GIGA COPPER NETWORKS

G4224 Switch User Manual

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.

Reversion History

Reversion	Date	Reason for Change
V1.0	Jan 3, 2020	Initial release
V1.1	July17, 2020	Fixed some typo

Table of Contents

1 Overview

The G4224 system contains two devices: the headend switch G4224 and the client device G4202TCP, G4224 have 2 slots for hot-swappable G.hn or standard Ethernet, power over cable capable, line cards.

It supports 3 types of line cards:

G4224-12BP: 12*BNC Connector, Data rate up to Gigabit, 10* 802.3at (30W) and 2*802.3bt (90W) over coax with 500m reach

G4224-12CP: 12*F female Connector, Data rate up to Gigabit, 10* 802.3at (30W) and 2*802.3bt (90W) over coax with 500m reach

G4224-12TP: 12*RJ45 Connector, Data rate up to Gigabit, 10* 802.3at (30W) and 2*802.3bt (90W) over twisted-pair with 600m reach

G4202TCP can get power supply from G4224 or get from power adapter. And the G4202TCP also can work as a PSE device, provide power to PD devices.

It enables IP-based Video, Data and VoIP applications over existing telephone lines, coax cables and copper cables. 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 home wires with significantly lower installation and operating costs, the legacy home wires are those using telephone lines. With scalability to over 40 units, the G4224 solution can scale to serve several hundred of end users connected on a copper network, G4224 is the ideal solution for FTTH MDU deployments.

1.1 Features

Key Highlights:

- DMT/OFDM line modulation, with 200 MHz
- TDD multiplexing for programmable upstream/downstream ratio
- Programmable PSD masks for xDSL/radio coexistence or FEXT management

- power save mode
- Adaptive bit loading with fast adaptation
- Self-install
- Open Standards Based and Compatible with Existing RF Video
- State-of-the-Art LDPC forward error correction (FEC)
- IEEE 802.1Q tagged VLAN
- Local device and remote device Firmware upgrade via TFTP.
- Dynamic bandwidth allocation optimizes throughput based on activity
- Remote power on / off detection with dying gasp alarm.
- MSTP
- Data Security Features
- DHCP snooping option82
- SNMPv1/v2c/v3
- Upload and download configuration file.
- Egress /Ingress rate management control.
- Support port mirroring and port isolate
- Various QoS capability (IEEE 802.1p / port / MAC / Diffserv)
- Monitor and configure remote devices
- Standard 19 inch rack mounted or miniature custom rack mounted available.
- Reliable HD IPTV and internet distribution
- Up to 800 Mbps of actual throughput over telephone line or coax cable

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	Ethernet Port	Console Port	G.hn Port	Power Supply
G4224	2* 1/10 Gb SFP ports or 2*10/100/1000BaseTX copper ports	1*RS-232 and 1*USB Type-C 3.1	24* G.hn ports (RJ45,F female, BNC or female)	100-240VAC or 48V DC
G4202TCP	2x10/100/1000 Base-TX copper port	None	1*RJ45 1*F female or BNC female connector	20V/3A DC or get power supply from G4224

1.3 Default Configuration

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

Account:

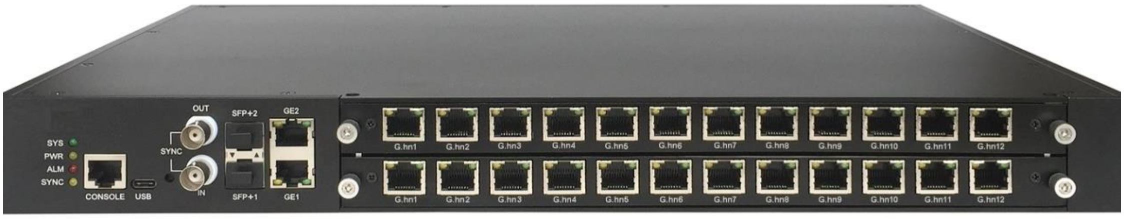
Access Level	User Name	Password	Rights
Administrator	superuser	123	All operations on the switch
User	admin	123	All operations except the following ● Create or delete accounts ● Reset ● Software upgrade, backup and restoration through TFTP
Visitor	guest		Networking utility such as “ping” and “show”, but 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.

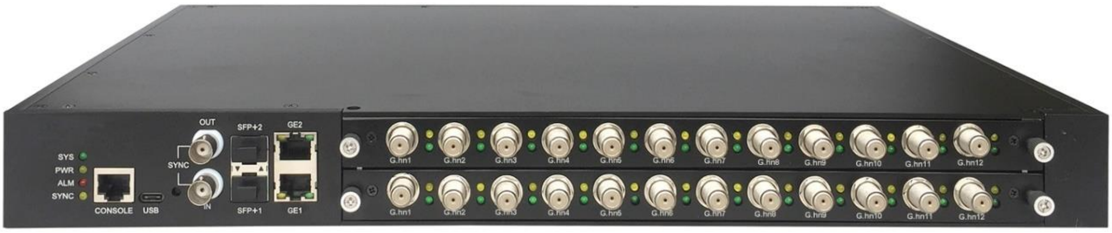
2 Hardware Descriptions

The system contains two devices, local device（G4224） and remote device（G4202TCP）, as shown in the following drawings.

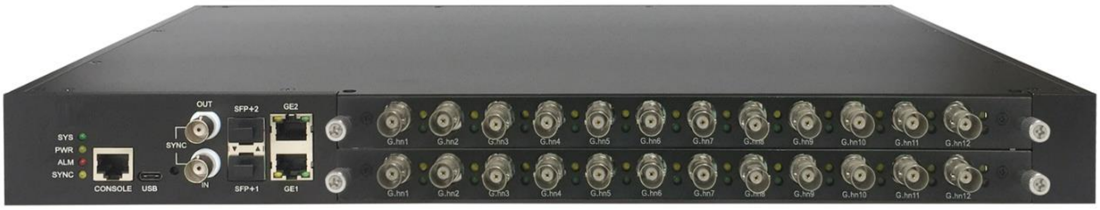
G4224:



(G4224 chassis with two G4224-12TP line cards)

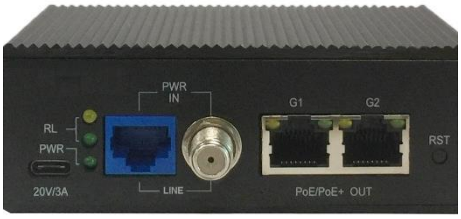


(G4224 chassis with two G4224-12CP line cards)



(G4224 chassis with two G4224-12BP line cards)

G4202TCP

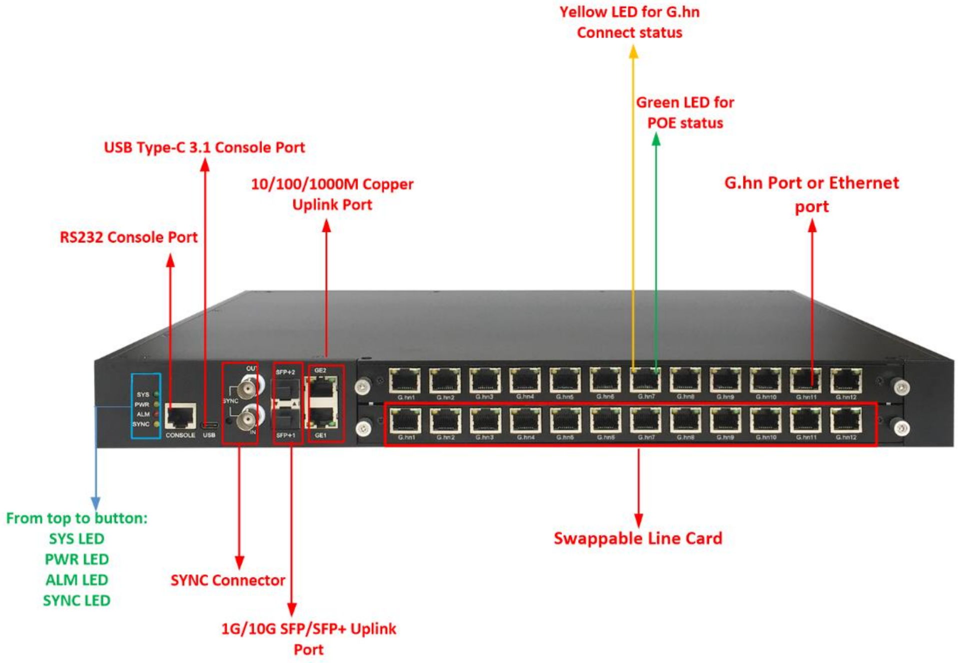


2.1 G4224 (Local Device)

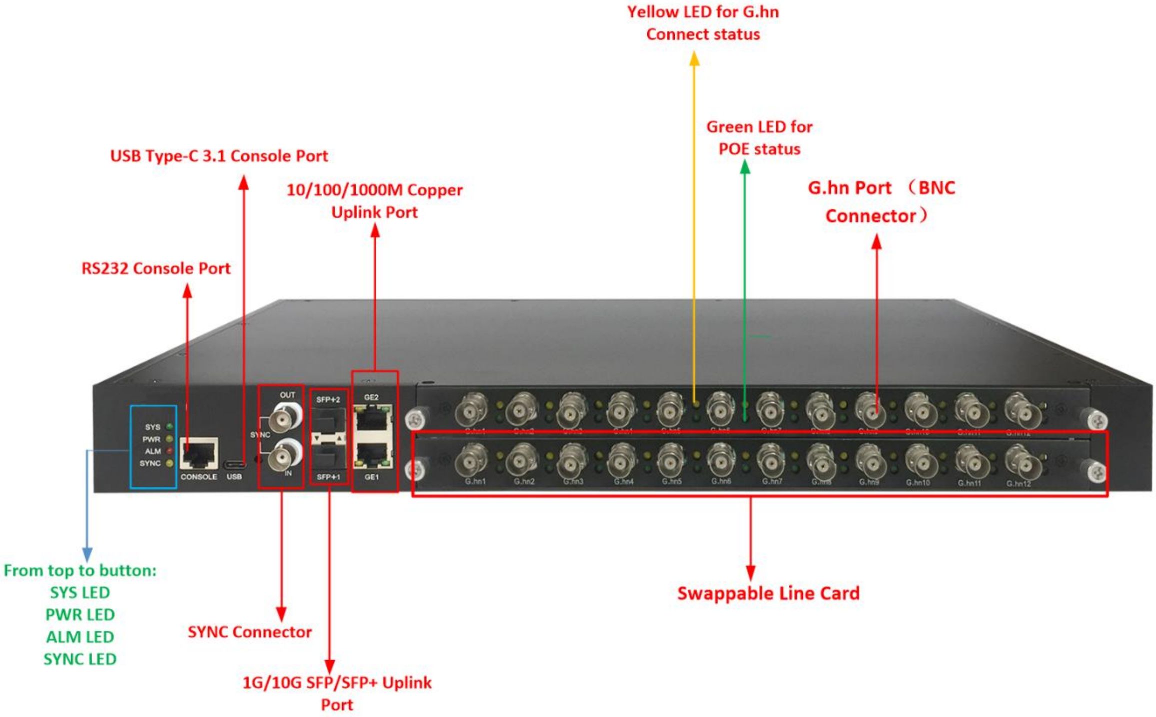
2.1.1 G4224 Panel

The front panel is shown as below:

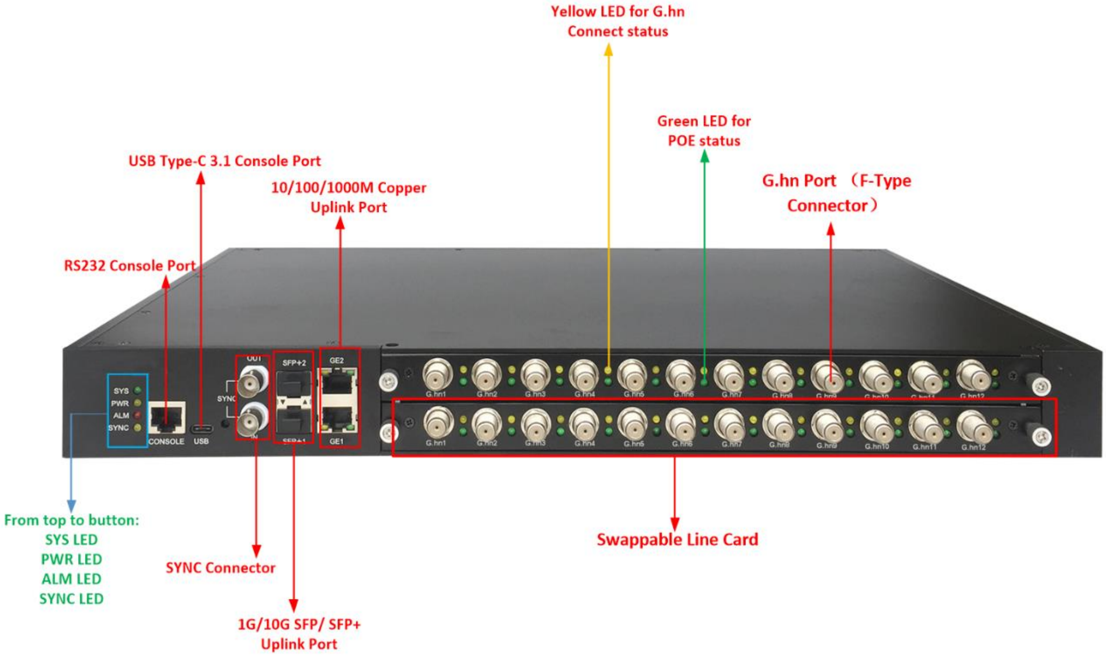
G4224 Chassis with Two G4224-12TP Line Cards



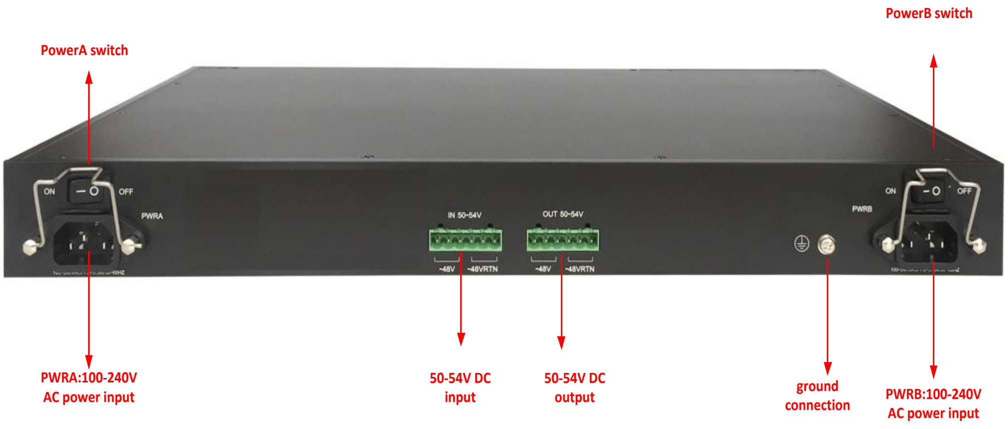
G4224 Chassis with Two G4224-12BP Line Cards



G4224 Chassis with Two G4224-12CP Line Cards:



The rear panel is shown as below:



The following table shows the port descriptions.

Label	Description
CONSOLE	A RJ45 connector RS232 console for connection to a computer control/ administration. The RS-232 console port can be used for accessing the device CLI (command line interface) for out-of-band management. Bit per second:115200
USB	A USB Type-C 3.1 connector console for connection to a computer control/ administration. The USB console port can be used for accessing the device CLI (command line interface) for out-of-band management. Bit per second:115200 **Note**: (1) The driver needs to be installed (2) As different types of laptops have different ways to detect USB port, it is recommended that do not connect other USB devices (such as USB mouse and power adapter) on the laptop when using USB serial port to avoid affecting the use of USB serial port
SYNC	2 BNC connectors, one for signal input and one for signal output, used for transmitting 50Hz SYNC clock.
SFP+1/SFP+2	2 *SFP or SFP+, Support 1/10 Gbps

GE1/GE2	2 *10/100/1000Base-T RJ-45 Ethernet Port
G.hn port (line card)	G.hn ports with POE output feature (G.hn1-G.hn10 support 30W, G.hn11 and G.hn12 support 90W). The G.hn port include 3 types: BNC female connector, F female connector, RJ45, each type of connector is related to a corresponding line card
Hot-swappable Line card	2 slots for hot-swappable G.hn or standard Ethernet, power over cable capable. There are 3 types of line cards: Type1:G4224-12BP (12*BNC, female connector) Type2:G4224-12CP (12* F female connector) Type3:G4224-12TP (12* RJ45, for G.hn)
PWR A/Power B	100-240V AC power input
-48VRTN	-48V DC output, provide power to other G4224 device

The following table shows the LED descriptions.

Label	Type	Color	State	Description
PWR A/B	Power status	Yellow	On	Lights to indicate the power is on
			Off	Indicate that the power is off
SYS	System status	Green	On	Lights to indicate that System is started
			Off	Indicates that system is not started
G.hn	G.hn link status	Yellow	On	Lights to indicate the coaxial/UTP link is established
			Off	Indicates that the coaxial/UTP link is down
POE	Poe link status	Green	On	Lights to indicate that the PoE power supply is normal
			Off	Indicates no PoE power supply
SFP+1/SFP+2	10G Ethernet link status	Green	On	Lights to indicate the port is link up
			Off	Indicates that the port is link down
Alarm	Alarm	Red	On	Lights to indicates FAN fault

			Off	Indicates that the FAN is normal
SYNC	SYNC Status	Yellow	On	Lights to indicate the 50Hz SYNC clock is working
			Off	Indicates that the 50Hz SYNC clock is not working
GE1/GE2	Ethernet link status	Green	On	Lights to indicate the port is link up and the rate is 1000Mbps
			Off	Indicates that the port is link down or the port is link up but connect rate is 10/100 Mbps
		Yellow	On	Lights to indicate the port is link up
			Off	Indicates that the port is link down
			Blink	The port is up and has data transmission

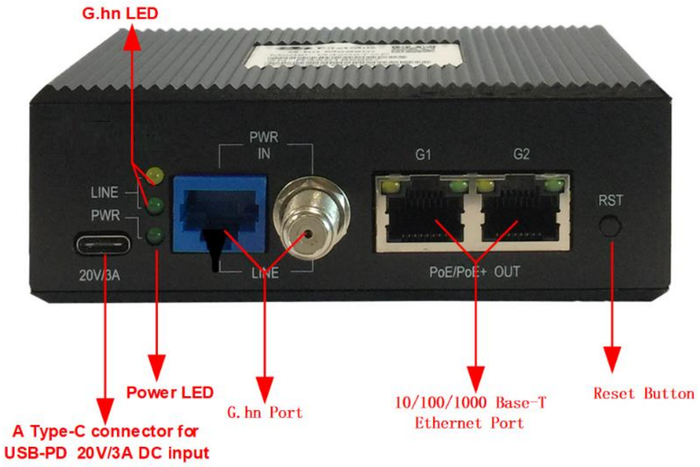
2.1.2 Physical and Environmental

- Dimension (W*D*H):440mm *300mm *44mm , 1U high
- Weight: <4.2Kg
- Operating temperature: 0℃ ~ 40℃
- Storage temperature: -25℃ ~ 70℃
- Power consumption: 600 watts
- Power consumption:10% ~ 90% non-condensing

2.2 G4202TCP (Remote Device)

2.2.1 G4202TCP Panel

The G4202TCP front panel is shown as below:



The G4202TCP rear panel is shown as below:

The following table shows the port descriptions.

Label	Description
20V/3A	A Type-C connector for USB-PD 20V/3A DC input
LINE	G.hn port, optional for RJ45 cable or coax cable, and support POE power input
G1/G2	2 *10/100/1000BT RJ-45 Ethernet ports, can provide power for device which supports POE power supply.
RST	Reset G4202TCP to factory default

The following table shows the LED descriptions:

Label	**Type**	**Color**	**State**	**Description**
PWR	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
LINE	G.hn link status	Green	On	The corresponding port connection is normal
			Off	The link condition is poor or there is no connection to this port
		Yellow	On	The corresponding port connection is abnormal and link quality is poor
			Off	The link condition is normal or there is no connection to this port (it can be judged from the G.hn green LED status)
G1/G2	Ethernet link status	Green	On	Lights to indicate the port is link up and the rate is 1000Mbps
			Off	Indicates that the port is link down or the port is link up but connect rate is 10/100 Mbps
		Yellow	On	Lights to indicate the port is link up
			Off	Indicates that the port is link down
			Blink	The port is up and has data transmission

2.2.2 Physical and Environmental

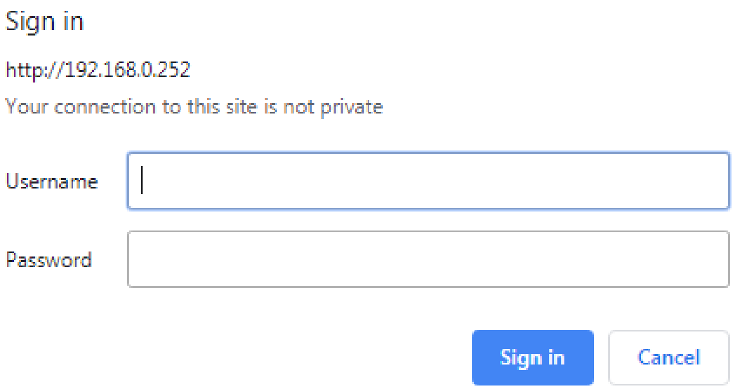
- Dimensions: 107mm x 77mm x 38mm（W×D×H）
- Weight: 340g
- Operating temperature: 0℃ ~ 50℃
- Storage temperature: -25℃ ~ 70℃
- Humidity: 10% ~ 90% RH Non-condensing, Storage: 5~95%(non-condensing)
- Consumption: No-load: <5W

Note: The G4202TCP has two power input options. Only one mode is available at the same time, when both local DC power and remote G.hn power provide power for G4202TCP, it is recommended to connect the local DC power first, and then remote G.hn power.

