XS26GS

Managed Optical Ethernet Switch

User Manual

Nov 2, 2012

Version: V2.1

Table of Contents

Revision History

Date	Version	Description
Dec 23, 2011	V1.0	Initial release
April 10,2012	V2.0	Add network management view
Nov 2, 2012	V2.1	Modified the manual format. Added IP Source Guard.

0 Prefaces

0.1 Audience

This manual is intended for network installers and system administrators who are responsible for installing, configuring or maintaining networks. It assumes that you understand the transmission and management protocols used on your network.

This manual also assumes prior knowledge and understanding of the terminology, theories, practices and specific knowledge about the networking devices, protocols, and interfaces that comprise your network. You should have working experiences of the graphical user interfaces (GUIs), Command Line Interface (CLI), Simple Network Management Protocol (SNMP) and Web browsers.

0.2 Conventions

GUI Convention	Description
Boldface	Keywords on web management page are in **Boldface**
Italic	Tab page names are in *italic*
<>	Buttons are in <>
🕮	This icon is added to the notes.

1 Device Introduction

1.1 Brief Introduction

XS26GS Managed SFP-Based Optical Ethernet Switch is a high-performance managed Layer 2+ Gigabit Ethernet switch for service providers. It offers up to twenty-four SFP based Gigabit Ethernet fiber optic ports and two 100/1000M SFP fiber ports or two 10/100/1000BaseTX RJ45 copper ports. XS26GS is targeted at the emerging market of Ethernet based FTTx. It comes with a rich feature set to meet the requirements of a wide range of applications, especially the access network and the small-to-medium-scale customized network. The design of dual power supply provides the power redundancy for applications requiring high reliability. XS26GS is low-profile with a standard rack-mount size. It achieves the highest fiber port density within a single rack, providing users with the best performance/price ratio.

1.2 Features

- A range of configurable copper and fiber ports to meet the requirement of various applications, such as FTTH, optical LAN, Ethernet-based DCS and security surveillance system
- 8K address table for auto-learned unicast or static unicast/multicast addresses
- Jumbo frame of up to 9216 bytes
- 802.1p, Port, and DiffServ based QoS package classification with 4 priority queues. Support queue mapping and DSCP mapping
- 4K 802.1Q based VLAN
- Port based VLAN
- 16 Protocol based VLAN
- MAC based VLAN
- Guest VLAN
- VLAN VPN, QinQ
- GARP/GVRP
- 16 trunk groups of up to 8 member ports with flexible load distribution control and fail-over functions
- Manual, static, and dynamic port aggregation
- 802.1d Spanning Tree Protocol, 802.1w Rapid Spanning Tree Protocol, and 802.1s Multiple Spanning Tree Protocol
- By-port egress, ingress, and bi-direction rate control
- Multi combination of MAC address, VID, and port binding
- Static and dynamic MAC addressing
- Blackhole MAC address filtering
- IGMP Snooping
- Multicast VLAN Registration (MVR)
- Link Layer Discovery Protocol (LLDP)
- Storm Control for any combination of multicast, broadcast, and DLF traffic
- Access Control Lists (ACL)
- Secure Shell (SSH) v2.0
- 802.1x Port-based access control and MAC authentication
- User configurable port mirroring supports ingress/egress/both data flow monitoring on one or more ports.
- SNMP v1/v2c/v3

- Web page management
- Command Line Interface (CLI)
- Telnet and RS232 console management
- User account assignable to one of the three access privilege levels
- On-line firmware upgrade
- Configuration file backup and restore
- Dual power supply modules provide power redundancy with status monitoring features
- Embedded XS View Network management System (Optional)

1.3 Face Panel

The face panel of XS26GS optical Ethernet switch is shown in the following figure.

1.4 SFP Based Optical Interface Options

- Two 100/1000M SFP Fiber or 10/100/1000BaseTX RJ45 copper combo ports
- Twenty-four standard SFP based 100/1000Base-X ports
- Support third-party standard SFP modules

1.5 Power Supply Options

- AC90~264V/1.2A max, 50/60Hz, or
- DC18~36V/2A, or
- DC36~72V/1.5A
- Power Consumption: no more than 45W

1.6 Physical and Environmental

- Dimension: 19-inch rack-mount wide, 1.0U high
- Weight: ~5Kg
- Operating temperature: 0℃~ 50℃
- Storage temperature: -25℃~ 85℃
- Humidity: 5% ~ 95% RH Non-condensing

1.7 Default Configuration

(1) Administration

IP:

IP Address:	192.168.0.253
IP Sub network:	255.255.255.0
IP Gateway:	192.168.0.201

Accounts:

User Level	User Name	Password	Privilege
Administrator	superuser	123	Can carry out all the functions of the switch.
User	manager	123	Can carry out all the funcitons except bulid or delete an account, reset to default configuration, use the TFTP service to update firmware, backup and restore configuration.
Visitor	guest	(none)	Can use the internet diagnosis commands, such as ping command for system maintainace, and the “show” commands except “show user”, “show snmp community”, “show snmp traps-host” and “show snmp user”. Note: Visitor can only access the switch by Console port.

(2) Port

State: enabled
Flow Control: disabled
Learning: enabled
Rate limit: disabled
Negotiation: enabled

(3) VLAN

VLAN mode: none
Static VLAN: 1, including all ports
Port VID: 1
Port link type: hybrid
Frame type: admit all

(4) SNMP

Version: v1
Community: public
Privilege: RO
User: (none)
SNMP trap: enabled
Trap host IP: (none)

(5) Protocols

IGMP Snooping: Disabled
GARP/GVRP: Disabled
STP: Disabled
LACP: Disabled
802.1x: Disabled
LLDP: Disabled

1.8 Management Software Specification

The following table summarizes the protocols supported by the managed optical Ethernet

switch in the current software released.

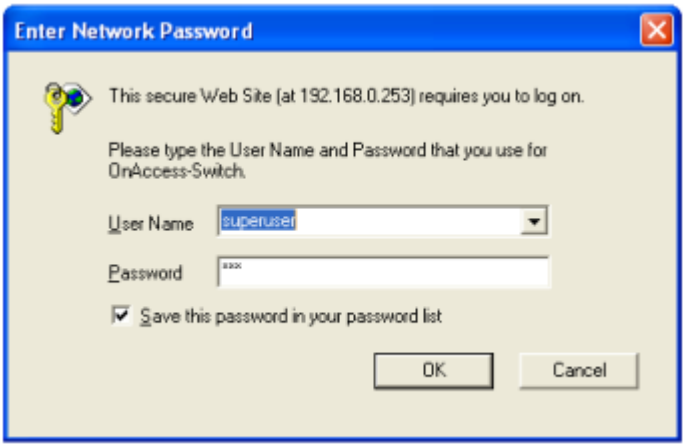
TCP/IP	ARP, ICMP, IP, TCP, UDP
SNMP	SNMP v2(1,2,3,9), FMC private MIBS, MIB counters of groups 1, 2, 4, 9
Web management server	Http Server. Support goahead-2.1.8.Java scripts, Java Applet, CGI
Telnet server	Telnet 1.0
Console	Standard UART
Spanning tree protocol	IEEE 802.1d/1w/1s
Four-level priority queuing	IEEE 802.1p
Port-based VLAN	SVL
Tag-based VLAN	IEEE 802.1q (IVL and SVL), GVRP
Protocol-based VLAN	IEEE 802.1v
Trunking	IEEE 802.3ad, LACP
Authentication	IEEE 802.1x
IGMP Snooping	RFC2236

2 Login to the Switch

To access the switch web management funciton, open a web-browser and type in the default address http://192.168.0.253 in the address field of the browser, then press the **Enter** key.

> Note:
>
> To log in to the Switch, the IP address of your PC should be set in the same subnet addresses of the Switch. The IP address is 192.168.0.x ("x" is any number from 2 to 254), Subnet Mask is 255.255.255.0.

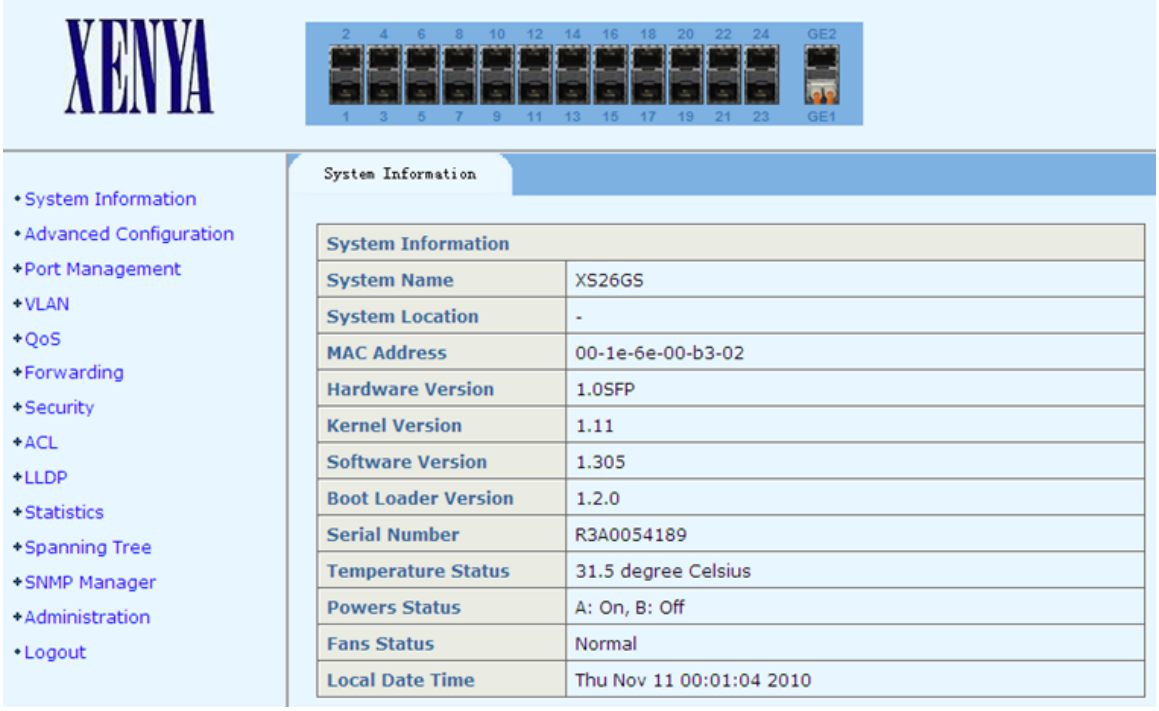
And then a login window will appear, as shown follows. Enter the default User Name and Password. The default values are set in section 1.7 of this manual. Then click the Login button or press the **Enter** key, so that you can see the switch system information.



If you need to change the switch IP address at the first time, you can modify it through RS232 console, or using telnet to login, you can refer to “XS26GS Managed Optical Ethernet Switch CLI Manual V1.0”.

3 System Information

After logining, the web is on System Information page, which shows the basic information of the switch as follows.



4 Advanced Configuration

This page configures whether to globally enable or disable the following protocols:

- IGMP Snooping
- DHCP Snooping
- GVRP
- STP
- LACP
- Authentication
- LLDP
- LBD
- LBD Interval Time
- XS View

IGMP Snooping	Globally enable/disable the protocol
DHCP Snooping	Globally enable/disable the DHCP Snooping function
GVRP	Globally enable/disable GVRP protocol
STP	Globally enable/disable STP protocol
LACP	Globally enable/disable LACP protocol
Authentication	Select authentication between 802.1x and MAC Authentication, or disable the authentication
LLDP	Globally enable/disable LLDP protocol
LBD	Used to globally enable loopback detection function on this switch. It will check whether there is a loop on the switch on any VLAN. If there is one on a VLAN, it will shut down the port or will send out a trap.
LBD Interval Time	Time interval for loopback detection, in the range of 5 to 300 (seconds). The default value is 30 seconds.
XS View	Two modes for it: Enabled and Disabled. If it is enabled, it can be managed by the XS View NMS.

System Advanced Configuration	
Igmp Snooping	Disabled
DHCP Snooping	Disabled
GVRP	Disabled
STP	Enabled
LACP	Disabled
Authentication	Disabled
LLDP	Disabled
LBD	Disabled
LBD Interval Time (5-300)	30 sec
XS View	Disabled
	Apply

5 Port Management

This page configures port related management functions as follows.

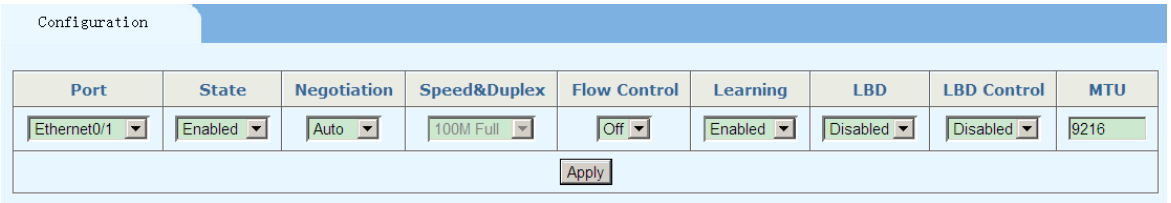
- Port Configuration
- Port Aggregation
- Port Bandwidth
- Port Mirroring

5.1 Port Configuration

This page configures a port. When the setup is completed, click <Apply> to take effect.

Port	Specify a port to configure
State	Enable/disable the state of the specified port
Negotiation	Select Auto or Fore
Speed&Duplex	Select a speed
Flow Control	Select On or Off
Learning	Enable/disable learning function
LBD	Enable or disable loopback detection for the specific port.
LBD Control	Enable or disable LBD Control for the specific port. If the loopback port control function is enabled on a trunk or hybrid port, when a loop is found, the switch will disable the port, and remove the corresponding MAC forwarding entries. On the other hand, if the loopback port control function is disabled on a trunk or hybrid port when a loop is found, the port will not be disabled. For an access port, the switch will disable the port if a loop is found, as far as LBD is enabled, no matter LBD Control is enabled or disabled.
MTU	The maximum transmissiton unit, in the range of 1518-9216 bytes.

By default, the loopback port control function is disabled on a trunk or hybrid port. A list of the port status is also provided. See the following figure for more details.



Port Status

Port	State	Link	Negotiation	Speed&Duplex Config	Speed&Duplex Actual	Flow Control Config	Flow Control Actual	Learning	LBD	LBD Control	MTU
Ethernet0/1	Enabled	Down	Auto	-	-	Off	-	Enabled	Disabled	Disabled	9216
Ethernet0/2	Enabled	Down	Auto	-	-	Off	-	Enabled	Disabled	Disabled	9216
Ethernet0/3	Enabled	Down	Auto	-	-	Off	-	Enabled	Disabled	Disabled	9216
Ethernet0/4	Enabled	Down	Auto	-	-	Off	-	Enabled	Disabled	Disabled	9216
Ethernet0/5	Enabled	Down	Auto	-	-	Off	-	Enabled	Disabled	Disabled	9216
Ethernet0/6	Enabled	Down	Auto	-	-	Off	-	Enabled	Disabled	Disabled	9216
Ethernet0/7	Enabled	Down	Auto	-	-	Off	-	Enabled	Disabled	Disabled	9216
Ethernet0/8	Enabled	Down	Auto	-	-	Off	-	Enabled	Disabled	Disabled	9216
Ethernet0/9	Enabled	Down	Auto	-	-	Off	-	Enabled	Disabled	Disabled	9216
Ethernet0/10	Enabled	Down	Auto	-	-	Off	-	Enabled	Disabled	Disabled	9216

5.2 Port Aggregation

XS26GS switch supports up to 16 link aggregation groups, and each group can have up to 8 ports.

This page sets link aggregation. There are three types of aggregation: **manual**, **static**, and **dynamic**. The following provides a detailed description of each type of aggregation:

Manual aggregation a manual trunk can only be manually set or deleted; any port in a manual trunk shall have this port's Link Aggregation Control Protocol (LACP) disabled, while the global LACP can be either enabled or disabled.

Static LACP aggregation a static LACP trunk can only be manually set or deleted; any port in a static LACP trunk shall have this port's Link LACP enabled. When a static LACP trunk is (manually) deleted, all ports of this trunk with "up" status will generate one or more dynamic LACP trunks automatically.

Dynamic LACP aggregation a dynamic LACP trunk can only be set or deleted automatically by the protocol; any port in a dynamic LACP trunk shall have this port's LACP enabled.

A trunk may be configured as a mirror port, but it is not allowed to configure a trunk as a monitoring port.

There are four tab pages on this webpage to configure various parameters:

Aggregate Groups – Create and configure a trunk. The switch can have up to 16 trunks.

Trunk ID One of the 16 trunk IDs (from T1 to T16) for the user to choose.
Trunk Name Enter a name for the selected trunk.
Trunk Type Select the trunk to be a manual trunk, or static LACP trunk.
Port Choose up to 8 ports to form the trunk.

The bottom part of this tab page lists all existing trunks.

Note:

Only when **LACP** in **System Advanced Configuration** page is enabled, **Trunk Type** can be selected; otherwise, the **Trunk Type** is **Manual** by default.

Aggregate Groups | Lacp Port Setting | Aggregate Based | Lacp Status Setting

Link-aggregation Setting

Trunk ID	T1
Trunk Name	DEFAULT
Trunk Type	Manual

Port	Ethernet0/																								Ethernet1/	
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	1	2
Member	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

apply

Link-aggregation Information

Trunk ID	Trunk Name	Trunk Type	Port List	Delete

Lacp Port Setting – Configures LACP ports

Aggregate Groups | Lacp Port Setting | Aggregate Based | Lacp Status Setting

LACP Port Configuration

Port	Ethernet0/																								Ethernet1/	
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	1	2
LACP Port	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

Apply

Aggregate Based Setting – Sets LACP system priority, between 1 and 65535

Aggregate Groups | Lacp Port Setting | Aggregate Based | Lacp Status Setting

Aggregator Based Setting

LACP System Priority(1-65535)	1

apply

Lacp Status Setting – Sets LACP active or passive for each port

Passive The port does not automatically send LACP protocol packets; it responds only if it receives an LACP protocol packet from the opposite device.

Active The port automatically sends LACP protocol packets.

A link having either one or two active LACP ports can perform dynamic LACP trunking. A link having two passive LACP ports will not perform dynamic LACP trunking as both ports are waiting for LACP protocol packet from the opposite device.

Aggregate Groups | Lacp Port Setting | Aggregate Based | Lacp Status Setting

LACP State Activity Setting

Port		Ethernet0/																							Ethernet1/	
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	1	2
LACP State	Passive	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
	Active	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉

Apply

5.3 Port Bandwidth

This page sets the ingress and/or egress rate limit for each port.

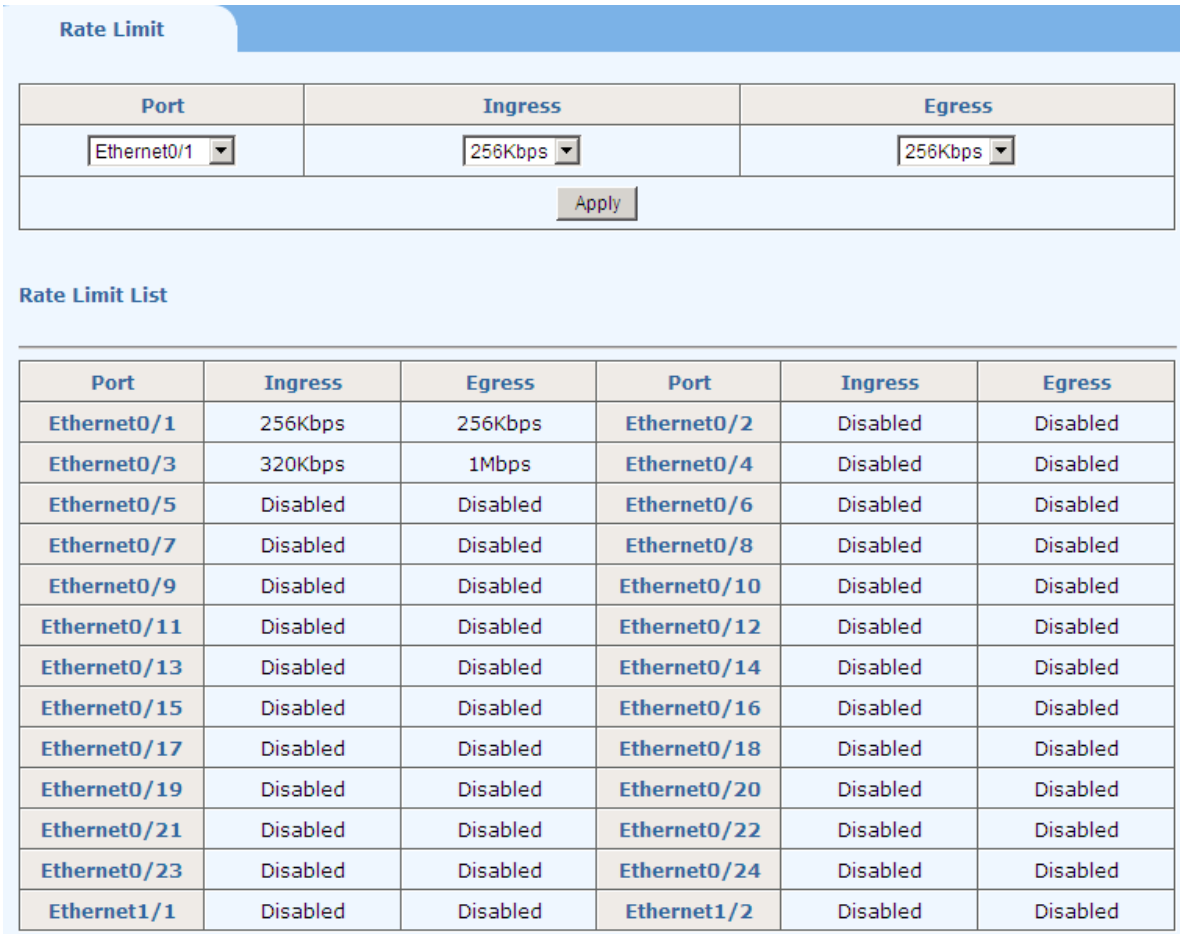
Port the port for which the rate limit is configured.

Ingress the desired ingress rate limit to be configured. Choose “disabled” to set the port with no ingress rate limit, which means the port will run in full speed for ingress traffic. You can also select a specific ingress rate from the drop-down list for a port.

Egress the desired egress rate limit to be configured. Choose “disabled” to set the port with no egress rate limit, which means the port will run in full speed for egress traffic. You can also select a specific egress rate from the drop-down list for a port.

When completing the configuration, click <apply> to take effect.

The bottom part of this page shows a full list of rate limit for each port.



Port	Ingress	Egress	Port	Ingress	Egress
Ethernet0/1	256Kbps	256Kbps	Ethernet0/2	Disabled	Disabled
Ethernet0/3	320Kbps	1Mbps	Ethernet0/4	Disabled	Disabled
Ethernet0/5	Disabled	Disabled	Ethernet0/6	Disabled	Disabled
Ethernet0/7	Disabled	Disabled	Ethernet0/8	Disabled	Disabled
Ethernet0/9	Disabled	Disabled	Ethernet0/10	Disabled	Disabled
Ethernet0/11	Disabled	Disabled	Ethernet0/12	Disabled	Disabled
Ethernet0/13	Disabled	Disabled	Ethernet0/14	Disabled	Disabled
Ethernet0/15	Disabled	Disabled	Ethernet0/16	Disabled	Disabled
Ethernet0/17	Disabled	Disabled	Ethernet0/18	Disabled	Disabled
Ethernet0/19	Disabled	Disabled	Ethernet0/20	Disabled	Disabled
Ethernet0/21	Disabled	Disabled	Ethernet0/22	Disabled	Disabled
Ethernet0/23	Disabled	Disabled	Ethernet0/24	Disabled	Disabled
Ethernet1/1	Disabled	Disabled	Ethernet1/2	Disabled	Disabled

5.4 Port Mirroring

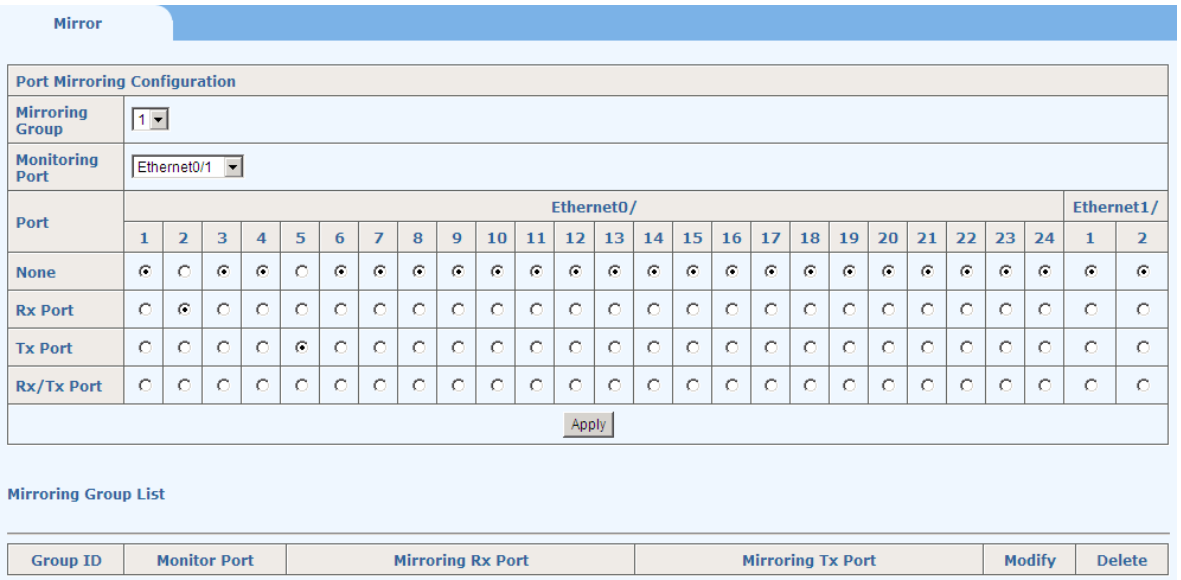
This page configures the port mirroring function. You can set up 1 to 4 Mirroring Groups; you can select one Monitoring Port for each Mirroring group from the Monitoring Port drop-down list, but more than one Mirroring port.

Monitoring Port the port or ports to which the traffic is mirrored

Rx Port all ingress traffic of this port will be mirrored to each of the Monitoring Port(s)

Tx Portall egress traffic of this port will be mirrored to each of the Monitoring Port(s)

Rx/Tx Port all ingress and egress traffic of this port will be mirrored to each of the Monitoring Port(s)

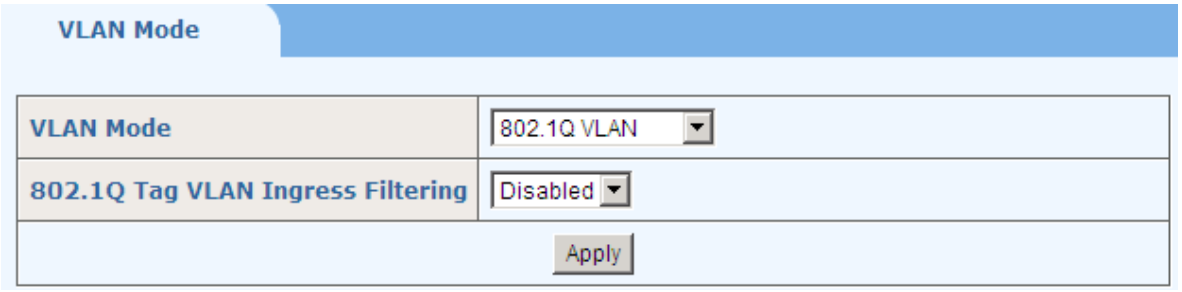


6 VLAN

This managed switch supports 802.1Q, port-based VLAN, Protocol VLAN, Mac Based VLAN, VLAN-VPN and GARP. VLAN is in 802.1Q mode in default configuration.

6.1 Advanced

This page globally sets the VLAN mode from the following: NO VLAN, port-based VLAN and 802.1Q VLAN.

