GIGA COPPER NETWORKS

User Guide

G4200-4T/ G4200-8T Switch

GIGA Copper Networks GmbH

Disclaimer Notice

No license is granted, implied or otherwise, under any patent or patent rights of GIGA Copper Networks GmbH. GIGA Copper Networks GmbH makes no warranties, implied or otherwise, in regard to this document and to the products described in this document. The information provided by this document is believed to be accurate and reliable to the publication date of this document. However, GIGA Copper Networks GmbH no responsibility for any errors in this document. Furthermore, GIGA Copper Networks GmbH assumes no responsibility for the use or misuse of the information in this document and for any patent infringements that may arise from the use of this document. The information and product specifications within this document are subject to change at any time, without notice and without obligation to notify any person of such change.

Revision History

Revision	Date	Reason for change
V 1.0	July 30, 2020	Initial release

Table of Contents

1 Overview

The G4200-4T/G4200-8T system contains two devices, the Headend Switch G4200-4T/G4200-8T and the Client device. It enables IP-based Video, Data and VoIP applications over existing coax cabling or telephone lines. It is the industry leading solution solving the secure delivery of IP Multiservice in a high density copper environment.

In a Fiber to the Building (FTTB) network solution, this device can deliver high-speed networking over legacy wires with significantly lower installation and operating costs, the legacy wires are those using coaxial cables, telephone lines or power lines. With scalability of up to 64 units the G4200-4T/ G4200-8T solution can scale to serve several hundred of end users connected on a copper network, GL-8xMT is the Ideal Solution for FTTH MDU Deployments.

1.1 Features

Key Highlights:

- Egress /Ingress rate management control and broadcast storm control
- IEEE 802.1Q tagged VLAN, port based VLAN
- Various QoS capability (IEEE 802.1p / port / Diffserv)
- SFF 8472, Digital Diagnostic Monitor
- Support port mirroring and port isolate
- Support SNMP trap and SNMP client
- MIB Counter
- Upgrade firmware, backup configuration, restore configuration
- Firmware upgrade via TFTP
- IGMP snooping for filtering multicast traffic
- Perfect network management through web browser, CLI, Telnet /serial console
- Support SNMP v1/v2c/v3 for different levels of network management
- Support three level user for manage
- Supports 1Gbps PHY bit rate over single medium
- State-of-the-Art LDPC forward error correction (FEC)
- Remote configuration management integrated on-chip
- Remote one-step firmware upgrade

- Upload configuration files, notches management
- Reliable HD IPTV and internet distribution
- Unique solution for Last Mile, MDU & Campus
- Up to 1 Km Bi-Directional solution with no need to upgrade/change the existing infrastructure
- Up to 900 Mbps of actual throughput over twisted pair

Applications:

- Fiber to the Building (FTTB) network
- Small and medium enterprises network
- Condos and Townhomes
- Mid-rise Apartments
- Garden-Style Apartments

1.2 Port Configuration

Model	G.hn Port	Console Port	Ethernet Port	Monitor Port	SYNC Port	Power Supply
G4200-4T	4x/RJ45	1xRS-232 RJ45	2x10G BaseX SFP 2x10/100/1000BaseT RJ45	1 x10/100/1000BaseT RJ45	1x50Hz BNC input 1x50Hz BNC output	2x100-240VAC
G4200-8T	8x/RJ45	1xRS-232 RJ45	2x10G BaseX SFP 2x10/100/1000BaseT RJ45	1 x10/100/1000BaseT RJ45	1x50Hz BNC input 1x50Hz BNC output	2x100-240VAC

1.3 Default Configuration

- IP Address: 192.168.0.252
- Subnet Mask: 255.255.255.0
- Default Gateway: 192.168.0.1

Account:

Access Level	User Name	Password	Rights
Administrator	superuser	123	All operations on the switch

User	manager	123	All oper ations except the following ● Create or delete accounts ● Reset ● Software upgrade, backup and restoration through TFTP
Visitor	guest	123	Networking utility such as “ping” and “show”, but the following are not allowed to be used: “show user”, “show snmp community”, “show snmp traps-host”, and “show snmp user”. Note: Visitor can only access the switch through a serial port.

2 Hardware Descriptions

The system contains two devices, local device（G4200-4T/ G4200-8T）and remote device, as show in the following drawings.

G4200-4T

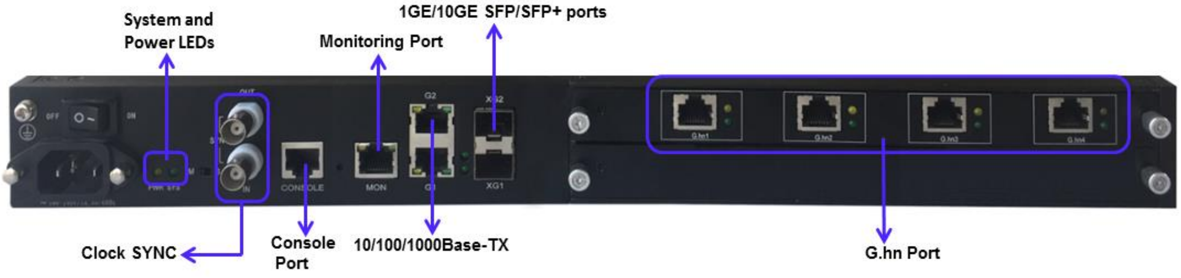
G4200-8T

2.1 G4200-4T (Local device)

G4200-4T is the device of multiplexer system, as shown in the following drawings. It supports 2 x10G SFP ports, 2 x 10/100/1000BT ports, 4 x RJ45 Ports, one gigabit monitor port.

2.1.1 Panel

The front panel is shown below:



The following table shows the port descriptions.

Label	Description
Console	Console port: A RS-232 connector for connection to a computer for console control/administration. The RS-232 console port can be used for accessing the device CLI (command line interface) for out-of-band management.
MON	Monitor port , 1 x 1GE local system provision/monitoring port
G1/G2	2 x 1GE Ethernet ports for uplink aggregation
XG1/XG2	2 x 10GE SFP Ethernet ports for uplink aggregation
G.hn1/G.hn2	G.hn ports for data signal and Phone signal
SYNC	Clock SYNC

The following table shows the LED descriptions.

Label	Type	Color	State	Description
PWR A/B	Power status	Yellow	On	The power is on and supplying the current to the system
			Off	The power is off or it is not supplying the current to the system
SYS	System status	Green	On	System is started
			Off	System has not started
G.hn 1/G.hn2	G.hn link status	Green	On	The corresponding port connection normal
			Off	The link condition is poor or there is no connection to this port
		Yellow	On	The corresponding port connection abnormal and link quality is poor
			Off	The link condition is normal or there is no connection to this port
XG1/XG2	Ethernet link status	Green	On	The corresponding port connection normal
			Off	there is no connection to this port
G.hn	G.hn port status	Green	On	The corresponding port is selected.
			Off	The corresponding port is not selected.
Slot	Slot status		On	The corresponding slot is selected.

			Off	The corresponding slot is not selected.
G1/G2/ MON	Ethernet link status	Green	On	Connection Rate 1000Mbps
			Off	Connection Rate 10/100 Mbps
		Yellow	On	The corresponding port connection normal
			Off	There is no connection to this port
			Blink	The G1/G2/ MON port is up and this port is working.

2.1.2 Physical and Environmental

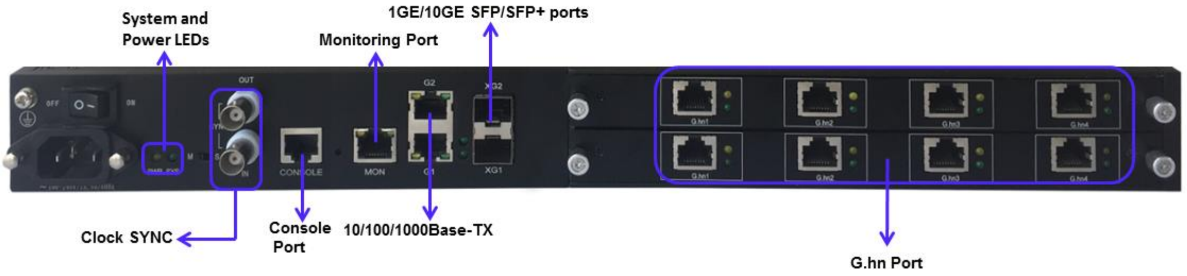
- Dimension: 19-inch rack-mount width, 1.0U height.
- Case: Aluminum, degree of protection IP30
- Weight: 3.2Kg
- Operating temperature: 0℃ ~ 60℃
- Storage temperature: -25℃ ~ 70℃
- Humidity: 10% ~ 90% RH Non-condensing
- Maximum power consumption: ~32W

2.2 G4200-8T (Local device)

G4200-8T is the device of multiplexer system, as shown in the following drawings. It supports 2 x10G SFP ports, 2 x 10/100/1000BT ports, 8 x RJ45 Ports, one gigabit monitor port.

2.2.1 Panel

The front panel is shown below:



The following table shows the port descriptions.

Label	Description
Console	Console port: A RS-232 connector for connection to a computer for console control/administration. The RS-232 console port can be used for accessing the device CLI (command line interface) for out-of-band management.
MON	Monitor port , 1 x 1GE local system provision/monitoring port
G1/G2	2 x 1GE Ethernet ports for uplink aggregation
XG1/XG2	2 x 10GE SFP Ethernet ports for uplink aggregation
G.hn1/G.hn2/G.hn3/G.hn4	G.hn ports for data signal and Phone signal
SYNC	Clock SYNC

The following table shows the LED descriptions.

Label	Type	Color	State	Description
PWR A/B	Power status	Yellow	On	The power is on and supplying the current to the system
			Off	The power is off or it is not supplying the current to the system
SYS	System status	Green	On	System is started
			Off	System has not started
G.hn1/ G.hn2/ G.hn3/ G.hn4	G.hn link status	Green	On	The corresponding port connection normal
			Off	The link condition is poor or there is no connection to this port
		Yellow	On	The corresponding port connection abnormal and link quality is poor
			Off	The link condition is normal or there is no connection to this port
XG1/XG2	Ethernet link status	Green	On	The corresponding port connection normal
			Off	there is no connection to this port
G.hn	G.hn port status	Green	On	The corresponding port is selected.
			Off	The corresponding port is not selected.
Slot	Slot status		On	The corresponding slot is selected.
			Off	The corresponding slot is not selected.

G1/G2/ MON	Ethernet link status	Green	On	Connection Rate 1000Mbps
			Off	Connection Rate 10/100 Mbps
		Yellow	On	The corresponding port connection normal
			Off	There is no connection to this port
			Blink	The G1/G2/ MON port is up and this port is working.

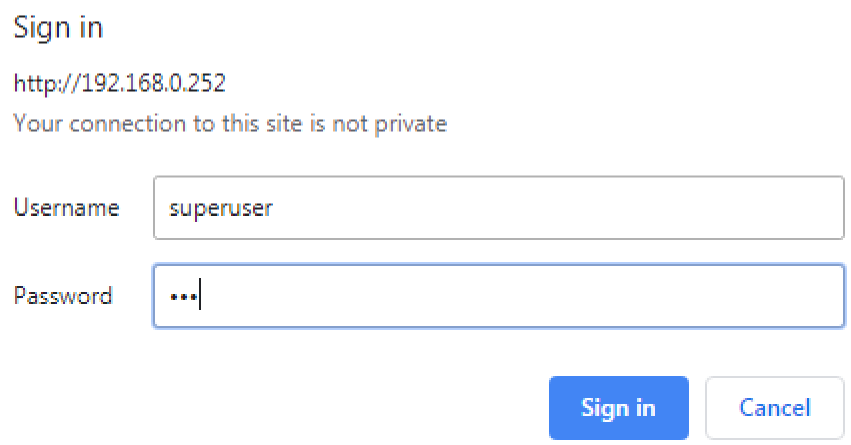
2.2.2 Physical and Environmental

- Dimension: 19-inch rack-mount width, 1.0U height.
- Case: Aluminum, degree of protection IP30
- Weight: 3.2Kg
- Operating temperature: 0℃ ~ 60℃
- Storage temperature: -25℃ ~ 70℃
- Humidity: 10% ~ 90% RH Non-condensing
- Maximum power consumption: ~32W

3 G4200-4T Web-based Management

The Web-based management interface is one of many tools specifically designed to assist the network manager in creating complex standalone or network configurations. The G4200-4T provides the default network settings for the Web browsers as section Default Configuration, It offers three different login privileges: superuser, manager and guest.

You can browse http://192.168.0.252, type user name and password as section Default Configuration, if you have not made any change to the network setting.



Sign in

http://192.168.0.252

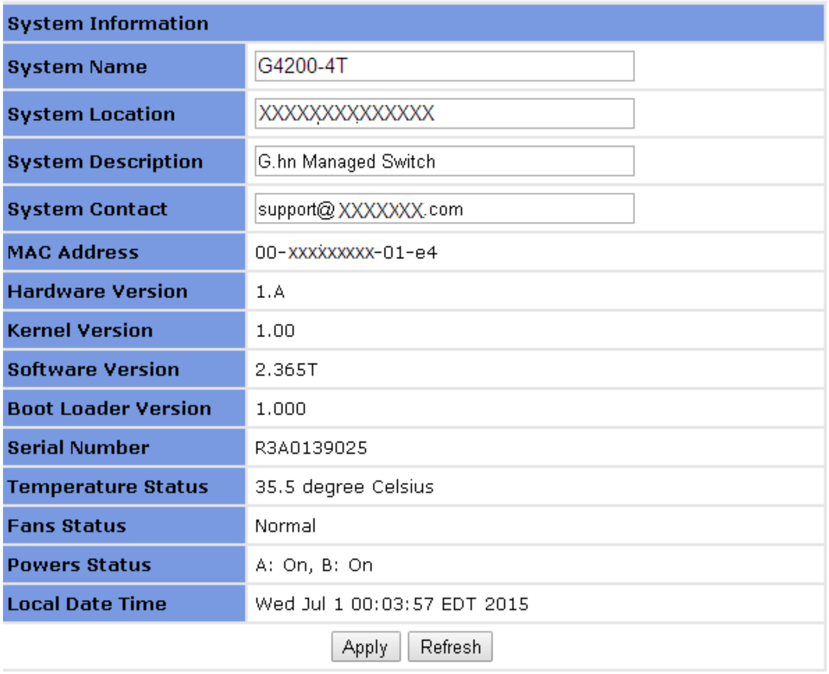
Your connection to this site is not private

Username: superuser

Password: •••

3.1 System Information

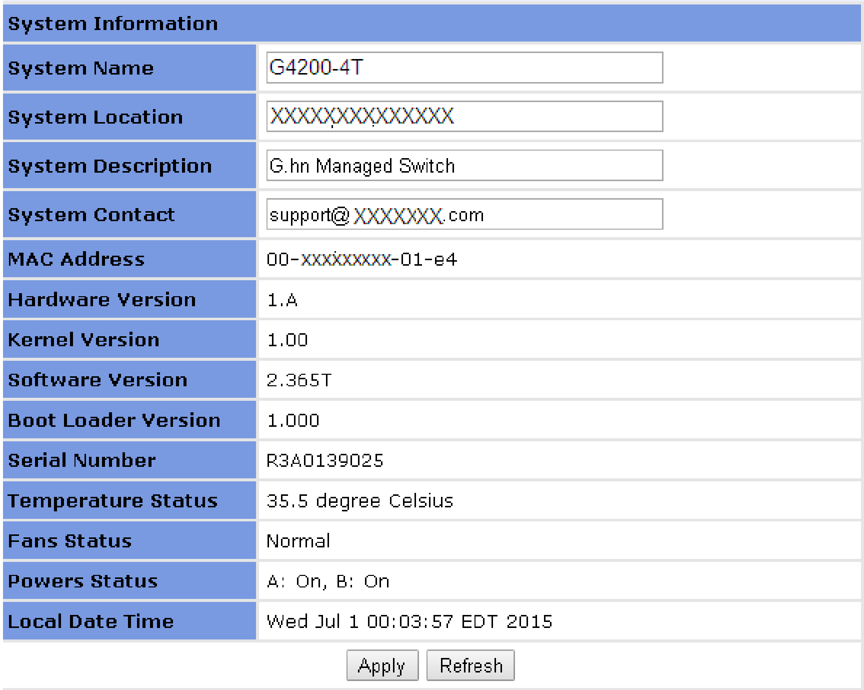
After login, the system Information page is shown, displaying the basic information of the switch as below.



System Information	
System Name	G4200-4T
System Location	XXXXXXXXXXXXXX
System Description	G.hn Managed Switch
System Contact	support@XXXXXXX.com
MAC Address	00-xxxxxxxxx-01-e4
Hardware Version	1.A
Kernel Version	1.00
Software Version	2.365T
Boot Loader Version	1.000
Serial Number	R3A0139025
Temperature Status	35.5 degree Celsius
Fans Status	Normal
Powers Status	A: On, B: On
Local Date Time	Wed Jul 1 00:03:57 EDT 2015

3.1.1 Basic Information

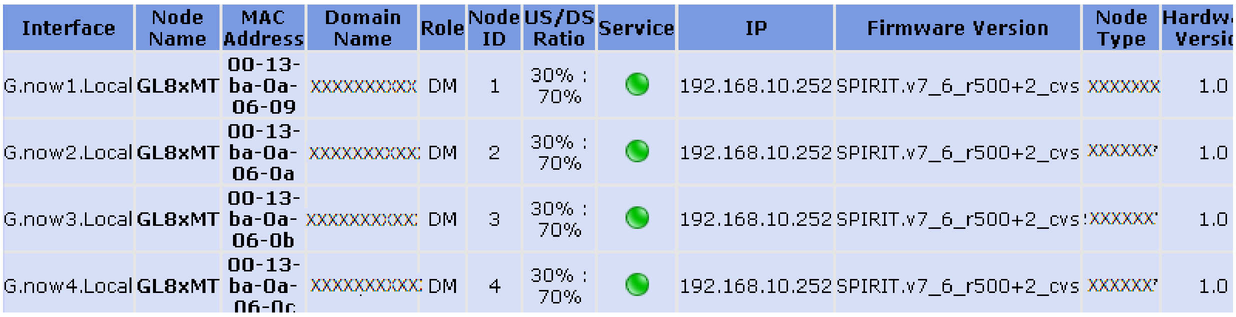
The Basic Information is shown as below:



System Information	
System Name	G4200-4T
System Location	XXXXXXXXXXXXXX
System Description	G.hn Managed Switch
System Contact	support@ XXXXXXX.com
MAC Address	00-xxxxxxxxx-01-e4
Hardware Version	1.A
Kernel Version	1.00
Software Version	2.365T
Boot Loader Version	1.000
Serial Number	R3A0139025
Temperature Status	35.5 degree Celsius
Fans Status	Normal
Powers Status	A: On, B: On
Local Date Time	Wed Jul 1 00:03:57 EDT 2015

3.1.2 Node Summary

Detailed information of all the devices in the system is shown below.



Interface	Node Name	MAC Address	Domain Name	Role	Node ID	US/DS Ratio	Service	IP	Firmware Version	Node Type	Hardw Versi
G.now1.Local	GL8xMT	00-13-ba-0a-06-09	XXXXXXXXXX	DM	1	30% : 70%	●	192.168.10.252	SPIRIT.v7_6_r500+2_cvs	XXXXXXX	1.0
G.now2.Local	GL8xMT	00-13-ba-0a-06-0a	XXXXXXXXXX	DM	2	30% : 70%	●	192.168.10.252	SPIRIT.v7_6_r500+2_cvs	XXXXXX	1.0
G.now3.Local	GL8xMT	00-13-ba-0a-06-0b	XXXXXXXXXX	DM	3	30% : 70%	●	192.168.10.252	SPIRIT.v7_6_r500+2_cvs	XXXXXX	1.0
G.now4.Local	GL8xMT	00-13-ba-0a-06-0c	XXXXXXXXXX	DM	4	30% : 70%	●	192.168.10.252	SPIRIT.v7_6_r500+2_cvs	XXXXXX	1.0

Interface Ghn port node.

Node Name Name of designated port

MAC Address Designated port MAC address

Domain Name Designated port domain name, local name is the same as remote name.

Role The role of designated ports: Local DM, Remote DM. DM: Domain Master EP: Endpoint

Node ID Designated port ID,

US/DS Ratio Designated port US/DS Ratio,。
US: upstream，transmitter data stream from remote EP to local DM.
DS: downstream， transmitter data stream from local DM to remote EP.

Service Ethernet port service status of designated port. Green: Connected state; Orange: Off state

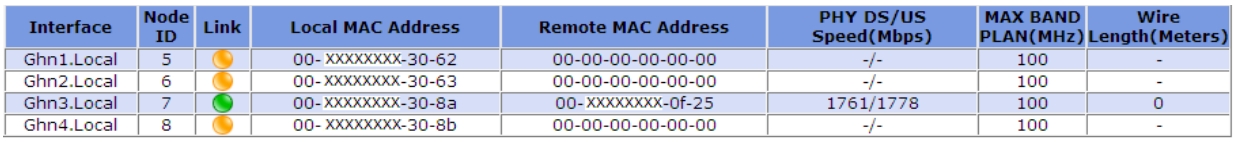
IP IP Address of designated port.

Firmware Version Firmware version of designated port.

Node Type Type of designated port.

Hardware Version Hardware version of designated port.

3.1.3 Interface Information



Interface	Node ID	Link	Local MAC Address	Remote MAC Address	PHY DS/US Speed(Mbps)	MAX BAND PLAN(MHz)	Wire Length(Meters)
Ghn1.Local	5	🟠	00- XXXXXXXX-30-62	00-00-00-00-00-00	-/-	100	-
Ghn2.Local	6	🟠	00- XXXXXXXX-30-63	00-00-00-00-00-00	-/-	100	-
Ghn3.Local	7	🟢	00- XXXXXXXX-30-8a	00- XXXXXXXX-0f-25	1761/1778	100	0
Ghn4.Local	8	🟠	00- XXXXXXXX-30-8b	00-00-00-00-00-00	-/-	100	-

Interface Ghn Port Node

Link Connection status of designated port

Local MAC Address Local node MAC address of designated port

Remote MAC Address Remote node MAC address of designated port

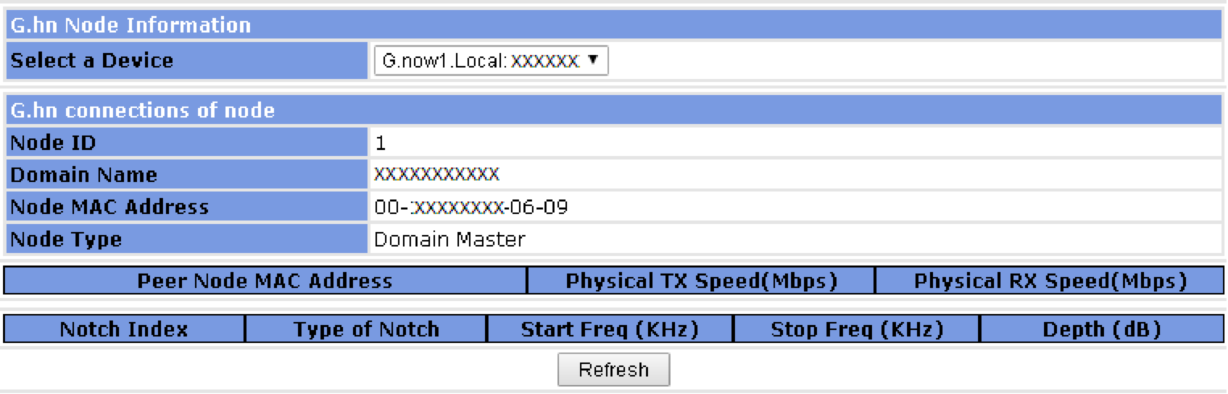
PHY DS/US Speed(Mbps) PHY rate of designated port, Unit: Mbps。 US: upstream，transmitter data stream from remote EP to local DM。 DS: downstream，transmitter data stream from local DM to remote EP

MAX BAND PLAN(MHz) Maximum band plan capability of designated port，Unit: MHz。

Wire Length(Meters) The distance between local node and remote node of designated port . Unit: Meters

3.1.4 Node Details

On this page, the connection information of selected devices is shown below.



G.hn Node Information	
Select a Device	G.now1.Local:XXXXXX ▼

G.hn connections of node	
Node ID	1
Domain Name	XXXXXXXXXXX
Node MAC Address	00-:XXXXXXXX-06-09
Node Type	Domain Master

Peer Node MAC Address	Physical TX Speed(Mbps)	Physical RX Speed(Mbps)

Notch Index	Type of Notch	Start Freq (KHz)	Stop Freq (KHz)	Depth (dB)

Select a Device Designate Ghn node

Peer Node MAC Address MAC address for the node connected with designated port.

Physical TX Speed(Mbps) Physical TX rate of designated portthe data stream rate from designated node to peer node. Unit: Mbps

Physical RX Speed(Mbps) Physical RX rate for designated port, the data stream rate from peer node to designated node. Unit: Mbps

Notch Index Notch Information Index of Designated Node.

Type of Notch Notch type. User means the Notch created by User.

Start Frequency (KHz) Band started frequency, unit KHz

Stop Frequency (KHz) Band stop frequency, unit KHz

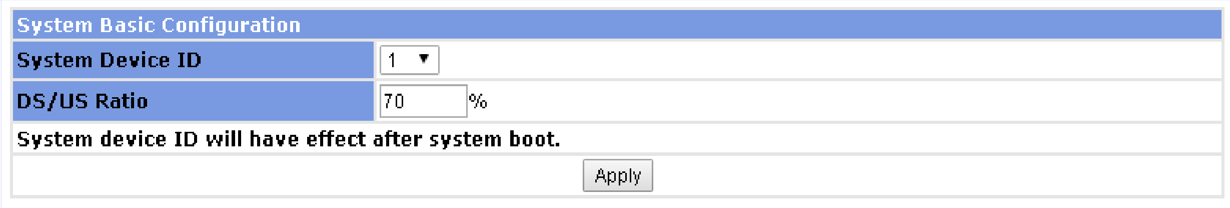
Depth (1.40dB) Attenuation value, unit dB

3.2 Configuration

3.2.1 Basic Configuration

On this page, you can configure system device ID, US/DS ratio.

Node ID will refresh with the reset of system device ID.

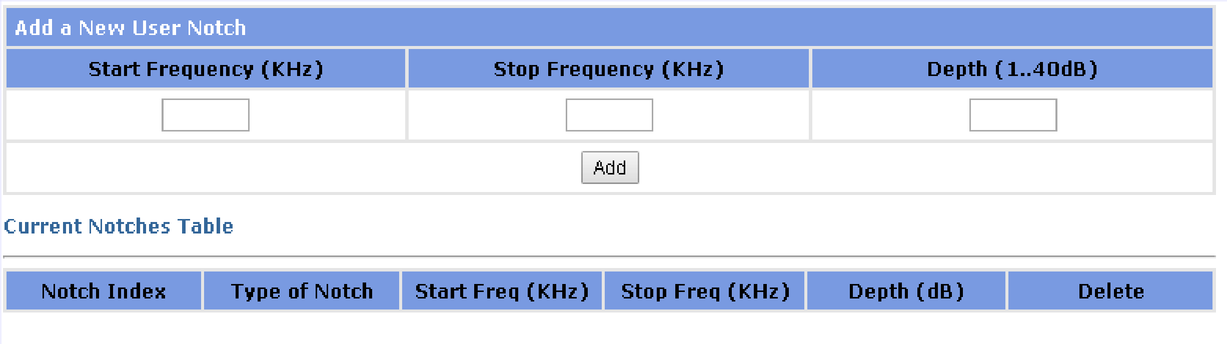


System Basic Configuration	
System Device ID	1 ▼
DS/US Ratio	70 %
System device ID will have effect after system boot.	

3.2.2 Spectrum Filtering

This tab page configures certain band attenuation. Generally, G.hn some band will be shield when G.hn and other signal share the same telephone line.

Start Frequency (KHz)：Band started frequency, unit: KHzStop Frequency (KHz)：Band stop frequency, unit: KHz
Depth (1.40dB): Attenuation value, unit: dB



Add a New User Notch

Start Frequency (KHz)	Stop Frequency (KHz)	Depth (1..40dB)

Current Notches Table

Notch Index	Type of Notch	Start Freq (KHz)	Stop Freq (KHz)	Depth (dB)	Delete

3.2.3 Node Configuration

On this page,you can configure selected devices basic configuration, enable or disable DHCP Client，VLAN, and broadcast IGMP.

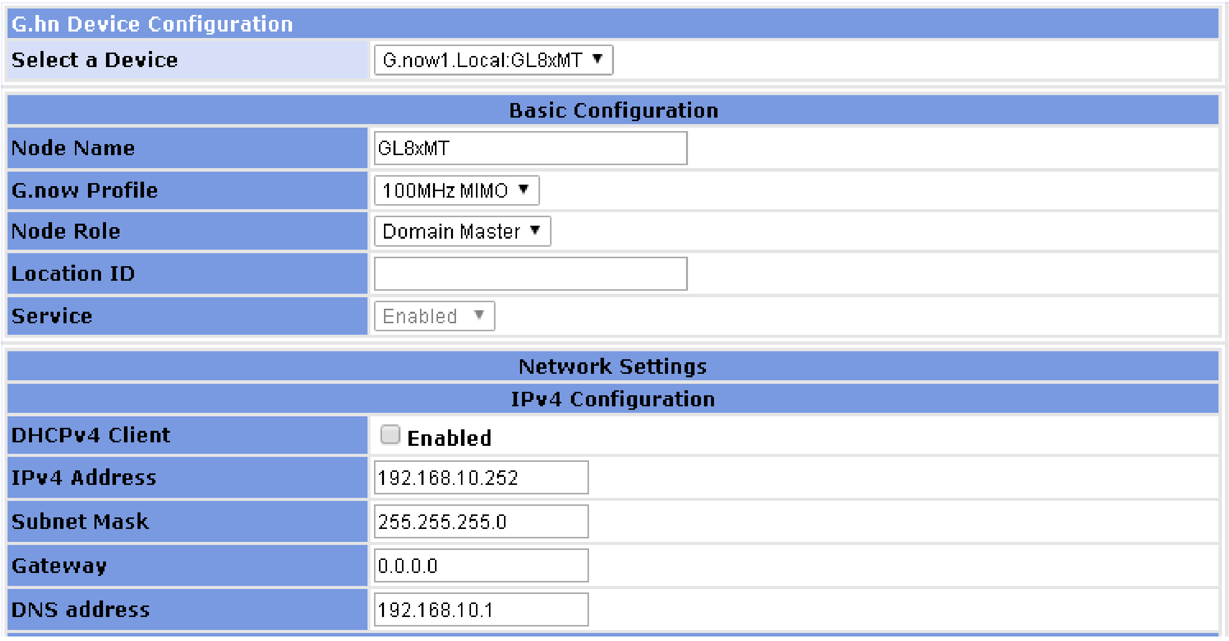
G.now Profile: Specifies the frequency mode used in the G.hn communication.

Optional Mode: 100MHz MIMO or 200MHz. 100MHz, connect with local node and remote node by 1 channel.

VLAN: VLAN function control switch

Ethernet Port Trunk： When downstream packets is “tag=Ethernet pvid”，the packets tag will be deleted, otherwise it will be saved.

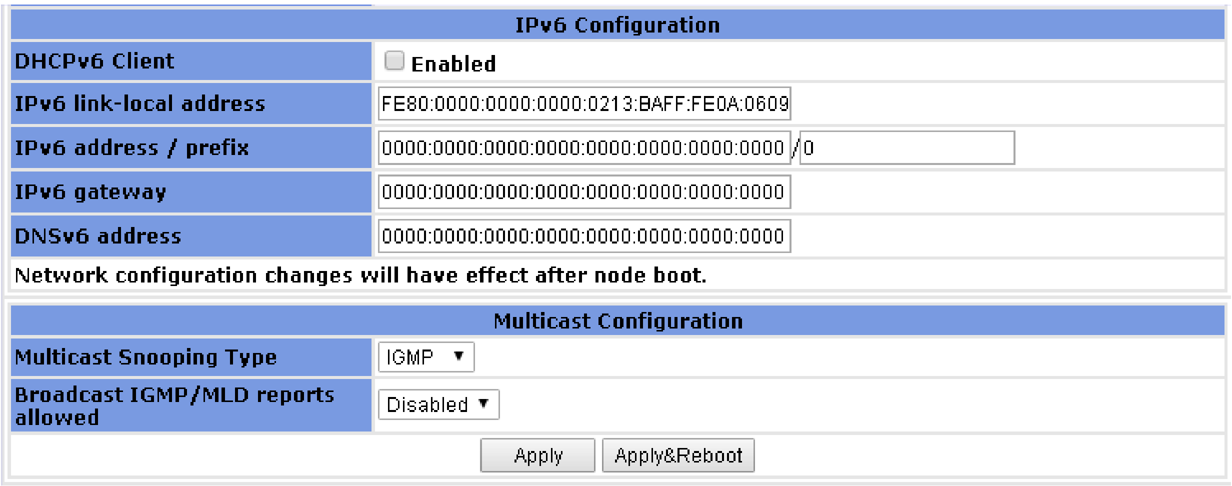
Ethernet PVID：When upstream Ethernet data packages without tags reach the port, it will have PVID tag.



G.hn Device Configuration	
Select a Device	G.now1.Local:GL8xMT ▼

Basic Configuration	
Node Name	GL8xMT
G.now Profile	100MHz MIMO ▼
Node Role	Domain Master ▼
Location ID	
Service	Enabled ▼

Network Settings	
IPv4 Configuration	
DHCPv4 Client	□ Enabled
IPv4 Address	192.168.10.252
Subnet Mask	255.255.255.0
Gateway	0.0.0.0
DNS address	192.168.10.1



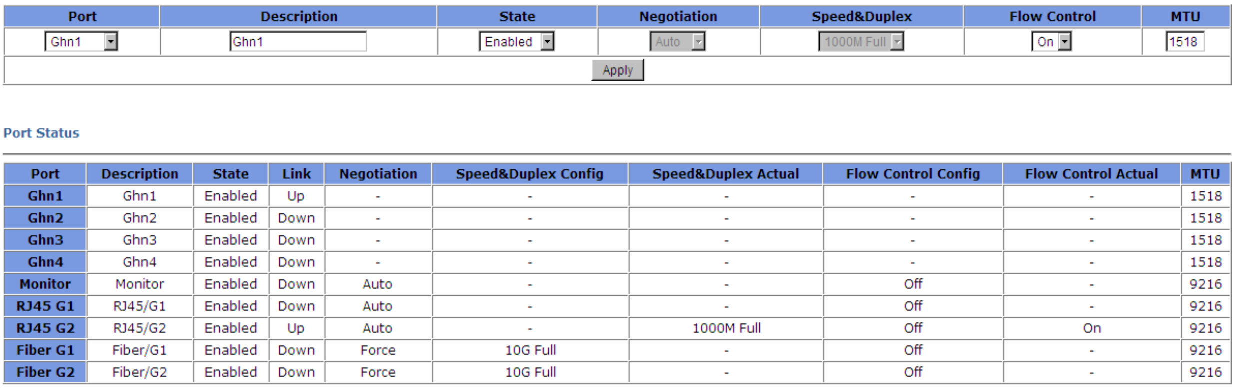
IPv6 Configuration	
DHCPv6 Client	□ Enabled
IPv6 link-local address	FE80:0000:0000:0000:0213:BAFF:FE0A:0609
IPv6 address / prefix	0000:0000:0000:0000:0000:0000:0000:0000 / 0
IPv6 gateway	0000:0000:0000:0000:0000:0000:0000:0000
DNSv6 address	0000:0000:0000:0000:0000:0000:0000:0000

Network configuration changes will have effect after node boot.

Multicast Configuration	
Multicast Snooping Type	IGMP ▼
Broadcast IGMP/MLD reports allowed	Disabled ▼

3.2.4 Port Configuration

At first, you should select a port for configuration. You can cofigure the port state, negotiation, speed and duplex, flow control, MAC learning and MDI/MDIX.



Port	Description	State	Negotiation	Speed&Duplex	Flow Control	MTU
Ghn1 ▼	Ghn1	Enabled ▼	Auto ▼	1000M Full ▼	On ▼	1518

Port Status

Port	Description	State	Link	Negotiation	Speed&Duplex Config	Speed&Duplex Actual	Flow Control Config	Flow Control Actual	MTU
Ghn1	Ghn1	Enabled	Up	-	-	-	-	-	1518
Ghn2	Ghn2	Enabled	Down	-	-	-	-	-	1518
Ghn3	Ghn3	Enabled	Down	-	-	-	-	-	1518
Ghn4	Ghn4	Enabled	Down	-	-	-	-	-	1518
Monitor	Monitor	Enabled	Down	Auto	-	-	Off	-	9216
RJ45 G1	RJ45/G1	Enabled	Down	Auto	-	-	Off	-	9216
RJ45 G2	RJ45/G2	Enabled	Up	Auto	-	1000M Full	Off	On	9216
Fiber G1	Fiber/G1	Enabled	Down	Force	10G Full	-	Off	-	9216
Fiber G2	Fiber/G2	Enabled	Down	Force	10G Full	-	Off	-	9216

⚠ Caution:

- Only when the state is enbaled, can you configure the negotiation, speed and duplex, flow control, MAC learning and MDI/MDIX.
- Only when the negotiation is in Force mode, can you configure the speed and duplex.

Port Specifies a port to configure

Description **Port Description**

State Enable/disble the port

Negotiation Selects Auto or Force, if Auto is selected, the port will automatically use the best operating mode; whereas if Force is selected, it needs to configure the speed and duplex manually.

Speed & Duplex There are four choices: 10M Half, 10M Full, 100M Half, and 100M Full.

Flow Control If flow control is enabled on both the local and peer switches. If congestion occurs on the local switch:

- The local switch sends a message to notify the peer switch to stop sending packets to itself or reduce the sending rate temporarily.
- The peer switch will stop sending packets to the local switch or reduce the sending rate temporarily when it receives the message; and vice versa. This allows packet loss to be avoided and the network service to operate normally.

If it is off, the port runs at full speed.

MTU The maximum transmission unit, in the range of 1518-9216 bytes.

After clicking <Apply>, the lower part lists the port status.

3.2.4 Aggregation

Link aggregation means aggregating several links together to form an aggregation group, so as to implement outgoing/incoming load balance among the member ports in the group and to enhance the connection reliability. Depending on different aggregation modes, aggregation groups fall into three types: manual, static LACP, and dynamic LACP.