3. G4224 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. G4224 provides the default network settings for the Web browsers as section 1.3 Default Configuration, It offers three different login privileges: superuser, admin and guest.

You can browse http://192.168.0.252, type user name and password as section 1.3 Default Configuration, if you have not made any change to the network setting.



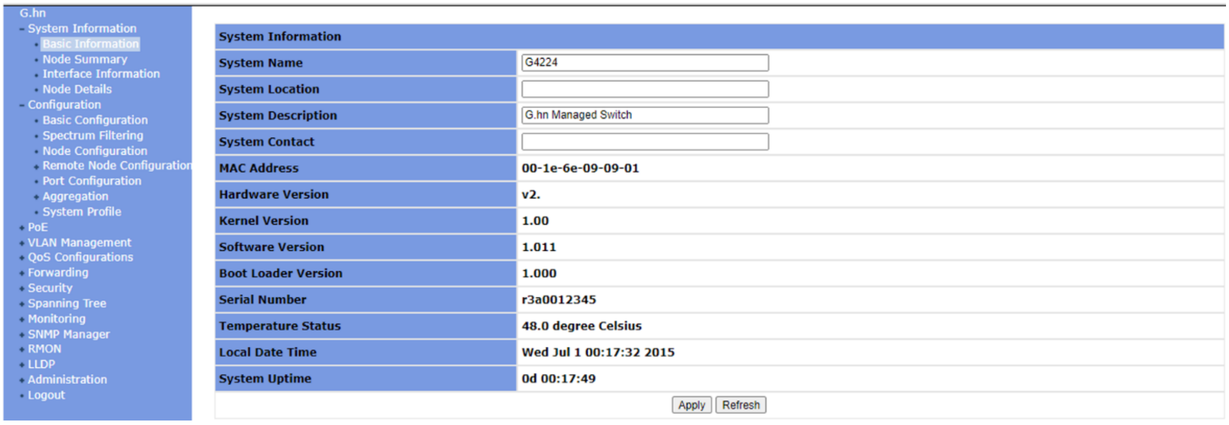
Sign in

http://192.168.0.252

Your connection to this site is not private

3.1 System Information

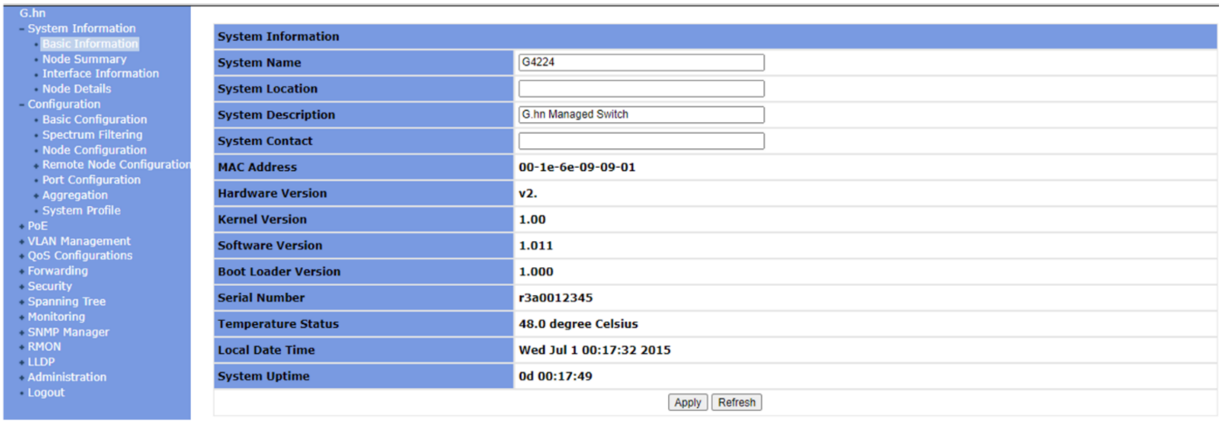
Login the WEB GUI, the home page is shown as below:



System Information	
System Name	G4224
System Location	
System Description	G.hn Managed Switch
System Contact	
MAC Address	00-1e-6e-09-09-01
Hardware Version	v2.
Kernel Version	1.00
Software Version	1.011
Boot Loader Version	1.000
Serial Number	r3a0012345
Temperature Status	48.0 degree Celsius
Local Date Time	Wed Jul 1 00:17:32 2015
System Uptime	0d 00:17:49

3.1.1 Basic Information

The Basic Information is shown as below:

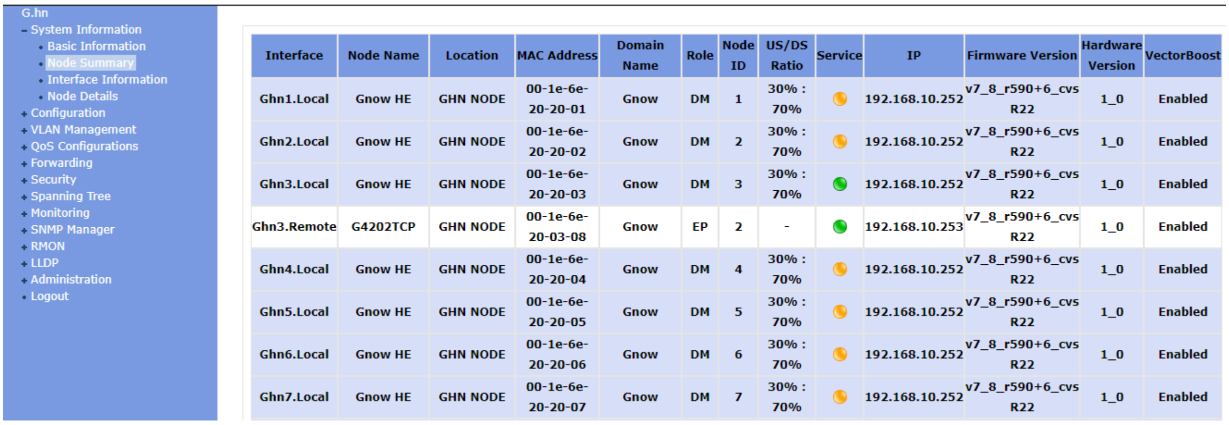


System Information	
System Name	G4224
System Location	
System Description	G.hn Managed Switch
System Contact	
MAC Address	00-1e-6e-09-09-01
Hardware Version	v2.
Kernel Version	1.00
Software Version	1.011
Boot Loader Version	1.000
Serial Number	r3a0012345
Temperature Status	48.0 degree Celsius
Local Date Time	Wed Jul 1 00:17:32 2015
System Uptime	0d 00:17:49

Note: The System Name is depended on system profile, different system profile shows different system name, current system profile is PTP mode (G4224-12TP)

3.1.2 Node Summary

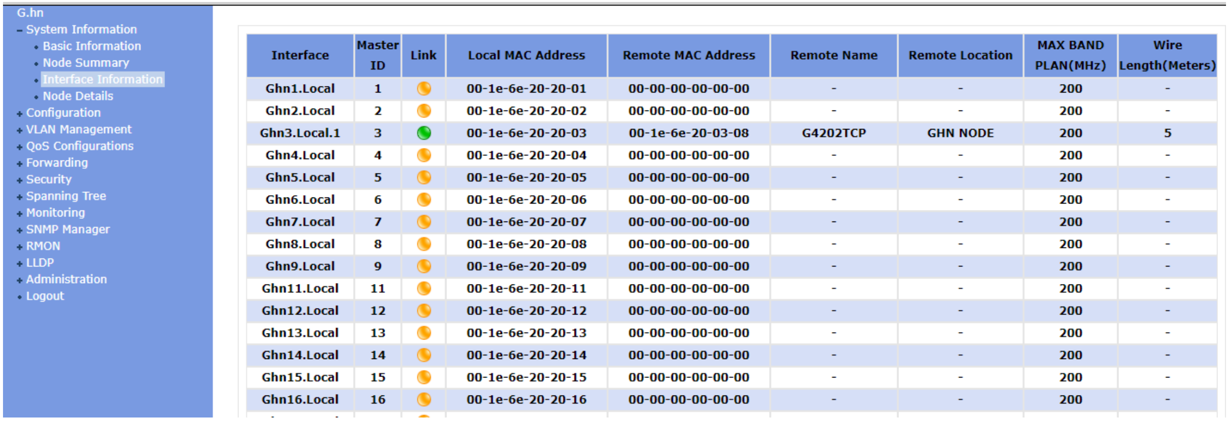
Detail information of all devices in the system are shown as below.



Interface	Node Name	Location	MAC Address	Domain Name	Role	Node ID	US/DS Ratio	Service	IP	Firmware Version	Hardware Version	VectorBoost
Ghn1.Local	Gnow HE	GHN NODE	00-1e-6e-20-20-01	Gnow	DM	1	30% : 70%	●	192.168.10.252	v7_8_r590+6_cvs R22	1_0	Enabled
Ghn2.Local	Gnow HE	GHN NODE	00-1e-6e-20-20-02	Gnow	DM	2	30% : 70%	●	192.168.10.252	v7_8_r590+6_cvs R22	1_0	Enabled
Ghn3.Local	Gnow HE	GHN NODE	00-1e-6e-20-20-03	Gnow	DM	3	30% : 70%	●	192.168.10.252	v7_8_r590+6_cvs R22	1_0	Enabled
Ghn3.Remote	G4202TCP	GHN NODE	00-1e-6e-20-03-08	Gnow	EP	2	-	●	192.168.10.253	v7_8_r590+6_cvs R22	1_0	Enabled
Ghn4.Local	Gnow HE	GHN NODE	00-1e-6e-20-20-04	Gnow	DM	4	30% : 70%	●	192.168.10.252	v7_8_r590+6_cvs R22	1_0	Enabled
Ghn5.Local	Gnow HE	GHN NODE	00-1e-6e-20-20-05	Gnow	DM	5	30% : 70%	●	192.168.10.252	v7_8_r590+6_cvs R22	1_0	Enabled
Ghn6.Local	Gnow HE	GHN NODE	00-1e-6e-20-20-06	Gnow	DM	6	30% : 70%	●	192.168.10.252	v7_8_r590+6_cvs R22	1_0	Enabled
Ghn7.Local	Gnow HE	GHN NODE	00-1e-6e-20-20-07	Gnow	DM	7	30% : 70%	●	192.168.10.252	v7_8_r590+6_cvs R22	1_0	Enabled

3.1.3 Interface Information

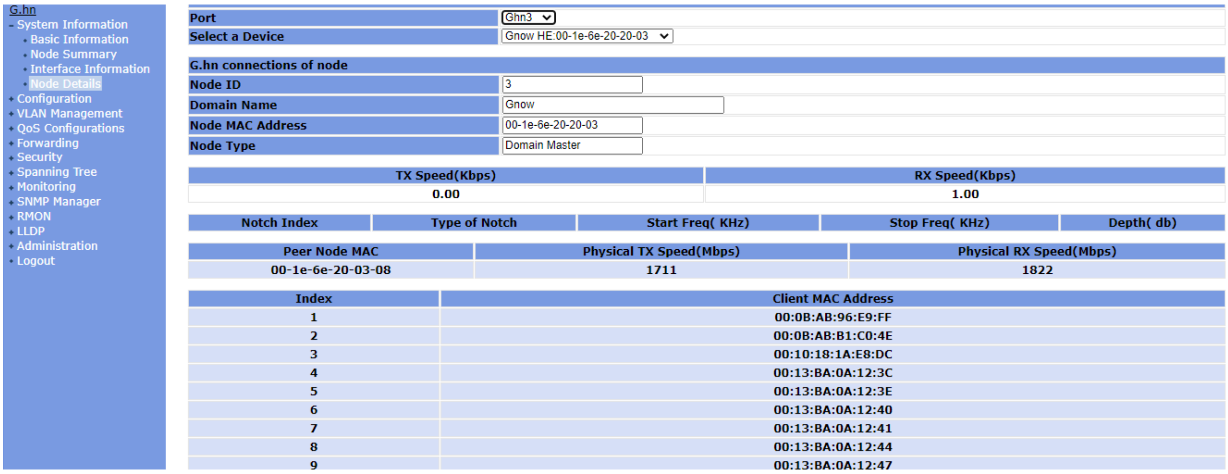
You can check the G.hn connection information from this page as below



Interface	Master ID	Link	Local MAC Address	Remote MAC Address	Remote Name	Remote Location	MAX BAND PLAN(MHz)	Wire Length(Meters)
Ghn1.Local	1	🟠	00-1e-6e-20-20-01	00-00-00-00-00-00	-	-	200	-
Ghn2.Local	2	🟠	00-1e-6e-20-20-02	00-00-00-00-00-00	-	-	200	-
Ghn3.Local.1	3	🟢	00-1e-6e-20-20-03	00-1e-6e-20-03-08	G4202TCP	GHN NODE	200	5
Ghn4.Local	4	🟠	00-1e-6e-20-20-04	00-00-00-00-00-00	-	-	200	-
Ghn5.Local	5	🟠	00-1e-6e-20-20-05	00-00-00-00-00-00	-	-	200	-
Ghn6.Local	6	🟠	00-1e-6e-20-20-06	00-00-00-00-00-00	-	-	200	-
Ghn7.Local	7	🟠	00-1e-6e-20-20-07	00-00-00-00-00-00	-	-	200	-
Ghn8.Local	8	🟠	00-1e-6e-20-20-08	00-00-00-00-00-00	-	-	200	-
Ghn9.Local	9	🟠	00-1e-6e-20-20-09	00-00-00-00-00-00	-	-	200	-
Ghn11.Local	11	🟠	00-1e-6e-20-20-11	00-00-00-00-00-00	-	-	200	-
Ghn12.Local	12	🟠	00-1e-6e-20-20-12	00-00-00-00-00-00	-	-	200	-
Ghn13.Local	13	🟠	00-1e-6e-20-20-13	00-00-00-00-00-00	-	-	200	-
Ghn14.Local	14	🟠	00-1e-6e-20-20-14	00-00-00-00-00-00	-	-	200	-
Ghn15.Local	15	🟠	00-1e-6e-20-20-15	00-00-00-00-00-00	-	-	200	-
Ghn16.Local	16	🟠	00-1e-6e-20-20-16	00-00-00-00-00-00	-	-	200	-

3.1.4 Node Details

On this page, the connect information of selected devices are shown as below.



Port	Ghn3
Select a Device	Gnow HE:00-1e-6e-20-20-03

G.hn connections of node	
Node ID	3
Domain Name	Gnow
Node MAC Address	00-1e-6e-20-20-03
Node Type	Domain Master

TX Speed(Kbps)	RX Speed(Kbps)
0.00	1.00

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

Peer Node MAC	Physical TX Speed(Mbps)	Physical RX Speed(Mbps)
00-1e-6e-20-03-08	1711	1822

Index	Client MAC Address
1	00:0B:AB:96:E9:FF
2	00:0B:AB:B1:C0:4E
3	00:10:18:1A:E8:DC
4	00:13:BA:0A:12:3C
5	00:13:BA:0A:12:3E
6	00:13:BA:0A:12:40
7	00:13:BA:0A:12:41
8	00:13:BA:0A:12:44
9	00:13:BA:0A:12:47

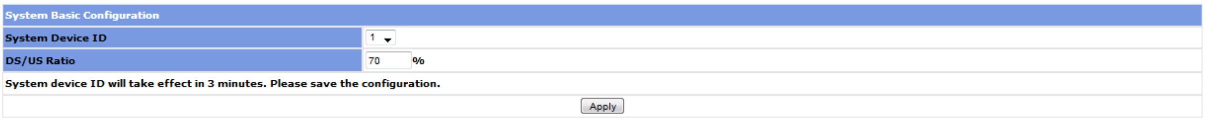
3.2 Configuration

3.2.1 Basic Configuration

On this page, you can configure basic configuration for the selected devices.

Configure system devices ID. If system device's ID is configured as 1, node devices ID will be assigned from 1 to 24. If system device's ID is configured as 2, node devices ID will be assigned from 25 to 48. Take it effect after reboot system.

Configure US/DS Ratio for all ports. The range is 30-70, it is set % of time used for downstream.

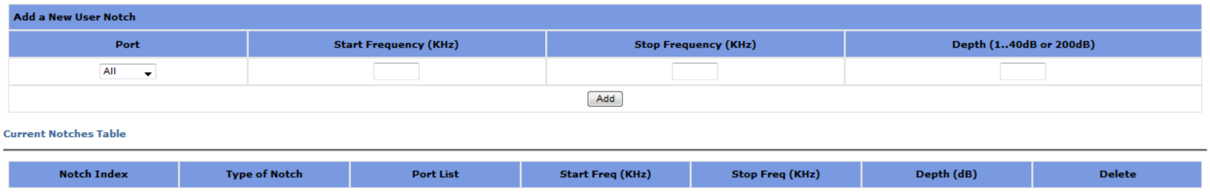


System Basic Configuration	
System Device ID	1
DS/US Ratio	70 %
System device ID will take effect in 3 minutes. Please save the configuration.	

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 KHz
Stop Frequency (KHz) ： Band stop frequency, unit KHz
Depth (1-40dB, or 200dB) ： Attenuation value, unit dB



Add a New User Notch

Port	Start Frequency (KHz)	Stop Frequency (KHz)	Depth (1..40dB or 200dB)
All			

Current Notches Table

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

Note: 32000-50000KHz are reserved for system, can’t be notched, when Spectrum Filtering configuration range is 5000-18000 or more, and Depth is 40, the remote device will lose connection with local node.

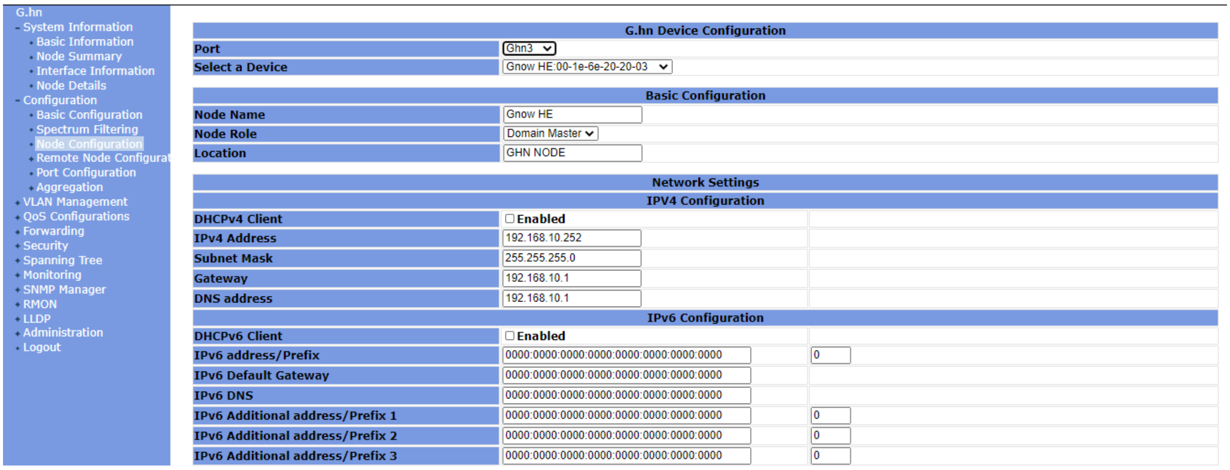
3.2.3 Node Configuration

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

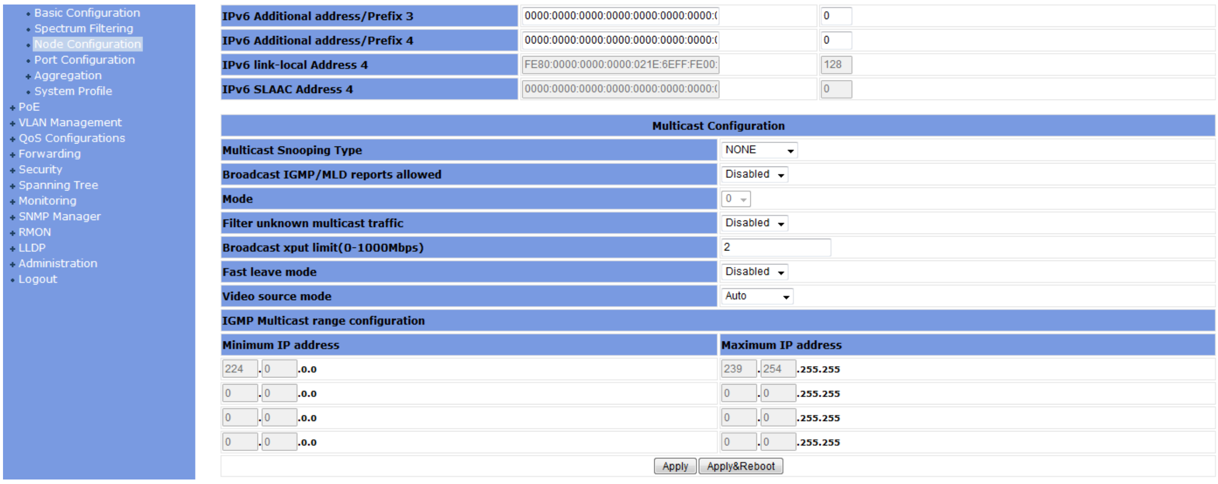
VLAN: VLAN function control switch

Ethernet Port Trunk：When downstream packets is “tag=Ethernet pvid”，the packets tag will be deleted, otherwise it will keep the original VID and send out the packets.