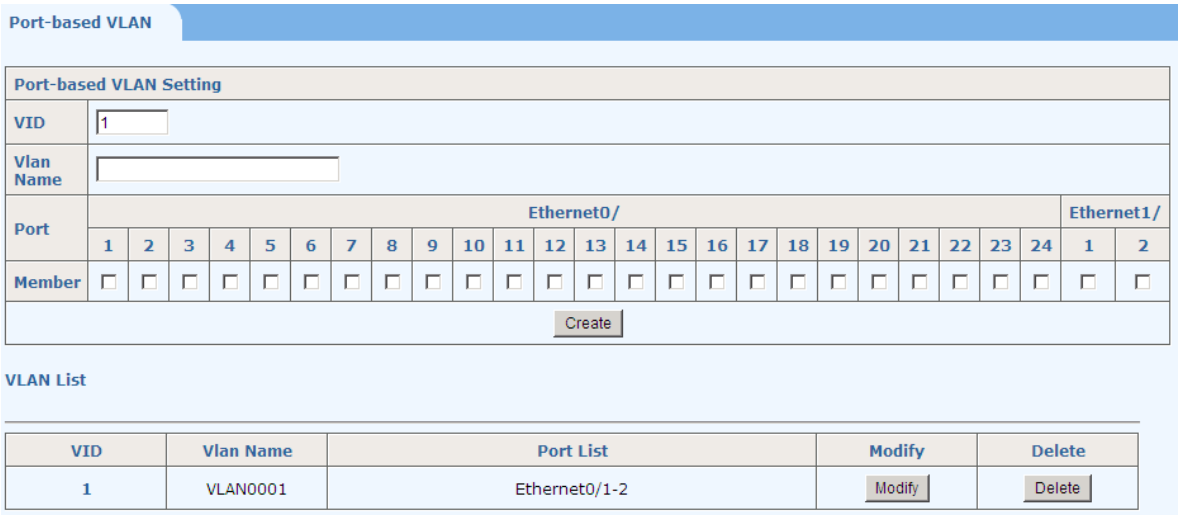


6.2 Port-based VLAN

If you select Port-based VLAN from the VLAN Mode in Advanced page and click <Apply>, then you will find there is “Port-based VLAN” in the left of the page. On its page, the user can create a new VLAN group with specific VID and VLAN group name. Up to 256 VLAN groups can be created; each VLAN group can have an ID number from 1 to 4094.

Member: checks to indicate the port is a member of the VLAN group.

The bottom part of this page lists all port-based VLAN groups configured, they can be modified or deleted.



6.3 802.1Q VLAN

If you select 802.1Q VLAN from the VLAN Mode in Advanced page and click <Apply>, then you will find **802.1Q VLAN**, **Protocol VLAN**, **Mac Based VLAN**, **VLAN VPN** and **GARP** under **Advanced** in the left of the page. On “802.1Q VLAN” page, there is a default VLAN group with VLAN identifier (VID) of 1, each port is a member of this group in default, and remains as a member before it is removed from the group.

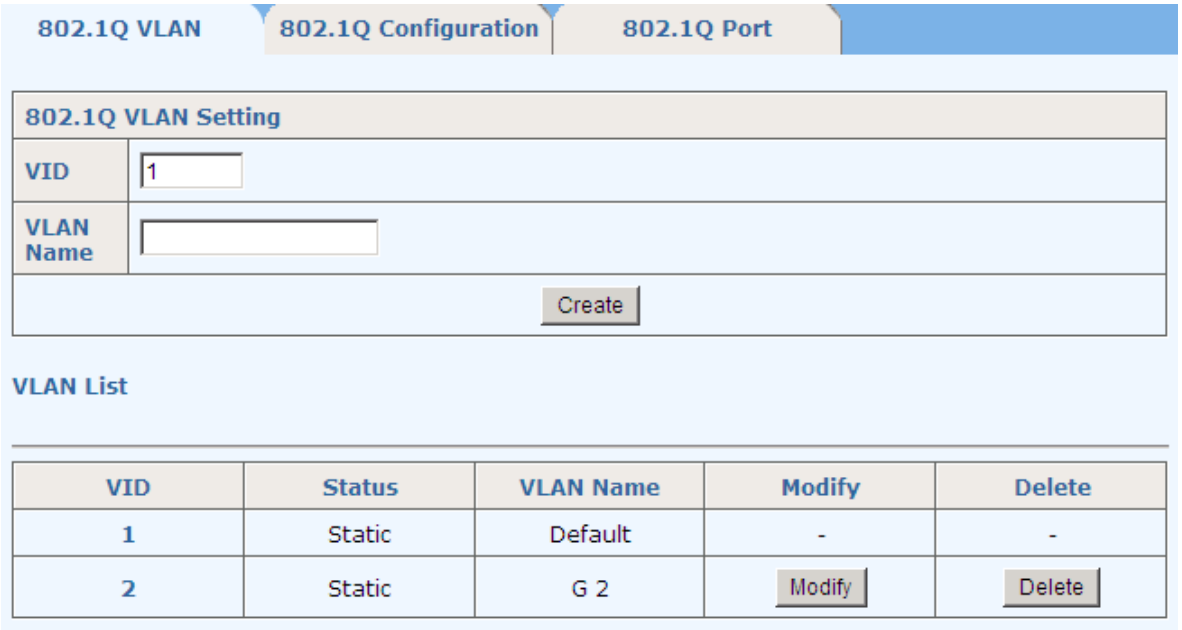
There are three tab pages on this webpage for you to configure various parameters:

6.3.1 802.1Q VLAN

On this tab page, you can create a new VLAN group with specific VID and VLAN group name. Up to 256 VLAN groups can be created; each VLAN group can have an ID number from 1 to 4094.

The bottom part of this page lists all existing VLAN groups, as well as the information on each VLAN group. Users can also modify or delete an existing VLAN group.

Note: It is not allowed to delete VLAN group 1.



6.3.2 802.1Q Configuration

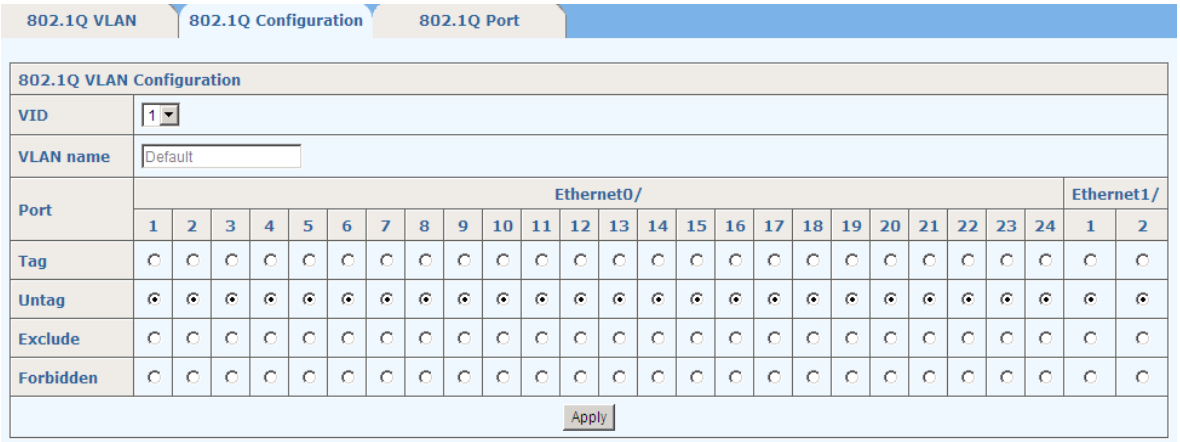
This tab page configures a VLAN group; each port can be configured as a specific state for this VLAN group:

Tag indicates the port is a tagged member of the VLAN group. All packets forwarded by the port are tagged. The packets contain VLAN information.

Untag indicates the port is an untagged VLAN member of the VLAN group. Packets forwarded by the port are untagged.

Exclude excludes the port from the VLAN group. However, the port can be added to the VLAN group through GARP.

Forbidden does not allow the port to be added to the VLAN group, even if GARP indicates so.



6.3.3 802.1Q Port

This tab page configures 802.1Q VLAN port parameters:

PVID: each port can have only one Port VLAN ID (PVID), an untagged Ethernet package will be tagged a VID of PVID when arriving at the port. The default PVID is 1 for each port.

Link Type can choose **Hybrid** (by default), **Access** or **Trunk** from this drop-down list. An **Access** port has only one VLAN and the tag is removed when it is egessing packets (i.e. **Untagged**); a **Trunk** port can have multiple VLANs, and all packages are tagged, except when an egress package is in a VLAN group with VID the same as PVID; a **Hybrid** port is similar to a **Trunk** port, except it leaves the user a flexibility of configuring each port's **Tagged** or **Untagged**.

Ingress Filter When enabled, an Ethernet package is discarded if this port is not a member of the VLAN with which this package is associated. When disabled (by default), all packages are forwarded in accordance with the 802.1Q VLAN bridge specification.

Frame Type chooses how the port accepts Ethernet package. When **Admit All** is selected, the port accepts all ingress packages; while **Admit Only Tagged** accepts only tagged packages, and discards untagged ones.

The bottom part of this tab page lists the status of all ports.

802.1Q VLAN | 802.1Q Configuration | 802.1Q Port

Port	PVID	Link Type	Ingress Filter	Frame Type
Ethernet0/1	1	Hybrid	Disabled	Admit All

Apply

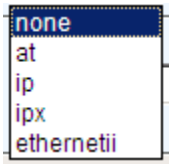
Port Status

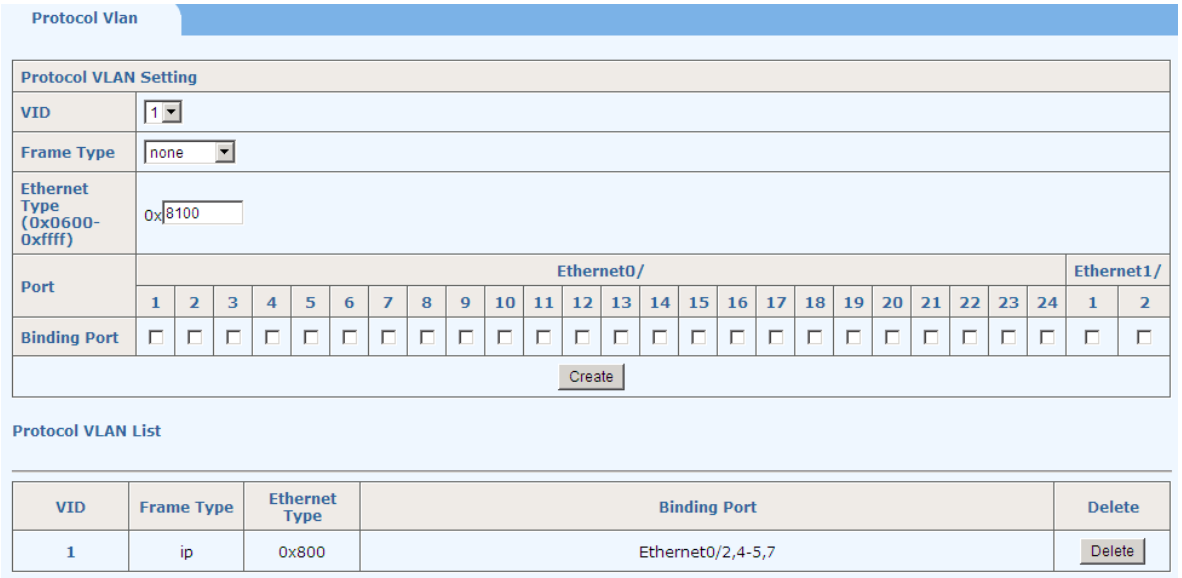
Port	PVID	Link Type	Ingress Filter	Frame Type
Ethernet0/1	1	Hybrid	Disabled	Admit All
Ethernet0/2	1	Access	Enabled	Admit Only Tagged
Ethernet0/3	1	Hybrid	Disabled	Admit All
Ethernet0/4	1	Hybrid	Disabled	Admit All
Ethernet0/5	1	Hybrid	Disabled	Admit All
Ethernet0/6	1	Hybrid	Disabled	Admit All
Ethernet0/7	1	Hybrid	Disabled	Admit All
Ethernet0/8	1	Hybrid	Disabled	Admit All
Ethernet0/9	1	Hybrid	Disabled	Admit All
Ethernet0/10	1	Hybrid	Disabled	Admit All

6.4 Protocol VLAN

This page configures protocol VLAN. The drop-down **VID** list shows all existing VLAN groups for users to choose a group to configure. For a selected VLAN group, the **Frame Type** lists all protocols for which users can choose. **Ethernet Type** is bundled with the **Frame Type** chosen, except for **Ethernet II**, for which users can type in an **Ethernet Type**. Corresponding **Port** is selected when setting **Protocol VLAN** group.

The bottom part of this page lists all protocol VLAN groups configured.

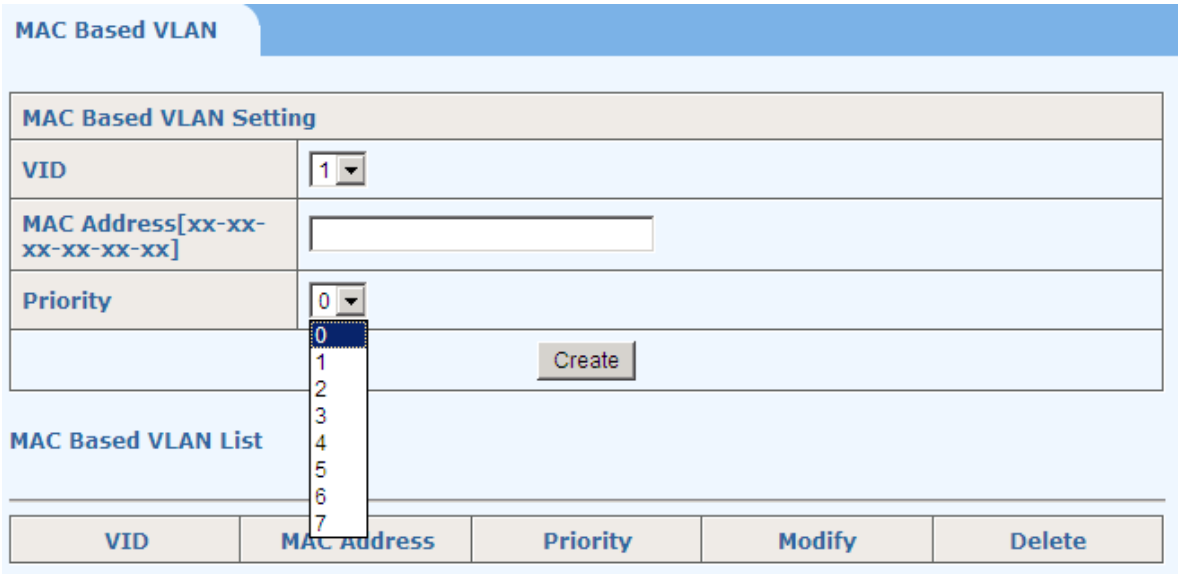




6.5 MAC-based VLAN

This page configures Mac-based VLAN. The drop-down **VID** list shows all existing VLAN groups for the user to choose a group to configure. For a selected VLAN group, the **MAC Address** is the source MAC address of incoming packets, and the **Priority** is the added VLAN tag priority.

The bottom part of this page lists all Mac-based VLAN groups configured.



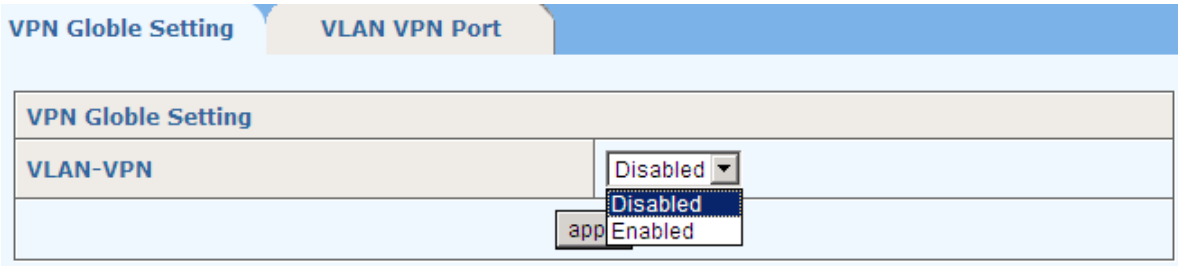
6.6 VLAN VPN

There are three tab pages: **VPN Global Setting**, **VLAN VPN Port** and **QinQ**.

6.6.1 VPN Global Setting

This page enables or disables global VLAN VPN.

VLAN VPN: enable or disable the global VLAN VPN.



6.6.2 VLAN VPN Port

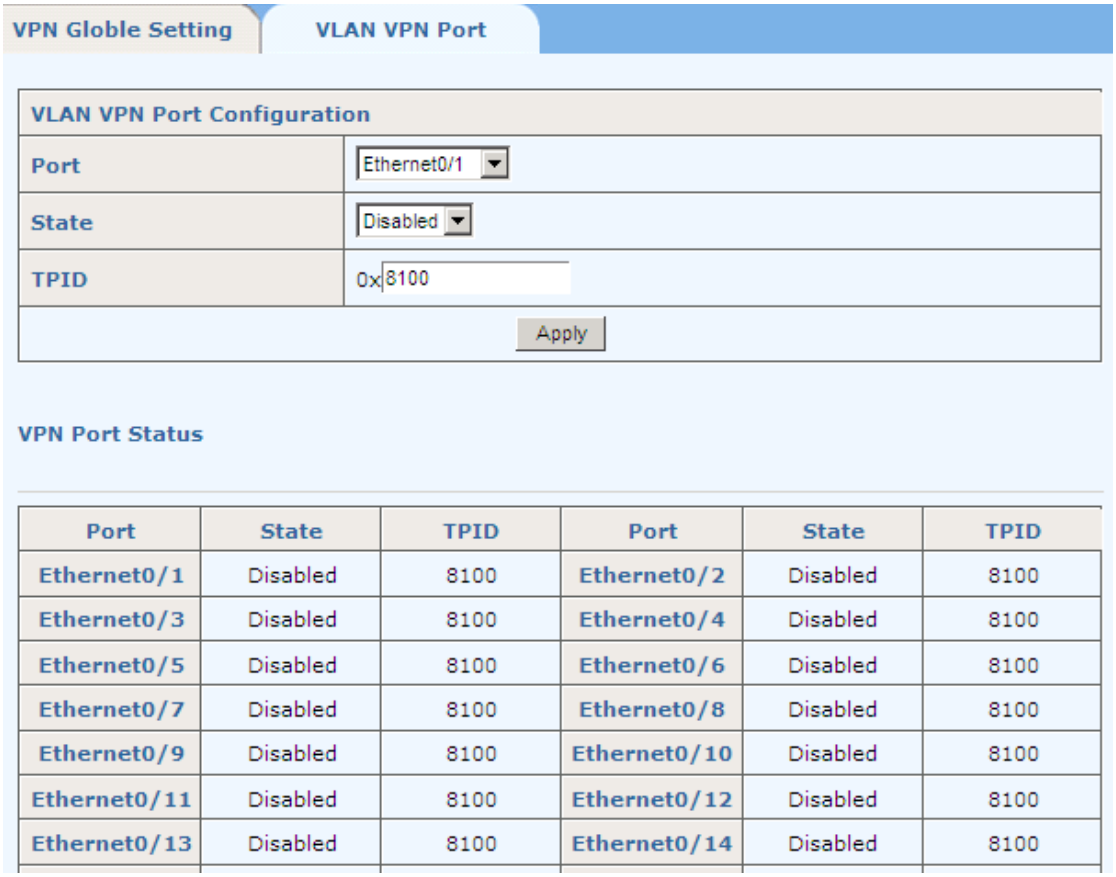
This page enables or disables VLAN VPN and sets TPID (Tag Protocol Identifier) value for a specific port. The default TPID value is 0x8100. Be aware that some other vendors' switches may set this value to be 0x9100.

Port: select a specific port for setting

State: to enable/disable a specific port

TPID: to set TPID value, 0x8100 by default. TPID is used to identify whether the packets carry specific VLAN Tag. Note that the location of the TPID field in an Ethernet packet is the same as the protocol type field in a packet without VLAN Tag. Thus, to prevent confusion, the following protocol type values should not be configured as a TPID value.

- ARP: 0x0806
- IP: 0x0800
- MPLS: 0x8847/0x8848
- IPX: 0x8137
- IS-IS: 0x8000
- LACP: 0x8809
- 802.1x: 0x888E

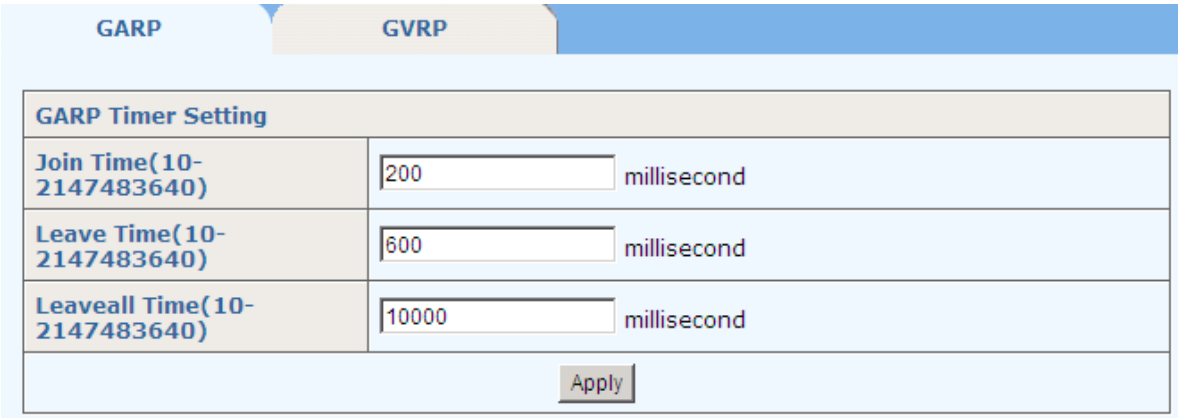


6.7 GARP

GARP VLAN Registration Protocol (GVRP) is based on Generic Attribute Registration Protocol (GARP). They are standard protocols described in IEEE 802.1D.

Before configuring GARP, make sure GVRP is enabled (see section 2.3 of this manual for details). There are two tab pages:

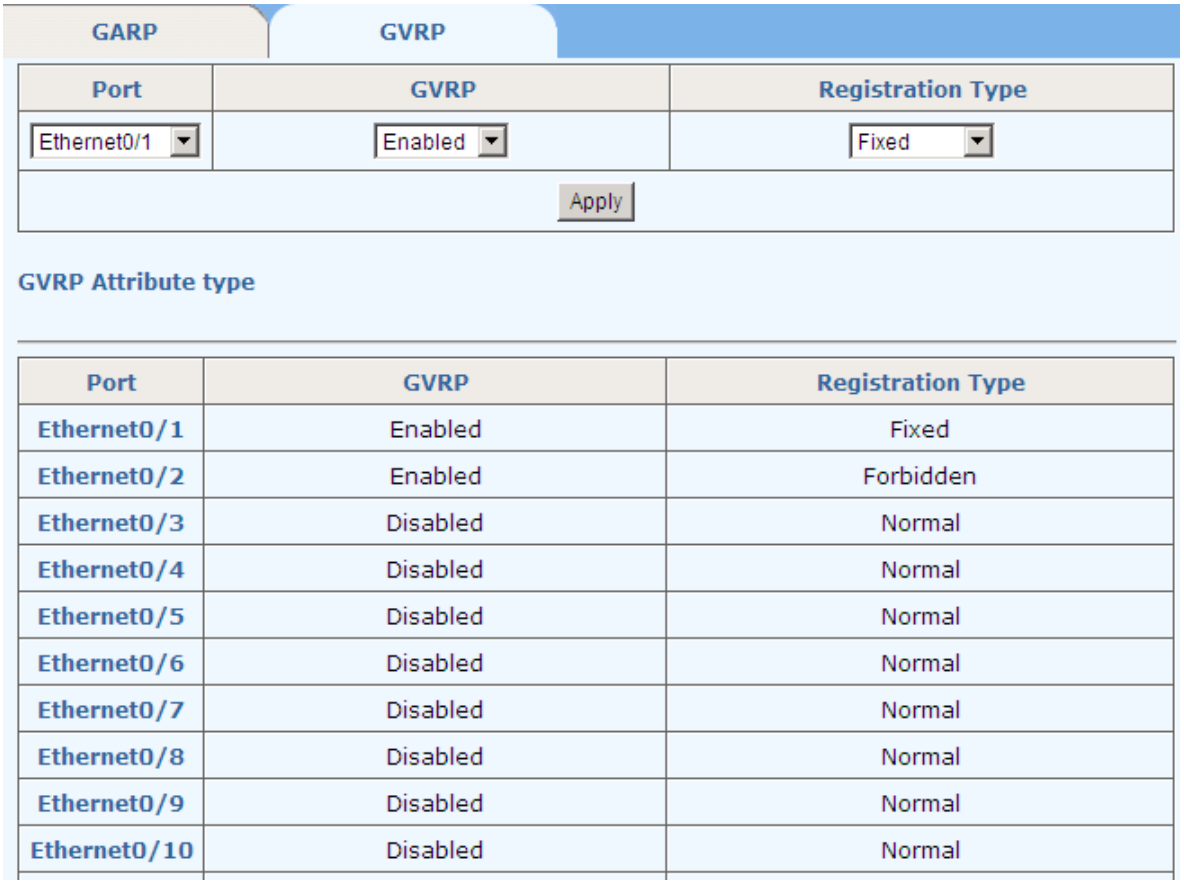
GARP: This tab page sets GARP **Join Time**, **Leave Time**, and **Leaveall Time**. **Leaveall Time** must be greater than **Leave Time**, and **Leave Time** must be greater than twice the **Join Time**.



GVRP: This tab page sets GVRP parameters of each port. For a selected **Port**, enabled **GVRP**, the **Registration Type** can be set to **Normal** (default), **Fixed**, or **Forbidden**. **Normal** registration allows dynamic passing, registration and de-registration of both dynamic and static VLANs; **Fixed** registration allows passing static VLANs, as well as

manual registration and de-registration of VLANs; while **Forbidden** prohibits the port from passing, registration, or de-registration of VLANs.

The bottom part of *GVRP* tab page lists the GVRP attribute of all ports.



7 QoS

This managed switch supports Quality of Service (QoS). QoS priority is disabled in default configuration. There are the following sub-menus.

- QoS
  - QoS Configuration
  - Scheduling Mechanism
  - Transmit Queues
  - DSCP Map

7.1 QoS Configuration

*T*his tab page sets QoS parameters of each port. For a selected **Port**, set the **Priority,** with **DSCP** enabled or disabled, the **Default Priority** can be set from 0 to 7.

The bottom part of QoS Configuration tab page lists the default priority of all ports and the state of DSCP.

QoS

Port	Default Priority	DSCP
Ethernet0/1	6	Disabled
	Apply	

Port Priority List

Port	Default Priority	DSCP	Port	Default Priority	DSCP
Ethernet0/1	6	Disabled	Ethernet0/2	0	Disabled
Ethernet0/3	4	Enabled	Ethernet0/4	4	Enabled
Ethernet0/5	7	Enabled	Ethernet0/6	0	Disabled
Ethernet0/7	0	Disabled	Ethernet0/8	0	Disabled
Ethernet0/9	0	Disabled	Ethernet0/10	0	Disabled
Ethernet0/11	0	Disabled	Ethernet0/12	0	Disabled
Ethernet0/13	0	Disabled	Ethernet0/14	0	Disabled
Ethernet0/15	0	Disabled	Ethernet0/16	0	Disabled
Ethernet0/17	0	Disabled	Ethernet0/18	0	Disabled
Ethernet0/19	0	Disabled	Ethernet0/20	0	Disabled
Ethernet0/21	0	Disabled	Ethernet0/22	0	Disabled
Ethernet0/23	0	Disabled	Ethernet0/24	0	Disabled
Ethernet1/1	0	Disabled	Ethernet1/2	0	Disabled

7.2 Scheduling Mechanism

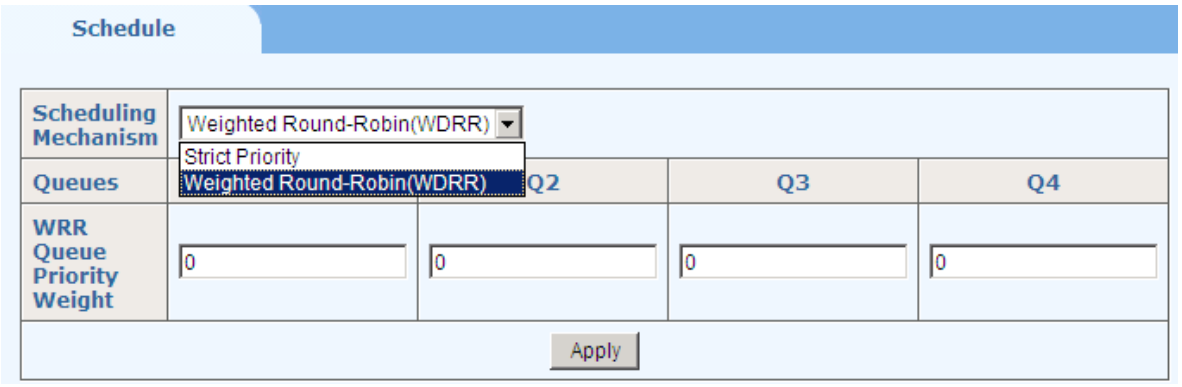
This page sets the queue scheduling algorithm and related parameters.