3.2.4.1 Aggregate Groups

Configuration steps:

Step 1 Select Trunk ID. There are 13 groups (T1 ~ T13);

Step 2 Specify the trunk name;

Step 3 Specify the trunk type;

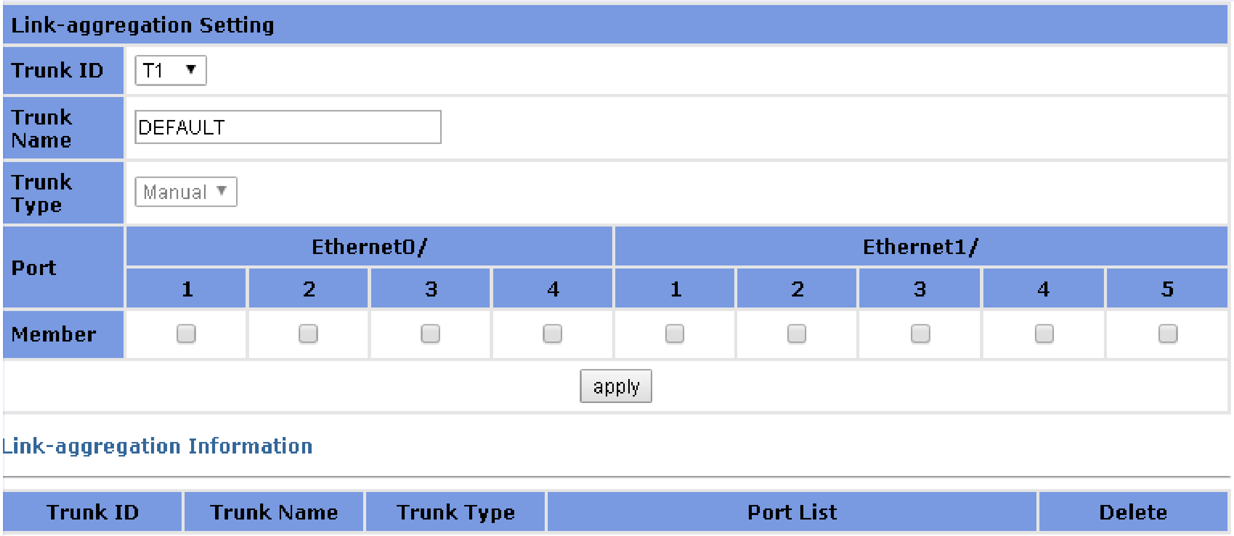
Manual: a manual trunk can only be manually set or deleted; LACP can be disabled.

Static: a static LACP trunk can only be manually set or deleted; any port in a static LACP trunk shall enable LACP protocol. 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.

Step 4 Select the ports as members of an aggregate group (2 ~ 8 ports);

Step 5 Click <Apply>, and then the link-aggregation Information will be listed at the lower part.

📖 Note: A trunk may be configured as a mirroring port, but it is not allowed to configure a trunk as a monitoring port.



Link-aggregation Setting

Trunk ID	T1 ▼								
Trunk Name	DEFAULT								
Trunk Type	Manual ▼								
Port	Ethernet0/				Ethernet1/				
	1	2	3	4	1	2	3	4	5
Member	□	□	□	□	□	□	□	□	□

apply

Link-aggregation Information

Trunk ID	Trunk Name	Trunk Type	Port List	Delete

⚠ Caution:

- The ports of the same link-aggregregation group should have the same basic configuration, such as STP, QoS, VLAN and port attribute and so on.

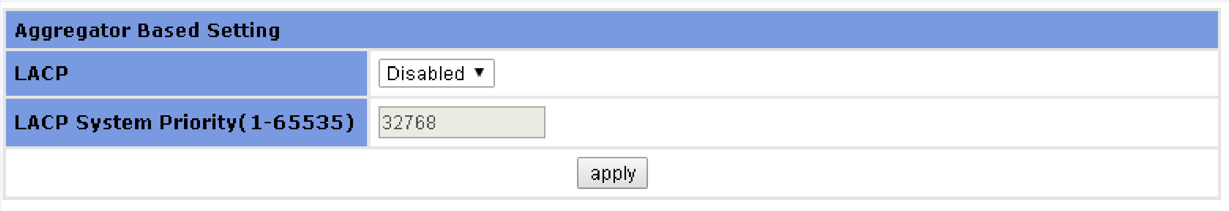
3.2.4.2 Lacp Basic

LACP determines the dynamic aggregation group members according to the priority of the port ID on the end with the preferred device ID. The device ID consists of two-byte system priority and six-byte system MAC address, that is, device ID = system priority + system MAC address.

When two device IDs are compared, the system priorities are compared first, and the system MAC addresses are compared when the system priorities are the same. The device with smaller device ID will be considered as the preferred one.

There is a limit on the number of selected ports in an aggregation group. Therefore, if the number of selected ports in an aggregation group exceeds the maximum member port number supported by the device, the system will choose the ports with lower port numbers as the member ports.

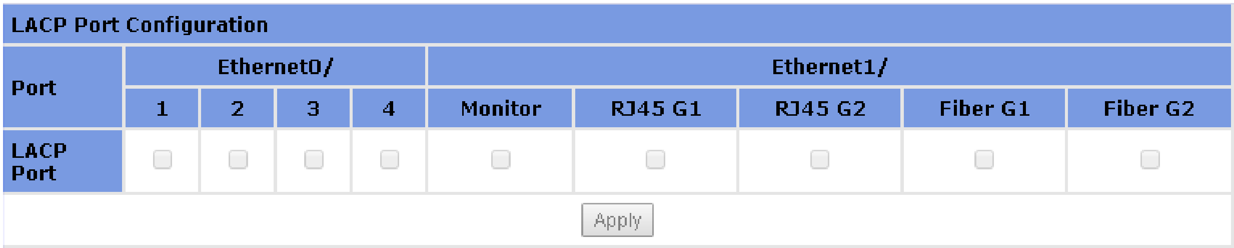
Set LACP system priority (from 1 to 65535).



Aggregator Based Setting	
LACP	Disabled ▾
LACP System Priority(1-65535)	32768
apply	

3.2.3.3 LACP Port

On this page, you can configure dynamic LACP aggregation. A dynamic LACP trunk can only be set or deleted automatically by the protocol. This protocol is based on IEEE802.3ad and uses LACPDUs (link aggregation control protocol data unit) to interact with its peer. After LACP is enabled on a port, LACP notifies the following information of the port to its peer by sending LACPDUs: priority and MAC address of this system, priority, number and operation key of the port. Upon receiving the information, the peer compares the information with the information of other ports on the peer device to determine the ports that can be aggregated. In this way, the two parties can reach an agreement in adding/removing the port to/from a dynamic aggregation group. Any port in a dynamic LACP trunk shall have this port's LACP enabled.A dynamic LACP aggregation group is automatically created and removed by the system. Users cannot add/remove ports to/from it. A port can participate in dynamic link aggregation only when it is LACP-enabled. Ports can be aggregated into a dynamic aggregation group only when they are connected to the same peer device and have the same basic configuration (such as rate and duplex mode).



LACP Port Configuration

Port	Ethernet0/				Ethernet1/				
	1	2	3	4	Monitor	RJ45 G1	RJ45 G2	Fiber G1	Fiber G2
LACP Port	□	□	□	□	□	□	□	□	□
Apply									

3.2.3.4 LACP Status

Set LACP port status as active or passive.

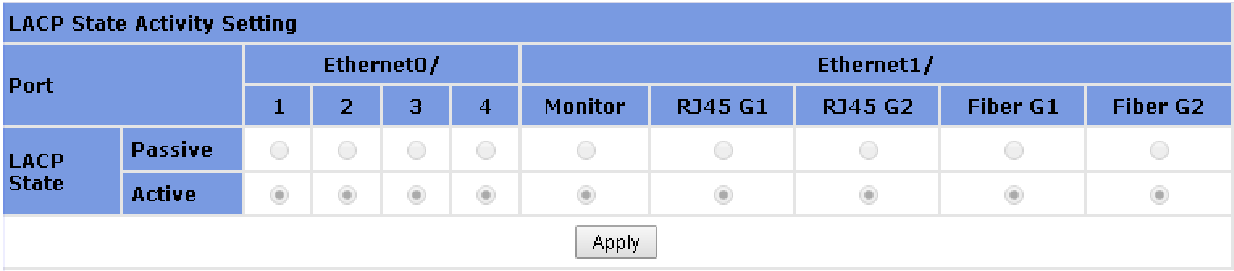
Passive The port does not automatically send LACP protocol packets; it responds only if it receives an LACP protocol packet from the peer device.

Active The port automatically sends LACP protocol packets.

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

📖 Note:

The dynamic active LACP ports on this device can aggregate with the active or passive LACP ports of the peer devices, but the passive LACP ports of this device can only aggregate with the active LACP ports of the peer devices.



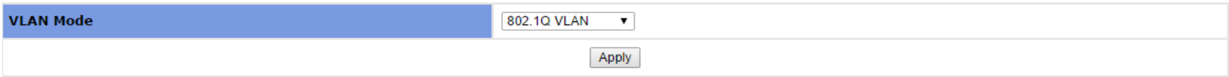
LACP State Activity Setting

Port		Ethernet0/				Ethernet1/				
		1	2	3	4	Monitor	RJ45 G1	RJ45 G2	Fiber G1	Fiber G2
LACP State	Passive	○	○	○	○	○	○	○	○	○
	Active	●	●	●	●	●	●	●	●	●

3.3 VLAN Management

3.3.1 Advanced

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



VLAN Mode: 802.1Q VLAN ▾

3.3.2 802.1Q VLAN

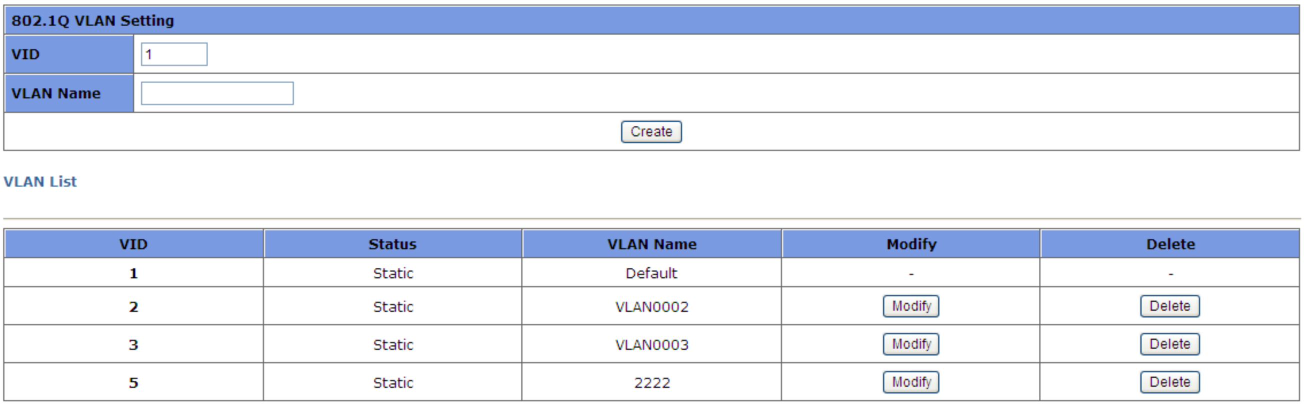
3.3.2.1 VLAN Configuration

On this tab page, you can create a new VLAN group with specific VID and VLAN group name. Up to 4K VLAN groups can be created; each VLAN group can have an ID number from 1 to 4094.

The VLAN group with VLAN identifier (VID) of 1 is a default VLAN group. Each port is a member of this group by default, and its value can be modified.

The lower part of this page lists all existing VLAN groups, as well as the information of each VLAN group. Users can also modify or delete an existing VLAN group except the default VLAN with VID 1.

⚠ Caution: It is not allowed to delete VLAN group 1.



802.1Q VLAN Setting	
VID	1
VLAN Name	
	Create

VLAN List

VID	Status	VLAN Name	Modify	Delete
1	Static	Default	-	-
2	Static	VLAN0002	Modify	Delete
3	Static	VLAN0003	Modify	Delete
5	Static	2222	Modify	Delete

3.3.2.2 Member Configuration

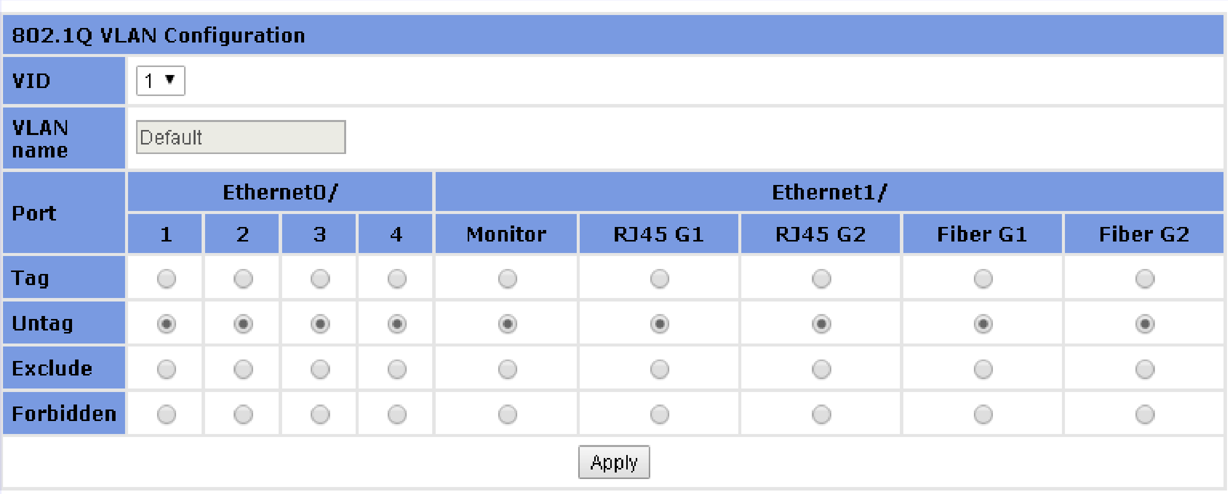
This tab page configures a VLAN group; each port can be configured as a specific state for this VLAN group:

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 GVRP.

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



802.1Q VLAN Configuration

VID: 1 ▾

VLAN name: Default

Port	Ethernet0/				Ethernet1/				
	1	2	3	4	Monitor	RJ45 G1	RJ45 G2	Fiber G1	Fiber G2
Tag	○	○	○	○	○	○	○	○	○
Untag	●	●	●	●	●	●	●	●	●
Exclude	○	○	○	○	○	○	○	○	○
Forbidden	○	○	○	○	○	○	○	○	○

3.3.2.3 Port Configration

This tab page configures 802.1Q VLAN port parameters :

Port : Specify the port to be configured.

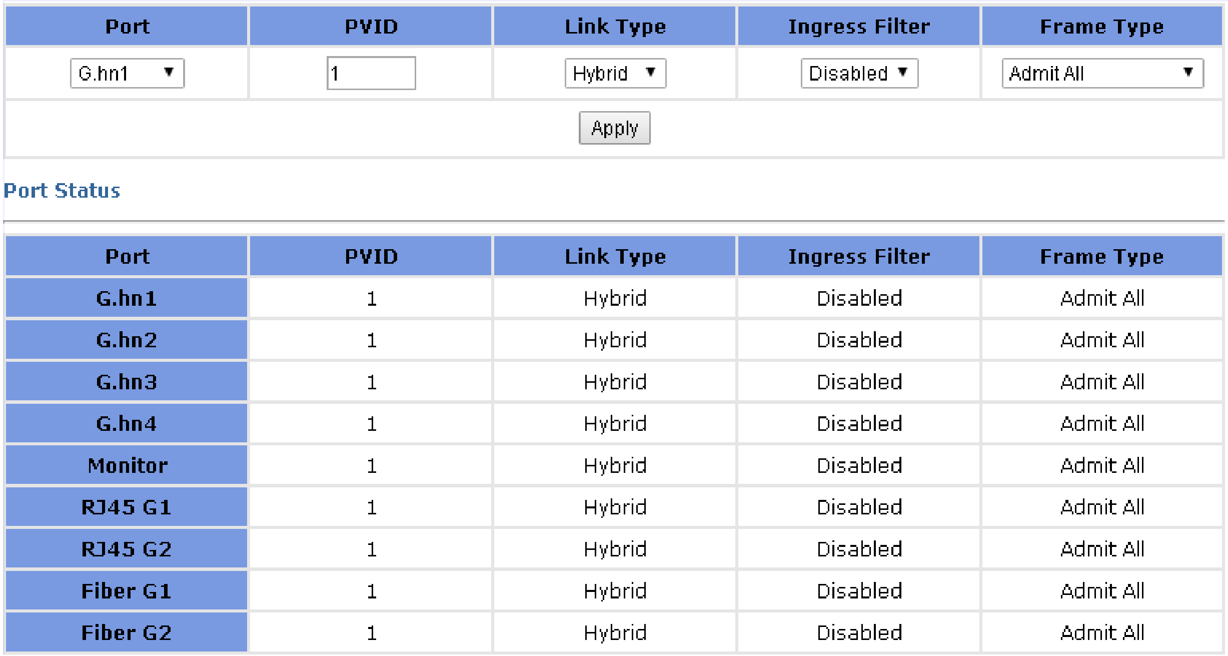
PVID: Each port can have only one Port VLAN ID (PVID), an untagged Ethernet package will be tagged a VID of PVID when arriving at the port. The default PVID is 1 for each port.

Link Type: Can choose **Hybrid** (by default), **Access** or **Trunk** from this drop-down list.

- **Access**: An access port can belong to only one VLAN, and is generally used to connect user PCs. Tag is deleted when transmitting packets.
- **Trunk**: A trunk port can belong to more than one VLAN. It can receive/send packets from/to multiple VLANs, and is generally used to connect another switch. A trunk port can belong to multiple VLANs, but it can only be configured as untagged in one VLAN. All packages are tagged, except when an egress package is in a VLAN group with VID the same as PVID.
- **Hybrid**: A hybrid port can belong to more than one VLAN. It can receive/send packets from/to multiple VLANs, and can be used to connect either a switch or user PCs. A Hybrid port is similar to a Trunk port, except it leaves the user a flexibility of configuring each port as tagged or untagged.

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 lower part of this tab page lists the status of all ports.



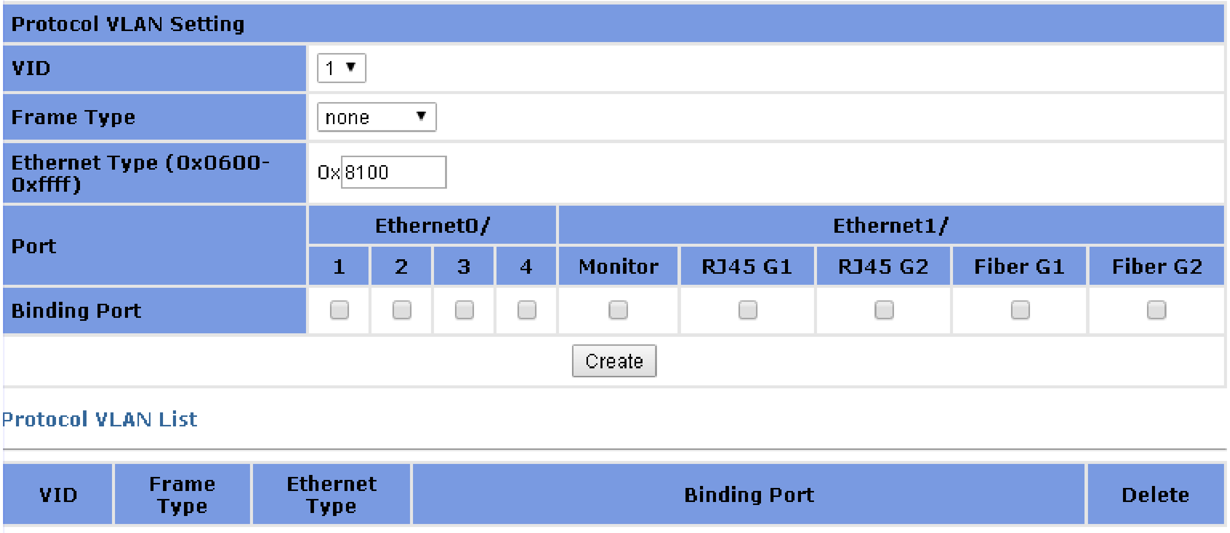
Port	PVID	Link Type	Ingress Filter	Frame Type
G.hn1 ▼	1	Hybrid ▼	Disabled ▼	Admit All ▼

Port Status

Port	PVID	Link Type	Ingress Filter	Frame Type
G.hn1	1	Hybrid	Disabled	Admit All
G.hn2	1	Hybrid	Disabled	Admit All
G.hn3	1	Hybrid	Disabled	Admit All
G.hn4	1	Hybrid	Disabled	Admit All
Monitor	1	Hybrid	Disabled	Admit All
RJ45 G1	1	Hybrid	Disabled	Admit All
RJ45 G2	1	Hybrid	Disabled	Admit All
Fiber G1	1	Hybrid	Disabled	Admit All
Fiber G2	1	Hybrid	Disabled	Admit All

3.3.3 Protocol VLAN

This page configures protocol VLAN. The pull down **VID** block lists 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**. Coressponding **Port** is selected when setting **Protocol VLAN** group.
The bottom part of this page lists all protocol VLAN groups configured.



Protocol VLAN Setting									
VID	1 ▼								
Frame Type	none ▼								
Ethernet Type (0x0600-0xffff)	0x 8100								
Port	Ethernet0/				Ethernet1/				
	1	2	3	4	Monitor	RJ45 G1	RJ45 G2	Fiber G1	Fiber G2
Binding Port	□	□	□	□	□	□	□	□	□

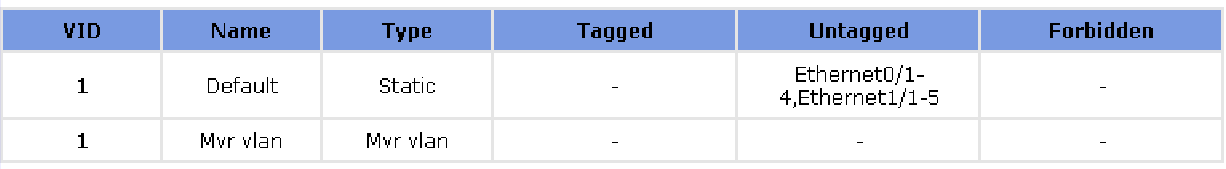
Create

Protocol VLAN List

VID	Frame Type	Ethernet Type	Binding Port	Delete

3.3.4 VLAN List

This page lists the information of all VLANs, including VID, Name, Type, Tagged ports, Untagged ports, and Forbidden ports. 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.



VID	Name	Type	Tagged	Untagged	Forbidden
1	Default	Static	-	Ethernet0/1-4,Ethernet1/1-5	-
1	Mvr vlan	Mvr vlan	-	-	-

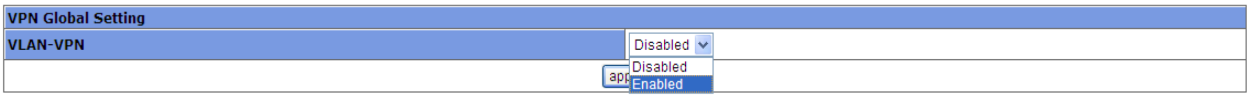
3.3.5 VLAN VPN

With the increasing application of the Internet, the VPN (Virtual Private Network) technology is developed and used to establish the private network through the operators' backbone networks. The VLAN-VPN function enables packets to be transmitted across the operators' backbone networks with VLAN tags of private networks encapsulated in those of public networks. In public networks, packets of this type are transmitted by their outer VLAN tags (that is, the VLAN tags of public networks). And those of private networks which are encapsulated in the VLAN tags of public networks are shielded.

3.3.5.1 Global Configuration

This page enables or disables global VLAN VPN.

VLAN VPN: enable or disable the global VLAN VPN.



VPN Global Setting	
VLAN-VPN	Disabled ▼

3.3.5.2 Port Configuration

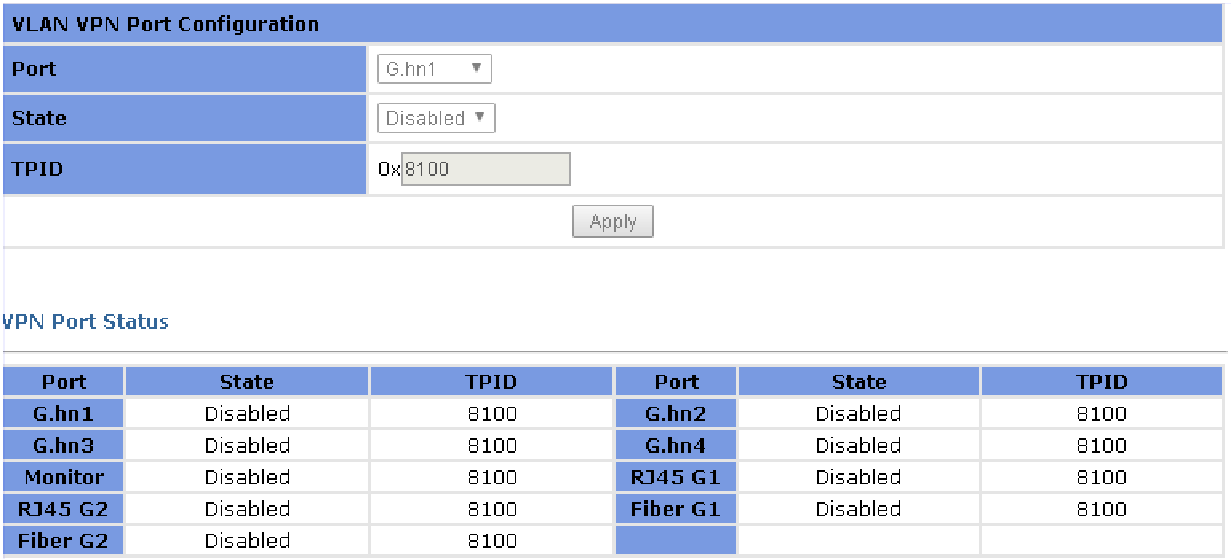
With the VLAN VPN function enabled on port, a received packet is tagged with the default VLAN tag of the receiving port no matter whether or not the packet already carries a VLAN tag. If the packet already carries a VLAN tag, the packet becomes a double-tagged packet. Otherwise, the packet becomes a packet carrying the default VLAN tag of the port.

Configuration Steps:

Step 1 Select a specific port for setting;

Step 2 Enable or disable the VLAN VPN on the port;

Step 3 Specify the TPID value for the port; it is 0x8100 by default. TPID is used to identify whether the packets carry specific VLAN Tag.



VLAN VPN Port Configuration

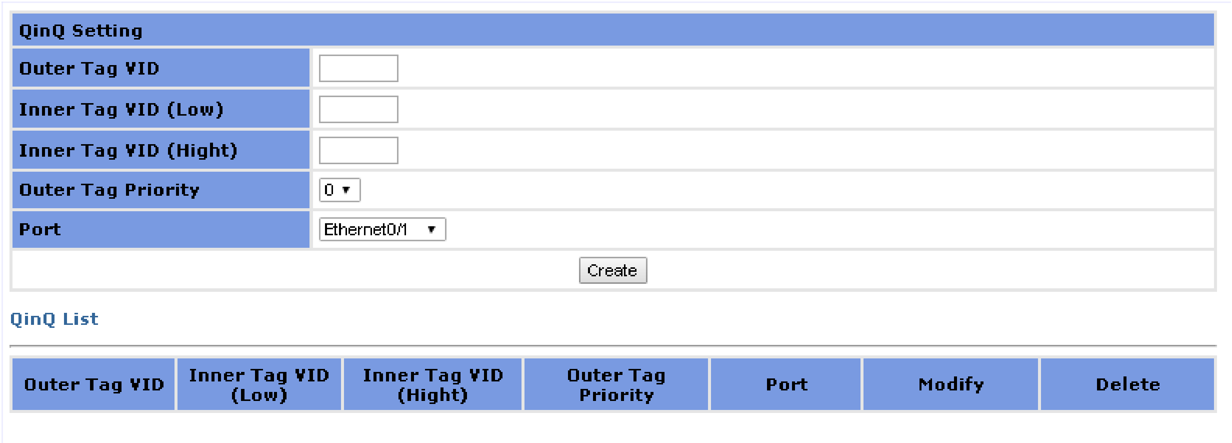
Port	G.hn1 ▼
State	Disabled ▼
TPID	0x 8100

VPN Port Status

Port	State	TPID	Port	State	TPID
G.hn1	Disabled	8100	G.hn2	Disabled	8100
G.hn3	Disabled	8100	G.hn4	Disabled	8100
Monitor	Disabled	8100	RJ45 G1	Disabled	8100
RJ45 G2	Disabled	8100	Fiber G1	Disabled	8100
Fiber G2	Disabled	8100			

3.3.5.3 QinQ configuration

On this page, you can add outer vlan through specified inner vlan.



QinQ Setting

Outer Tag VID	
Inner Tag VID (Low)	
Inner Tag VID (Hight)	
Outer Tag Priority	0 ▼
Port	Ethernet0/1 ▼

QinQ List

Outer Tag VID	Inner Tag VID (Low)	Inner Tag VID (Hight)	Outer Tag Priority	Port	Modify	Delete

Outer Tag VID: A VLAN ID for the outer tag that will be added to the packet.

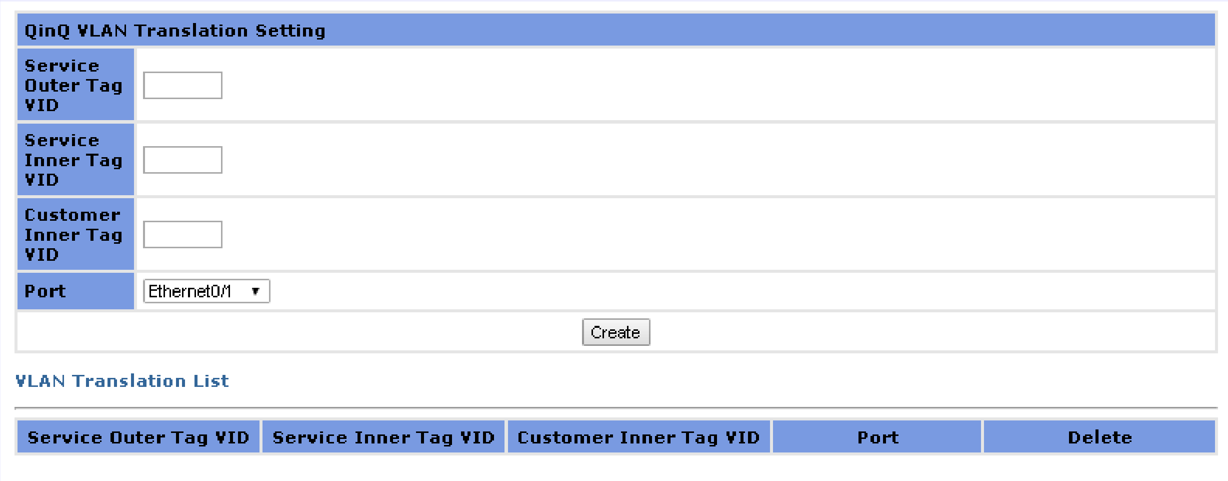
Inner tag VID (Low)/ Inner tag VID (High): An outer tag is added to form a double tag package, if the incoming package has a VLAN ID value between **Inner tag VID (Low)** and **Inner tag VID(High)** (all inclusive).

Outer Tag Priority: the outer tag VLAN priority, in the range of 0 to 7.

Port: the double tag port from which a package is received.

3.3.6 VLAN Mapping

VLAN Mapping also called VLAN translation, its main function is to replace the private network VLAN Tag users in the network of VLAN Tag, which was in accordance with the public network transmission network planning.



QinQ VLAN Translation Setting

Service Outer Tag VID	
Service Inner Tag VID	
Customer Inner Tag VID	
Port	Ethernet0/1 ▾

VLAN Translation List

Service Outer Tag VID	Service Inner Tag VID	Customer Inner Tag VID	Port	Delete

Service Outer Tag VID: Outer vid

Service Innerr Tag VID: Inner vid

Customer Inner TagVID: customer vid

Port: output port

3.4 QoS Configurations

In data communications, Quality of Service (QoS) is the ability of a network to provide differentiated service guarantees for diversified traffic in terms of bandwidth, delay, jitter, and drop rate.

On traditional IP networks, devices treat all packets equally and handle them using the first in first out (FIFO) policy. All packets share the resources of the network and devices. How many resources the packets can obtain completely depends on the time they arrive. This service is called best-effort. It delivers packets to their destinations as quickly as it can, without any guarantee for delay, jitter, packet loss ratio, reliability and so on.

The Internet has been growing along with the fast development of networking technologies. More and more users take the Internet as their data transmission platform to implement various applications. Besides traditional applications such as WWW, e-mail and FTP, network users are experiencing new services, such as tele-education, telemedicine, video telephone, video conference and Video-on-Demand (VoD). The enterprise users expect to connect their regional branches together through VPN technologies to carry out operational applications, for instance, to access the database of the company or to monitor remote devices through Telnet. These new applications have one thing in common, that is, they all have special requirements for bandwidth, delay, and jitter. For instance, videoconference and VoD need large bandwidth, low delay and jitter. As for mission-critical applications, such as transactions and Telnet, they may not require large bandwidth but do require low delay and preferential service during congestion.

3.4.1 Rate Limit

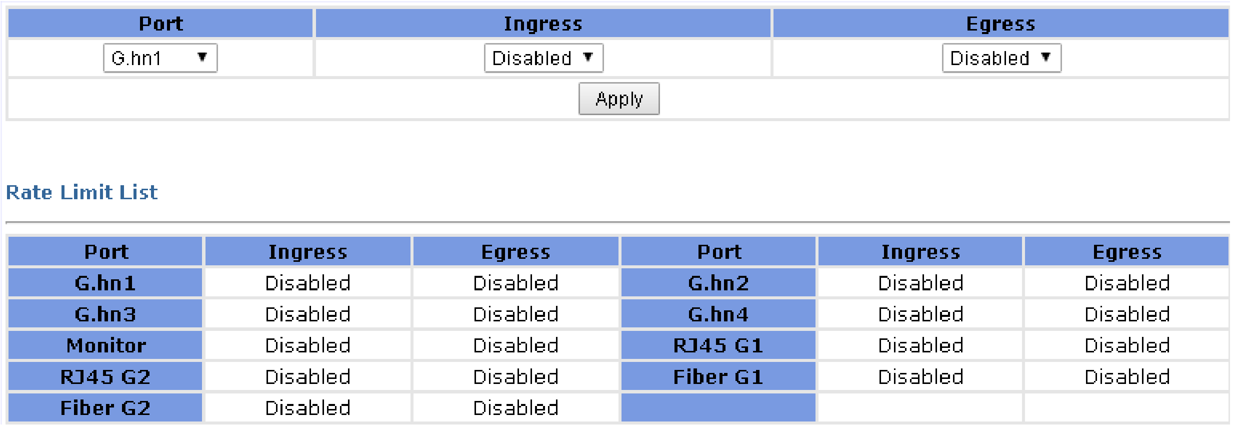
You can configure the egress traffic limit on individual ports, to keep normal network service. The bottom of the page will show the rate limit list.

Port Select the port to configure

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.

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.

When completing the configuration, click <apply> to take effect. The next page shows a full list of rate limit for each port.



Port	Ingress	Egress
G.hn1 ▼	Disabled ▼	Disabled ▼

Rate Limit List

Port	Ingress	Egress	Port	Ingress	Egress
G.hn1	Disabled	Disabled	G.hn2	Disabled	Disabled
G.hn3	Disabled	Disabled	G.hn4	Disabled	Disabled
Monitor	Disabled	Disabled	RJ45 G1	Disabled	Disabled
RJ45 G2	Disabled	Disabled	Fiber G1	Disabled	Disabled
Fiber G2	Disabled	Disabled			

⚠ Caution: Egress rate cannot be enabled on the aggregration ports.

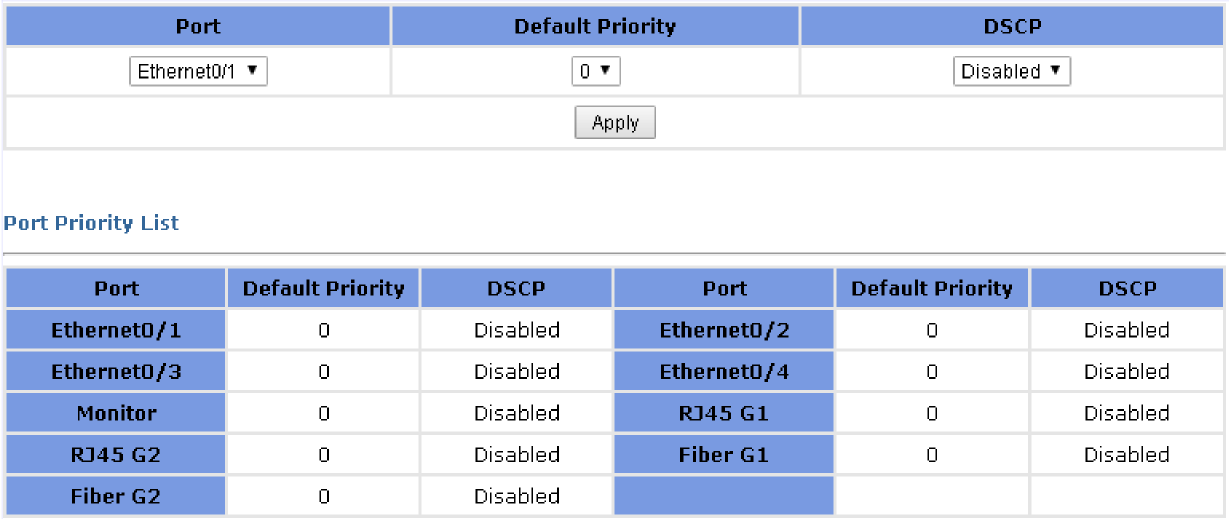
3.4.2 Port Configuration

This 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.

Default Priority There is 8 priorities from 0 to 7.