Ethernet PVID：When an Ethernet packet without VLAN tag is entering to this port, the packet will be added a PVID of this port as VLAN tag.



G.hn Device Configuration		
Port	Ghn3	
Select a Device	Gnow HE:00-1e-6e-20-20-03	
Basic Configuration		
Node Name	Gnow HE	
Node Role	Domain Master	
Location	GHN NODE	
Network Settings		
IPV4 Configuration		
DHCPv4 Client	□ Enabled	
IPv4 Address	192.168.10.252	
Subnet Mask	255.255.255.0	
Gateway	192.168.10.1	
DNS address	192.168.10.1	
IPv6 Configuration		
DHCPv6 Client	□ Enabled	
IPv6 address/Prefix	0000:0000:0000:0000:0000:0000:0000:0000	0
IPv6 Default Gateway	0000:0000:0000:0000:0000:0000:0000:0000	
IPv6 DNS	0000:0000:0000:0000:0000:0000:0000:0000	
IPv6 Additional address/Prefix 1	0000:0000:0000:0000:0000:0000:0000:0000	0
IPv6 Additional address/Prefix 2	0000:0000:0000:0000:0000:0000:0000:0000	0
IPv6 Additional address/Prefix 3	0000:0000:0000:0000:0000:0000:0000:0000	0



IPv6 Additional address/Prefix 3	0000:0000:0000:0000:0000:0000:0000:(	0
IPv6 Additional address/Prefix 4	0000:0000:0000:0000:0000:0000:0000:(	0
IPv6 link-local Address 4	FE80:0000:0000:0000:021E:6EFF:FE00:	128
IPv6 SLAAC Address 4	0000:0000:0000:0000:0000:0000:0000:(	0

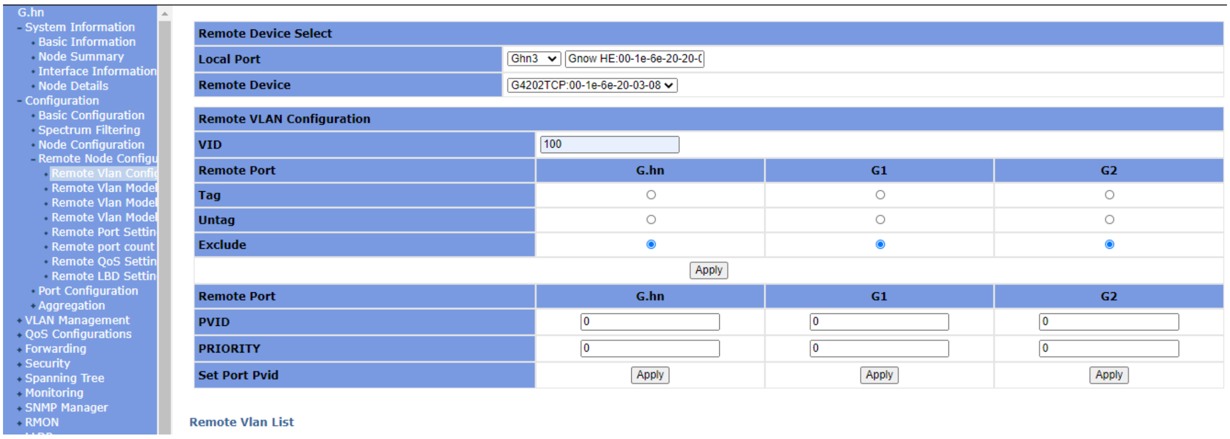
Multicast Configuration	
Multicast Snooping Type	NONE
Broadcast IGMP/MLD reports allowed	Disabled
Mode	0
Filter unknown multicast traffic	Disabled
Broadcast xput limit(0-1000Mbps)	2
Fast leave mode	Disabled
Video source mode	Auto
IGMP Multicast range configuration	
Minimum IP address	**Maximum IP address**
224.0.0.0	239.254.255.255
0.0.0.0	0.0.255.255
0.0.0.0	0.0.255.255
0.0.0.0	0.0.255.255

3.2.4 Remote Node Configuration

This page is to configure remote node and show remote Node State. Include VLAN, VID, tag/untag/exclude port, PVID, priority of the remote node.

3.2.4.1 Remote Vlan Configuration

This page is to configure remote node and show remote node state of the selected remote node.

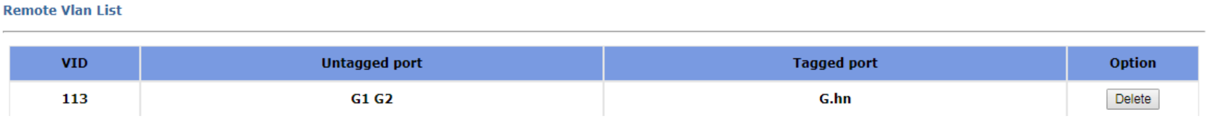


Remote Device Select	
Local Port	Ghn3 Gnow HE:00-1e-6e-20-20-(
Remote Device	G4202TCP:00-1e-6e-20-03-08

Remote VLAN Configuration			
VID	100		
Remote Port	G.hn	G1	G2
Tag	○	○	○
Untag	○	○	○
Exclude	●	●	●

Remote Port	G.hn	G1	G2
PVID	0	0	0
PRIORITY	0	0	0
Set Port Pvid	Apply	Apply	Apply

Remote Vlan List



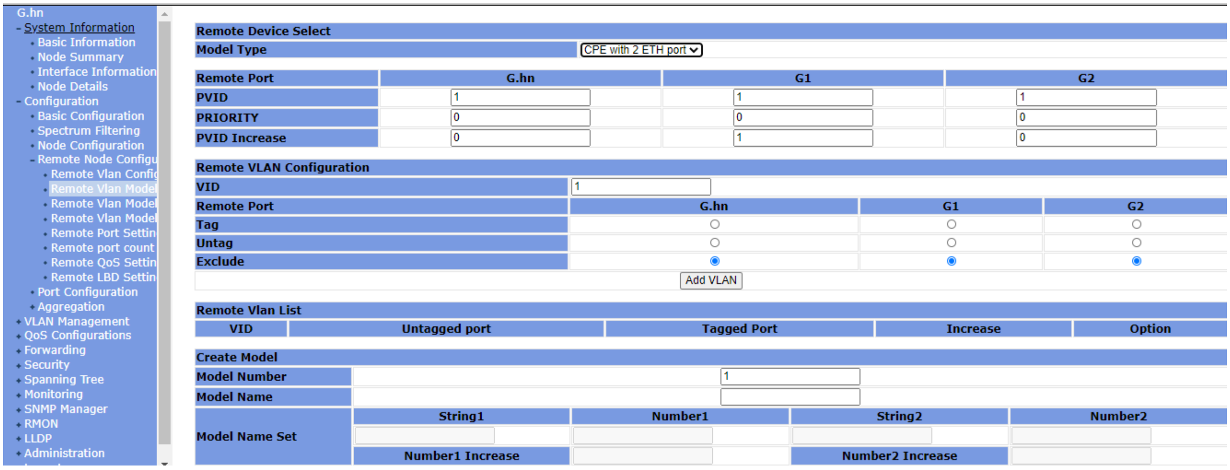
Remote Vlan List

VID	Untagged port	Tagged port	Option
113	G1 G2	G.hn	Delete

Priority: the VLAN priority, in the range of 0 to 7.

3.2.3.2 Remote Vlan Model Create

This page is to create remote node VLAN configuration model. Allow to create in batch.



Remote Device Select	
Model Type	CPE with 2 ETH port

Remote Port	G.hn	G1	G2
PVID	1	1	1
PRIORITY	0	0	0
PVID Increase	0	1	0

Remote VLAN Configuration			
VID	1		
Remote Port	G.hn	G1	G2
Tag	○	○	○
Untag	○	○	○
Exclude	●	●	●

Remote Vlan List

VID	Untagged port	Tagged Port	Increase	Option

Create Model				
Model Number	1			
Model Name				
Model Name Set	String1	Number1	String2	Number2
	Number1 Increase		Number2 Increase	

Model Number： Model number is to create.

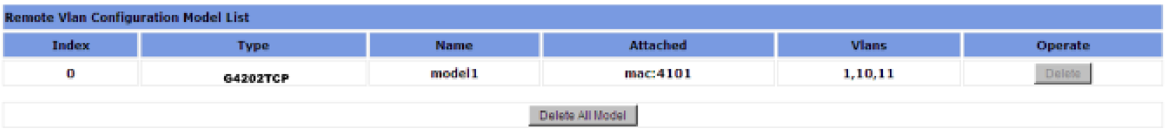
Model Name： Model name is to create.

Model Name Set： Set model name by compound mode.

3.2.3.3 Remote Vlan Model List

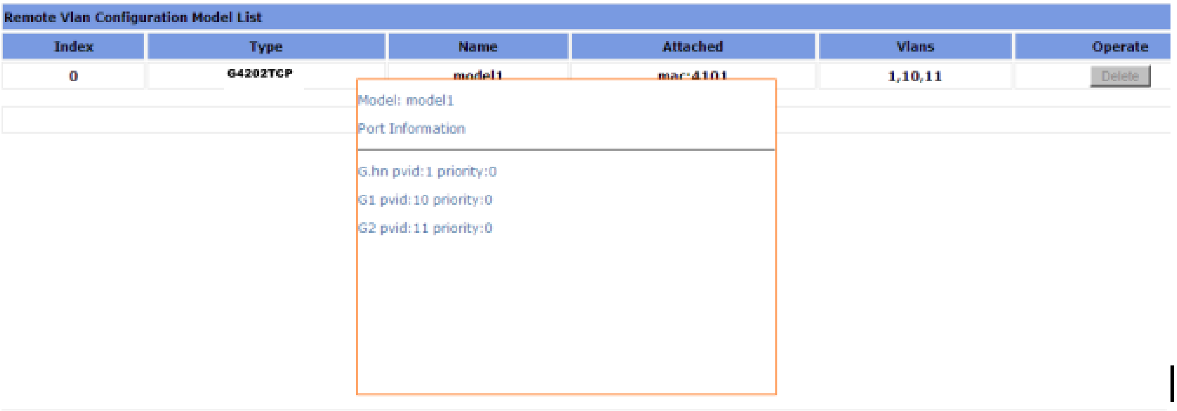
This page is to show Remote Node VLAN Configuration Model table, Configuration Model is deletable, mouse hover to display more information.

Content display include all the configuration model type, name, attached device, VLAN, VID, tag/untag/exclude port, PVID, priority.



Remote Vlan Configuration Model List

Index	Type	Name	Attached	Vlans	Operate
0	G4202TCP	model1	mac:4101	1,10,11	Delete



Remote Vlan Configuration Model List

Index	Type	Name	Attached	Vlans	Operate
0	G4202TCP	model1	mac:4101	1,10,11	Delete

Model: model1

Port Information

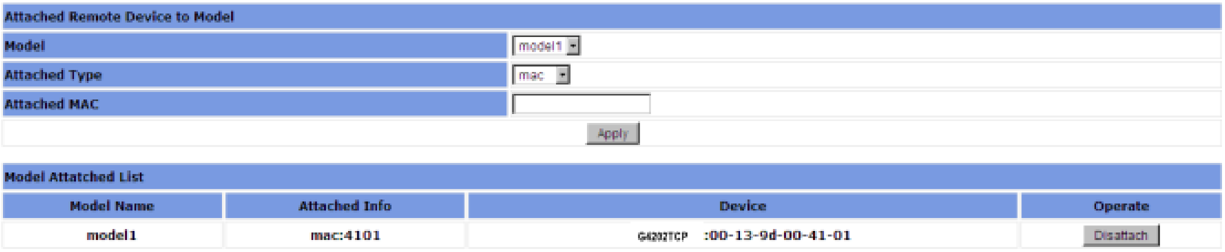
G.hn pvid:1 priority:0

G1 pvid:10 priority:0

G2 pvid:11 priority:0

3.2.3.4 Remote Vlan Model Attach

This page is to bind remote node VLAN configuration model, show binding table of remote node model, after binding, the binding remote node come into effect.



Attached Remote Device to Model

Model	model1
Attached Type	mac
Attached MAC	

Model Attatched List

Model Name	Attached Info	Device	Operate
model1	mac:4101	G4202TCP :00-13-9d-00-41-01	Disattach

Model： Model to bind.

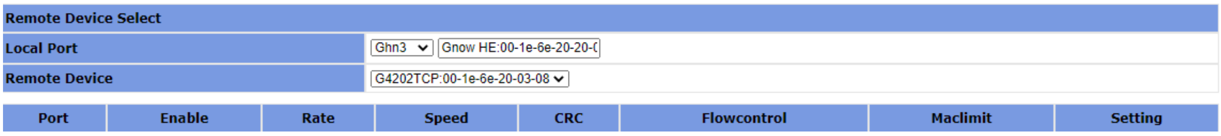
Attached Type： Designate the binding type.

Attached MAC： MAC or name of the designated binding device

Device： Name and MAC information of the binding remote node

3.2.3.5 Remote Port Setting

This page is to display remote Node port information

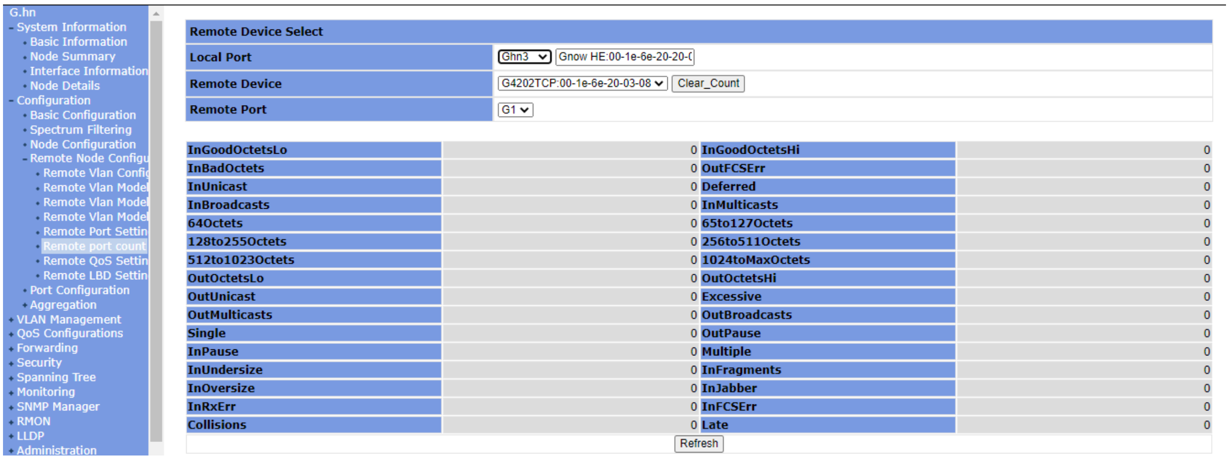


Remote Device Select	
Local Port	Ghn3 ⌄ Gnow HE:00-1e-6e-20-20-(
Remote Device	G4202TCP:00-1e-6e-20-03-08 ⌄

Port	Enable	Rate	Speed	CRC	Flowcontrol	Maclimit	Setting

3.2.3.6 Remote Port Count

This page is to display remote Node port count



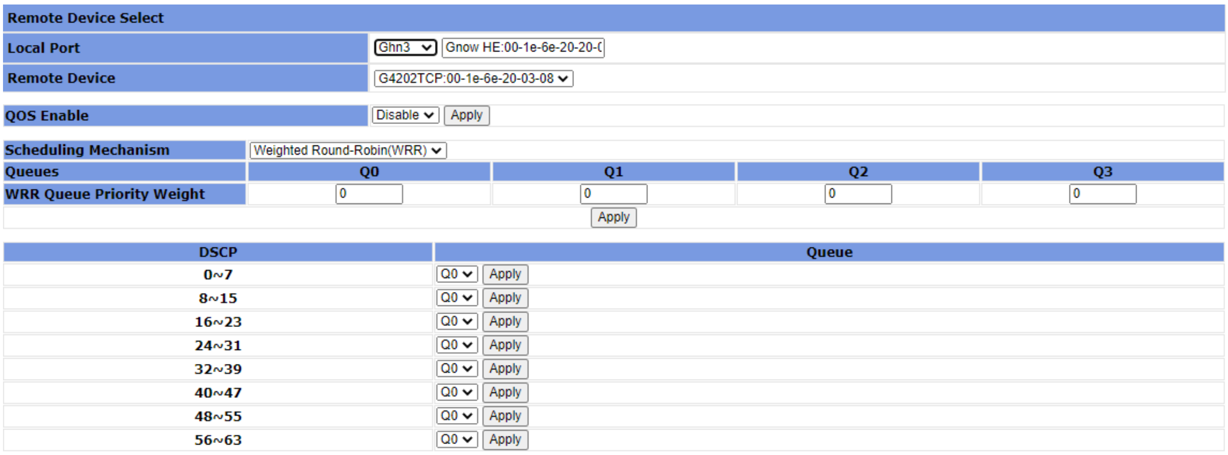
Remote Device Select	
Local Port	Ghn3 ⌄ Gnow HE:00-1e-6e-20-20-(
Remote Device	G4202TCP:00-1e-6e-20-03-08 ⌄ Clear_Count
Remote Port	G1 ⌄

InGoodOctetsLo	0	InGoodOctetsHi	0
InBadOctets	0	OutFCSErr	0
InUnicast	0	Deferred	0
InBroadcasts	0	InMulticasts	0
64Octets	0	65to127Octets	0
128to255Octets	0	256to511Octets	0
512to1023Octets	0	1024toMaxOctets	0
OutOctetsLo	0	OutOctetsHi	0
OutUnicast	0	Excessive	0
OutMulticasts	0	OutBroadcasts	0
Single	0	OutPause	0
InPause	0	Multiple	0
InUndersize	0	InFragments	0
InOversize	0	InJabber	0
InRxErr	0	InFCSErr	0
Collisions	0	Late	0

Refresh

3.2.3.7 Remote QoS Setting

This page is to set remote Node Qos



Remote Device Select	
Local Port	Ghn3 ⌄ Gnow HE:00-1e-6e-20-20-(
Remote Device	G4202TCP:00-1e-6e-20-03-08 ⌄

QOS Enable	Disable ⌄ Apply

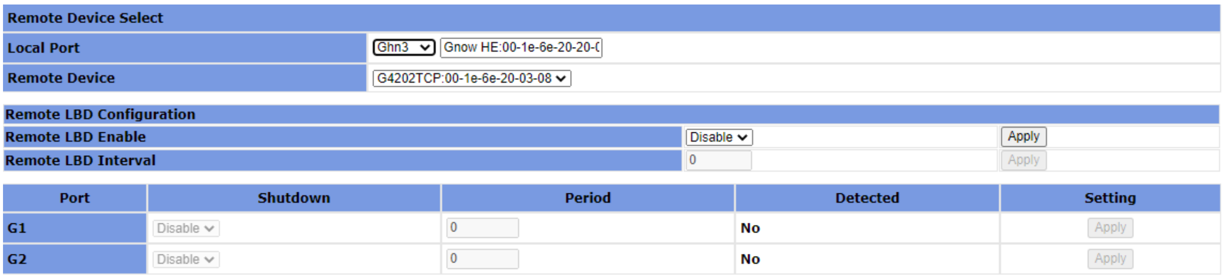
Scheduling Mechanism	Weighted Round-Robin(WRR) ⌄			
Queues	Q0	Q1	Q2	Q3
WRR Queue Priority Weight	0	0	0	0

Apply

DSCP	Queue
0~7	Q0 ⌄ Apply
8~15	Q0 ⌄ Apply
16~23	Q0 ⌄ Apply
24~31	Q0 ⌄ Apply
32~39	Q0 ⌄ Apply
40~47	Q0 ⌄ Apply
48~55	Q0 ⌄ Apply
56~63	Q0 ⌄ Apply

3.2.3.8 Remote LBD Setting

This page is to set remote Node LBD



Remote Device Select	
Local Port	Ghn3 Gnow HE:00-1e-6e-20-20-(
Remote Device	G4202TCP:00-1e-6e-20-03-08

Remote LBD Configuration		
Remote LBD Enable	Disable	Apply
Remote LBD Interval	0	Apply

Port	Shutdown	Period	Detected	Setting
G1	Disable	0	No	Apply
G2	Disable	0	No	Apply

3.2.5 Port Configuration

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

⚠ Caution:

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

Port Specifies a port to configure

State Enable/disable the port

Negotiation Selects Auto or Force, if Auto is selected, the port will automatically use the best operating mode; while is Force is selected, it needs to configure the speed and duplex manually. For G.hn port, it’s force Auto mode

Speed & Duplex Can’t be configured for G.hn port, and for Ethernet port, it can be set as 1G/2.5G/5G/10G

Flow Control For G.hn port, Flow Control is force off. For Ethernet port, you can set flow control off or flow control off.