Scheduling Mechanism can be set to **Strict Priority** or **Weighted Round-Robin (WRR)**

Strict Priority uses the strict priority (SP) algorithm for queue scheduling

Weighted Round-Robin (WRR) uses the weighted round robin (WRR) algorithm for queue scheduling

WRR Queue Priority Weight customizes the weights to be assigned to queues 1 through 4. The value ranges from 1 to 55.



7.3 Transmit Queues

This page sets the 802.1p priority to local precedence mapping. The following table lists the default mapping between 802.1p priority and local precedence:

802.1p priority	Local precedence
0	Q1
1	Q1
2	Q2
3	Q2
4	Q3
5	Q3
6	Q4
7	Q4

Queues

Transmit Queues Setting								
Priority	0	1	2	3	4	5	6	7
Transmit Queues	◉ Q1	◉ Q1	○ Q1	○ Q1	○ Q1	○ Q1	○ Q1	○ Q1
	○ Q2	○ Q2	◉ Q2	◉ Q2	○ Q2	○ Q2	○ Q2	○ Q2
	○ Q3	○ Q3	○ Q3	○ Q3	◉ Q3	◉ Q3	○ Q3	○ Q3
	○ Q4	○ Q4	○ Q4	○ Q4	○ Q4	○ Q4	◉ Q4	◉ Q4

Apply

7.4 DSCP Map

This page sets the mapping between the DSCP value and the 802.1p priority.

DSCP map

DSCP Map Setting															
DSCP Map	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
Priority	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
DSCP Map	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29
Priority	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
DSCP Map	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44
Priority	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
DSCP Map	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59
Priority	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
DSCP Map	60	61	62	63	.										
Priority	0	0	0	0	.										

Apply

8 Forwarding

There are **Unicast MAC Address**, **Multicast MAC Address**, **IGMP Snooping**, **MVR** and **Unknown Multicast** in Forwarding, shown as follows.

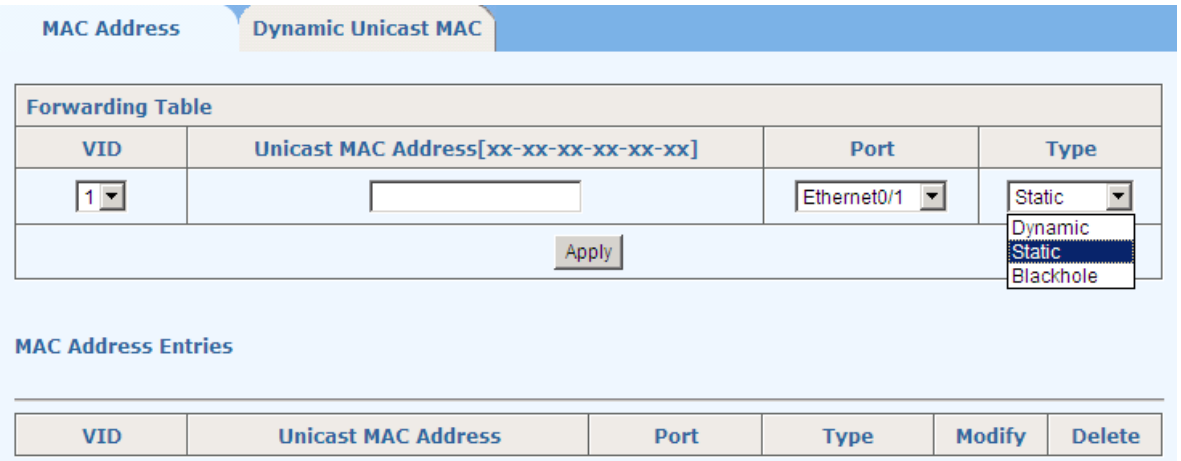
8.1 Unicast MAC Address

8.1.1 MAC Address

On this page, you can add, modify, or delete an entry in MAC table.

VID	Specifies a VLAN group with which the MAC address corresponds.
Unicast MAC Address	Specifies the destination MAC address.
Port	Specifies the port of the outbound interface.
Type	Choose among **Dynamic, Static and Blackhole**. **Dynamic** indicates a dynamic MAC address entry, **Static** indicates a static MAC address entry, and **Blackhole** indicates a blackhole MAC address entry.

The bottom part of *MAC Address* tab page lists all existing unicast MAC addresses, as well as the information of each unicast MAC address. The user can also modify or delete an existing unicast MAC address.



8.1.2 Dynamic Unicast MAC

This page lists all dynamic unicast MAC addresses. An entry can be deleted.

MAC Address | Dynamic Unicast MAC

VID	Unicast MAC Address	Port	Type	Delete
1	00-1f-d0-6a-de-f0	Ethernet1/1	Learned	Delete
1	00-1e-6e-00-81-64	Ethernet1/2	Learned	Delete
1	00-1e-6e-00-34-9a	Ethernet1/2	Learned	Delete

8.2 Multicast MAC Address

This page sets multicast MAC address entries. Each multicast MAC address entry contains multicast address, forward ports, and VID.

VID Specifies the VLAN group of which the forwarding ports are members.

Multicast MAC Address Multicast MAC address, in the form of H-H-H-H-H-H.

Member Specifies forwarding ports for the specified multicast MAC group address. One or more ports can be added as the member.

The bottom part of this page lists all existing multicast MAC addresses, as well as the information of each multicast MAC address. The user can also modify or delete an existing multicast MAC address.

Multicast MAC Address

Static Multicast Forwarding Table

VID	1																													
Multicast MAC Address	[xx-xx-xx-xx-xx-xx]																													
Port	Ethernet0/																								Ethernet1/			
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	1	2	3	4
Member	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

Apply

Static Multicast MAC Address Entries

VID	Multicast MAC Address	Member Ports	Modify	Delete

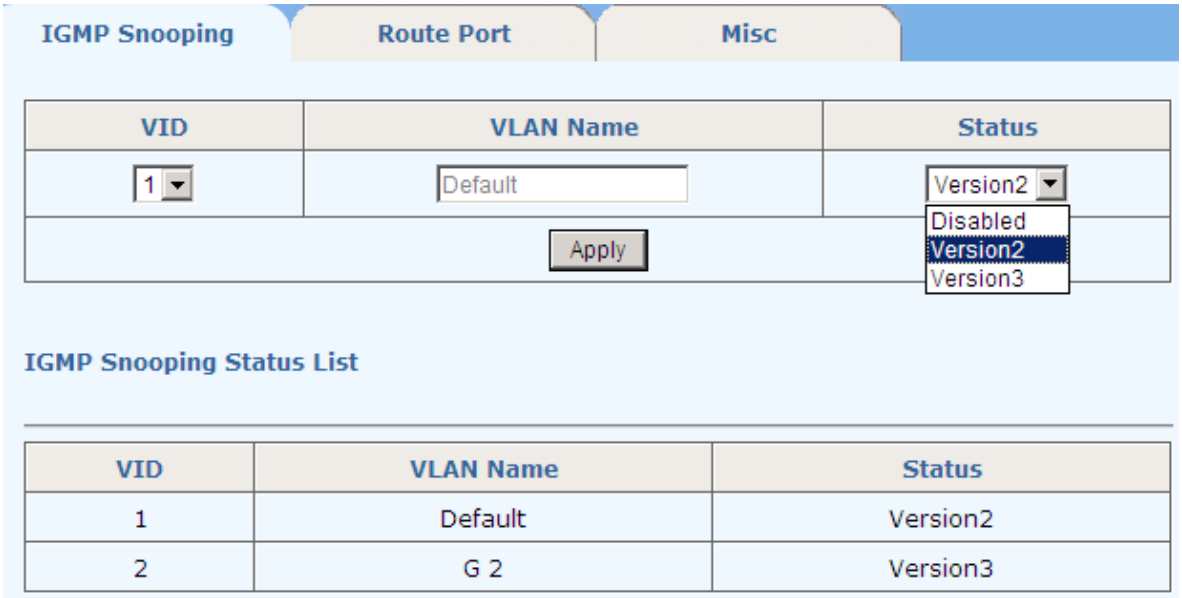
8.3 IGMP Snooping

There are three tab pages on this webpage for configuration: **IGMP Snooping**, **Route Prot** and **Misc**. IGMP Snooping should be enabled in Advanced Configuration first.

(1) *IGMP Snooping*

In this page, you can enable IGMP Snooping feature for a VLAN group. By default, the IGMP Snooping feature is disabled.

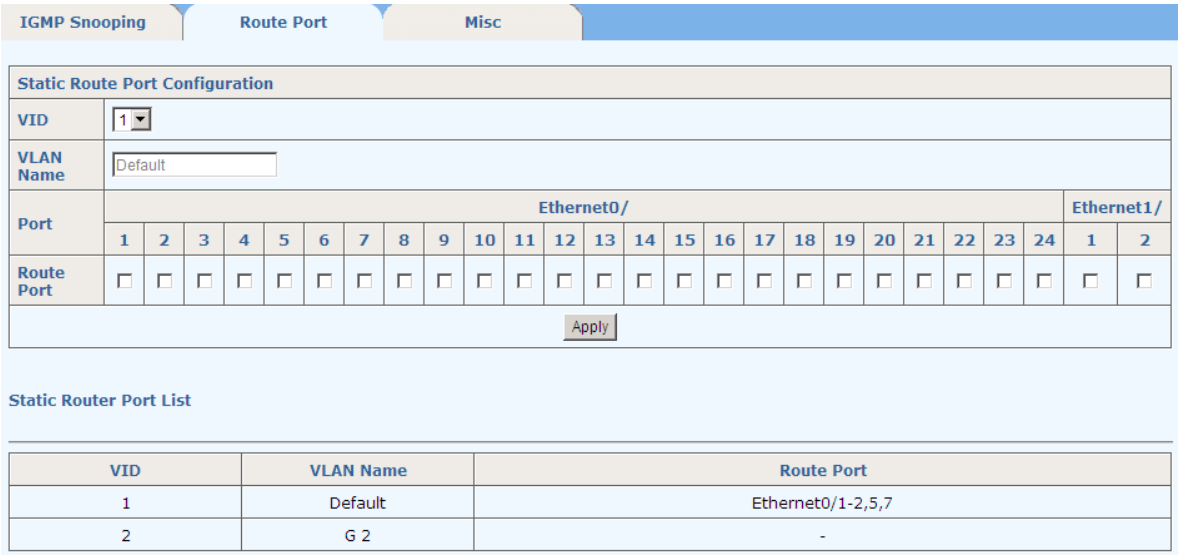
The bottom part of this page lists all VLAN IGMP Snooping feature status.



(2) *Route Port*

In this page, you can configure a port in a specified VLAN group as a static router port. By default, a port is not a static router port.

The bottom part of this page lists static router ports of all VLANs.



(3) *Misc*

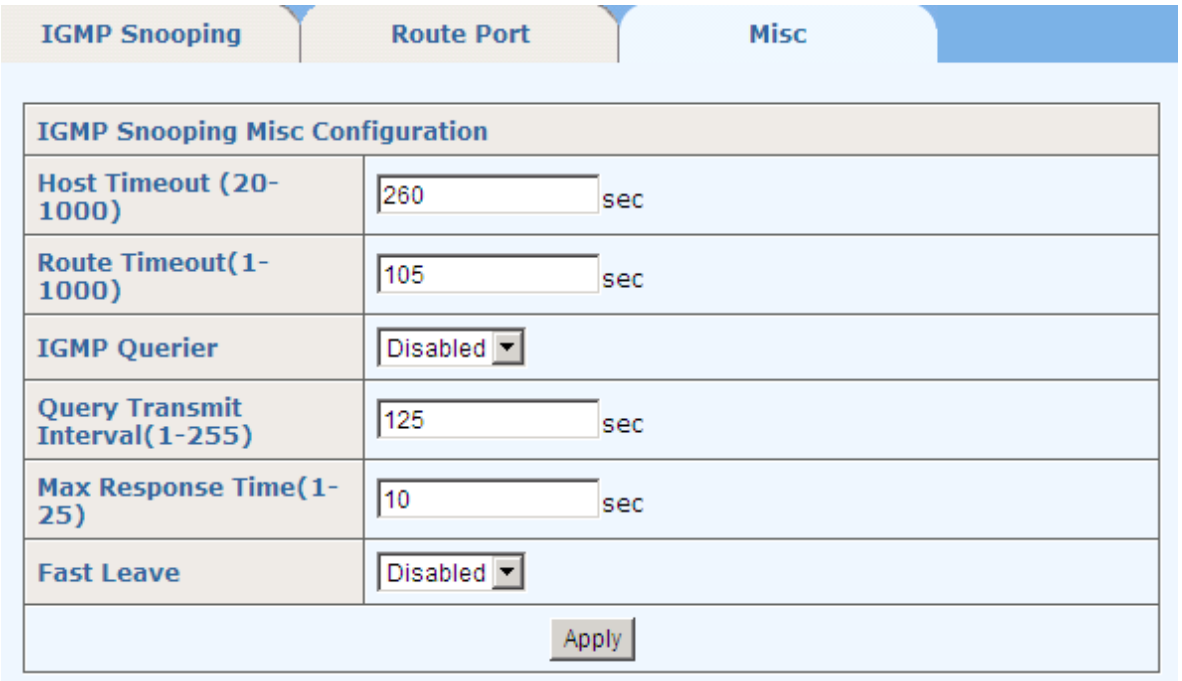
This tab page sets IGMP Snooping Misc configuration parameters: Host Timeout, Route Timeout, IGMP Querier, Query Transmit Interval, Max Response Time, and Fast Leave.

Host Timeout	It is in the range of 200 to 1000; by default, the value is 260 seconds.
Route Timeout	It is in the range of 1 to 1000; by default, the value is 105 seconds.
IGMP Querier	Enable/disable IGMP Querier function.

Query Transmit Interval It is in the range of 1 to 300, by default, the value is 125 seconds.

Max Response Time It is in the range of 1 to 25, by default, the value is 10 seconds.

Fast Leave To enable/disable the Fast Leave feature.



8.4 MVR

MVR (Multicast VLAN Registration) allows a subscriber on a port to subscribe or unsubscribe a multicast stream on the network-wide multicast VLAN. It allows the single multicast VLAN to be shared in the network while subscribers remain in separate VLANs. MVR provides the ability to continuously send multicast streams in the multicast VLAN, but it isolates the streams from the subscriber VLANs for bandwidth and security reasons.

8.4.1 MVR Configuration

This page sets MVR State, Multicast VLAN ID, MVR Mode, Source Port and Receive Port for MVR configuration.

MVR State Globally enable or disable MVR on the switch.

Multicast VLAN ID Specify the VLAN group in which multicast data is received. All source ports must be members of this VLAN. The default VLAN ID is 1.

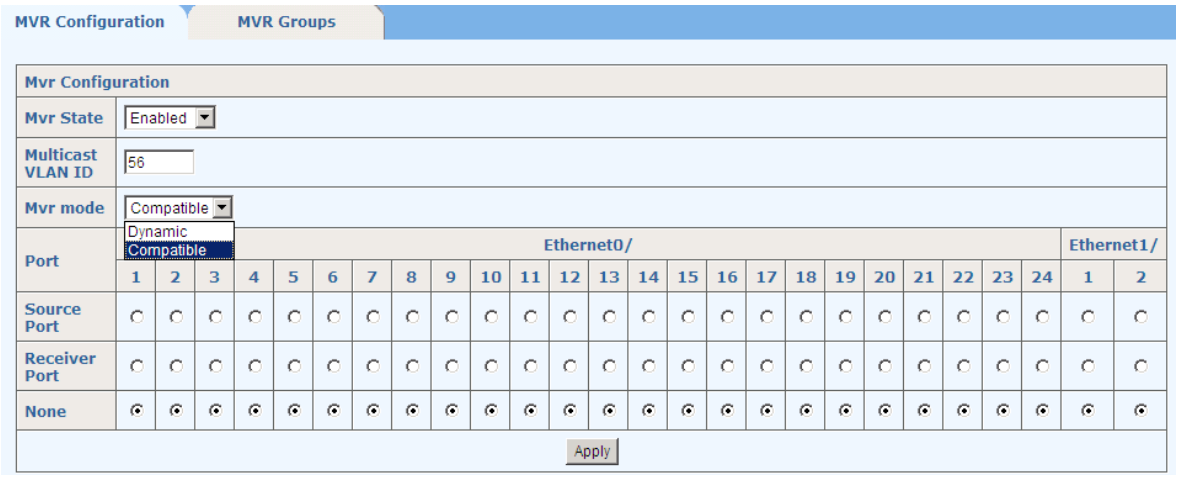
MVR Mode Choose the mode between **compatible** and **dynamic**.

Compatible mode The switch does not send out any IGMP reports to source port(s), a manual multicast forwarding configuration is needed. In the case that MVR Group is not configured, multicast data received by the switch is forwarded to all ports, regardless of the port MVR membership setting. In the case that MVR Group is successfully configured, the multicast data is forwarded only to those joined receiver ports set by MVR static configuration.

Dynamic mode The switch sends IGMP “leave” and “join” reports through the source port(s) to the other multicast devices (such as multicast routes or servers) in the multicast VLAN. This allows the multicast devices to update the multicast forwarding table to forward or not to forward multicast traffic to the receiver ports.

Source Port Configure uplink ports that receive and send multicast data as source ports. Subscribers cannot be directly connected to source ports. All source ports on a switch are members of a single multicast VLAN group.

Receive Port Configure a port as a receiver port if it is a subscriber port and thus should receive multicast data. However, it won’t be able to receive the multicast data until it becomes a member of the multicast group, either statically or by using IGMP join messages. Receiver ports are untagged members of the multicast VLAN group.

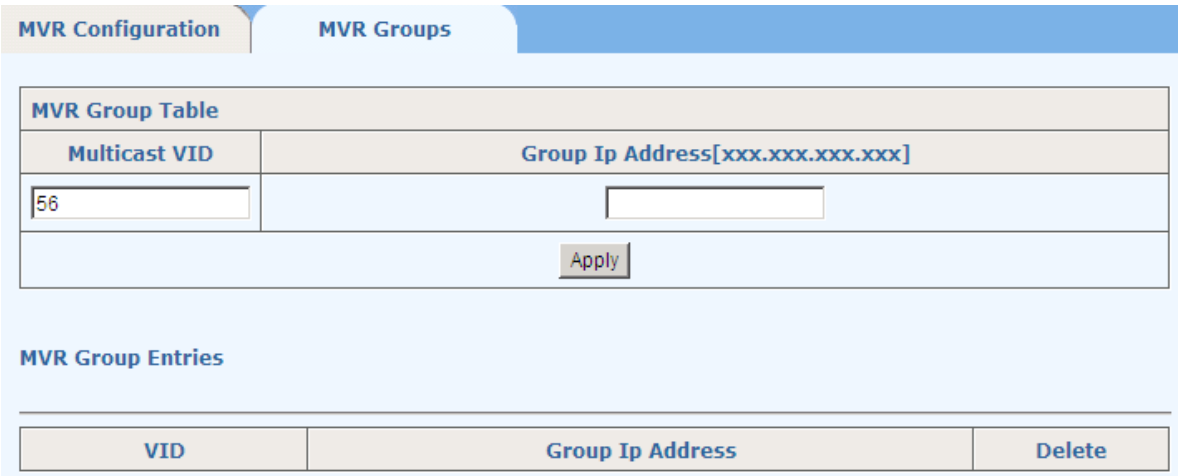


8.4.2 MVR Groups

This page sets specific static **Group IP Address (es)** for MVR.

Multicast VID multicast VLAN ID
Group IP Address static IP multicast address to be added

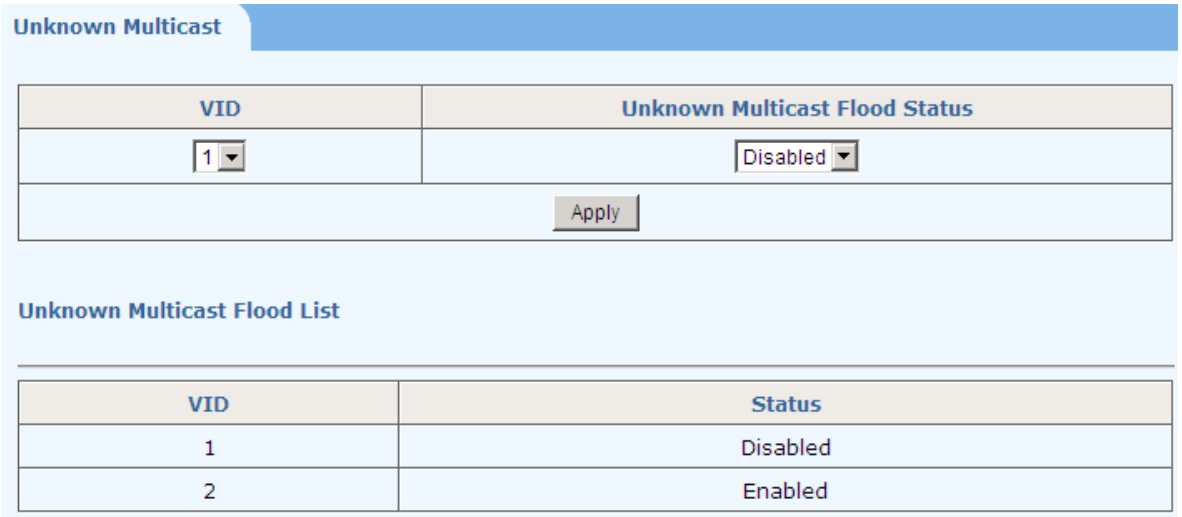
The bottom part of this page lists all group IP addresses for the multicast VLAN.



8.5 Unknown Multicast

Unknown Multicast Flood Status: Enable/disable Unknown Multiscast Flood Status for a specified VLAN group.

The bottom part of this page lists all of the unknown multicast flood lists.



9 Security

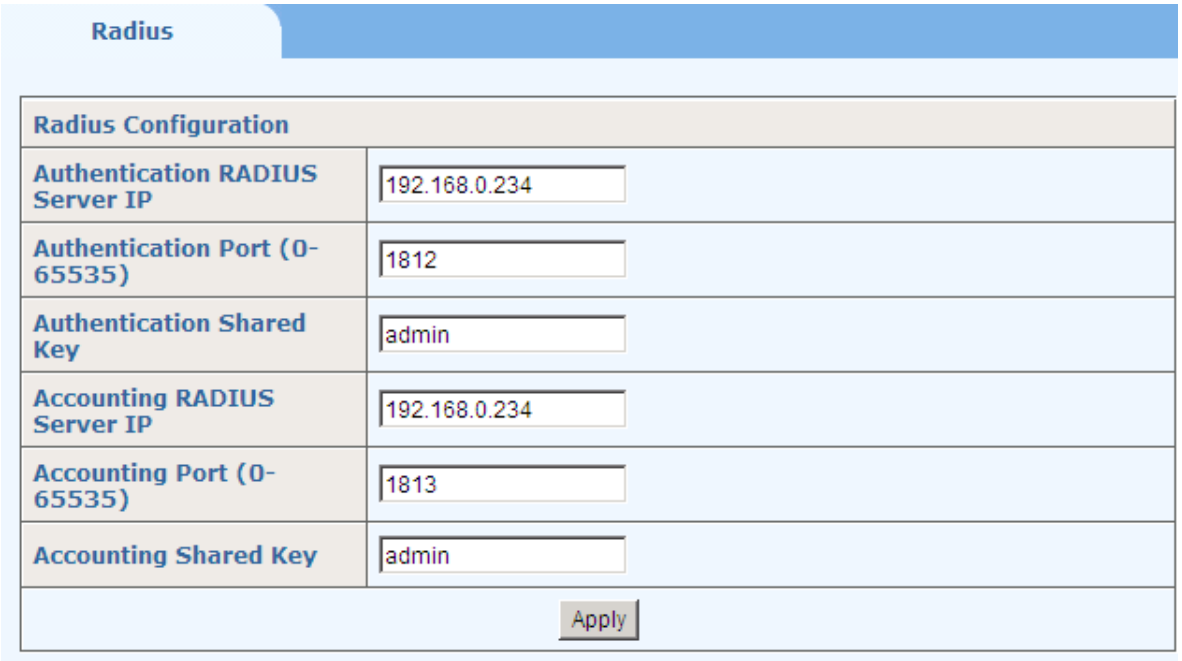
There are 12 sub-menus in Security, shown as follows.

- Security
  - Management Security
  - Port Authentication
  - MAC Authentication
  - IP Binding
  - DHCP Snooping
  - IP Source Guard
  - DHCP Limit
  - Dynamic ARP Inspection
  - ARP Limit
  - Storm Control
  - Port Security
  - Vlan Isolation

9.1 Management Security

This page configures the 802.1x system as follows: Authentication RADIUS Server IP, Authentication Port, Authentication Shared Key, Accounting RADIUS Server IP, Accounting Port and Accounting Shared Key.

Authentication RADIUS Server IP	IP address of the radius server to be used, a valid unicast address in dotted decimal notation; the default value is 192.168.0.234.
Authentication Port	UDP port number of the radius server, ranging from 0 to 65535; the default value is 1812.
Authentication Shared Key	Sets a shared key for radius messages. String length is 1 to 15 characters.
Accounting RADIUS Server IP	IP address of accounting radius server to be used, a valid unicast address in dotted decimal notation; the default value is 192.168.0.234.
Accounting Port	UDP port number of the radius server, ranging from 0 to 65535; the default value is 1813.
Accounting Shared Key	Sets a shared key for accounting radius. String length is from 1 to 15 characters.



9.2 Port Authentication

802.1x should be enabled in Authentification mode first in Advanced Configuration. There are two tab pages on this webpage for the user to configure various parameters of 802.1x: 802.1x Port and 802.1x Misc.

9.2.1 802.1x Port

This tab page sets 802.1x port enabling, re-authentication, access control, and Guest VLAN for a specified Ethernet port. There are three choices for **Port Control**: **Auto**, **Force Authorized** and **Force Unauthorized**.

Auto specify to operate in auto access control mode. When one port operates in this mode, all the unauthenticated hosts connected to it are unauthorized. In this case, only EAPoL packets can be exchanged between the switch and the hosts. And the authenticated hosts connected to the port are authorized to access the network resources.

Force Authorized specify to operate in authorized-force access control mode. When one port operates in this mode, all the hosts connected to it can access the network resources without the need of authentication.

Force Unauthorized specify to operate in unauthorized-force access control mode. When one port operates in this mode, the hosts connected to it cannot access the network resources.

Guest VLAN a guest VLAN can be enabled for each IEEE 802.1x port on the switch to provide limited services to the clients.

The bottom part of this page lists all 802.1x port status.

802.1x Port | 802.1x Misc

Port	802.1x Admin	PortControl	ReAuth	Guest VLAN
Ethernet0/1	Enabled	ForceAuthorized	Enabled	Enabled

Apply

802.1x Port Status List

Port	802.1x Admin	PortControl	ReAuth	Guest VLAN	Port State
Ethernet0/1	Enabled	ForceAuthorized	Enabled	Enabled	Link Down
Ethernet0/2	Enabled	ForceUnauthorized	Enabled	Disabled	Link Down
Ethernet0/3	Enabled	Auto	Disabled	Enabled	Link Down
Ethernet0/4	Enabled	Auto	Disabled	Enabled	Link Down
Ethernet0/5	Disabled	ForceAuthorized	Disabled	Disabled	Link Down
Ethernet0/6	Disabled	ForceAuthorized	Disabled	Disabled	Link Down
Ethernet0/7	Disabled	ForceAuthorized	Disabled	Disabled	Link Down
Ethernet0/8	Disabled	ForceAuthorized	Disabled	Disabled	Link Down
Ethernet0/9	Disabled	ForceAuthorized	Disabled	Disabled	Link Down
Ethernet0/10	Disabled	ForceAuthorized	Disabled	Disabled	Link Down

9.2.2 802.1x Misc

This tab page configures 802.1x: Quiet Period, Tx Period, Supplicant Timeout, Server Timeout, Max Request Count, Reauth Period, and Guest VLAN.

Quiet Period

Sets the quiet-period, when a supplicant system fails to pass the authentication, the switch quiets for the set period before it processes another authentication request re-initiated by the supplicant system. During this quiet period, the switch does not perform any 802.1x authentication-related actions for the supplicant system. The value is in the range of 1 to 65535, and is set to 60 seconds by default.

Tx Period

Sets the transmission timer, and is triggered in two cases. The first case is when the client requests authentication, the switch sends a unicast request/identity packet to a supplicant system and then triggers the transmission timer. The switch sends another request/identity packet to the supplicant system if it does not receive the reply packet from the supplicant system when this timer times out. The second case is when the switch authenticates the 802.1x client which cannot request for authentication actively. The switch sends multicast request/identity packets periodically through the port enabled

by 802.1x function. In this case, this timer sets the interval to send the multicast request/identity packets. It is in the range of 1 to 65535; the default value is 30 seconds.