DSCP Enable or disable DSCP

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



Port	Default Priority	DSCP
Ethernet0/1 ▼	0 ▼	Disabled ▼

Port Priority List

Port	Default Priority	DSCP	Port	Default Priority	DSCP
Ethernet0/1	0	Disabled	Ethernet0/2	0	Disabled
Ethernet0/3	0	Disabled	Ethernet0/4	0	Disabled
Monitor	0	Disabled	RJ45 G1	0	Disabled
RJ45 G2	0	Disabled	Fiber G1	0	Disabled
Fiber G2	0	Disabled			

3.4.3 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)**

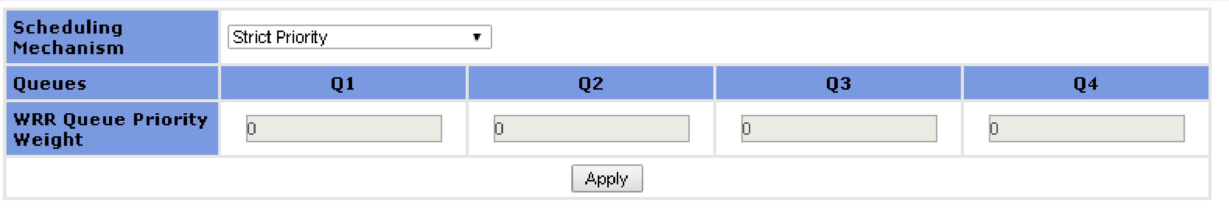
Strict Priority: SP queue-scheduling algorithm is specially designed for critical service applications. An important feature of critical services is that they demand preferential service in congestion in order to reduce the response delay. Assume that there are eight output queues on the port and the preferential queue classifies the eight output queues on the port into eight classes, which are queue 7, queue 6, queue 5, queue 4, queue 3, queue 2, queue 1, and queue 0. Their priorities decrease in order.

In queue scheduling, SP sends packets in the queue with higher priority strictly following the priority order from high to low. When the queue with higher priority is empty, packets in the queue with lower priority are sent. You can put critical service packets into the queues with higher priority and put non-critical service (such as e-mail) packets into the queues with lower priority. In this case, critical service packets are sent preferentially and non-critical service packets are sent after critical service groups are sent.

The disadvantage of SP queue is that: if there are packets in the queues with higher priority for a long time in congestion, the packets in the queues with lower priority will be “starved” because they are not served.

Weighted Round-Robin (WRR) (8:4:2:1): WRR queue-scheduling algorithm schedules all the queues in turn and every queue can be assured of a certain service time. Assume there are four priority queues on a port. WRR configures a weight value for each queue, which are Q1, Q2, Q3 and Q4. The weight value indicates the proportion of obtaining resources. On a 150 M port, configure the weight value of WRR queue-scheduling algorithm to 8, 4, 2 and 1 (corresponding to Q1, Q2, Q3 and Q4 in order). In this way, the queue with the lowest priority can get 10 Mbps bandwidth at least, and the disadvantage of SP queue-scheduling that the packets in queues with lower priority may not get service for a long time is avoided. Another advantage of WRR queue is that: though the queues are scheduled in order, the service time for each queue is not fixed; that is to say, if a queue is empty, the next queue will be scheduled. In this way, the bandwidth resources will be fully used.

Weight values for WRR: Q1~Q4 can be set from 1 to 55.



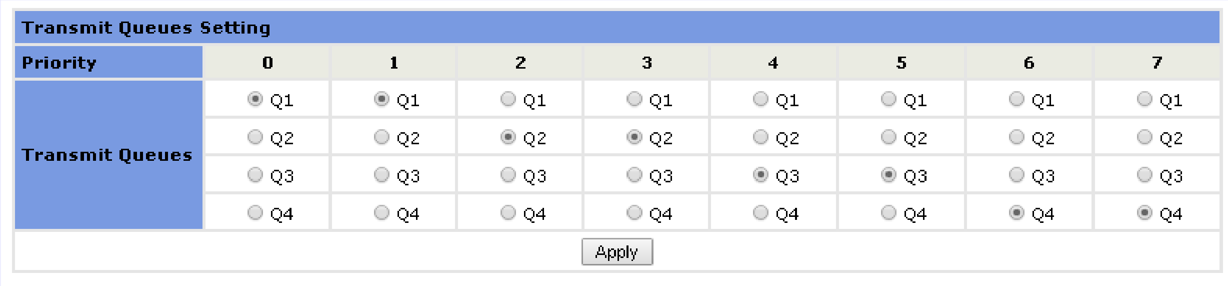
Scheduling Mechanism	Strict Priority ▾			
Queues	Q1	Q2	Q3	Q4
WRR Queue Priority Weight	0	0	0	0

3.4.4 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

You can modify the transmit queues here. Click <Apply> to make it take effect. If there is no modification for the queues, directly click <Apply>.



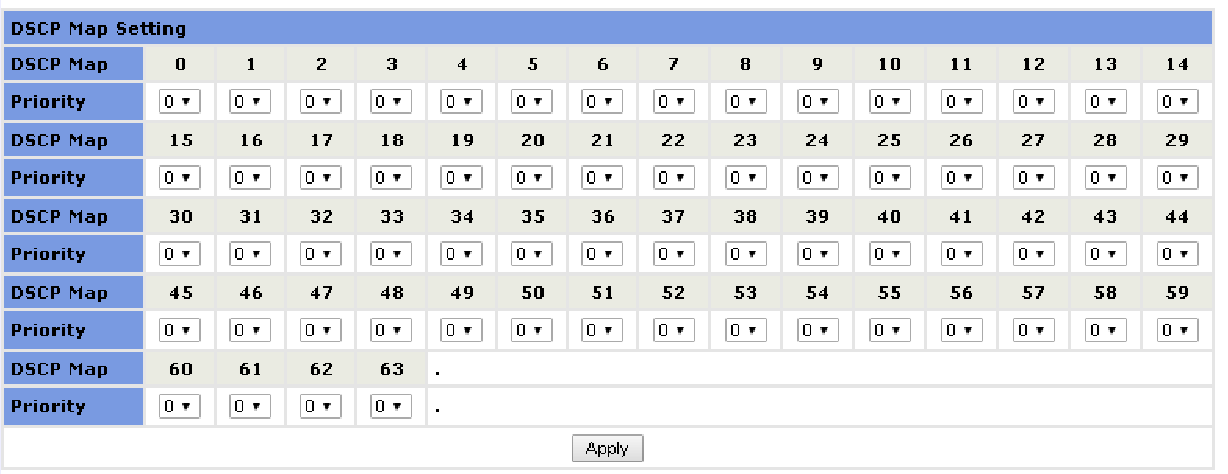
Transmit Queues Setting

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

3.4.5 DSCP map

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



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

3.5 Forwarding

The switch has unicast MAC address forwarding, multicast MAC address forwarding, IGMP Snooping, MVR , and unknown muticast. Specifications are below.

3.5.1 Unicast Control

MAC address forwarding table: the device forwards the packets to the corresponding port according to the packet destination MAC address. The MAC address forwarding table reflects the relationship between the MAC address and the forwarding port.

A MAC address table is maintained for packet forwarding. Each entry in this table indicates the following information:

- The MAC address of a connected network device
- The interface to which the device is connected
- The VLAN to which the interface belongs

Unicast MAC address configuration is for the unicast forwarding mode.

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

VID Specifies a VLAN group with which the MAC address corresponds.

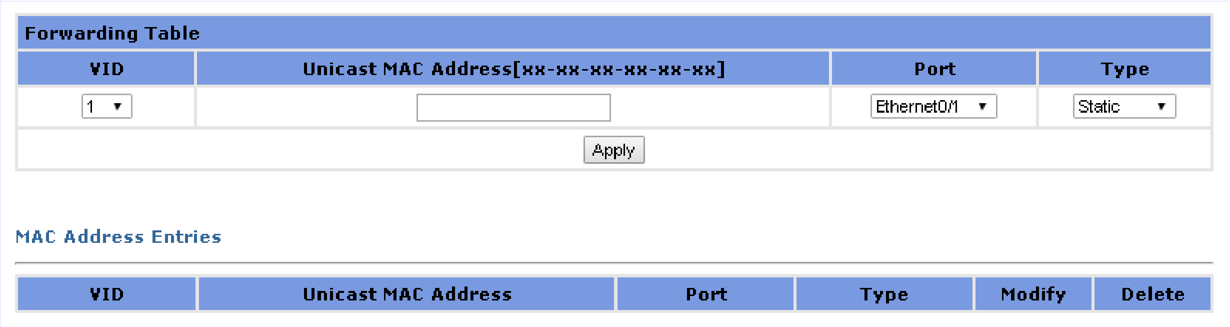
Unicast MAC Address Specifies the destination MAC address.

Port Specifies the port of the outbound interface.

Type Choose among **Dynamic, Static and Blackhole**.

- Static MAC address entry: Also known as permanent MAC address entry. These types of MAC address entries are added/removed manually and cannot age out by themselves. Using static MAC address entries can reduce broadcast packets remarkably and are suitable for networks where network devices seldom change.
- Dynamic MAC address entry: These types of MAC address entries age out after the configured aging time. They are generated by the MAC address learning mechanism or are configured manually.
- Blackhole MAC address entry: These types of MAC address entries are configured manually. A switch discards the packets destined for or originated from the MAC addresses contained in blackhole MAC address entries.

The lower part 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. Dynamic MAC addresses will also be shown on the Dynamic MAC Address page.



Forwarding Table

VID	Unicast MAC Address[xx-xx-xx-xx-xx-xx]	Port	Type
1		Ethernet0/1	Static

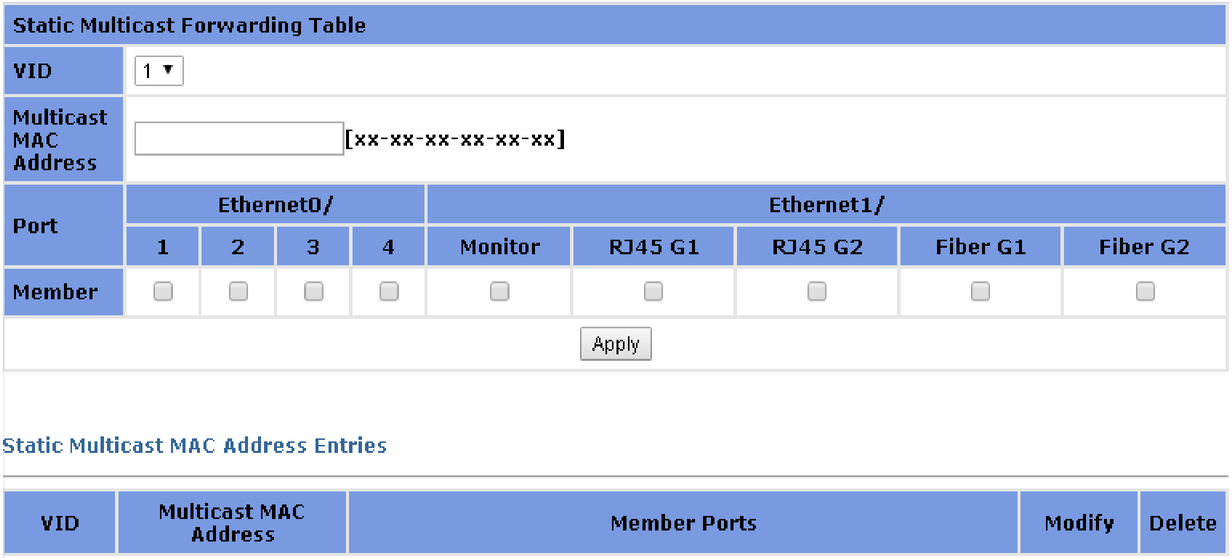
MAC Address Entries

VID	Unicast MAC Address	Port	Type	Modify	Delete

3.5.2 Multicast Control

3.5.2.1Static multicast

This page set static multicast forwarding table



Static Multicast Forwarding Table

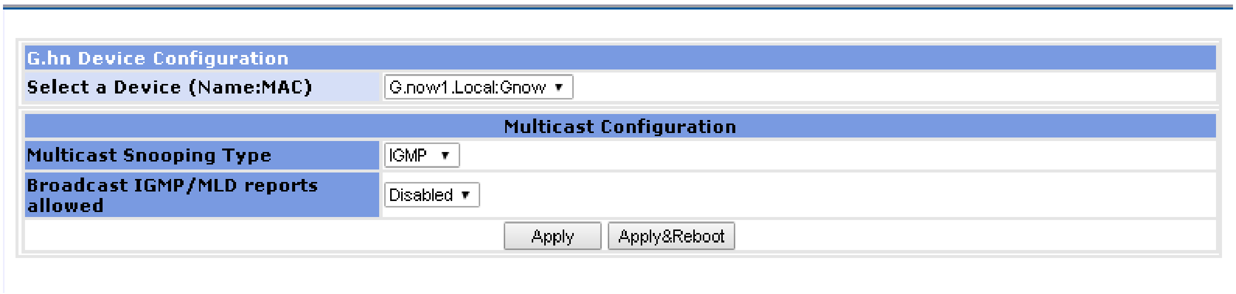
VID	1 ▾								
Multicast MAC Address	[xx-xx-xx-xx-xx-xx]								
Port	Ethernet0/				Ethernet1/				
	1	2	3	4	Monitor	RJ45 G1	RJ45 G2	Fiber G1	Fiber G2
Member	□	□	□	□	□	□	□	□	□

Apply

Static Multicast MAC Address Entries

VID	Multicast MAC Address	Member Ports	Modify	Delete

3.5.2.2 Node IGMP



G.hn Device Configuration

Select a Device (Name:MAC)	G.now1.Local:Gnow ▾

Multicast Configuration

Multicast Snooping Type	IGMP ▾
Broadcast IGMP/MLD reports allowed	Disabled ▾

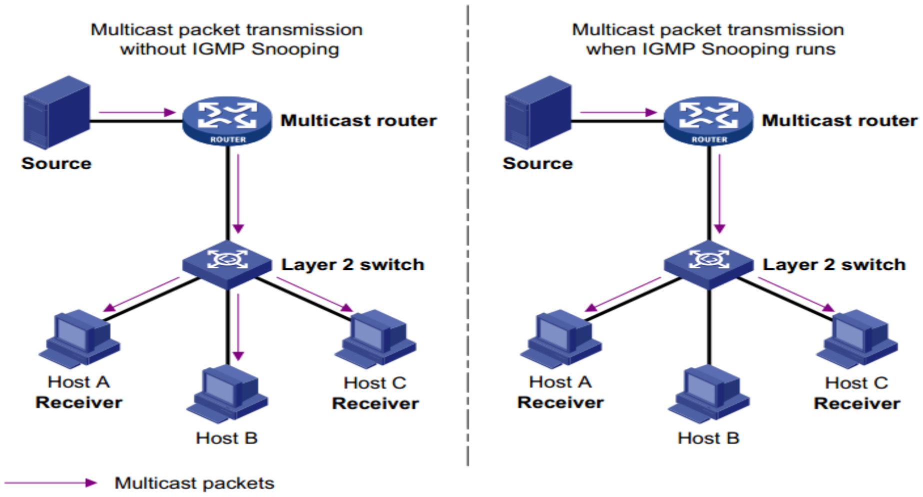
Apply Apply&Reboot

3.5.2.3 IGMP Snooping

Internet Group Management Protocol Snooping (IGMP Snooping) is a multicast constraining mechanism that runs on Layer 2 devices to manage and control multicast groups.

By listening to and analyzing IGMP messages, a Layer 2 device running IGMP Snooping establishes mappings between ports and multicast MAC addresses and forwards multicast data based on these mappings.

As shown in the following figure, when IGMP Snooping is not running on the device, multicast packets are broadcasted to all devices at Layer 2. When IGMP Snooping is running on the switch, multicast packets for known multicast groups are multicast to the receivers, rather than broadcast to all hosts, at Layer 2.



(1) Basic Configuration

This tab page sets the following IGMP Snooping Misc configuration parameters:

IGMP Snooping Globally enable/disable IGMP Snooping function

Host Timeout The switch starts for a port after the port joins a multicast group. After it times out, the port will be deleted from the group. It is in the range of 200 to 1000; by default, the value is 260 seconds.

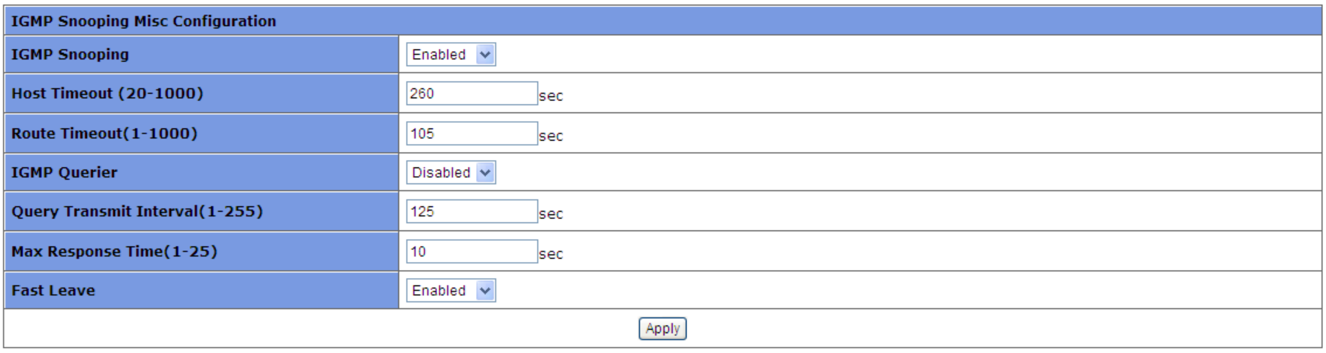
Route Timeout The switch starts Router Timeout for each router port, when it times out it will be deleted from the router port list. It is in the range of 1 to 1000; by default, the value is 105 seconds.

IGMP Querier IGMP Querier sends IGMP general query packets to all the hosts and router ports in the network segment to check the multicast group members. By default, IGMP Querier is disabled.

Query Transmit Interval The interval IGMP Querier sends IGMP general query packets to all the hosts and router ports. After it times out, it will delete the port from the group. It ranges from 1 to 255, by default, the value is 125 seconds.

Max Response Time The maximum response time of the IGMP general query packets. After it times out, it will delete the port form the group. It is in the range of 1 to 25, by default, the value is 10 seconds.

Fast Leave If Fast Leave is enabled, when a port receives a leave message from a multicast group, the switch will delete the port directly. In this way, when the port has only one user, it can save bandwidth.



IGMP Snooping Misc Configuration

IGMP Snooping	Enabled
Host Timeout (20-1000)	260 sec
Route Timeout(1-1000)	105 sec
IGMP Querier	Disabled
Query Transmit Interval(1-255)	125 sec
Max Response Time(1-25)	10 sec
Fast Leave	Enabled

(2) Detail Configuration

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

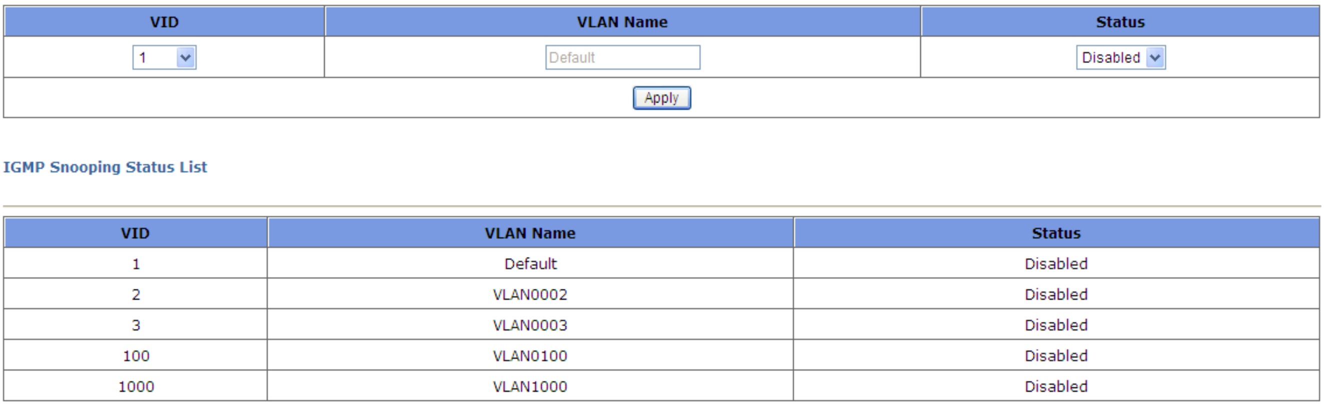
With the wide use of multicast, IGMPv3 is used more and more. It adds the multicast source filtering function, which enables the receiver to be able to specify the multicast group to join in as well as specify the multicast source to receive multicast information from.

The configuration steps are as follows:

Step 1 Specify the VLAN ID of a multicast group, the VLAN name cannot be changed here.

Step 2 Enable or disable IGMP Snooping on the field of Status, if it is enabled, select IGMP version 2 or 3. Until now, IGMP has three versions: including IGMP Version 1 (defined by RFC1112), IGMP Version 2 (defined by RFC2236), and IGMP Version 3 (defined by RFC 3376). IGMP Version 2 is compatible with IGMP Version 1.

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



VID	VLAN Name	Status
1	Default	Disabled

IGMP Snooping Status List

VID	VLAN Name	Status
1	Default	Disabled
2	VLAN0002	Disabled
3	VLAN0003	Disabled
100	VLAN0100	Disabled
1000	VLAN1000	Disabled

(3) Route Port

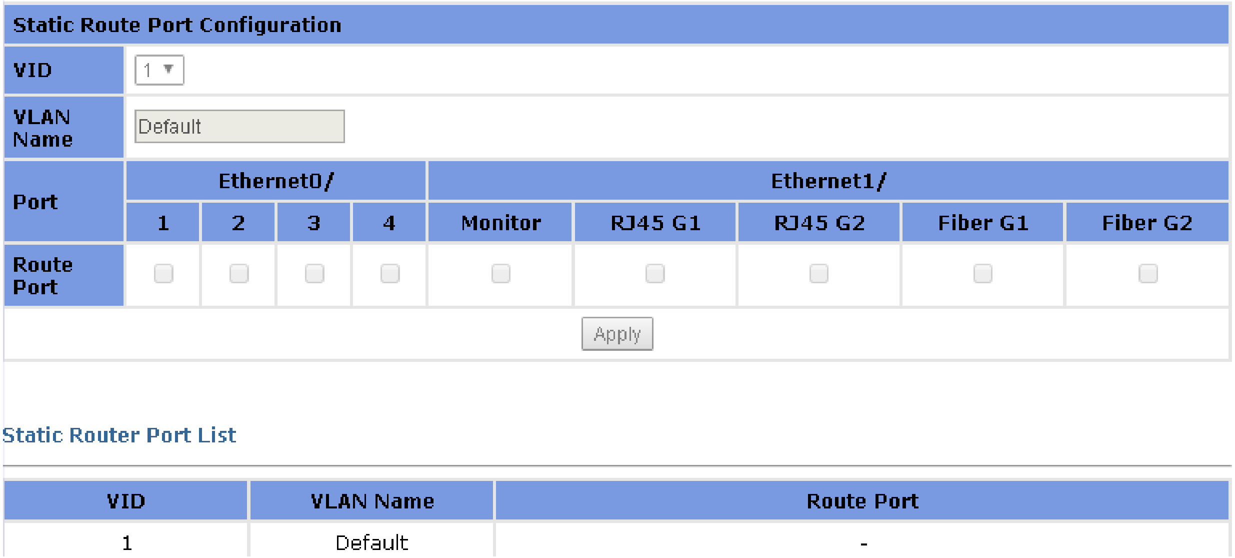
On this page, you can configure a port in a specified VLAN group as a static router port. By default, a port is not a static router port.

If a port is fixed to receive the packets from a multicast group, it can be configured to join in the multicast group statically, so that the device can receive IGMP message by the port from router.

Route port: The port directly connected to multicast devices, which is the IGMP Querier.

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

⚠Caution: the router port should be within the VLAN.



Static Route Port Configuration

VID	1 ▾								
VLAN Name	Default								
Port	Ethernet0/				Ethernet1/				
	1	2	3	4	Monitor	RJ45 G1	RJ45 G2	Fiber G1	Fiber G2
Route Port	□	□	□	□	□	□	□	□	□

Apply

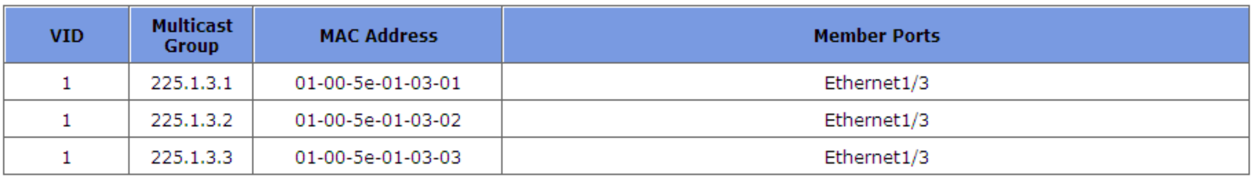
Static Router Port List

VID	VLAN Name	Route Port
1	Default	-

(4) Multicast Group

This page shows IGMP Snooping multicast group information.

VID：vlan id
Multicast Group：IP address of Multicast Group
MAC Address：MAC address of Multicast Group
Member Ports：Member Ports of Multicast Group



VID	Multicast Group	MAC Address	Member Ports
1	225.1.3.1	01-00-5e-01-03-01	Ethernet1/3
1	225.1.3.2	01-00-5e-01-03-02	Ethernet1/3
1	225.1.3.3	01-00-5e-01-03-03	Ethernet1/3

3.5.2.4 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.

（1） Basic 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.

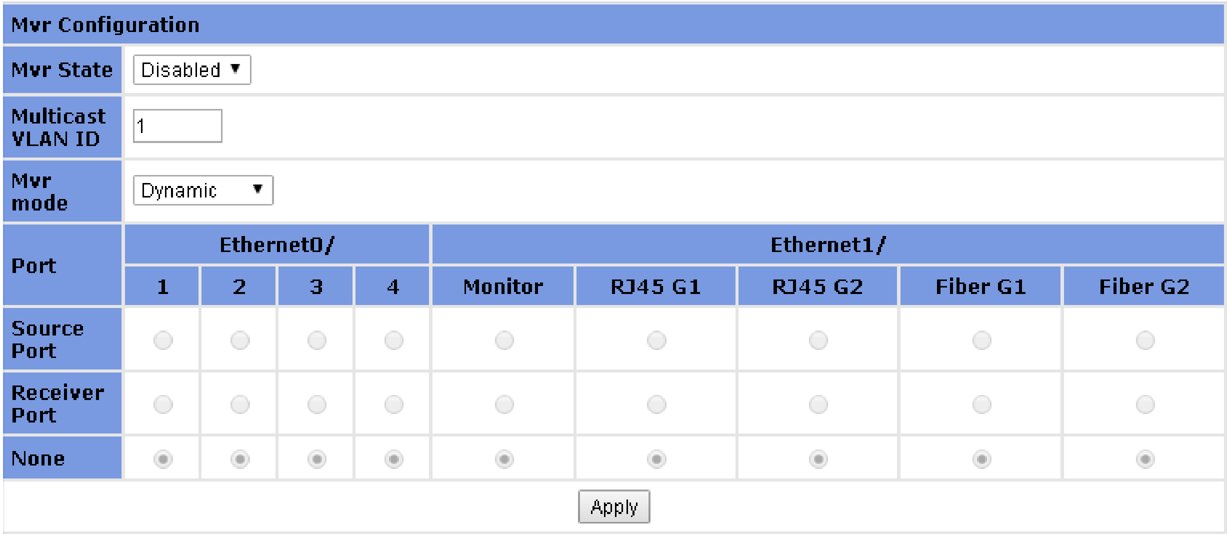
MVR Mode Choose the mode between **compatible** and **dynamic**.

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.



Mvr Configuration

Mvr State	Disabled ▼
Multicast VLAN ID	1
Mvr mode	Dynamic ▼

Port	Ethernet0/				Ethernet1/				
	1	2	3	4	Monitor	RJ45 G1	RJ45 G2	Fiber G1	Fiber G2
Source Port	○	○	○	○	○	○	○	○	○
Receiver Port	○	○	○	○	○	○	○	○	○
None	●	●	●	●	●	●	●	●	●

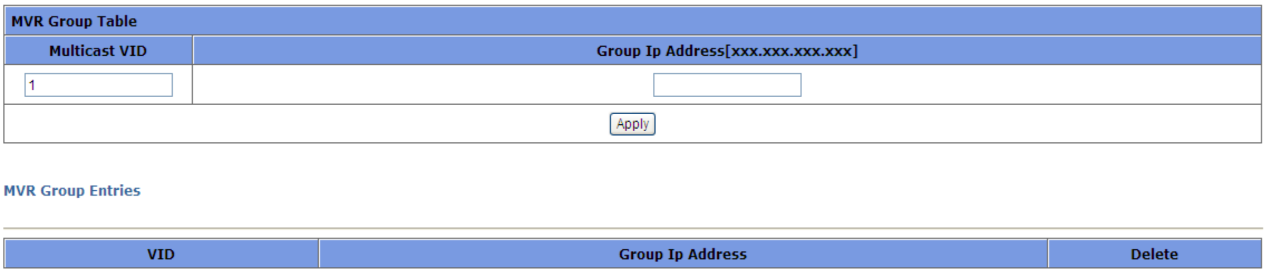
（2）Group Configuration

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



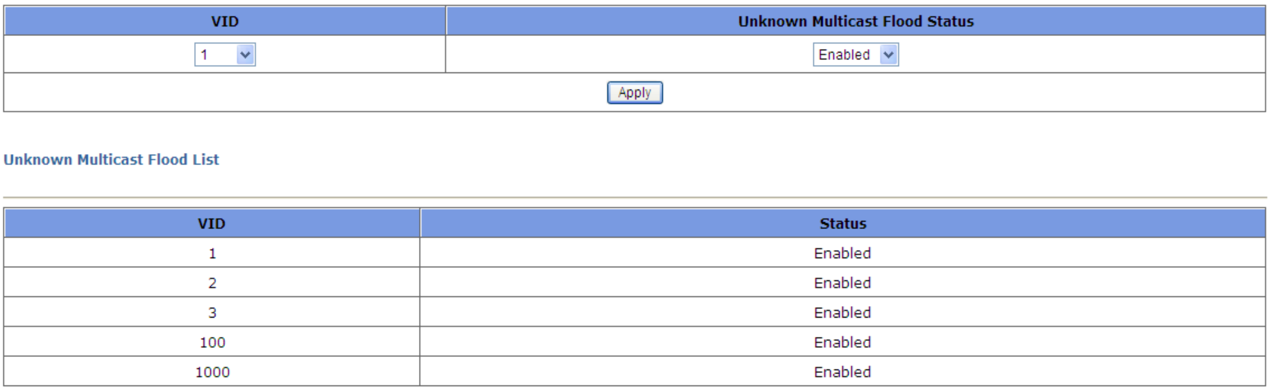
MVR Group Table

Multicast VID	Group Ip Address[xxx.xxx.xxx.xxx]
1	

MVR Group Entries

VID	Group Ip Address	Delete

3.5.2.5 Unknown Multicast



VID	Unknown Multicast Flood Status
1	Enabled

Unknown Multicast Flood List

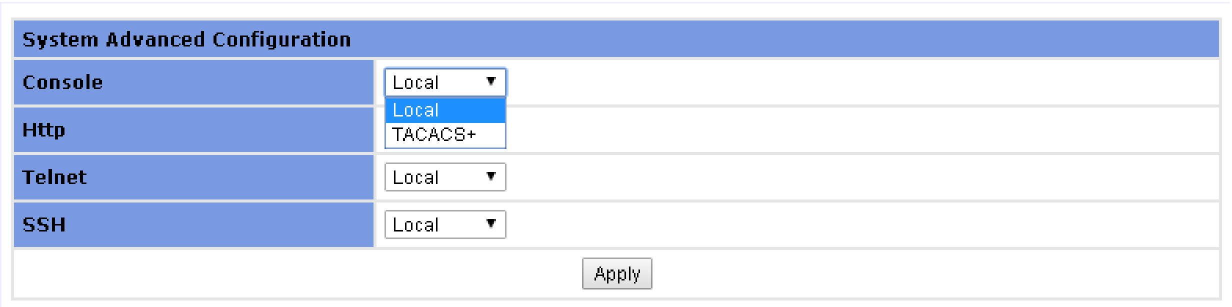
VID	Status
1	Enabled
2	Enabled
3	Enabled
100	Enabled
1000	Enabled

3.6 Security

3.6.1 Management

3.6.1.1 Login

There are four switch access methods, including via console, http, telnet and SSH. Each method has two ways: local and TACACS+. Local means you can log in with default account and password. For example, the default account is superuser, and default password is 123. TACACS+ means you can log in with account and password created on TACACS+ server.

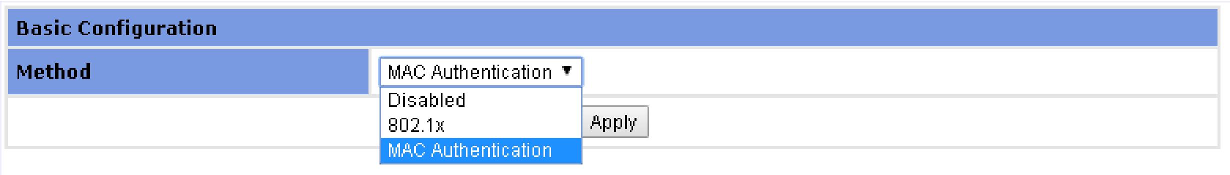


System Advanced Configuration

Console	Local
Http	
Telnet	Local
SSH	Local

3.6.1.2 Method

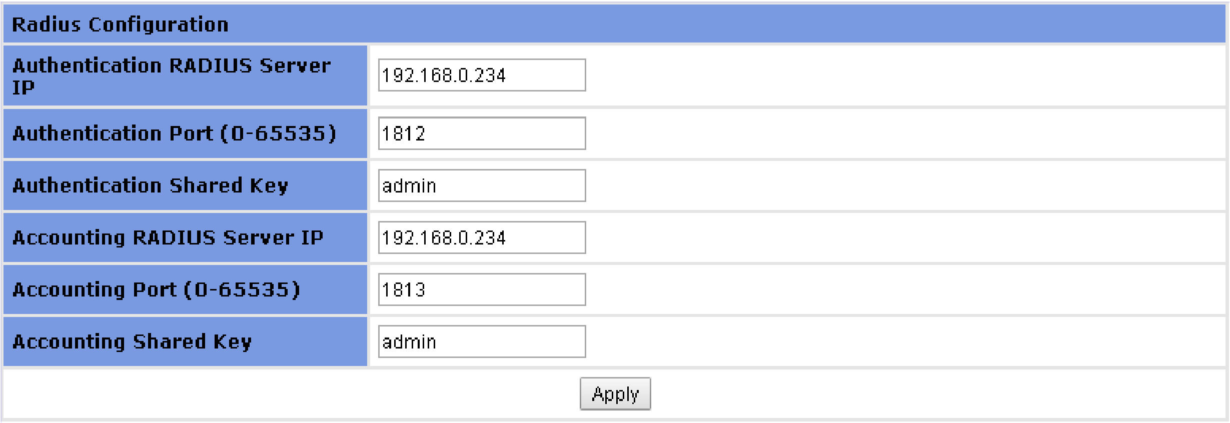
The page sets users authentication method



Basic Configuration	
Method	MAC Authentication ▼

3.6.1.3 Radius

This page configures Radius configuration



Radius Configuration	
Authentication RADIUS Server IP	192.168.0.234
Authentication Port (0-65535)	1812
Authentication Shared Key	admin
Accounting RADIUS Server IP	192.168.0.234
Accounting Port (0-65535)	1813
Accounting Shared Key	admin

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.

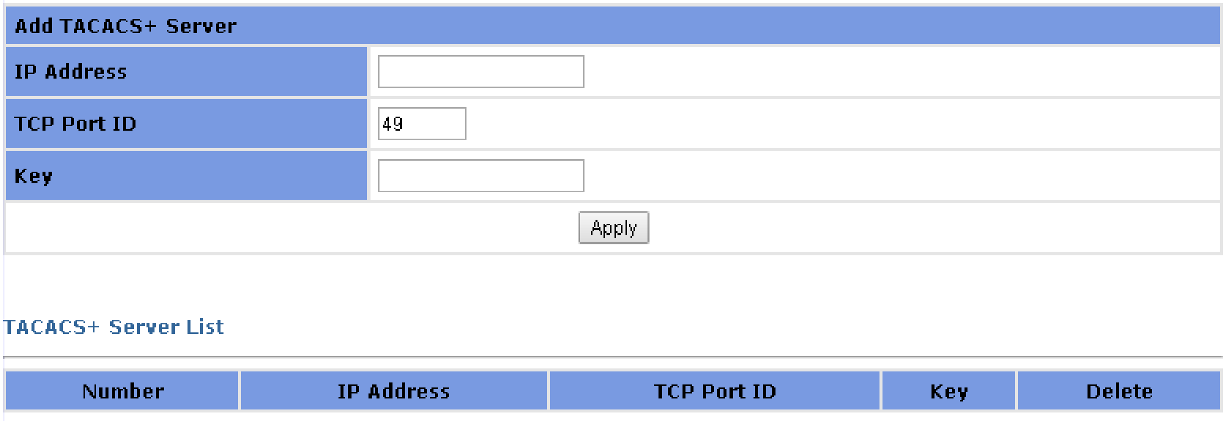
Accounting RADIUS Server IP IP address of accounting radius server to be used, a valid unicast address in dotted decimal notation; the default value is 192.168.0.234.

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.

3.6.1.4 TACACS+

This page configures TACACS+ configuration



Add TACACS+ Server	
IP Address	
TCP Port ID	49
Key	
Apply	

TACACS+ Server List

Number	IP Address	TCP Port ID	Key	Delete

IP Address Configure TACACS+ server IP address.

