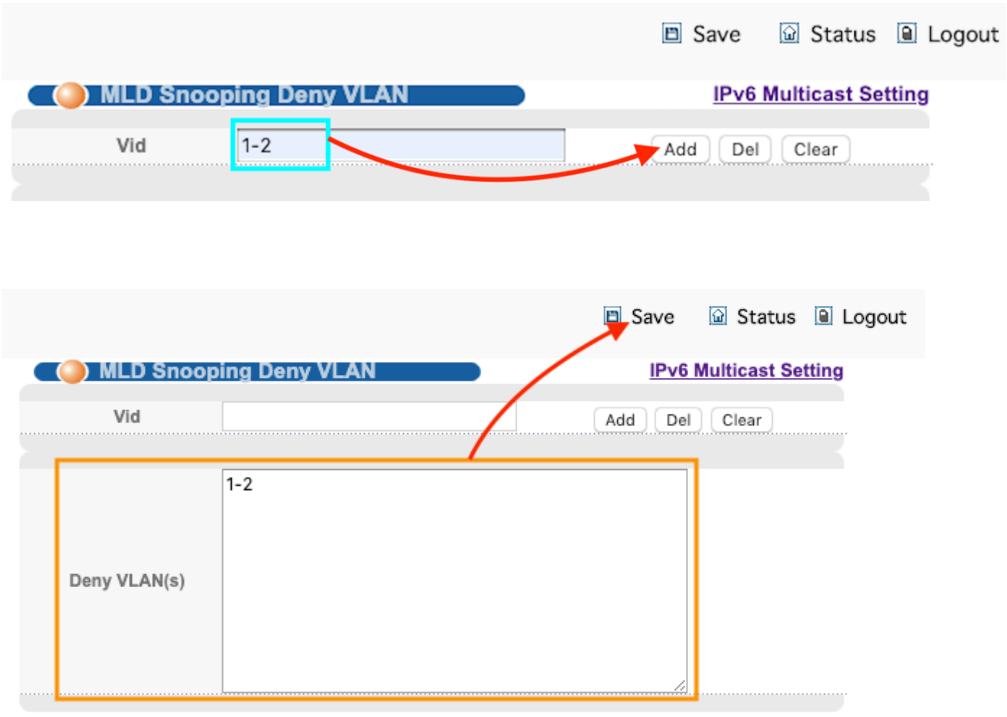


【Parameter Description】

Parameter	Description
Active	Enable or disable MLD snooping
Querier	Enable or disable MLD snooping timed Querier
Host Timeout	Configure Dynamic IPv6 multicast aging time (default 300s)
MLD Route Port Forward	Enable or disable MLD Route Port Forward
Port	Specifies the interface assigned to a multicast group.
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	Specifies the VLAN which is to propagate the multicast service. (Range: 1-4094)

MLD Snooping Dney VLAN

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



【Parameter Description】

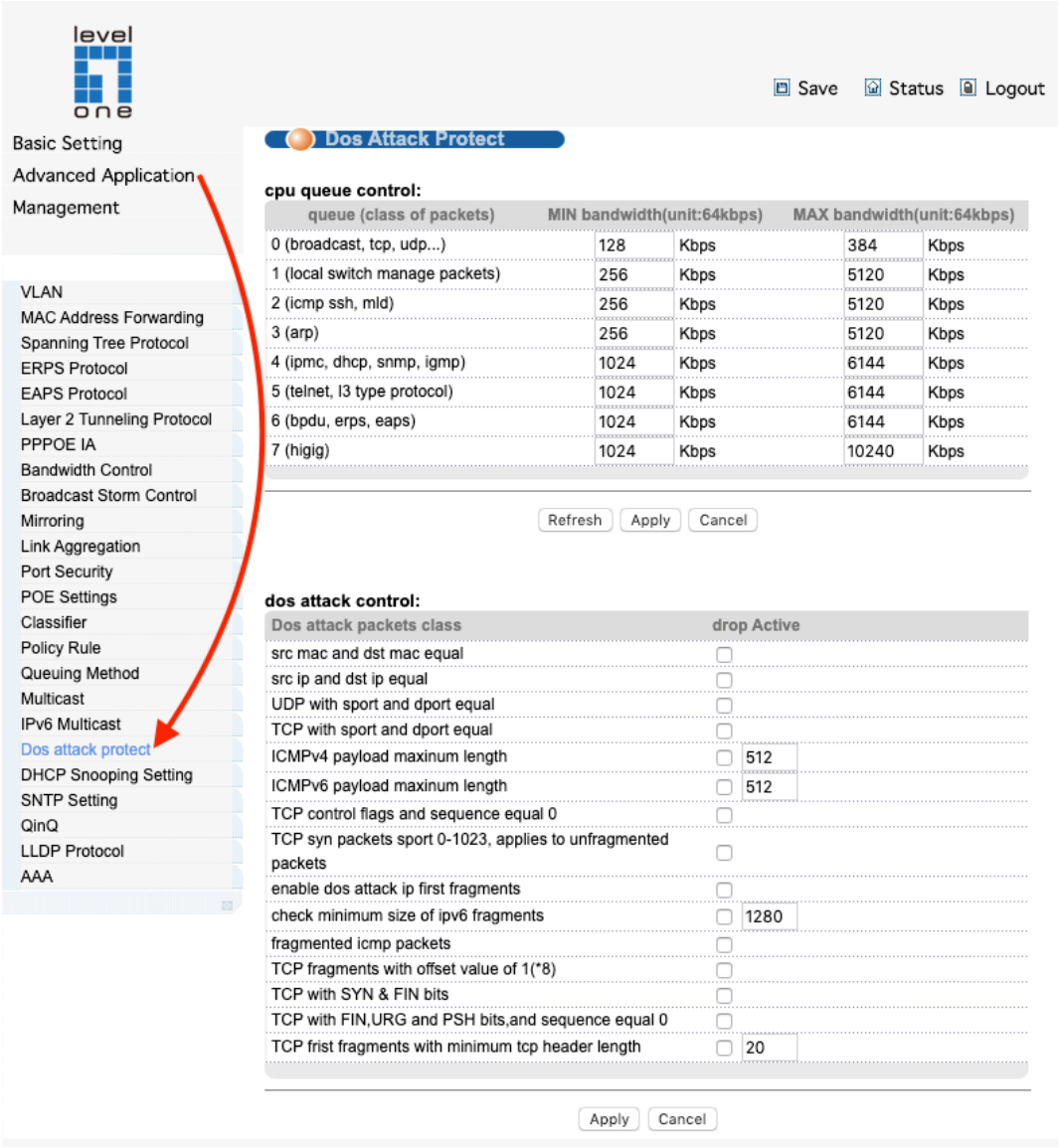
Parameter	Description
Vid	Vlan ID

19. Dos attack protect

Use the Advanced Application > Dos Attack Protect to protect against denial-of-service (DoS) attacks. A DoS attack is an attempt to block the services provided by a computer or network resource. This kind of attack tries to prevent an Internet site or service from functioning efficiently or at all. In general, DoS attacks are implemented by either forcing the target to reset, to consume most of its resources so that it can no longer provide its intended service, or to obstruct the communication media between the intended users and the target so that they can no longer communicate adequately. This section describes how to protect against DoS attacks.

This section describes how to protect against DoS attacks.

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



【Parameter Description】

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

Parameters

These parameters are displayed:

◆ UDP Flooding Attack – Attacks in which a perpetrator sends a large number of UDP packets (with or without a spoofed-Source IP) to random ports on a remote host. The target will determine that application is listening at that port, and reply with an ICMP Destination Unreachable packet. It will be forced to send many ICMP packets, eventually leading it to be unreachable by other clients. (Default: Disabled)

◆ UDP Flooding Attack Rate – Maximum allowed rate. (Range: 64-2000 kbits/ second; Default: 1000 kbits/second)

◆ TCP Flooding Attack – Attacks in which a perpetrator sends a succession of TCP SYN requests (with or without a spoofed-Source IP) to a target and never returns ACK packets. These half-open connections will bind resources on the target, and no new connections can be made, resulting in a denial of service. (Default: Disabled)

◆ TCP Flooding Attack Rate – Maximum allowed rate. (Range: 64-2000 kbits/ second; Default: 1000 kbits/second)

◆ TCP Null Scan – A TCP NULL scan message is used to identify listening TCP ports. The scan uses a series of strangely configured TCP packets which contain a sequence number of 0 and no flags. If the target's TCP port is closed, the target replies with a TCP RST (reset) packet. If the target TCP port is open, it simply discards the TCP NULL scan. (Default: Enabled)

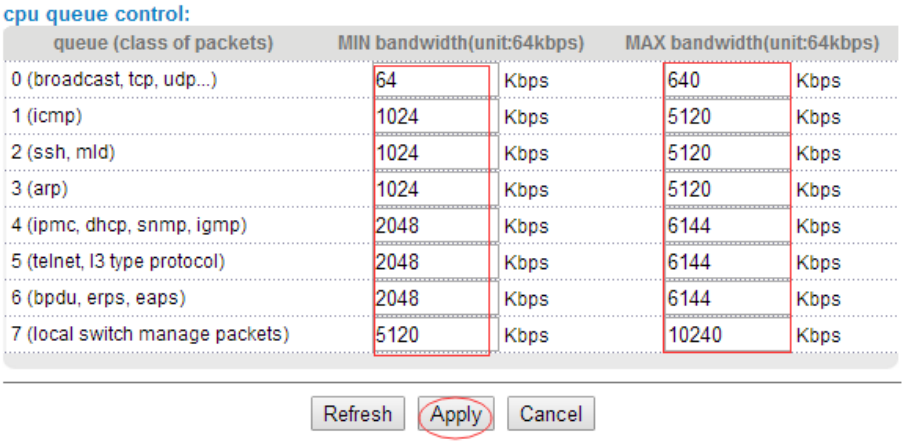
◆ TCP-SYN/FIN Scan – A TCP SYN/FIN scan message is used to identify listening TCP ports. The scan uses a series of strangely configured TCP packets which contain SYN (synchronize) and FIN (finish) flags. If the target's TCP port is closed, the target replies with a TCP RST (reset) packet. If the target TCP port is open, it simply discards the TCP SYN FIN scan. (Default: Enabled)

◆ TCP Xmas Scan – A so-called TCP XMAS scan message is used to identify listening TCP ports. This scan uses a series of strangely configured TCP packets which contain a sequence number of 0 and the URG, PSH and FIN flags. If the target's TCP port is closed, the target replies with a TCP RST packet. If the target TCP port is open, it simply discards the TCP XMAS scan. (Default: Enabled)

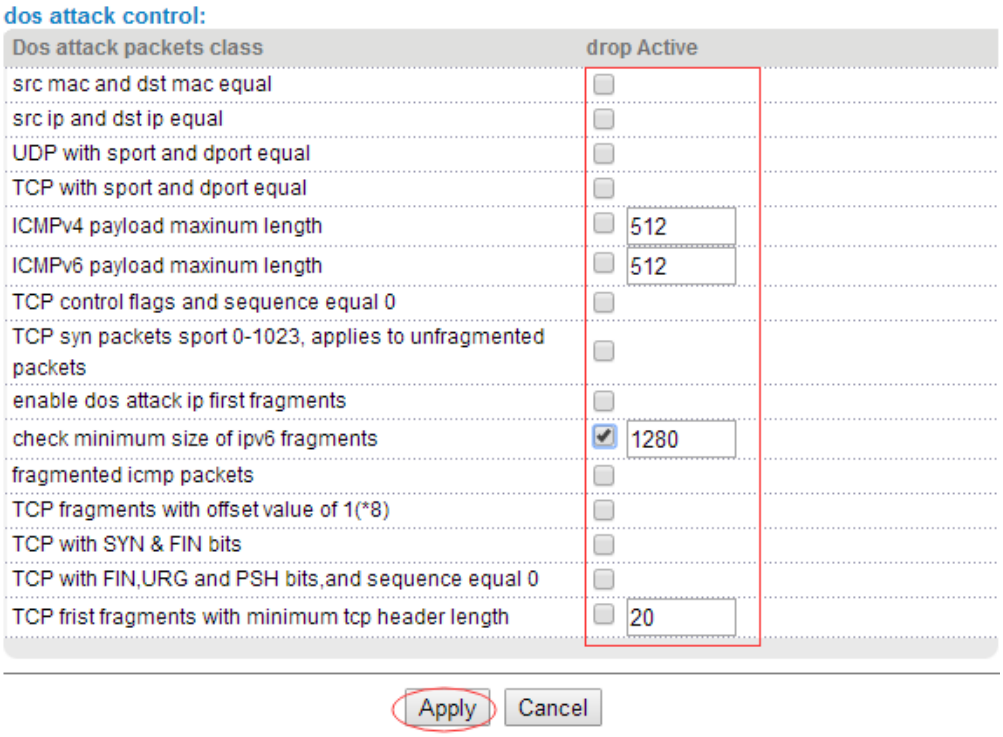
Web Interface

To protect against DoS attacks:

1. Click Security, DoS Protection.
2. Enable protection for specific DoS attacks, and set the maximum allowed rate as required.
3. Click Apply
4. Click Save