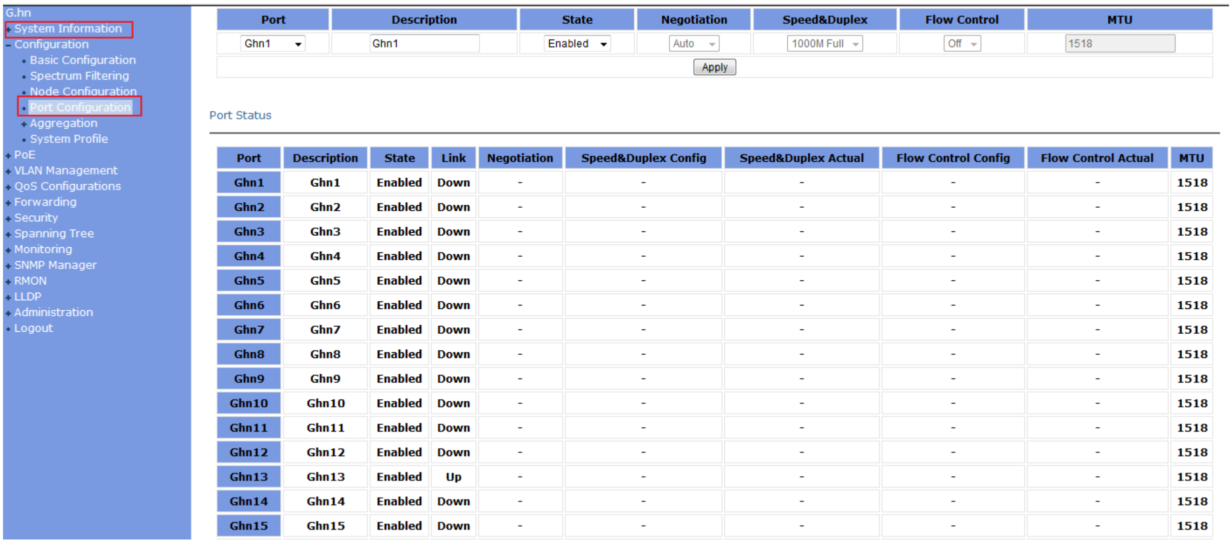
- The local switch sends a message to notify the peer switch of stopping sending packets to itself or reducing the sending rate temporarily.
- The peer switch will stop sending packets to the local switch or reduce the sending rate temporarily when it receives the message; and vice versa. By this way, packet loss is avoided and the network service operates normally.

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

Learning Enable/disable learning function

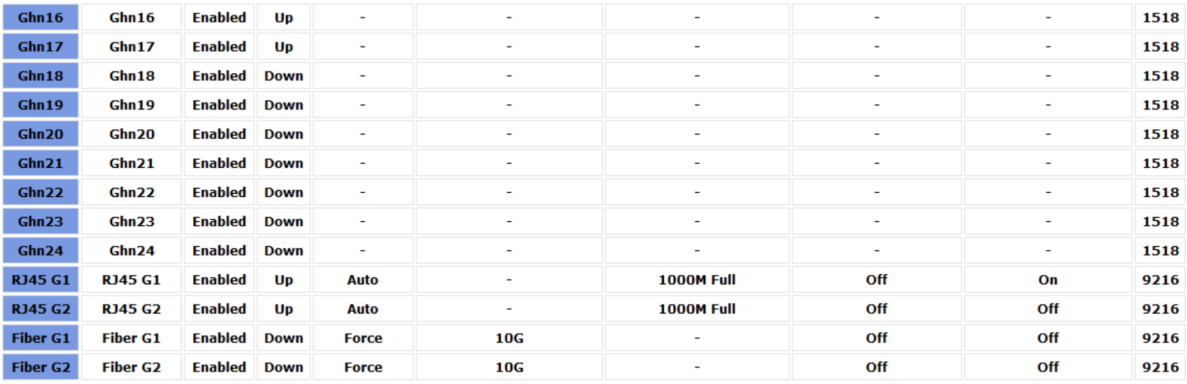
MTU The maximum transmission unit, in the range of 1518-9216 bytes.

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



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

Port Status



Port	Description	State	Link	Negotiation	Speed&Duplex Config	Speed&Duplex Actual	Flow Control Config	Flow Control Actual	MTU
Ghn1	Ghn1	Enabled	Down	-	-	-	-	-	1518
Ghn2	Ghn2	Enabled	Down	-	-	-	-	-	1518
Ghn3	Ghn3	Enabled	Down	-	-	-	-	-	1518
Ghn4	Ghn4	Enabled	Down	-	-	-	-	-	1518
Ghn5	Ghn5	Enabled	Down	-	-	-	-	-	1518
Ghn6	Ghn6	Enabled	Down	-	-	-	-	-	1518
Ghn7	Ghn7	Enabled	Down	-	-	-	-	-	1518
Ghn8	Ghn8	Enabled	Down	-	-	-	-	-	1518
Ghn9	Ghn9	Enabled	Down	-	-	-	-	-	1518
Ghn10	Ghn10	Enabled	Down	-	-	-	-	-	1518
Ghn11	Ghn11	Enabled	Down	-	-	-	-	-	1518
Ghn12	Ghn12	Enabled	Down	-	-	-	-	-	1518
Ghn13	Ghn13	Enabled	Up	-	-	-	-	-	1518
Ghn14	Ghn14	Enabled	Down	-	-	-	-	-	1518
Ghn15	Ghn15	Enabled	Down	-	-	-	-	-	1518
Ghn16	Ghn16	Enabled	Up	-	-	-	-	-	1518
Ghn17	Ghn17	Enabled	Up	-	-	-	-	-	1518
Ghn18	Ghn18	Enabled	Down	-	-	-	-	-	1518
Ghn19	Ghn19	Enabled	Down	-	-	-	-	-	1518
Ghn20	Ghn20	Enabled	Down	-	-	-	-	-	1518
Ghn21	Ghn21	Enabled	Down	-	-	-	-	-	1518
Ghn22	Ghn22	Enabled	Down	-	-	-	-	-	1518
Ghn23	Ghn23	Enabled	Down	-	-	-	-	-	1518
Ghn24	Ghn24	Enabled	Down	-	-	-	-	-	1518
RJ45 G1	RJ45 G1	Enabled	Up	Auto	-	1000M Full	Off	On	9216
RJ45 G2	RJ45 G2	Enabled	Up	Auto	-	1000M Full	Off	Off	9216
Fiber G1	Fiber G1	Enabled	Down	Force	10G	-	Off	Off	9216
Fiber G2	Fiber G2	Enabled	Down	Force	10G	-	Off	Off	9216

3.2.6 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.

3.2.7.1 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;

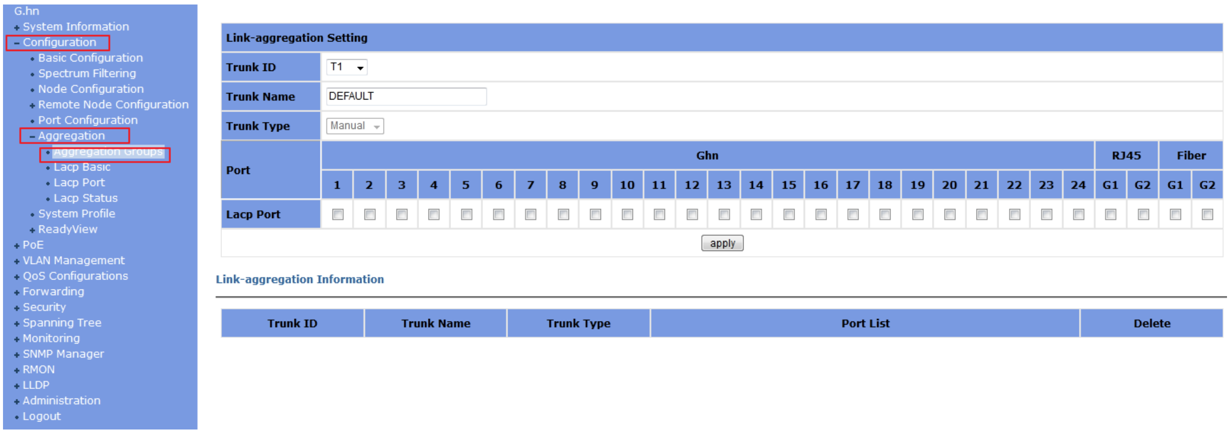
Manual: a manual trunk can only be manually set or deleted; LACP can be disabled.

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	Ghn																								RJ45		Fiber	
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	G1	G2	G1	G2
Lacp Port	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

apply

Link-aggregation Information

Trunk ID	Trunk Name	Trunk Type	Port List	Delete

⚠ Caution:

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

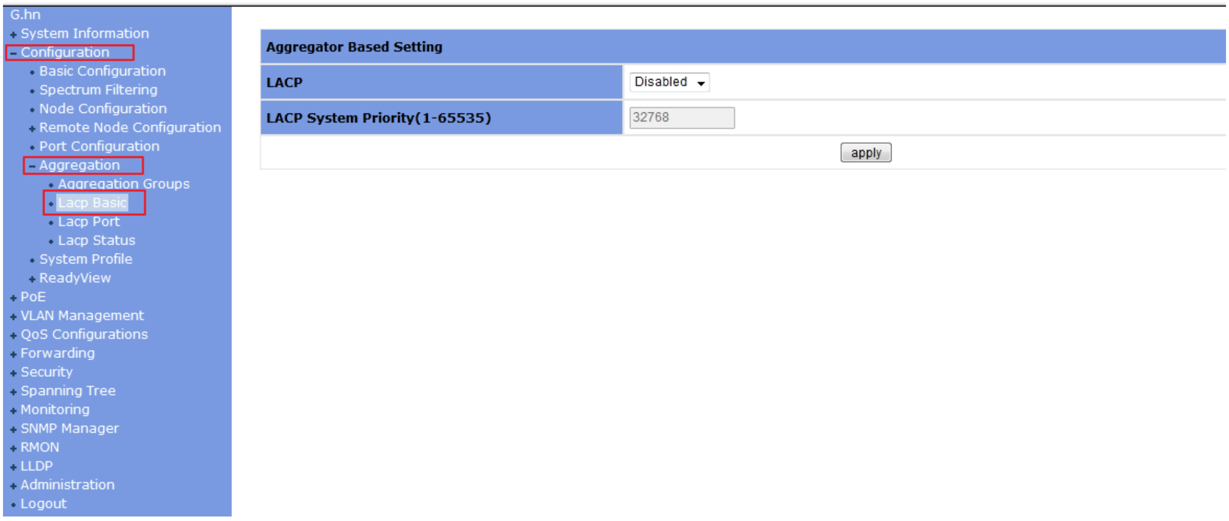
3.2.7.2 LACP Basic

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.

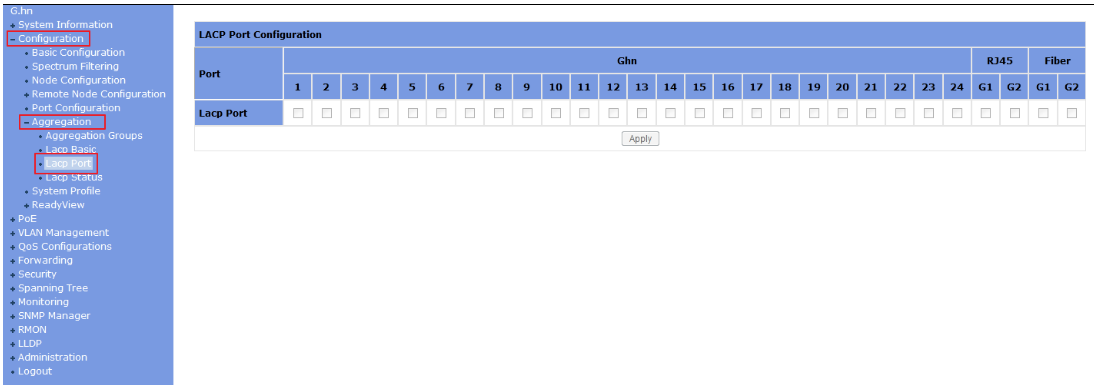
Set LACP system priority (from 1 to 65535).



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

3.2.6.3 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	Ghn																								RJ45		Fiber	
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	G1	G2	G1	G2
Lacp Port	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□

3.2.6.4 LACP Status

Set LACP port status as active or passive.

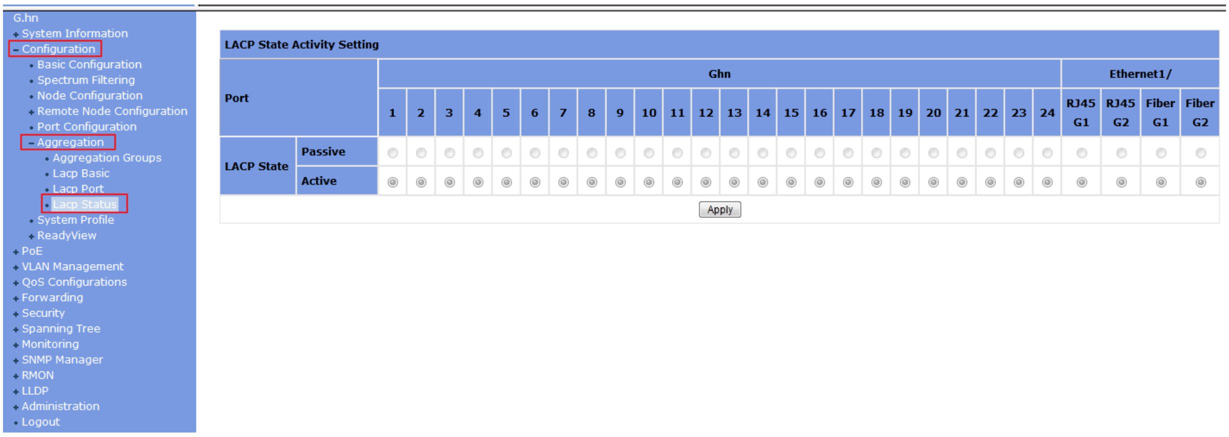
Passive The port does not automatically send LACP protocol packets; it responds only if it receives an LACP protocol packet from the peer device.

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		Ghn																								Ethernet1/			
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	RJ45 G1	RJ45 G2	Fiber G1	Fiber G2
LACP State	Passive	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
	Active	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●

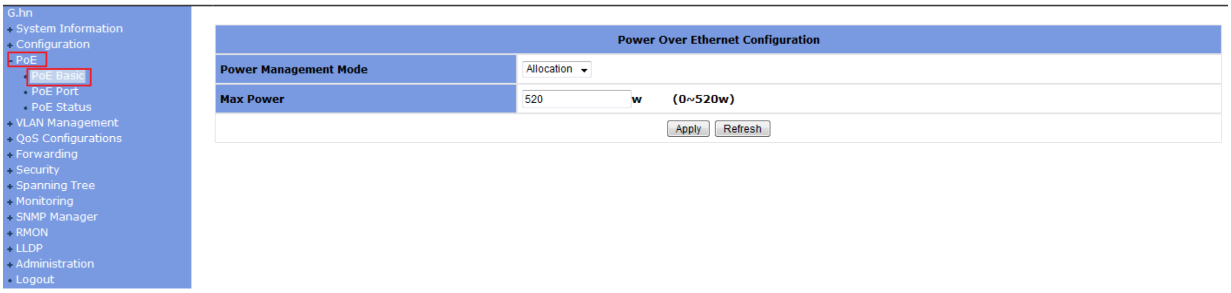
Apply

3.3 PoE

POE (Power Over Ethernet) is referred to a technology as the existing Ethernet cabling infra structure Cat.5 which do not make any changes, transmits data signals for some IP-based te rminals(such as IP telephones, wireless LAN access point AP, network cameras etc.) , mean while provids DC power supply technology for such equipment

3.3.1 PoE Basic

In this page, you can set the PoE management mode and the max power output as below:



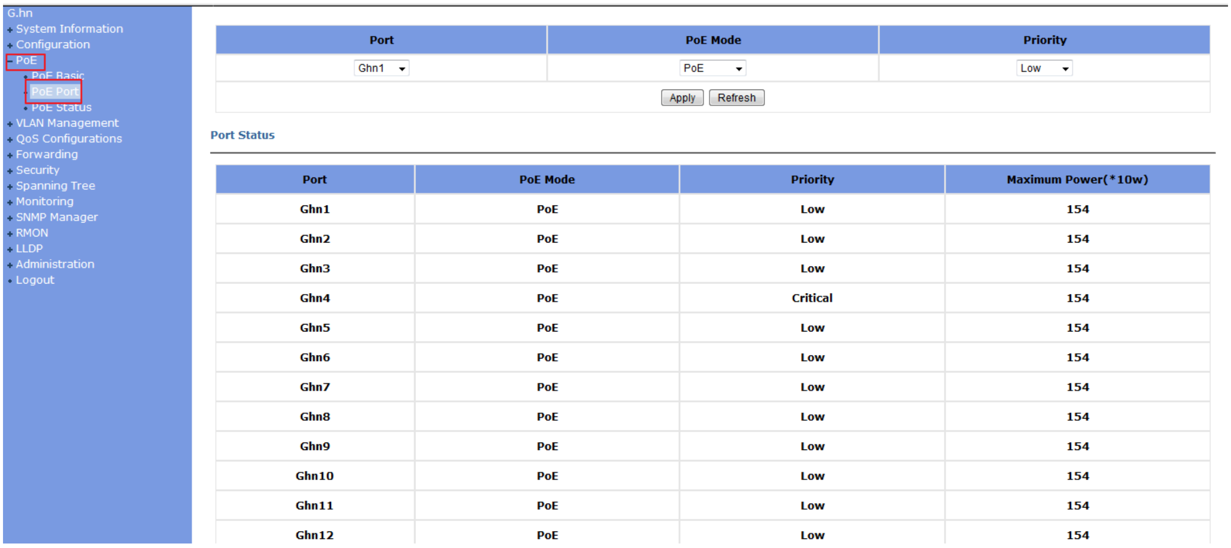
Power Over Ethernet Configuration

Power Management Mode	Allocation
Max Power	520 w (0~520w)

Apply Refresh

3.3.2 PoE Port

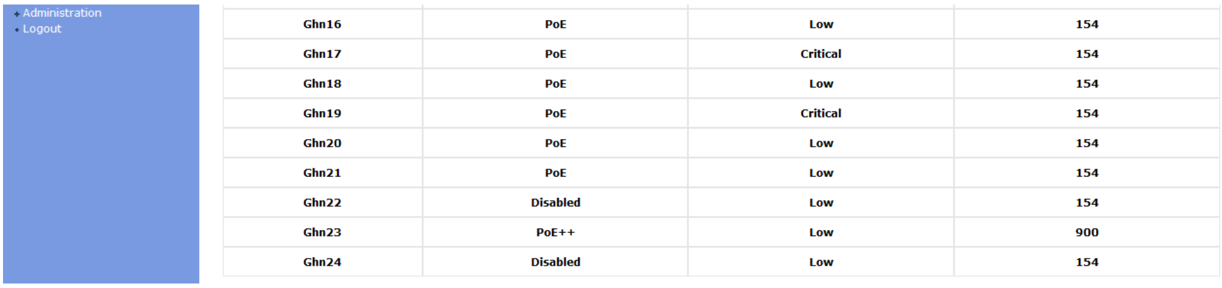
You can set the PoE parameters for ports in this page.