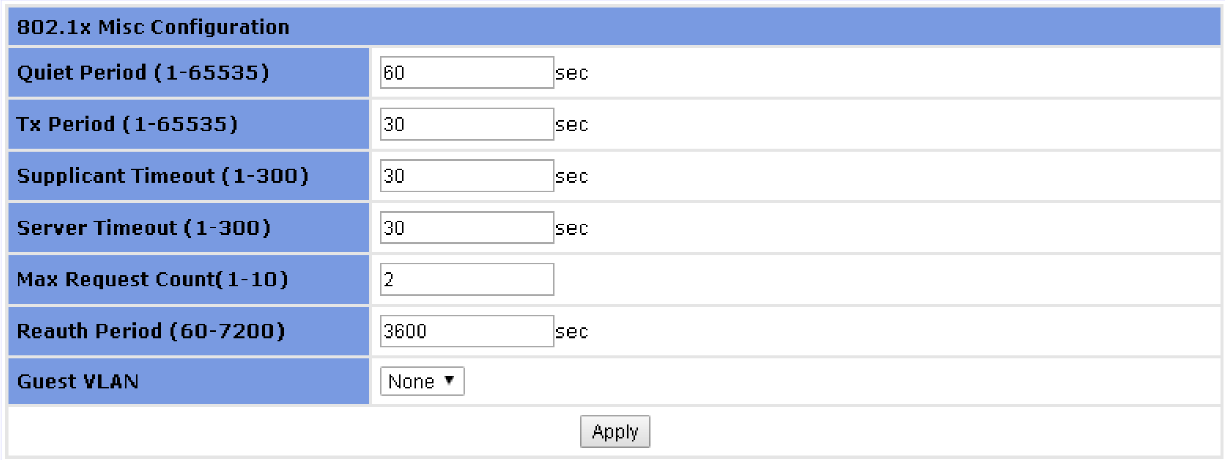
TCP Port No. Configure TCP transmission port number, range is 0~65535，default value is 49. Generally, default configuration is OK.

Encryption Key Configure the same key as TACACS+ server.

3.6.2 Port Authentication

3.6.2.1 Basic Configuration

IEEE 802.1x authentication system uses extensible authentication protocol (EAP) to exchange information between supplicant systems and the authentication servers. When a supplicant system passes the authentication, the authentication server passes the information about the supplicant system to the authenticator system. The authenticator system in turn determines the state (authorized or unauthorized) of the controlled port according to the instructions (accept or reject) received from the RADIUS server.



802.1x Misc Configuration	
Quiet Period (1-65535)	60 sec
Tx Period (1-65535)	30 sec
Supplicant Timeout (1-300)	30 sec
Server Timeout (1-300)	30 sec
Max Request Count(1-10)	2
Reauth Period (60-7200)	3600 sec
Guest VLAN	None ▼
Apply	

In 802.1 x authentication, the following timers are used to ensure that the supplicant system, the switch, and the RADIUS server interact in an orderly way.

Quiet Period Set 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 Set 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: Set 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 Set 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 Set 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.

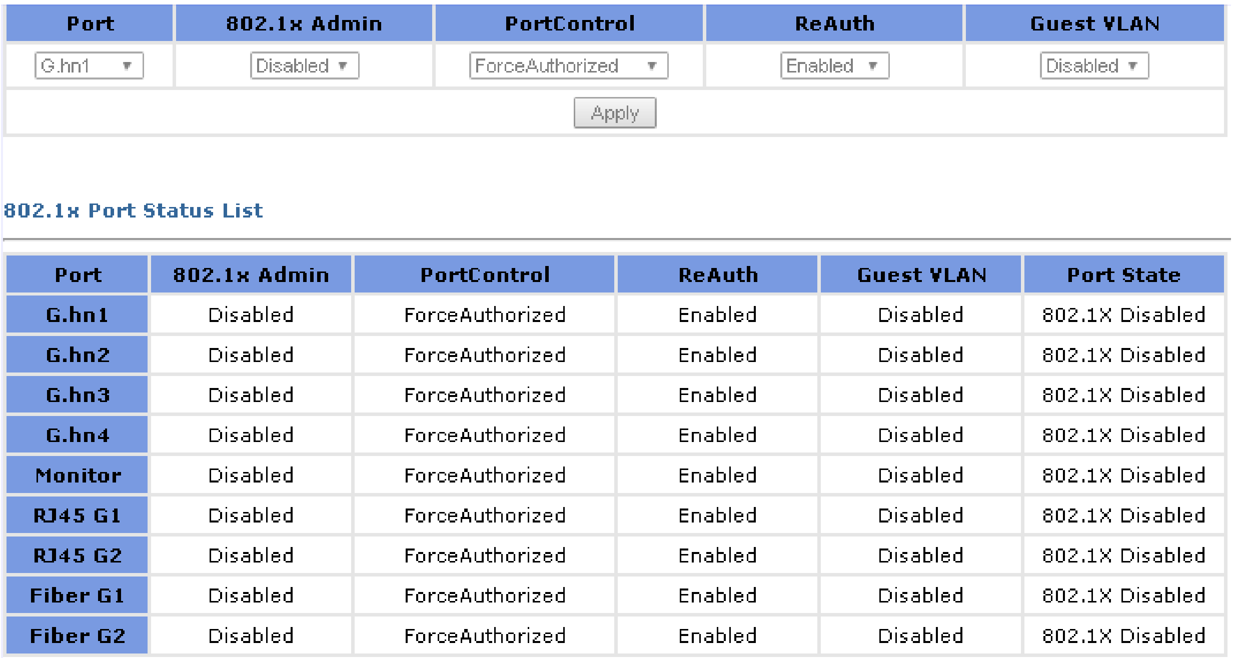
Reauth Period Set re-authentication interval in second. After this timer expires, the switch indicates: 802.1x re-authentication. It is in the range of 60 to 7200; the default value is 60 seconds.

Guest VLAN Can choose a guest VLAN on the switch to provide limited services to clients, such as downloading. By default, there is none guest VLAN.

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.

3.6.2.2 802.1x Port-based

This tab page sets 802.1x port enabling, port control, re-authentication and Guest VLAN for a specified Ethernet port.



Port	802.1x Admin	PortControl	ReAuth	Guest VLAN
G.hn1 ▾	Disabled ▾	ForceAuthorized ▾	Enabled ▾	Disabled ▾

802.1x Port Status List

Port	802.1x Admin	PortControl	ReAuth	Guest VLAN	Port State
G.hn1	Disabled	ForceAuthorized	Enabled	Disabled	802.1X Disabled
G.hn2	Disabled	ForceAuthorized	Enabled	Disabled	802.1X Disabled
G.hn3	Disabled	ForceAuthorized	Enabled	Disabled	802.1X Disabled
G.hn4	Disabled	ForceAuthorized	Enabled	Disabled	802.1X Disabled
Monitor	Disabled	ForceAuthorized	Enabled	Disabled	802.1X Disabled
RJ45 G1	Disabled	ForceAuthorized	Enabled	Disabled	802.1X Disabled
RJ45 G2	Disabled	ForceAuthorized	Enabled	Disabled	802.1X Disabled
Fiber G1	Disabled	ForceAuthorized	Enabled	Disabled	802.1X Disabled
Fiber G2	Disabled	ForceAuthorized	Enabled	Disabled	802.1X Disabled

There are three choices for **Port Control**: **Auto**, **Force Authorized** and **Force Unauthorized**.

Configuration Steps:

Step 1 Specify the port to configure

⚠ Caution: The port to configure authentication cannot be link-aggregation port.

Step 2 Enable or disable the 802.1x authentication function

Step 3 If 802.1x is enabled, you can further configure port control, re-authentication and Guest VLAN;

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.

Step 4 Enable or disable Re-authentication

Step 5 Enable or disable Guest VLAN

The Guest VLAN function enables supplicant systems that that are not authenticated to access network resources in a restrained way. It enables supplicant systems that do not have 802.1x client installed to access specific network resources. It also enables supplicant systems that are not authenticated to upgrade their 802.1x client programs.

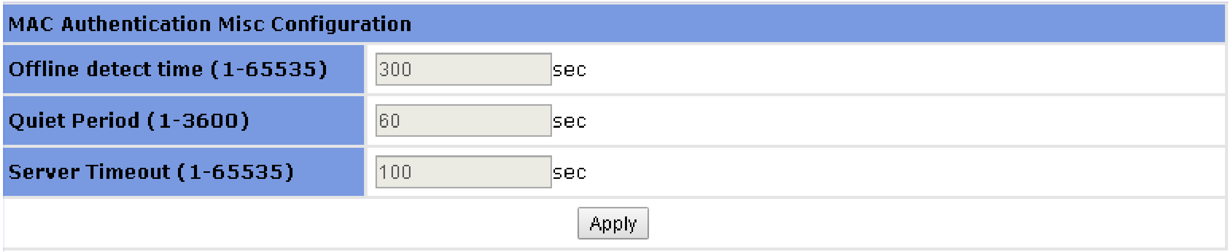
With this function enabled:

- After the maximum number retries have been made and there are still ports that have not sent any response back, the switch will then add these ports to the Guest VLAN.
- Users belonging to the Guest VLAN can access the resources of the Guest VLAN without being authenticated. But they need to be authenticated when accessing external resources.

3.6.3 MAC Authentication

MAC address authentication is port- and MAC address-based authentication used to control user permissions to access a network. MAC address authentication can be performed without client-side software. With this type of authentication employed, a switch authenticates a user upon detecting the MAC address of the user for the first time.

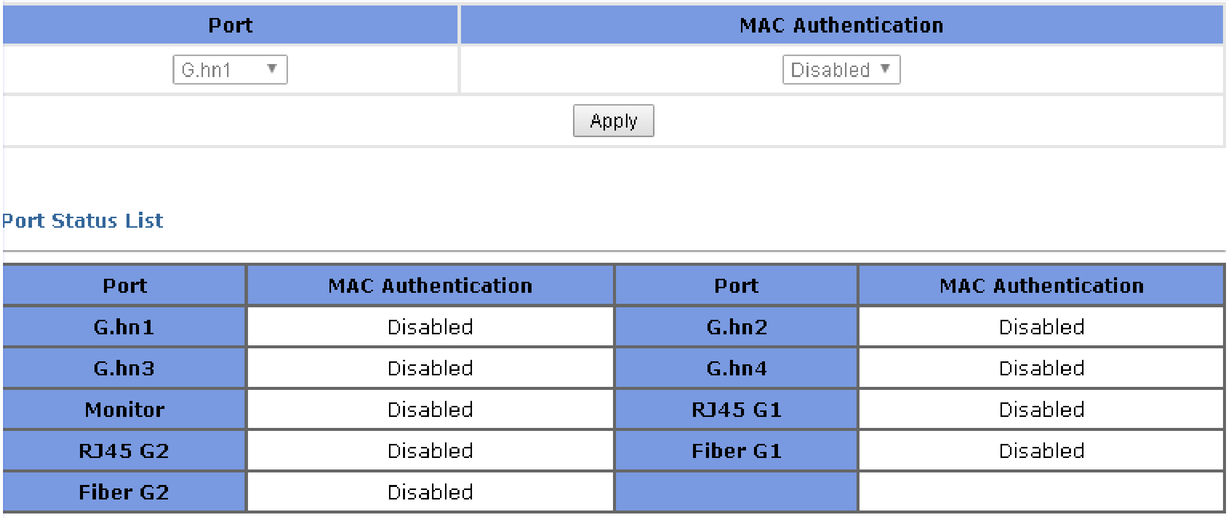
3.6.3.1 Basic Configuration



MAC Authentication Misc Configuration	
Offline detect time (1-65535)	300 sec
Quiet Period (1-3600)	60 sec
Server Timeout (1-65535)	100 sec

3.6.3.2 Port Configuration

This page enables **MAC Authentication** on a specific port. The lower part shows the port status list.



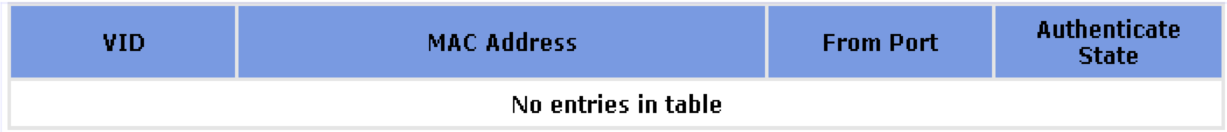
Port	MAC Authentication
G.hn1 ▼	Disabled ▼

Port Status List

Port	MAC Authentication	Port	MAC Authentication
G.hn1	Disabled	G.hn2	Disabled
G.hn3	Disabled	G.hn4	Disabled
Monitor	Disabled	RJ45 G1	Disabled
RJ45 G2	Disabled	Fiber G1	Disabled
Fiber G2	Disabled		

3.6.3.3 Authentication Infor

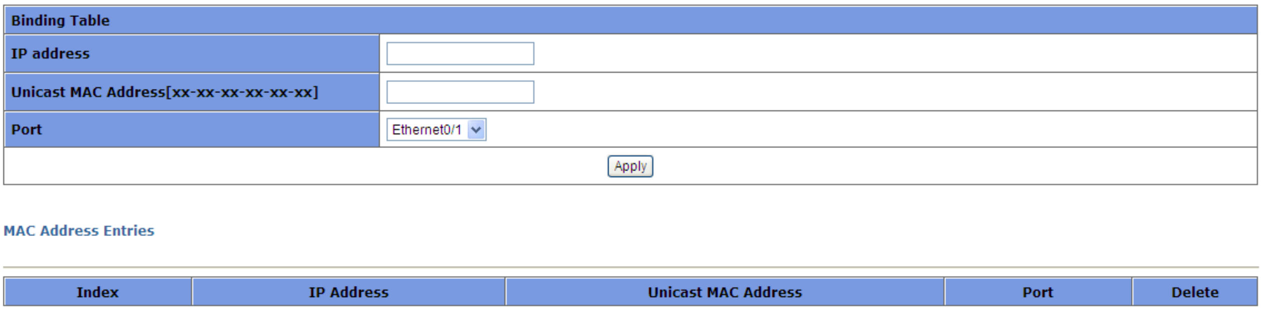
This page lists all the MAC authentication information including MAC Address, From Port, and Authenticate state.



VID	MAC Address	From Port	Authenticate State
No entries in table			

3.6.4 IP Binding

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



Binding Table	
IP address	
Unicast MAC Address[xx-xx-xx-xx-xx-xx]	
Port	Ethernet0/1 ▼

MAC Address Entries

Index	IP Address	Unicast MAC Address	Port	Delete

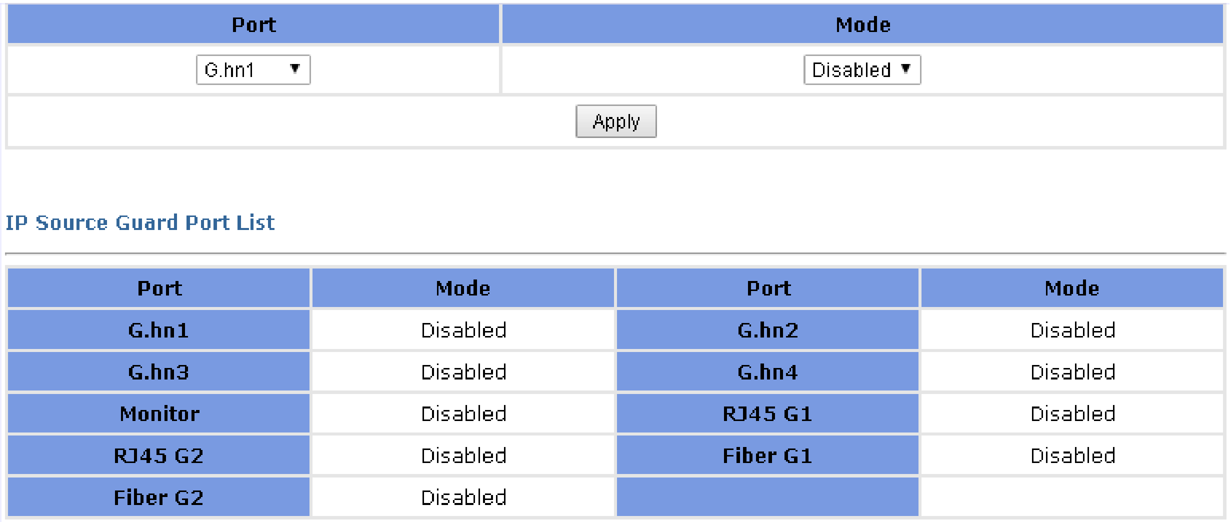
3.6.5 IP Source Guard

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.

3.6.5.1 Port Configuration

On this page, you can enable or disable the IP Source Guard function on a specified port. It also shows the IP Source Guard Port List at the lower of the page.



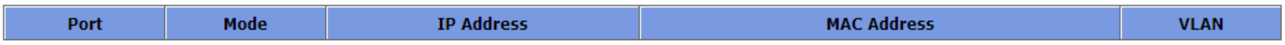
Port	Mode
G.hn1 ▼	Disabled ▼

IP Source Guard Port List

Port	Mode	Port	Mode
G.hn1	Disabled	G.hn2	Disabled
G.hn3	Disabled	G.hn4	Disabled
Monitor	Disabled	RJ45 G1	Disabled
RJ45 G2	Disabled	Fiber G1	Disabled
Fiber G2	Disabled		

3.6.5.2 Status Information

It shows the IP Source Guard status, shown as follows, including the port number, mode, IP address, MAC address and VLAN. Such as in the following screen, it represents that the IP source guard is dynamically set on the port Ethernet 0/1, and only the packets from the device with the IP address of 192.168.104.250, the MAC address of 6c-f0-49-82-be-cf and the VLAN of 1, can pass the port Ethernet 0/1.



Port	Mode	IP Address	MAC Address	VLAN

3.6.6 DHCP Snooping

With networks getting larger in size and more complicated in structure, lack of available IP addresses becomes the common situation the network administrators have to face, and network configuration becomes a tough task for the network administrators. With the emerging of wireless networks and the use of laptops, the position change of hosts and frequent change of IP addresses also require new technology. Dynamic host configuration protocol (DHCP) is developed to solve these issues.

DHCP adopts a client/server model, where the DHCP clients send requests to DHCP servers for configuration parameters; and the DHCP servers return the corresponding configuration information such as IP addresses to implement dynamic allocation of network resources.

Currently, DHCP provides the following three IP address assignment policies to meet the requirements of different clients:

Manual assignment The administrator configures static IP-to-MAC bindings for some special clients, such as a WWW server. Then the DHCP server assigns these fixed IP addresses to the clients.

Automatic assignment The DHCP server assigns IP addresses to DHCP clients. The DHCP clients will occupy the IP addresses permanently.

Dynamic assignment The DHCP server assigns IP addresses to DHCP clients for a predetermined period of time. In this case, a DHCP client must apply for an IP address again at the expiration of the period. This policy applies to most clients.

After a DHCP server dynamically assigns an IP address to a DHCP client, the IP address keeps valid only within a specified lease time and will be reclaimed by the DHCP server when the lease expires. If the DHCP client wants to use the IP address for a longer time, it must update the IP lease.

By default, a DHCP client updates its IP address lease automatically by unicasting a DHCP-REQUEST packet to the DHCP server when half of the lease time elapses. The DHCP server responds with a DHCP-ACK packet to notify the DHCP client of a new IP lease if the server can assign the same IP address to the client. Otherwise, the DHCP server responds with a DHCP-NAK packet to notify the DHCP client that the IP address will be reclaimed when the lease time expires.

For the sake of security, the IP addresses used by online DHCP clients need to be tracked for the administrator to verify the corresponding relationship between the IP addresses the DHCP clients obtained from DHCP servers and the MAC addresses of the DHCP clients.

3.6.6.1 Basic Configuration

Option 82 is the relay agent information option in the DHCP message. It records the location information of the DHCP client. When a DHCP relay agent (or a device enabled with DHCP snooping) receives a client’s request, it adds the Option 82 to the request message and sends it to the server. The administrator can locate the DHCP client to further implement security control and accounting. The Option 82 supporting server can also use such information to define individual assignment policies of IP addresses and other parameters for the clients.

Option 82 involves at most 255 sub-options. If Option 82 is defined, at least one sub-option must be defined. Currently the DHCP relay agent supports only one sub-option: remote ID sub-option.

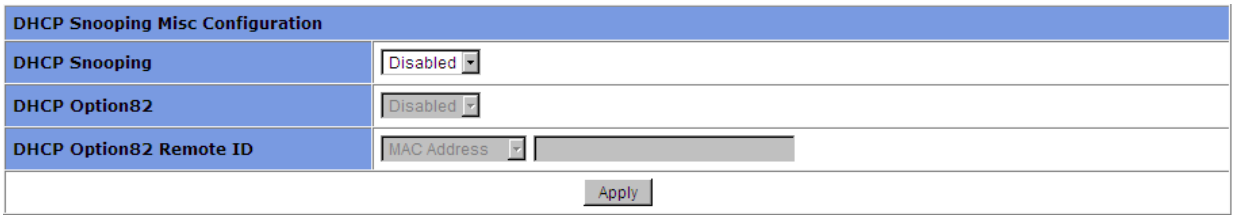
There is no specification for what should be padded in Option 82. Manufacturers can pad it as required. By default, the sub-options of Option 82 for IPC-1840 Switches (enabled with DHCP snooping) are padded as follows:

Remote ID sub-option is padded with the MAC address, system name or other (a string of 1 to 63 ASCII characters) of the DHCP snooping device that received the client’s request.

With DHCP snooping and DHCP-snooping Option 82 support enabled, when the DHCP snooping device receives a DHCP client’s request containing Option 82, it will handle the packet according to the handling policy and the configured contents in sub-options. For details, see the following table.

Handling strategy	The DHCP Snooping device will…

Replace	If no sub-option is configured, forward the packet after replacing the original Option 82 with the default content. If remote ID sub-option is configured, forward the packet after replacing the remote ID sub-option of the original Option 82 with the configured remote ID sub-option in ASCII format.
Drop	Drop the packet.
Keep	Forward the packet without changing Option 82.



DHCP Snooping Misc Configuration	
DHCP Snooping	Disabled
DHCP Option82	Disabled
DHCP Option82 Remote ID	MAC Address

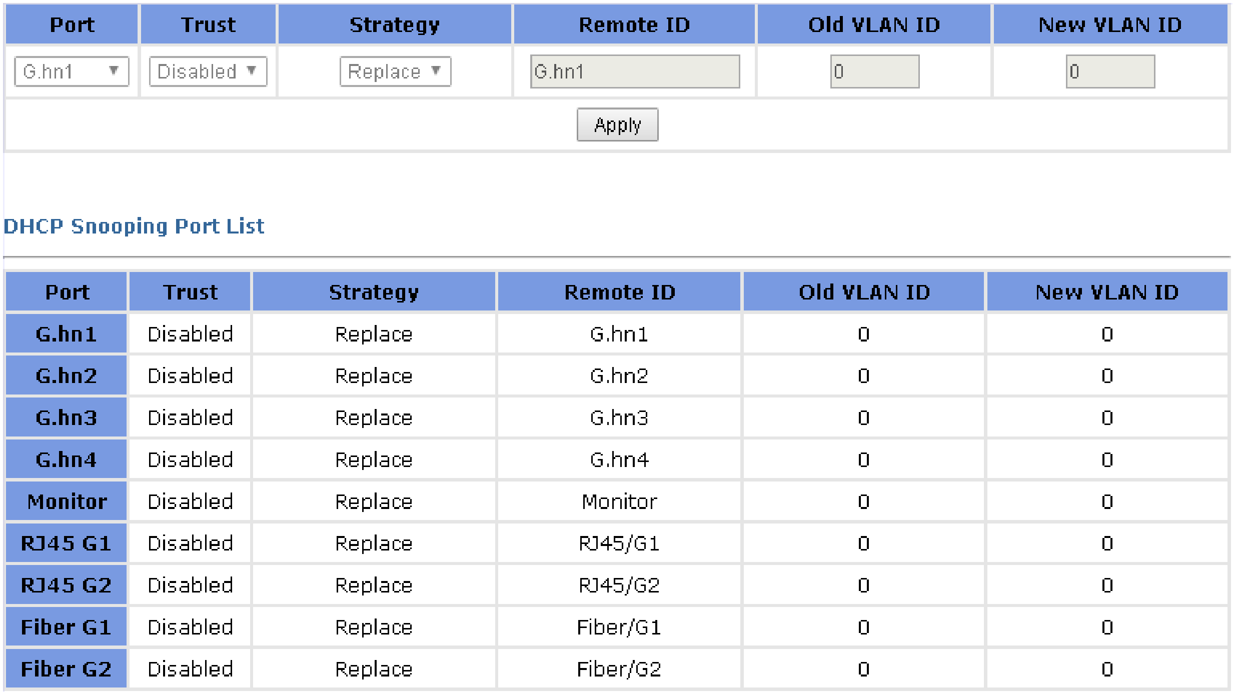
3.7.6.2 Port Configuration

When an unauthorized DHCP server exists in the network, a DHCP client may obtains an illegal IP address. To ensure that the DHCP clients obtain IP addresses from valid DHCP servers, The IPC-1840 switches can specify a port to be a trusted port or an untrusted port by the DHCP snooping function.

Trusted A trusted port is connected to an authorized DHCP server directly or indirectly. It forwards DHCP messages to guarantee that DHCP clients can obtain valid IP addresses.

Untrusted An untrusted port is connected to an unauthorized DHCP server. The DHCP-ACK or DHCP-OFFER packets received from the port are discarded, preventing DHCP clients from receiving invalid IP addresses.

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



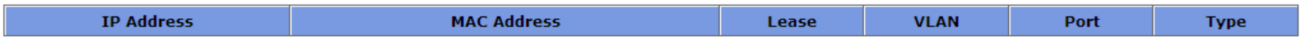
Port	Trust	Strategy	Remote ID	Old VLAN ID	New VLAN ID
G.hn1 ▾	Disabled ▾	Replace ▾	G.hn1	0	0

DHCP Snooping Port List

Port	Trust	Strategy	Remote ID	Old VLAN ID	New VLAN ID
G.hn1	Disabled	Replace	G.hn1	0	0
G.hn2	Disabled	Replace	G.hn2	0	0
G.hn3	Disabled	Replace	G.hn3	0	0
G.hn4	Disabled	Replace	G.hn4	0	0
Monitor	Disabled	Replace	Monitor	0	0
RJ45 G1	Disabled	Replace	RJ45/G1	0	0
RJ45 G2	Disabled	Replace	RJ45/G2	0	0
Fiber G1	Disabled	Replace	Fiber/G1	0	0
Fiber G2	Disabled	Replace	Fiber/G2	0	0

3.6.6.3 Group Information

This page displays the DHCP Snooping group information. Take the configuration in the following figure as an example for illustration. A device with the MAC 6c-f0-49-82-be-cf of VLAN 1, connected with the Ethernet 0/1 port, successfully got an IP address 192.168.104.250 from a DHCP server, and the lease time is 259200 seconds.



IP Address	MAC Address	Lease	VLAN	Port	Type

3.6.7 DHCP Limit

To prevent attacks from unauthorized DHCP servers, the switch CPU for validity checking will process DHCP packets; but if attackers generate a large number of DHCP packets, the switch CPU will be under extremely heavy load. As a result, the switch cannot work normally and even goes down.

IPC-1840 switches support DHCP packet rate limit on a port and shut down the port under attack to prevent hazardous impact on the device CPU.

After DHCP packet rate limit is enabled on an Ethernet port, the switch counts the number of DHCP packets received on this port per second. If the number of DHCP packets received per second exceeds the specified value, packets are passing the port at an over-high rate, which implies an attack to the port. In this case, the switch shuts down this port so that it cannot receive any packet, thus protect the switch from attacks.

In addition, the switch supports port state auto-recovery. After a port is shut down due to over-high packet rate, it resumes automatically after a configurable period of time.

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

3.6.7.1 Port Configuration

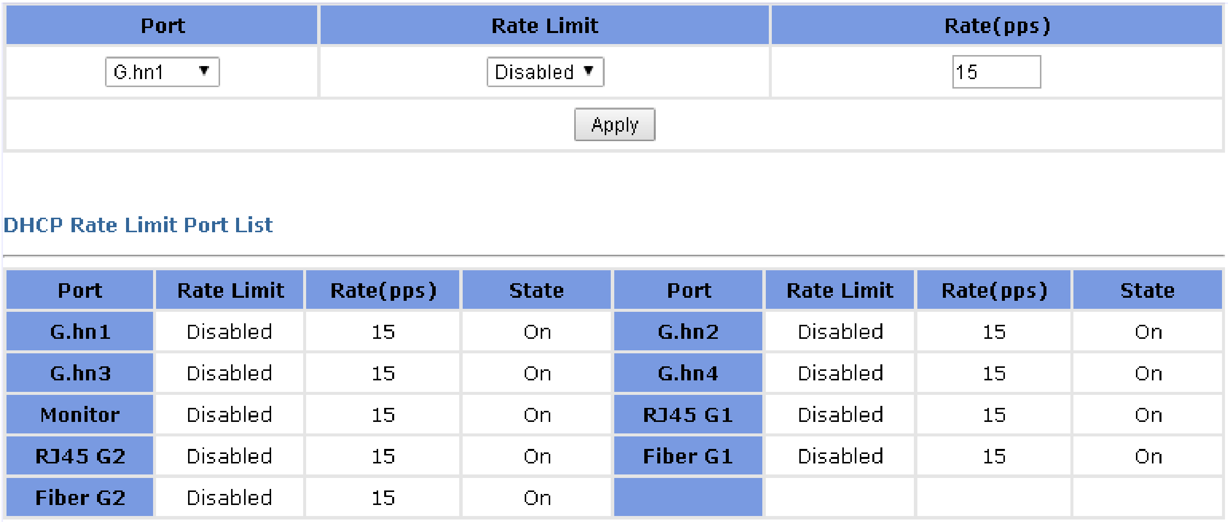
This page sets the DHCP Rate Limit for a specified Ethernet Port.

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 15 pps.

State Port state, when it over speeds, it will be shown as “OFF”.

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



Port	Rate Limit	Rate(pps)
G.hn1 ▼	Disabled ▼	15

Apply

DHCP Rate Limit Port List

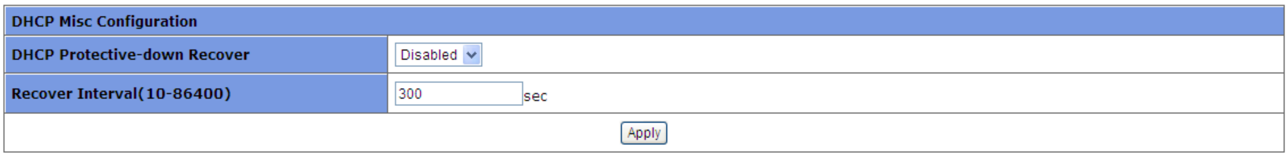
Port	Rate Limit	Rate(pps)	State	Port	Rate Limit	Rate(pps)	State
G.hn1	Disabled	15	On	G.hn2	Disabled	15	On
G.hn3	Disabled	15	On	G.hn4	Disabled	15	On
Monitor	Disabled	15	On	RJ45 G1	Disabled	15	On
RJ45 G2	Disabled	15	On	Fiber G1	Disabled	15	On
Fiber G2	Disabled	15	On				

3.6.7.2 Basic Configuration

This page sets the DHCP Misc Configuration.

DHCP Protective-down Recover 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 time interval, the port will recover automatically and enable itself. It is in the range of 10 to 86400 seconds, the default value is 300 seconds.



DHCP Misc Configuration

DHCP Protective-down Recover	Disabled ▾
Recover Interval(10-86400)	300 sec

Apply

3.6.8 Dynamic ARP Inspection

To guard against the man-in-the-middle attacks launched by hackers or attackers, IPC-1840 switches support the ARP attack detection function. All ARP (both request and response) packets passing through the switch are redirected to the CPU, which checks the validity of all the ARP packets by using the DHCP snooping table or the manually configured IP binding table. For description of DHCP snooping table and the manually configured IP binding table, refer to the DHCP snooping section in the part discussing

DHCP in this manual.

After you enable the ARP attack detection function, the switch will check the following items of an ARP packet: the source MAC address, source IP address, port number of the port receiving the ARP packet, and the ID of the VLAN the port resides. If these items match the entries of the DHCP snooping table or the manual configured IP binding table, the switch will forward the ARP packet; if not, the switch discards the ARP packet.

- With trusted ports configured, ARP packets coming from the trusted ports will not be checked, while those from other ports will be checked through the DHCP snooping table or the manually configured IP binding table.
- With the ARP restricted forwarding function enabled, ARP request packets are forwarded through trusted ports only; ARP response packets are forwarded according to the MAC addresses in the packets, or through trusted ports if the MAC address table contains no such destination MAC addresses.

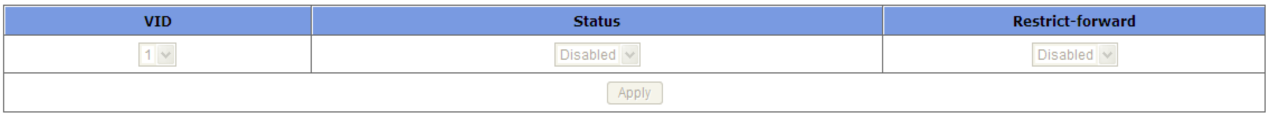
3.6.8.1 VLAN Configuration

VID Specify the VLAN needed to configure

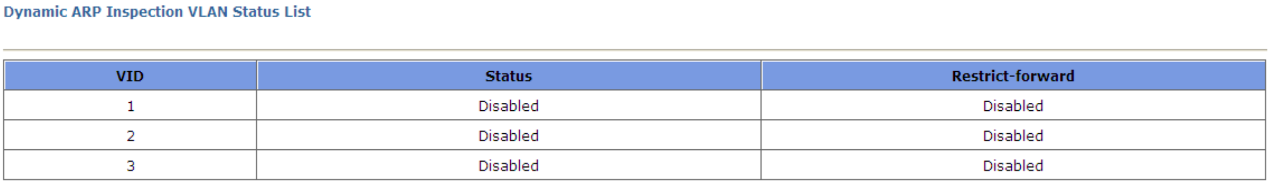
Status Enable/disable the Dynamic ARP Inspection function based on VLAN

Restrict-forward 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 lower part of this page lists all Dynamic ARP Inspection VLAN status.



VID	Status	Restrict-forward
1	Disabled	Disabled

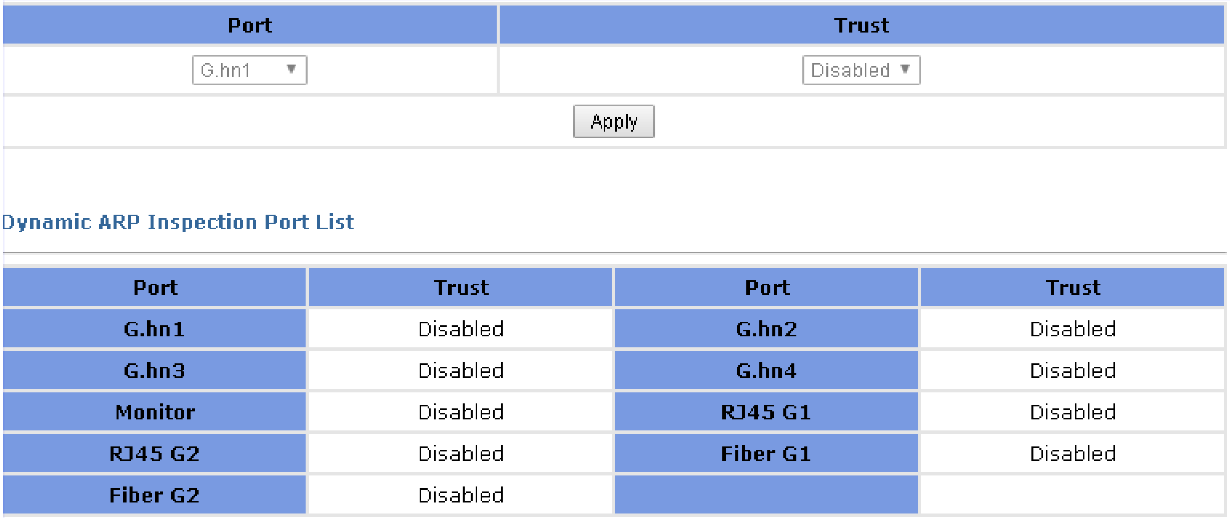


Dynamic ARP Inspection VLAN Status List

VID	Status	Restrict-forward
1	Disabled	Disabled
2	Disabled	Disabled
3	Disabled	Disabled

3.6.8.2 Port Configuration

This page sets the Dynamic ARP Inspection trust port for the specified Ethernet Port. ARP packets coming from the trusted ports will not be checked. The lower part of this page lists all the Dynamic ARP Inspection Ports.



Port	Trust
G.hn1 ▼	Disabled ▼

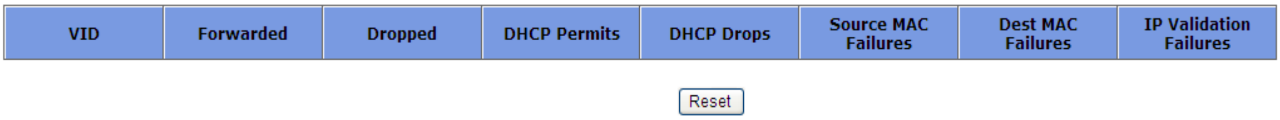
Apply

Dynamic ARP Inspection Port List

Port	Trust	Port	Trust
G.hn1	Disabled	G.hn2	Disabled
G.hn3	Disabled	G.hn4	Disabled
Monitor	Disabled	RJ45 G1	Disabled
RJ45 G2	Disabled	Fiber G1	Disabled
Fiber G2	Disabled		

3.6.8.3 Group Information

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



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

Reset

3.6.9 ARP Limit

To prevent ARP attacks from unauthorized DHCP servers, the switch CPU for validity checking will process ARP packets; but if attackers generate a large number of ARP packets, the switch CPU will be under extremely heavy load. As a result, the switch cannot work normally and even goes down.

In addition, the switch supports port state auto-recovery. After a port is shut down due to over-high packet rate, it resumes automatically after a configurable period of time.

3.6.9.1 Port Configuration

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

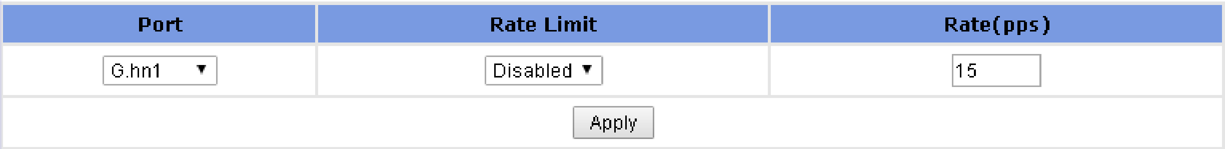
Port Specify a port to configure DHCP rate limit

Rate Limit Enable/disable the function of ARP Rate limit for the specified port

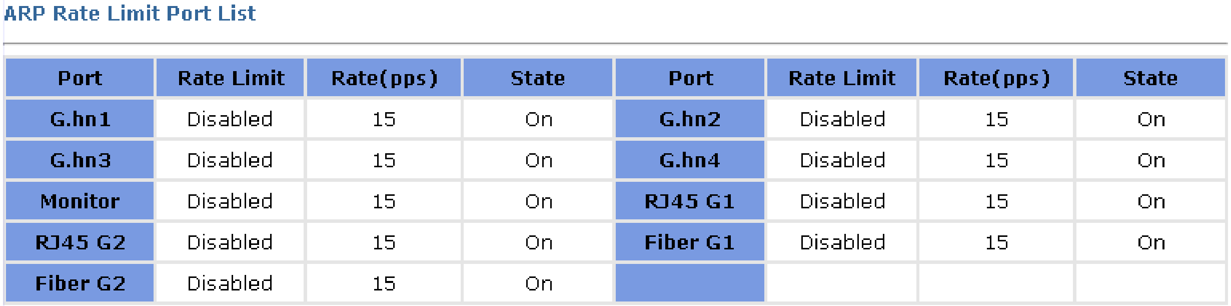
Rate It is in the range of 10 to 150 pps, the default value is 15 pps.