2.dos attack control



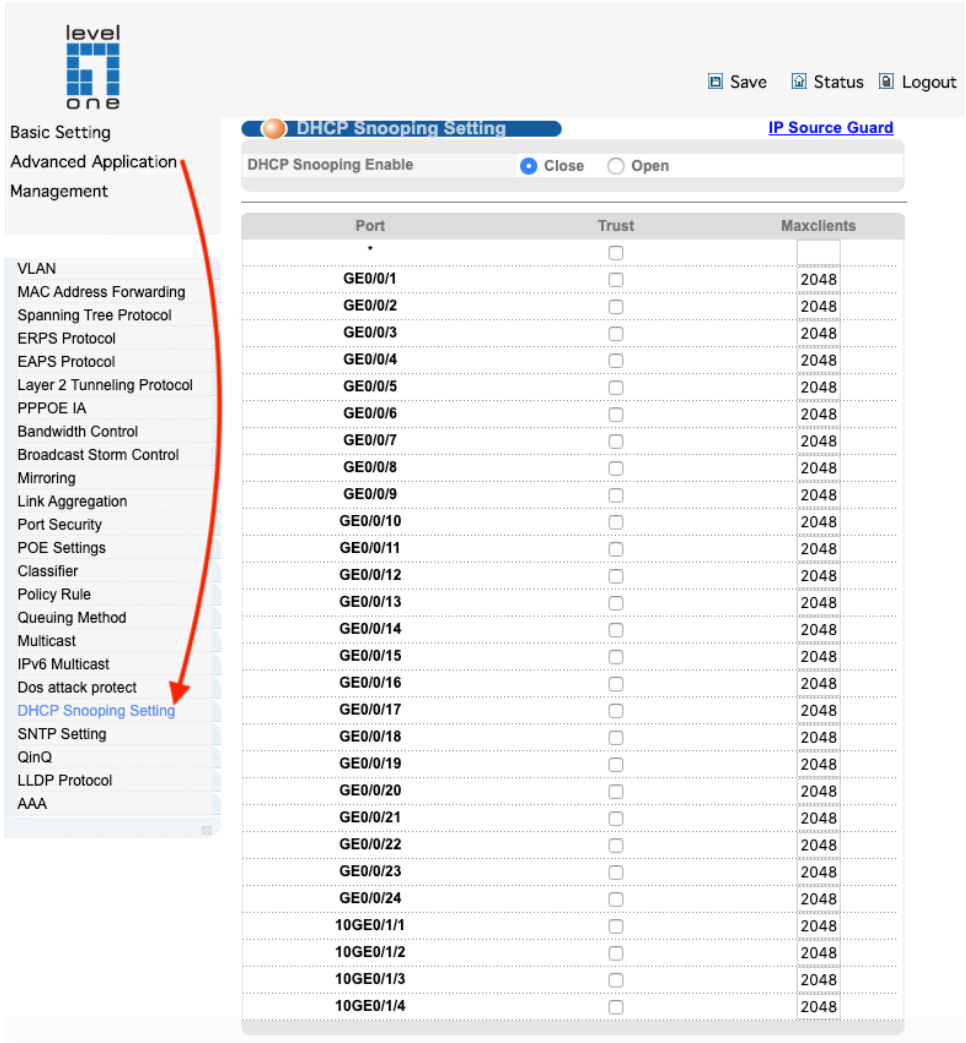
20. DHCP Snooping Setting

The addresses assigned to DHCP clients on insecure ports can be carefully controlled using the dynamic bindings registered with DHCP Snooping (or using the static bindings configured with IP Source Guard). DHCP snooping allows a switch to protect a network from rogue DHCP servers or other devices which send port-related information to a DHCP server. This information can be useful in tracking an IP address back to a physical port.

Network traffic may be disrupted when malicious DHCP messages are received from an outside source. DHCP snooping is used to filter DHCP messages received on a non-secure interface from outside the network or fire wall. When DHCP snooping is enabled globally and enabled on a VLAN interface, DHCP messages received on an untrusted interface from a device not listed in the DHCP snooping table will be dropped.

This section describes how to DHCP Snooping Setting：

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



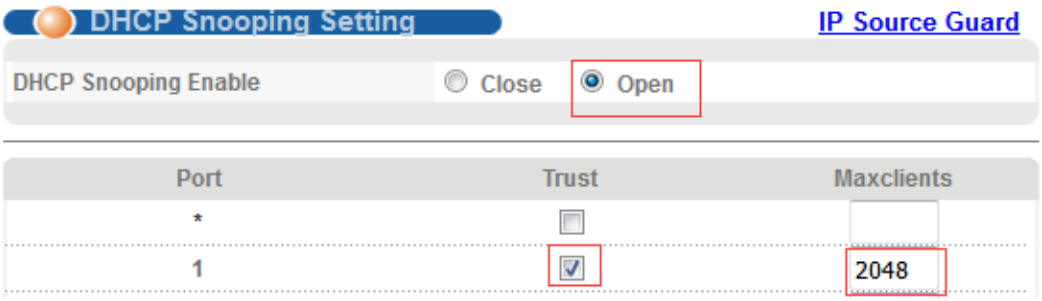
DHCP Snooping Setting

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

【Parameter Description】

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

【Configuration Example】

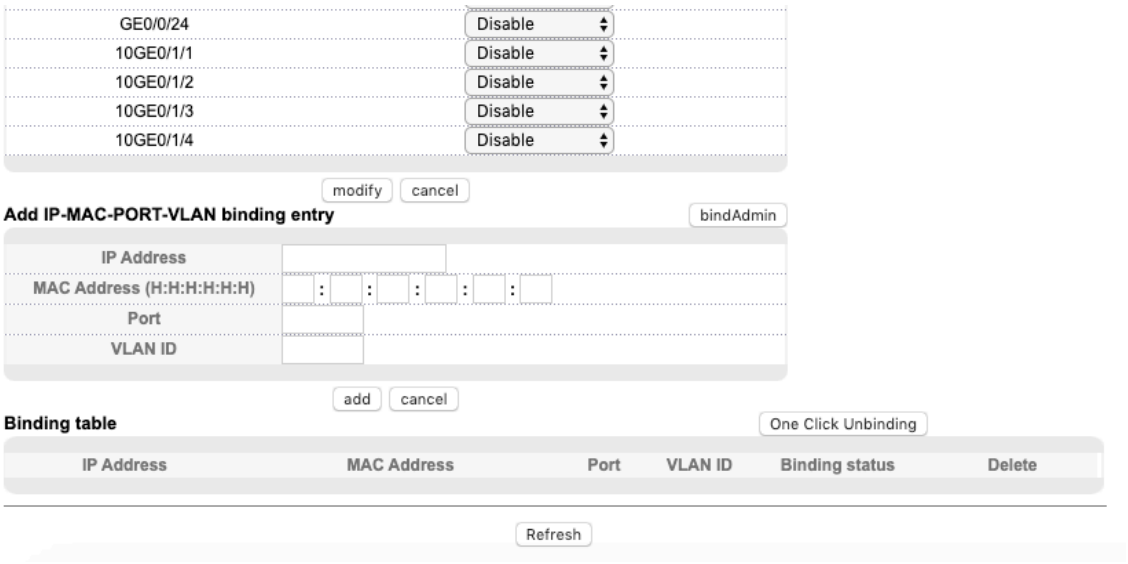


IP Source Guard

If IP source guard is enabled, an inbound packet's IP address (SIP option) or both its IP address and corresponding MAC address (SIP-MAC option) will be checked against the binding table. If no matching entry is found, the packet will be dropped.

This section describes how to IP source guard：

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



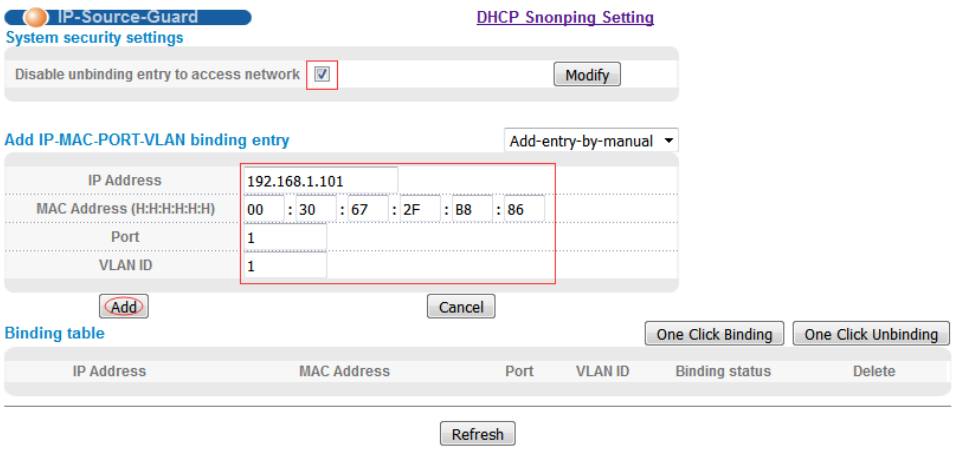
【Parameter Description】

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

【Instructions】

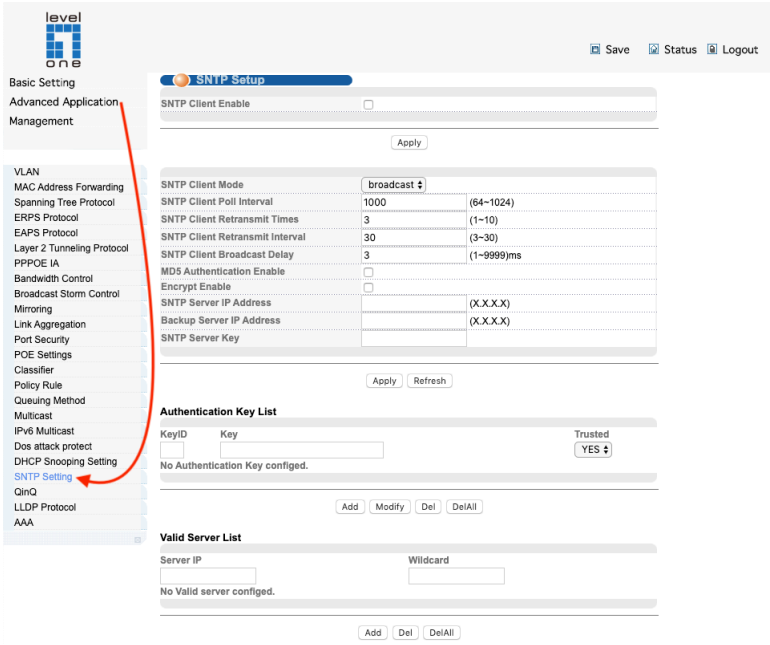
If you want to access shall be binding and switch the IP address of the same network segment.

【Configuration Example】



21. SNTP Setting

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



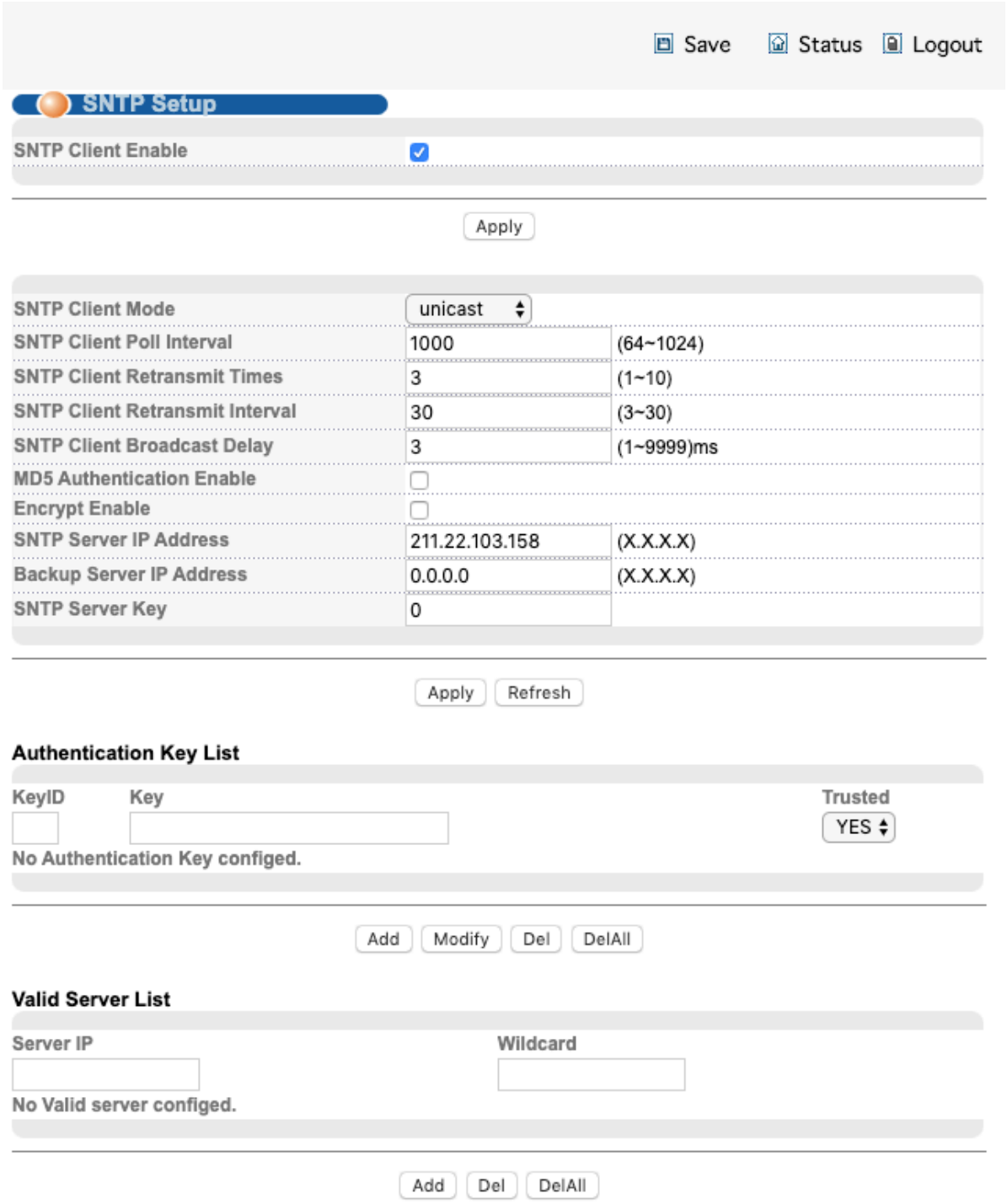
【Parameter Description】

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

【Instructions】

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

【Configuration Example】



22. QinQ

IEEE 802.1Q Tunneling

IEEE 802.1Q Tunneling (QinQ) is designed for service providers carrying traffic for multiple customers across their networks. QinQ tunneling is used to maintain customer-specific VLAN and Layer 2 protocol configurations even when different customers use the same internal VLAN IDs. This is accomplished by inserting Service Provider VLAN (SPVLAN) tags into the customer's frames when they enter the service provider's network, and then stripping the tags when the frames leave the network.