Supplicant Timeout: Sets the supplicant system timer, this timer sets the supp-timeout period and is triggered by the switch after the switch sends a request/challenge packet to a supplicant system. The switch sends another request/challenge packet to the supplicant system if the switch does not receive any response from the supplicant system when this timer times out. It is in the range of 1 to 300; the default value is 30 seconds.

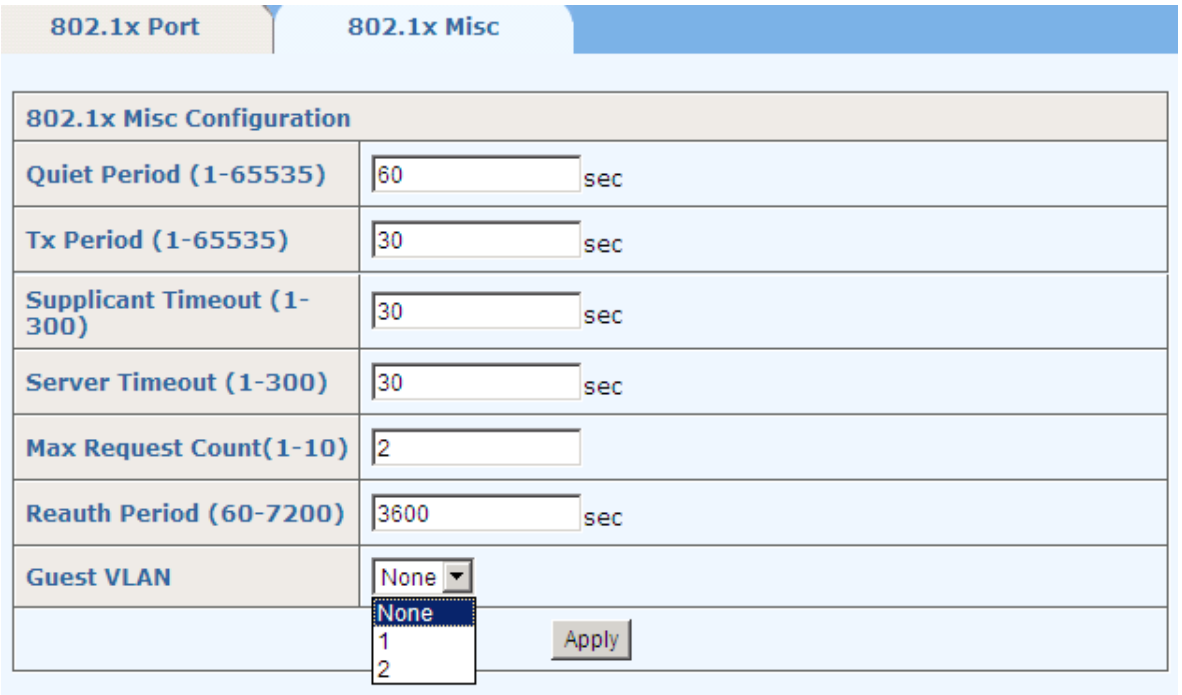
Server Timeout Sets the radius server timer, this timer sets the server-timeout period. After sending an authentication request packet to the radius server, a switch sends another authentication request packet if it does not receive any response from the radius server when this timer times out. It is in the range of 1 to 300; the default value is 30 seconds.

Max Request Count Sets the maximum number of times that a switch sends authentication request packets to a user. It is in the range of 1 to 10, and the default value is 2.

Reauth Period Sets re-authentication interval in seconds. After this timer expires, the switch indicates: 802.1x re-authentication. It is in the range of 60 to 7200; the default value is 3600 seconds.

Guest VLAN Can choose a guest VLAN on the switch to provide limited services to clients, such as downloading.

When enabling a guest VLAN on an IEEE 802.1x port, the switch assigns the client port to a guest VLAN in case that the switch does not receive any response to its EAP request/identity frame, or EAPOL packets are not sent by the client. The switch allows the client that is failed in authentication to access the guest VLAN, regardless of whether EAPOL packets have been detected. However, access to external ports out of guest VLAN still needs to be authorized.

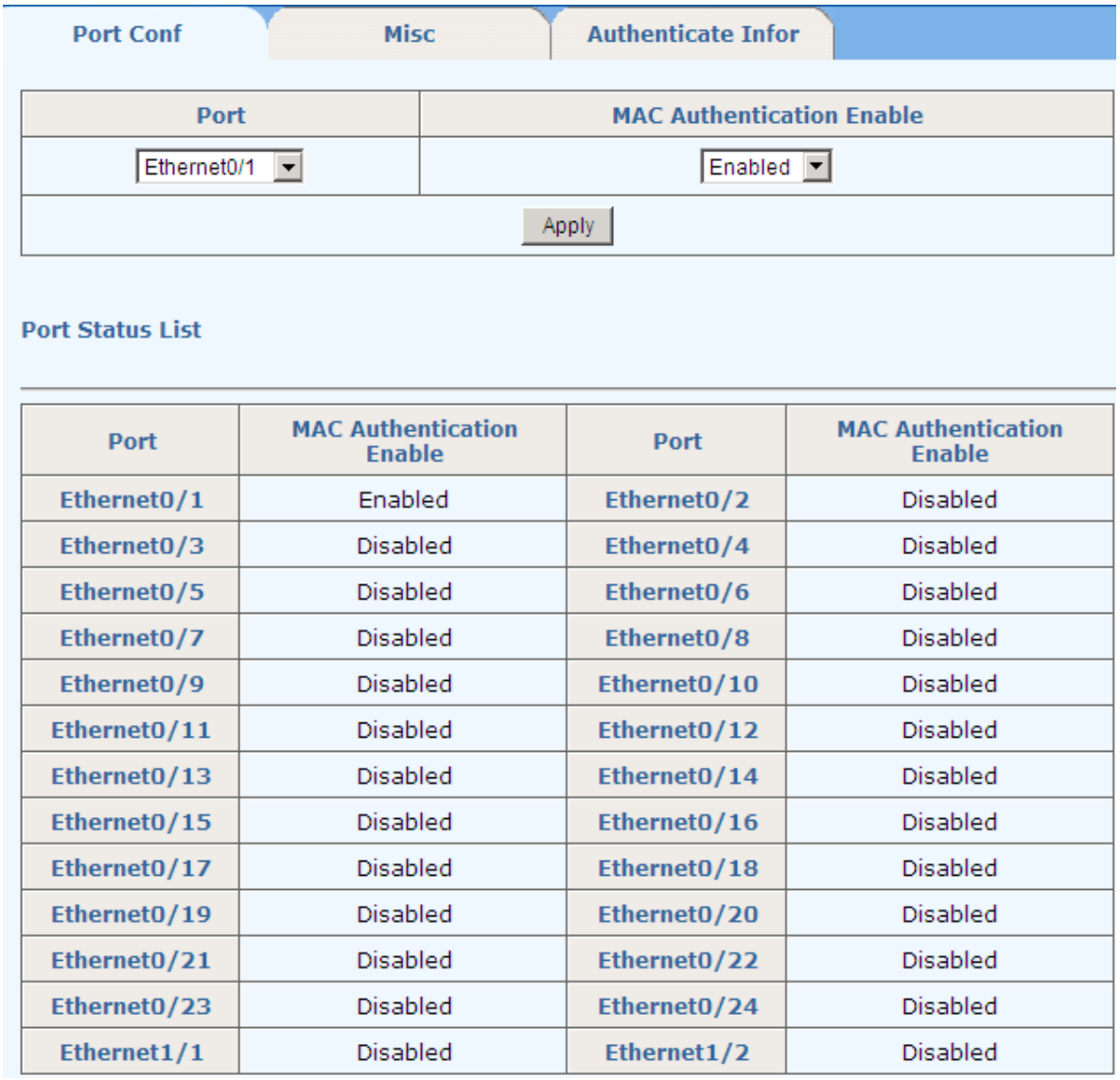


9.3 MAC Authentication

MAC Authentication should be enabled in Authentification mode first in Advanced Configuration. There are three tab pages in this page: Port Conf, Misc and Authenticate Infor.

9.3.1 Port Conf

This page enables **MAC Authentication** on a specific port.



Port	MAC Authentication Enable	Port	MAC Authentication Enable
Ethernet0/1	Enabled	Ethernet0/2	Disabled
Ethernet0/3	Disabled	Ethernet0/4	Disabled
Ethernet0/5	Disabled	Ethernet0/6	Disabled
Ethernet0/7	Disabled	Ethernet0/8	Disabled
Ethernet0/9	Disabled	Ethernet0/10	Disabled
Ethernet0/11	Disabled	Ethernet0/12	Disabled
Ethernet0/13	Disabled	Ethernet0/14	Disabled
Ethernet0/15	Disabled	Ethernet0/16	Disabled
Ethernet0/17	Disabled	Ethernet0/18	Disabled
Ethernet0/19	Disabled	Ethernet0/20	Disabled
Ethernet0/21	Disabled	Ethernet0/22	Disabled
Ethernet0/23	Disabled	Ethernet0/24	Disabled
Ethernet1/1	Disabled	Ethernet1/2	Disabled

9.3.2 Misc

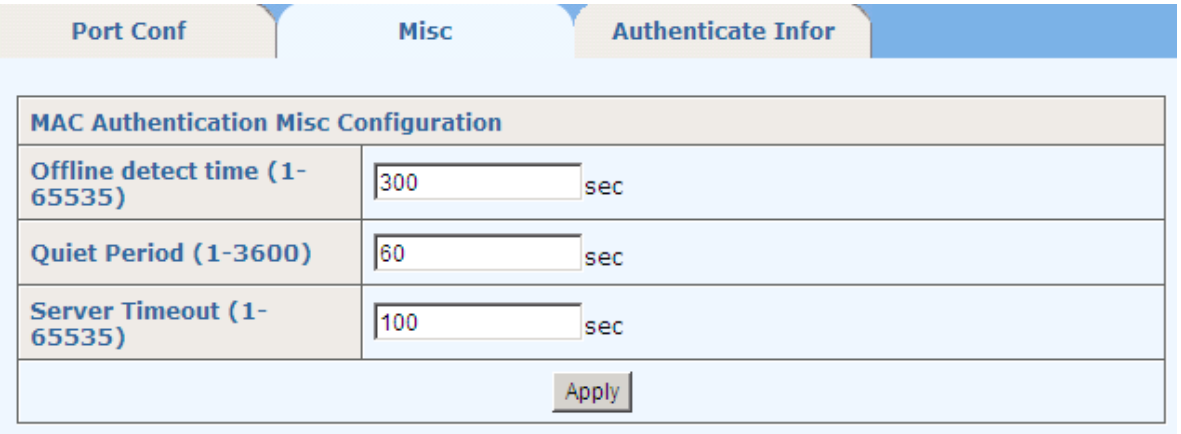
This page sets **Offline detect time**, **Quiet Period,** and **Server Timeout** for MAC Authentication.

Offline detect time To check whether the client is offline in this time interval. The switch will immediately notify the RADIUS server to stop billing from the client when offline is detected. The value ranges from 1 to 65535, and the default value is 300 seconds.

Quiet Period To set the time interval the client must wait after a client

authentication fails. During this time interval, the switch does not perform the user authentication function. The value ranges from 1 to 3600, and the default value is 60 seconds.

Server Timeout To set the time interval the switch waits for a response, when there is a connection request from the authentication server to the client. The value ranges from 1 to 65535, and the default value is 100 seconds.

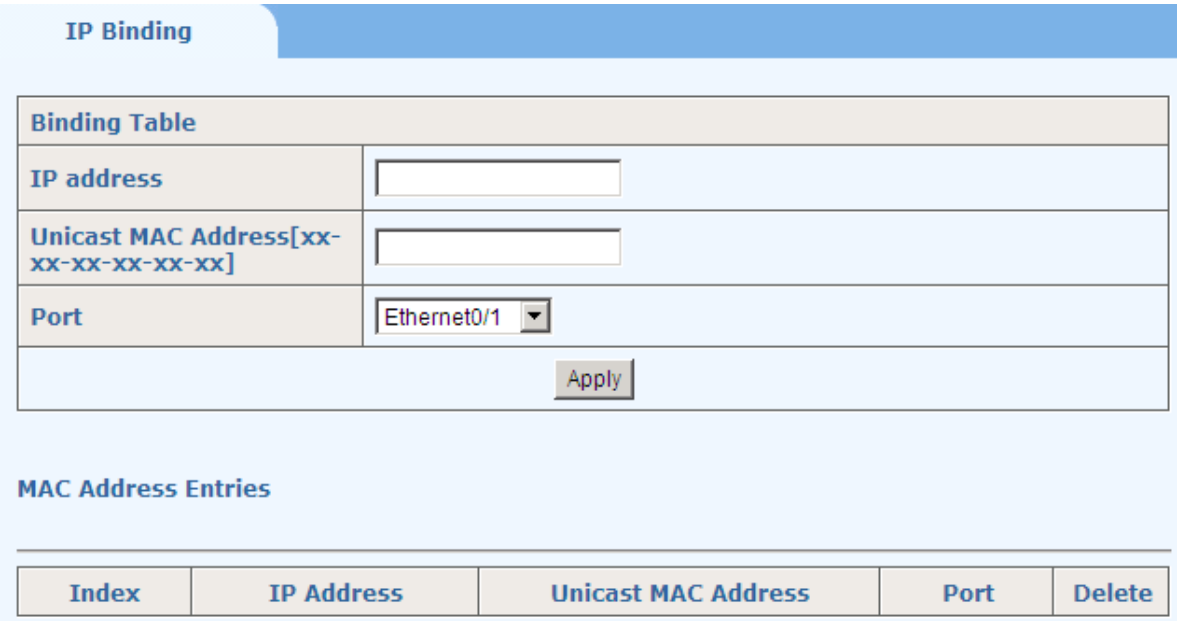


9.3.3 Authenticate Infor

This page lists all the MAC authentication information including **MAC Address, From Port, and Authenticate state.**

9.4 IP Binding

This page sets **IP address**, **Unicast MAC Address,** and **Port** for IP binding. The bottom part of this page lists all the IP binding information.

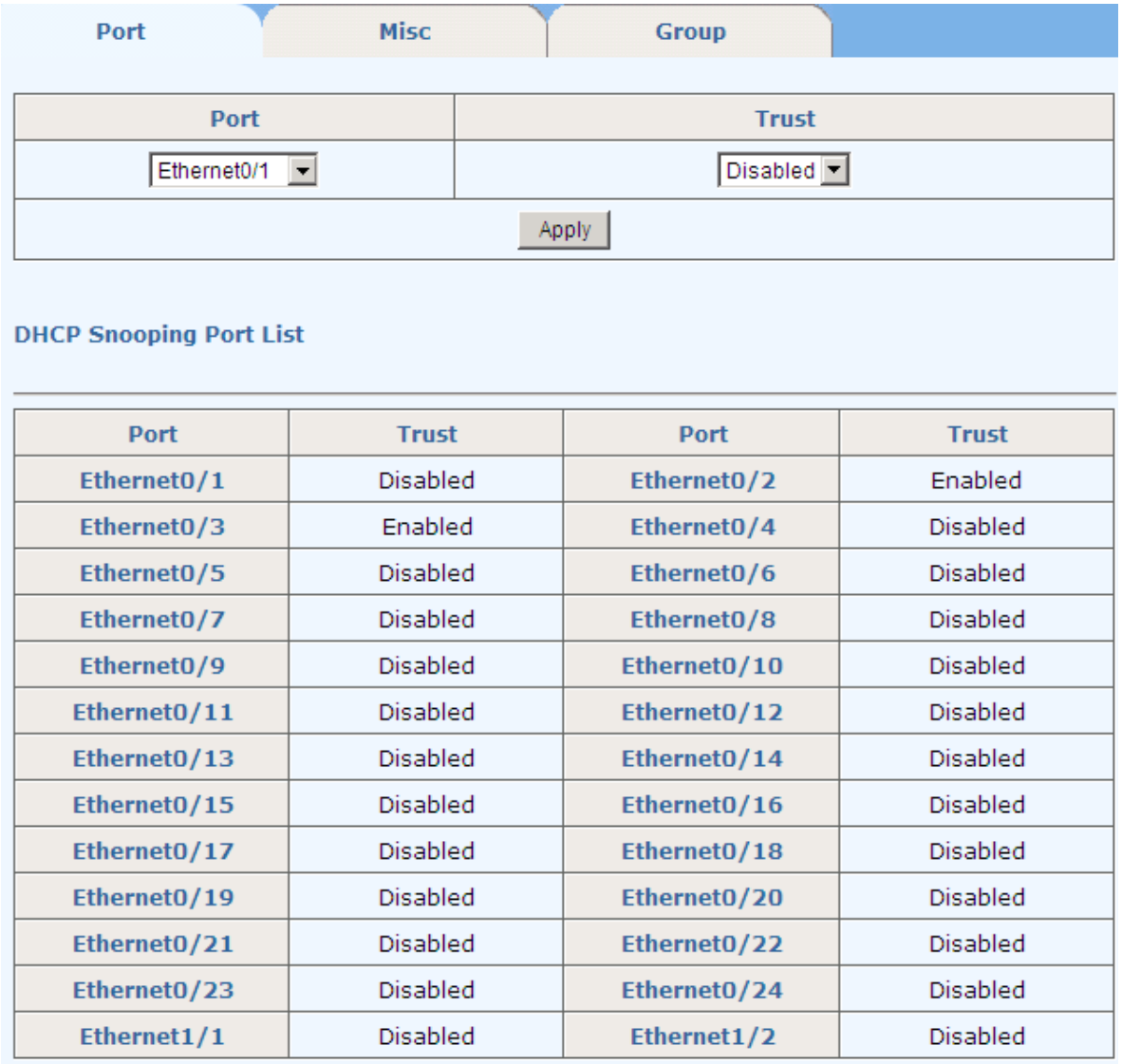


9.5 DHCP Snooping

DHCP Snooping should be enabled in System Advanced Configuration first. There are three tab pages to configure the **DHCP Snooping** function: **Port**, **Misc** and **Group**.

9.5.1 Port

This page sets the DHCP trust port for the specified Ethernet Port**.** The bottom part of this page lists all the DHCP Snooping Port.

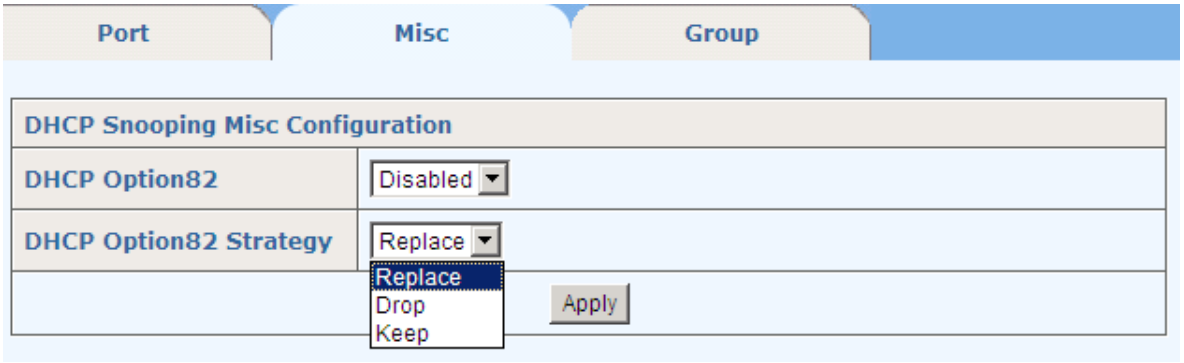


9.5.2 Misc

This page sets the DHCP Snooping Misc Configuration.

DHCP Option82 to enable/disable the DHCP Option82 function.

DHCP Option82 Strategy the relaying modes of DHCP Option82, there are three modes of this strategy: **Replace**, **Drop** and **Keep**.

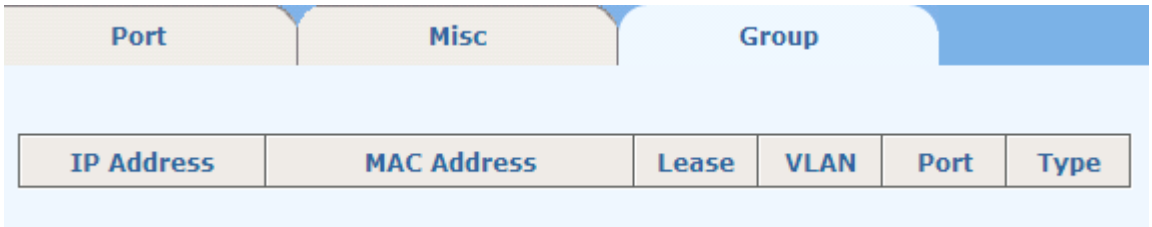


9.5.3 Group

This page displays the information of DHCP group.

Lease lease time.
Type the type of DHCP.

The bottom part of this page lists all the information of DHCP groups.



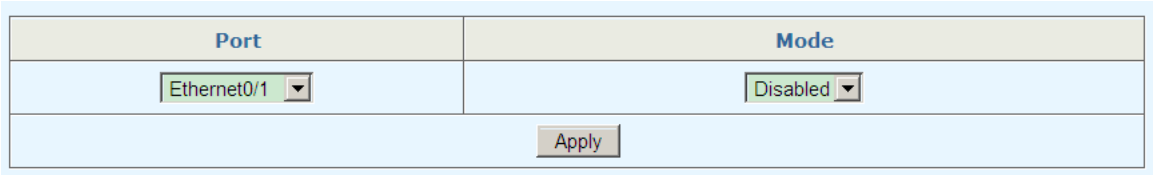
9.6 IP Source Guard

By filtering packets on a per-port basis, IP source guard prevents illegal packets from traveling through, thus improving the network security. After receiving a packet, the port looks up the key attributes (including IP address, MAC address and VLAN tag) of the packet in the binding entries of the IP source guard. If there is a match, the port forwards the packet. Otherwise, the port discards the packet.

You can manually set static IP Binding entries, or use DHCP Snooping to provide dynamic binding entries. Binding is on a per-port basis. After a binding entry is configured on a port, it is effective only to the port.

9.6.1 IP Source Guard Setting

On this page, you can enable or disable the IP Soure Guard function on a specified port. And is shows the IP Source Guard Port List at the bottom of the page.



IP Source Guard Port List

Port	Mode	Port	Mode
Ethernet0/1	Disabled	Ethernet0/2	Disabled
Ethernet0/3	Disabled	Ethernet0/4	Disabled
Ethernet0/5	Disabled	Ethernet0/6	Disabled
Ethernet0/7	Disabled	Ethernet0/8	Disabled
Ethernet0/9	Disabled	Ethernet0/10	Disabled
Ethernet0/11	Disabled	Ethernet0/12	Disabled
Ethernet0/13	Disabled	Ethernet0/14	Disabled
Ethernet0/15	Disabled	Ethernet0/16	Disabled
Ethernet0/17	Disabled	Ethernet0/18	Disabled
Ethernet0/19	Disabled	Ethernet0/20	Disabled
Ethernet0/21	Disabled	Ethernet0/22	Disabled
Ethernet0/23	Disabled	Ethernet0/24	Disabled
Ethernet1/1	Disabled	Ethernet1/2	Disabled

9.6.2 IP Source Guard Status

It shows the IP Source Guard status, shown as follows, including the port number, mode, IP address, MAC addreass and VLAN. Such as in the following screen, it represents that the IP source guard is dynamically set on the port Ethernet1/1, and only the packets from the device with the IP address of 192.168.131.254, the MAC address of 20-cf-30-53-4d-a1 and the VLAN of 2, can pass the port Ethernet1/1.

Port	Mode	IP Address	MAC Address	VLAN
Ethernet1/1	dynamic	192.168.131.254	20-cf-30-53-4d-a1	2

9.7 DHCP Limit

There are two tab pages to configure the related rate parameters of **DHCP Limit**.

9.7.1 Port

This page sets the DHCP Rate Limit for a specified Ethernet Port.

Rate Limit Enable /disable the function of DHCP Rate limit for a specified port
Rate It is in the range of 10 to 150, the default value is 15pps.
State Port state, when it over speeds, it will be shown as “OFF”.

The bottom part of this page lists all the DHCP Rate Limit ports.

Port | Misc

Port	Rate Limit	Rate(pps)
Ethernet0/1	Enabled	20
Apply		

DHCP Rate Limit Port List

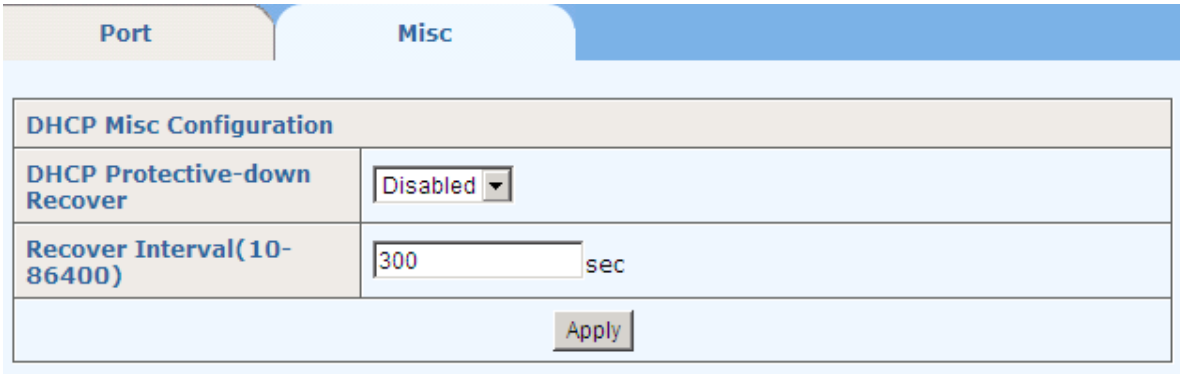
Port	Rate Limit	Rate (pps)	State	Port	Rate Limit	Rate (pps)	State
Ethernet0/1	Enabled	20	On	Ethernet0/2	Enabled	20	On
Ethernet0/3	Enabled	50	On	Ethernet0/4	Disabled	60	On
Ethernet0/5	Disabled	15	On	Ethernet0/6	Disabled	15	On
Ethernet0/7	Disabled	15	On	Ethernet0/8	Disabled	15	On
Ethernet0/9	Disabled	15	On	Ethernet0/10	Disabled	15	On
Ethernet0/11	Disabled	15	On	Ethernet0/12	Disabled	15	On
Ethernet0/13	Disabled	15	On	Ethernet0/14	Disabled	15	On
Ethernet0/15	Disabled	15	On	Ethernet0/16	Disabled	15	On
Ethernet0/17	Disabled	15	On	Ethernet0/18	Disabled	15	On
Ethernet0/19	Disabled	15	On	Ethernet0/20	Disabled	15	On
Ethernet0/21	Disabled	15	On	Ethernet0/22	Disabled	15	On
Ethernet0/23	Disabled	15	On	Ethernet0/24	Disabled	15	On
Ethernet1/1	Disabled	15	On	Ethernet1/2	Disabled	15	On

9.7.2 Misc

This page set the DHCP Misc Configuration.

DHCP Protective-down Recover to enable/disable the recovering function when DHCP has been off due to exceeding the speed limit.

Recover Interval When DHCP traffic over-speeds the rate limit, the specified port will be disabled for a specified time. After this interval, the portwill recover automatically to be enabled. It is in the range of 10 to 86400, the default value is 300 second.



9.8 Dynamic ARP Inspection

There are three tab pages to set the **Dynamic ARP Inspection** function.

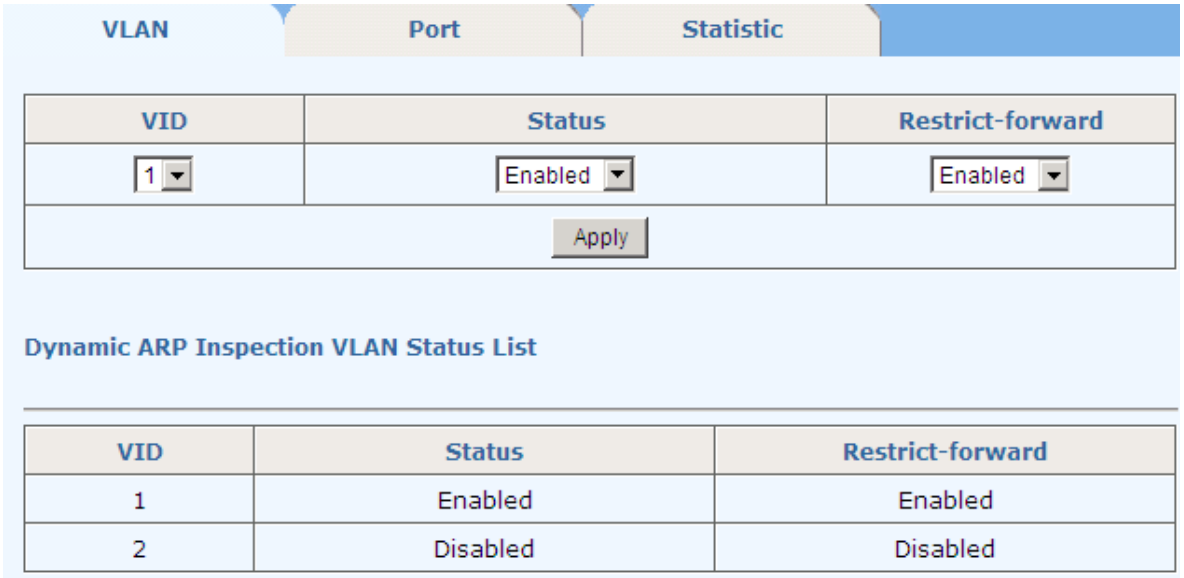
9.8.1 VLAN

VID: to specify the VLAN needed to configure

Status to enable/disable the Dynamic ARP Inspection function based on VLAN

Restrict-forward to enable/disable the function of restrict-forward ARP. When enabled, ARP packets on the un-trust port will be checked if they are consistent with the DHCP-Snooping information, if matching, ARP packets will be forwarded.