State Port state, when it over speeds, it will be shown as “OFF”.

The lower part of this page lists the ARP Rate Limit of all the ports.



Port	Rate Limit	Rate(pps)
G.hn1 ▼	Disabled ▼	15



ARP Rate Limit Port List

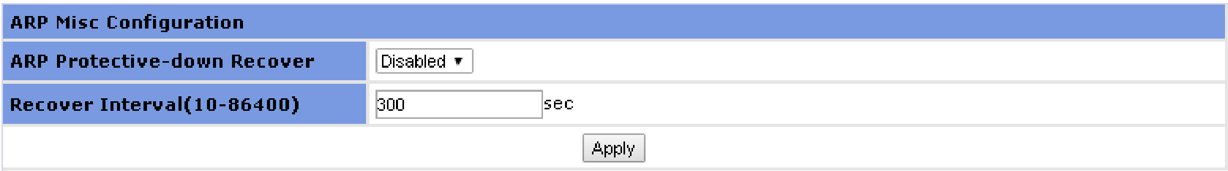
Port	Rate Limit	Rate(pps)	State	Port	Rate Limit	Rate(pps)	State
G.hn1	Disabled	15	On	G.hn2	Disabled	15	On
G.hn3	Disabled	15	On	G.hn4	Disabled	15	On
Monitor	Disabled	15	On	RJ45 G1	Disabled	15	On
RJ45 G2	Disabled	15	On	Fiber G1	Disabled	15	On
Fiber G2	Disabled	15	On				

3.6.9.2 Basic Configuration

This page sets the ARP Misc Configuration.

ARP Protective-down Recover 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 seconds, the default value is 300 seconds.



ARP Misc Configuration

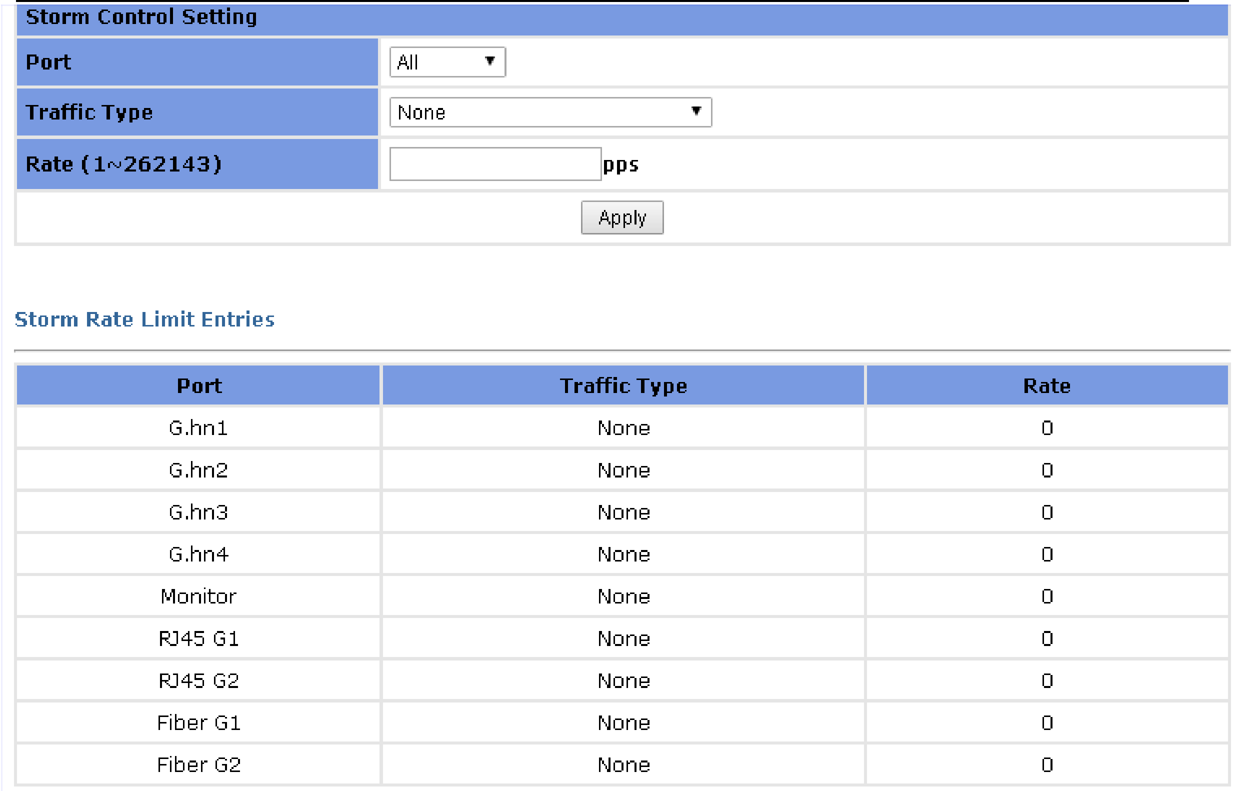
ARP Protective-down Recover	Disabled ▼
Recover Interval(10-86400)	300 sec

3.6.10 Storm Control

Traffic storm will be generated when there are multiple broadcast / multicast / DLF (Destination Lookup Failed) packets passing through a port, thus it will lead to traffic congestion. If the transmission rate of the three kinds of packets exceeds the set bandwidth, the packets will automatically be discarded to avoid network broadcast storm.

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

Select the Traffic Type from none, Broadcast, Multicast, Unknown Unicast, Broadcast + Multicast, Broadcast + Unknown Unicast, and Broadcast + Unknown Unicast and Broadcast + Multicast + Unknown Unicast. Specify a rate limit within the range of 1 - 262143 PPS. Storm control is disabled by default.



Storm Control Setting

Port	All ▼
Traffic Type	None ▼
Rate (1~262143)	pps

Storm Rate Limit Entries

Port	Traffic Type	Rate
G.hn1	None	0
G.hn2	None	0
G.hn3	None	0
G.hn4	None	0
Monitor	None	0
RJ45 G1	None	0
RJ45 G2	None	0
Fiber G1	None	0
Fiber G2	None	0

3.6.11 Port Security

Port security is a security mechanism for network access control. It is an expansion to the current 802.1x and MAC address authentication.

Port security allows you to define various security modes that enable devices to learn legal source MAC addresses, so that you can implement different network security management as needed.

With port security enabled, packets whose source MAC addresses cannot be learned by your switch in a security mode are considered illegal packets. The events that cannot pass 802.1x authentication or MAC authentication are considered illegal.

With port security enabled, upon detecting an illegal packet or illegal event, the system triggers the corresponding port security features and takes pre-defined actions automatically. This reduces your maintenance workload and greatly enhances system security and manageability.

Port security allows more than one user to be authenticated on a port. The number of authenticated users allowed, however, cannot exceed the configured upper limit.

By setting the maximum number of MAC addresses allowed on a port, you can

- Control the maximum number of users who are allowed to access the network through the port

- Control the number of Security MAC addresses that can be added with port security

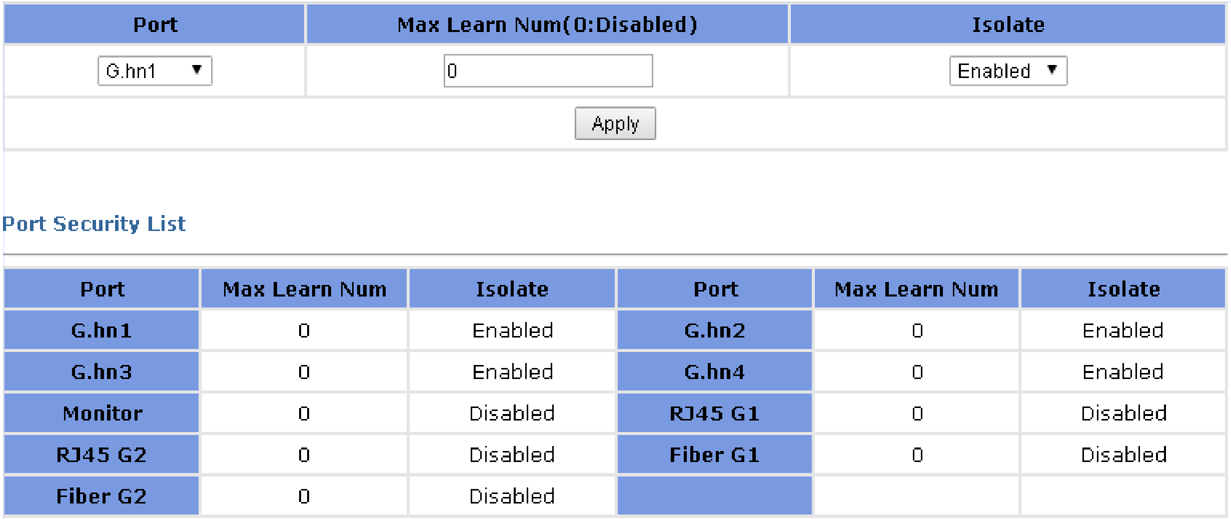
This configuration is different from that of the maximum number of MAC addresses that can be learned by a port in MAC address management.

Port Specify the port.

Max Learn Num Set the maximum MAC number, it is in the range of 1 ~ 1024. And “0” means to disable it.

Isolate Enable/disable port isolation.

Through the port isolation feature, you can add the ports to be controlled into an isolation group to isolate the Layer 2 and Layer 3 data between each port in the isolation group. Thus, you can construct your network in a more flexible way and improve your network security.



Port	Max Learn Num(0:Disabled)	Isolate
G.hn1 ▼	0	Enabled ▼

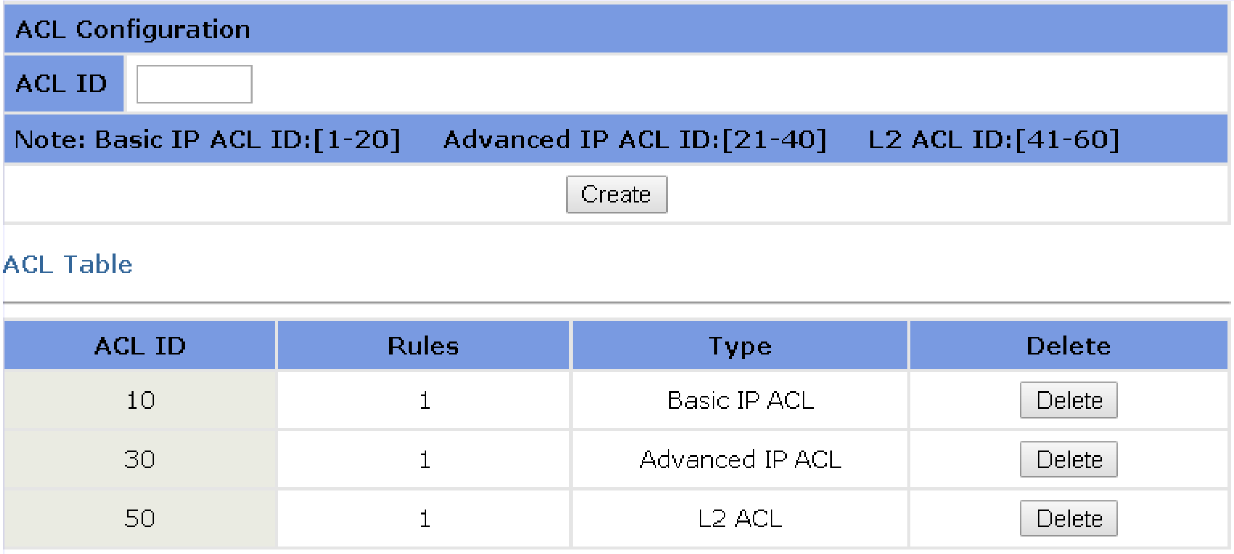
Port Security List

Port	Max Learn Num	Isolate	Port	Max Learn Num	Isolate
G.hn1	0	Enabled	G.hn2	0	Enabled
G.hn3	0	Enabled	G.hn4	0	Enabled
Monitor	0	Disabled	RJ45 G1	0	Disabled
RJ45 G2	0	Disabled	Fiber G1	0	Disabled
Fiber G2	0	Disabled			

3.6.12 ACL Configuration

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.

3.6.12.1 Basic Configuration



ACL Configuration

ACL ID	

Note: Basic IP ACL ID:[1-20]   Advanced IP ACL ID:[21-40]   L2 ACL ID:[41-60]

ACL Table

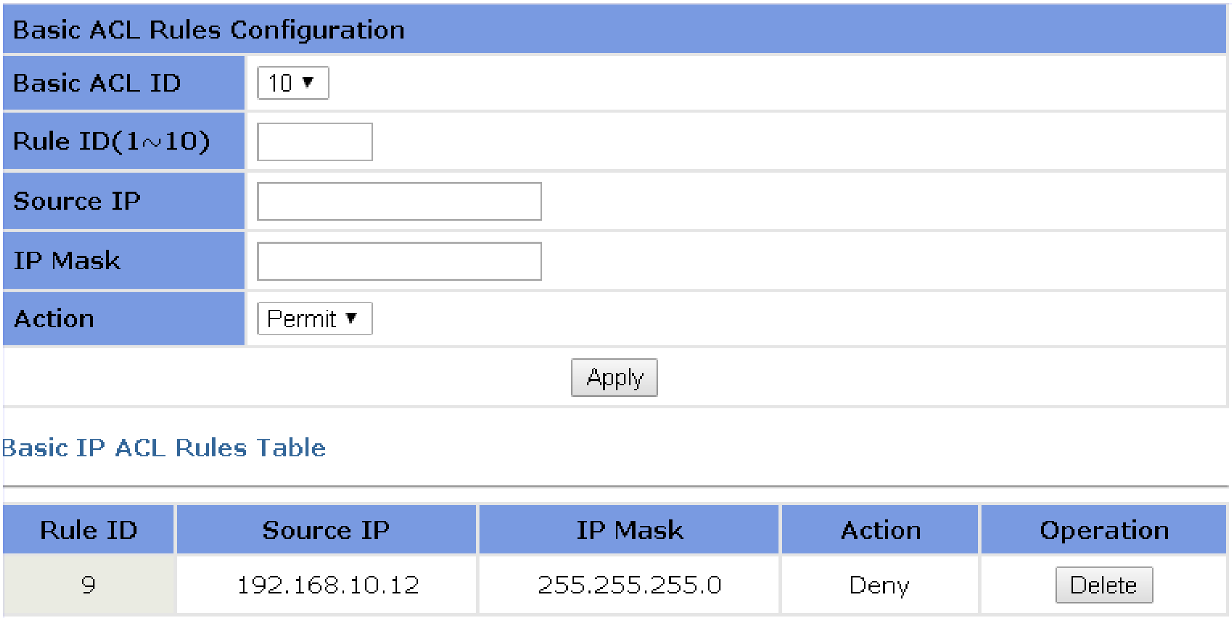
ACL ID	Rules	Type	Delete
10	1	Basic IP ACL	Delete
30	1	Advanced IP ACL	Delete
50	1	L2 ACL	Delete

On this tab page, you can create a new ACL with specific ACL ID and type of ACL.
There are three types of ACL:
Basic IP ACL: The filtering packets only based on source IP address.
Advance IP ACL: The filtering packets based on source IP address, destination IP address, IP protocol type, and more.
L2 ACL: The filtering packets based on source MAC address, destination MAC addresses, 802.1p priority, and L2 protocol type.

3.6.12.2 Basic IP ACL

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

Permit: To permit the access of rule-matched IP**.**
Deny: To deny the access of rule-matched IP**.**



Basic ACL Rules Configuration

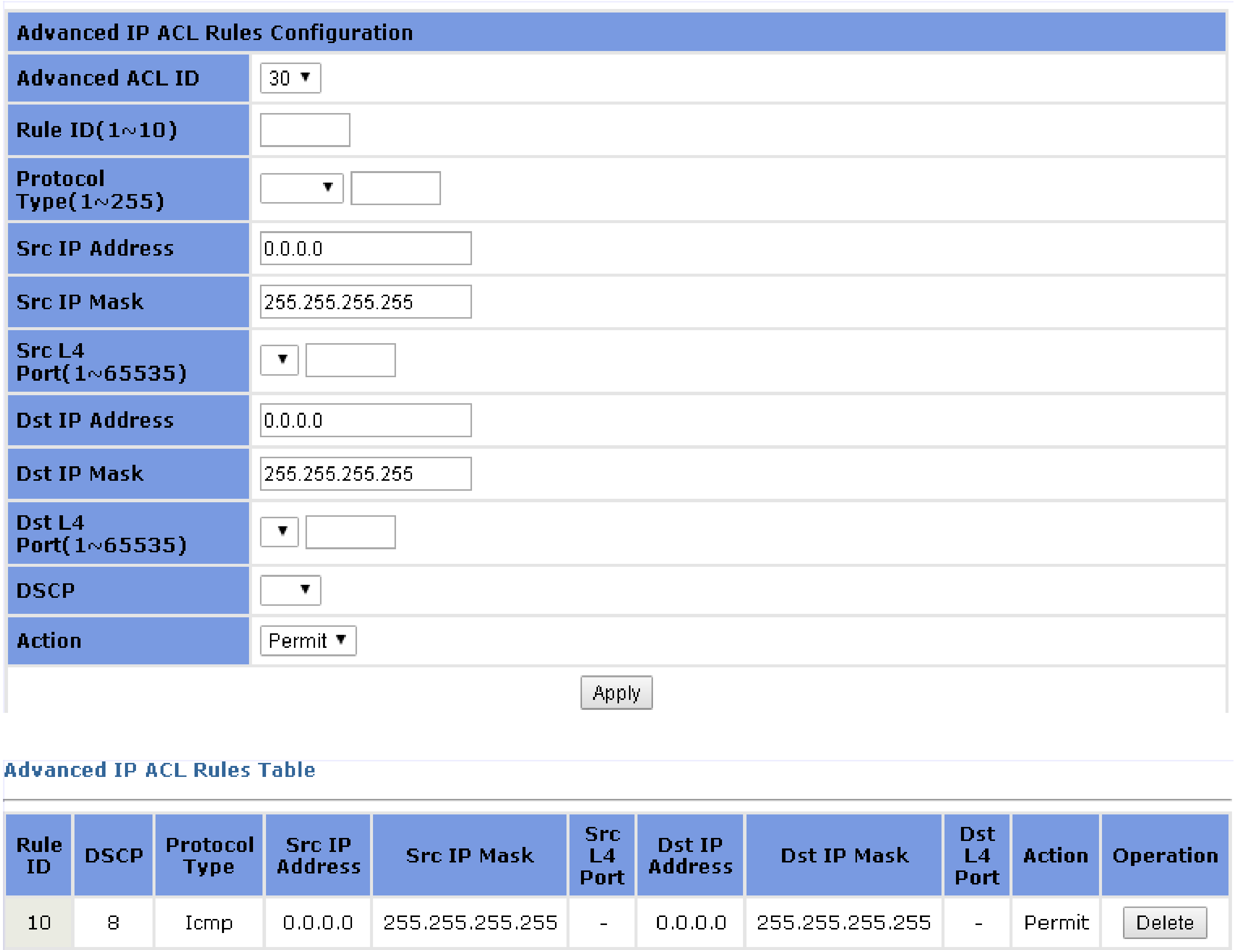
Basic ACL ID	10 ▾
Rule ID(1~10)	
Source IP	
IP Mask	
Action	Permit ▾

Basic IP ACL Rules Table

Rule ID	Source IP	IP Mask	Action	Operation
9	192.168.10.12	255.255.255.0	Deny	Delete

3.6.12.3 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 type etc.



Advanced IP ACL Rules Configuration

Advanced ACL ID	30 ▾
Rule ID(1~10)	
Protocol Type(1~255)	▾
Src IP Address	0.0.0.0
Src IP Mask	255.255.255.255
Src L4 Port(1~65535)	▾
Dst IP Address	0.0.0.0
Dst IP Mask	255.255.255.255
Dst L4 Port(1~65535)	▾
DSCP	▾
Action	Permit ▾

Advanced IP ACL Rules Table

Rule ID	DSCP	Protocol Type	Src IP Address	Src IP Mask	Src L4 Port	Dst IP Address	Dst IP Mask	Dst L4 Port	Action	Operation
10	8	Icmp	0.0.0.0	255.255.255.255	-	0.0.0.0	255.255.255.255	-	Permit	Delete

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 to 65535. It can be set only when protocol type is TCP or UDP.

Note: 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.

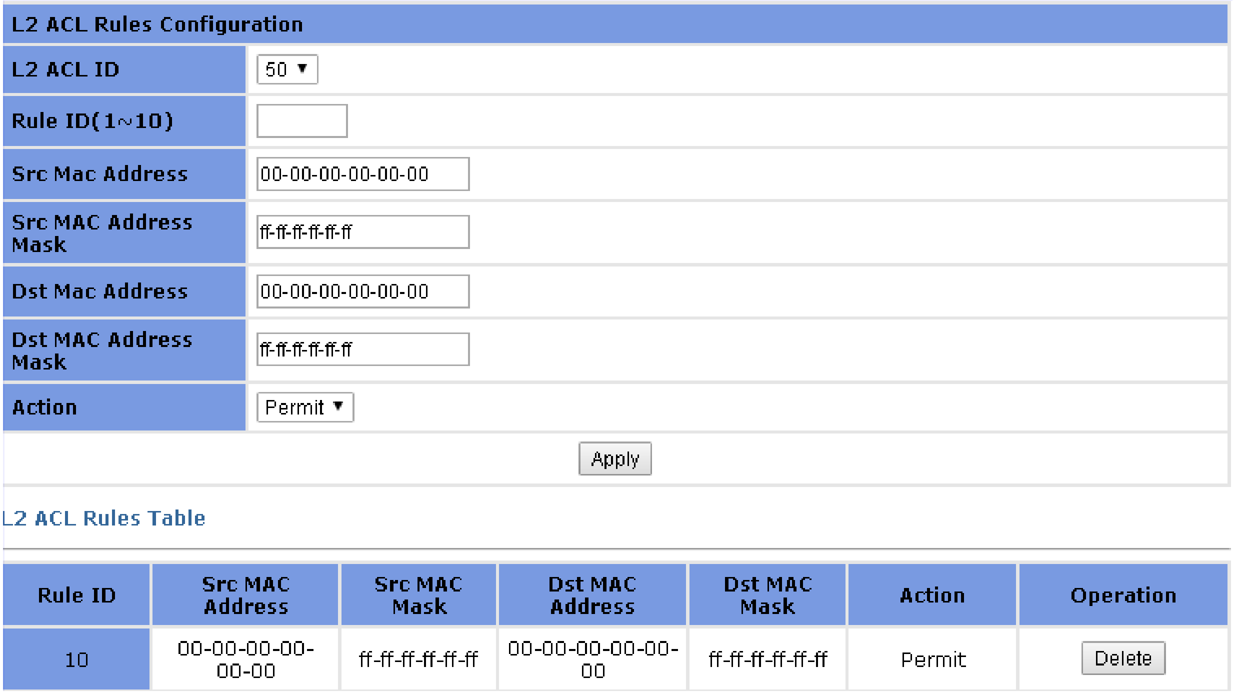
Dst IP Mask: destination host IP subnet mask

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.

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

3.6.12.4 L2 ACL

This page sets **Src MAC Address, Src MAC Address Mask, Dst Mac Address, and Dst MAC address Mask**, and the **Action** that can be set as **Permit** or **Deny.**



L2 ACL Rules Configuration

L2 ACL ID	50 ▾
Rule ID(1~10)	
Src Mac Address	00-00-00-00-00-00
Src MAC Address Mask	ff-ff-ff-ff-ff-ff
Dst Mac Address	00-00-00-00-00-00
Dst MAC Address Mask	ff-ff-ff-ff-ff-ff
Action	Permit ▾

L2 ACL Rules Table

Rule ID	Src MAC Address	Src MAC Mask	Dst MAC Address	Dst MAC Mask	Action	Operation
10	00-00-00-00-00-00	ff-ff-ff-ff-ff-ff	00-00-00-00-00-00	ff-ff-ff-ff-ff-ff	Permit	Delete

Rule ID: Identification of the ACL rule.

Src MAC Address: Source host mac address.

Src MAC Address Mask: Source host mac address mask.

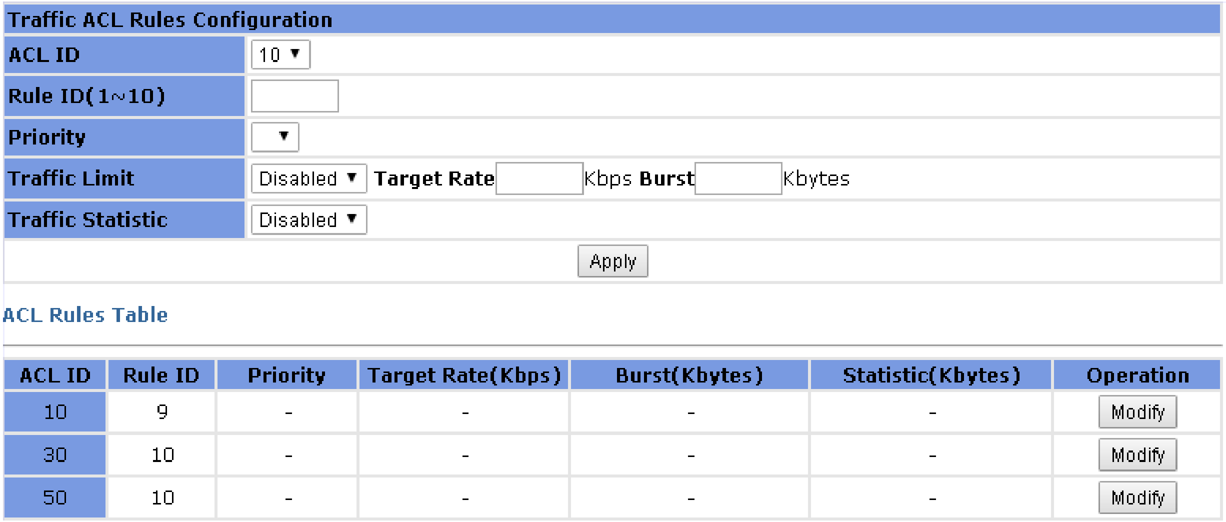
Dst MAC Address: Destination host mac address.

Dst MAC address Mask: Destination host mac address mask.

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

3.6.12.5 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.



Traffic ACL Rules Configuration	
ACL ID	10 ▾
Rule ID(1~10)	
Priority	▾
Traffic Limit	Disabled ▾ Target Rate Kbps Burst Kbytes
Traffic Statistic	Disabled ▾
	Apply

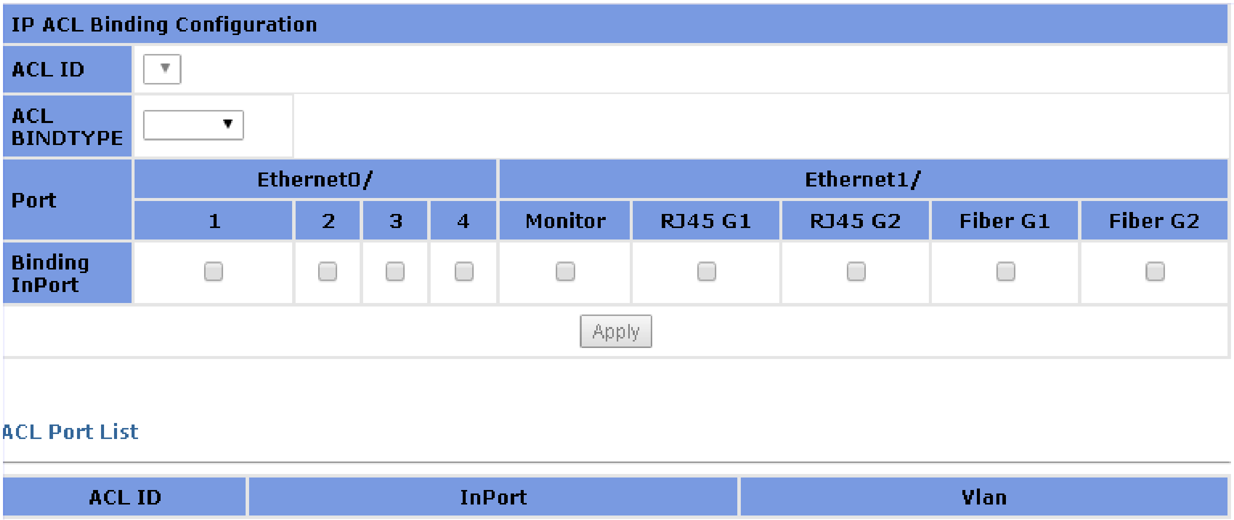
ACL Rules Table

ACL ID	Rule ID	Priority	Target Rate(Kbps)	Burst(Kbytes)	Statistic(Kbytes)	Operation
10	9	-	-	-	-	Modify
30	10	-	-	-	-	Modify
50	10	-	-	-	-	Modify

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.

3.6.12.6 Port Binding

This page sets the binding of an Ethernet port to a specified ACL ID. If a port is bound, the binding will be applied to all the rules associated to this ACL ID.



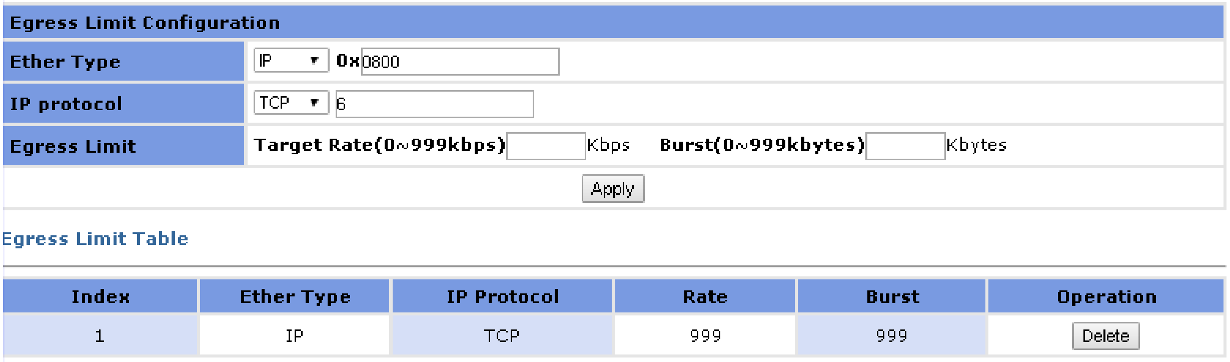
IP ACL Binding Configuration									
ACL ID	▾								
ACL BINDTYPE	▾								
Port	Ethernet0/				Ethernet1/				
	1	2	3	4	Monitor	RJ45 G1	RJ45 G2	Fiber G1	Fiber G2
Binding InPort	□	□	□	□	□	□	□	□	□
	Apply								

ACL Port List

ACL ID	InPort	Vlan

3.6.13 Egress Limit

This page sets the egress limit configuration



Egress Limit Configuration	
Ether Type	IP ▾ 0x0800
IP protocol	TCP ▾ 6
Egress Limit	Target Rate(0~999kbps) Kbps Burst(0~999kbytes) Kbytes
	Apply

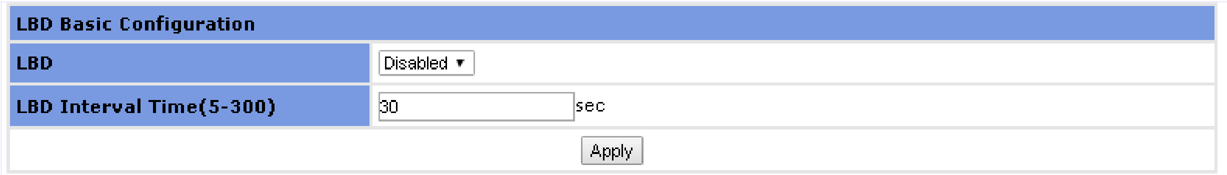
Egress Limit Table

Index	Ether Type	IP Protocol	Rate	Burst	Operation
1	IP	TCP	999	999	Delete

3.6.14 LBD

Loopback Detection to monitor whether the packet from the port back through the port equipment, used to determine under port network whether there is a loop.

3.6.14.1 Basic Configuration

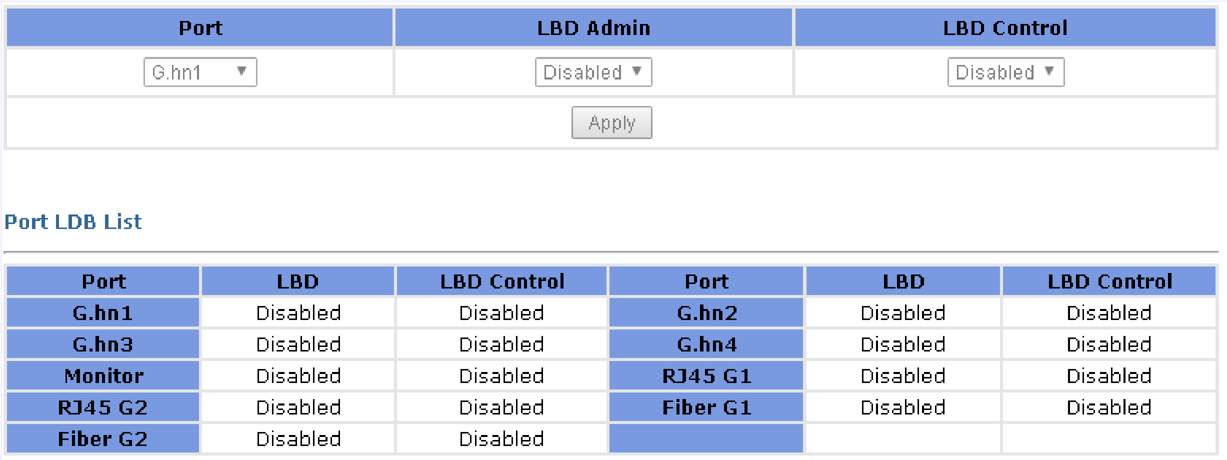


LBD Basic Configuration	
LBD	Disabled ▾
LBD Interval Time(5-300)	30 sec
	Apply

LBD: enable or disabled

LBD Interval Times: config interval time for loopback detection

3.6.14.2 Port Configuration



Port	LBD Admin	LBD Control
G.hn1 ▾	Disabled ▾	Disabled ▾
	Apply	

Port LDB List

Port	LBD	LBD Control	Port	LBD	LBD Control
G.hn1	Disabled	Disabled	G.hn2	Disabled	Disabled
G.hn3	Disabled	Disabled	G.hn4	Disabled	Disabled
Monitor	Disabled	Disabled	RJ45 G1	Disabled	Disabled
RJ45 G2	Disabled	Disabled	Fiber G1	Disabled	Disabled
Fiber G2	Disabled	Disabled			

LBD Admin: enable or disable Loopback detection on this port

LBD Control: configure port loopback detection control.

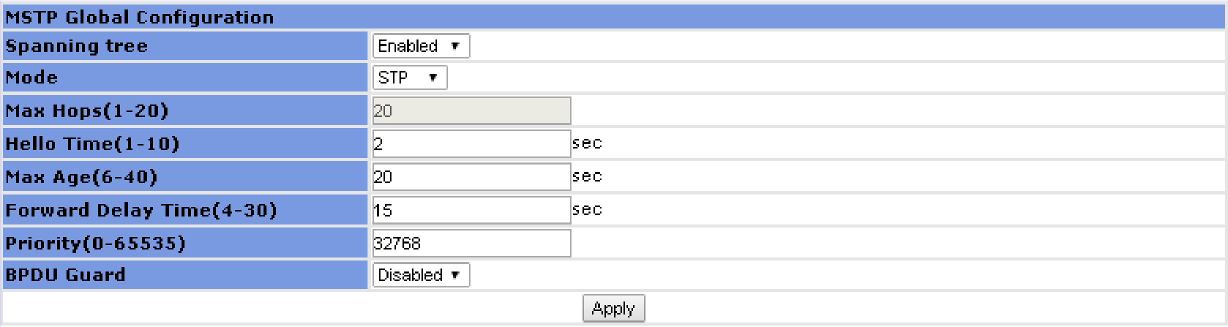
3.7 Spanning Tree

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.

3.7.1 Global Configuration

Before configuring STP, make sure STP is enabled



MSTP Global Configuration		
Spanning tree	Enabled ▼	
Mode	STP ▼	
Max Hops(1-20)	20	
Hello Time(1-10)	2	sec
Max Age(6-40)	20	sec
Forward Delay Time(4-30)	15	sec
Priority(0-65535)	32768	
BPDU Guard	Disabled ▼	
	Apply	

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.