Port	PoE Mode	Priority
Ghn1	PoE	Low

Port Status

Port	PoE Mode	Priority	Maximum Power(*10w)
Ghn1	PoE	Low	154
Ghn2	PoE	Low	154
Ghn3	PoE	Low	154
Ghn4	PoE	Critical	154
Ghn5	PoE	Low	154
Ghn6	PoE	Low	154
Ghn7	PoE	Low	154
Ghn8	PoE	Low	154
Ghn9	PoE	Low	154
Ghn10	PoE	Low	154
Ghn11	PoE	Low	154
Ghn12	PoE	Low	154



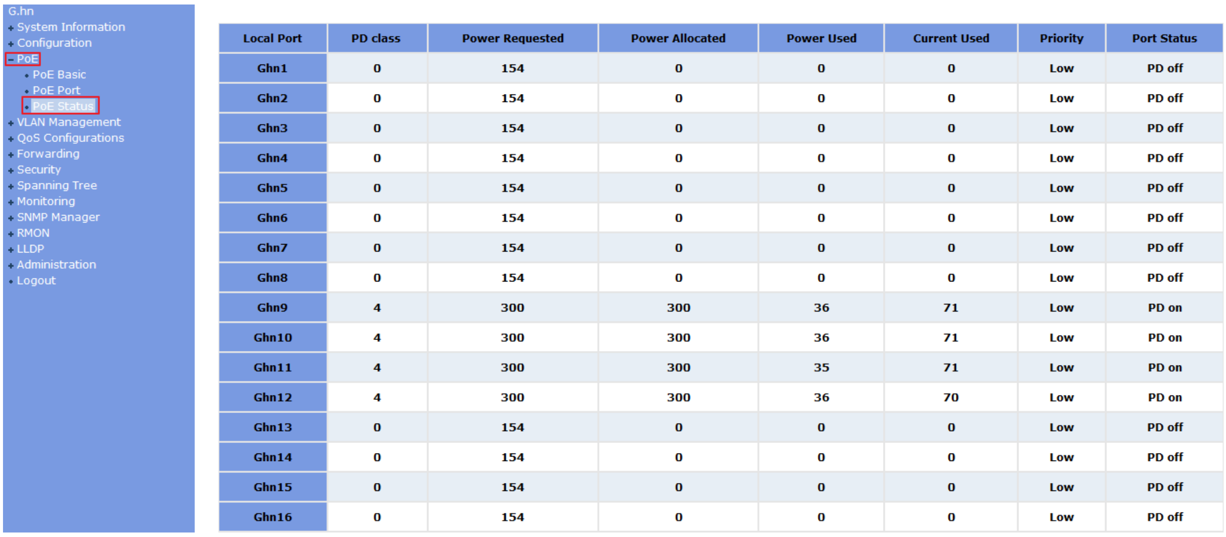
Ghn16	PoE	Low	154
Ghn17	PoE	Critical	154
Ghn18	PoE	Low	154
Ghn19	PoE	Critical	154
Ghn20	PoE	Low	154
Ghn21	PoE	Low	154
Ghn22	Disabled	Low	154
Ghn23	PoE++	Low	900
Ghn24	Disabled	Low	154

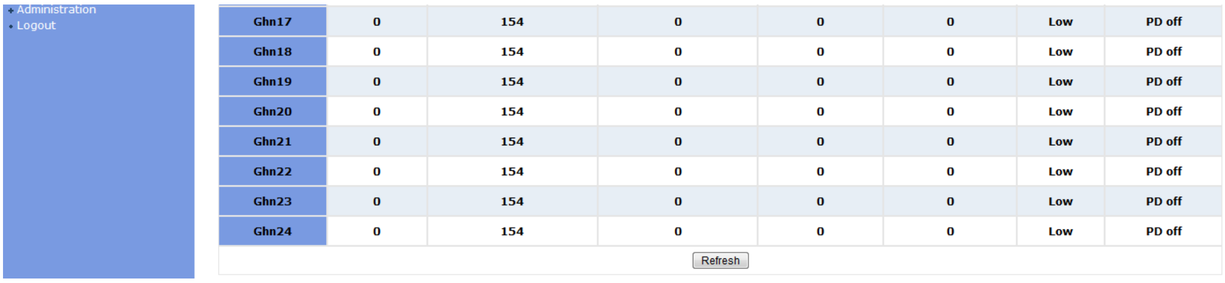
POE Mode： There are 4 options can be selected: Disabled, POE, POE+ and POE++. Disabled means the port disable POE function, and will not supply power to remote devices; POE mode in accordance with the IEEE 802.3 AF protocol transmission, provide up to 15.4W power supply; POE+ model in accordance with the IEEE 802.3 AT protocol transmission, provide up to 30W power supply for each POE port; POE++ model in accordance with the IEEE 802.3 BT protocol transmission, provide up to 90W power supply for each POE port;

Priority： You can select the Optional of low, high, Critical, by default, the priority is low.

3.3.3 POE Status

You can check POE information of the ports as followings:



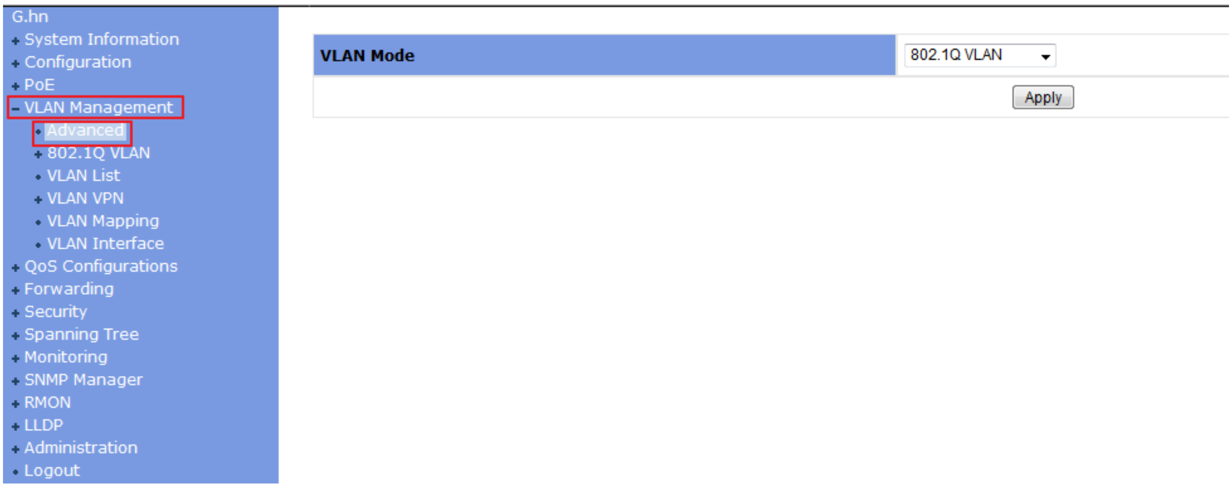


Local Port	PD class	Power Requested	Power Allocated	Power Used	Current Used	Priority	Port Status
Ghn1	0	154	0	0	0	Low	PD off
Ghn2	0	154	0	0	0	Low	PD off
Ghn3	0	154	0	0	0	Low	PD off
Ghn4	0	154	0	0	0	Low	PD off
Ghn5	0	154	0	0	0	Low	PD off
Ghn6	0	154	0	0	0	Low	PD off
Ghn7	0	154	0	0	0	Low	PD off
Ghn8	0	154	0	0	0	Low	PD off
Ghn9	4	300	300	36	71	Low	PD on
Ghn10	4	300	300	36	71	Low	PD on
Ghn11	4	300	300	35	71	Low	PD on
Ghn12	4	300	300	36	70	Low	PD on
Ghn13	0	154	0	0	0	Low	PD off
Ghn14	0	154	0	0	0	Low	PD off
Ghn15	0	154	0	0	0	Low	PD off
Ghn16	0	154	0	0	0	Low	PD off
Ghn17	0	154	0	0	0	Low	PD off
Ghn18	0	154	0	0	0	Low	PD off
Ghn19	0	154	0	0	0	Low	PD off
Ghn20	0	154	0	0	0	Low	PD off
Ghn21	0	154	0	0	0	Low	PD off
Ghn22	0	154	0	0	0	Low	PD off
Ghn23	0	154	0	0	0	Low	PD off
Ghn24	0	154	0	0	0	Low	PD off

3.4 VLAN Management

3.4.1 Advanced

This page globally sets the VLAN mode from the following port-based VLAN and 802.1Q VLAN.



VLAN Mode: 802.1Q VLAN

3.4.2 802.1Q VLAN

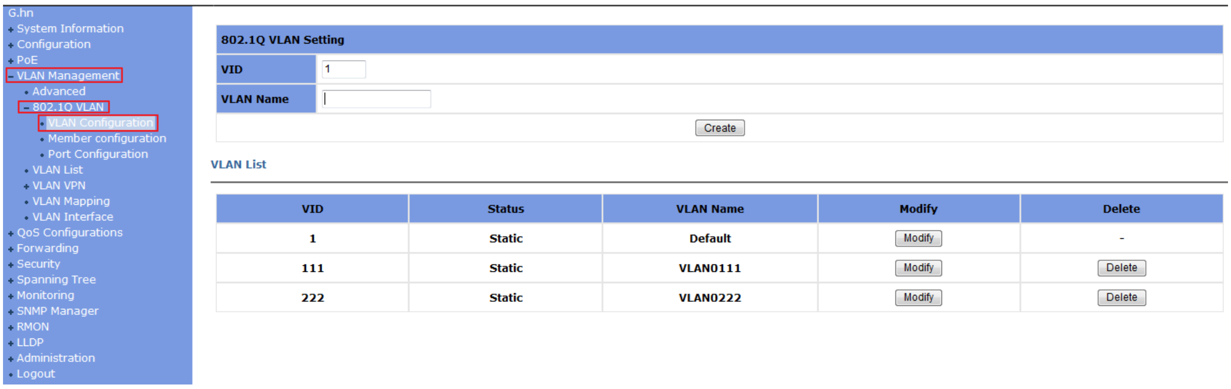
(1) VLAN Configuration

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

The 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:

VLAN List

VID	Status	VLAN Name	Modify	Delete
1	Static	Default	Modify	-
111	Static	VLAN0111	Modify	Delete
222	Static	VLAN0222	Modify	Delete

(2) Member Configuration

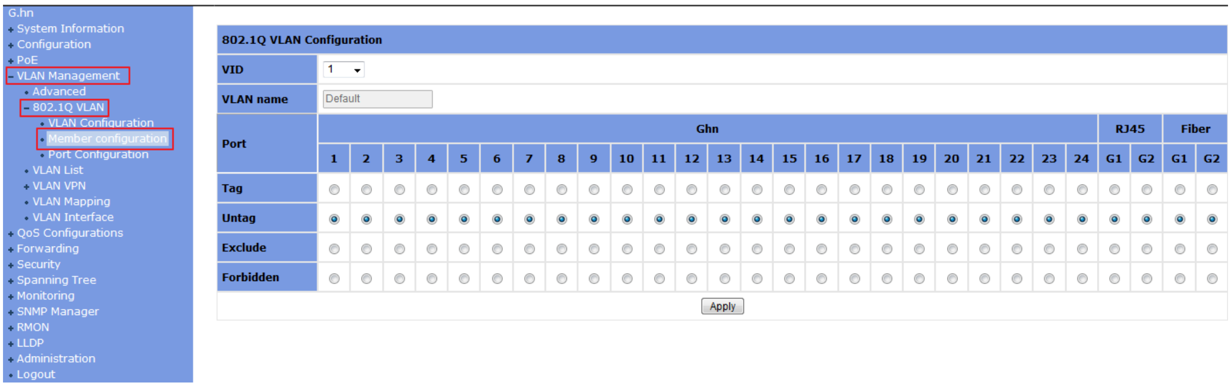
This tab page configures a VLAN group; each port can be configured as a specific state for this VLAN group:

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	Ghn																								RJ45		Fiber	
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	G1	G2	G1	G2
Tag	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Untag	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Exclude	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Forbidden	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○

Apply

(3) Port Configuration

This tab page configures 802.1Q VLAN port parameters:

Port : Specify the port to be configured.

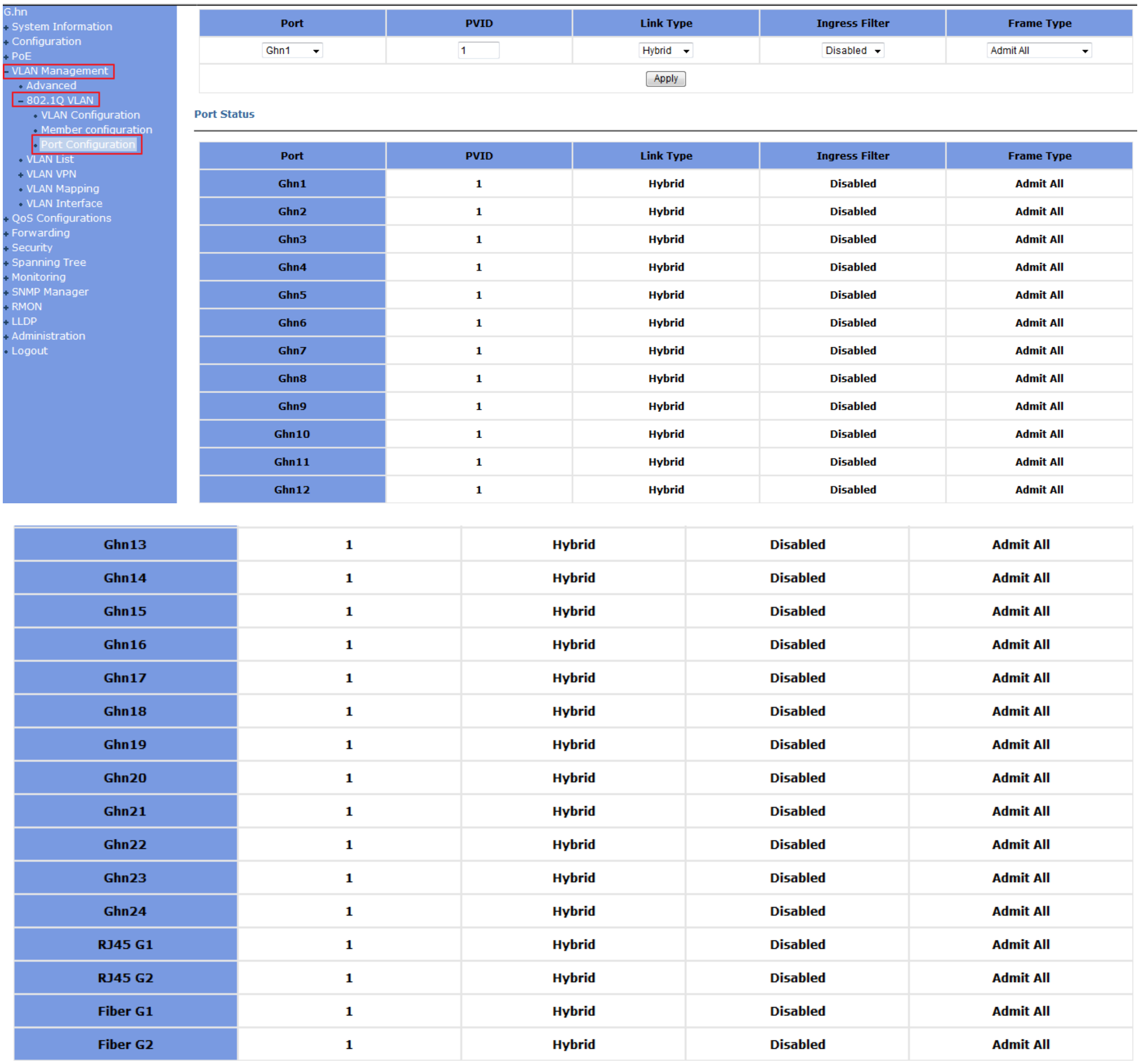
PVID: Each port can have only one Port VLAN ID (PVID), an untagged Ethernet package will be tagged a VID of PVID when arriving at the port. The default PVID is 1 for each port.

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.



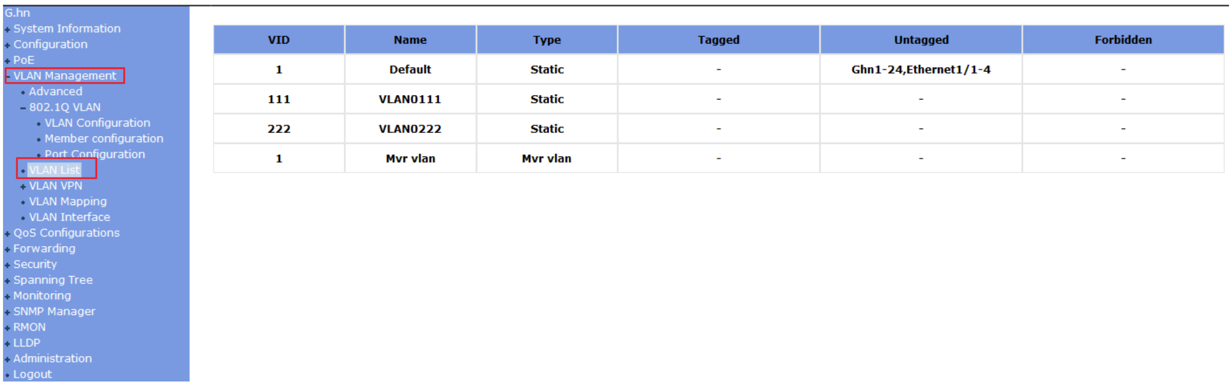
Port	PVID	Link Type	Ingress Filter	Frame Type
Ghn1	1	Hybrid	Disabled	Admit All

Port Status

Port	PVID	Link Type	Ingress Filter	Frame Type
Ghn1	1	Hybrid	Disabled	Admit All
Ghn2	1	Hybrid	Disabled	Admit All
Ghn3	1	Hybrid	Disabled	Admit All
Ghn4	1	Hybrid	Disabled	Admit All
Ghn5	1	Hybrid	Disabled	Admit All
Ghn6	1	Hybrid	Disabled	Admit All
Ghn7	1	Hybrid	Disabled	Admit All
Ghn8	1	Hybrid	Disabled	Admit All
Ghn9	1	Hybrid	Disabled	Admit All
Ghn10	1	Hybrid	Disabled	Admit All
Ghn11	1	Hybrid	Disabled	Admit All
Ghn12	1	Hybrid	Disabled	Admit All
Ghn13	1	Hybrid	Disabled	Admit All
Ghn14	1	Hybrid	Disabled	Admit All
Ghn15	1	Hybrid	Disabled	Admit All
Ghn16	1	Hybrid	Disabled	Admit All
Ghn17	1	Hybrid	Disabled	Admit All
Ghn18	1	Hybrid	Disabled	Admit All
Ghn19	1	Hybrid	Disabled	Admit All
Ghn20	1	Hybrid	Disabled	Admit All
Ghn21	1	Hybrid	Disabled	Admit All
Ghn22	1	Hybrid	Disabled	Admit All
Ghn23	1	Hybrid	Disabled	Admit All
Ghn24	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

3.4.3 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	-	Ghn1-24,Ethernet1/1-4	-
111	VLAN0111	Static	-	-	-
222	VLAN0222	Static	-	-	-
1	Mvr vlan	Mvr vlan	-	-	-

3.4.4 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.

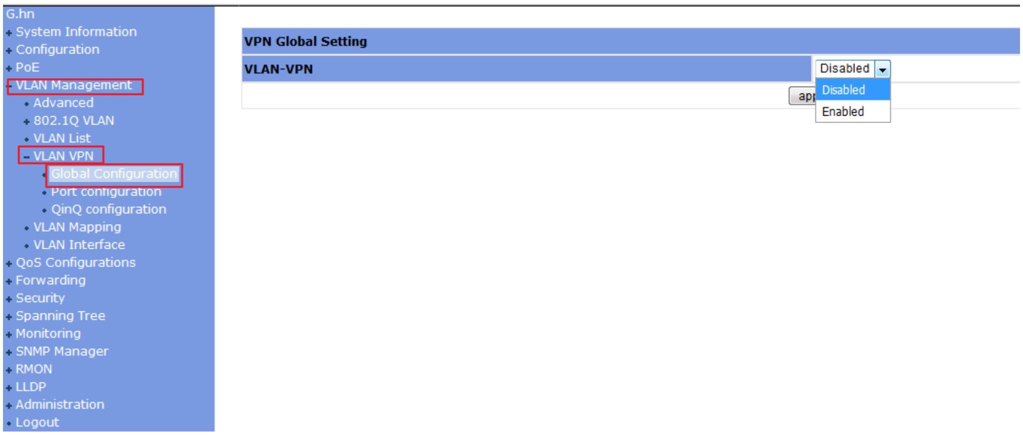
This VLAN VPN function is implemented on the **VPN Config** and **Port Enable** pages.

This page allows you to enable the VPN function, adjust the global TPID for VLAN-VPN packets and enable the VPN up-link port. When VPN mode is enabled, the switch will add a tag to the received tagged packet based on the PVID of the received port.

3.4.4.1 VPN Global Setting

This page enables or disables global VLAN VPN.

VLAN VPN: enable or disable the global VLAN VPN.



VPN Global Setting

VLAN-VPN: Disabled

3.4.4.2 VLAN VPN Port

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.

G4224 series switches adopt the protocol default TPID value (0x8100). Other vendors use other TPID values (such as 0x9100 or 0x9200) in the outer tags of VLAN-VPN packets. To be compatible with devices coming from other vendors, G4224 series switches can adjust the TPID values of VLAN-VPN packets based on ports. You can configure the TPID value of a port connecting to the public network side by yourself. When a packet is forwarded through the port, the port replaces the TPID value in the outer VLAN tag of this packet with the user-defined value. Thus, the VLAN-VPN packets sent to the public network can be recognized by devices of other vendors.