A service provider's customers may have specific requirements for their internal VLAN IDs and number of VLANs supported. VLAN ranges required by different customers in the same service-provider network might easily overlap, and traffic passing through the infrastructure might be mixed. Assigning a unique range of VLAN IDs to each customer would restrict customer configurations, require intensive processing of VLAN mapping tables, and could easily exceed the maximum VLAN limit of 4096.

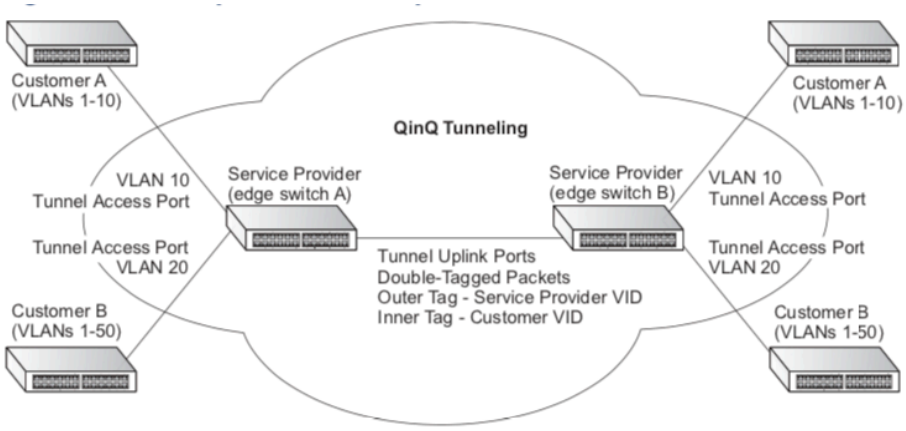
QinQ tunneling uses a single Service Provider VLAN (SPVLAN) for customers who have multiple VLANs. Customer VLAN IDs are preserved and traffic from different customers is segregated within the service provider's network even when they use the same customer-specific VLAN IDs. QinQ tunneling expands VLAN space by using a VLAN-in-VLAN hierarchy, preserving the customer's original tagged packets, and adding SPVLAN tags to each frame (also called double tagging).

A port configured to support QinQ tunneling must be set to tunnel port mode. The Service Provider VLAN (SPVLAN) ID for the specific customer must be assigned to the QinQ tunnel access port on the edge switch where the customer traffic enters the service provider's network. Each customer requires a separate SPVLAN, but this VLAN supports all of the customer's internal VLANs. The QinQ tunnel uplink port that passes traffic from the edge switch into the service provider's metro network must also be added to this SPVLAN. The uplink port can be added to multiple SPVLANs to carry inbound traffic for different customers onto the service provider's network.

When a double-tagged packet enters another trunk port in an intermediate or core switch in the service provider's network, the outer tag is stripped for packet processing. When the packet exits another trunk port on the same core switch, the same SPVLAN tag is again added to the packet.

When a packet enters the trunk port on the service provider's egress switch, the outer tag is again stripped for packet processing. However, the SPVLAN tag is not added when it is sent out the tunnel access port on the edge switch into the customer's network. The packet is sent as a normal IEEE 802.1Q-tagged frame, preserving the original VLAN numbers used in the customer's network.

Figure : QinQ Operational Concept



Layer 2 Flow for Packets Coming into a Tunnel Access Port

A QinQ tunnel port may receive either tagged or untagged packets. No matter how many tags the incoming packet has, it is treated as tagged packet.

The ingress process does source and destination lookups. If both lookups are successful, the ingress process writes the packet to memory. Then the egress process transmits the packet. Packets entering a QinQ tunnel port are processed in the following manner:

1. An SPVLAN tag is added to all outbound packets on the SPVLAN interface, no matter how many tags they already have. The switch constructs and inserts the outer tag (SPVLAN) into the packet based on the default VLAN ID and Tag Protocol Identifier (TPID, that is, the ether-type of the tag), The priority of the inner tag is copied to the outer tag if it is a tagged or priority tagged packet.

2.After successful source and destination lookup, the ingress process sends the packet to the switching process with two tags. If the incoming packet is untagged, the outer tag is an SPVLAN tag, and the inner tag is a dummy tag (8100 0000). If the incoming packet is tagged, the outer tag is an SPVLAN tag, and the inner tag is a CVLAN tag.

3. After packet classification through the switching process, the packet is written to memory with one tag (an outer tag) or with two tags (both an outer tag and inner tag).
4. The switch sends the packet to the proper egress port.
5. If the egress port is an untagged member of the SPVLAN, the outer tag will be

stripped. If it is a tagged member, the outgoing packets will have two tags.

Layer 2 Flow for Packets Coming into a Tunnel Uplink Port

An uplink port receives one of the following packets:

- Untagged
- One tag (CVLAN or SPVLAN)
- Double tag (CVLAN + SPVLAN)

The ingress process does source and destination lookups. If both lookups are successful, the ingress process writes the packet to memory. Then the egress process transmits the packet. Packets entering a QinQ uplink port are processed in

the following manner:

1. If incoming packets are untagged, the PVID VLAN native tag is added.

2. If the ether-type of an incoming packet (single or double tagged) is not equal to the TPID of the uplink port, the VLAN tag is determined to be a Customer VLAN (CVLAN) tag. The uplink port's PVID VLAN native tag is added to the packet. This outer tag is used for learning and switching packets within the service provider's network. The TPID must be configured on a per port basis, and the verification cannot be disabled.

3. If the ether-type of an incoming packet (single or double tagged) is equal to the TPID of the uplink port, no new VLAN tag is added. If the uplink port is not the member of the outer VLAN of the incoming packets, the packet will be dropped when ingress filtering is enabled. If ingress filtering is not enabled, the packet will still be forwarded. If the VLAN is not listed in the VLAN table, the packet will be dropped.

4. After successful source and destination lookups, the packet is double tagged. The switch uses the TPID of 0x8100 to indicate that an incoming packet is double-tagged. If the outer tag of an incoming double-tagged packet is equal to the port TPID and the inner tag is 0x8100, it is treated as a double-tagged packet. If a single-tagged packet has 0x8100 as its TPID, and port TPID is not 0x8100, a new VLAN tag is added and it is also treated as double-tagged packet.

5. If the destination address lookup fails, the packet is sent to all member ports of the outer tag's VLAN.

6. After packet classification, the packet is written to memory for processing as a single-tagged or double-tagged packet.

7. The switch sends the packet to the proper egress port.

8. If the egress port is an untagged member of the SPVLAN, the outer tag will be stripped. If it is a tagged member, the outgoing packet will have two tags.

Configuration Limitations for QinQ

◆ The native VLAN of uplink ports should not be used as the SPVLAN. If the SPVLAN is the uplink port's native VLAN, the uplink port must be an untagged member of the SPVLAN. Then the outer SPVLAN tag will be stripped when the packets are sent out. Another reason is that it causes non-customer packets to be forwarded to the SPVLAN.

◆ Static trunk port groups are compatible with QinQ tunnel ports as long as the QinQ configuration is consistent within a trunk port group.

◆ The native VLAN (VLAN 1) is not normally added to transmitted frames. Avoid using VLAN 1 as an SPVLAN tag for customer traffic to reduce the risk of misconfiguration. Instead, use VLAN 1 as a management VLAN instead of a data VLAN in the service provider network.

◆ There are some inherent incompatibilities between Layer 2 and Layer 3 switching:

Tunnel ports do not support IP Access Control Lists.

Layer 3 Quality of Service (QoS) and other QoS features containing Layer 3 information are not supported on tunnel ports.

Spanning tree bridge protocol data unit (BPDU) filtering is automatically disabled on a tunnel port.

General Configuration Guidelines for QinQ

1. Enable Tunnel Status, and set the Tag Protocol Identifier (TPID) value of the tunnel access port (in the Ethernet Type field). This step is required if the attached client is using a nonstandard 2-byte ethertype to identify 802.1Q tagged frames. The default ethertype value is 0x8100.

2. Create a Service Provider VLAN, also referred to as an SPVLAN.

3. Configure the QinQ tunnel access port to Access mode.

4. Configure the QinQ tunnel access port to join the SPVLAN as an untagged member.

5. Configure the SPVLAN ID as the native VID on the QinQ tunnel access port.

6. Configure the QinQ tunnel uplink port to Uplink mode.

7. Configure the QinQ tunnel uplink port to join the SPVLAN as a tagged member

Enabling QinQ Tunneling on the Switch

Use the VLAN > Tunnel (Configure Global) page to configure the switch to operate in IEEE 802.1Q (QinQ) tunneling mode, which is used for passing Layer 2 traffic across a service provider's metropolitan area network. You can also globally set the Tag Protocol Identifier (TPID) value of the tunnel port if the attached client is using a nonstandard 2-byte ethertype to identify 802.1Q tagged frames.

Parameters

These parameters are displayed:

- **Tunnel Status** – Sets the switch to QinQ mode. (Default: Disabled)
- **Ethernet Type** – The Tag Protocol Identifier (TPID) specifies the ethertype of incoming packets on a tunnel port. (Range: hexadecimal 0800-FFFF; Default: 8100)

  Use this field to set a custom 802.1Q ethertype value for the 802.1Q Tunnel TPID. This feature allows the switch to interoperate with third-party switches that do not use the standard 0x8100 ethertype to identify 802.1Q-tagged frames. For example, if 0x1234 is set as the custom 802.1Q ethertype on a trunk port, incoming frames containing that ethertype are assigned to the VLAN contained in the tag following the ethertype field, as they would be with a standard 802.1Q trunk. Frames arriving on the port containing any other ethertype are looked upon as untagged frames, and assigned to the native VLAN of that port.

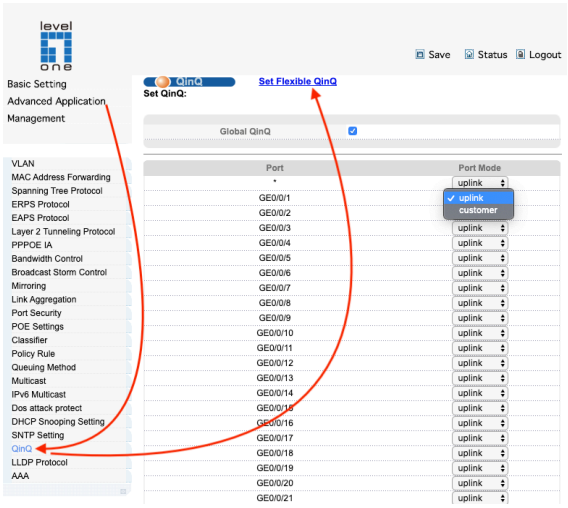
  The specified ethertype only applies to ports configured in Uplink mode. If the port is in normal mode, the TPID is always 8100. If the port is in Access mode, received packets are processes as untagged packets.

  Avoid using well-known ethertypes for the TPID unless you can eliminate all side effects. For example, setting the TPID to 0800 hexadecimal (which is used for IPv4) will interfere with management access through the web interface.

Web Interface

To enable QinQ Tunneling on the switch:

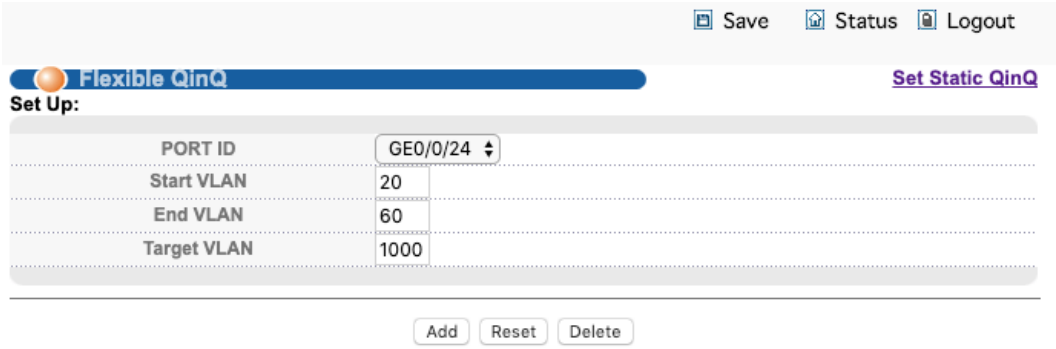
1. Click **Advanced Application**, **QinQ, Set Static QinQ** .



2. Select Configure Global from the Step list.

3. Enable Tunnel Status, and specify the TPID if a client attached to a tunnel port is using a non-standard ethertype to identify 802.1Q tagged frames.
4. Click Apply.
5. Click Save.

【Configuration Example】



23. LLDP Protocol

Link Layer Discovery Protocol

Link Layer Discovery Protocol (LLDP) is used to discover basic information about neighboring devices on the local broadcast domain. LLDP is a Layer 2 protocol that uses periodic broadcasts to advertise information about the sending device. Advertised information is represented in Type Length Value (TLV) format according to the IEEE 802.1AB standard, and can include details such as device identification, capabilities and configuration settings. LLDP also defines how to store and maintain information gathered about the neighboring network nodes it discovers.

Link Layer Discovery Protocol - Media Endpoint Discovery (LLDP-MED) is an extension of LLDP intended for managing endpoint devices such as Voice over IP phones and network switches. The LLDP-MED TLVs advertise information such as network policy, power, inventory, and device location details. LLDP and LLDP-MED information can be used by SNMP applications to simplify troubleshooting, enhance network management, and maintain an accurate network topology.