The bottom part of this page lists all Dynamic ARP Inspection VLAN status.



9.8.2 Port

This page sets the Dynamic ARP Inspection trust port for the specified Ethernet Port**.** The bottom part of this page lists all the Dynamic ARP Inspection Ports.

VLAN | Port | Statistic

Port	Trust
Ethernet0/1	Disabled

Apply

Dynamic ARP Inspection Port List

Port	Trust	Port	Trust
Ethernet0/1	Disabled	Ethernet0/2	Enabled
Ethernet0/3	Enabled	Ethernet0/4	Disabled
Ethernet0/5	Disabled	Ethernet0/6	Disabled
Ethernet0/7	Disabled	Ethernet0/8	Disabled
Ethernet0/9	Disabled	Ethernet0/10	Disabled
Ethernet0/11	Disabled	Ethernet0/12	Disabled
Ethernet0/13	Disabled	Ethernet0/14	Disabled
Ethernet0/15	Disabled	Ethernet0/16	Disabled
Ethernet0/17	Disabled	Ethernet0/18	Disabled
Ethernet0/19	Disabled	Ethernet0/20	Disabled
Ethernet0/21	Disabled	Ethernet0/22	Disabled
Ethernet0/23	Disabled	Ethernet0/24	Disabled
Ethernet1/1	Disabled	Ethernet1/2	Disabled

9.8.3 Statistic

This page displays the statistic information of ARP packets. It can be cleared by clicking <Reset> button.

VLAN | Port | Statistic

VID	Forwarded	Dropped	DHCP Permits	DHCP Drops	Source MAC Failures	Dest MAC Failures	IP Validation Failures

Reset

9.9 ARP Limit

There are two tab pages here: Port and Misc

9.9.1 Port

This page sets the ARP Rate Limit for a specified Ethernet Port.

Rate Limit to enable/disable the function of ARP Rate limit for the specified port
Rate It is in the range of 10 to 150, the default value is 15 pps.
State port state, when over-speeds, it will be shown as “OFF”.

The bottom part of this page lists all the DHCP Rate Limit ports.

Port | Misc

Port	Rate Limit	Rate(pps)
Ethernet0/1	Enabled	55
	Apply	

ARP Rate Limit Port List

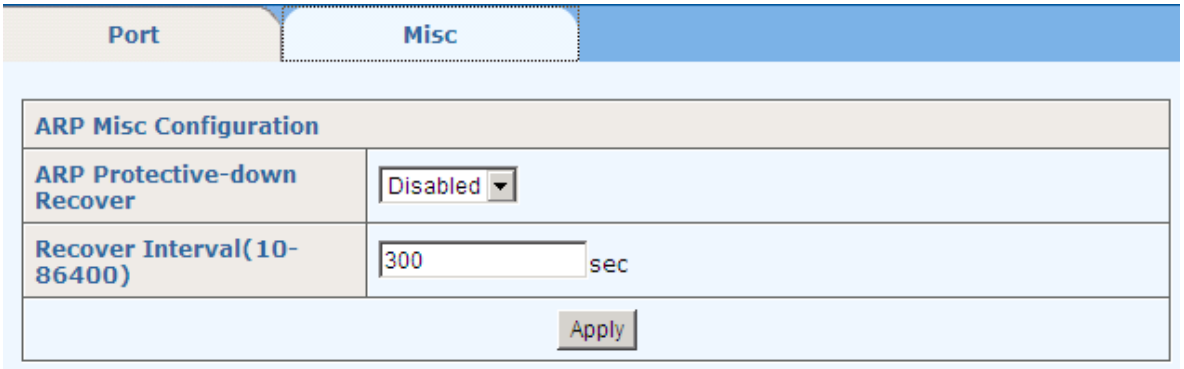
Port	Rate Limit	Rate (pps)	State	Port	Rate Limit	Rate (pps)	State
Ethernet0/1	Enabled	55	On	Ethernet0/2	Disabled	100	On
Ethernet0/3	Disabled	15	On	Ethernet0/4	Disabled	15	On
Ethernet0/5	Disabled	15	On	Ethernet0/6	Disabled	15	On
Ethernet0/7	Disabled	15	On	Ethernet0/8	Disabled	15	On
Ethernet0/9	Disabled	15	On	Ethernet0/10	Disabled	15	On
Ethernet0/11	Disabled	15	On	Ethernet0/12	Disabled	15	On
Ethernet0/13	Disabled	15	On	Ethernet0/14	Disabled	15	On
Ethernet0/15	Disabled	15	On	Ethernet0/16	Disabled	15	On
Ethernet0/17	Disabled	15	On	Ethernet0/18	Disabled	15	On
Ethernet0/19	Disabled	15	On	Ethernet0/20	Disabled	15	On
Ethernet0/21	Disabled	15	On	Ethernet0/22	Disabled	15	On
Ethernet0/23	Disabled	15	On	Ethernet0/24	Disabled	15	On
Ethernet1/1	Disabled	15	On	Ethernet1/2	Disabled	15	On

9.9.2 Misc

This page sets the ARP Misc Configuration.

ARP Protective-down Recover to enable/disable the recovering function when ARP has been off due to exceeding the speed limit.

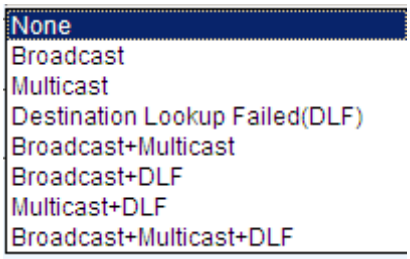
Recover Interval When ARP traffic over-speeds the rate limit, the specified port will be disabled for a specified time, after this interval, the port will recover automatic to be enabled. It is in the range of 10 to 86400, the default value is 300 second.

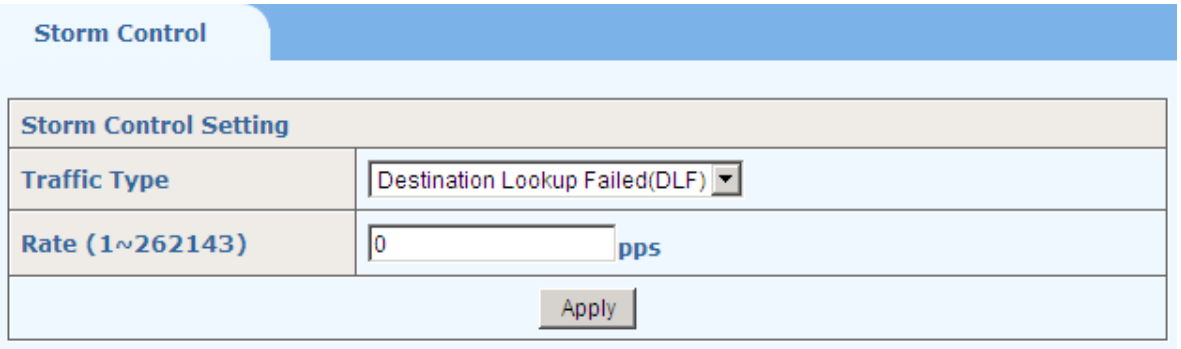


9.10 Storm Control

This page sets thresholds of the specified **Traffic Type**.

Traffic Type can be selected from: None, Broadcast, Multicast, Destination Lookup Failed (DLF), Broadcast + Multicast, Broadcast + DLF, Multicast + DLF, and Broadcast + Multicast + DLF. The Rate is in the range from 1 to 262143. By default, the traffic type is “None”.

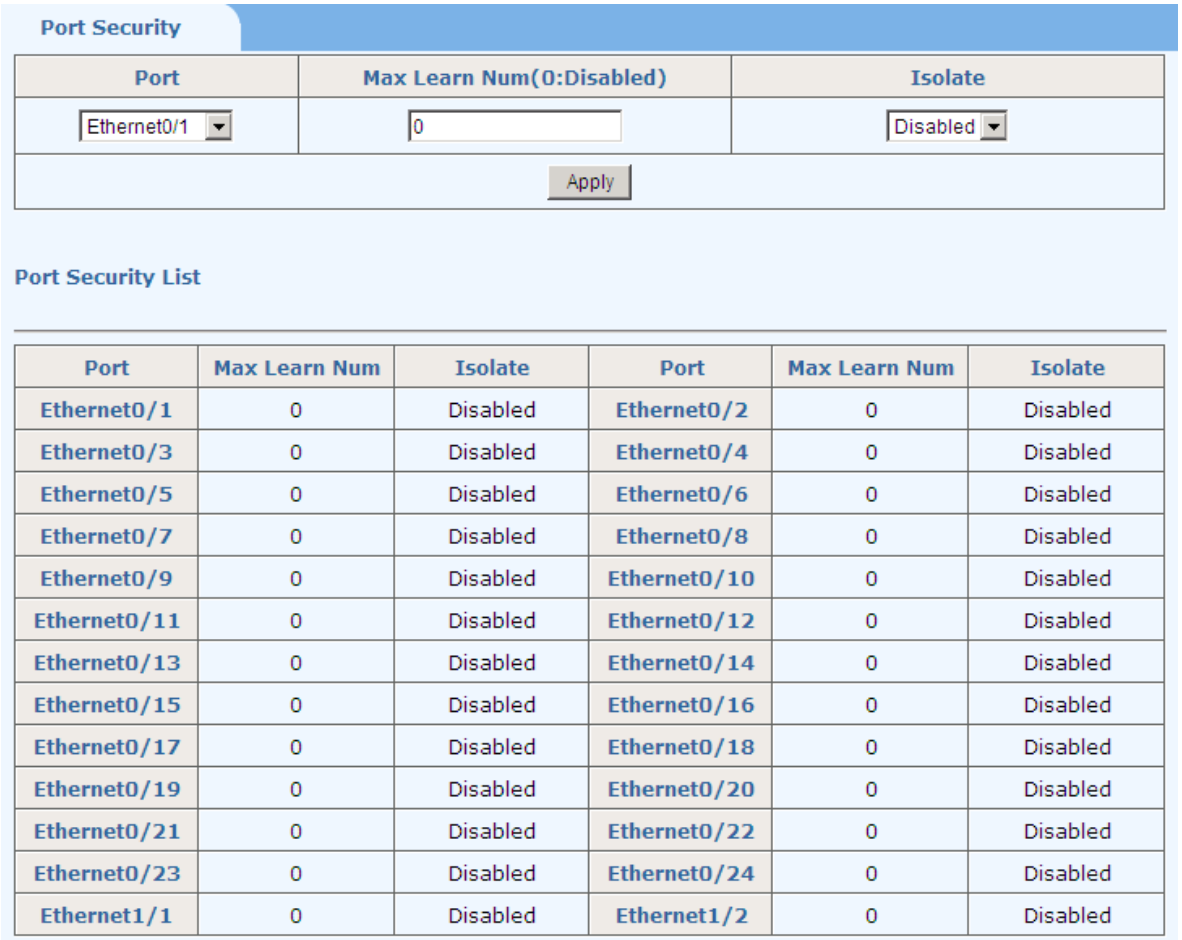




9.11 Port Security

This page sets the maximum learn number of ports and port isolation.

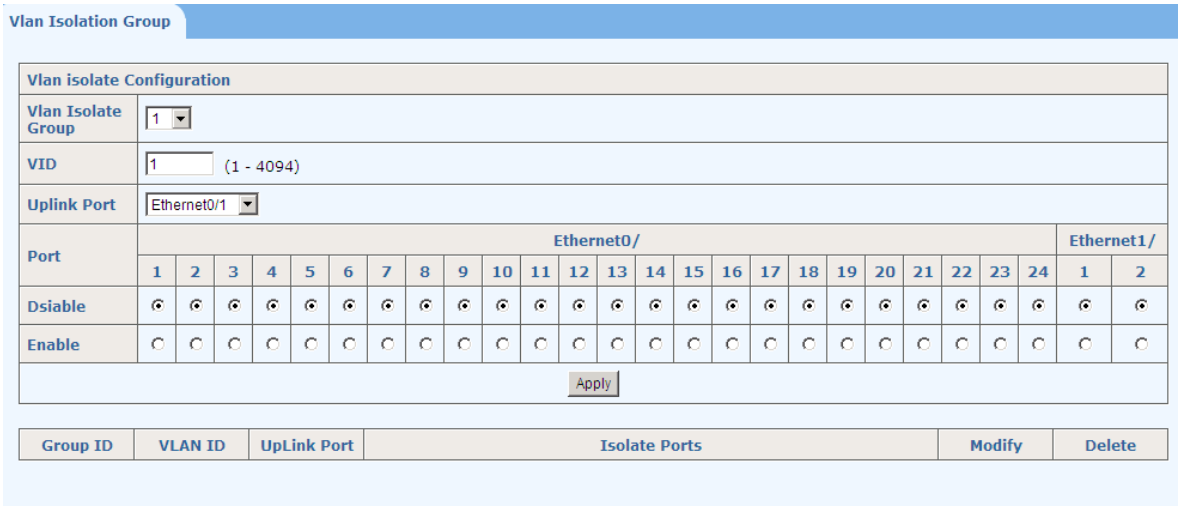
Port	Specify the port.
Max Learn Num	Set the maximum learn number, it is in the range of 1 to 1024. And “0” means this function is disabled.
Isolate	Enable/disable port isolation.



9.12 VLAN Isolation

This page configures VLAN isolate groups.

VLAN Isolate Group	Specify the VLAN isolate group.
VID	ID of a specified VLAN group.
Uplink Port	Uplink port of a specified VLAN group.
Port	Downlink port of a specified VLAN group. All the downlink ports of a specified VLAN isolate group should communicate with its uplink ports.
Disable	Delete the downlink ports of VLAN isolate group.
Enable	Add the downlink ports of VLAN isolate group.


Vlan Isolation Group
Vlan isolate Configuration
Vlan Isolate Group
1
VID
1
(1 - 4094)
Uplink Port
Ethernet0/1
Port
Ethernet0/
Ethernet1/
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 1 2
Dsiable
Enable
Apply
Group ID
VLAN ID
UpLink Port
Isolate Ports
Modify
Delete

10 ACL

ACL (Access Control List) is used to achieve the packet filtering function by the configuration of matching rules and processing operation(s). An ACL is a sequential collection of permit and deny conditions that apply to packets. When a packet is received on an interface, the switch compares the fields in the packet against any applied ACLs to verify that the packet has the required permissions to be forwarded, based on the criteria specified in the access lists. There are four sub-menus in ACL, shown as follows.

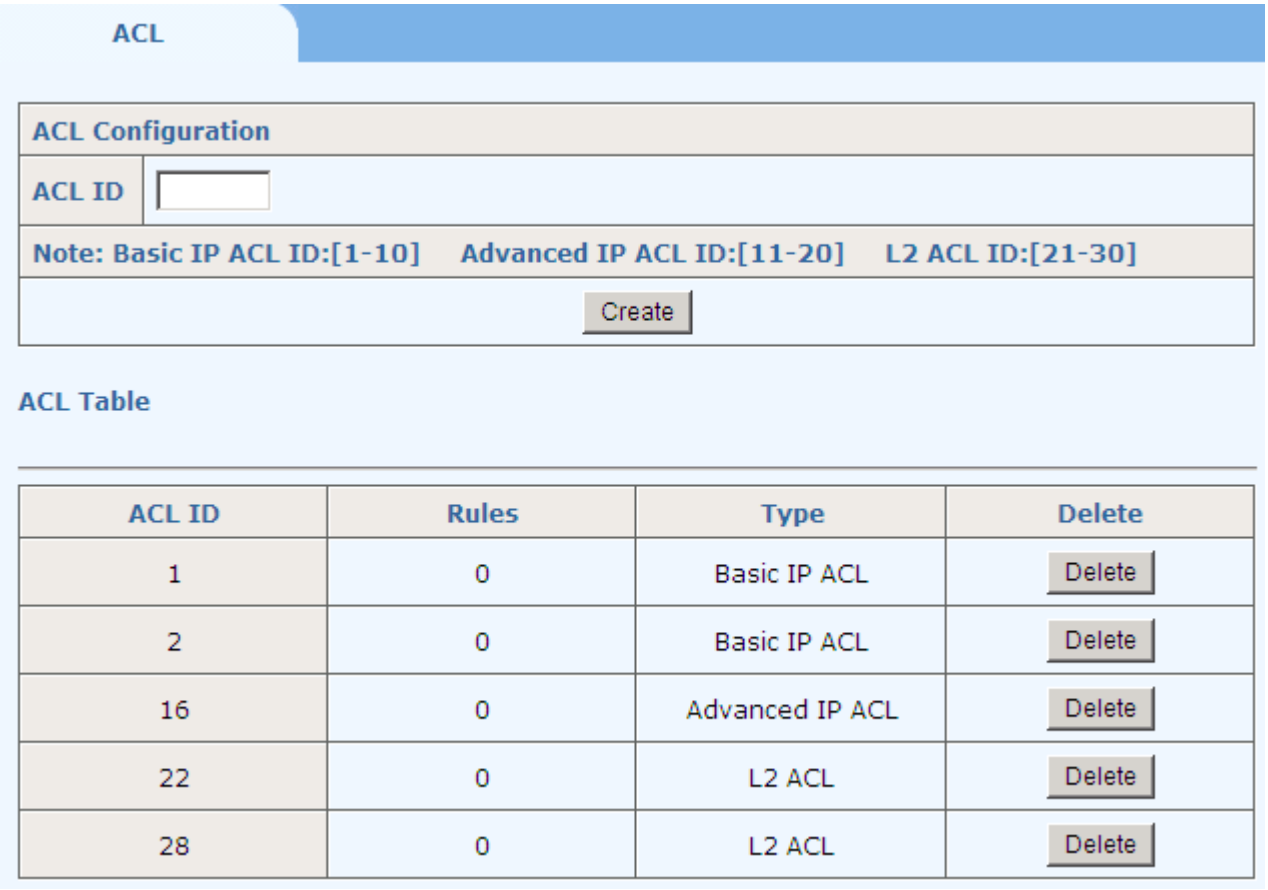
There are three types of ACL:

Basic IP ACL	filtering packets only based on source IP address.
Advance IP ACL	filtering packets based on source IP address, destination IP address, IP protocol type, and more.
L2 ACL	filtering packets based on source MAC address, destination MAC addresses, 802.1p priority, and L2 protocol type.

10.1 Management ACL

In order to flexibly configure ACL rule, the ACL ID is divided into three segments: 1-10 for Basic IP ACL, 11-20 for Advanced IP ACL, and 21-30 for L2 ACL. **ACL Rule** page sets different ACL rules based on the range of ACL ID.

The bottom part of this page lists all configured ACL IDs. Parameter **Rules** shows the number of rules that has already been configured for this ACL ID.



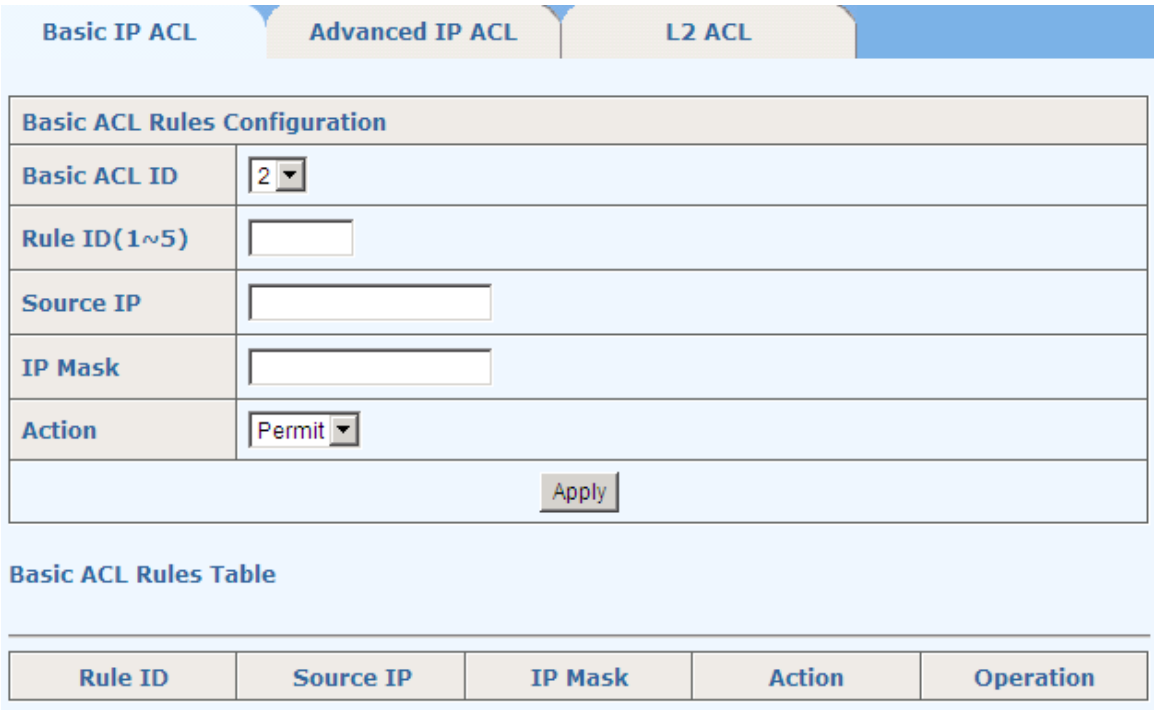
10.2 ACL Rule

10.2.1 Basic IP ACL

This page sets Basic IP ACL rules. To ACL ID, Up to 10 rules can be set; each rule ID can only be used once. All parameters of **Rule ACL ID**, **Source IP** and **IP Mask** must be set, and the **Action** can be **Permit** or **Deny.**

Permit Permit the access of IP matched with rule**.**
Deny Deny the access of IP matched with rule**.**

The bottom part of this page lists all configured Basic IP ACL rules.



10.2.2 Advanced IP ACL

This page sets ACL rules based on packet Src IP Address, Dst IP Address, IP Protocol type and other protocol features, such as TCP or UDP source port, destination port, ICMP protocol message types etc.

Rule ID identification of the ACL rule

Protocol Type an existing protocol type such as Icmp, Igmp, Udp, Tcp, Ospf, or an integer between 1 and 255

Src IP Address source host IP address

Src IP Mask source host IP subnet mask

Src L4 Port TCP/UDP source port, an existing Echo, Frp, telnet, Smtp, WWW, or an integer between 1 and 65535. It can be set only when protocol type is TCP or UDP.

Note that IETF IANA defines three groups of ports: Well Known Ports (0-1023), Registered Ports (1024-49151), and Dynamic and/or Private Ports (49152-65535).

Dst IP Address destination host IP address.

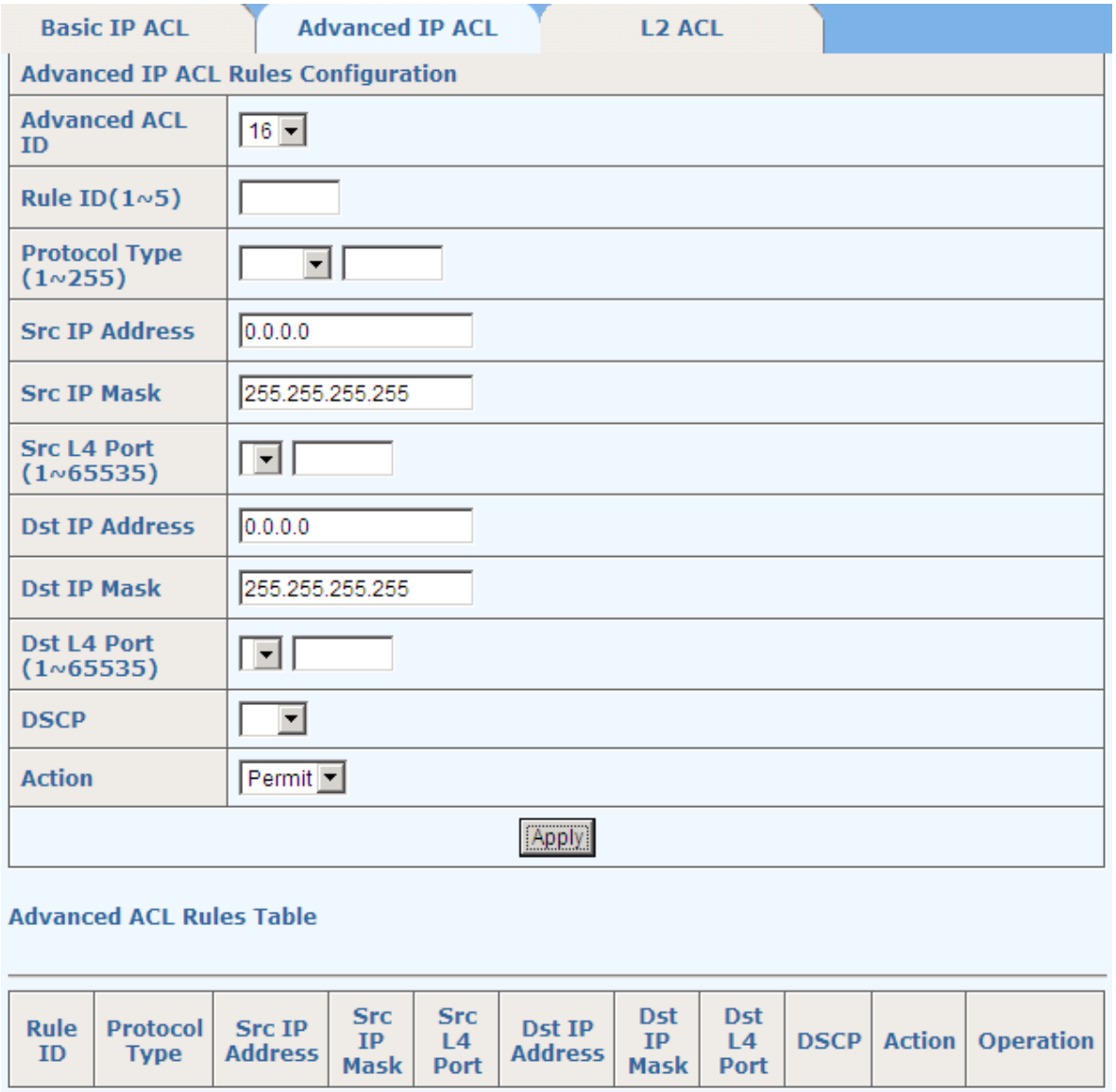
Dst IP Mask destination host IP subnet mask

Dst L4 Port TCP/UDP destination port, an existing Echo, Frp, telnet, Smtp, WWW, or an integer 1-65535. It can be set only when protocol type is TCP or UDP.

DSCP Priority of DSCP

Action: permit or deny access of the package with matched rules**.**

The bottom part of this page lists all configured Advanced IP ACL rules.