As the position of the TPID field in an Ethernet packet is the same as that of the protocol type field in a packet without VLAN Tag, to avoid confusion in the process of receiving/forwarding a packet, the TPID value cannot be any of the Commonly used protocol type values in Ethernet frames listed in the following table.

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

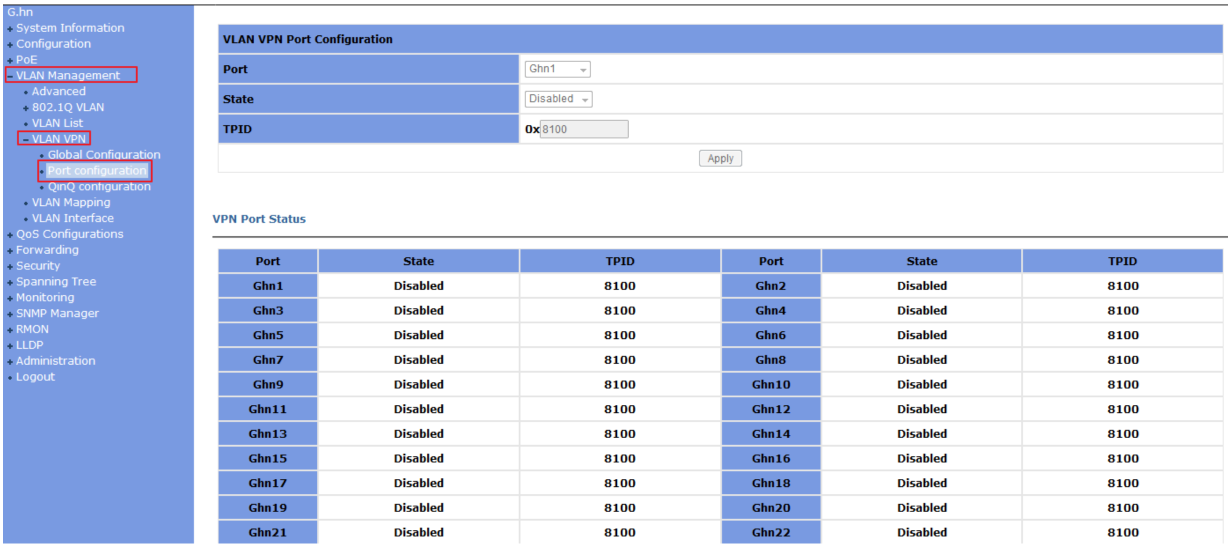
Configuration Steps:

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.

Then the VLAN VPN Port Configuration will be listed at the bottom.



VLAN VPN Port Configuration

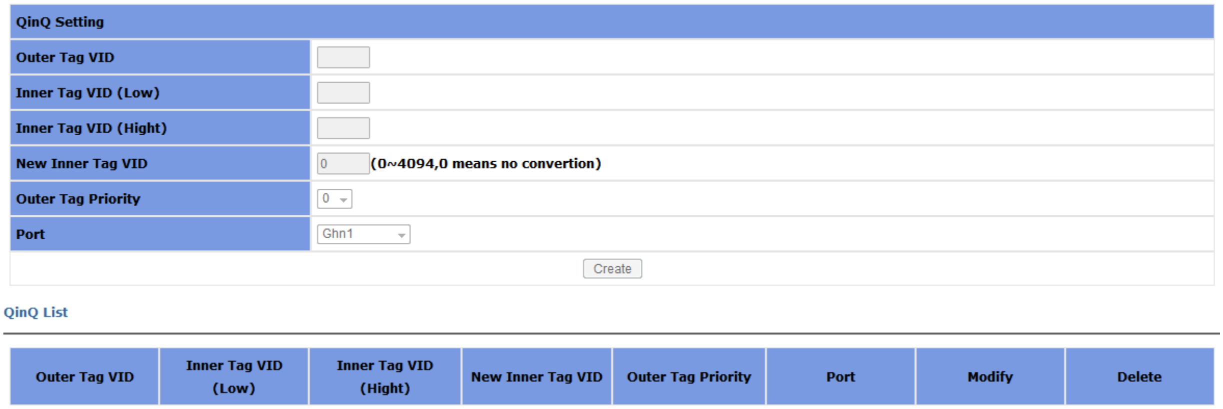
Port	Ghn1
State	Disabled
TPID	0x 8100

VPN Port Status

Port	State	TPID	Port	State	TPID
Ghn1	Disabled	8100	Ghn2	Disabled	8100
Ghn3	Disabled	8100	Ghn4	Disabled	8100
Ghn5	Disabled	8100	Ghn6	Disabled	8100
Ghn7	Disabled	8100	Ghn8	Disabled	8100
Ghn9	Disabled	8100	Ghn10	Disabled	8100
Ghn11	Disabled	8100	Ghn12	Disabled	8100
Ghn13	Disabled	8100	Ghn14	Disabled	8100
Ghn15	Disabled	8100	Ghn16	Disabled	8100
Ghn17	Disabled	8100	Ghn18	Disabled	8100
Ghn19	Disabled	8100	Ghn20	Disabled	8100
Ghn21	Disabled	8100	Ghn22	Disabled	8100

3.4.4.3 QinQ

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)	
New Inner Tag VID	0 (0~4094,0 means no convertion)
Outer Tag Priority	0
Port	Ghn1

QinQ List

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

Outer Tag VID: Outer vid

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.

New Inner Tag VID:A VLAN ID for replaced the old inner tag

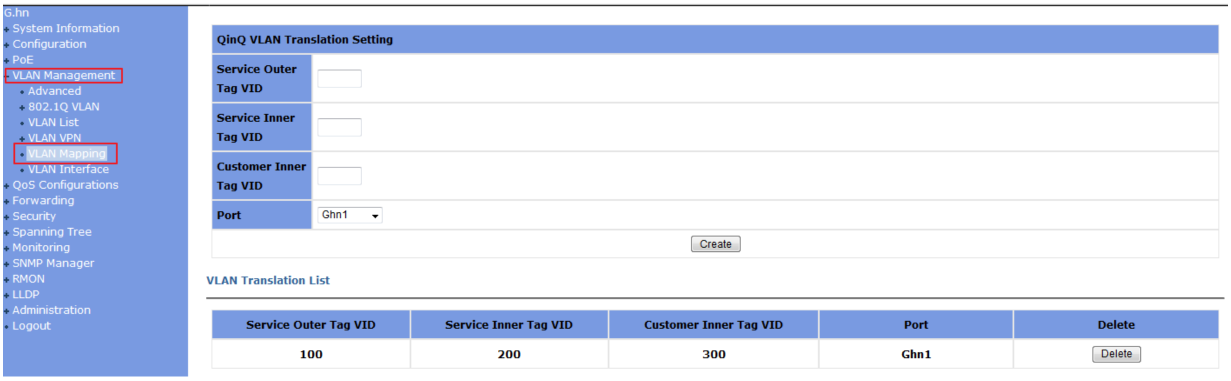
Port: the port from which a package is received

Note: Before use this function, you must enable QinQ of global and port.

3.4.5 VLAN Mapping

With the increasing application of the Internet, the VLAN Mapping (QinQ VLAN Transmission) technology is developed and used to establish the private network through the operators' backbone networks. The VLAN Mapping 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.

You can set the VLAN Mapping for ports as below:



QinQ VLAN Translation Setting

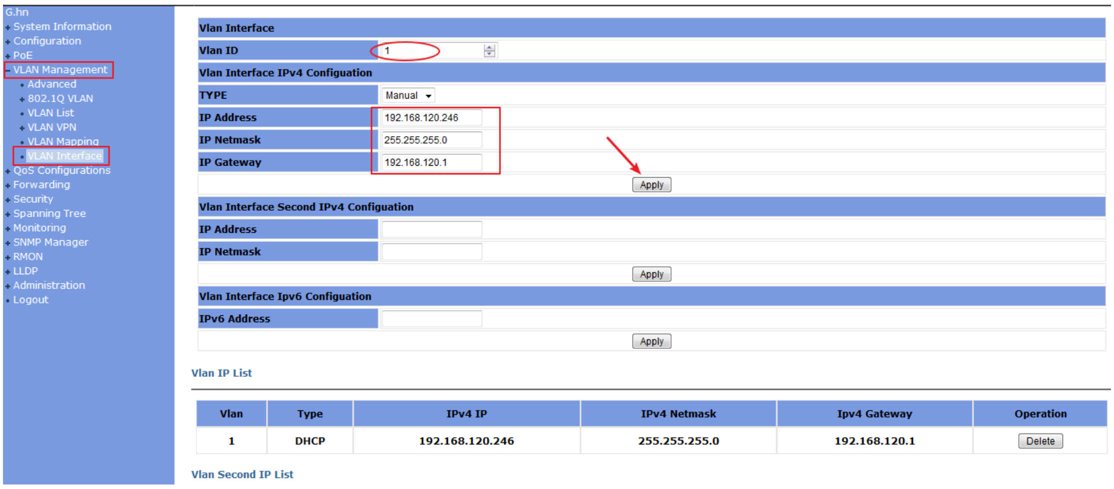
Service Outer Tag VID	
Service Inner Tag VID	
Customer Inner Tag VID	
Port	Ghn1

VLAN Translation List

Service Outer Tag VID	Service Inner Tag VID	Customer Inner Tag VID	Port	Delete
100	200	300	Ghn1	Delete

3.4.6 VLAN Interface

You can configure IP address for G4224 switch from this page as below



Vlan Interface

Vlan ID	1

Vlan Interface IPv4 Configuation

TYPE	Manual
IP Address	192.168.120.246
IP Netmask	255.255.255.0
IP Gateway	192.168.120.1

Vlan Interface Second IPv4 Configuation

IP Address	
IP Netmask	

Vlan Interface Ipv6 Configuation

IPv6 Address	

Vlan IP List

Vlan	Type	IPv4 IP	IPv4 Netmask	Ipv4 Gateway	Operation
1	DHCP	192.168.120.246	255.255.255.0	192.168.120.1	Delete

Vlan Second IP List

3.5 Qos Configuration

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 possibly 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.

3.5.1 Rate Limit

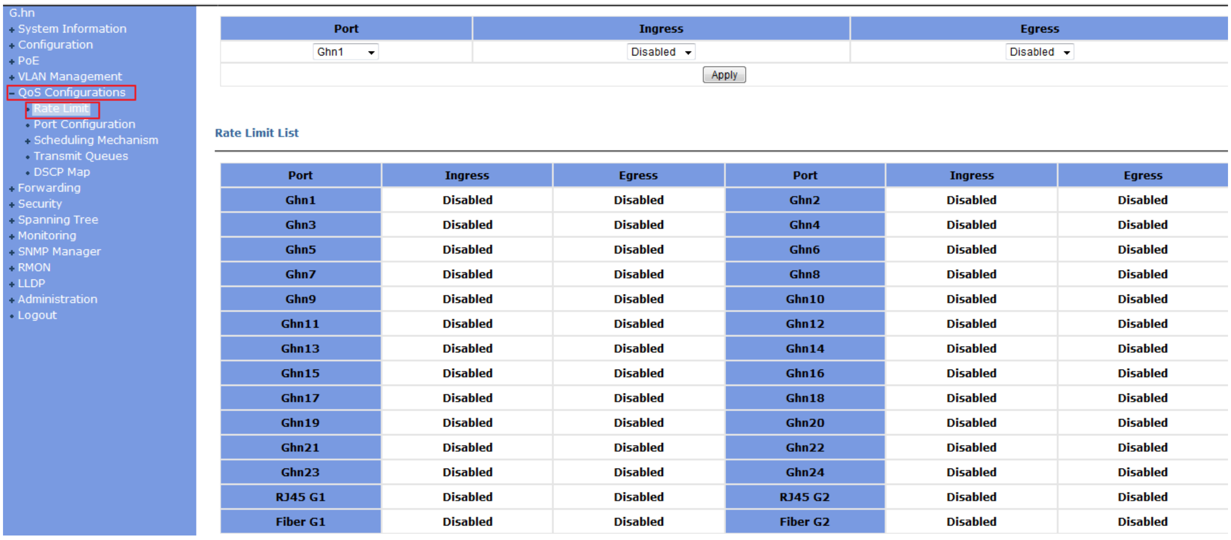
You can configure the egress traffic limit on individual ports, so as to keep normal network service. The bottom of the page will show the rate limit list.

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



Port	Ingress	Egress
Ghn1	Disabled	Disabled

Rate Limit List

Port	Ingress	Egress	Port	Ingress	Egress
Ghn1	Disabled	Disabled	Ghn2	Disabled	Disabled
Ghn3	Disabled	Disabled	Ghn4	Disabled	Disabled
Ghn5	Disabled	Disabled	Ghn6	Disabled	Disabled
Ghn7	Disabled	Disabled	Ghn8	Disabled	Disabled
Ghn9	Disabled	Disabled	Ghn10	Disabled	Disabled
Ghn11	Disabled	Disabled	Ghn12	Disabled	Disabled
Ghn13	Disabled	Disabled	Ghn14	Disabled	Disabled
Ghn15	Disabled	Disabled	Ghn16	Disabled	Disabled
Ghn17	Disabled	Disabled	Ghn18	Disabled	Disabled
Ghn19	Disabled	Disabled	Ghn20	Disabled	Disabled
Ghn21	Disabled	Disabled	Ghn22	Disabled	Disabled
Ghn23	Disabled	Disabled	Ghn24	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 aggregation ports.

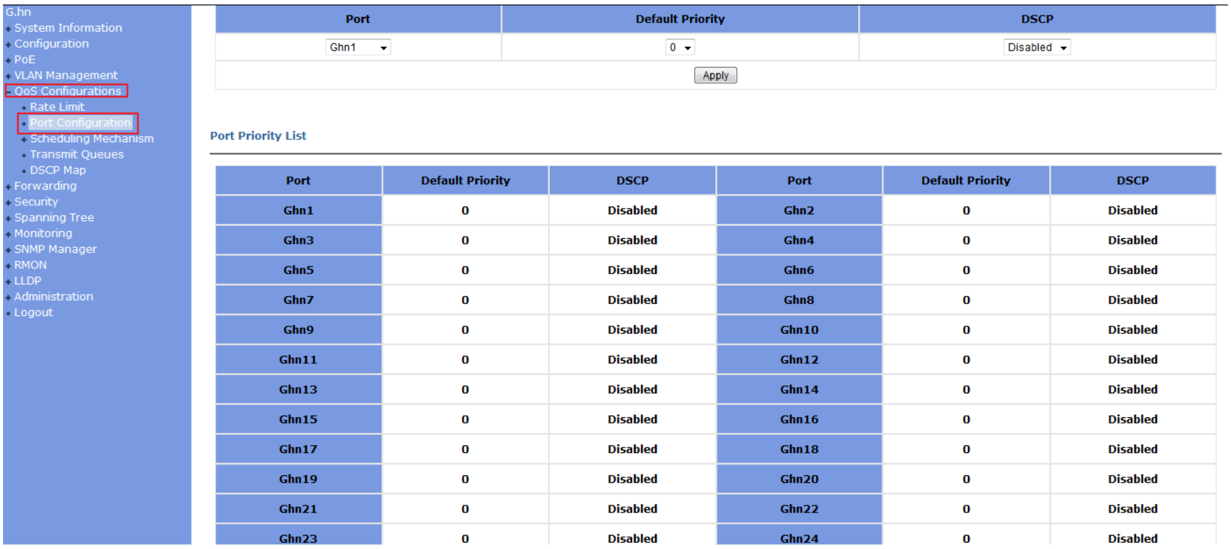
3.5.2 Port Configuration

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

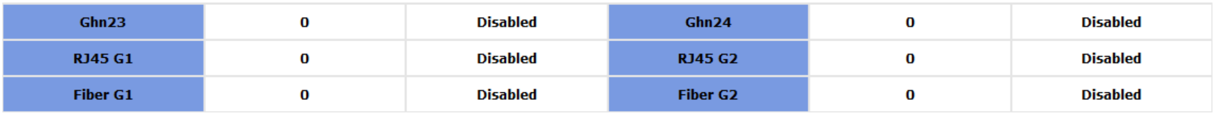
The lower part of QoS Configuration tab page lists the default priority of all ports and the state of DSCP.



Port	Default Priority	DSCP
Ghn1	0	Disabled

Port Priority List

Port	Default Priority	DSCP	Port	Default Priority	DSCP
Ghn1	0	Disabled	Ghn2	0	Disabled
Ghn3	0	Disabled	Ghn4	0	Disabled
Ghn5	0	Disabled	Ghn6	0	Disabled
Ghn7	0	Disabled	Ghn8	0	Disabled
Ghn9	0	Disabled	Ghn10	0	Disabled
Ghn11	0	Disabled	Ghn12	0	Disabled
Ghn13	0	Disabled	Ghn14	0	Disabled
Ghn15	0	Disabled	Ghn16	0	Disabled
Ghn17	0	Disabled	Ghn18	0	Disabled
Ghn19	0	Disabled	Ghn20	0	Disabled
Ghn21	0	Disabled	Ghn22	0	Disabled
Ghn23	0	Disabled	Ghn24	0	Disabled



Ghn23	0	Disabled	Ghn24	0	Disabled
RJ45 G1	0	Disabled	RJ45 G2	0	Disabled
Fiber G1	0	Disabled	Fiber G2	0	Disabled

3.5.3 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)**

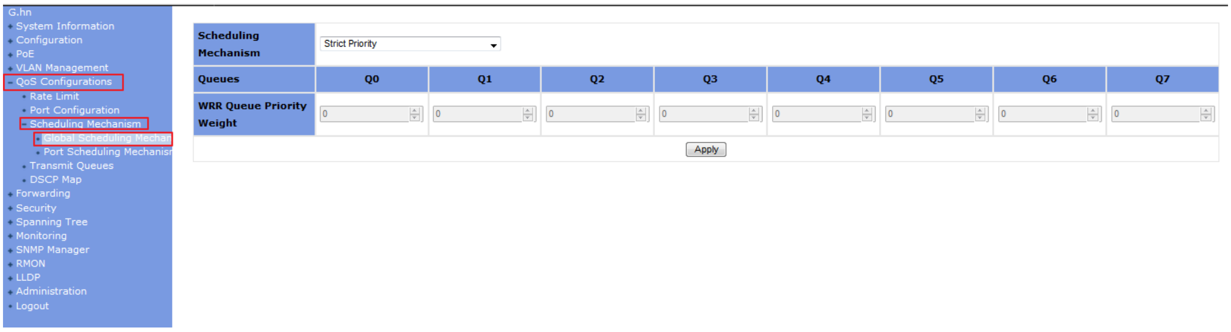
Strict Priority: SP queue-scheduling algorithm is specially designed for critical service applications. An important feature of critical services is that they demand preferential service in congestion in order to reduce the response delay. Assume that there are eight output queues on the port and the 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.

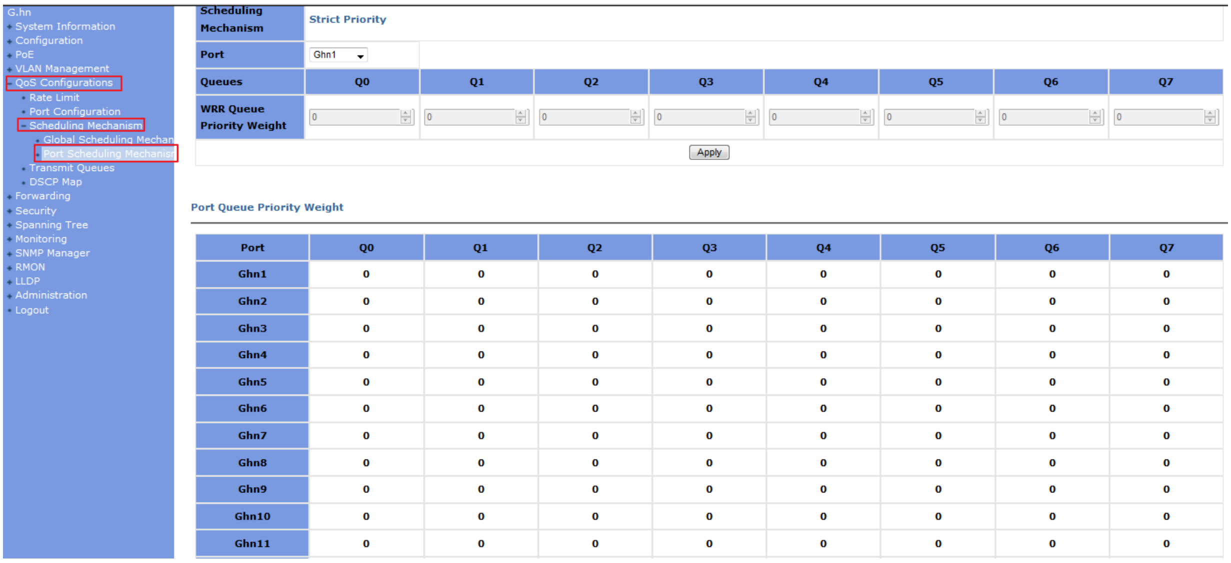
The disadvantage of SP queue is that: if there are packets in the queues with higher priority for a long time in congestion, the packets in the queues with lower priority will be “starved” because they are not served.