Setting LLDP Timing Attributes

Use the Administration > LLDP (Configure Global) page to set attributes for general functions such as globally enabling LLDP on the switch, setting the message ageout time, and setting the frequency for broadcasting general advertisements or reports about changes in the LLDP MIB.

Parameters

These parameters are displayed:

- **LLDP** – Enables LLDP globally on the switch. (Default: Disabled)

- **Hello-time** (**Transmission Interval)** – Configures the periodic transmit interval for LLDP advertisements. (Range: 5-32768 seconds; Default: 30 seconds)

- **Hold-time** (**Hold Time Multiplier)** – Configures the time-to-live (TTL) value sent in LLDP advertisements as shown in the formula below. (Range: 2-10; Default: 4)

  The time-to-live tells the receiving LLDP agent how long to retain all information pertaining to the sending LLDP agent if it does not transmit updates in a timely manner.

  TTL in seconds is based on the following rule:

  minimum value ((Transmission Interval * Holdtime Multiplier), or 65535)

  Therefore, the default TTL is 4*30 = 120 seconds.

Web Interface

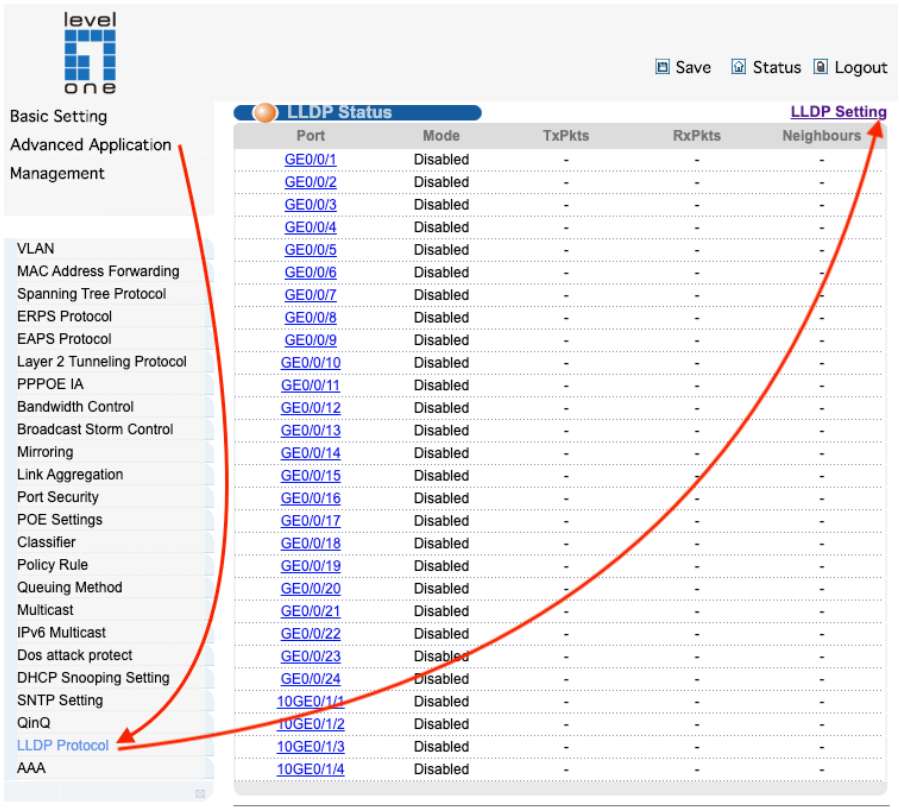
To configure LLDP timing attributes:

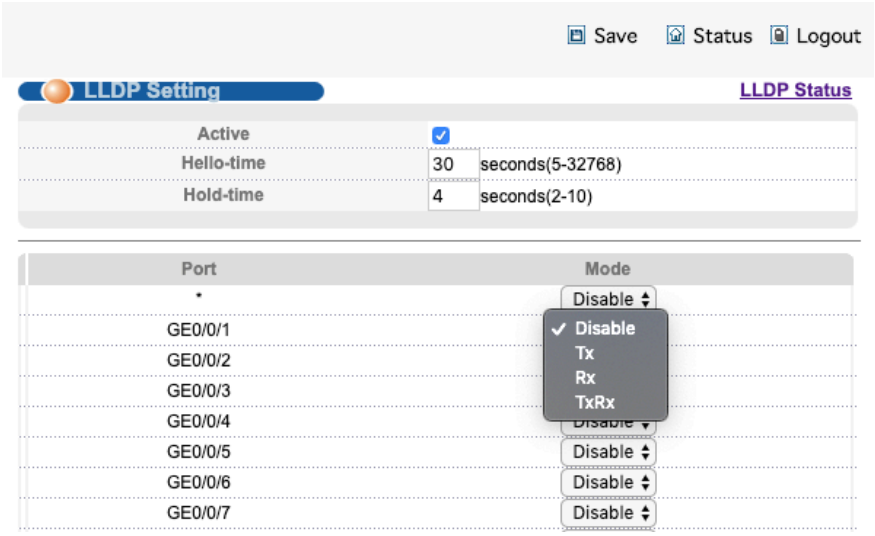
1. Click Administration, LLDP.

2. Select Configure Global from the Step list.

3. Enable LLDP, and modify any of the timing parameters as required.

4. Click Apply.





24. AAA

AAA (Authentication, Authorization and Accounting)

The authentication, authorization, and accounting (AAA) feature provides the main framework for configuring access control on the switch. The three security functions can be summarized as follows:

- Authentication — Identifies users that request access to the network.
- Authorization — Determines if users can access specific services.
- Accounting — Provides reports, auditing, and billing for services that users have accessed on the network.

The AAA functions require the use of configured RADIUS or TACACS+ servers in the network. The security servers can be defined as sequential groups that are applied as a method for controlling user access to specified services. For example, when the switch attempts to authenticate a user, a request is sent to the first server in the defined group, if there is no response the second server will be tried, and so on. If at any point a pass or fail is returned, the process stops.

The switch supports the following AAA features:

- Accounting for IEEE 802.1X authenticated users that access the network through the switch.
- Accounting for users that access management interfaces on the switch through the console and Telnet.
- Accounting for commands that users enter at specific CLI privilege levels.
- Authorization of users that access management interfaces on the switch through the console and Telnet.

To configure AAA on the switch, you need to follow this general process:

1. Configure RADIUS and TACACS+ server access parameters.
2. Define RADIUS and TACACS+ server groups to support the accounting and authorization of services.
3. Define a method name for each service to which you want to apply accounting or authorization and specify the RADIUS or TACACS+ server groups to use.
4. Apply the method names to port or line interfaces.

Note: This guide assumes that RADIUS and TACACS+ servers have already been configured to support AAA. The configuration of RADIUS and TACACS+ server software is beyond the scope of this guide, refer to the documentation provided with the RADIUS or TACACS+ server software.

Configuring Local/ Remote Logon Authentication

Use the Advanced Application > AAA > System Authentication page to specify local or remote authentication. Local authentication restricts management access based on user names and passwords manually configured on the switch. Remote authentication uses a remote access authentication server based on RADIUS or TACACS+ protocols to verify management access.

Command Usage

- By default, management access is always checked against the authentication database stored on the local switch. If a remote authentication server is used, you must specify the authentication sequence. Then specify the corresponding parameters for the remote authentication protocol using the Advanced Application > AAA > Server page. Local and remote logon authentication control management access via the console port, web browser, or Telnet.

- You can specify up to three authentication methods for any user to indicate the authentication sequence. For example, if you select (1) RADIUS, (2) TACACS and (3) Local, the user name and password on the RADIUS server is verified first. If the RADIUS server is not available, then authentication is attempted using the TACACS+ server, and finally the local user name and password is checked.

Parameters

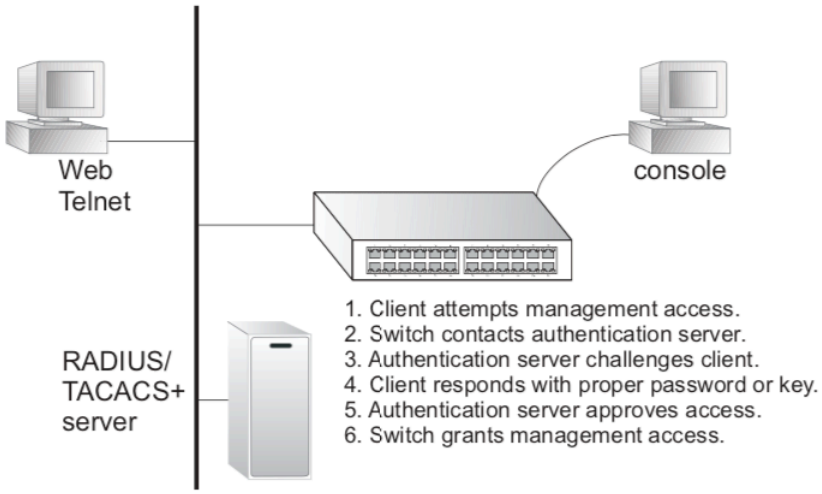
These parameters are displayed:

- **Authentication Sequence** – Select the authentication, or authentication sequence required:
  - **Local** – User authentication is performed only locally by the switch.
  - **RADIUS** – User authentication is performed using a RADIUS server only.
  - **TACACS** – User authentication is performed using a TACACS+ server only.
  - [authentication sequence] – User authentication is performed by up to three authentication methods in the indicated sequence.

Configuring Remote Logon Authentication Servers

Use the Advanced Application > AAA > Server page to configure the message exchange parameters for RADIUS or TACACS+ remote access authentication servers.
Remote Authentication Dial-in User Service (RADIUS) and Terminal Access Controller Access Control System Plus (TACACS+) are logon authentication protocols that use software running on a central server to control access to RADIUS- aware or TACACS-aware devices on the network. An authentication server contains a database of multiple user name/password pairs with associated privilege levels for each user that requires management access to the switch.

Figure : Authentication Server Operation



RADIUS uses UDP while TACACS+ uses TCP. UDP only offers best effort delivery, while TCP offers a more reliable connection-oriented transport. Also, note that RADIUS encrypts only the password in the access-request packet from the client to the server, while TACACS+ encrypts the entire body of the packet.

Command Usage

◆ If a remote authentication server is used, you must specify the message exchange parameters for the remote authentication protocol. Both local and remote logon authentication control management access via the console port, web browser, or Telnet.

◆ RADIUS and TACACS+ logon authentication assign a specific privilege level for each user name/password pair. The user name, password, and privilege level must be configured on the authentication server. The encryption methods used for the authentication process must also be configured or negotiated between the authentication server and logon client. This switch can pass authentication messages between the server and client that have been encrypted using MD5 (Message-Digest 5), TLS (Transport Layer Security), or TTLS (Tunneled Transport Layer Security).

Parameters

These parameters are displayed:
Configure Server

◆ RADIUS

• **Global** – Provides globally applicable RADIUS settings.

• **Server Index** – Specifies one of five RADIUS servers that may be configured. The switch attempts authentication using the listed sequence of servers. The process ends when a server either approves or denies access to a user.

- **Server IP Address** – Address of authentication server.
  (A Server Index entry must be selected to display this item.)

- **Accounting Server UDP Port** – Network (UDP) port on authentication server used for accounting messages. (Range: 1-65535; Default: 1813)

- **Authentication Server UDP Port** – Network (UDP) port on authentication server used for authentication messages. (Range: 1-65535; Default: 1812)

- **Authentication Timeout** – The number of seconds the switch waits for a reply from the RADIUS server before it resends the request.
  (Range: 1-65535; Default: 5)

- **Authentication Retries** – Number of times the switch tries to authenticate logon access via the authentication server. (Range: 1-30; Default: 2)

- **Set Key** – Mark this box to set or modify the encryption key.

- **Authentication Key** – Encryption key used to authenticate logon access for client. Enclose any string containing blank spaces in double quotes. (Maximum length: 48 characters)

- **Confirm Authentication Key** – Re-type the string entered in the previous field to ensure no errors were made. The switch will not change the encryption key if these two fields do not match.

◆ TACACS+

- **Global** – Provides globally applicable TACACS+ settings.

- **Server Index** – Specifies the index number of the server to be configured.
  The switch currently supports only one TACACS+ server.

- **Server IP Address** – Address of the TACACS+ server.
  (A Server Index entry must be selected to display this item.)

- **Authentication Server TCP Port** – Network (TCP) port of TACACS+ server used for authentication messages. (Range: 1-65535; Default: 49)

- **Authentication Timeout** – The number of seconds the switch waits for a reply from the TACACS+ server before it resends the request.
  (Range: 1-65535; Default: 5)

- **Authentication Retries** – Number of times the switch tries to authenticate logon access via the authentication server. (Range: 1-30; Default: 2)

- **Set Key** – Mark this box to set or modify the encryption key.

- **Authentication Key** – Encryption key used to authenticate logon access for client. Enclose any string containing blank spaces in double quotes. (Maximum length: 48 characters)

- **Confirm Authentication Key** – Re-type the string entered in the previous field to ensure no errors were made. The switch will not change the encryption key if these two fields do not match.

Configure Group

◆ **Server Type** – Select RADIUS or TACACS+ server.