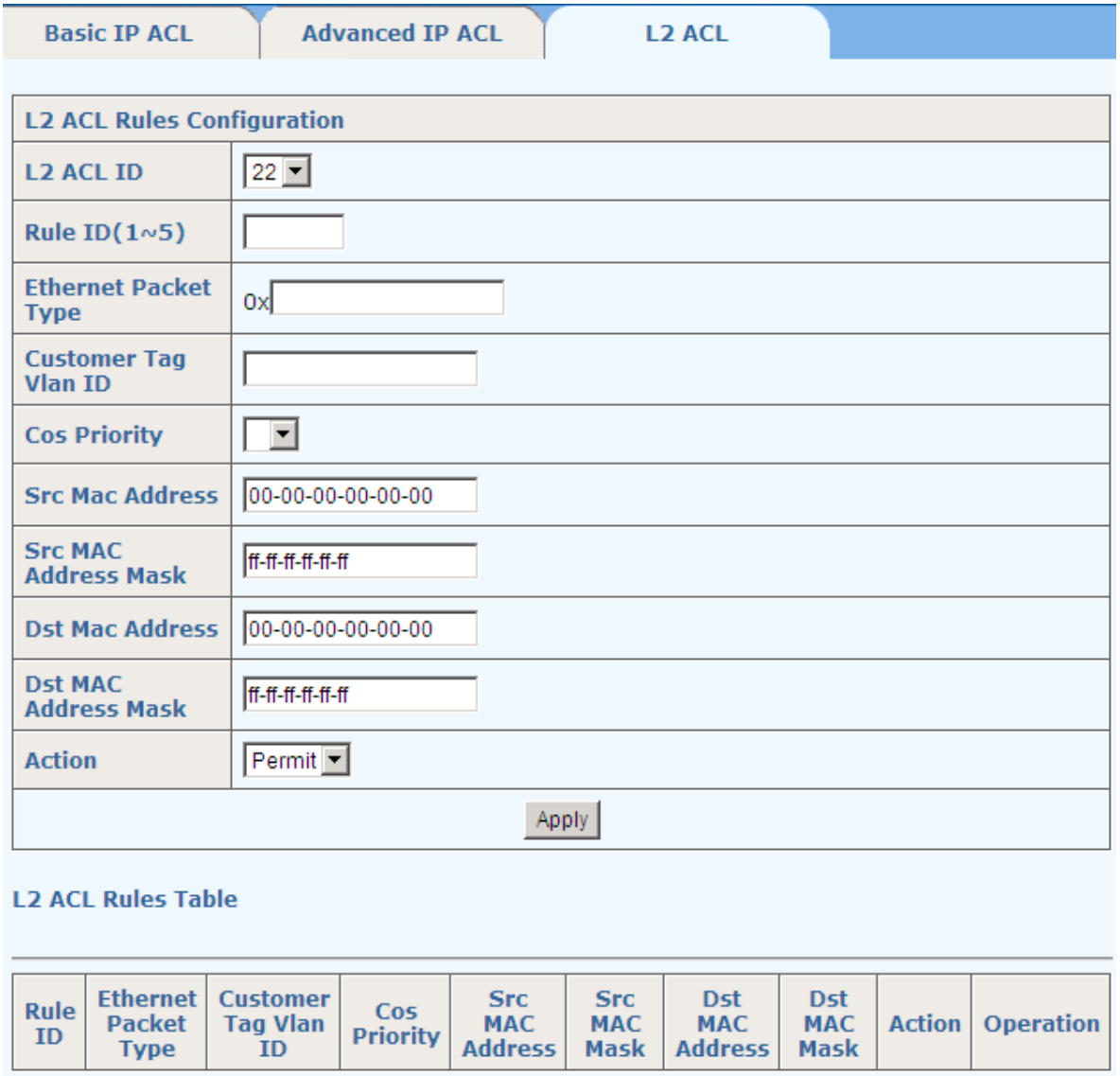


10.2.3 L2 ACL

This page sets L2 ACL ID, Rule ID, Ethernet Packet Type, Customer Tag Vlan ID, Cos Priority, Src MAC Address, Src MAC Address Mask, Dst Mac Address, and Dst MAC address Mask, and the Action that can be selected as Permit or Deny.

L2 ACL ID	Specify L2 ACL ID.
Rule ID	Identification of the ACL rule, in the range of 1 to 5.
Ethernet Packet Type	Specify Ethernet packet type, in the range of 0x0-0xffff
Customer Tag Vlan ID	Vlan ID of customer, in the range of 1-4094.
Cos Priority	Cos priority, in the range of 1 to 7.
Src MAC Address	source host MAC address.
Src MAC Address Mask	source host MAC address mask.
Dst MAC Address	destination host MAC address.
Dst MAC address Mask	destination host MAC address mask.
Action	permit or deny the access for the package matched with rules**.**

The bottom part of this page lists all configured L2 ACL rules.



10.3 Traffic ACL

The page configure traffic limit of ACL rules. It is for the ACL rules whose action is set to be permit. “Action” must be set in “ACL Rule” page.

Rule ID	Specify ACL rules.
Priority	Re-set packet priority.
Traffic Limit	Enable/disable traffic limit.
Target Rate	Set target rate.
Burst	Set burst rate.
Traffic Statistic	Enable/disable traffic statistics.

The bottom part of the page lists all ACL rules traffic limit.

Traffic ACL

Traffic ACL Rules Configuration	
ACL ID	1
Rule ID(1~5)	
Priority	
Traffic Limit	Disabled Target Rate Kbps Burst Kbytes
Traffic Statistic	Disabled
	Apply

ACL Rules Table

ACL ID	Rule ID	Priority	Target Rate (Kbps)	Burst(Kbytes)	Statistic	Operation

10.4 Port Binding

This page sets the binding of an Ethernet port to a specified ACL ID. If a port is bound, it will take effect on all the rules associated to this ACL ID. The bottom part of this page lists all ACL binding Ports.

Binding Port

IP ACL Binding Configuration

ACL ID	1																									
Port	Ethernet0/																								Ethernet1/	
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	1	2
Binding Port	☑	☐	☑	☐	☐	☐	☐	☑	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
	Apply																									

ACL Port List

ACL ID	Port
1	Ethernet0/1,3,8
2	Ethernet0/6-9
16	Ethernet0/9-10,16-18
22	Ethernet0/17-19,21
28	Ethernet0/23-24,Ethernet1/1-2

11 LLDP

LLDP (Link Layer Discovery Protocol) defines a standard way for an Ethernet device to advertise its information to its network neighbors and to store the information discovered from other devices, as described in IEEE 802.1AB. There are three sub-menus in LLDP, shown as follows.

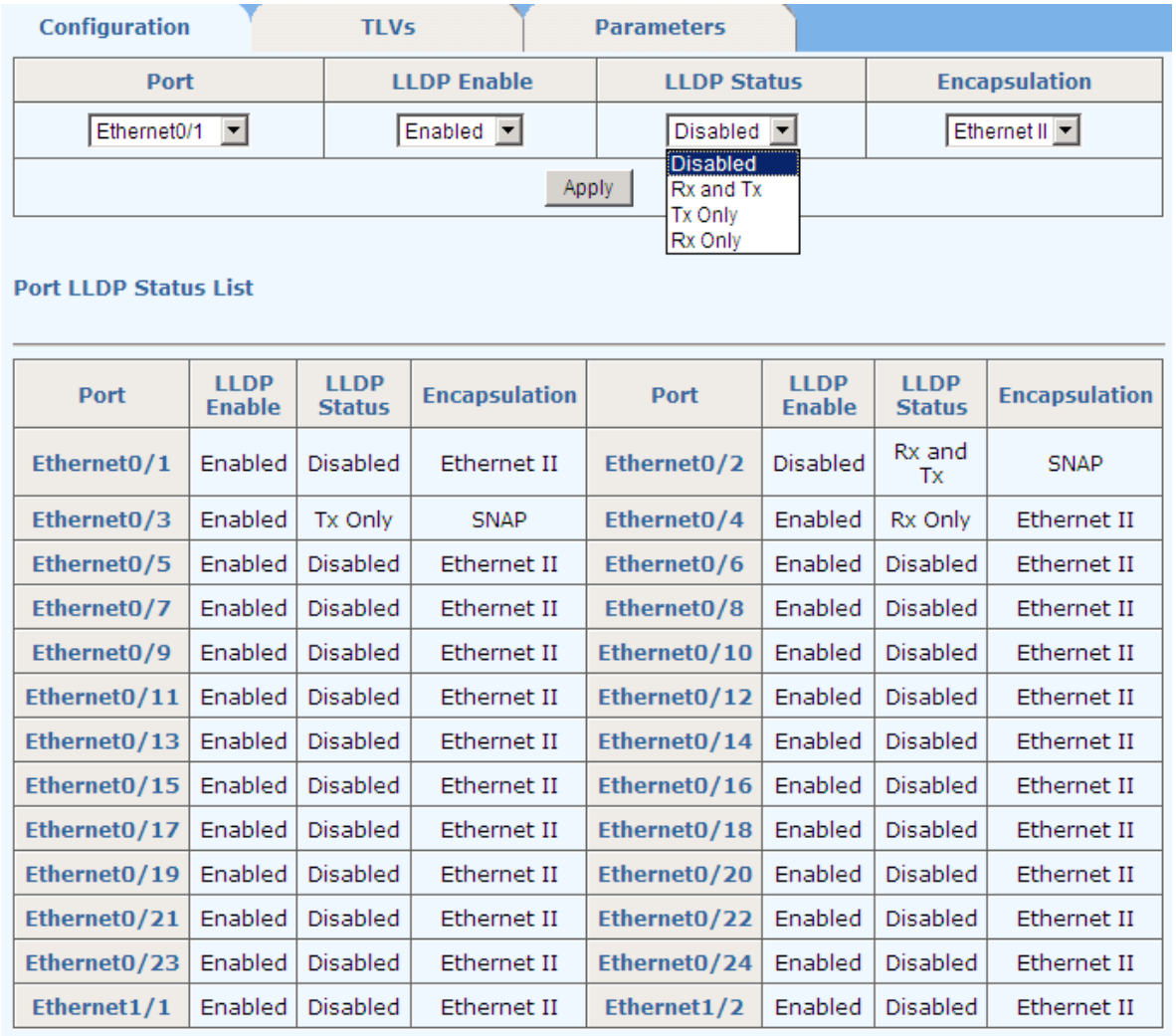
11.1 Management LLDP

11.1.1 Configuration

LLDP should be enabled in System Advanced Configuraiton first. This page sets transmit LLDP status from **Disabled**, **Rx and Tx, Tx only** and **Rx only,** and also specifies the LLDP Encapsulation to be **Ethernet II** or **SNAP** for a specified Ethernet port.

Ethernet II The Ethernet frame of type 0x88cc.
SNAP The Ethernet frame of type 0xAAAA-0300-0000-88CC.

The bottom part of this page lists the LLDP status for all ports.



Port	LLDP Enable	LLDP Status	Encapsulation	Port	LLDP Enable	LLDP Status	Encapsulation
Ethernet0/1	Enabled	Disabled	Ethernet II	Ethernet0/2	Disabled	Rx and Tx	SNAP
Ethernet0/3	Enabled	Tx Only	SNAP	Ethernet0/4	Enabled	Rx Only	Ethernet II
Ethernet0/5	Enabled	Disabled	Ethernet II	Ethernet0/6	Enabled	Disabled	Ethernet II
Ethernet0/7	Enabled	Disabled	Ethernet II	Ethernet0/8	Enabled	Disabled	Ethernet II
Ethernet0/9	Enabled	Disabled	Ethernet II	Ethernet0/10	Enabled	Disabled	Ethernet II
Ethernet0/11	Enabled	Disabled	Ethernet II	Ethernet0/12	Enabled	Disabled	Ethernet II
Ethernet0/13	Enabled	Disabled	Ethernet II	Ethernet0/14	Enabled	Disabled	Ethernet II
Ethernet0/15	Enabled	Disabled	Ethernet II	Ethernet0/16	Enabled	Disabled	Ethernet II
Ethernet0/17	Enabled	Disabled	Ethernet II	Ethernet0/18	Enabled	Disabled	Ethernet II
Ethernet0/19	Enabled	Disabled	Ethernet II	Ethernet0/20	Enabled	Disabled	Ethernet II
Ethernet0/21	Enabled	Disabled	Ethernet II	Ethernet0/22	Enabled	Disabled	Ethernet II
Ethernet0/23	Enabled	Disabled	Ethernet II	Ethernet0/24	Enabled	Disabled	Ethernet II
Ethernet1/1	Enabled	Disabled	Ethernet II	Ethernet1/2	Enabled	Disabled	Ethernet II

11.1.2 TLVs

This page sets the type of transmitted information: Port Description, System Name, System Description, System Capability, and Management.

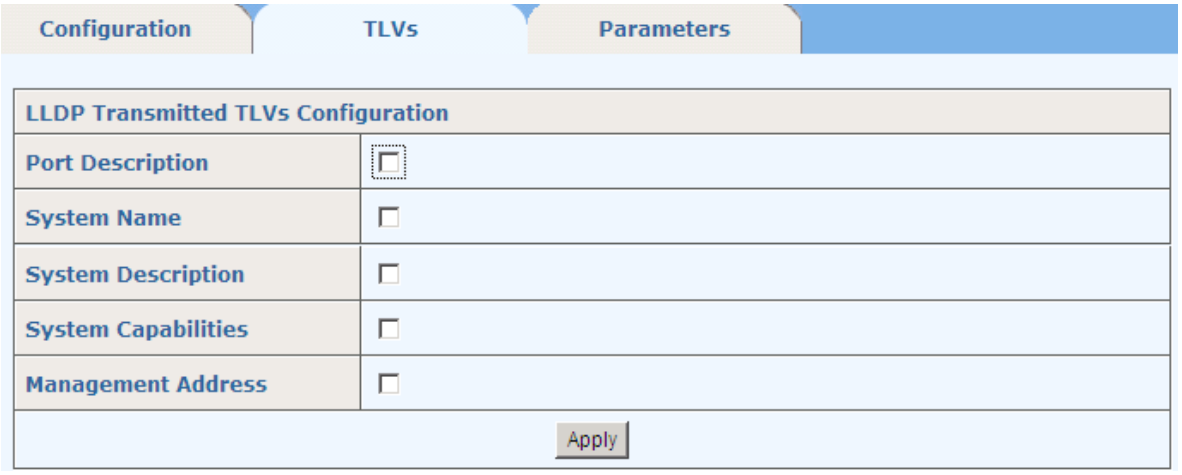
Port Description identifies information of the interface, including the name of manufacturer, product name, and the version of the interface hardware & software.

System Name identifies the administratively-assigned name for the device.

System Description a textual description of the device. This value typically includes the full name and version identification of the system's hardware type, software operating system, and networking software.

System Capability identifies the capabilities of the device and its primary function (e.g. repeater, Bridge, WLAN, Access Point, Router, Telephone, DOCSIS cable device, Station, etc.)

Management Address identifies the IP address or MAC address of the device.



11.1.3 Parameters

This page sets LLDP parameters: **TX Interval**, **Tx Hold**, **Tx Delay**, **Re-init Delay,** and **Fast Count**.

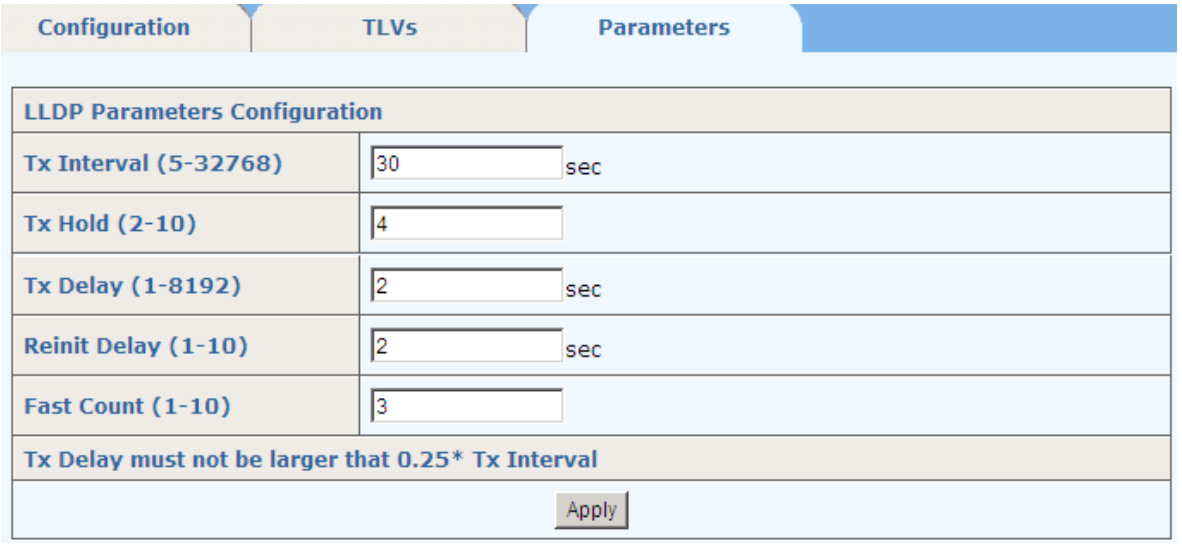
Tx Interval — The time interval between sending LLDP packets, its range is from 5 to 32768 seconds. The default value is 30 seconds.

Tx Hold — TTL multiplier. TTL of TLV carried in LLDPDU is used to set the aging time on the neighbor device. Since TTL of TLV = TTL multiplier × **Tx Interval**, the aging time on the neighbor device can be adjusted by the TTL multiplier. The range of this value is from 2 to 10, and the default value is 4.

Tx Delay — The delay period between successive LLDP packets which are initiated by port parameter changes. The range is from 1 to 8192, and the default value is 2.

Re-init Delay — in the case of **LLDP Status** mode changes, the port will initialize the protocol state machine, and the switch will need to wait for **Re-init Delay** to be able to start the next initialization. The range of this value is from 1 to 10 seconds, and the default value is 2.

Fast Count — The number of fast sending packets. It is in the range of 1 to 10, and the default value is 3.



11.2 Neighbor Information

This page shows the **Local Port, Chassis Id** of a local device**,** and the **Remote Port ID, System name, Port description, System Capabilities**, and **Management Address** of a neighbor device.

LLDP Neighbor

Local Port	Chassis Id	Remote Port ID	System Name	Port description	System Capabilities	Management Address
No entries in table						

11.3 LLDP Statistics

This page shows the statistics **Tx Frames, Rx Frames, Rx Error Frames, Discarded Frames, TLVs discarded, TLVs unrecognized**, **Org.TLVs discarded,** and **Age out** packet counts of LLDP packets on each Ethernet port.

LLDP Statistics

Port	Tx Frames	Rx Frames	Rx Error Frames	Discarded Frames	TLVs discarded	TLVs unrecognized	Org. TLVs discarded	Aged out
Ethernet0/1	0	0	0	0	0	0	0	0
Ethernet0/2	0	0	0	0	0	0	0	0
Ethernet0/3	0	0	0	0	0	0	0	0
Ethernet0/4	0	0	0	0	0	0	0	0
Ethernet0/5	0	0	0	0	0	0	0	0
Ethernet0/6	0	0	0	0	0	0	0	0
Ethernet0/7	0	0	0	0	0	0	0	0
Ethernet0/8	0	0	0	0	0	0	0	0
Ethernet0/9	0	0	0	0	0	0	0	0
Ethernet0/10	0	0	0	0	0	0	0	0

12 Statistics

All the sub-menus in this menu show various statistics information of the switch.

- Statistics
  - Port Status
  - Port Statistics
  - VLAN List
  - MAC Address Table
  - IGMP Snooping Group
  - Link Aggregation

12.1 Port Status

This page shows the **State**, **Media**, **Link**, **Negotiation**, **Speed & Duplex**, **Flow Control**, **Learning** of each Ethernet port.

Port Status

Port	State	Media	Link	Negotiation	Speed&Duplex	Flow Control	Learning	LBD	LBD Control
Ethernet0/1	Enabled	-	Down	Auto	-	-	Enabled	Disabled	Disabled
Ethernet0/2	Enabled	-	Down	Auto	-	-	Enabled	Disabled	Disabled
Ethernet0/3	Enabled	-	Down	Auto	-	-	Enabled	Disabled	Disabled
Ethernet0/4	Enabled	-	Down	Auto	-	-	Enabled	Disabled	Disabled
Ethernet0/5	Enabled	-	Down	Auto	-	-	Enabled	Disabled	Disabled
Ethernet0/6	Enabled	-	Down	Auto	-	-	Enabled	Disabled	Disabled
Ethernet0/7	Enabled	-	Down	Auto	-	-	Enabled	Disabled	Disabled
Ethernet0/8	Enabled	-	Down	Auto	-	-	Enabled	Disabled	Disabled
Ethernet0/9	Enabled	-	Down	Auto	-	-	Enabled	Disabled	Disabled
Ethernet0/10	Enabled	-	Down	Auto	-	-	Enabled	Disabled	Disabled
Ethernet0/11	Enabled	-	Down	Auto	-	-	Enabled	Disabled	Disabled
Ethernet0/12	Enabled	-	Down	Auto	-	-	Enabled	Disabled	Disabled
Ethernet0/13	Enabled	-	Down	Auto	-	-	Enabled	Disabled	Disabled

Ethernet0/14	Enabled	-	Down	Auto	-	-	Enabled	Disabled	Disabled
Ethernet0/15	Enabled	-	Down	Auto	-	-	Enabled	Disabled	Disabled
Ethernet0/16	Enabled	COPPER 100m	Up	Auto	1000M Full	Off	Enabled	Disabled	Disabled
Ethernet0/17	Enabled	-	Down	Auto	-	-	Enabled	Disabled	Disabled
Ethernet0/18	Enabled	-	Down	Auto	-	-	Enabled	Disabled	Disabled
Ethernet0/19	Enabled	-	Down	Auto	-	-	Enabled	Disabled	Disabled
Ethernet0/20	Enabled	-	Down	Auto	-	-	Enabled	Disabled	Disabled
Ethernet0/21	Enabled	-	Down	Auto	-	-	Enabled	Disabled	Disabled
Ethernet0/22	Enabled	-	Down	Auto	-	-	Enabled	Disabled	Disabled
Ethernet0/23	Enabled	-	Down	Auto	-	-	Enabled	Disabled	Disabled
Ethernet0/24	Enabled	-	Down	Auto	-	-	Enabled	Disabled	Disabled
Ethernet1/1	Enabled	-	Down	Auto	-	-	Enabled	Disabled	Disabled
Ethernet1/2	Enabled	-	Up	Auto	100M Full	Off	Enabled	Disabled	Disabled

12.2 Port Statistics

This page shows the TxGoodPkts, TxBadPkts, RxGoodPkts, RxBadPkts, TxAbort, Collision, and DropPkt of each Ethernet port.

TxGoodPkts the total number of outgoing normal packets on the port, including outgoing normal packets and normal pause frames

TxBadPkts the total byte number of outgoing error frames

RxGoodPkts the total number of incoming normal packets on the port, including incoming normal packets and normal pause frames

RxBadPkts the total number of incoming error frames

TxAbort the number of transmission failures due to various reasons, such as collisions

Collision the number of detected collisions

DropPkt the number of packets dropped for various reasons

Port Statistics

Port	TxGoodPkts	TxBadPkts	RxGoodPkts	RxBadPkts	TxAbort	Collision	DropPkt
Ethernet0/1	0	0	0	0	0	0	0
Ethernet0/2	0	0	0	0	0	0	0
Ethernet0/24	0	0	0	0	0	0	0
Ethernet1/1	19458	0	16919	0	0	0	0
Ethernet1/2	2994	0	2559	0	0	0	0

Reset

12.3 VLAN List

This page lists the information of all VLANs, including **VID**, **Name**, **Type**, **Tagged**, **Untagged**, and **Forbidden**. **Type** includes **Static** and **Dynamic**; **Tagged** lists all ports from which packets are sent tagged; **Untagged** lists all ports from which packets are sent

untagged; and **Forbidden** lists all ports that cannot be added to the VLAN group.

VLAN List

VID	Name	Type	Tagged	Untagged	Forbidden
1	Default	Static	-	Ethernet0/1-24,Ethernet1/1-2	-
2	G 2	Static	-	-	Ethernet0/6,11
56	Mvr vlan	Mvr vlan	-	-	-

12.4 MAC Address Table

This page shows information of MAC address entries in the MAC address table, including **VID**, **Unicast MAC Address**, **Port**, and **Type**. **Type** includes **Dynamic**, **Static**, **Blackhole** and **Learned**.

Unicast MAC Address

VID	Unicast MAC Address	Port	Type
1	00-1f-d0-6a-de-f0	Ethernet1/1	Learned
1	00-00-dd-11-29-22	CPU	Static
2	00-00-dd-11-29-22	CPU	Static

12.5 IGMP Snooping Group

This page shows IGMP Snooping multicast group information, including **VID**, **Multicast Group**, **MAC Address**, and **Member Ports**. **Multicast Group** is the IP address of a multicast group, **MAC Address** is the address of a MAC multicast group, and **Member Ports** include all ports belonging to this IGMP Snooping group.

Group

VID	Multicast Group	MAC Address	Member Ports

12.6 Link Aggregation

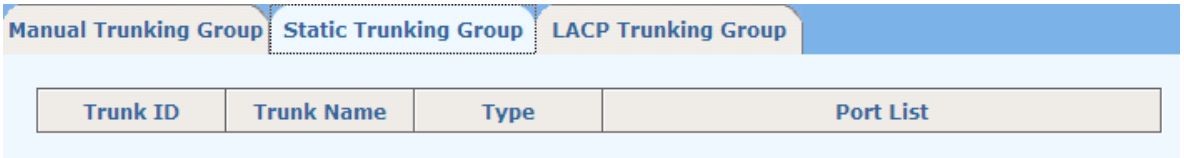
There are three tab pages on this webpage.

Manual Trunking Group: shows manual trunk information, including **Trunk ID**, **Trunk Name**, **Type**, and **Port List**. **Type** is fixed to **Manual**.

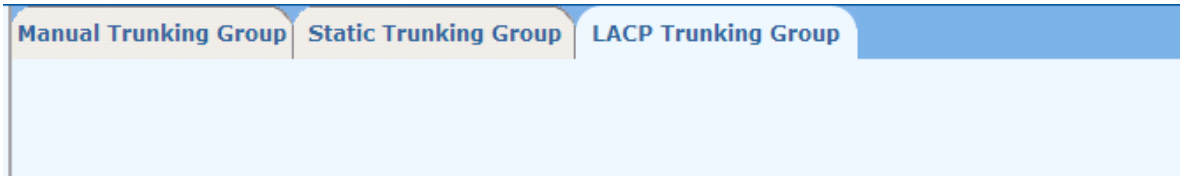
Manual Trunking Group | Static Trunking Group | LACP Trunking Group

Trunk ID	Trunk Name	Type	Port List

Static Trunking Group: shows static trunk information, including **Trunk ID**, **Trunk Name**, **Type**, and **Port List**. **Type** is fixed to **Static**.



LACP Trunking Group: shows LACP trunk information, including **Priority**, **MAC** of Actor and Partner. It also shows the **Key**, **priority**, **Active state** of member ports.



13 Spanning Tree

Spanning Tree Protocol (STP) is a standard protocol described in IEEE 802.1D. Rapid Spanning Tree Protocol (RSTP, IEEE 802.1w) is an evolution of the 802.1D. And Multiple Spanning Tree Protocol (MSTP, IEEE 802.1s) is also an evolution of the 802.1D. There are five sub-menus in Spanning Tree page shown as follows.

13.1 Global

Before configuring STP, make sure STP is enabled (see section 2.3 of this manual for details). There is one tab page: **Configuration.**

This page sets bridge configurations: **Mode**, **Max Hops**, **Hello Time**, **Max Age**, **Forward Delay Time**, **Priority**, and **BPDU Guard**.

Mode: Three spanning tree modes are supported: STP, RSTP, and MSTP.

Max Hops: This value is in the range of 1 to 20, and is 20 by default.

This parameter is used in MSTP mode only to limit the size of MST domain, and the root switch of the instance always sends a BPDU (or M-record) with a cost of 0 and the hop count of the maximum value. When a switch receives this BPDU, it decrements the received remaining hop count by one and propagates this value as the remaining hop count in the BPDUs it generates. When the count reaches zero, the switch discards the BPDU and ages the information held for the port. By default, this value is set to 20.

Hello Time: This value is in the range from 1 to 10 seconds, and is 2 seconds by default.

A root bridge regularly sends out configuration BPDUs to maintain the stability of the existing spanning tree. If the switch does not receive a BPDU packet in a specified period, the spanning tree will be recalculated at BPDU packet times out. When a switch becomes to a root bridge, it regularly sends BPDUs at the interval specified by this hello time. A non-root-bridge switch adopts the interval specified by this hello time.

Max Age: This value is in the range of 6 to 40 seconds, and is 20 seconds by default.

MSTP is capable of detecting link failures and automatically restoring redundant links to the forwarding state. In CIST, switches use max age parameter to determine whether a received configuration BPDU times out. Spanning trees will be recalculated if a configuration BPDU received by a port times out.

Forward Delay Time: This value is in the range of 4 to 30 seconds, and is 15 seconds by default.

To prevent the occurrence of a temporary loop, when a port changes its state from discarding to forwarding, it undergoes an intermediate state and waits for a specific period of time to synchronize with the state transition of the remote switches. This state transition period is determined by **Forward Delay Time** configured on the root bridge, and applies to all non-root bridges.

As for the configuration of **Hello Time, Forward Delay Time, and Max Age**, the following formulas must be met to prevent frequent network jitter:

2 × (**Forward Delay Time** – 1 second) >= **Max Age**, and

Max Age >= 2 × (**Hello Time** + 1 second).