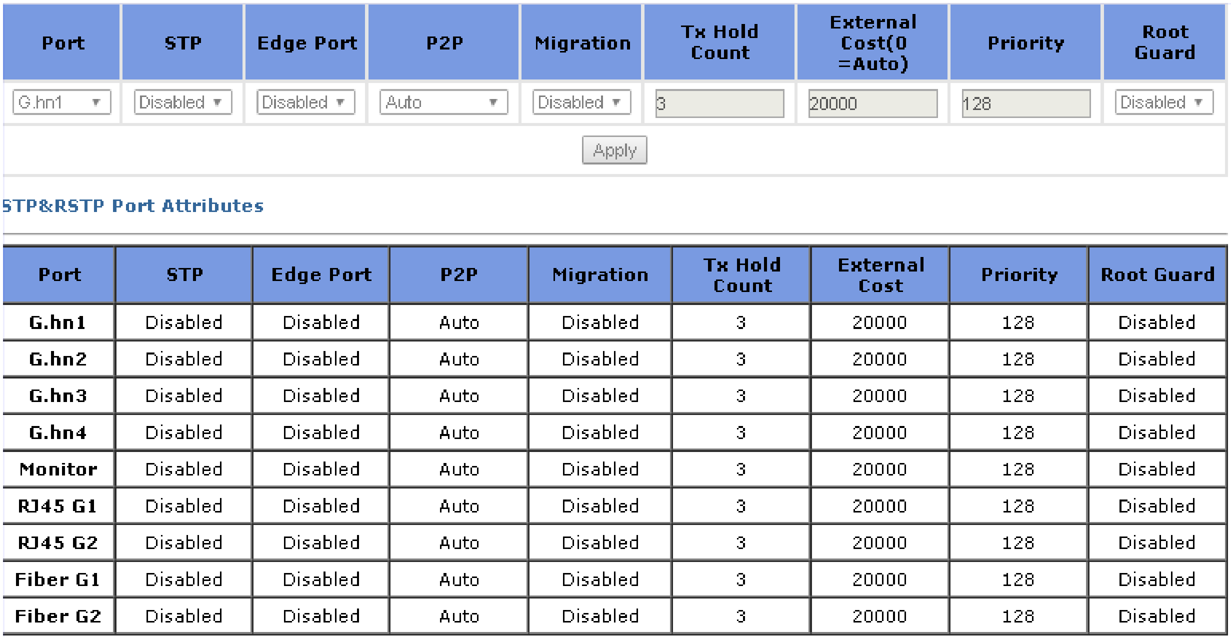
BPDU Guard: Some ports are usually configured as edge ports to achieve rapid transition, while they will become to non-edge ports automatically upon receiving configuration BPDUs, which may cause spanning trees regeneration and network topology jitter.

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.

3.7.2 STP&RSTP

3.7.2.1 Ports Configuration



Port	STP	Edge Port	P2P	Migration	Tx Hold Count	External Cost(0=Auto)	Priority	Root Guard
G.hn1 ▾	Disabled ▾	Disabled ▾	Auto ▾	Disabled ▾	3	20000	128	Disabled ▾

STP&RSTP Port Attributes

Port	STP	Edge Port	P2P	Migration	Tx Hold Count	External Cost	Priority	Root Guard
G.hn1	Disabled	Disabled	Auto	Disabled	3	20000	128	Disabled
G.hn2	Disabled	Disabled	Auto	Disabled	3	20000	128	Disabled
G.hn3	Disabled	Disabled	Auto	Disabled	3	20000	128	Disabled
G.hn4	Disabled	Disabled	Auto	Disabled	3	20000	128	Disabled
Monitor	Disabled	Disabled	Auto	Disabled	3	20000	128	Disabled
RJ45 G1	Disabled	Disabled	Auto	Disabled	3	20000	128	Disabled
RJ45 G2	Disabled	Disabled	Auto	Disabled	3	20000	128	Disabled
Fiber G1	Disabled	Disabled	Auto	Disabled	3	20000	128	Disabled
Fiber G2	Disabled	Disabled	Auto	Disabled	3	20000	128	Disabled

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). 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.

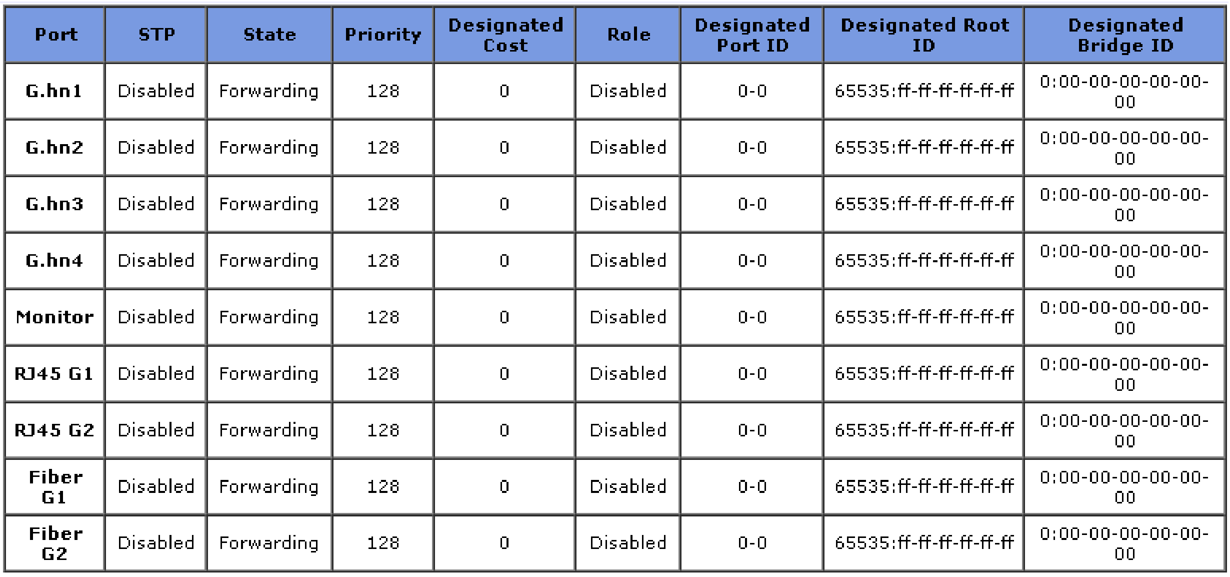
Root Guard: by default, the root protection function is disabled.

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).

3.7.2.2 Ports Status

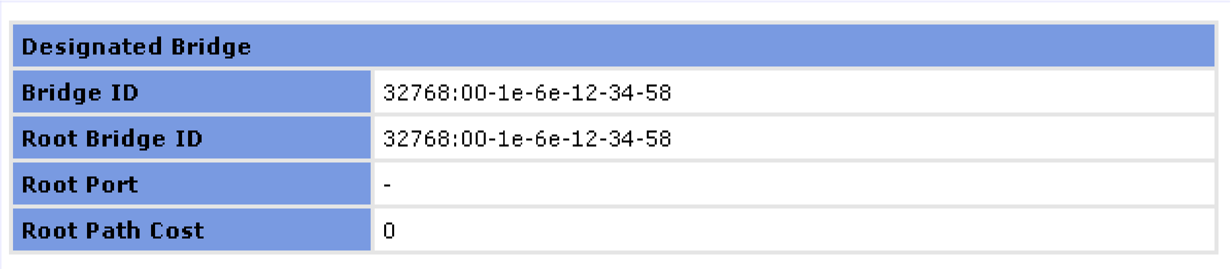
This page lists all port parameters and spanning tree information, including **STP**, **State**, **Priority**, **Cost**, **Role**, **Designated Port ID**, **Designated Root ID**, and **Designated Bridge ID.**



Port	STP	State	Priority	Designated Cost	Role	Designated Port ID	Designated Root ID	Designated Bridge ID
G.hn1	Disabled	Forwarding	128	0	Disabled	0-0	65535:ff-ff-ff-ff-ff-ff	0:00-00-00-00-00-00
G.hn2	Disabled	Forwarding	128	0	Disabled	0-0	65535:ff-ff-ff-ff-ff-ff	0:00-00-00-00-00-00
G.hn3	Disabled	Forwarding	128	0	Disabled	0-0	65535:ff-ff-ff-ff-ff-ff	0:00-00-00-00-00-00
G.hn4	Disabled	Forwarding	128	0	Disabled	0-0	65535:ff-ff-ff-ff-ff-ff	0:00-00-00-00-00-00
Monitor	Disabled	Forwarding	128	0	Disabled	0-0	65535:ff-ff-ff-ff-ff-ff	0:00-00-00-00-00-00
RJ45 G1	Disabled	Forwarding	128	0	Disabled	0-0	65535:ff-ff-ff-ff-ff-ff	0:00-00-00-00-00-00
RJ45 G2	Disabled	Forwarding	128	0	Disabled	0-0	65535:ff-ff-ff-ff-ff-ff	0:00-00-00-00-00-00
Fiber G1	Disabled	Forwarding	128	0	Disabled	0-0	65535:ff-ff-ff-ff-ff-ff	0:00-00-00-00-00-00
Fiber G2	Disabled	Forwarding	128	0	Disabled	0-0	65535:ff-ff-ff-ff-ff-ff	0:00-00-00-00-00-00

3.7.2.3 Bridge Information

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



Designated Bridge	
Bridge ID	32768:00-1e-6e-12-34-58
Root Bridge ID	32768:00-1e-6e-12-34-58
Root Port	-
Root Path Cost	0

Bridge ID: ID of this switch.
Root Bridge ID: ID of the root bridge.

Root Port: the spanning tree root port.

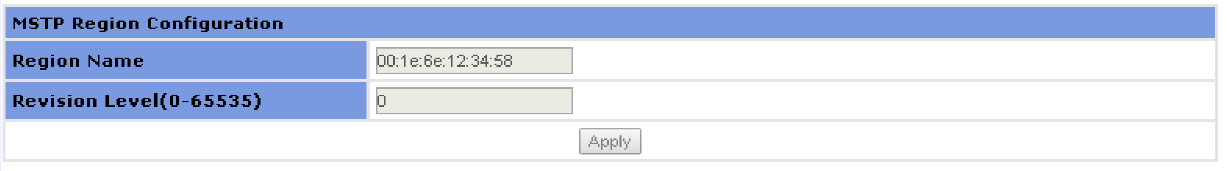
Root Path Cost: cost of the path from the switch to the root bridge.

3.7.3 MSTP Region

An MSTP region comprises one or more MST Bridges with the same MSTP configuration identifier.

3.7.3.1 Basic Configuration

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



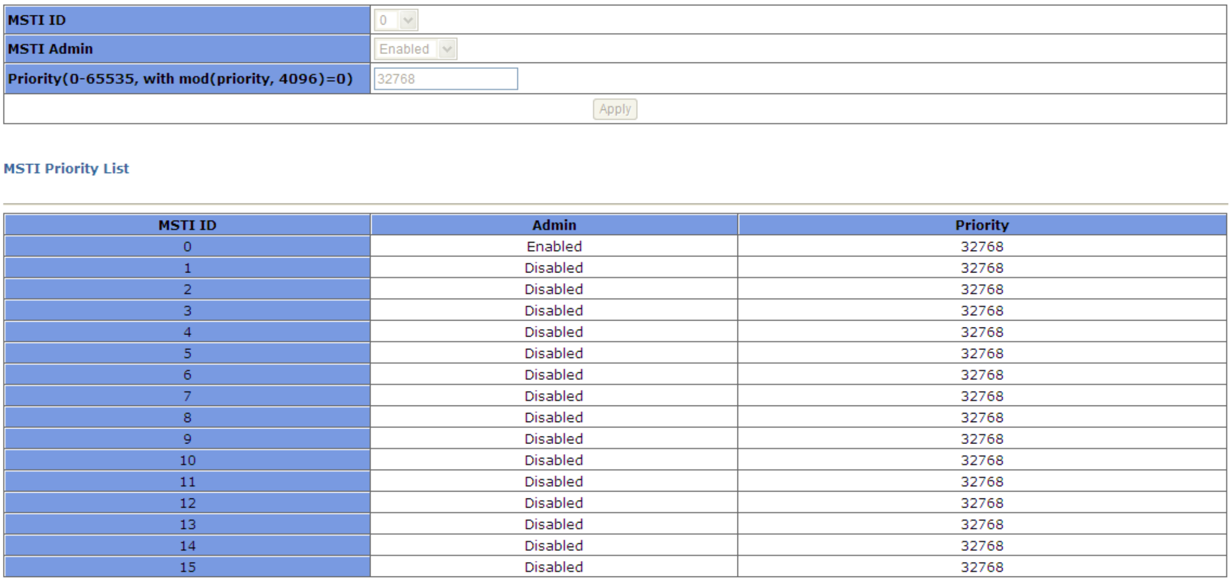
MSTP Region Configuration	
Region Name	00:1e:6e:12:34:58
Revision Level(0-65535)	0

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.

3.7.3.2 MSTI Configuration

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



MSTI ID	0
MSTI Admin	Enabled
Priority(0-65535, with mod(priority, 4096)=0)	32768

MSTI Priority List

MSTI ID	Admin	Priority
0	Enabled	32768
1	Disabled	32768
2	Disabled	32768
3	Disabled	32768
4	Disabled	32768
5	Disabled	32768
6	Disabled	32768
7	Disabled	32768
8	Disabled	32768
9	Disabled	32768
10	Disabled	32768
11	Disabled	32768
12	Disabled	32768
13	Disabled	32768
14	Disabled	32768
15	Disabled	32768

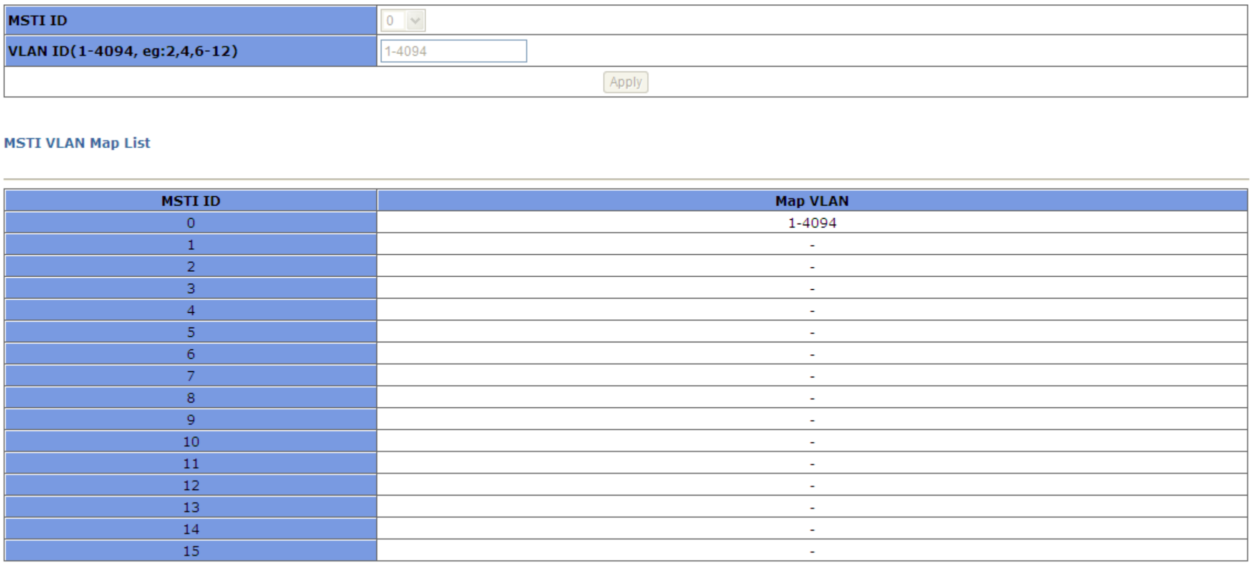
MSTI ID: MSTI identification, ranging from 0 to 15

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

3.7.3.3 Instance 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.



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

Apply

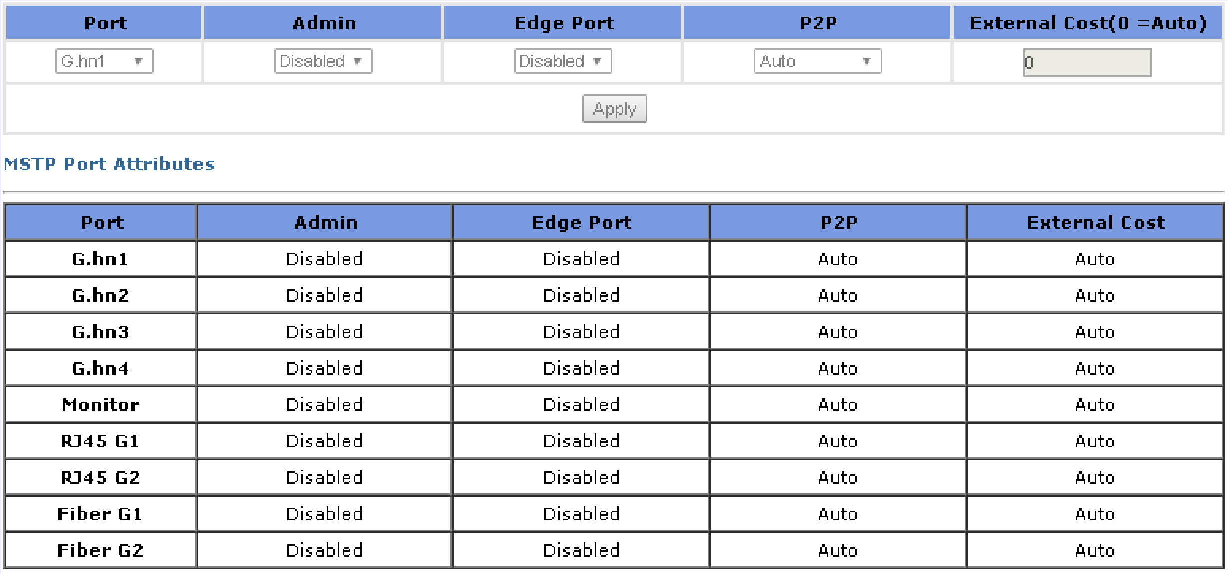
MSTI VLAN Map List

MSTI ID	Map VLAN
0	1-4094
1	-
2	-
3	-
4	-
5	-
6	-
7	-
8	-
9	-
10	-
11	-
12	-
13	-
14	-
15	-

3.7.4 MSTP Ports

3.7.4.1 Basic 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 3.4.2 Ports Configuration, this page sets MSTP port configuration.



Port	Admin	Edge Port	P2P	External Cost(0 =Auto)
G.hn1	Disabled	Disabled	Auto	0

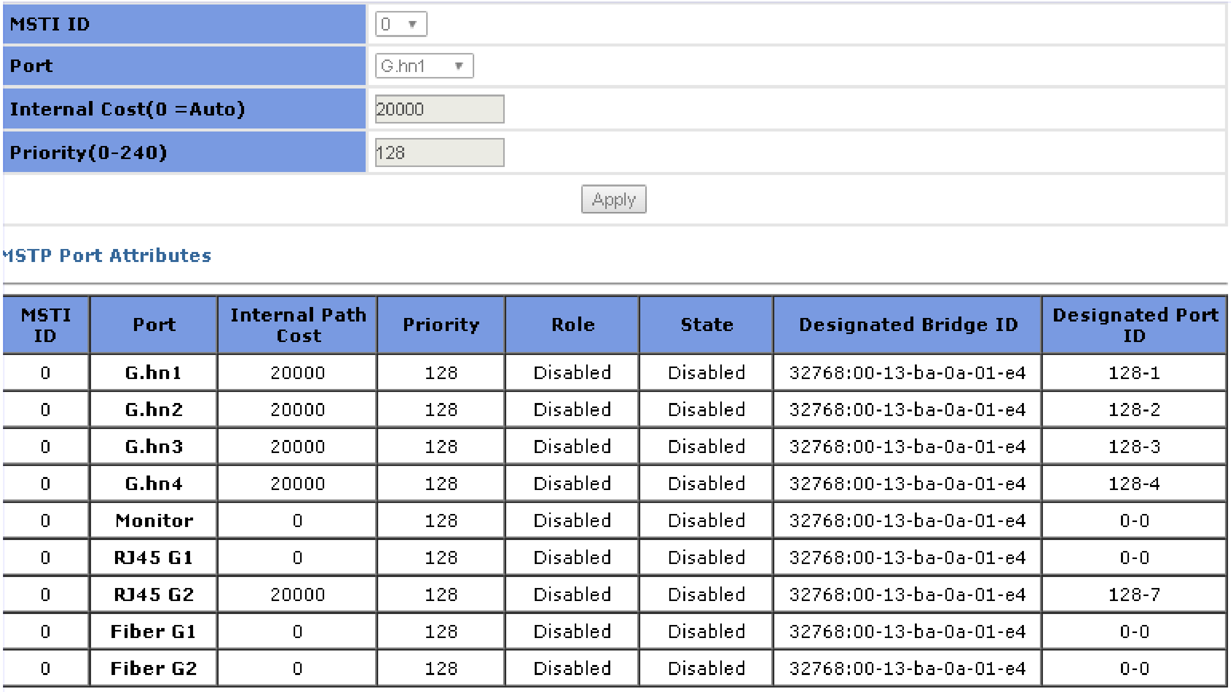
Apply

MSTP Port Attributes

Port	Admin	Edge Port	P2P	External Cost
G.hn1	Disabled	Disabled	Auto	Auto
G.hn2	Disabled	Disabled	Auto	Auto
G.hn3	Disabled	Disabled	Auto	Auto
G.hn4	Disabled	Disabled	Auto	Auto
Monitor	Disabled	Disabled	Auto	Auto
RJ45 G1	Disabled	Disabled	Auto	Auto
RJ45 G2	Disabled	Disabled	Auto	Auto
Fiber G1	Disabled	Disabled	Auto	Auto
Fiber G2	Disabled	Disabled	Auto	Auto

3.7.4.2 MSTI Ports

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



MSTI ID	0 ▾
Port	G.hn1 ▾
Internal Cost(0 =Auto)	20000
Priority(0-240)	128

MSTP Port Attributes

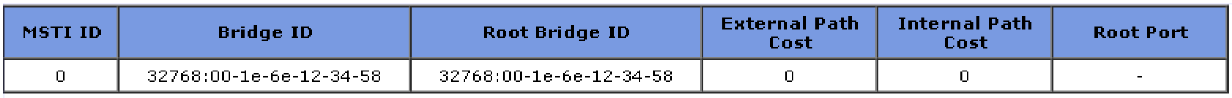
MSTI ID	Port	Internal Path Cost	Priority	Role	State	Designated Bridge ID	Designated Port ID
0	G.hn1	20000	128	Disabled	Disabled	32768:00-13-ba-0a-01-e4	128-1
0	G.hn2	20000	128	Disabled	Disabled	32768:00-13-ba-0a-01-e4	128-2
0	G.hn3	20000	128	Disabled	Disabled	32768:00-13-ba-0a-01-e4	128-3
0	G.hn4	20000	128	Disabled	Disabled	32768:00-13-ba-0a-01-e4	128-4
0	Monitor	0	128	Disabled	Disabled	32768:00-13-ba-0a-01-e4	0-0
0	RJ45 G1	0	128	Disabled	Disabled	32768:00-13-ba-0a-01-e4	0-0
0	RJ45 G2	20000	128	Disabled	Disabled	32768:00-13-ba-0a-01-e4	128-7
0	Fiber G1	0	128	Disabled	Disabled	32768:00-13-ba-0a-01-e4	0-0
0	Fiber G2	0	128	Disabled	Disabled	32768:00-13-ba-0a-01-e4	0-0

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.

3.7.5 MSTP Information

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

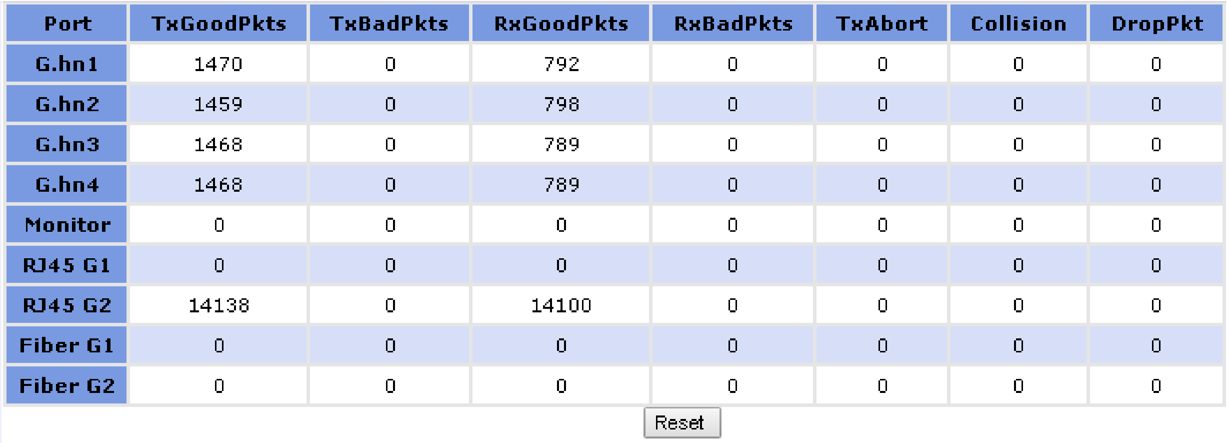


MSTI ID	Bridge ID	Root Bridge ID	External Path Cost	Internal Path Cost	Root Port
0	32768:00-1e-6e-12-34-58	32768:00-1e-6e-12-34-58	0	0	-

3.8 Monitoring

3.8.1 Port Statistics

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



Port	TxGoodPkts	TxBadPkts	RxGoodPkts	RxBadPkts	TxAbort	Collision	DropPkt
G.hn1	1470	0	792	0	0	0	0
G.hn2	1459	0	798	0	0	0	0
G.hn3	1468	0	789	0	0	0	0
G.hn4	1468	0	789	0	0	0	0
Monitor	0	0	0	0	0	0	0
RJ45 G1	0	0	0	0	0	0	0
RJ45 G2	14138	0	14100	0	0	0	0
Fiber G1	0	0	0	0	0	0	0
Fiber G2	0	0	0	0	0	0	0

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

TxFCSErr The number of FCS (Frame Check (Checking) Sequence) packets

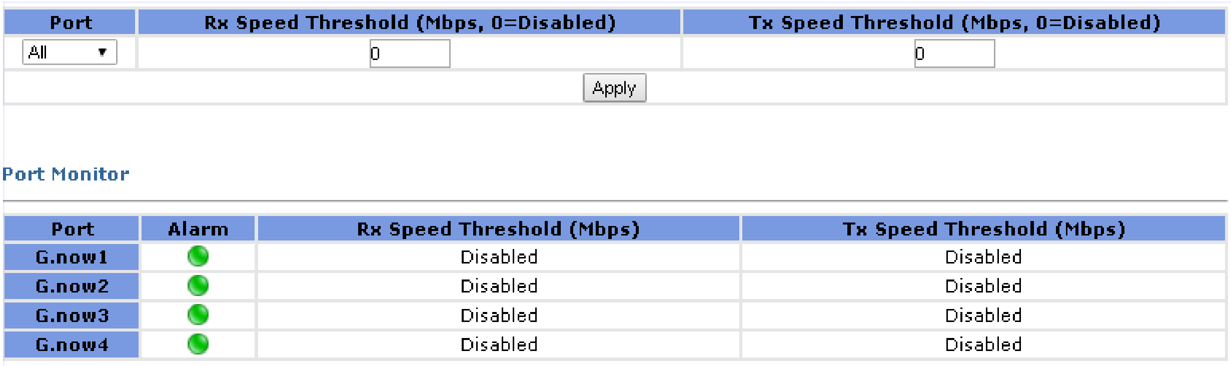
Collision The number of detected collisions

DropPkt The number of packets dropped for various reasons

3.8.2 Monitoring Rate

On this page, you can monitor the speed threshold by setting link Rx/Tx speed. When Rx/Tx speed is lower than threshold that you have set, it will send syslog alarm to syslog server.

Note: You need to configurate syslog configuration before.



Port	Rx Speed Threshold (Mbps, 0=Disabled)	Tx Speed Threshold (Mbps, 0=Disabled)
All ▾	0	0

Port Monitor

Port	Alarm	Rx Speed Threshold (Mbps)	Tx Speed Threshold (Mbps)
G.now1	●	Disabled	Disabled
G.now2	●	Disabled	Disabled
G.now3	●	Disabled	Disabled
G.now4	●	Disabled	Disabled

Port：Port number

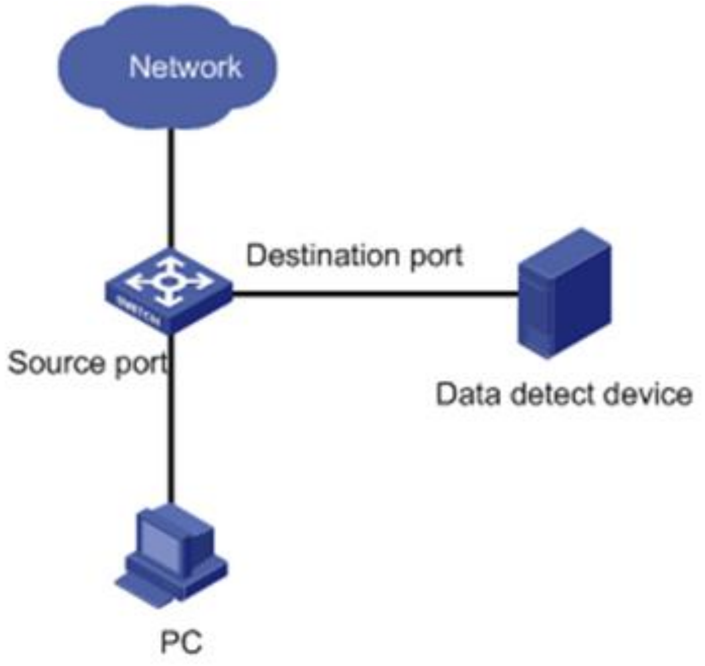
Rx Speed Threshold：Rx Speed Threshold（0=Disable）

Tx Speed Threshold：Tx Speed Threshold（0=Disable）

Alarm：Red is on if alarm occurs; Green is on if there is no alarm.

3.8.3 Port Mirroring

Port mirroring refers to the process of copying the packets received or sent by the specified port to the destination port for packet analysis and monitoring. Generally, a destination port is connected to a data detect device, which users can use to analyze the mirrored packets for monitoring and troubleshooting the network, shown as the following figure:



Configuration steps:

Step 1 Enable/disable mirroring state;

Step 2 If mirroring state is enabled, choose a port as the monitoring port;

⚠ Caution:

- Monitoring port cannot be link-aggregration port;
- Only one port can be selected as monitoring port;
- Monitoring port cannot be mirroring port at the same time.

Step 3 Select the mirroring ports and whether the packets to be mirrored are Rx, Tx or both Rx /Tx.

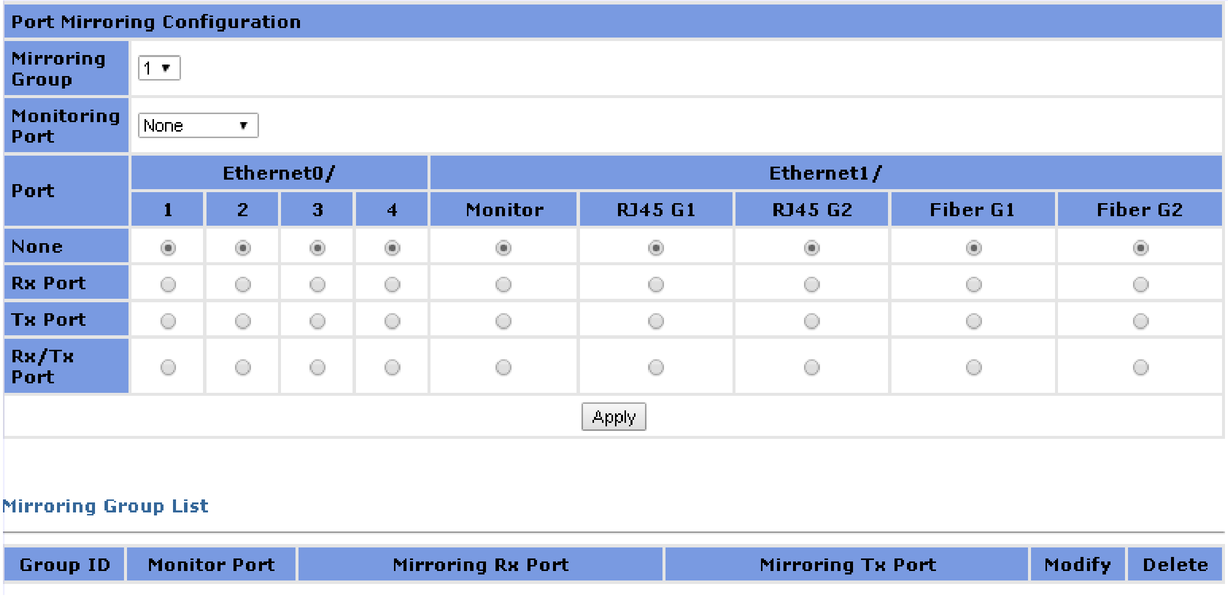
None: Means to mirror none packets on the port;

Rx Port: Means only to mirror the packets received by the port;

Tx Port: Means only to mirror the packets sent by the port;

Rx /Tx Port: Means to mirror the packets received and sent by the port.

Step 4 Click <Apply> to make it effective.



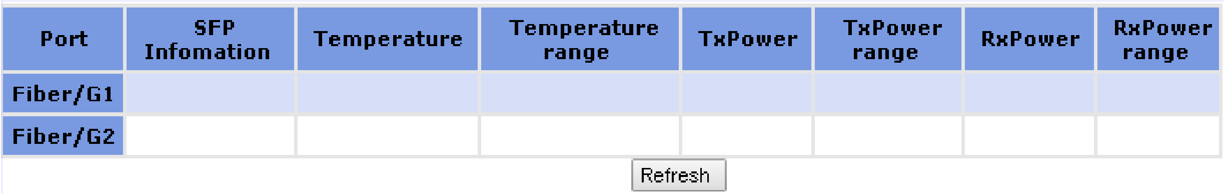
Port Mirroring Configuration									
Mirroring Group	1 ▾								
Monitoring Port	None ▾								
Port	Ethernet0/				Ethernet1/				
	1	2	3	4	Monitor	RJ45 G1	RJ45 G2	Fiber G1	Fiber G2
None	●	●	●	●	●	●	●	●	●
Rx Port	○	○	○	○	○	○	○	○	○
Tx Port	○	○	○	○	○	○	○	○	○
Rx/Tx Port	○	○	○	○	○	○	○	○	○

Mirroring Group List

Group ID	Monitor Port	Mirroring Rx Port	Mirroring Tx Port	Modify	Delete

3.8.4 Port SFP Information

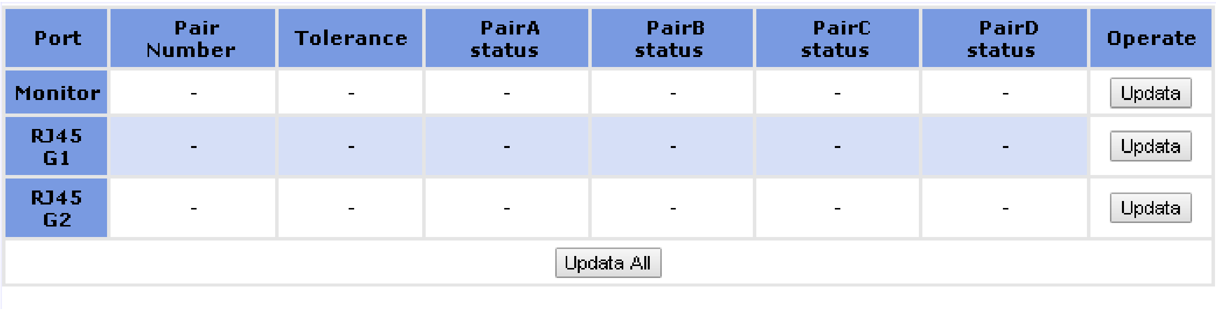
This page shows the optical module information



Port	SFP Infomation	Temperature	Temperature range	TxPower	TxPower range	RxPower	RxPower range
Fiber/G1							
Fiber/G2							

3.8.5 Port Cable Diag

This page shows the port cable diagnosis information



Port	Pair Number	Tolerance	PairA status	PairB status	PairC status	PairD status	Operate
Monitor	-	-	-	-	-	-	Updata
RJ45 G1	-	-	-	-	-	-	Updata
RJ45 G2	-	-	-	-	-	-	Updata

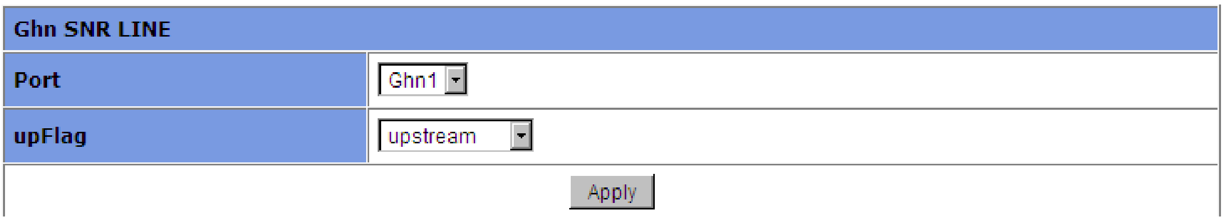
3.8.6 Ghn snr

This page will show Ghn snr Graph**Configuration steps:**

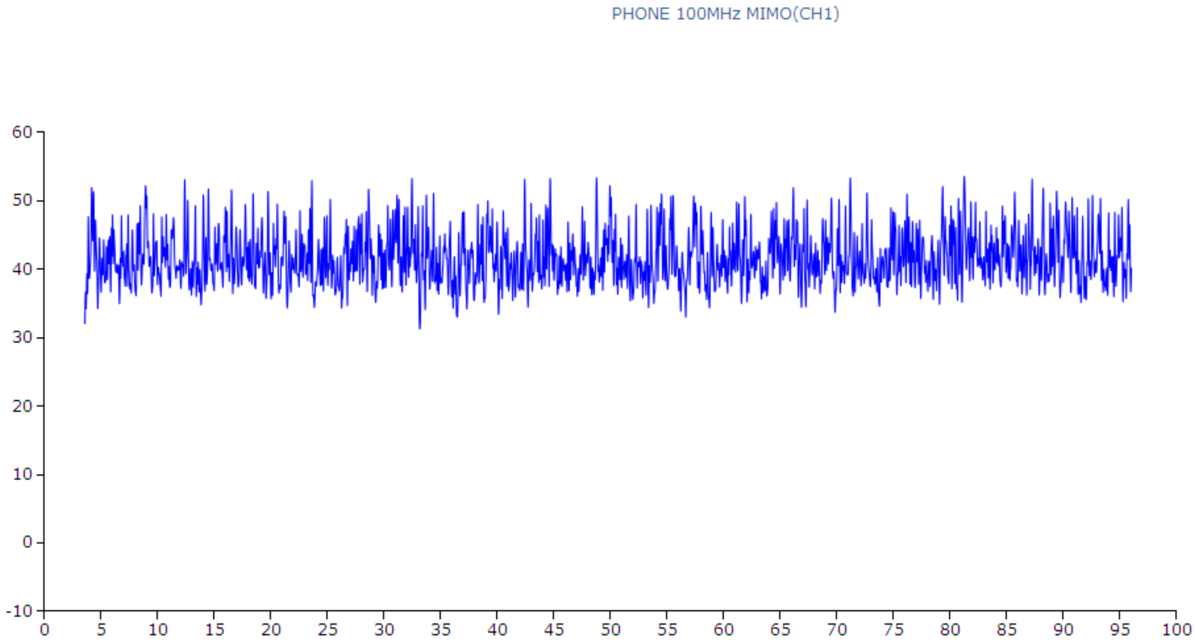
Step 1 Configurate PC, Switch, designated Ghn local-end, and different IP in the same network segment of GhnGhn remote-end connected with the designated GhnGhn local-end.