◆ **Group Name** - Defines a name for the RADIUS or TACACS+ server group. (Range: 1-64 characters)

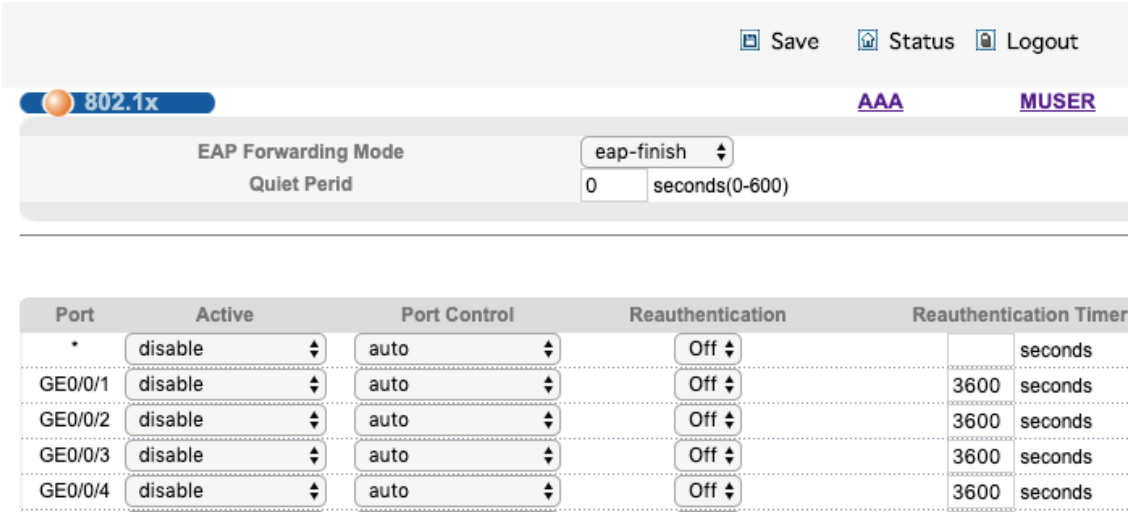
◆ **Sequence at Priority** - Specifies the server and sequence to use for the group. (Range: 1-5 for RADIUS; 1 for TACACS)

When specifying the priority sequence for a sever, the server index must already be defined

Web Interface

802.1x

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

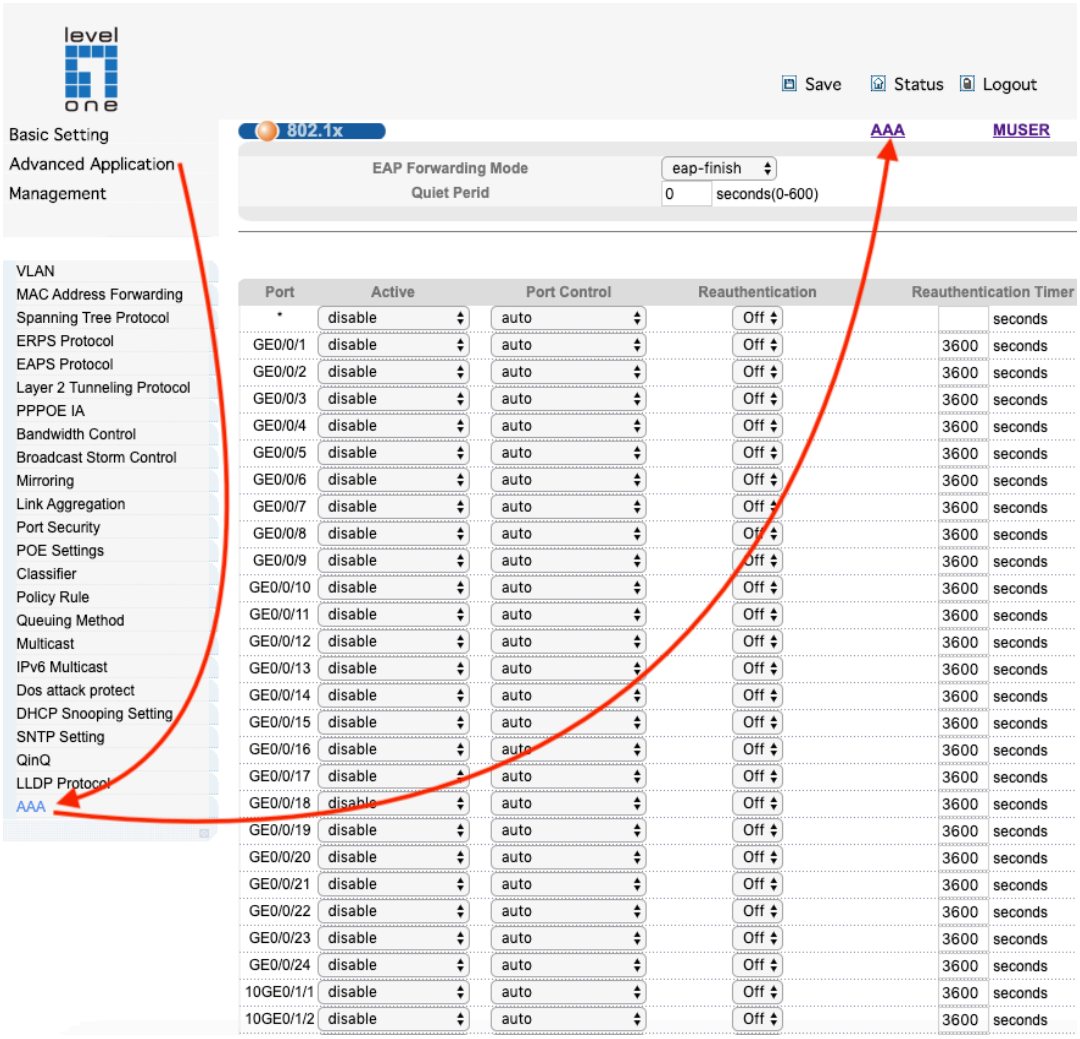


【Parameter Description】

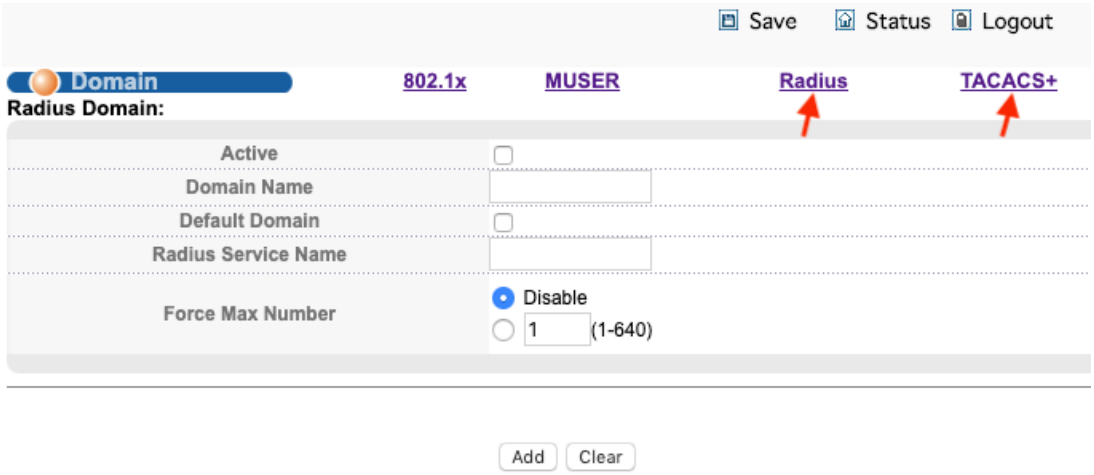
Parameter	Description
EAP Forwarding Mode	EAP Forwarding Mode : eap-finish, Eap-tansfer
Quiet Period	If the same user fails to log in more than the allowed value, he or she will not be allowed to try to log in at a certain time
Active	Active: disable portbased(multi) portbased(single) macbased
Port Control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

To configure the parameters for RADIUS or TACACS+ authentication:

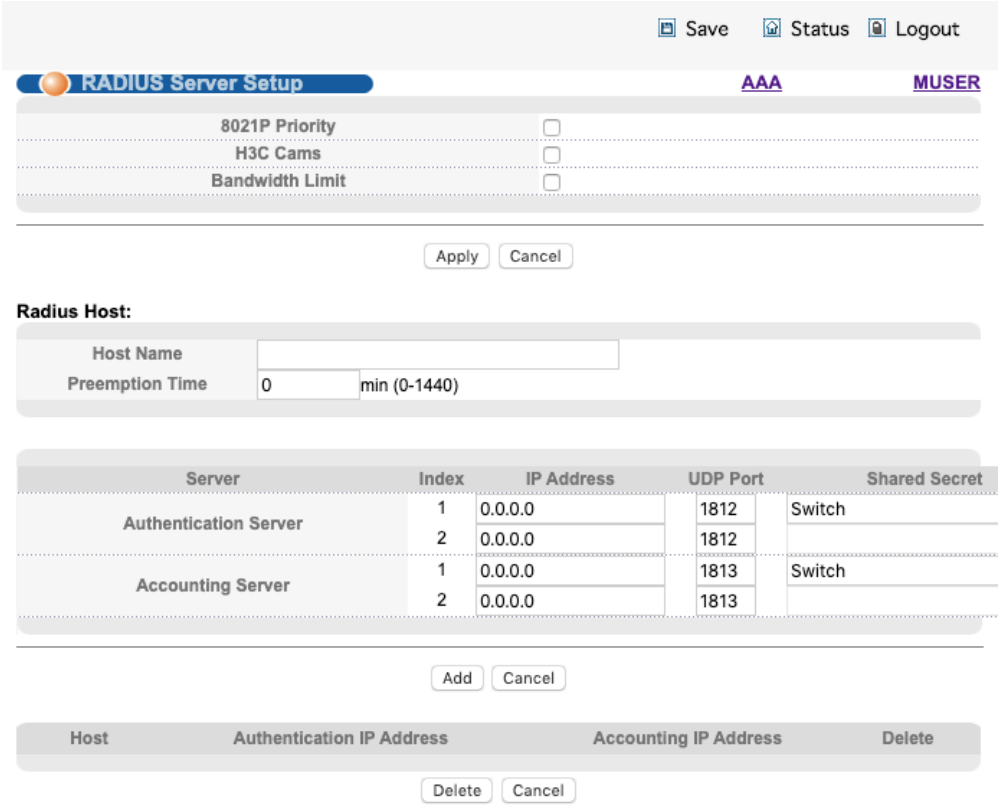
1. Click **Advanced Application**, AAA.



2. Select RADIUS or TACACS+ server type.



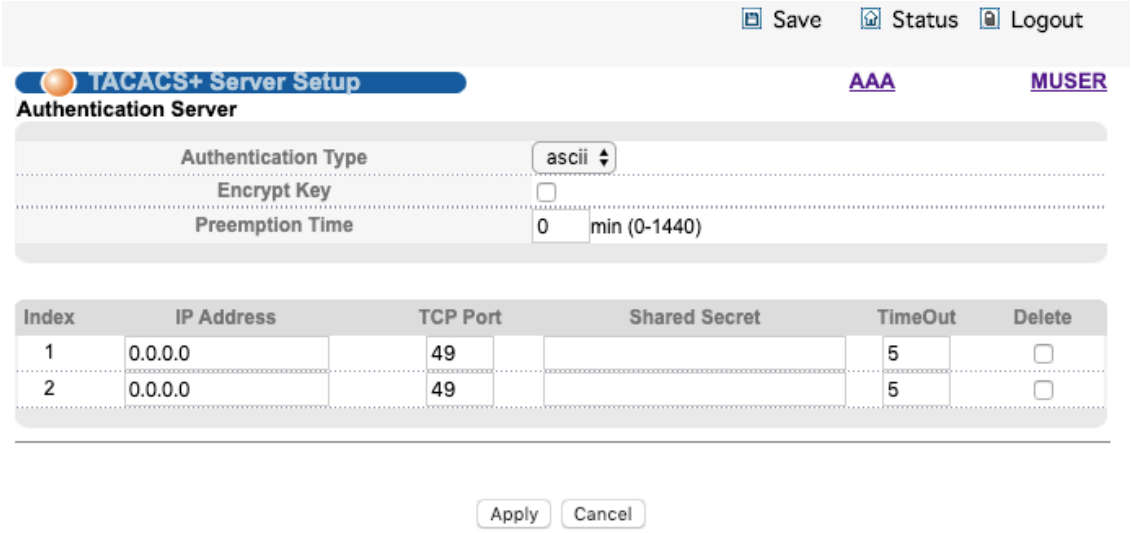
- **RADIUS Server Setup** – Select Global to specify the parameters that apply globally to all specified servers, or select a specific Server Index to specify the parameters that apply to a specific server.



【Parameter Description】

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

- **TACACS+ Server Setup** – Select Global to specify the parameters that apply globally to all specified servers, or select a specific Server Index to specify the parameters that apply to a specific server.