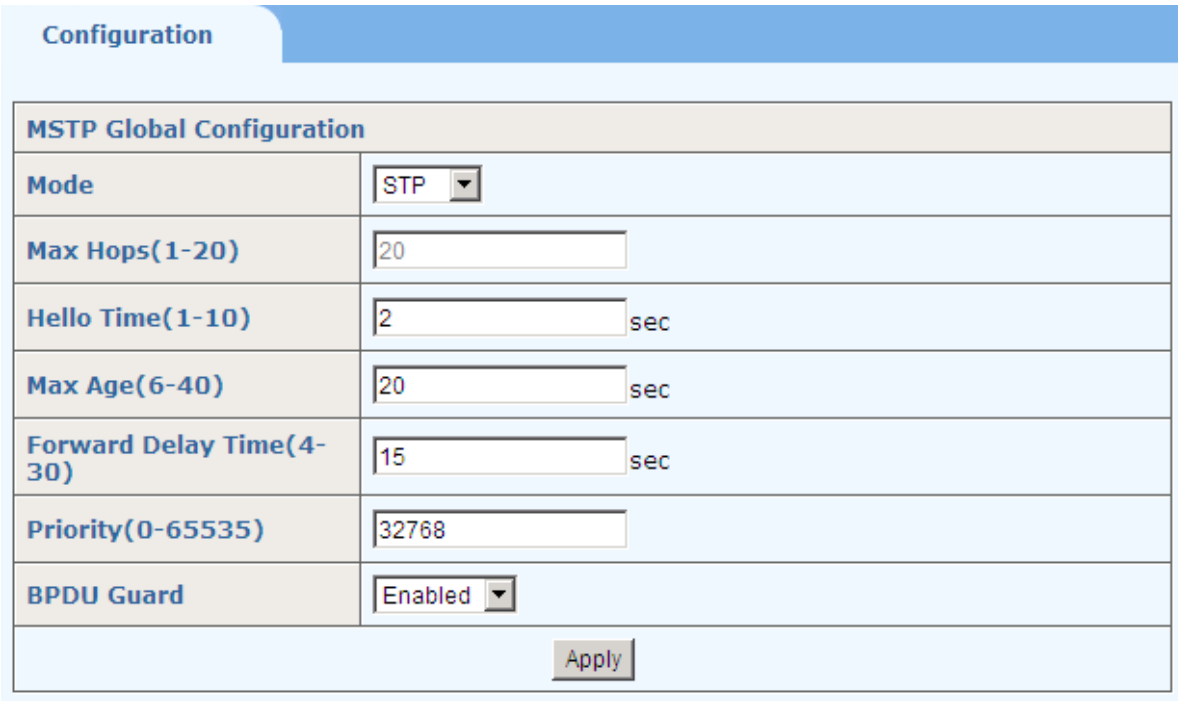
Priority: This value is in the range of 0 to 65535, and is 32768 by default. This parameter

is used in STP and RSTP modes only.

BPDU Guard: Some ports are usually configured as edge ports to achieve rapid transition, while they will become to non-edge ports automatically upon receiving configuration BPDUs, which may cause spanning trees regeneration and network topology jitter.

Normally, no configuration BPDU will reach edge ports, but malicious users can attack a network by sending configuration BPDUs deliberately to edge ports to cause network jitter, which can be prevented by utilizing this BPDU protection function. With this function enabled on a switch, the switch shuts down the edge ports that receive configuration BPDUs and then reports the cases to the network administrator. After a port is shut down, only the administrator can restore it.

By default, the BPDU protection function is disabled.



13.2 STP&RSTP

(1) *Ports Configuration*

This page sets STP, Edge Port, P2P, Migration, Tx Hold Count, External Cost, Priority, and Root Guard for each port.

Edge Port: selects **Enabled** to configure the specified Ethernet port as an edge port. By default, all Ethernet ports are non-edge ports.

An edge port is such a port that is directly connected to a user terminal instead of another switch or network segment. Rapid transition to the forwarding state is applied to edge ports, because no loop can be incurred by network topology change on edge ports. The spanning tree protocol allows a port to enter the forwarding state rapidly by setting it to be an edge port, and it is recommended to configure the Ethernet ports connected directly to user terminals as edge ports, so that they may enter the forwarding state immediately.

Normally, configuration BPDUs cannot reach an edge port because the port is not connected to another switch. But, in case that BPDU guard function is disabled on an edge port, configuration BPDUs sent deliberately by a malicious user may reach the port. If an edge port receives a BPDU, it changes itself to be a non-edge port.

P2P: select from **Force_True**, **Force_False**, and **Auto**.

Force_True: specifies that the link connected to the specified Ethernet port is a point-to-point link.

Force_False: specifies that the link connected to the specified Ethernet port is not a point-to-point link.

Auto: automatically determines whether the link connected to the specified Ethernet port is a point-to-point link.

Migration: For backward compatibility with switches running 802.1d, RSTP selectively sends 802.1d configuration BPDUs and TCN BPDUs on per-port basis.

When a port is initialized, the migration-delay timer is started, and RSTP BPDUs are sent in this time interval. When this timer is active, the switch processes all BPDUs received on the port and ignores the protocol type.

If the switch receives an 802.1d BPDU after the port's migration-delay timer is expired, it assumes that it is connected to an 802.1d switch and starts using only 802.1d BPDUs. However, if the RSTP switch is using 802.1d BPDUs on a port and receives an RSTP BPDU after the timer is timed out, it restarts the timer and starts using RSTP BPDUs on that port.

Tx Hold Count: the maximum number of configuration BPDUs a port can send in each Hello time. It is in the range of 1 to 10 and is 3 by default.

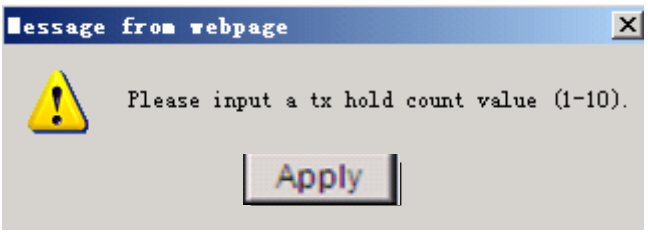
External Cost: sets the path cost of the specified port. It is in the range of 1 to 200000000, the default value is 0 (Auto).

Priority: port priority, it is in the range of 0 to 255; the default value is 128.

Root Guard: by default, the root protection function is disabled.

Due to configuration error or malicious attack, the root bridge in the network may receive configuration BPDUs with priorities higher than that of a root bridge, which will cause a new root bridge to be elected and network topology jitter will occur. In this case, data flows that should have been transmitted along a high-speed link may be led to a low-speed link.

This problem can be resolved by enabling the root protection function. Root-protection-enabled ports can only be kept as designated ports. When a port of this type receives configuration BPDUs with higher priorities, that is, when it is to become a non-designated port, it turns to the discarding state and stops forwarding packets (as if it were disconnected from the link).



Ports Configuration | Ports State | Bridge Information

Port	STP	Edge Port	P2P	Migration	Tx Hold Count	External Cost (0 =Auto)	Priority	Root Guard
Ethernet0/1	Disabled	Disabled	Auto	Disabled	3	20000	128	Disabled

Apply

STP&RSTP Port Attributes

Port	STP	Edge Port	P2P	Migration	Tx Hold Count	External Cost	Priority	Root Guard
Ethernet0/1	Disabled	Disabled	Auto	Disabled	3	20000	128	Disabled
Ethernet0/2	Enabled	Enabled	Force_True	Enabled	9	20000	176	Enabled
Ethernet0/3	Disabled	Disabled	Force_False	Disabled	5	20000	32	Disabled
Ethernet0/4	Disabled	Disabled	Auto	Disabled	3	20000	128	Disabled
Ethernet0/5	Disabled	Disabled	Auto	Disabled	3	20000	128	Disabled
Ethernet0/6	Disabled	Disabled	Auto	Disabled	3	20000	128	Disabled
Ethernet0/7	Disabled	Disabled	Auto	Disabled	3	20000	128	Disabled
Ethernet0/8	Disabled	Disabled	Auto	Disabled	3	20000	128	Disabled
Ethernet0/9	Disabled	Disabled	Auto	Disabled	3	20000	128	Disabled
Ethernet0/10	Disabled	Disabled	Auto	Disabled	3	20000	128	Disabled

(2) *Ports State*

This page lists all port parameters and spanning tree information, including **STP**, **State**, **Priority**, **Cost**, **Role**, **Designated Port ID**, **Designated Root ID**, and **Designated Bridge ID.**

Ports Configuration | Ports State | Bridge Information

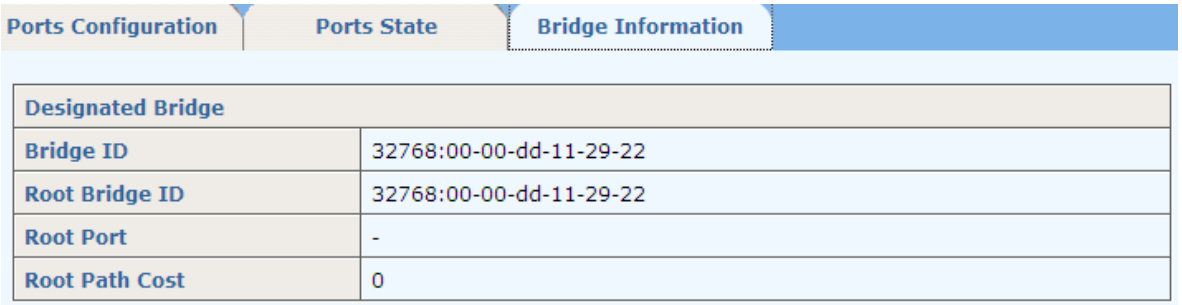
Port	STP	State	Priority	Cost	Role	Designated Port ID	Designated Root ID	Designated Bridge ID
Ethernet0/1	Disabled	Forwarding	128	0	Disabled	128-1	32768:00-00-dd-11-29-22	32768:00-00-dd-11-29-22
Ethernet0/2	Enabled	Forwarding	176	0	Disabled	176-2	32768:00-00-dd-11-29-22	32768:00-00-dd-11-29-22
Ethernet0/3	Disabled	Forwarding	32	0	Disabled	32-3	32768:00-00-dd-11-29-22	32768:00-00-dd-11-29-22
Ethernet0/4	Disabled	Forwarding	128	0	Disabled	128-4	32768:00-00-dd-11-29-22	32768:00-00-dd-11-29-22
Ethernet0/5	Disabled	Forwarding	128	0	Disabled	128-5	32768:00-00-dd-11-29-22	32768:00-00-dd-11-29-22
Ethernet0/6	Disabled	Forwarding	128	0	Disabled	128-6	32768:00-00-dd-11-29-22	32768:00-00-dd-11-29-22
Ethernet0/7	Disabled	Forwarding	128	0	Disabled	128-7	32768:00-00-dd-11-29-22	32768:00-00-dd-11-29-22
Ethernet0/8	Disabled	Forwarding	128	0	Disabled	128-8	32768:00-00-dd-11-29-22	32768:00-00-dd-11-29-22
Ethernet0/9	Disabled	Forwarding	128	0	Disabled	128-9	32768:00-00-dd-11-29-22	32768:00-00-dd-11-29-22
Ethernet0/10	Disabled	Forwarding	128	0	Disabled	128-10	32768:00-00-dd-11-29-22	32768:00-00-dd-11-29-22

(3) *Bridge Information*

This page lists basic information of **Designated Bridge**, including Bridge ID, Root Bridge ID, Root Port, and Root Path Cost.

Bridge ID ID of this switch.
Root Bridge ID ID of the root bridge.
Root Port the spanning tree root port.

Root Path Cost cost of the path from the switch to the root bridge.



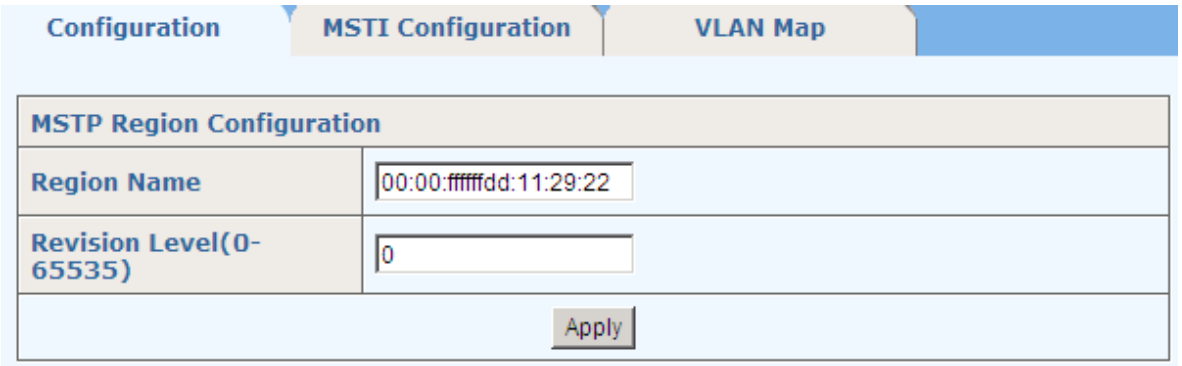
13.3 MSTP Region

MSTP mode should be enabled in MSTP Global Configuration. An MSTP region comprises one or more MST Bridges with the same MSTP configuration identifier.

(1) *Configuration*

This page sets **Region Name** and **Revision level** of MST configuration Identifiers.

Region Name a variable length text string of up to 32 octets
Revision level a 2-octet unsigned integer. It ranges from 0 to 65535.

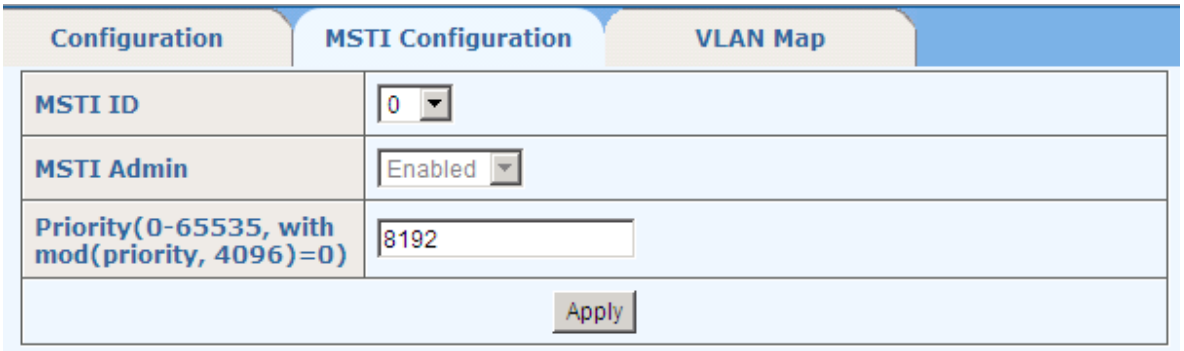


(2) *MSTI Configuration*

This page sets MSTI ID, MSTI Admin, and Priority for each MST instance.

MSTI ID MSTI identification, ranging from 0 to 15
MSTI Admin Enable/disable the specified instance
Priority Sets a priority for the specified instance. It is in the range from 0 to 65535; the default value is 32768

The bottom part of this page lists all MST instances information.



MSTI Priority List

MSTI ID	Admin	Priority
0	Enabled	8192
1	Disabled	32768
2	Enabled	32768
3	Disabled	32768
4	Disabled	32768
5	Disabled	32768
6	Disabled	32768
7	Disabled	32768
8	Disabled	32768

(3) *VLAN MAP*

This page maps one or more VLANs into a specific MST instance. One or more VLANs can be assigned to a spanning-tree instance at a time. The bottom part of this page lists the VLAN mapping table.

Configuration | MSTI Configuration | VLAN Map

MSTI ID	0
VLAN ID(1-4094, eg:2,4,6-12)	1-2,4023-4094
	Apply

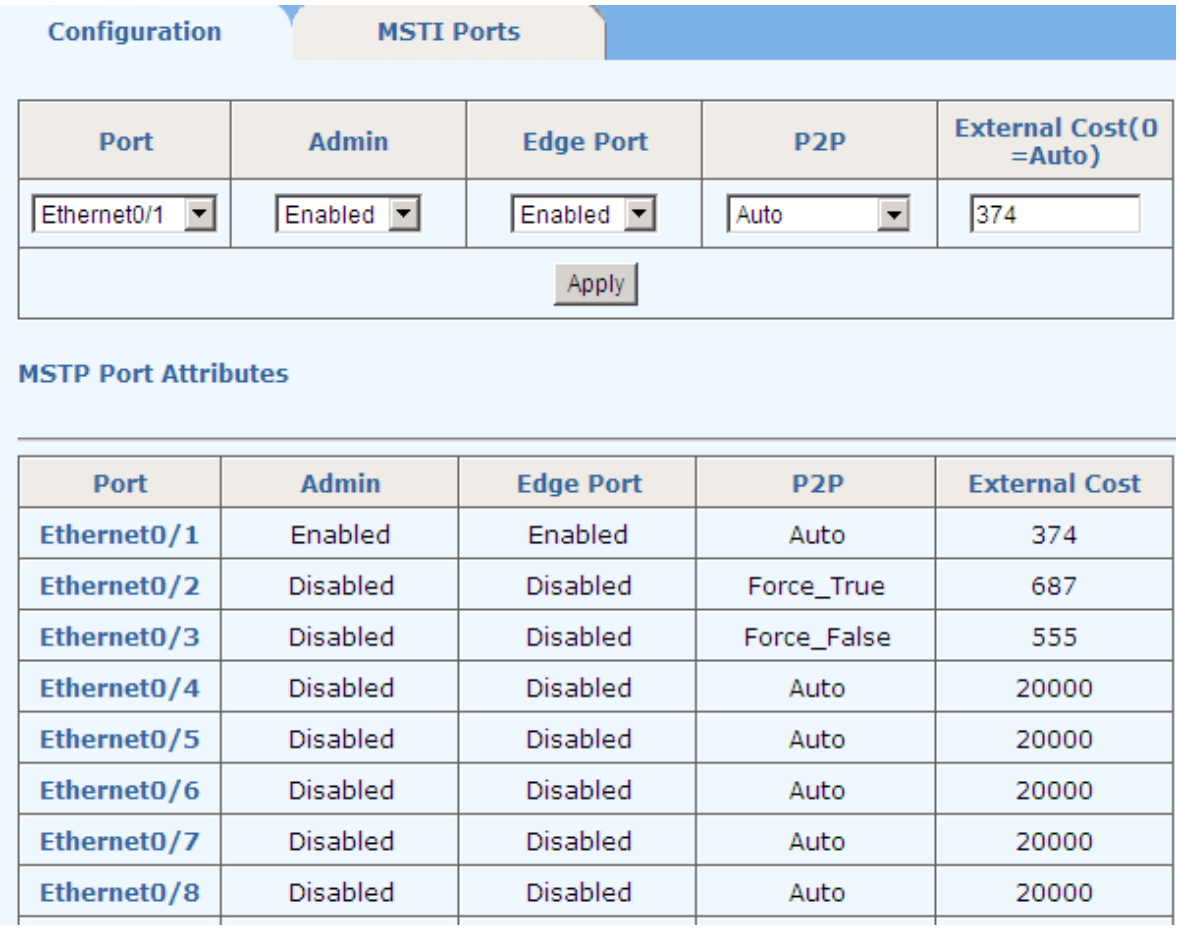
MSTI VLAN Map List

MSTI ID	Map VLAN
0	1-2,4023-4094
1	3-50
2	51-4022
3	-
4	-
5	-
6	-
7	-
8	-

13.4 MSTP Ports

(1) *Configuration*

This page can set **Port**, **Admin**, **Edge Port, P2P,** and **External Cost** for each port. Similar to STP and RSTP port configuration described in section 2.12.2.1 Ports Configuration, this page sets MSTP port configuration. The bottom part of this page lists the MSTP attributes for each port.



(2) *MSTI Ports*

This page sets the **Internal Cost** and **Priority** for each MST instance.

Internal Cost sets the path cost of the specified port in a specified MST instance. It is in the range from 1 to 200000000, and the default value is 0 (Auto).

Priority sets the port priority for the specified port in a specified MST instance. It is in the range from 0 to 240, and the default value is 128.

The bottom part of this page lists port parameters and spanning tree information for each MST instance.

Configuration | MSTI Ports

MSTI ID	1
Port	Ethernet0/1
Internal Cost(0 =Auto)	0
Priority(0-240)	128
	Apply

MSTP Port Attributes

MSTI ID	Port	Internal Path Cost	Priority	Role	State	Designated Bridge ID	Designated Port ID
1	Ethernet0/1	0	128	Disabled	Disabled	0:00-00-00-00-00-00	0-0
1	Ethernet0/2	23	80	Disabled	Disabled	0:00-00-00-00-00-00	0-0
1	Ethernet0/3	0	128	Disabled	Disabled	0:00-00-00-00-00-00	0-0
1	Ethernet0/4	0	128	Disabled	Disabled	0:00-00-00-00-00-00	0-0
1	Ethernet0/5	0	128	Disabled	Disabled	0:00-00-00-00-00-00	0-0

13.5 MSTP State

This page lists spanning tree information: **Bridge ID**, **Root Bridge ID, External Path Cost**, **Internal Path Cost,** and **Root Port** for each MST instance.

MSTP

MSTI ID	Bridge ID	Root Bridge ID	External Path Cost	Internal Path Cost	Root Port
0	8192:00-00-dd-11-29-22	8192:00-00-dd-11-29-22	0	0	0-0
1	32769:00-00-dd-11-29-22	32769:00-00-dd-11-29-22	0	0	0-0
2	32770:00-00-dd-11-29-22	32770:00-00-dd-11-29-22	0	0	0-0
3	32771:00-00-dd-11-29-22	32771:00-00-dd-11-29-22	0	0	0-0
4	32772:00-00-dd-11-29-22	32772:00-00-dd-11-29-22	0	0	0-0

14 SNMP Manager

There are SNMP Account and SNMP Trap in this item.

- SNMP Manager
  - SNMP Account
  - SNMP Trap

14.1 SNMP Account

There are three tab pages: *SNMP View*, *SNMP Community* and *SNMP User*.

14.1.1 SNMP View

This page sets which tree of SNMP-OID can be managed by an SNMP agent user; the default is all of them. For details of which MIBs are supported, please check section 6 “Appendix B: Supported MIBs” of this manual.

SNMP View | SNMP Community | SNMP User

SNMP View		
.1	default	☑
.1.0.8802.1.1.1	paeMIB	☐
.1.0.8802.1.1.2	lldpMIB	☐
.1.3.6.1.2.1.1	system	☐
.1.3.6.1.2.1.2	interfaces	☐
.1.3.6.1.2.1.3	at	☐
.1.3.6.1.2.1.4	ip	☐
.1.3.6.1.2.1.5	icmp	☐
.1.3.6.1.2.1.6	tcp	☐
.1.3.6.1.2.1.7	udp	☐
.1.3.6.1.2.1.10	transmission	☐
.1.3.6.1.2.1.11	snmp	☐
.1.3.6.1.2.1.16	rmon	☐
.1.3.6.1.2.1.17	dot1dBridge	☐
.1.3.6.1.2.1.31	ifMIB	☐
.1.3.6.1.2.1.67	radiusMIB	☐
.1.3.6.1.2.1.28350	privateMIB	☐

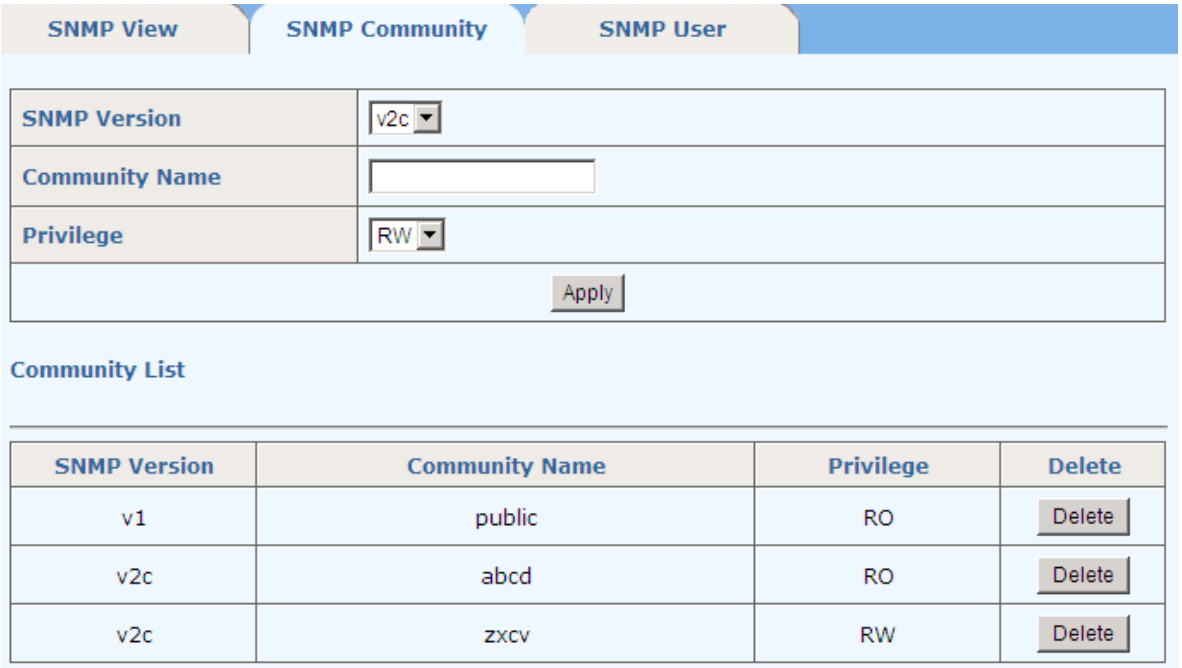
Apply

14.1.2 SNMP Community

This page sets **SNMP Version** between **v1** and **v2c; Community Name**, and **Privilege** between **RO** and **RW**.

v1	Creates an SNMPv1 user.
v2c	Creates an SNMPv2c user.
Community Name	Name of the community to be created. It is a string of 3 to 16 characters.
RO	Specifies that the community to be created has read-only permission to MIB objects. Communities of this type can only query MIBs for device information.
RW	Specifies that the community to be created has read-write permission to MIB objects. Communities of this type are capable of configuring devices.

The bottom part of this page lists all existing SNMP v1 and v2c communities, including **SNMP Version**, **Community Name** and **Privilege**. A community can be deleted.



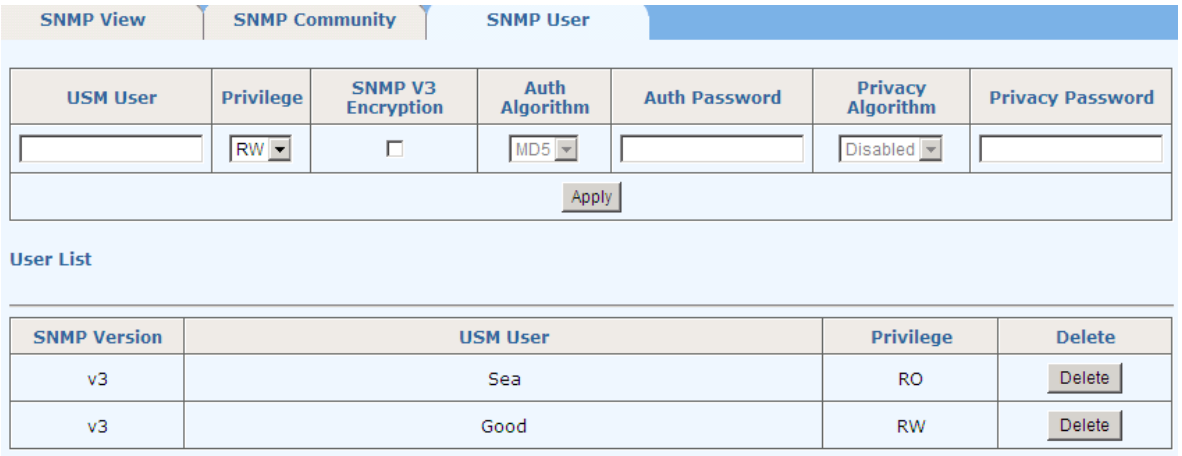
14.1.3 SNMP User

This page creates a SNMP v3 user, and sets **USM User**, **Privilege**, **SNMP V3 Encryption**, **Auth Algorithm**, **Auth Password**, **Privacy Algorithm**, and **Privacy Password**.