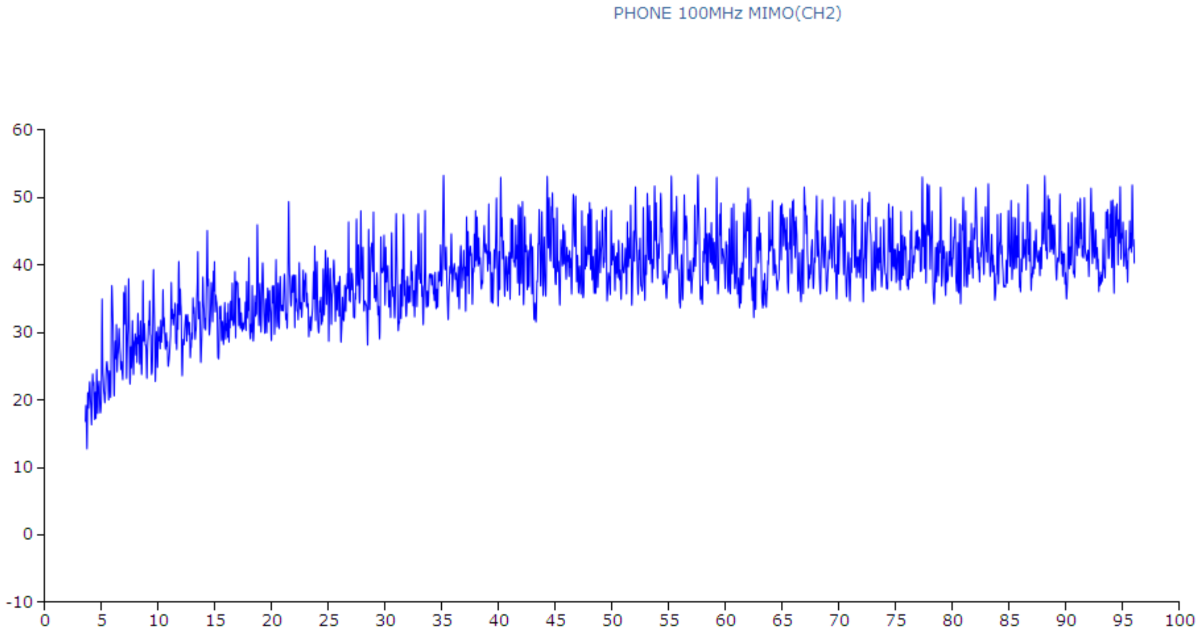
Step 2 show SNR Graph.of the designated Ghn port downstream or Upstream.

Step 3 Click <Apply> to make it effective.



Ghn SNR LINE	
Port	Ghn1
upFlag	upstream





3.9 SNMP Manager

The Simple Network Management Protocol (SNMP) is an Internet standard protocol used to transmit network management information between any two devices. It enables network administrators to read and set the variables on managed devices, diagnose network problems, plan for network capacity, and create reports.

SNMP employs a polling mechanism. It offers an essential set of features, and is especially suitable for small, fast, and low-cost networks. SNMP is based on the connectionless protocol UDP in the transport layer; therefore, it can easily manage devices on a network regardless of their vendors and interconnect technologies.

SNMP consists of two components:

- NMS (Network Management System) is the software that runs on the managing device, such as a switch.
- Agent is the software that runs on the managed device.

The NMS sends GetRequest, GetNextRequest, or SetRequest to an Agent. On receiving a request from NMS, the Agent performs Read or Write operation to MIB (Management Information Base), depending on the type of the request. It then creates and returns a Response to NMS.

Agent sends a Trap to notify NMS of a critical event or change in status, such as reset.

The SNMP Agent on the switch supports SNMP v1, SNMP v2c, and SNMP v3.

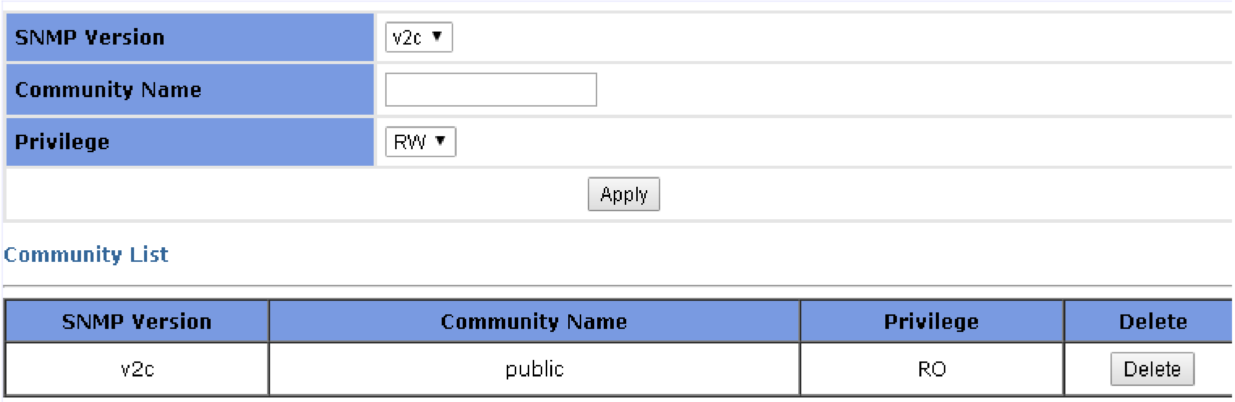
SNMP v3 performs authentication based on user name and password.

SNMP v1 and SNMP v2c performs authentication based on Community Name. SNMP packets will be discarded if the community name fails to be authenticated. SNMP's community is a relationship between an NMS and an agent. The community name is used like a password to authenticate SNMP NMS's access to the SNMP Agent on the switch. Users can set up one or more of the following attributes of a community name:

- Define the MIB view that can be accessed by the community.
- Set the access privilege for MIB objects to be write and/or read. A read-only community can only query MIBs for information about the switch. A read-write community is also capable of configuring the switch.
- Configure the basic ACL for a community.

3.9.1 SNMP Community

You can specify SNMP version (v1 or v2c), community name, and access privilege (RO or RW) on this page.



SNMP Version	v2c ▼
Community Name	
Privilege	RW ▼

Community List

SNMP Version	Community Name	Privilege	Delete
v2c	public	RO	Delete

SNMP Version

v1 To create a SNMPv1 user.

v2c To create a SNMPv2c user.

Community Name The name of the community. It is a string with 3 to 16 characters

Access Privilege The rights to read and/or write

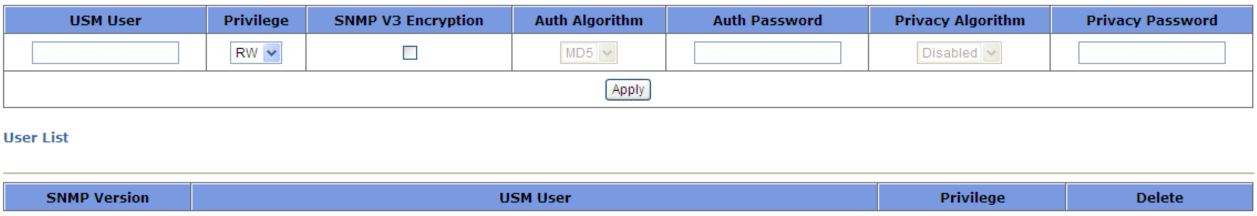
RO The community has read-only privilege of MIB objects. This type of communities can only query MIBs for device information.

RW The community has read-write privilege of MIB objects. This type of communities is capable of configuring devices.

The lower part of this page shows the configuration of the existing SNMP v1 and SNMP 2c communities, including their SNMP versions, community names, and access privileges. These communities can be deleted.

3.9.2 SNMP User

On this page, you can create SNMP v3 USM users, set up their access privilege, SNMP v3 encapsulation, authentication algorithm, authentication password, privacy algorithm, and privacy password.



USM User	Privilege	SNMP V3 Encryption	Auth Algorithm	Auth Password	Privacy Algorithm	Privacy Password
	RW	□	MD5		Disabled	

User List

SNMP Version	USM User	Privilege	Delete

USM User The user name is a string of 3 to 16 characters.

Auth Algorithm Select the Authentication Algorithm for the SNMP v3 Use**r.** SNMP v3 encapsulation must be selected; otherwise, authentication and encryption cannot be implemented.

MD5 The authentication is performed via HMAC-MD5 algorithm.

SHA The authentication is performed via SHA (Secure Hash Algorithm). This authentication mode is of higher security than MD5 mode.

Auth Password: Type the password for authentication. It is a string of 9 to 15 characters in plain text, or a 32-bit hexadecimal number in cipher text if MD5 algorithm is used, or a 40-bit hexadecimal number in cipher text if SHA algorithm is used.

Privacy Algorithm: Select the Privacy Algorithm for the SNMP v3 User.

DES DES encryption method is used.

AES AES encryption method is used. AEC is of higher security than DES.

Privacy Password Type the privacy password. It is a string of 9 to 15 characters in plain text, or a 32-bit hexadecimal number in cipher text if MD5 algorithm is used, or a 40-bit hexadecimal number in cipher text if SHA algorithm is used.

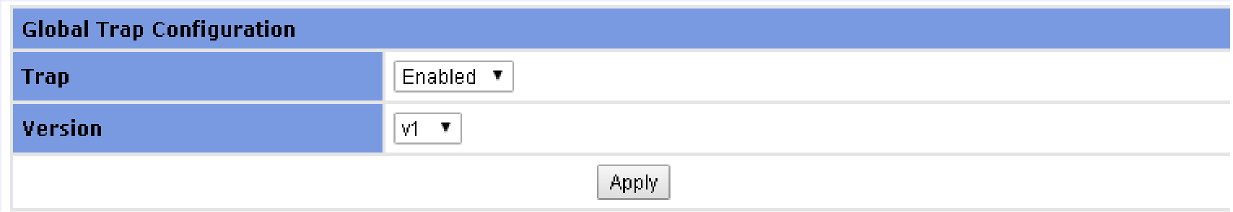
The lower part of this page shows the configuration of all existing SNMP v3 USM users, including their SNMP Version, USM User, and Privilege. These USM users can be deleted.

3.9.3 SNMP Trap

There are three tab pages: Global Trap, Trap Host IP, and Trap Port.

3.9.3.1 Global Trap

You can enable or disable traps globally. By default, traps are enabled globally.

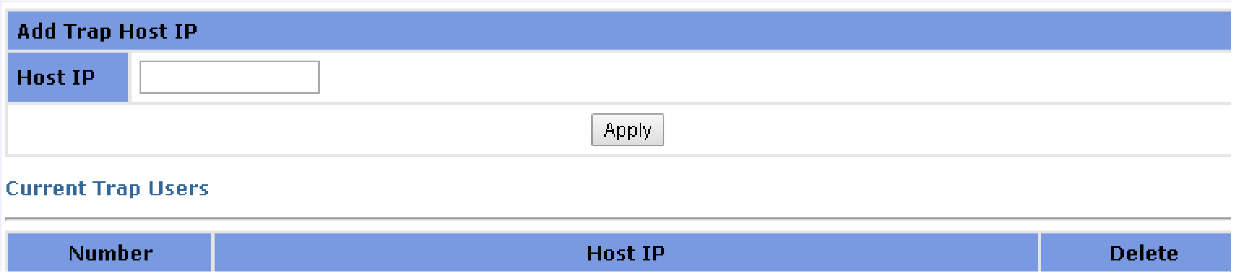


Global Trap Configuration	
Trap	Enabled ▼
Version	v1 ▼

3.9.3.2 Trap Host IP

This tab page specifies SNMP trap host IP. Host IP is the IPv4 address of the host to receive the traps.

The lower part of this page lists all existing trap host IP addresses. They can be deleted.



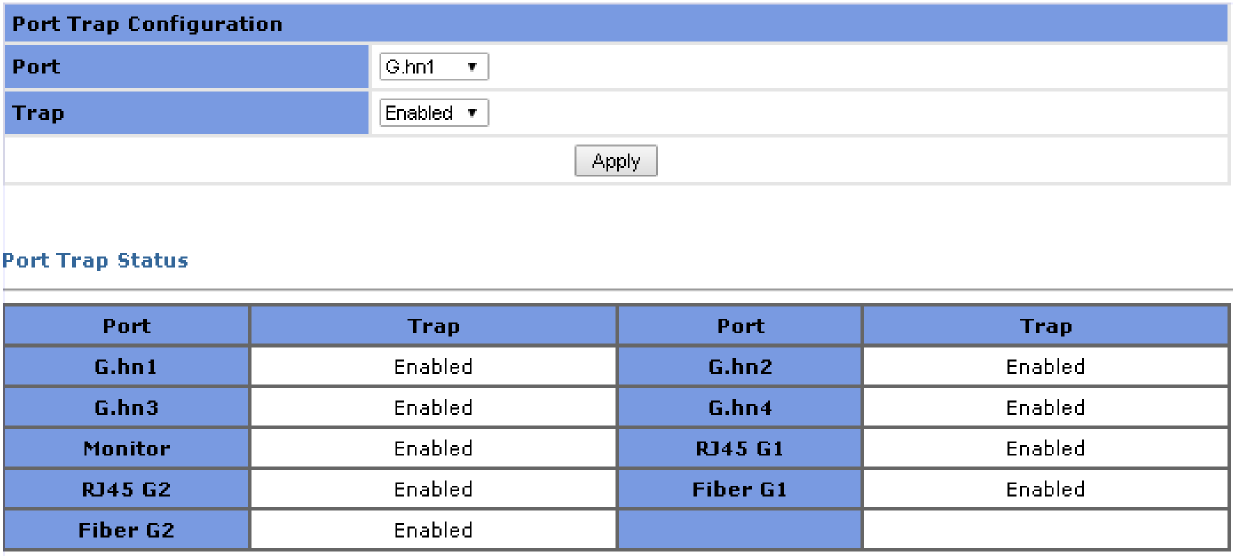
Add Trap Host IP	
Host IP	

Current Trap Users

Number	Host IP	Delete

3.9.3.3 Trap Port

Enable or disable the trap function for each port.
The lower part of this page lists the trap status of all ports.



Port Trap Configuration	
Port	G.hn1 ▼
Trap	Enabled ▼

Port Trap Status

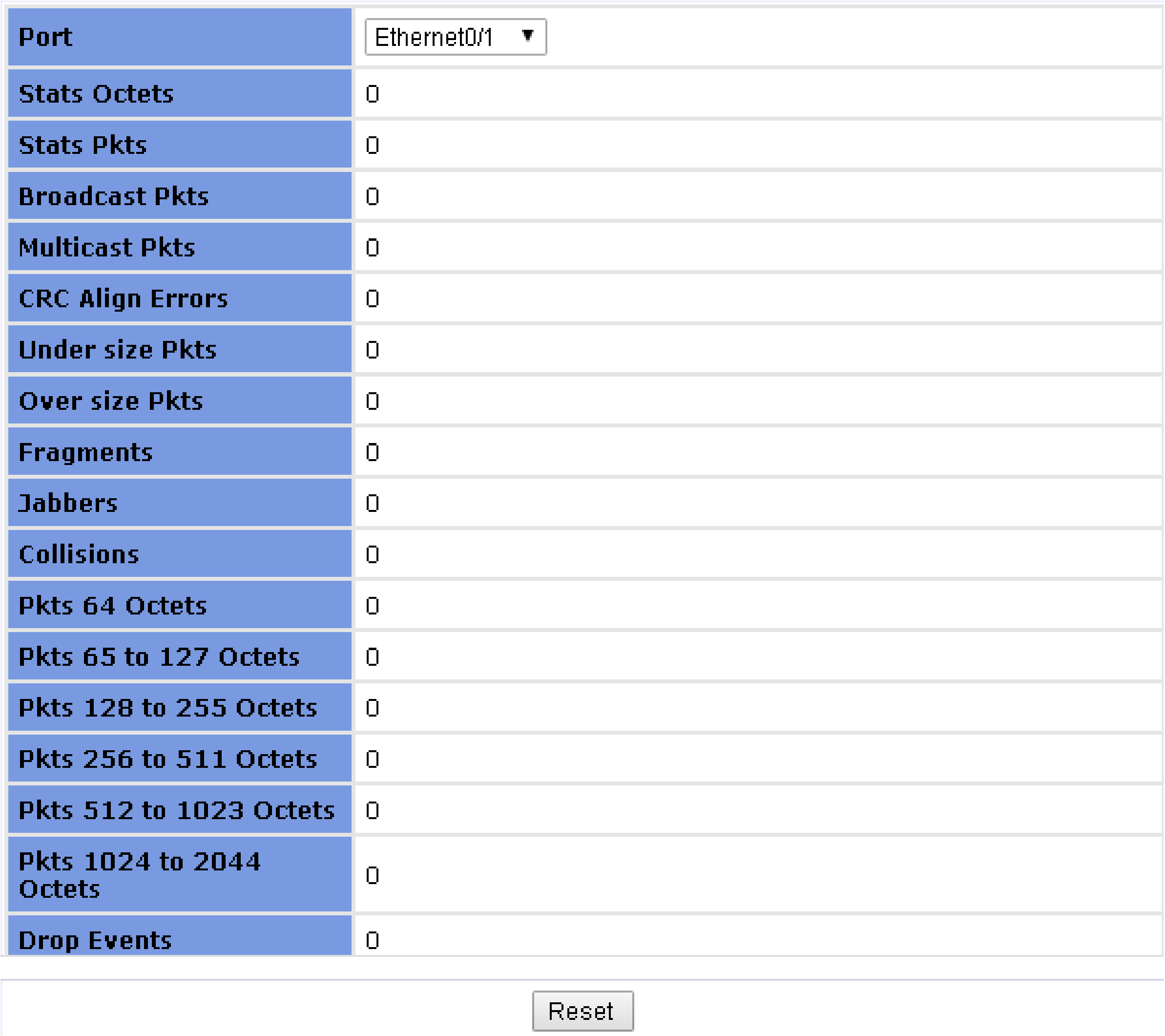
Port	Trap	Port	Trap
G.hn1	Enabled	G.hn2	Enabled
G.hn3	Enabled	G.hn4	Enabled
Monitor	Enabled	RJ45 G1	Enabled
RJ45 G2	Enabled	Fiber G1	Enabled
Fiber G2	Enabled		

3.10 RMON

Remote Monitoring (RMON) is used to realize the monitoring and management from the management devices to the managed devices on the network by implementing such functions as statistics and alarm. The statistics function enables a managed device to periodically or continuously track various traffic information on the network segments connecting to its ports, such as total number of received packets or total number of oversize packets received. The alarm function enables a managed device to monitor the value of a specified MIB variable, log the event and send a trap to the management device when the value reaches the threshold, such as the port rate reaches a certain value or the potion of broadcast packets received in the total packets reaches a certain value.

3.10.1 Statistic

This page shows the statistics of Stats Octets, Stats Pkts, Broadcastkts, MulticastPkts, CRC Align Errors, Under size Pkts, Over size Pkts, Fragments, Jabbers, Collisions, Pkts 64 Octets, Pkts 64 to 127 Octets, Pkts 128 to 255 Octets, Pkts 256 to 511 Octets, Pkts512 to 1023 Octets, Pkts1024 to 1518 Octets, and Drop Events of each ethernet port.



Port	Ethernet0/1 ▼
Stats Octets	0
Stats Pkts	0
Broadcast Pkts	0
Multicast Pkts	0
CRC Align Errors	0
Under size Pkts	0
Over size Pkts	0
Fragments	0
Jabbers	0
Collisions	0
Pkts 64 Octets	0
Pkts 65 to 127 Octets	0
Pkts 128 to 255 Octets	0
Pkts 256 to 511 Octets	0
Pkts 512 to 1023 Octets	0
Pkts 1024 to 2044 Octets	0
Drop Events	0

Stats Octets The total number of octets of received and sent data, including bad packets, received from network; it excludes framing bits but includes Frame Check Sequence (FCS) octets.

Stats Pkts The total number of packets received and sent, including bad packets, broadcast packets and multicast packets.

Broadcastkts The total number of the received good packets that are directed to the broadcast address, except the multicast packets.

MulticastPkts The total number of the received good packets that are directed to a multicast address, except the packets directed to the broadcast address.

CRC Align Errors The total number of the received packets that has a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets (both inclusive), and has either a bad FCS with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).

Under size Pkts The total number of the received packets that are less than 64 octets long (excluding framing bits, but including FCS octets).

Over size Pkts The total number of the received packets that are longer than 1518 octets (excluding framing bits, but including FCS octets).

Fragments The total number of the received packets that are less than 64 octets in length (excluding framing bits, but including FCS octets), and has either a bad FCS with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).

Jabbers The total number of the received packets that are longer than 1518 octets (excluding framing bits, but including FCS octets), and has either a bad FCS with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).

Collisions The best estimate of the total number of collisions on this Ethernet segment.

Pkts 64 Octets The total number of received packets, that are 64 octets in length (excluding framing bits, but including FCS octets), including bad packets.

Pkts 65 to 127 Octets The total number of received packets, that are between 65 and 127 octets in length inclusive (excluding framing bits, but including FCS octets), including bad packets.

Pkts 128 to 255 Octets The total number of received packets, that are between 128 and 255 octets in length inclusive (excluding framing bits, but including FCS octets), including bad packets.

Pkts 256 to 511 Octets The total number of packets, including bad packets, received that are between 256 and 511 octets in length inclusive (excluding framing bits, but including FCS octets).

Pkts 512 to 1023 Octets The total number of received packets, that are between 512 and 1023 octets in length inclusive (excluding framing bits, but including FCS octets), including bad packets.

Pkts 1024 to 1518 Octets The total number of received packets, that are between 102 4 and 1518 octets in length inclusive (excluding framing bits, but including FCS octets), including bad packets.

Drop Events The total number of events when packets are dropped by the probe due to lack of resources.

3.10.2 History

3.10.2.1 History control

This page sets a history control entry on each port. And then the port will be sampled with the specified interval and the specified sample number about its transmitting situation.

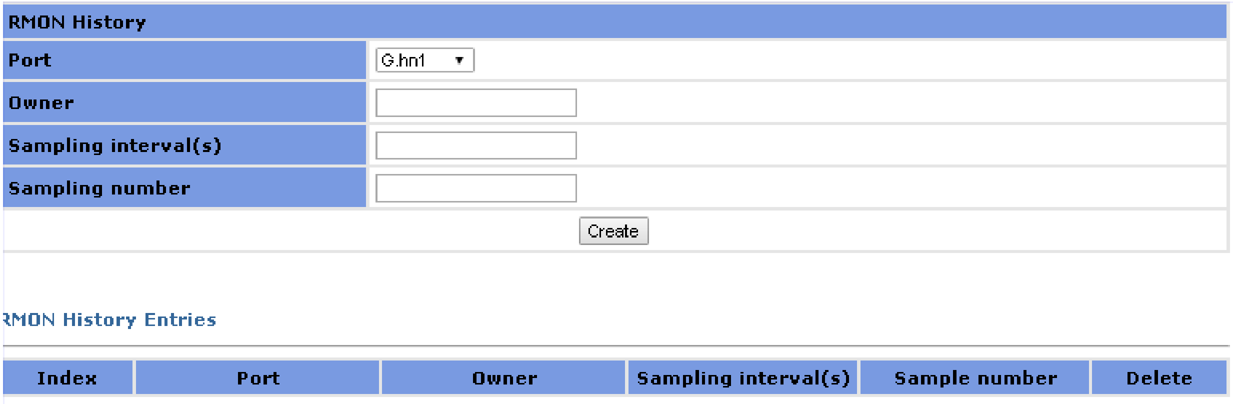
Port The Ethernet port for collecting statistics.

Owner The entity that configured this entry and is therefore using the resources assigned to it.

Sampling interval(s) The data sample time interval of each group. The interval range is from 1 and 3600(1 hour).

Sampling number The number of discrete sampling intervals over which data shall be saved in the part of the media-specific table associated with this history control entry.

The lower part of the interface will list the RMON history entries, which can be deleted.



RMON History

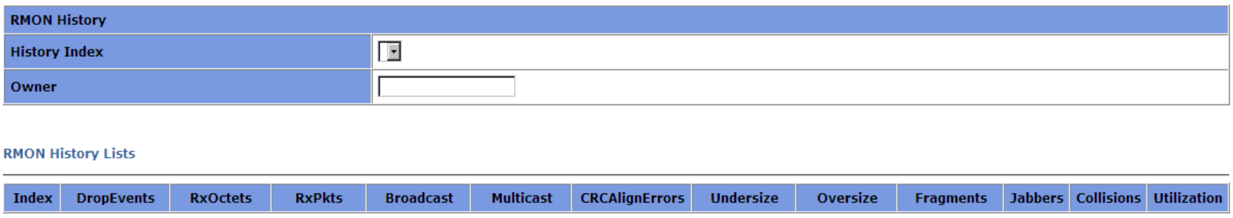
Port	G.hn1 ▾
Owner	
Sampling interval(s)	
Sampling number	

RMON History Entries

Index	Port	Owner	Sampling interval(s)	Sample number	Delete

3.10.2.2 History List

On this page, one of the history can be selected to show the relate statistics.



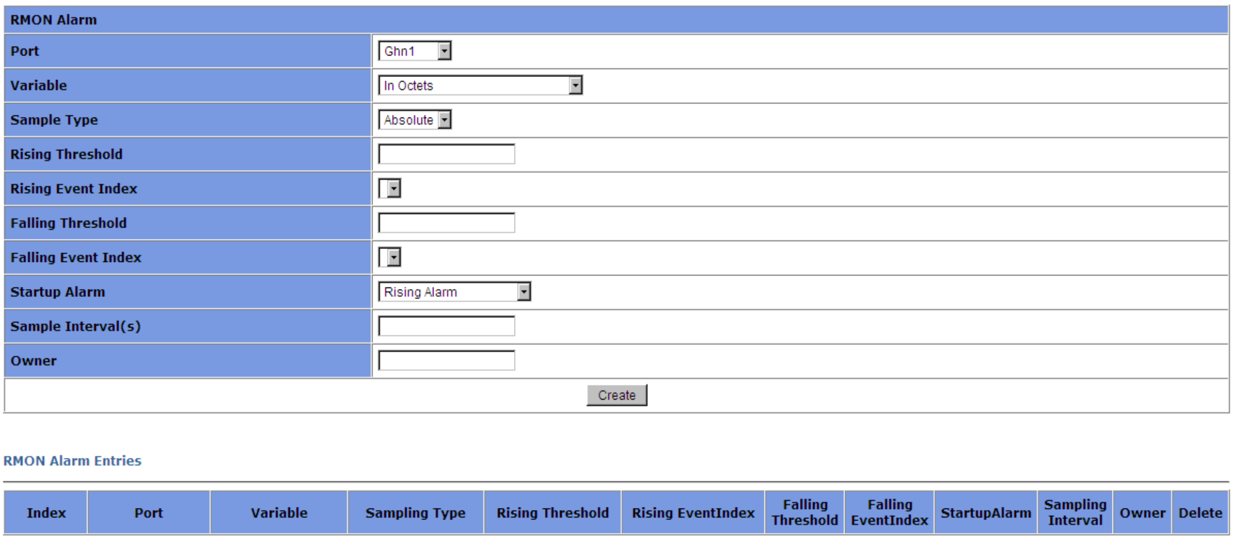
RMON History	
History Index	
Owner	

RMON History Lists

Index	DropEvents	RxOctets	RxPkts	Broadcast	Multicast	CRCAlignErrors	Undersize	Oversize	Fragments	Jabbers	Collisions	Utilization

3.10.3 Alarm

This page sets an alarm entry.



RMON Alarm	
Port	Ghn1
Variable	In Octets
Sample Type	Absolute
Rising Threshold	
Rising Event Index	
Falling Threshold	
Falling Event Index	
Startup Alarm	Rising Alarm
Sample Interval(s)	
Owner	

RMON Alarm Entries

Index	Port	Variable	Sampling Type	Rising Threshold	Rising EventIndex	Falling Threshold	Falling EventIndex	StartupAlarm	Sampling Interval	Owner	Delete

Port: The Ethernet port to collect statistics of **Variable**.

Variable: The drop-down list includes In Octets, In Unicast Pks, In None Unicast Pks,

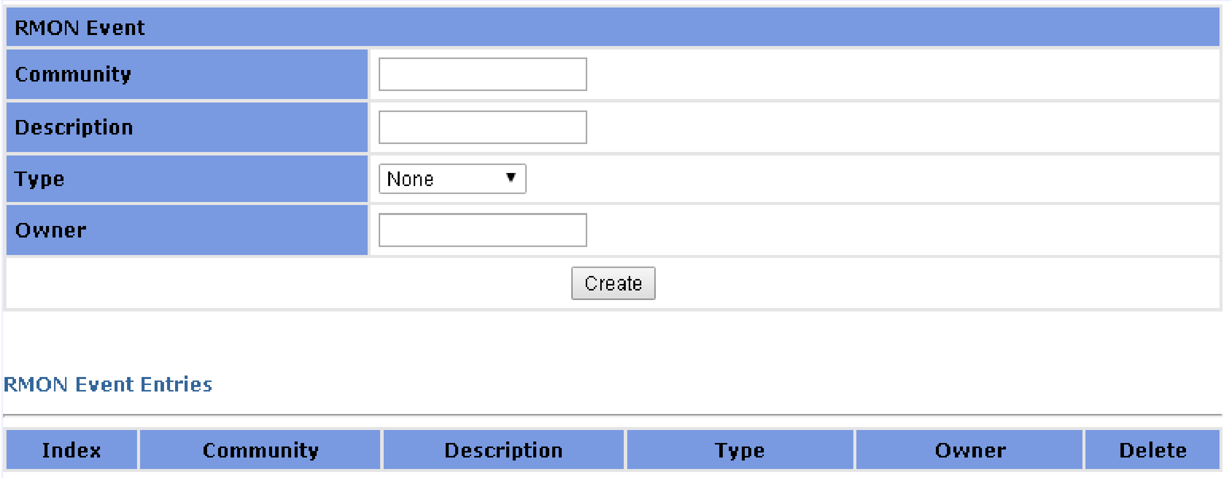
In Discarded Pks, In Error Pks, In Unknown Protocol Pks, Out Octets, Out Unicast Pks, Out None Unicast Pks, Out Discarded Pks, Out Error Pks, RMON Drop Events, RMON Received Octets, RMON Received Pks, RMON Broadcast Pks, RMON Multicast Pks, RMON CRC Align Pks, RMON Undersize Pks, RMON Oversize Pks, RMON Fragments, RMON Jabbers, RMON Collisions, 64 Octets Pks, 65 to 127 Octets Pks, 128 to 255 Octets Pks, 256 to 511 Octets Pks, 512 to 1023 Octets Pks, 1024 to 1518 Octets Pks, In Dot1d Topology Port Frames, Out Dot1d Topology Port Frames and In Dot1d Topology Discards.

Sample Type: Sets the type of sampling, the method of sampling the selected variable and calculating the value to be compared against the thresholds is as follows: If the value of this object is absoluteValue (1), the value of the selected variable will be compared directly with the thresholds at the end of the sampling interval. If the value of this object is deltaValue (2), the value of the selected variable at the last sample will be subtracted from the current value, and the difference will be compared with the thresholds.

3.10.4 Event

The event group defines event indexes and controls the generation and notifications of the events triggered by the alarms defined in the alarm group.

3.10.4.1 Event



RMON Event	
Community	
Description	
Type	None ▼
Owner	

RMON Event Entries

Index	Community	Description	Type	Owner	Delete

Configuration Steps:

Step 1 Specify the community. If an SNMP trap is to be sent, it will be sent to the SNMP community specified by this octet string.

Step 2 Add description

Step 3 Select type of notification that the probe makes about this event.

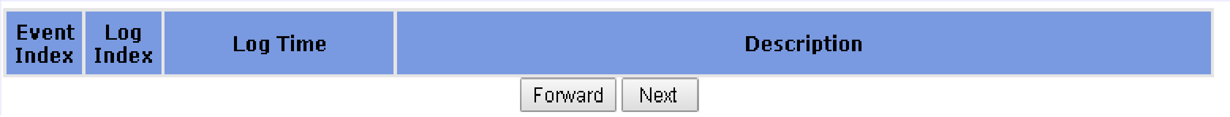
- **None**: No action;
- **Log** : The result will be shown in Event Log;
- **Trap**: The switch will send trap to the specified trap host
- **Log and trap**: The trap will be shown in Event Log and sent to the specified trap host.

Step 4 Specify the owner for available management in Event Log.

Step 5 Click <Create>. The bottom part of this tab page lists all existing event entries.

3.10.4.2 Event Log

This page shows information about event log entries, including **Event Index**, **Log Index**, **Log Time** and **Description**.



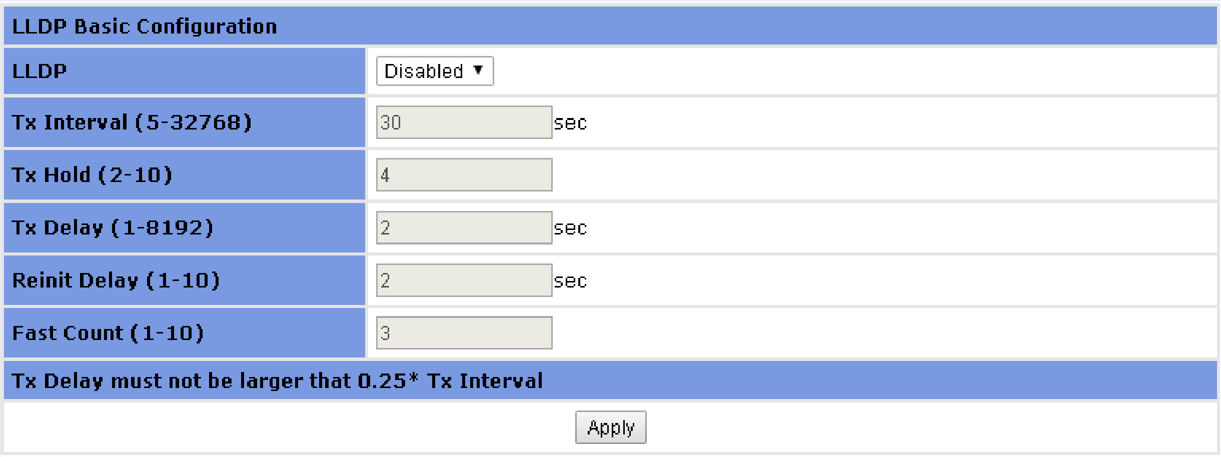
Event Index	Log Index	Log Time	Description

3.11 LLDP

3.11.1 Configuration

3.11.1.1 Basic

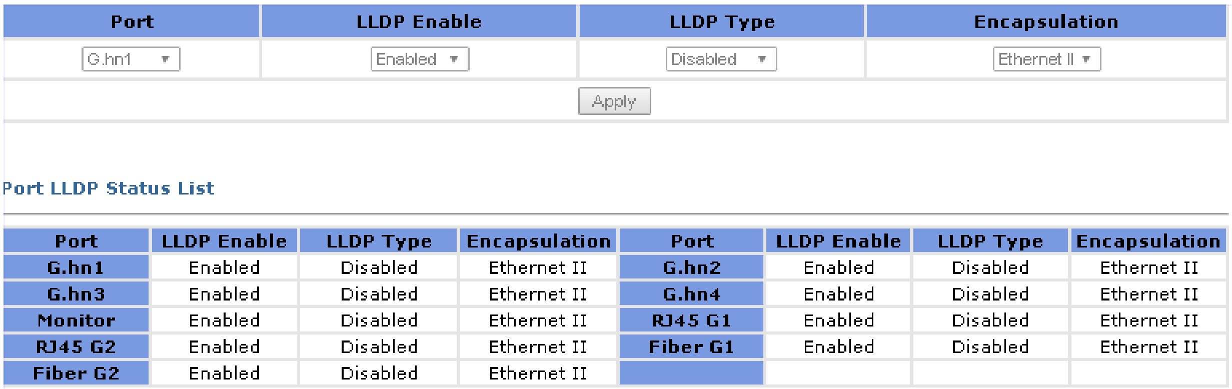
This page sets lldp enable or disabled



LLDP Basic Configuration	
LLDP	Disabled ▼
Tx Interval (5-32768)	30 sec
Tx Hold (2-10)	4
Tx Delay (1-8192)	2 sec
Reinit Delay (1-10)	2 sec
Fast Count (1-10)	3
Tx Delay must not be larger that 0.25* Tx Interval	

3.11.1.2 Ports

This page configures **LLDP Enable**, sets transmit **LLDP Status** mode to be **Disabled**, **Rx and Tx, Tx only,** or **Rx only**; and specifies the LLDP **Encapsulation** to be **ethernetII** or **SNAP** for a given Ethernet port.



Port	LLDP Enable	LLDP Type	Encapsulation
G.hn1 ▼	Enabled ▼	Disabled ▼	Ethernet II ▼

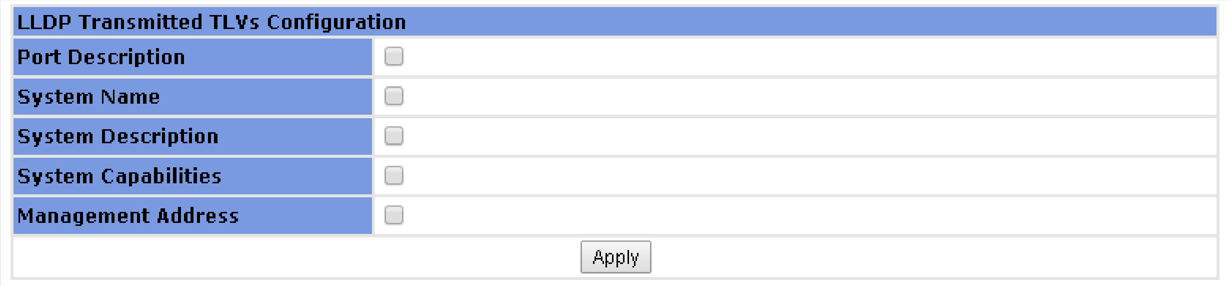
Port LLDP Status List

Port	LLDP Enable	LLDP Type	Encapsulation	Port	LLDP Enable	LLDP Type	Encapsulation
G.hn1	Enabled	Disabled	Ethernet II	G.hn2	Enabled	Disabled	Ethernet II
G.hn3	Enabled	Disabled	Ethernet II	G.hn4	Enabled	Disabled	Ethernet II
Monitor	Enabled	Disabled	Ethernet II	RJ45 G1	Enabled	Disabled	Ethernet II
RJ45 G2	Enabled	Disabled	Ethernet II	Fiber G1	Enabled	Disabled	Ethernet II
Fiber G2	Enabled	Disabled	Ethernet II				

EthernetII: the Ethernet frame of type 0x88cc.
SNAP: the Ethernet frame of type 0xAAAA-0300-0000-88CC.