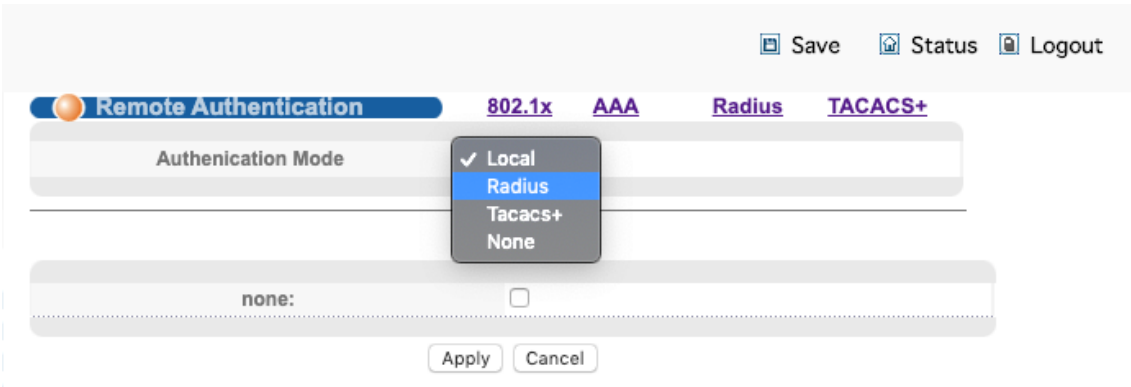


【Parameter Description】

Parameter	Description
Authenication Type	ascii (ASCII) chap pap (Password Authentication Protocol)
Preemption Time	The time range of Preemption Time: 0-1440 minutes

Radius Domain

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



【Parameter Description】

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

【Instructions】

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

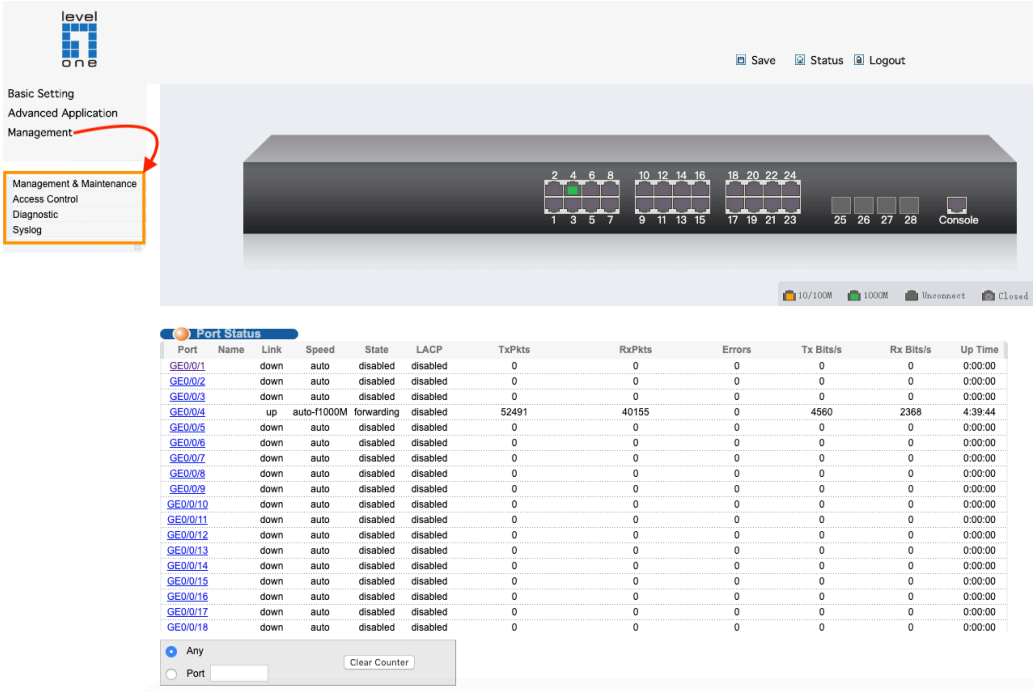
【Parameter Description】

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

Section III

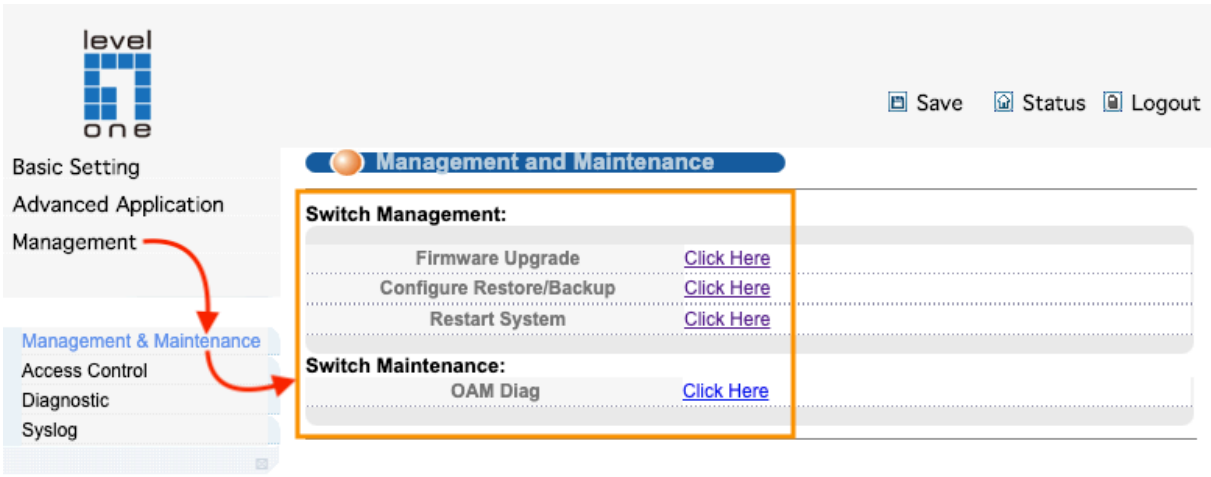
Management

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



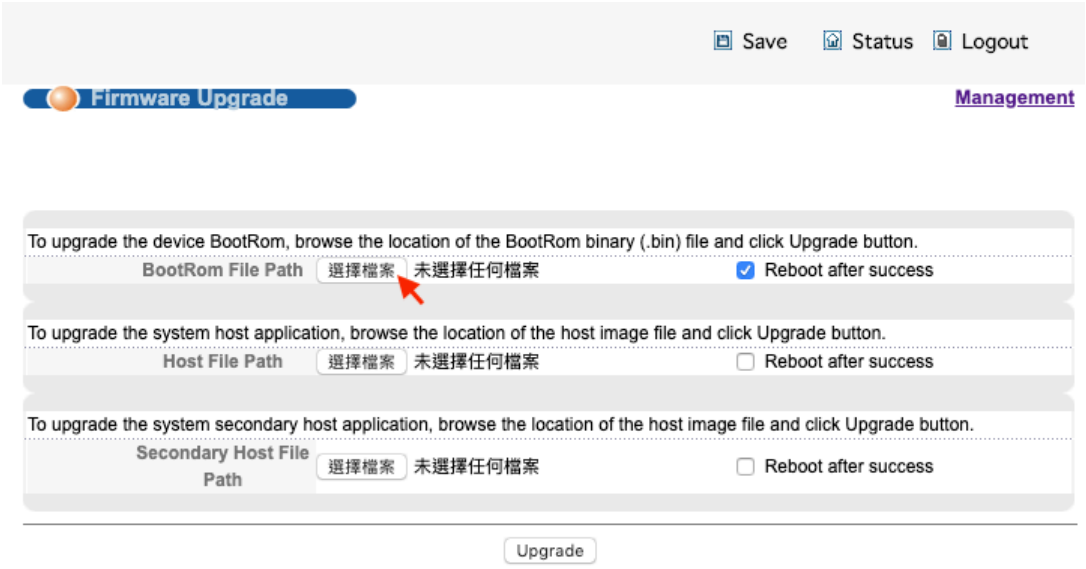
1. Management & Maintenance

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

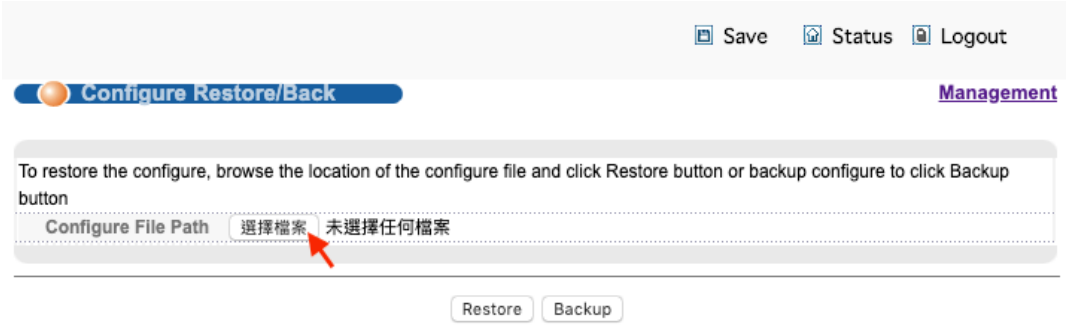


Switch Management :

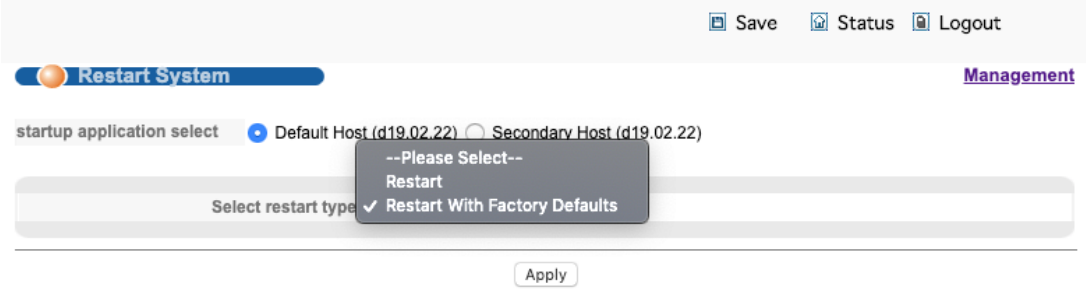
1.Firmware Upgrade



2. Configure Restore/Back



3. Restart System



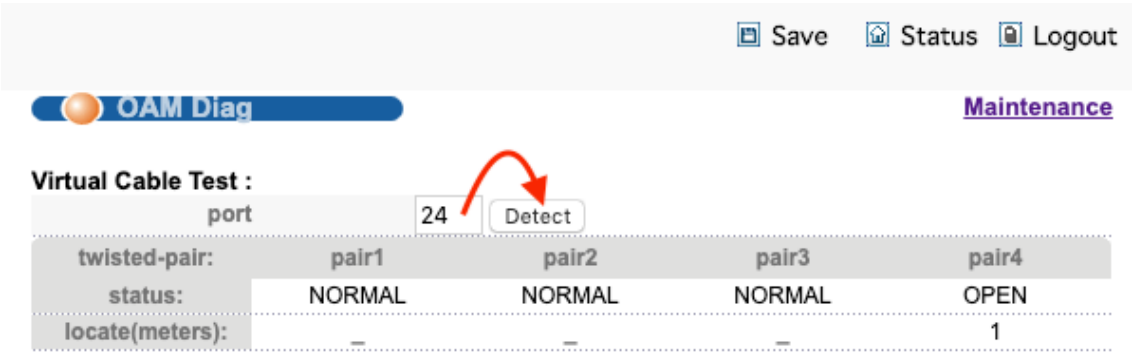
Switch Maintenance:

OAM Diag

Use the Management> Management & Maintenance > OAM Diag Test page to test the cable attached to a port. The cable test will check for any cable faults (short, open, etc.). If a fault is found, the switch reports the length to the fault. Otherwise, it reports the cable length. It can be used to determine the quality of the cable, connectors, and terminations. Problems such as opens, shorts, and cable impedance mismatch can be diagnosed with this test.

- Cable diagnostics can only be performed on twisted-pair media.
- This cable test is only accurate for Gigabit Ethernet cables 1 - 100 meters long.
- The test takes approximately 5 seconds. The switch displays the results of the test immediately upon completion, including common cable failures, as well as the status and approximate length to a fault.

Note: The SFP/SFP+ port does not support VCT!



2. Access Control

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

SNMP

Use the Management > Access Control > SNMP (Configure Trap) page to specify the host devices to be sent traps and the types of traps to send. Traps indicating status changes are issued by the switch to the specified trap managers. You must specify trap managers so that key events are reported by this switch to your management station (using network management software). You can specify up to 4 management stations that will receive authentication failure messages and other trap messages from the switch.

Command Usage

◆ Notifications are issued by the switch as trap messages by default. The recipient of a trap message does not send a response to the switch. Traps are therefore not as reliable as inform messages, which include a request for acknowledgement of receipt. Informs can be used to ensure that critical information is received by the host. However, note that informs consume more system resources because they must be kept in memory until a response is received. Informs also add to network traffic. You should consider these effects when deciding whether to issue notifications as traps or informs.

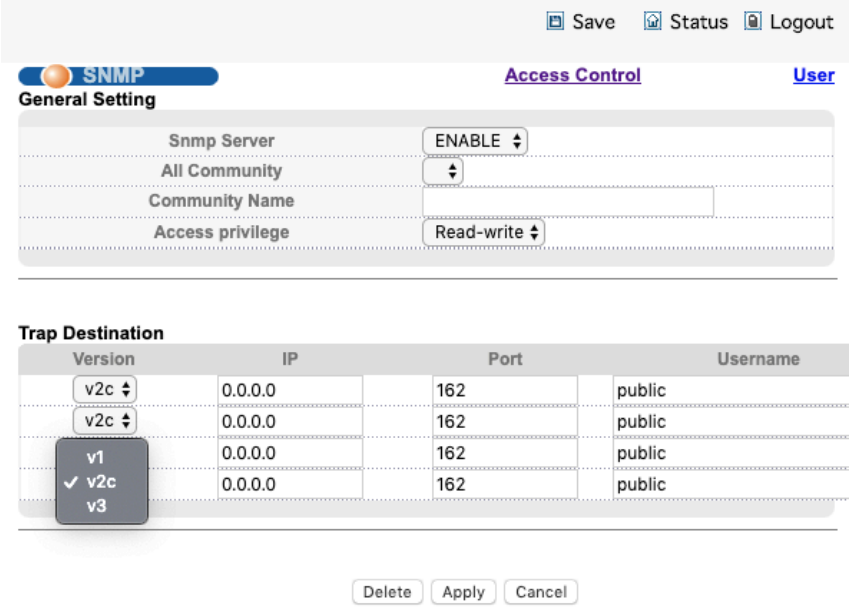
To send an inform to a SNMPv2c host, complete these steps:

1. Enable the SNMP agent.
2. Create a view with the required notification messages.
3. Configure the group (matching the community string specified on the Configure Trap - Add page) to include the required notify view.
4. Enable trap informs as described in the following pages.

To send an inform to a SNMPv3 host, complete these steps:

1. Enable the SNMP agent.
2. Create a remote SNMPv3 user to use in the message exchange process. If the user specified in the trap configuration page does not exist, an SNMPv3 group will be automatically created using the name of the specified remote user, and default settings for the read, write, and notify view.
3. Create a view with the required notification messages.
4. Create a group that includes the required notify view.
5. Enable trap informs as described in the following pages.