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 are made full use.

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



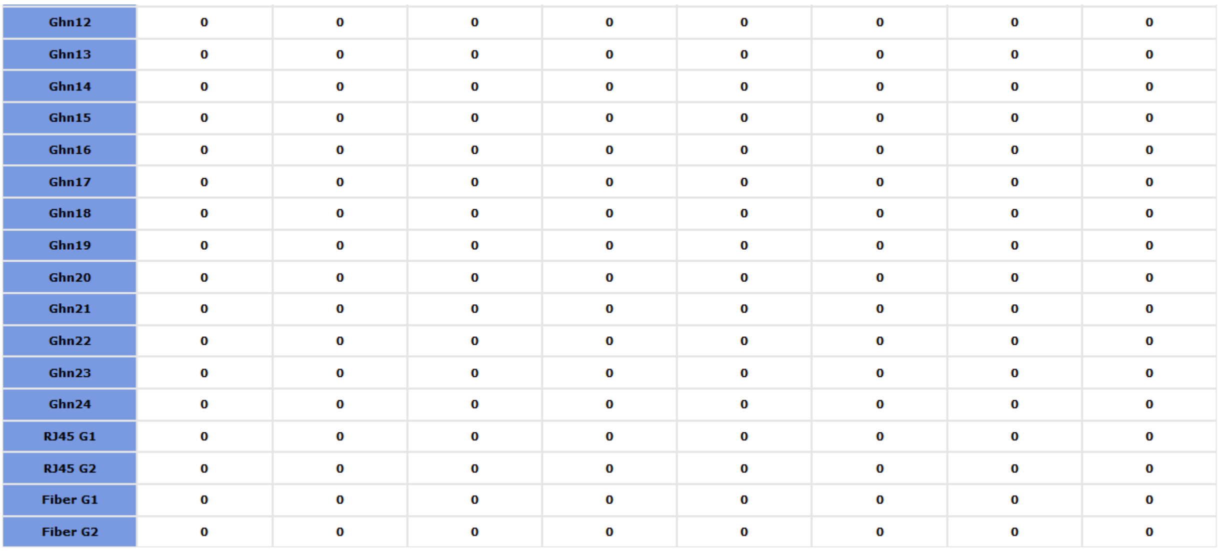
Scheduling Mechanism	Strict Priority							
Queues	Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7
WRR Queue Priority Weight	0	0	0	0	0	0	0	0



Scheduling Mechanism	Strict Priority							
Port	Ghn1							
Queues	Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7
WRR Queue Priority Weight	0	0	0	0	0	0	0	0

Port Queue Priority Weight

Port	Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7
Ghn1	0	0	0	0	0	0	0	0
Ghn2	0	0	0	0	0	0	0	0
Ghn3	0	0	0	0	0	0	0	0
Ghn4	0	0	0	0	0	0	0	0
Ghn5	0	0	0	0	0	0	0	0
Ghn6	0	0	0	0	0	0	0	0
Ghn7	0	0	0	0	0	0	0	0
Ghn8	0	0	0	0	0	0	0	0
Ghn9	0	0	0	0	0	0	0	0
Ghn10	0	0	0	0	0	0	0	0
Ghn11	0	0	0	0	0	0	0	0



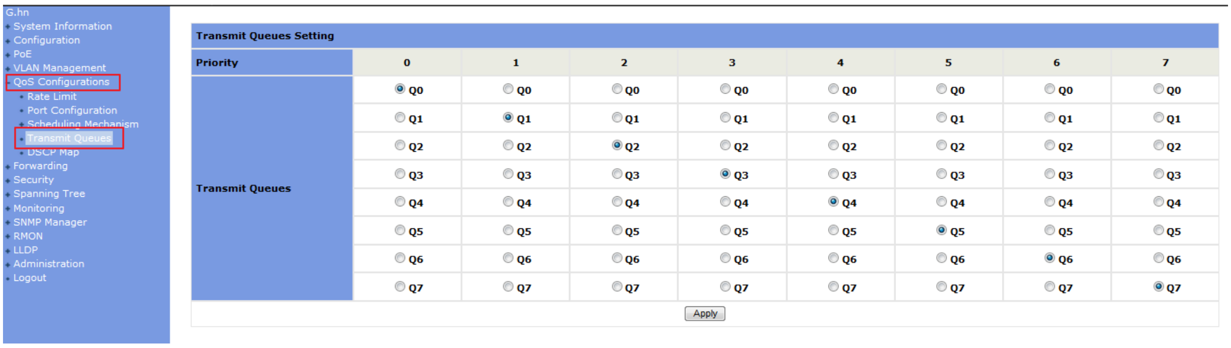
Ghn12	0	0	0	0	0	0	0	0
Ghn13	0	0	0	0	0	0	0	0
Ghn14	0	0	0	0	0	0	0	0
Ghn15	0	0	0	0	0	0	0	0
Ghn16	0	0	0	0	0	0	0	0
Ghn17	0	0	0	0	0	0	0	0
Ghn18	0	0	0	0	0	0	0	0
Ghn19	0	0	0	0	0	0	0	0
Ghn20	0	0	0	0	0	0	0	0
Ghn21	0	0	0	0	0	0	0	0
Ghn22	0	0	0	0	0	0	0	0
Ghn23	0	0	0	0	0	0	0	0
Ghn24	0	0	0	0	0	0	0	0
RJ45 G1	0	0	0	0	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

3.5.4 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>.

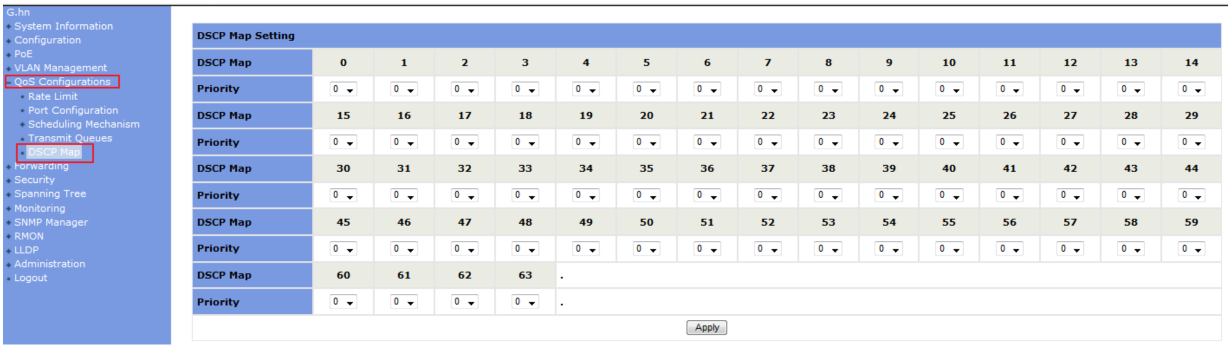


Transmit Queues Setting

Priority	0	1	2	3	4	5	6	7
Transmit Queues	● Q0	○ Q0	○ Q0	○ Q0	○ Q0	○ Q0	○ Q0	○ Q0
	○ 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
	○ Q5	○ Q5	○ Q5	○ Q5	○ Q5	● Q5	○ Q5	○ Q5
	○ Q6	○ Q6	○ Q6	○ Q6	○ Q6	○ Q6	● Q6	○ Q6
	○ Q7	○ Q7	○ Q7	○ Q7	○ Q7	○ Q7	○ Q7	● Q7

3.5.5 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	.										

3.6 Forwarding

G4224 has unicast MAC address forwarding, multicast MAC address forwarding, IGMP Snooping, MVR, unknown multicast the introduction is followed.

3.6.1 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.

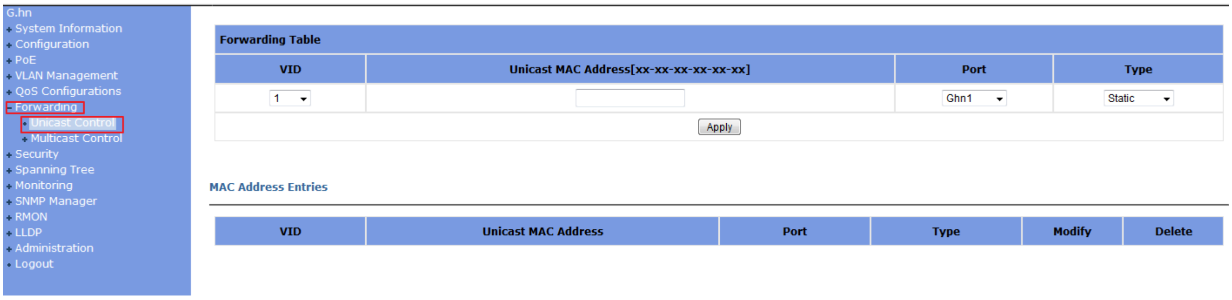
Type Choose among **Dynamic, Static and Blackhole**.

- Static MAC address entry: Also known as permanent MAC address entry. This type of MAC address entries is 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: This type of MAC address entries age out after the configured aging time. They are generated by the MAC address learning mechanism or configured manually.

- Blackhole MAC address entry: This type of MAC address entries is 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 address 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		Ghn1	Static

Apply

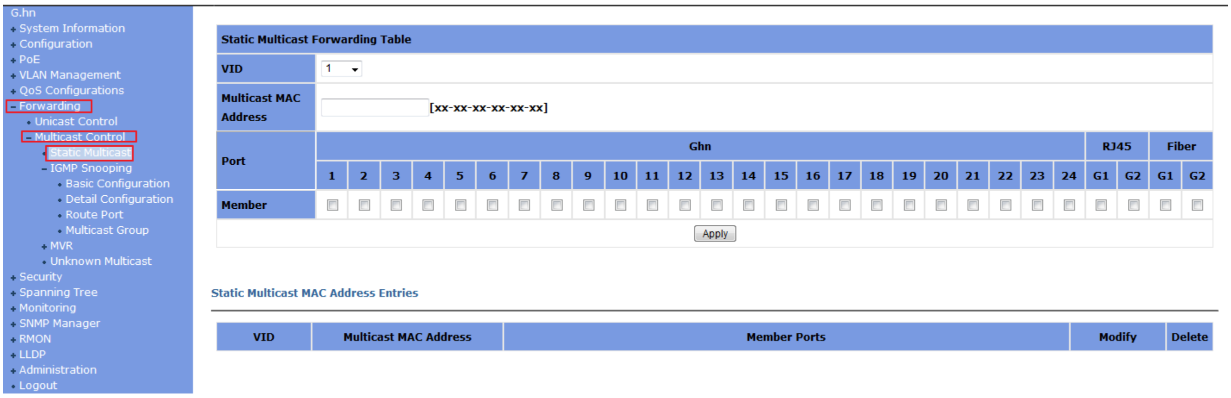
MAC Address Entries

VID	Unicast MAC Address	Port	Type	Modify	Delete

3.6.2 Multicast Control

3.6.2.1 Static Multicast

In this page, you can configure static multicast for ports as below:



Static Multicast Forwarding Table

VID	1																											
Multicast MAC Address	[xx-xx-xx-xx-xx-xx]																											
Port	Ghn																								RJ45		Fiber	
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	G1	G2	G1	G2
Member	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□

Apply

Static Multicast MAC Address Entries

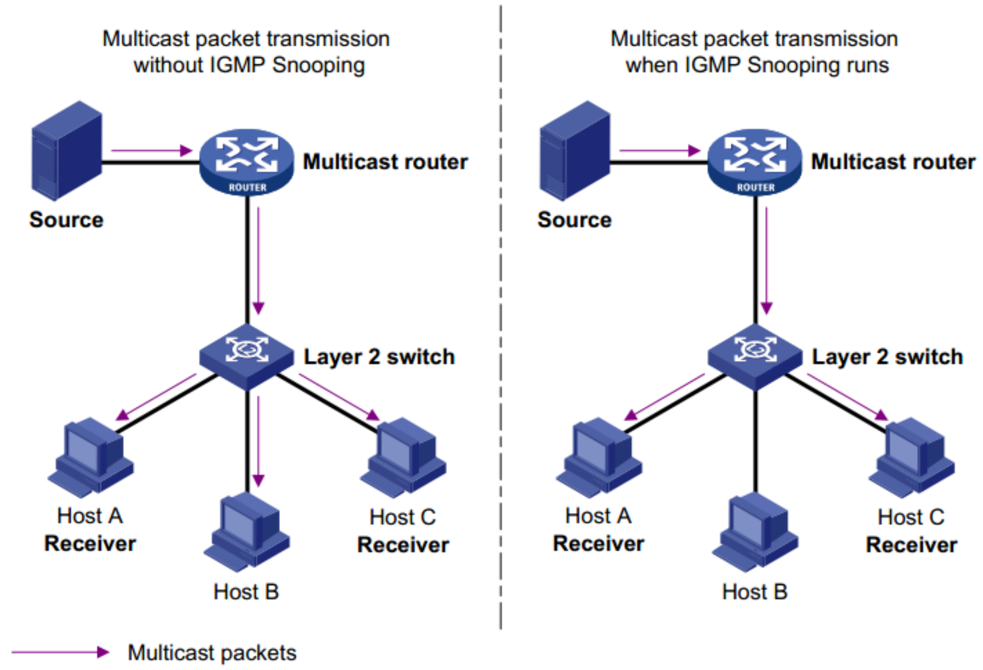
VID	Multicast MAC Address	Member Ports	Modify	Delete

3.6.2.2 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 broadcast 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 time 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.

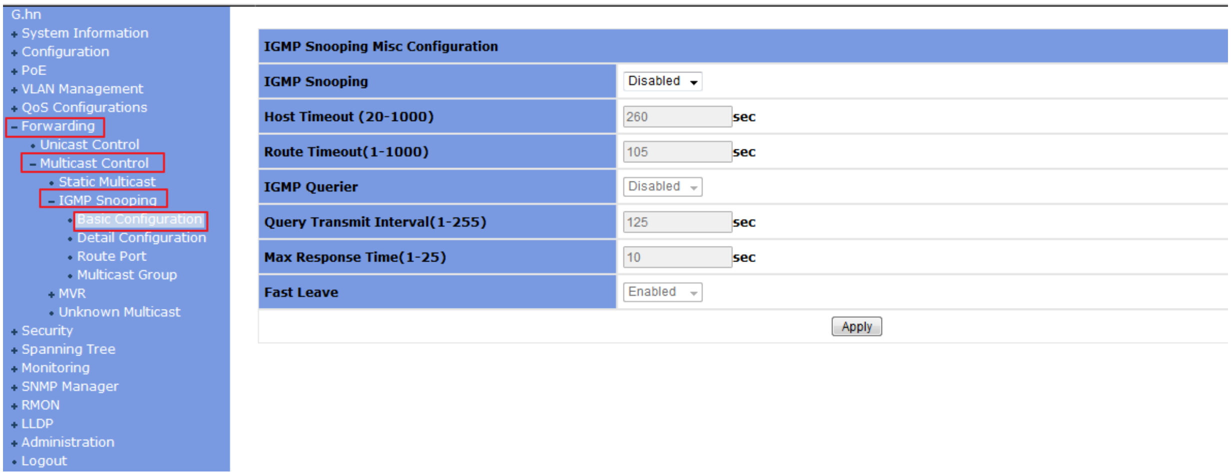
Route Timeout The switch starts Router Timeout for each router port when it time out, it will be deleted from the router port list. It is in the range of 1 to 1000; by default, the value is 105 seconds.

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 form the group. It is in the range of 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	Disabled
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 IGMP Snooping feature for a VLAN group. By default, the IGMP Snooping feature is disabled.

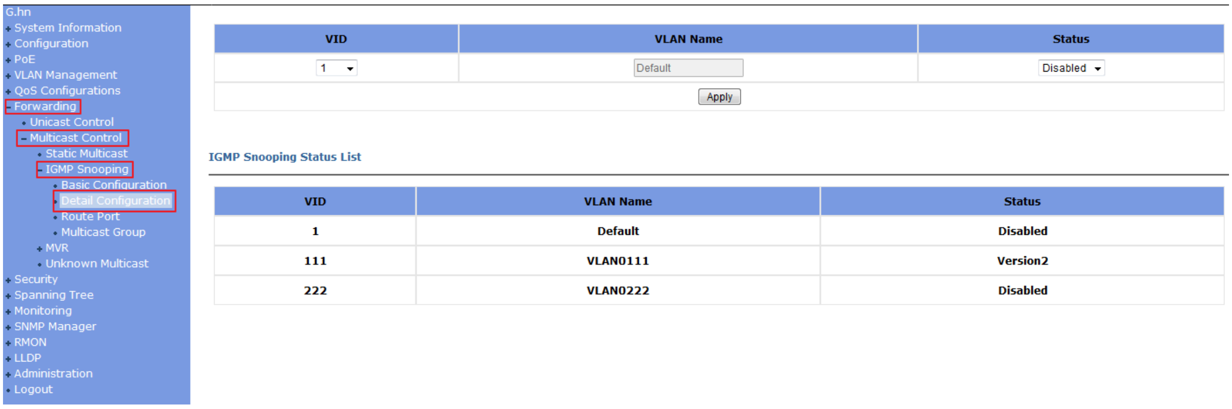
With the wide use of multicast, IGMPv3 is used more and more. It adds the multicast source filtering function, which enabled the receiver be able to specify the multicast group to join in as well as specify the multicast source to receive multicast information from.

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 enable it, 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
111	VLAN0111	Version2
222	VLAN0222	Disabled

(3) Route Port

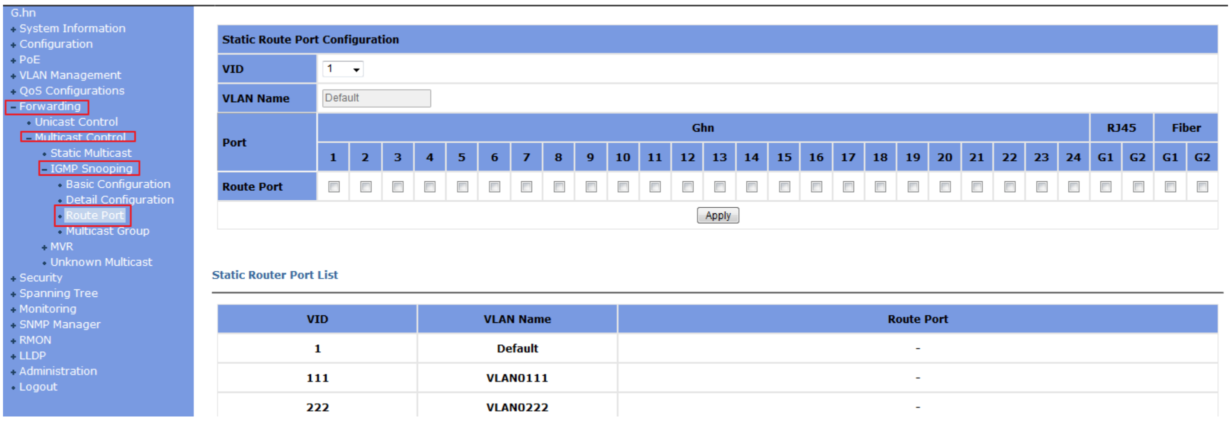
On this page, you can configure a port in a specified VLAN group as a static router port. By default, a port is not a static router port.

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. Please refer to 3.3 VLAN.



Static Route Port Configuration

VID	1
VLAN Name	Default

Port	Ghn																								RJ45		Fiber	
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	G1	G2	G1	G2
Route Port	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□

Apply

Static Router Port List

VID	VLAN Name	Route Port
1	Default	-
111	VLAN0111	-
222	VLAN0222	-

(4) Multicast Group

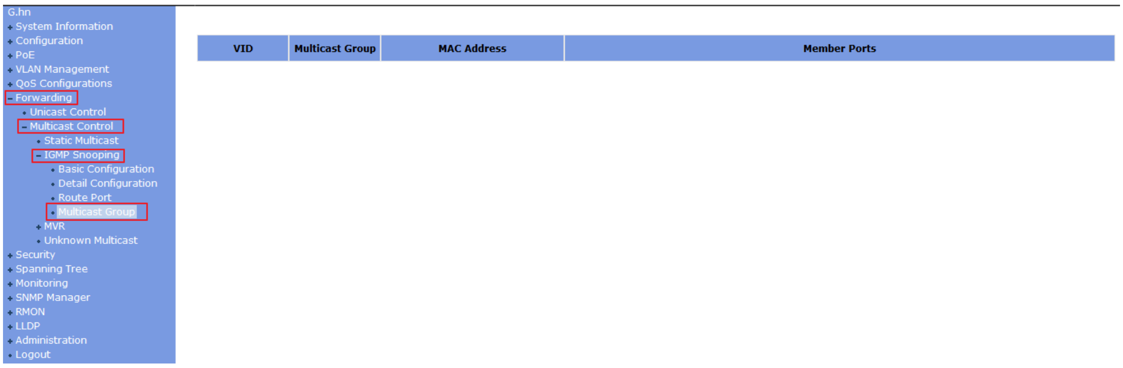
This page shows IGMP Snooping multicast group information.

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

3.6.2.3 MVR Snooping

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.