3.11.1.3 TLVs

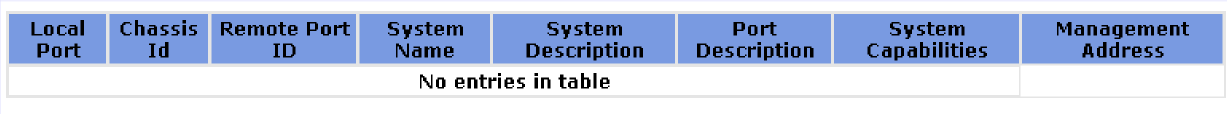
This page sets the type of transmitting information: **Port Description, System Name, System Description, System Capability,** and **Management Address**.



LLDP Transmitted TLVs Configuration	
Port Description	□
System Name	□
System Description	□
System Capabilities	□
Management Address	□

3.11.2 Neighbor

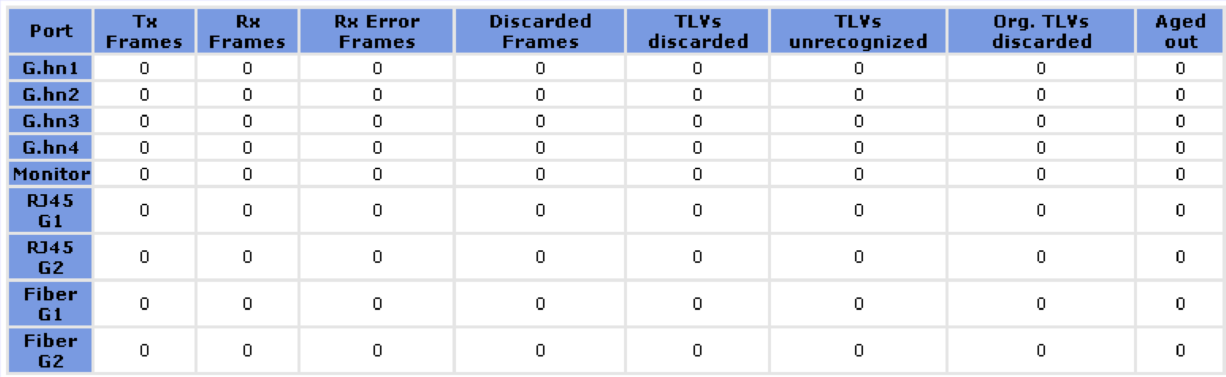
This page shows the **Local Port, Chassis Id** of a local device**,** and the **Remote Port ID, System name, Port description, System Capabilities**, and **Management Address** of a neighbor device.



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

3.11.3 Statistics

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

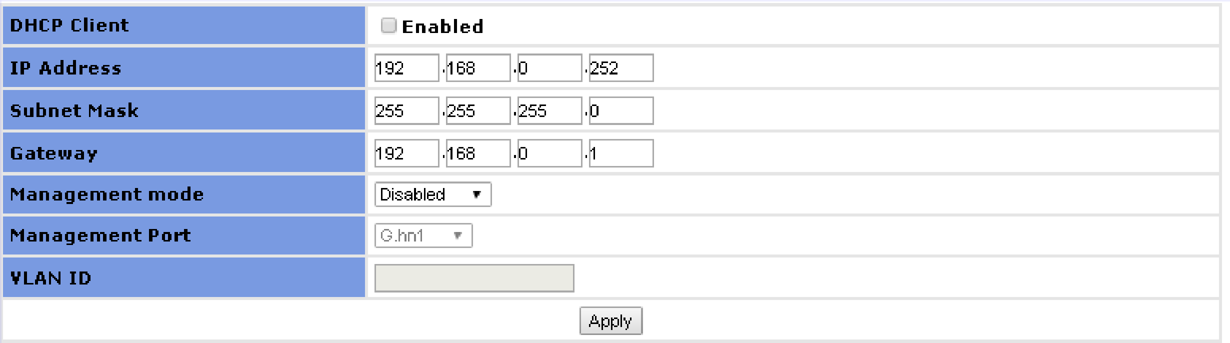


Port	Tx Frames	Rx Frames	Rx Error Frames	Discarded Frames	TLVs discarded	TLVs unrecognized	Org. TLVs discarded	Aged out
G.hn1	0	0	0	0	0	0	0	0
G.hn2	0	0	0	0	0	0	0	0
G.hn3	0	0	0	0	0	0	0	0
G.hn4	0	0	0	0	0	0	0	0
Monitor	0	0	0	0	0	0	0	0
RJ45 G1	0	0	0	0	0	0	0	0
RJ45 G2	0	0	0	0	0	0	0	0
Fiber G1	0	0	0	0	0	0	0	0
Fiber G2	0	0	0	0	0	0	0	0

3.12 Administration

3.12.1 IP Configuration

The switch supports DHCP and Static IP. **DHCP Client** can be enabled by checking the **Enabled** checkbox. To use static IP, the **IP Address**, **Subnet Mask**, and **Gateway** can be specified.

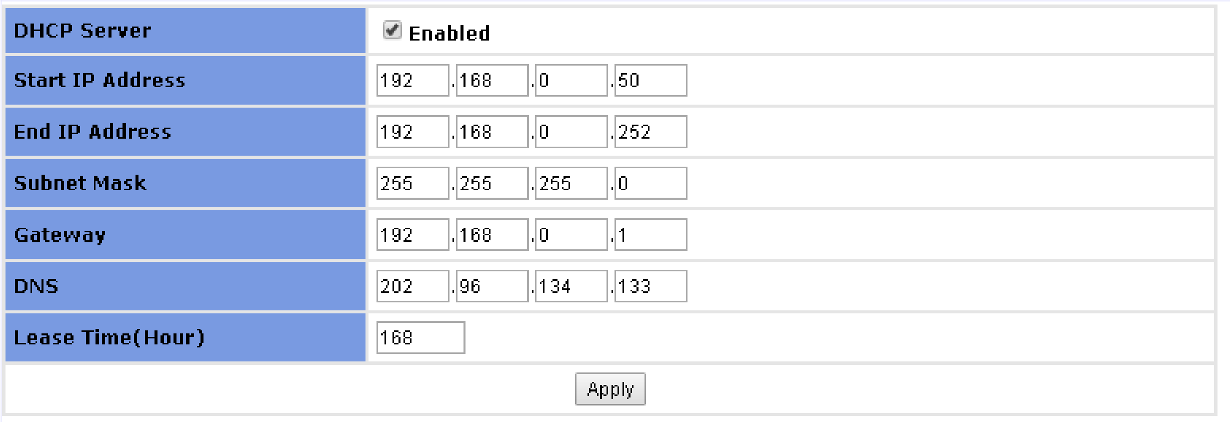


DHCP Client	□ Enabled
IP Address	192 . 168 . 0 . 252
Subnet Mask	255 . 255 . 255 . 0
Gateway	192 . 168 . 0 . 1
Management mode	Disabled ▾
Management Port	G.hn1 ▾
VLAN ID	

3.12.2 DHCP Server

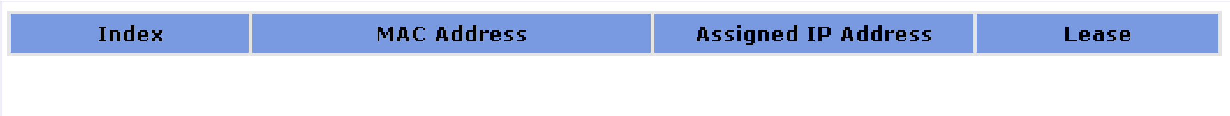
3.12.2.1 Configuration

This page sets dhcp server information



DHCP Server	☑ Enabled
Start IP Address	192 .168 .0 .50
End IP Address	192 .168 .0 .252
Subnet Mask	255 .255 .255 .0
Gateway	192 .168 .0 .1
DNS	202 .96 .134 .133
Lease Time(Hour)	168

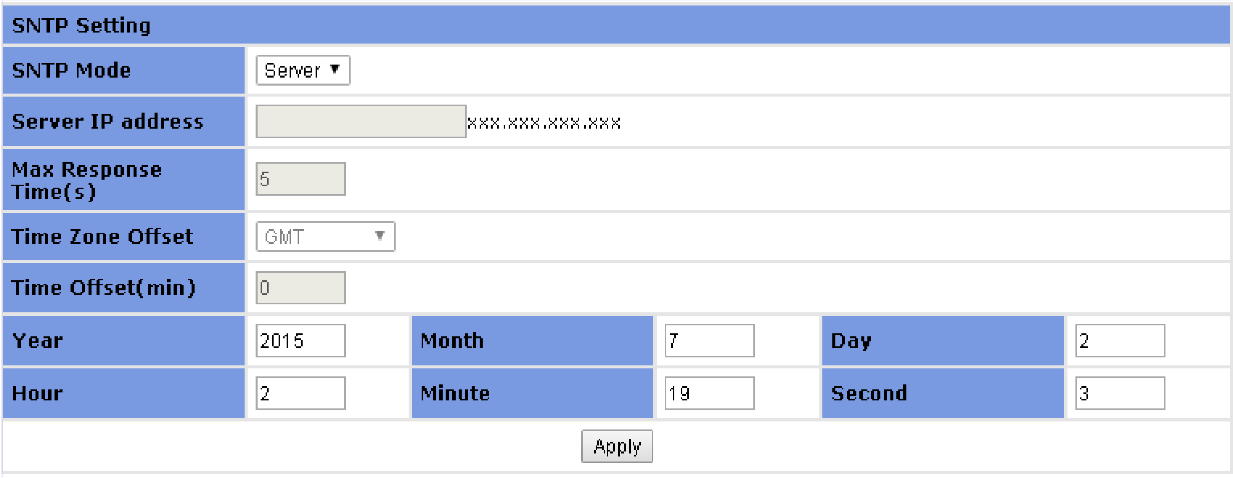
3.12.2.2 Client List



Index	MAC Address	Assigned IP Address	Lease

3.12.3 SNTP

An administrator is unable to keep time synchronized among all the devices within a network by changing the system clock on each device, because this is a significant amount of work and does not guarantee clock accuracy. NTP（Network Time Protocol) synchronizes timekeeping among distributed time servers and clients to ensure high clock accuracy.



SNTP Setting					
SNTP Mode	Server ▼				
Server IP address	xxx.xxx.xxx.xxx				
Max Response Time(s)	5				
Time Zone Offset	GMT ▼				
Time Offset(min)	0				
Year	2015	Month	7	Day	2
Hour	2	Minute	19	Second	3

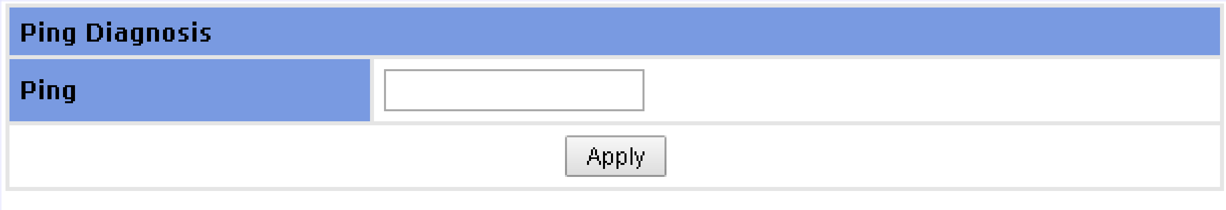
SNTP Mode Select Service mode or Client mode. If you select the Client mode, time synchronization on the switch can be achieved by sending a clock synchronization message to an SNTP server and receiving its reply.

Service IP address	IP address of the SNTP server
Response Time	Time interval in seconds for the switch to get a response from the SNTP server.
Time Zone Offset	Time difference between Greenwich standard time and local time.
Time Offset	Time difference in minutes between Greenwich standard time and local time.

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

3.12.4 Ping Diagnosis

On this page, an IP address can be pinged to check the connectivity between this switch and the IP.

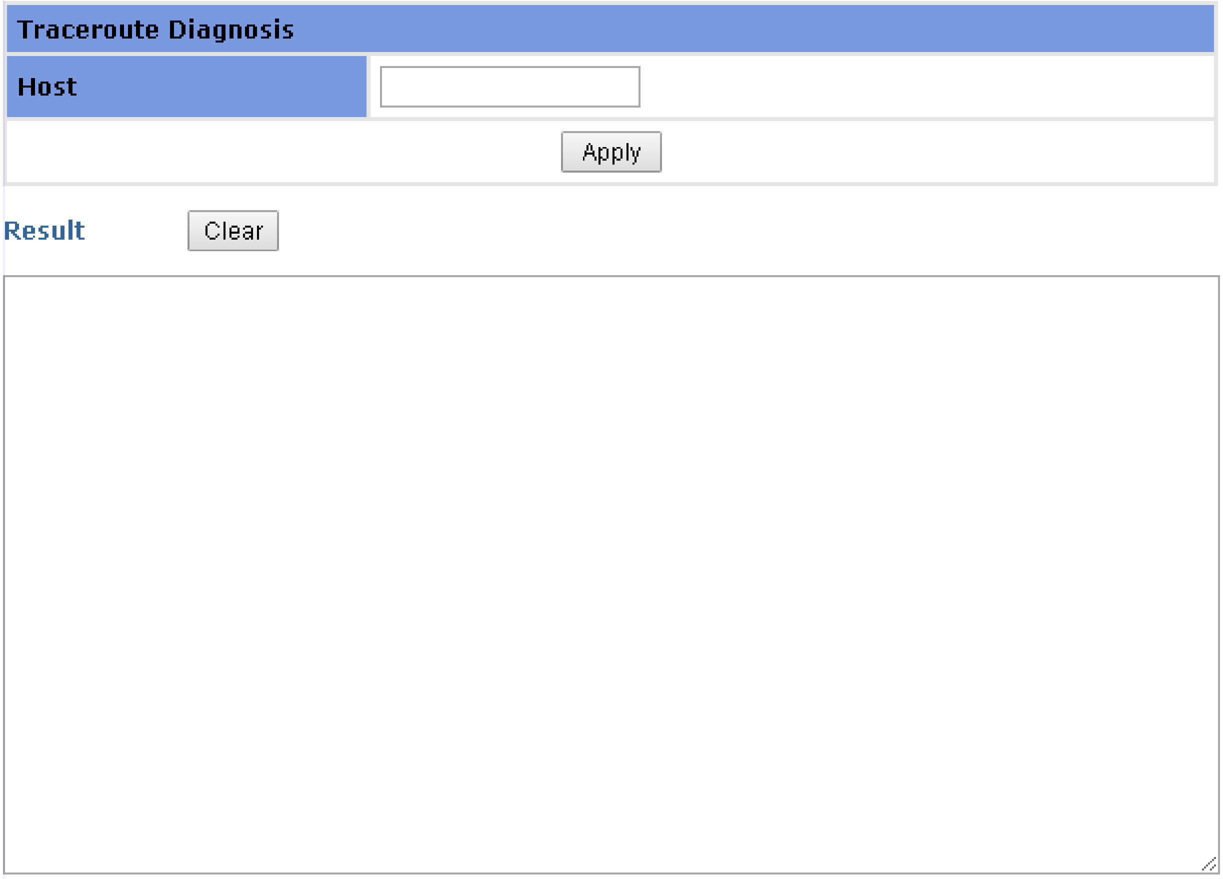


Ping Diagnosis

Ping:

3.12.5 Traceroute Diagnosis

On this page, an IP address can be tracert to check the router between this switch and the IP.



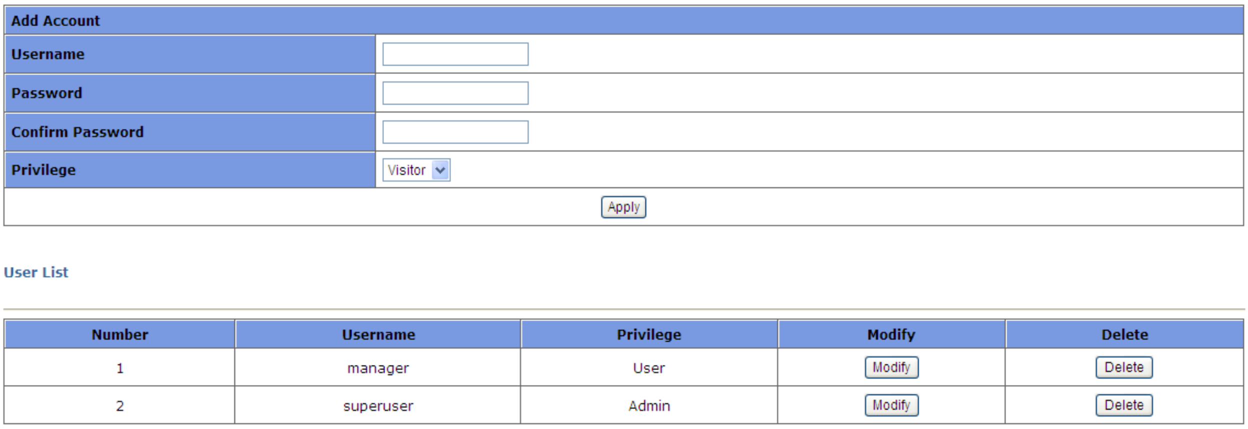
Traceroute Diagnosis	
Host	

3.12.6 Account

On this page, **Add Account** is used to add a new account. A set of specified **Username**, **Password** and **Privilege** for the new account shall be assigned.

Username: Username, a string of 3 to 16 characters.
Password: Password, a string of 1 to 16 characters.
Privilege: Includes **user** and **admin**.

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



Add Account	
Username	
Password	
Confirm Password	
Privilege	Visitor

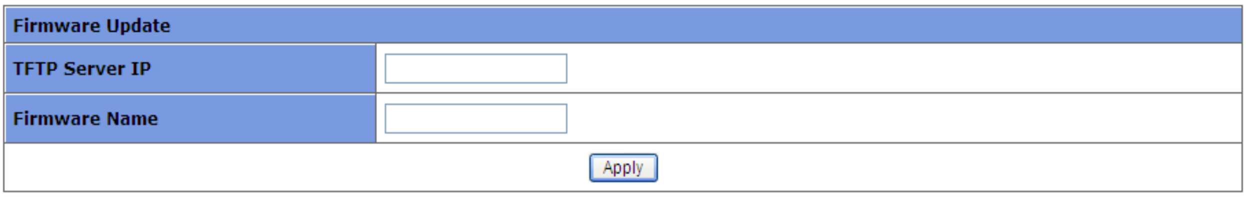
User List

Number	Username	Privilege	Modify	Delete
1	manager	User	Modify	Delete
2	superuser	Admin	Modify	Delete

3.12.7 Firmware Upgrade

3.12.7.1 Switch Firmware

This page sets **TFTP Server IP** and **Firmware Name**. Make sure the switch is connected to the TFTP server before clicking <Apply> to update the switch firmware.

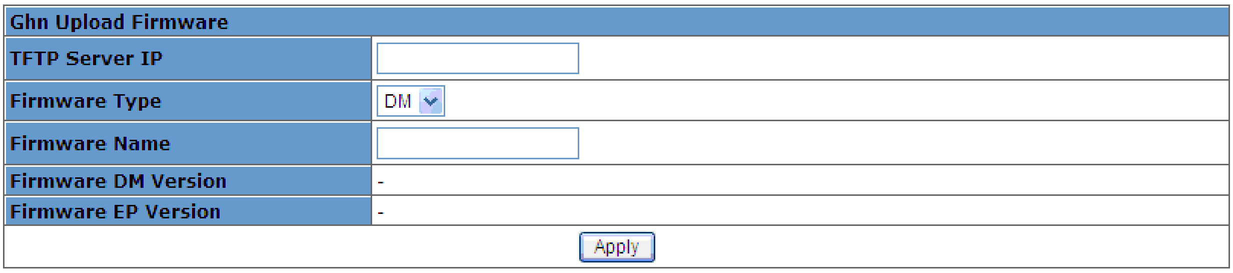


Firmware Update	
TFTP Server IP	
Firmware Name	
Apply	

3.12.7.2 Node Firmware

1) Firmare loader

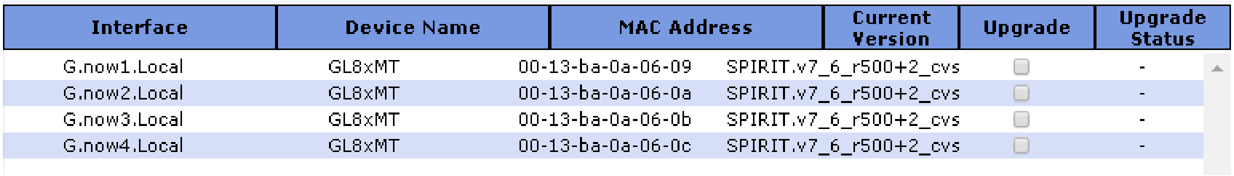
If you want to load local software, you must choose DM. If you want to load remote software, youmust choose EP. Then you can upgrade successfully. If you choose incorrectly or load wrong software, there will be a risk for Ghn device of failing to start.



Ghn Upload Firmware	
TFTP Server IP	
Firmware Type	DM
Firmware Name	
Firmware DM Version	-
Firmware EP Version	-
Apply	

2) Node upgrade

The selected devices will be upgraded firmware by this page.



Interface	Device Name	MAC Address	Current Version	Upgrade	Upgrade Status
G.now1.Local	GL8xMT	00-13-ba-0a-06-09	SPIRIT.v7_6_r500+2_cvs	□	-
G.now2.Local	GL8xMT	00-13-ba-0a-06-0a	SPIRIT.v7_6_r500+2_cvs	□	-
G.now3.Local	GL8xMT	00-13-ba-0a-06-0b	SPIRIT.v7_6_r500+2_cvs	□	-
G.now4.Local	GL8xMT	00-13-ba-0a-06-0c	SPIRIT.v7_6_r500+2_cvs	□	-

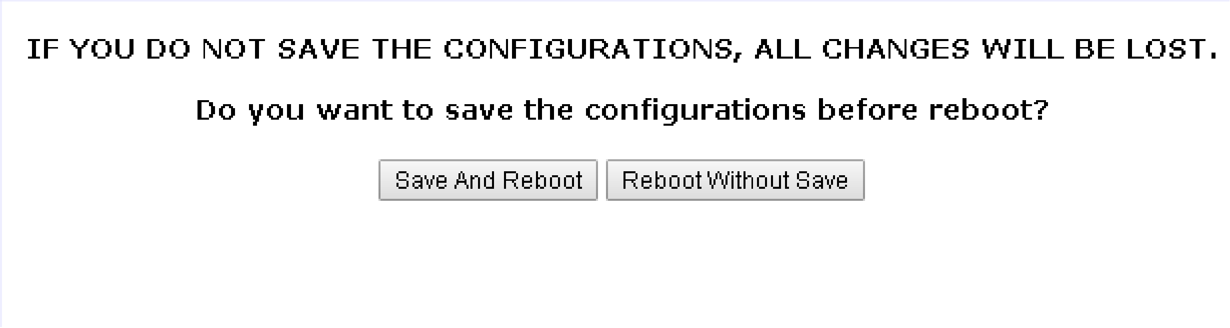
3.12.8 Reboot & Reset

3.12.8.1 Switch Reboot

There are two buttons on this page: <Save And Reboot>and <Reboot Without Save>.

Save And Reboot: To save current configuration and then reboot.

Reboot Without Save: To directly reboot without saving current configuration -- all changes may be lost.

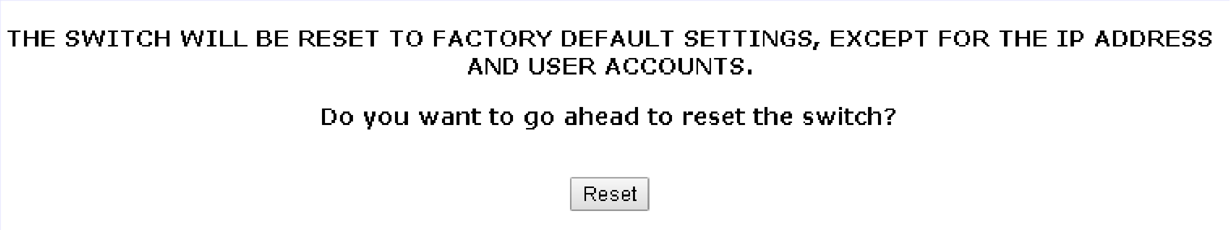


IF YOU DO NOT SAVE THE CONFIGURATIONS, ALL CHANGES WILL BE LOST.

Do you want to save the configurations before reboot?

3.12.8.2 Switch Reset

The switch will be reset to factory default setting, except for IP address and user accounts.

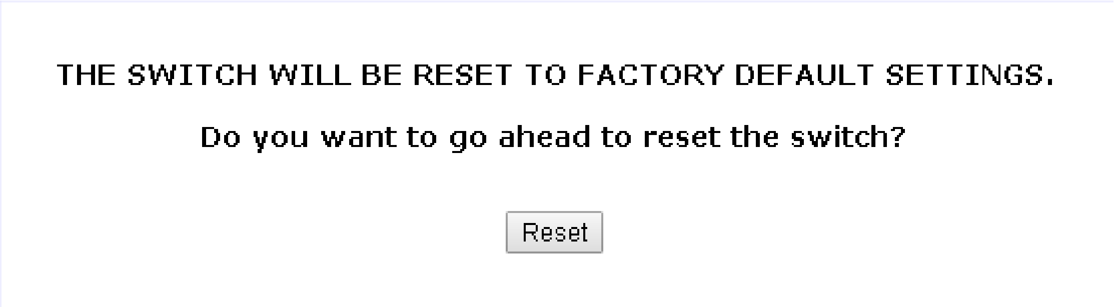


THE SWITCH WILL BE RESET TO FACTORY DEFAULT SETTINGS, EXCEPT FOR THE IP ADDRESS AND USER ACCOUNTS.

Do you want to go ahead to reset the switch?

3.12.8.3 Switch Reset to Default

The switch will be reset to factory default setting.

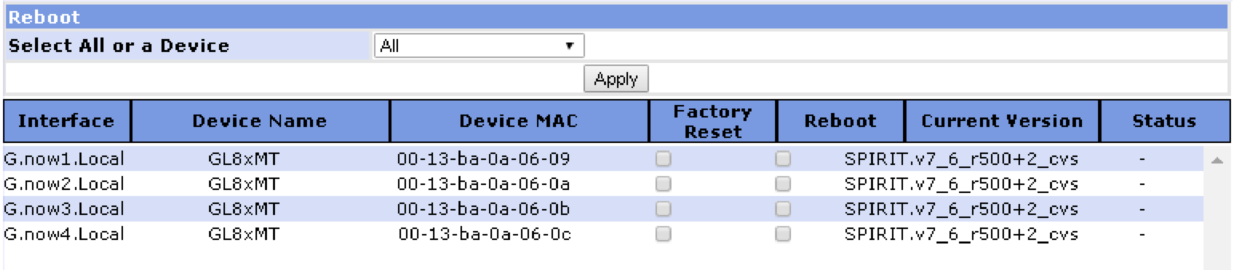


THE SWITCH WILL BE RESET TO FACTORY DEFAULT SETTINGS.

Do you want to go ahead to reset the switch?

3.12.8.4 Node Reboot & Reset

If you want to reboot specified device of system, the selected devices will be reboot by clicking<Apply> on this page.



Reboot

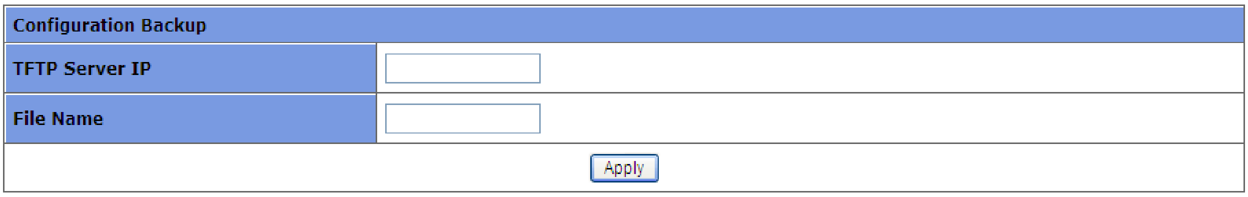
Select All or a Device: All ▾

Interface	Device Name	Device MAC	Factory Reset	Reboot	Current Version	Status
G.now1.Local	GL8xMT	00-13-ba-0a-06-09	☐	☐	SPIRIT.v7_6_r500+2_cvs	-
G.now2.Local	GL8xMT	00-13-ba-0a-06-0a	☐	☐	SPIRIT.v7_6_r500+2_cvs	-
G.now3.Local	GL8xMT	00-13-ba-0a-06-0b	☐	☐	SPIRIT.v7_6_r500+2_cvs	-
G.now4.Local	GL8xMT	00-13-ba-0a-06-0c	☐	☐	SPIRIT.v7_6_r500+2_cvs	-

3.12.9 Configuration Management

3.12.9.1 Backup Configuration

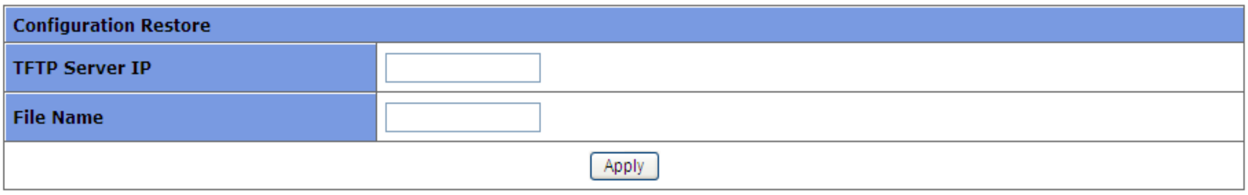
This page sets **TFTP Server IP** and **File Name**. Make sure the switch is connected to the TFTP server before clicking <Apply> to upload the switch configuration file specified in "**File Name**" to TFTP server.



Configuration Backup	
TFTP Server IP	
File Name	

3.12.9.2 Restore Configuration

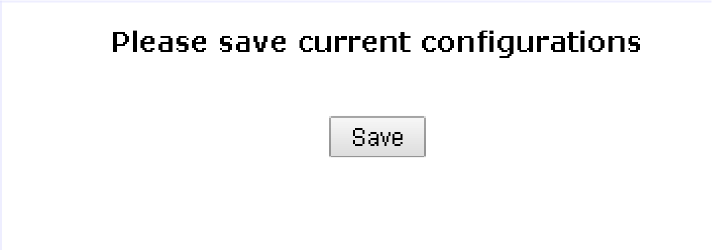
This page sets **TFTP Server IP** and **File Name**. Make sure the switch is connected to the TFTP server, and next click <Apply> to download the file specified in "**File Name**" from the TFTP server and use it as the configuration file for the switch.



Configuration Restore	
TFTP Server IP	
File Name	

3.12.10 Save Configuration

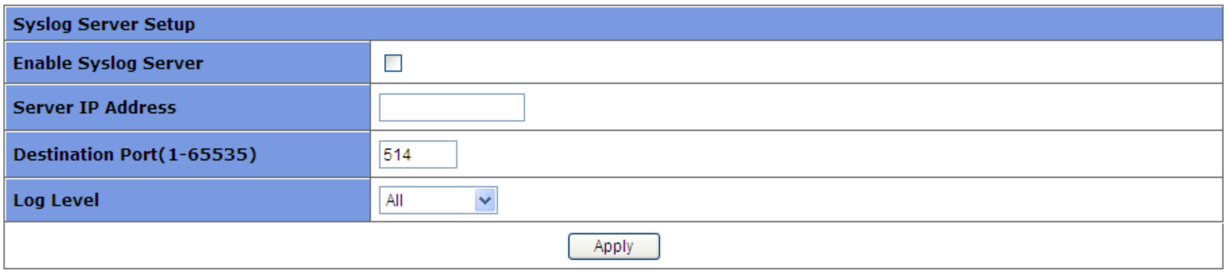
This page saves current configurations.



Please save current configurations

3.12.11 System Logs

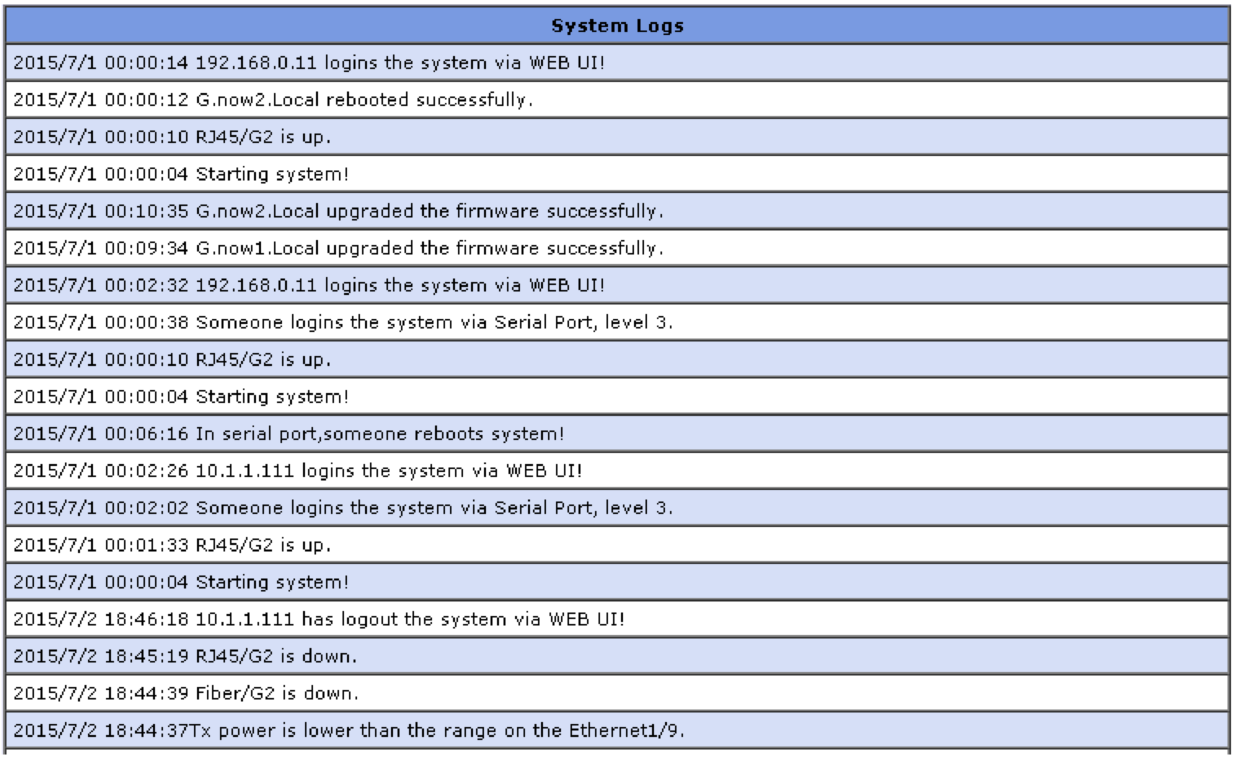
3.12.11.1 Syslog Server



Syslog Server Setup	
Enable Syslog Server	□
Server IP Address	
Destination Port(1-65535)	514
Log Level	All

3.12.11.2 System Logs

This page shows the system logs. All logs can be shown on one page. Click <Clear>, all system logs can be cleared.



System Logs

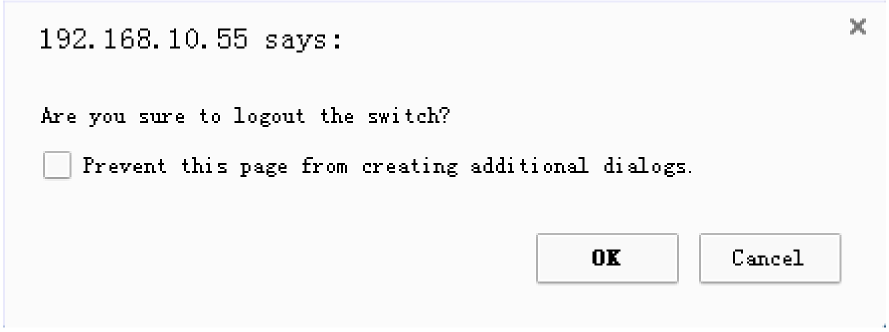
```
2015/7/1 00:00:14 192.168.0.11 logins the system via WEB UI!
2015/7/1 00:00:12 G.now2.Local rebooted successfully.
2015/7/1 00:00:10 RJ45/G2 is up.
2015/7/1 00:00:04 Starting system!
2015/7/1 00:10:35 G.now2.Local upgraded the firmware successfully.
2015/7/1 00:09:34 G.now1.Local upgraded the firmware successfully.
2015/7/1 00:02:32 192.168.0.11 logins the system via WEB UI!
2015/7/1 00:00:38 Someone logins the system via Serial Port, level 3.
2015/7/1 00:00:10 RJ45/G2 is up.
2015/7/1 00:00:04 Starting system!
2015/7/1 00:06:16 In serial port,someone reboots system!
2015/7/1 00:02:26 10.1.1.111 logins the system via WEB UI!
2015/7/1 00:02:02 Someone logins the system via Serial Port, level 3.
2015/7/1 00:01:33 RJ45/G2 is up.
2015/7/1 00:00:04 Starting system!
2015/7/2 18:46:18 10.1.1.111 has logout the system via WEB UI!
2015/7/2 18:45:19 RJ45/G2 is down.
2015/7/2 18:44:39 Fiber/G2 is down.
2015/7/2 18:44:37Tx power is lower than the range on the Ethernet1/9.
```

The main type of log:

- Port up/down
- System Restart
- Update Firmware
- Restore Configuration

3.13 Logout

Click <Logout> on the left menu to log out of the switch and close the browser.



192.168.10.55 says:

Are you sure to logout the switch?

□ Prevent this page from creating additional dialogs.