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

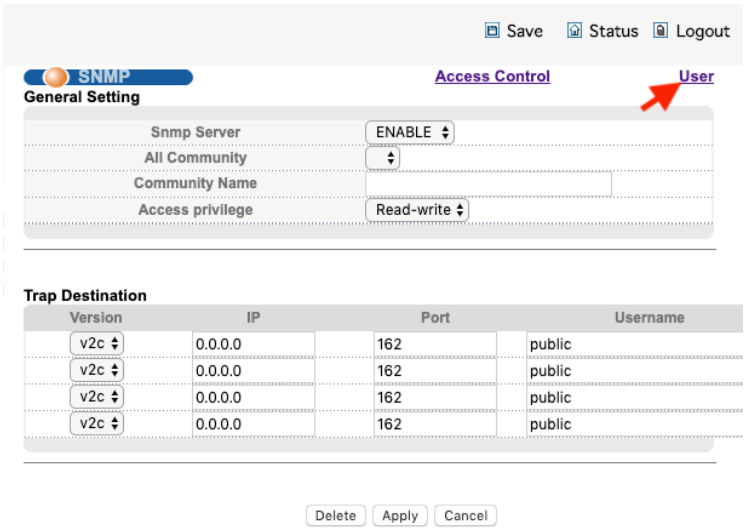


【Parameter Description】

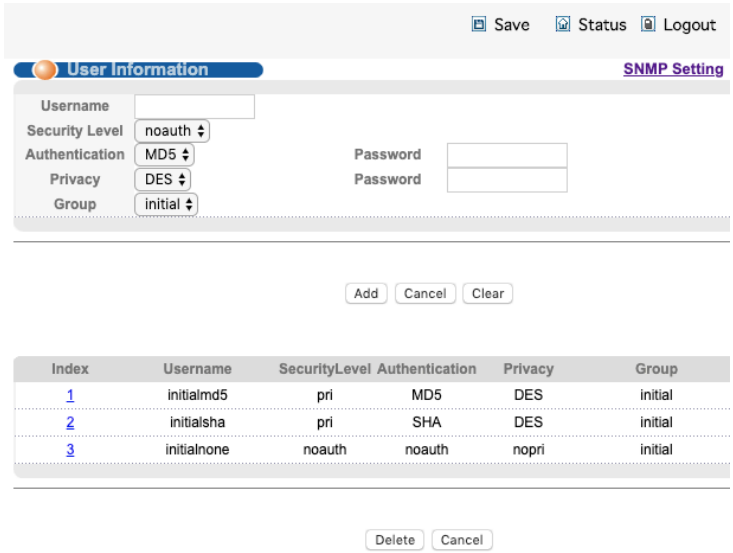
Parameter	Description
Community Name	Community string, is equal to the NMS and Snmp agent communication between the password
Access privilege	**Read-only**: specify the NMS (Snmp host) of MIB variables can only be read, cannot be modified **Read- write**: specify the NMS (Snmp host) of MIB variables can only read, can also be modified
Version	Specifies whether to send notifications as SNMP v1, v2c, or v3 traps. (Default: v2c)
IP	IPv4 address of a new management station to receive notification message (i.e., the targeted recipient).
Port	UDP Port – Specifies the UDP port number used by the trap manager. (Default: 162)

User Information

Selecting “**Management> Access Control>User** "



Add user, set Security Level, Authentication, Privacy, Group, Password

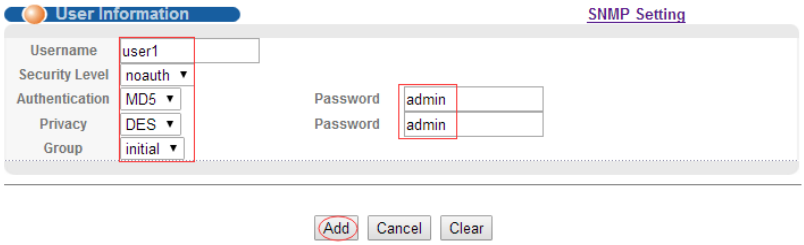


【Parameter Description】

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

【Configuration Example】

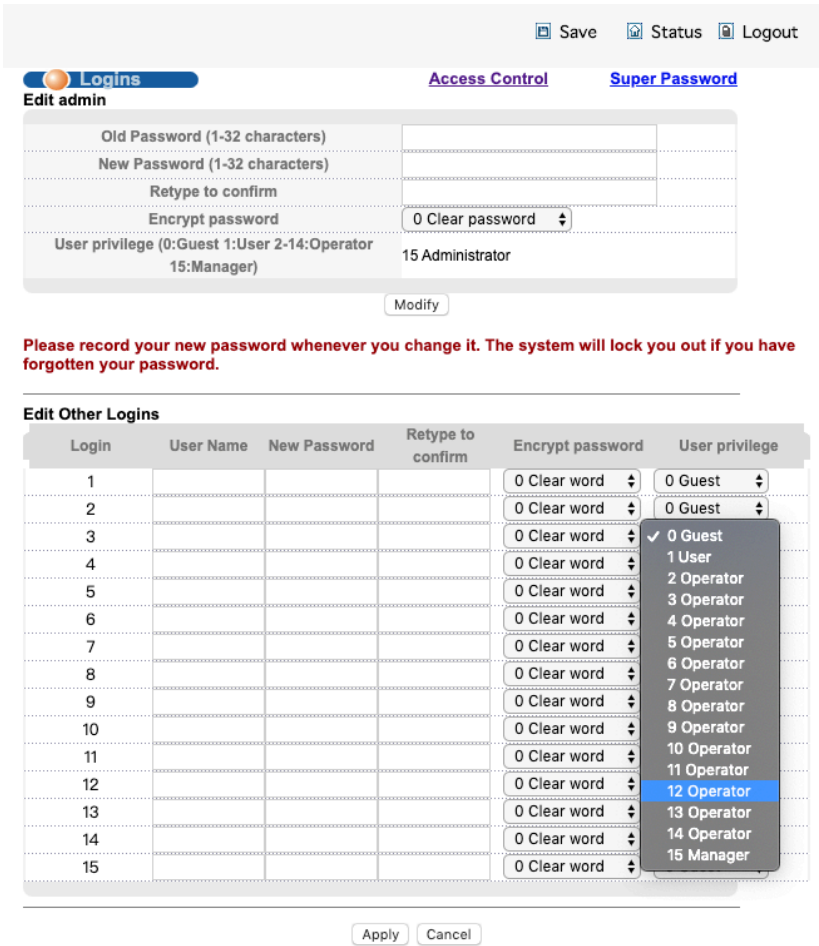
Such as: Add group initial, add username user1.



Logins

Configuring User Accounts

Use the Management > Access Control > Logins > User Accounts page to control management access to the switch based on manually configured user names and passwords.



Command Usage

◆ The default administrator name is “admin” with the password “admin.”

◆ The guest only has read access for most configuration parameters. However, the administrator has write access for all parameters governing the onboard agent. You should therefore assign a new administrator password as soon as possible, and store it in a safe place.

Parameters

These parameters are displayed:

◆ **User Name** – The name of the user.

(Maximum length: 32 characters; maximum number of users: 15)

◆ **Access Level** – Specifies command access privileges. (Range: 0-15)

Level 0 are designed for guest. The other levels can be used to configured specialized access profiles.
Level 2-14 provide the same default access to a limited number of commands which display the current status of the switch, as well as several database clear and reset functions. These commands are equivalent to those available under Normal Exec command mode in the CLI. Level 15 provides full access to all commands.

The privilege level associated with any command can be changed using the “privilege” command described in the CLI Reference Guide.
Any privilege level can access all of the commands assigned to lower privilege levels. For example, privilege level 8 can access all commands assigned to privilege levels 7-0 according to default settings, and to any other commands assigned to levels 7-0 using the “privilege” command described in the CLI Reference Guide.

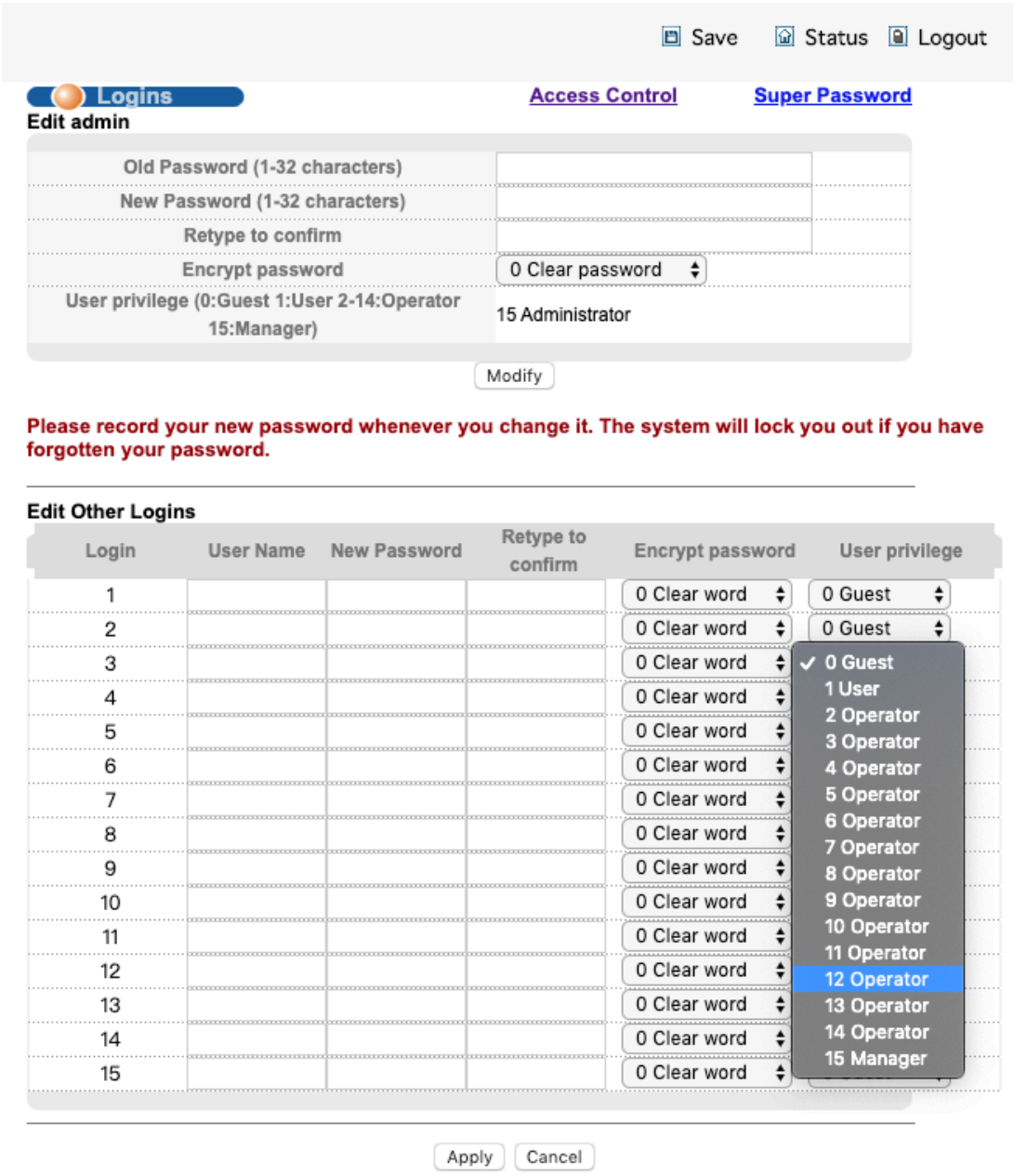
◆ **Password** – Specifies the user password. (Range: 0-32 characters, case sensitive)

◆ **Confirm Password** – Re-type the string entered in the previous field to ensure no errors were made. The switch will not change the password if these two fields do not match.

Web Interface

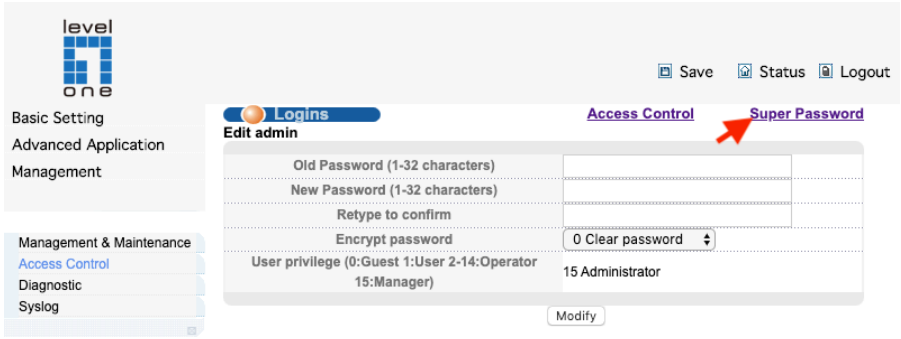
To configure user accounts:

1. Click Security, User Accounts.
2. Select Add or Modify from the Action list.
3. Specify or select a user name, select the user's access level, then enter a password if required and confirm it.
4. Click Apply.
5. Click Save.