USM User	username, a string of 3 to 16 characters
Auth Algorithm	specifies the security mode of authentication. If **SNMP V3 Encryption** is not elected, neither authentication nor encryption will be performed
MD5	uses HMAC MD5 algorithm for authentication
SHA	uses HMAC SHA algorithm for authentication, which is more secure than MD5
Auth Password	Authentication password, a string of 9 to 15 characters in plain text, a 32-bit hexadecimal number in cipher text if MD5 algorithm is used, and a 40-bit hexadecimal number in cipher text if SHA algorithm is used

Privacy Algorithm	specifies the security mode as encrypted
DES	specifies the encryption protocol as Data Encryption Standard (DES)
AES	specifies the encryption protocol as Advanced Encryption Standard (AES), which is more secure than DES
Privacy Password	encryption password, a string of 9 to 15 characters in plain text, a 32-bit hexadecimal number in cipher text if MD5 algorithm is used, and a 40-bit hexadecimal number in cipher text if SHA algorithm is used

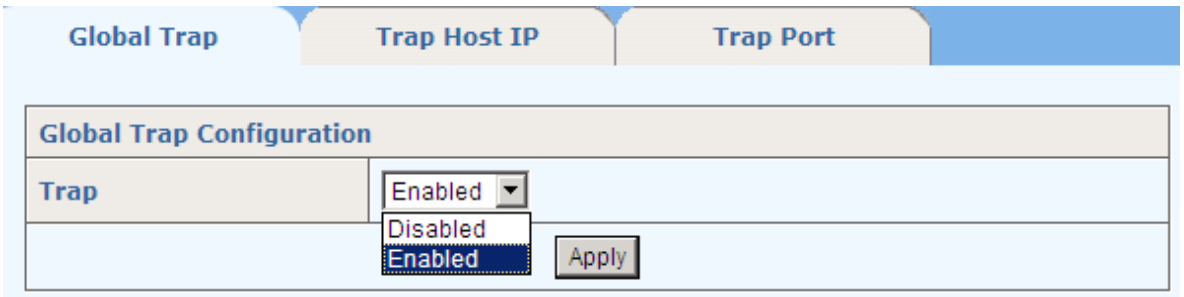
The bottom part of this page lists all existing SNMP v3 USM Users, including **SNMP Version**, **USM User**, and **Privilege**; you can delete any USM User.



14.2 SNMP Trap

There are three tab pages:

Global Trap: globally disables or enables the trap function; by default, the trap function is enabled.



Trap Host IP: specifies SNMP trap Host IP. Host IP is the IPv4 address of the host to receive the traps.

The bottom part of this page lists all existing hosts' IP addresses. You can delete any trap host IP address.

Global Trap | Trap Host IP | Trap Port

Add Trap Host IP

Host IP	

Apply

Current Trap Users

Number	Host IP	Delete

Trap Port: disables or enables the trap function for each port.

The bottom part of this page lists the trap status of all ports.

Global Trap | Trap Host IP | Trap Port

Port Trap Configuration

Port	Ethernet0/1
Trap	Enabled

Apply

Port Trap Status

Port	Trap	Port	Trap
Ethernet0/1	Enabled	Ethernet0/2	Disabled
Ethernet0/3	Enabled	Ethernet0/4	Enabled
Ethernet0/5	Enabled	Ethernet0/6	Enabled
Ethernet0/7	Enabled	Ethernet0/8	Enabled
Ethernet0/9	Enabled	Ethernet0/10	Enabled
Ethernet0/11	Enabled	Ethernet0/12	Enabled
Ethernet0/13	Enabled	Ethernet0/14	Enabled
Ethernet0/15	Enabled	Ethernet0/16	Enabled
Ethernet0/17	Enabled	Ethernet0/18	Enabled
Ethernet0/19	Enabled	Ethernet0/20	Enabled
Ethernet0/21	Enabled	Ethernet0/22	Enabled
Ethernet0/23	Enabled	Ethernet0/24	Enabled
Ethernet1/1	Enabled	Ethernet1/2	Enabled

15 Administration

This part covers switch management and maintenance functions, including Fgms, IP Configuration, SNTP, Ping Diagnosis, Account, TFTP Services, Reboot, Reset, Save Configuration and System Logs, shown as follows.

- Administration
  - Fgms
  - IP Configuration
  - SNTP
  - Ping Diagnosis
  - Account
  - TFTP Services
  - Reboot
  - Reset
  - Save Configuration
  - System Logs

15.1 IP Configuration

The managed switch supports DHCP and Static IP. **DHCP Client** can be enabled by checking the **Enabled** checkbox. If static IP is used, **IP Address**, **Subnet Mask**, and **Gateway** shall be specified.

IP Configuration

DHCP Client	☐ Enabled
IP Address	192 . 168 . 0 . 253
Subnet Mask	255 . 255 . 255 . 0
Gateway	192 . 168 . 0 . 201
	Apply

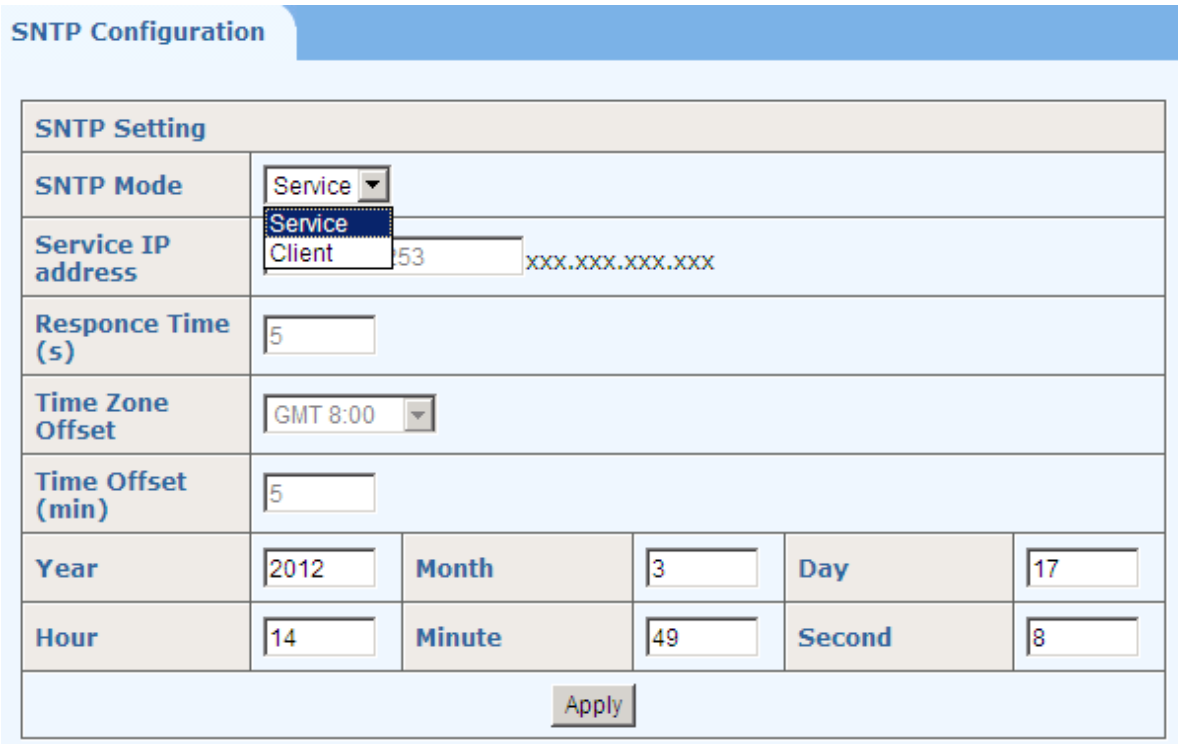
15.2 SNTP

This page configures SNTP (Simple Network Time Protocol).

SNTP Mode	Select Service mode or Client mode. If you select Client mode, you can set switch time through the SNTP server for synchronization time; If Service mode is selected, switch will be used as SNTP sever.
Service IP address	IP address of SNTP server

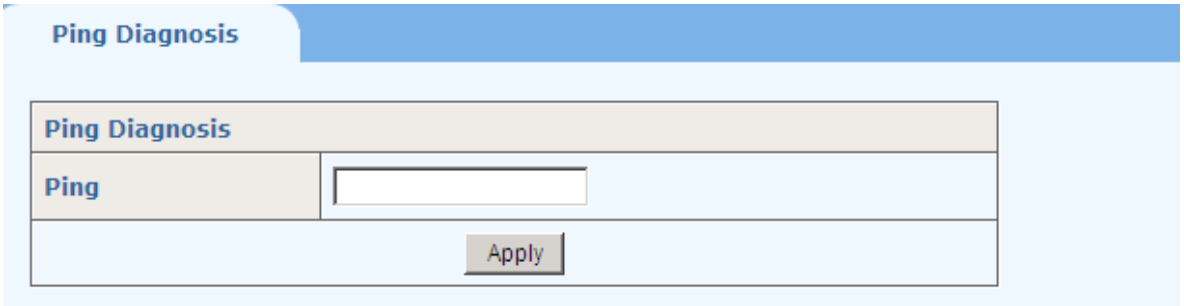
Response Time Time interval for the switch to get a response from SNTP server, in the unit of second
Time Zone Offset Time difference between Greenwich standard time and local time
Time Offset (min) Time difference in minute between Greenwich standard time and local time

In Service Mode, system time can be set with year, month, day, hour, minute and second.



15.3 Ping Diagnosis

This page can be used to ping a specific IP address.



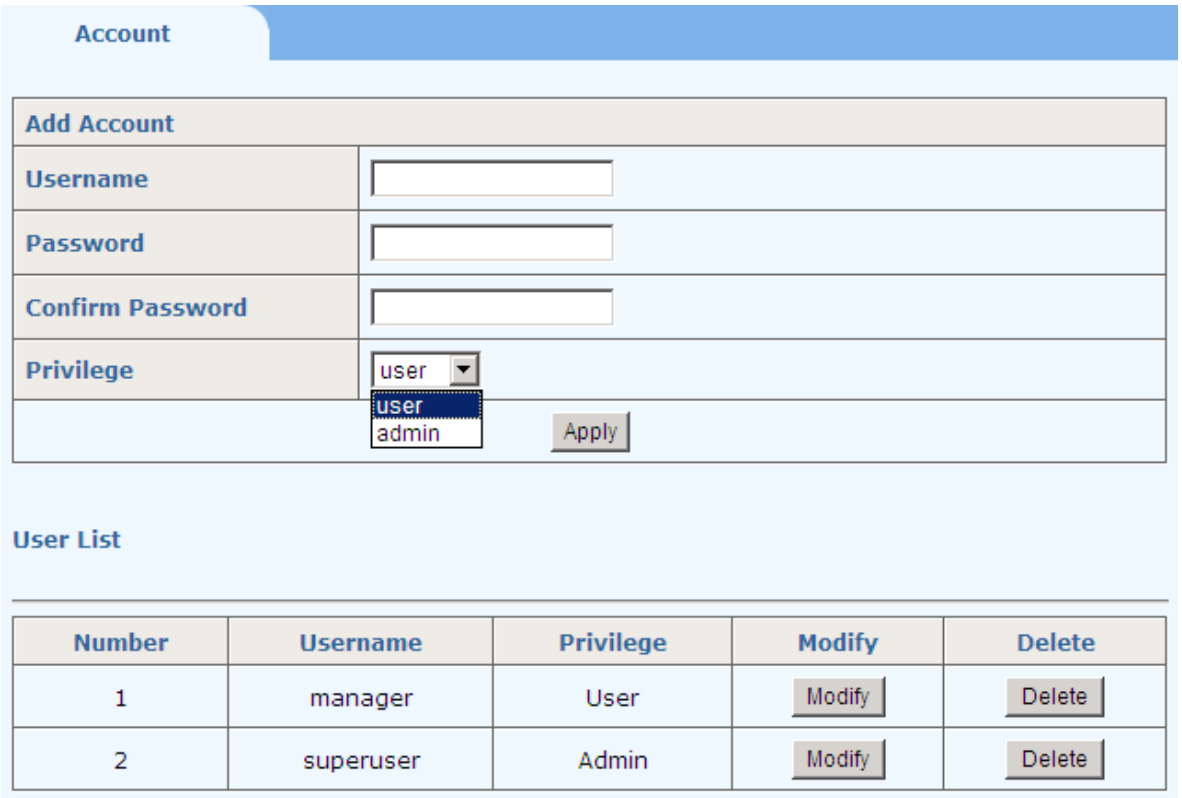
15.4 Account

This page can be used to add a new account. **Username**, **Password**, and **Privilege** for the new account are set on this page.

Username username, a string of 3 to 16 characters.
Password password, a string of 1 to 16 characters.
Privilege choose **user** or **admin**.

The bottom part of this page lists all accounts, including **Username** and **Privilege**. An account can be modified or deleted on this page.

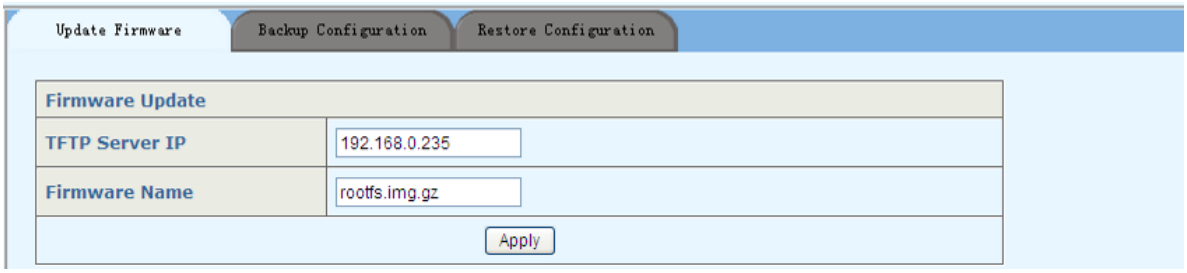
Note: Check section 1.7 Default Configuration of this manual for privilege details of each level of users.



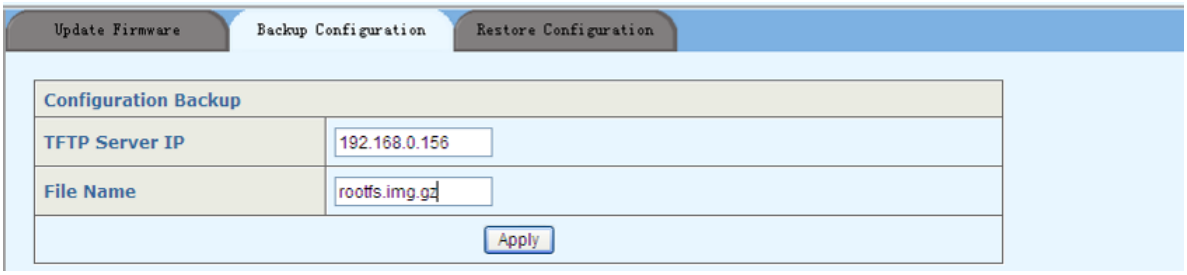
15.5 TFTP Services

There are three tab pages.

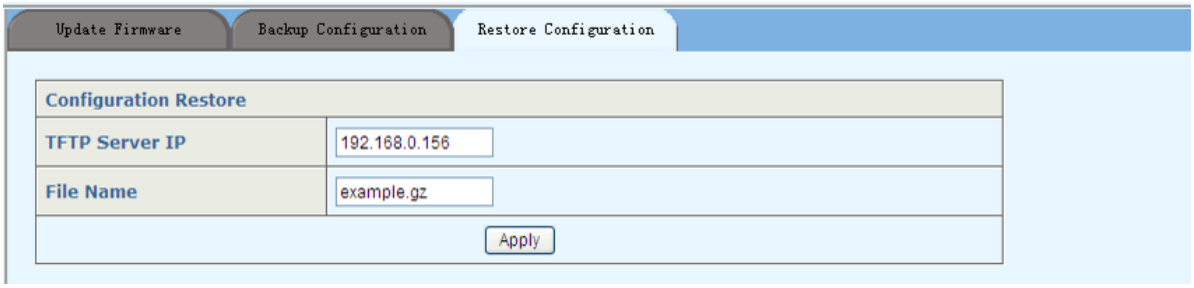
(1) *Update Firmware*: This page sets a **TFTP Server IP** and **Firmware Name**. Before doing firmware upgrade, make sure the switch is connected to the TFTP server and new firmware file exists on the server. The switch will begin to update firmware after **Apply** button is clicked.



(2) *Backup Configuration*: This page sets a **TFTP Server IP** and **File Name**. Before backing up configuration, make sure the switch is connected to the TFTP server. The switch configuration file will be uploaded to TFTP server with the specified **File Name** after **Apply** button is clicked.



(3) *Restore Configuration*: This page sets a **TFTP Server IP** and **File Name**. Before restoring a configuration, make sure the switch is connected to the TFTP server. The switch will download the file with the specified **File Name** and use it as the configuration file after **Apply** button is clicked.

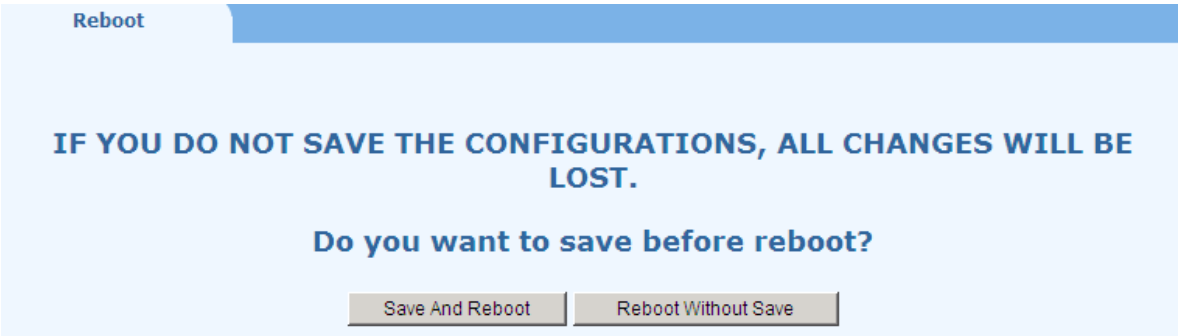


> 📖Note:
>
> During updating firmware, uploading or downloading a configuration file, make sure the power is on.

15.6 Reboot

In this page, there are two buttons: **Save And Reboot** and **Reboot Without Save**.

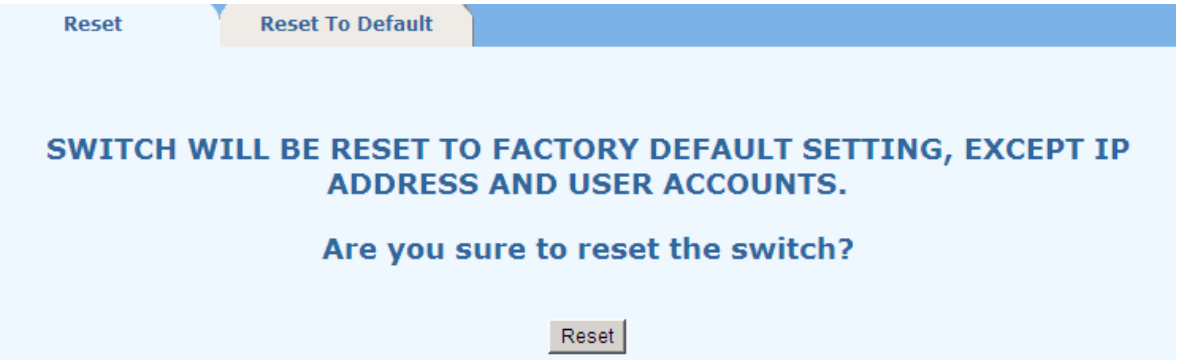
Save And Reboot: saves the current configuration and then reboot
Reboot Without Save: directly reboots without saving the current configuration. All changes may be lost.



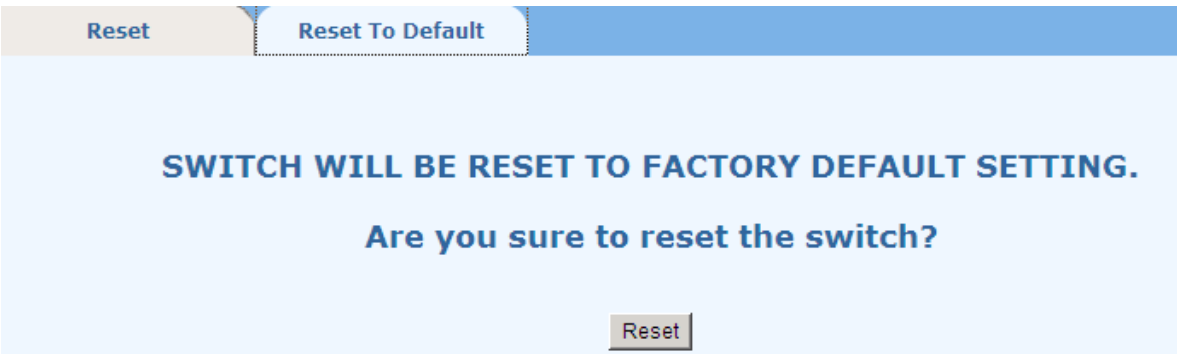
15.7 Reset

There are two tab pages: *Reset* and *Reset To Default*.

Reset: the switch will be reset to the factory default setting, except that the IP address and user accounts are kept unchanged.

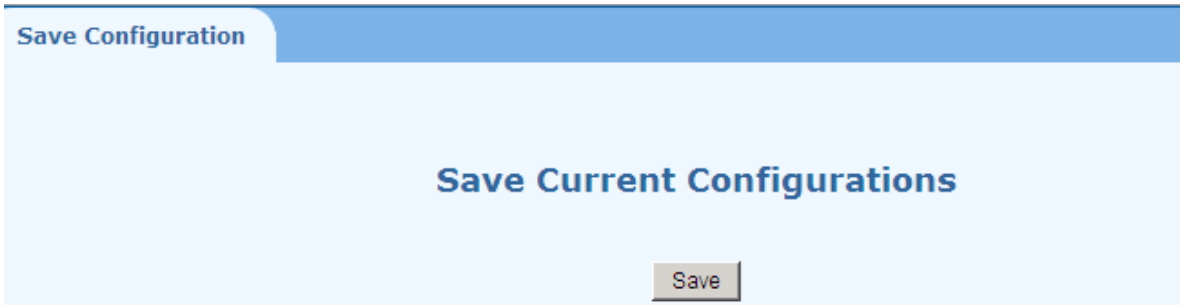


Reset To Default: the switch will be reset to the factory default setting.



15.8 Save Configuration

This page saves current configurations.

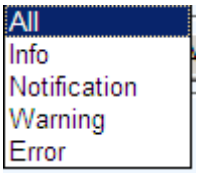


15.9 System Logs

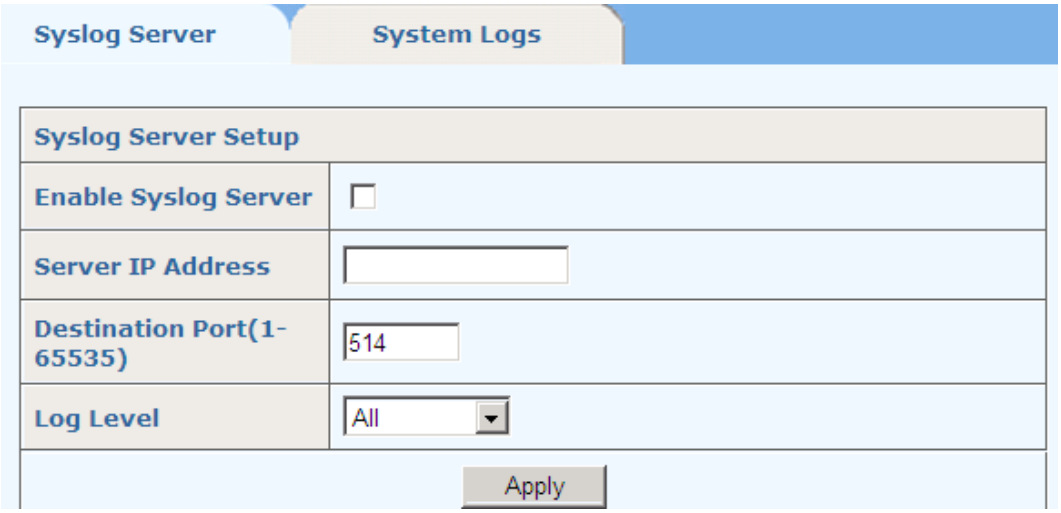
There are two tab pages: *Syslog Server* and *System Logs*.

(1) *Syslog Server*

This page is for setting syslog server.

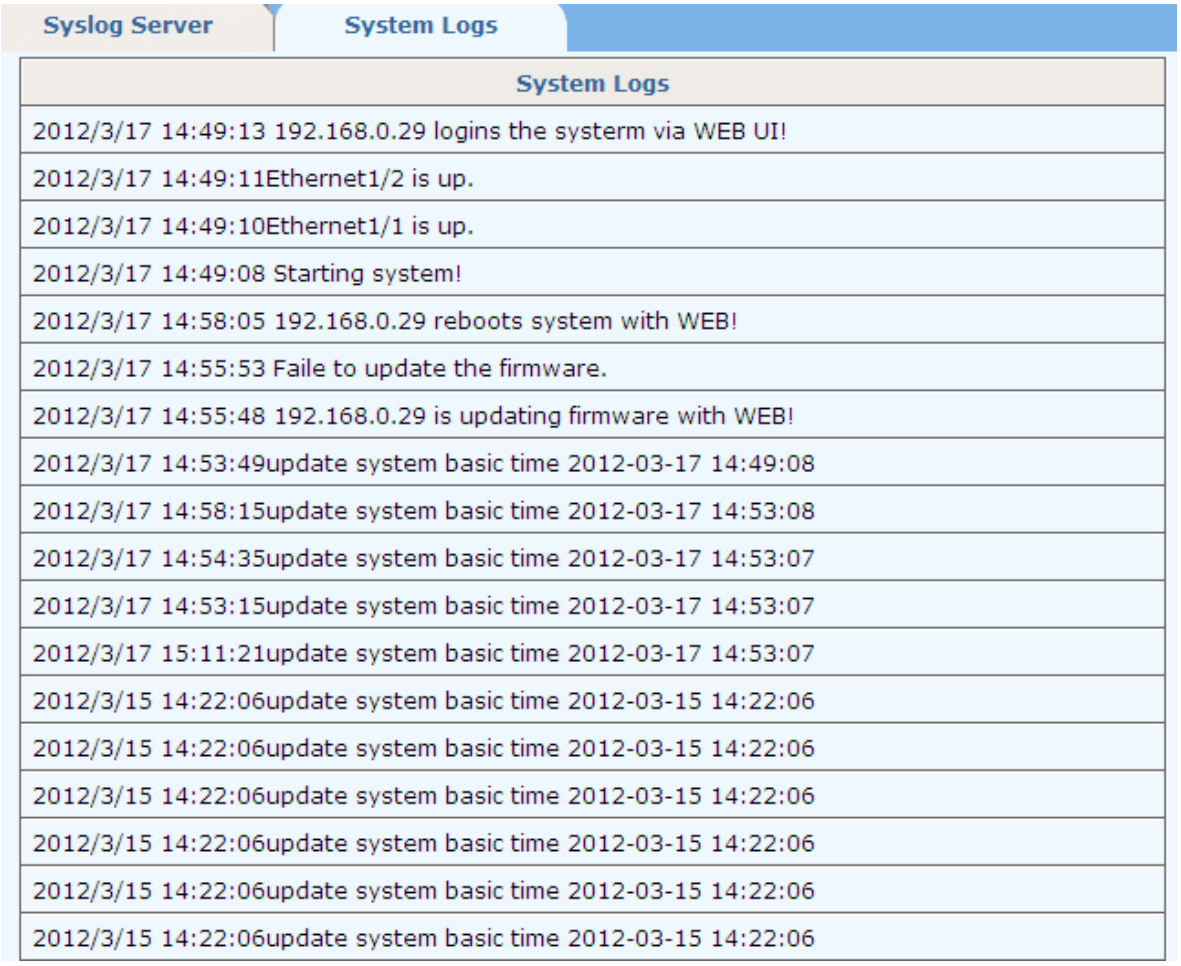


Syslog Server: can be enabled or disabled.
Server IP Address: Type the server IP address.
Destination Port: It is in the range of 1 to 65535, and the default value is 514.
Log Level: There are four log levels: Info, Notification, Warning and Error.



(2) *System Logs*

This page shows all of the system logs, clicking on <Clear> to clear all the records of the system logs.



16 Logout

Click <Logout> in the left menu to log out from the switch and close the browser.

Appendix A: Supported MIBs

This appendix lists the supported Management Information Base (MIBs) for this release of the XS26GS switch.

MIB list

RFC1213-MIB

RFC1493-BRIDGE-MIB

RFC1573-IF-MIB

RFC1643-EtherLike-MIB

RFC1757-RMON-MIB

RFC2618-RADIUS-AUTH-CLIENT-MIB

RFC2620-RADIUS-ACC-CLIENT-MIB

RFC2674-P-BRIDGE-MIB

RFC2674-Q-BRIDGE-MIB

LLDP-MIB

IEEE8021-PAE-MIB

FMC-SWITCH-MIB

FMC-IGMP-SNOOPING-MIB

FMC-SWITCH-MAC-AUTHENTICATION-MIB

FMC-SWITCH-RADIUS-MIB

FMC-MSTP-MIB

FMC-MVR-MIB

RSTP-MIB