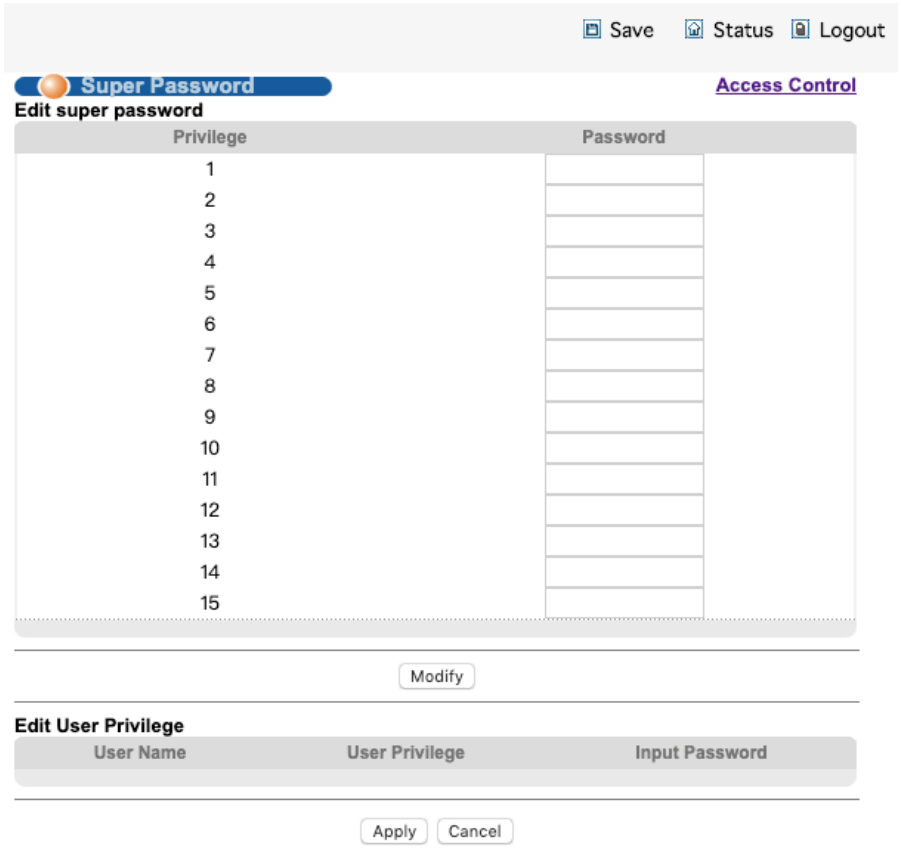


Super Password

Use the Management > Access Control > Logins > Super Password.



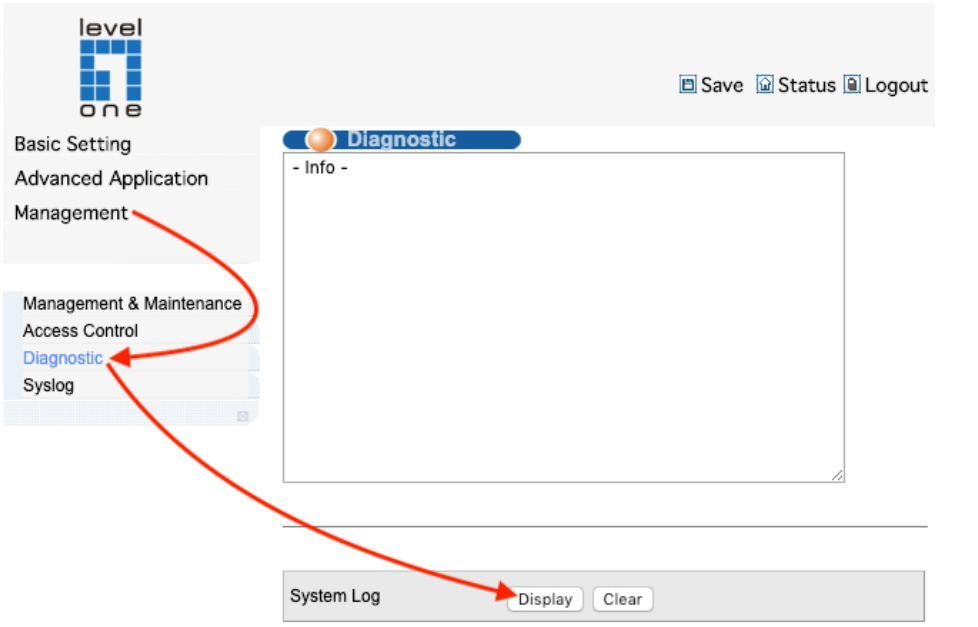
Set Super Password Enable Privileged Exec from Normal Exec Level.

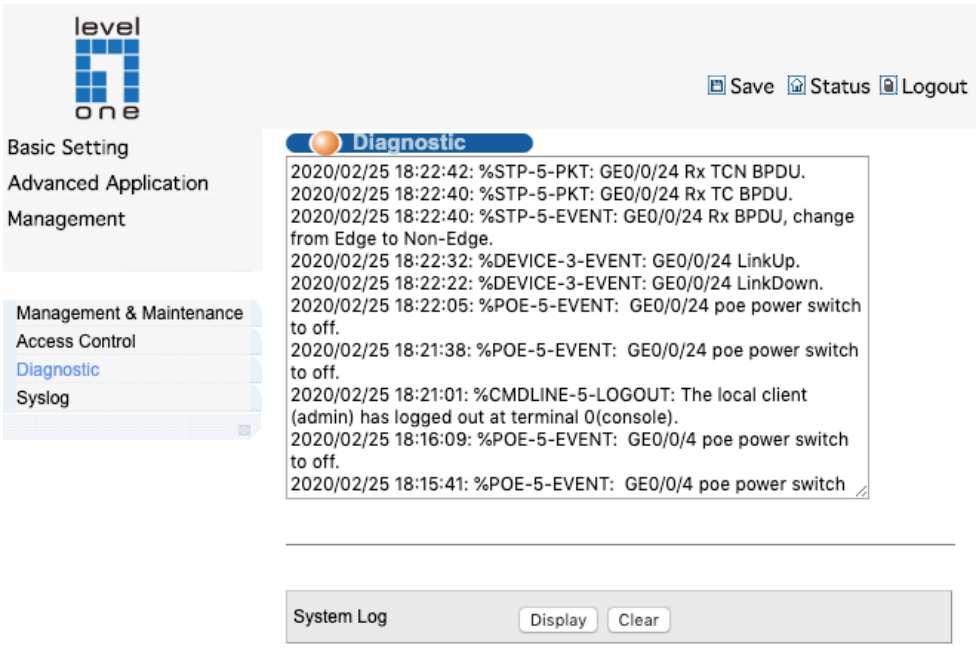


3. Diagnostic

The switch logging to a System Log (system log) server, and displays a list of recent event messages.

- **System Log Status** – The logging of debug or error messages to the logging process. (Default: Enabled)
- **Command Log Status** – Records the commands executed from the CLI, including the execution time and information about the CLI user including the user name, user interface (console port, telnet or SSH), and user IP address.



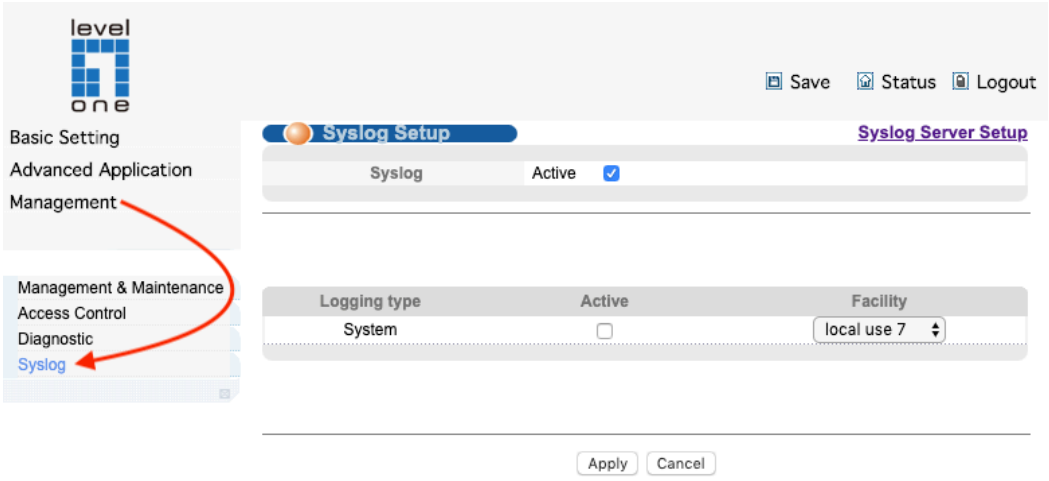


4. Syslog

System Log Configuration

Use the Management > Syslog (Configure Global) page to enable or disable event logging, and specify which levels are logged to RAM or flash memory.
Severe error messages that are logged to flash memory are permanently stored in the switch to assist in troubleshooting network problems. Up to 4096 log entries can be stored in the flash memory, with the oldest entries being overwritten first when the available log memory (256 kilobytes) has been exceeded.
The System Logs page allows you to configure and limit system messages that are logged to flash or RAM memory. The default is for event levels 0 to 3 to be logged to flash and levels 0 to 7 to be logged to RAM.
Parameters
These parameters are displayed:

◆ System Log Status – Enables/disables the logging of debug or error messages to the logging process. (Default: Enabled)

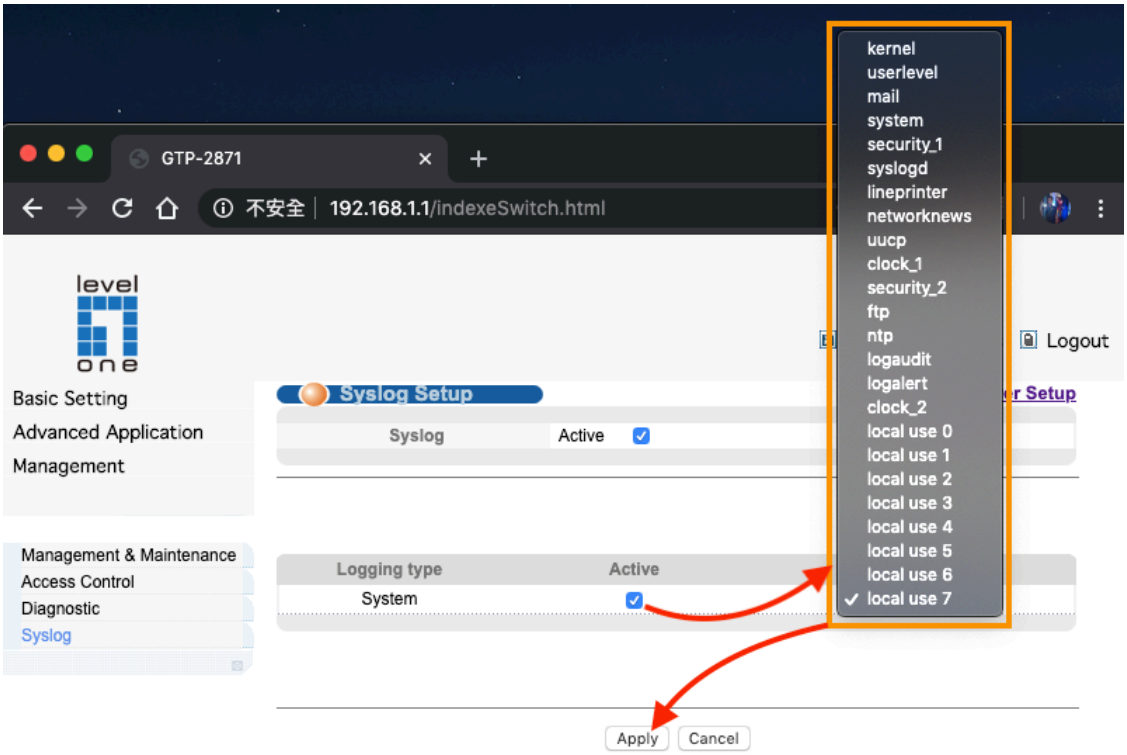


【Parameter Description】

Parameter	Description
Facility	local use 0-7 kernel userlevel mail system sercurity_1-2 sysogd lineprinter Networknews

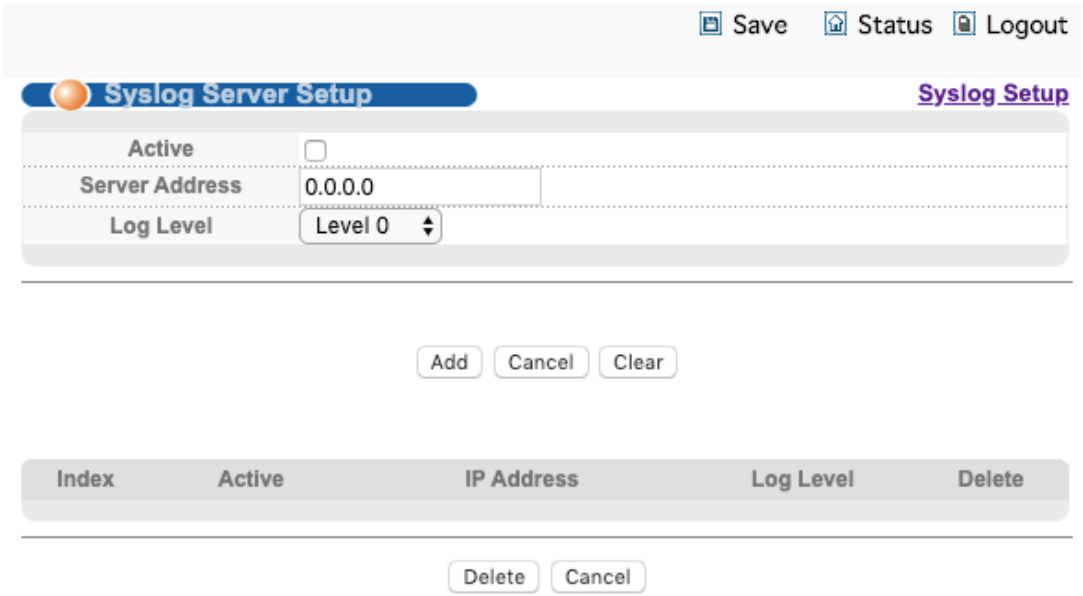
Parameter	Description
	uucp clock_1-2 ftp logaudit logalert

【Configuration Example】



Syslog Server Setup

Selecting "**Management**>**Syslog**>**Syslog Setup(Syslog Server Setup)**", in the navigation bar, you can set syslog server.



【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

【Instructions】

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

【Configuration Example】

Such as: 1)set server address is 192.168.1.100.