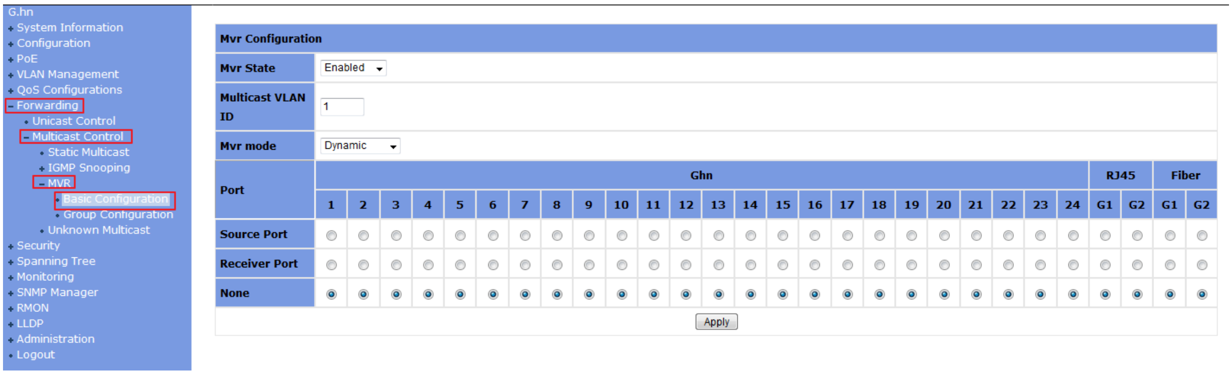
MVR Mode Choose the mode between **compatible** and **dynamic**.

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	Enabled
Multicast VLAN ID	1
Mvr mode	Dynamic

Port	Ghn																								RJ45		Fiber	
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	G1	G2	G1	G2
Source Port	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Receiver Port	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
None	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●

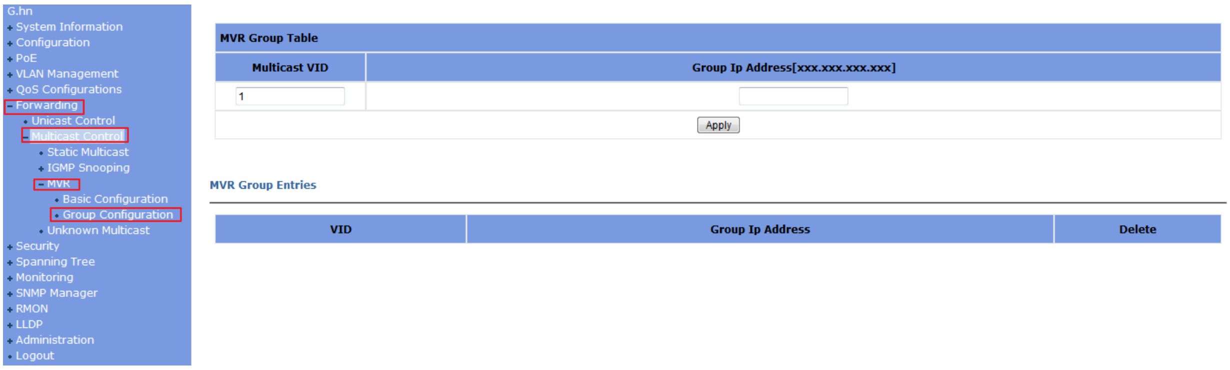
（2） Group Configuration

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.



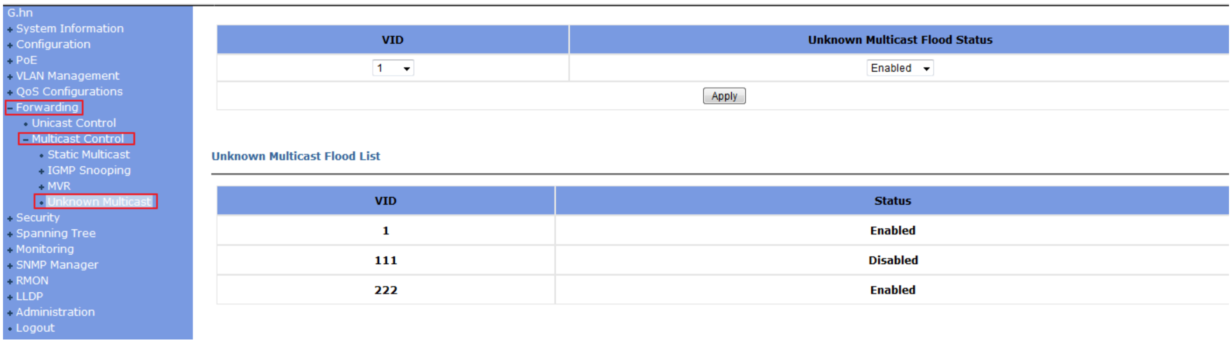
MVR Group Table

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

MVR Group Entries

VID	Group Ip Address	Delete

3.6.2.4 Unknown Multicast



VID	Unknown Multicast Flood Status
1	Enabled

Unknown Multicast Flood List

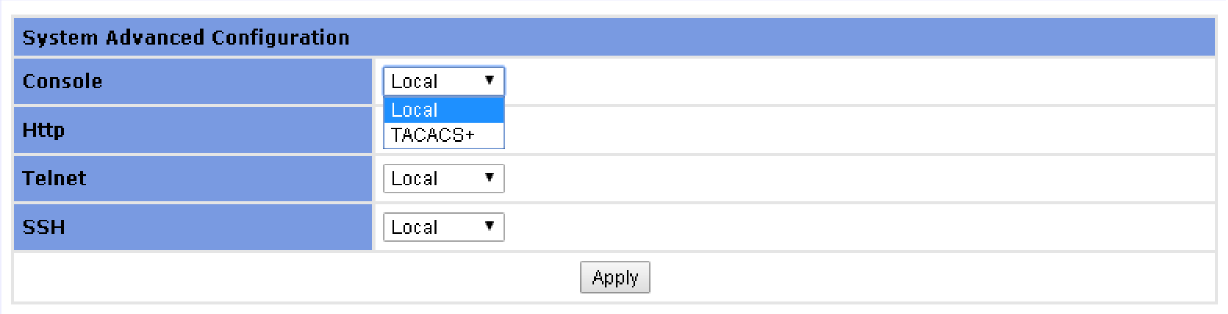
VID	Status
1	Enabled
111	Disabled
222	Enabled

3.7 Security

3.7.1 Switch Management

3.7.1.1 Login Options

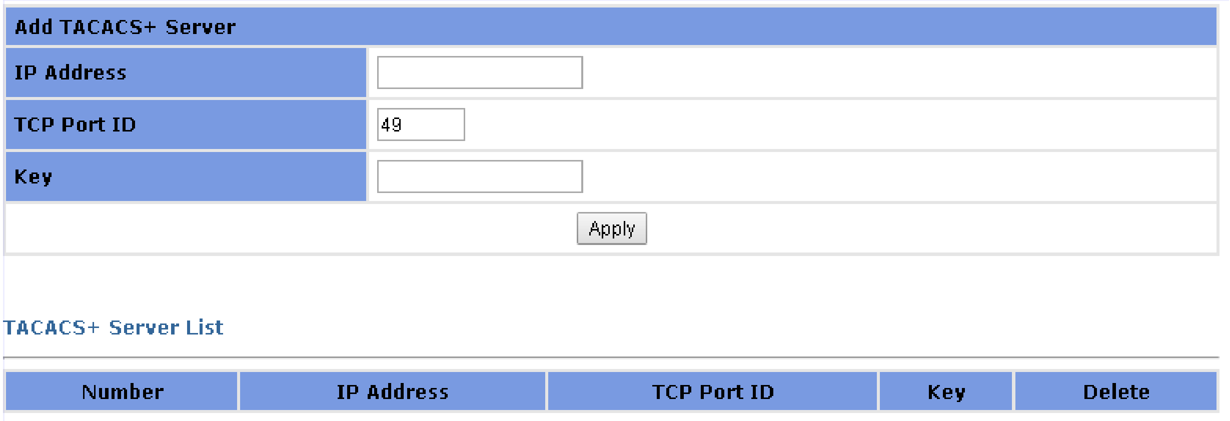
There are four switch management login options, including via serial console, http, telnet and SSH. The user can login into the system using Local and TACACS+ authentication for each option. Here “Local” means the user can login with default account and password or the account created, details please see the “Account” tab under the “Administration”. The default account is “superuser” with default password of “123”. The default and created account and password are stored in the system locally. While “TACACS+” means the user can login with account and password created on TACACS+ server. Before using TACACS+ option, the TACACS+ server has to be assigned with IP address, TCP port ID and Key. While on the TACACS+ server, the user name and password need to be created.



System Advanced Configuration	
Console	Local ▼ Local TACACS+
Http	
Telnet	Local ▼
SSH	Local ▼
	Apply

3.7.1.2 TACACS+ Configuration

As mentioned before, the system manager can login to the system using TACACS+ option. The following page shows the information needed to be configured for the TACACS+ server.



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.

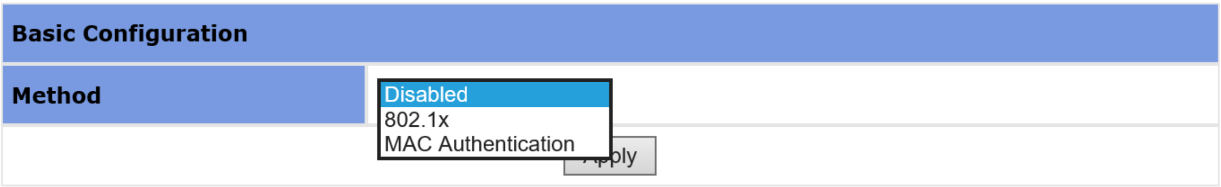
TCP Port ID Configure TCP transmission port number, range is 0~65535， the default value is 49. Normally, default configuration ID should be OK.

Encryption Key Configure the same key as TACACS+ server.

3.7.2 802.1x Port Authentication

3.7.2.1 User Authentication Options

The system provides two user authentication options to validate the user connected to each port when any of the authentication option is enabled. To enable 802.1x authentication option, you need to select “802.1x” option on the “Basic Configuration” under the “Method” tab page as shown below.



Basic Configuration	
Method	Disabled

For 802.1x port authentication, the configuration procedures include:

[Step 1]. Select “802.1x” option on “Security/Management/Method” page;

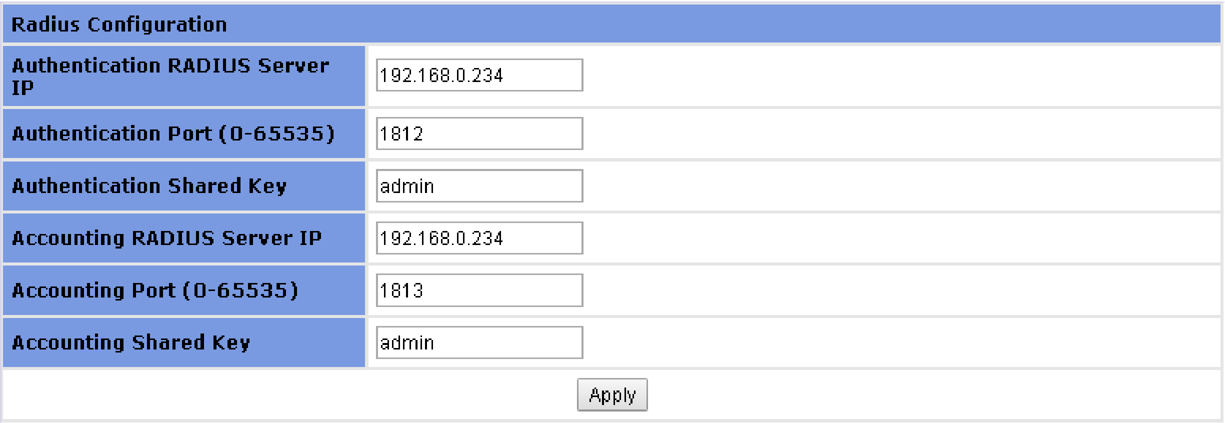
[Step 2]. Add the Radius server information on “Security/Management/Radius” page;

[Step 3]. Add the 802.1x Misc Configuration on “Security/Port Authentication /Basic Configuration” page;

[Step 4]. Configure the associated port on “Security/Port Authentication /802.1x Port-based” page.

3.7.2.2 Radius Server Configuration

In order to use 802.1x user authentication, you need to provide the Radius server information. The information is shown as below in the “Radius Configuration” page under the “Radius” tab.



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.

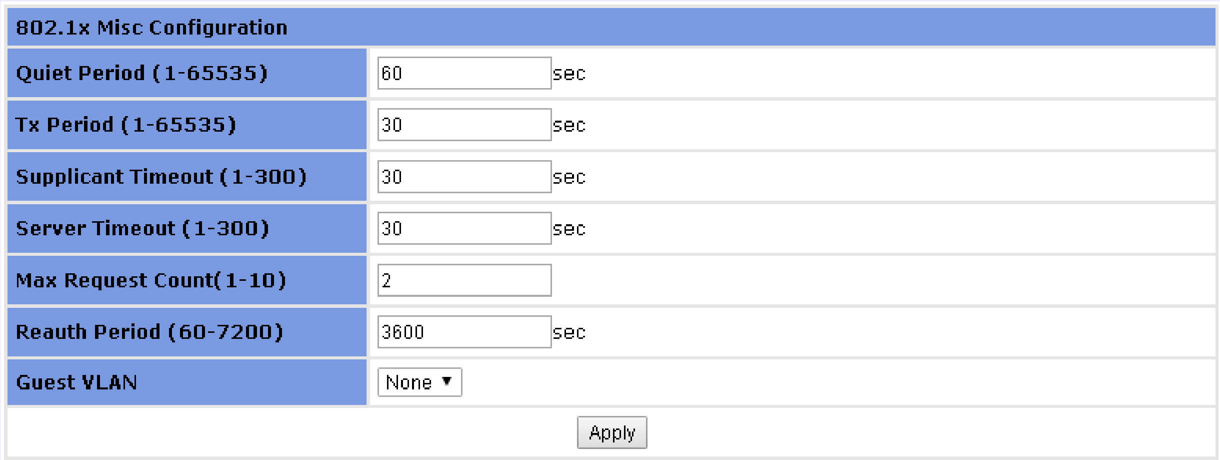
Accounting RADIUS Server IP IP address of accounting radius server to be used, a valid unicast address in dotted decimal notation; the default value is 192.168.0.234.

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.

3.7.2.3 802.1x Basic Configuration

IEEE 802.1x authentication system uses extensible authentication protocol (EAP) to exchange information between users and the authentication servers. When a user passes the authentication, the authentication server passes the information about the user 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 ▼

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

Quiet Period Set the quiet-period, when a user fails to pass the authentication; the switch quiets for the set period before it processes another authentication request re-initiated by the user. During this quiet period, the switch does not perform any 802.1x authentication-related actions for the user. 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 user and then triggers the transmission timer. The switch sends another request/identity packet to the user if it does not receive the reply packet from the user 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 user timer, this timer sets the supplicant timeout period and is triggered by the switch after the switch sends a request/challenge packet to a user. The switch sends another request/challenge packet to the user if the switch does not receive any response from the user 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.

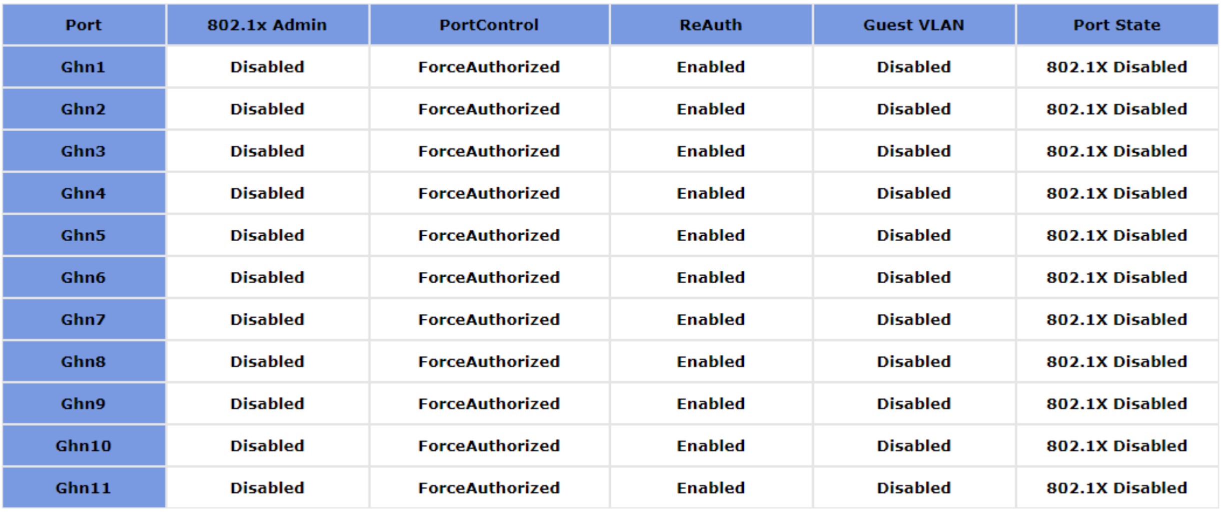
Reauth Period Set re-authentication interval in second. After this timer expires, the switch indicates: 802.1x re-authentication. It is in the range of 60 to 7200; the default value is 60 seconds.

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.

3.7.2.4 802.1x Port-based Authentication

As shown below, the “802.1x Port-based” tab page sets 802.1x port enabling, port control, re-authentication and guest VLAN for a specified user port. Note that there are three configuration options for Port Control, which are Auto, Force Authorized and Force Unauthorized.



Port	802.1x Admin	PortControl	ReAuth	Guest VLAN	Port State
Ghn1	Disabled	ForceAuthorized	Enabled	Disabled	802.1X Disabled
Ghn2	Disabled	ForceAuthorized	Enabled	Disabled	802.1X Disabled
Ghn3	Disabled	ForceAuthorized	Enabled	Disabled	802.1X Disabled
Ghn4	Disabled	ForceAuthorized	Enabled	Disabled	802.1X Disabled
Ghn5	Disabled	ForceAuthorized	Enabled	Disabled	802.1X Disabled
Ghn6	Disabled	ForceAuthorized	Enabled	Disabled	802.1X Disabled
Ghn7	Disabled	ForceAuthorized	Enabled	Disabled	802.1X Disabled
Ghn8	Disabled	ForceAuthorized	Enabled	Disabled	802.1X Disabled
Ghn9	Disabled	ForceAuthorized	Enabled	Disabled	802.1X Disabled
Ghn10	Disabled	ForceAuthorized	Enabled	Disabled	802.1X Disabled
Ghn11	Disabled	ForceAuthorized	Enabled	Disabled	802.1X Disabled

Here are the configuration steps:

Step 1 Specify the port needed to be configured for 802.1x authentication.

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

Step 2 Enable or disable the 802.1x authentication function.

Step 3 When 802.1x authentication is enabled, you need to further configure Port Control operation accordingly, the operation definitions are shown as below:

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 function.

Step 5 Enable or disable Guest VLAN.

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

3.7.3 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.

As mentioned before, the system provides two user authentication options to validate the user connected to each port when any of the authentication option is enabled. To enable MAC authentication option, first you need to select “MAC Authentication” on the “Basic Configuration” under the “Method” tab page. For MAC authentication, the configuration procedures include:

[Step 1]. Select “MAC authentication” option on “Security/Management/Method” page;

[Step 2]. Add the Radius server information on “Security/Management/Radius” page;

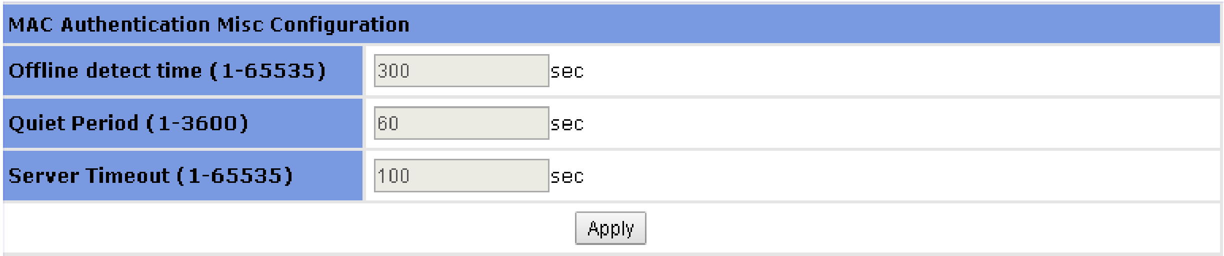
[Step 3]. Add the timer parameters of MAC Authentication Misc Configuration on “Security/MAC Authentication /Basic Configuration” page;

[Step 4]. Enable/disable the associated port on “Security/MAC Authentication /Port Configuration” page;

[Step 5]. Check the Authentication information on “Security/MAC Authentication /Authentication Infor” page.

3.7.3.1 Basic Configuration

The basic timer information for the MAC authentication is shown below.



MAC Authentication Misc Configuration

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

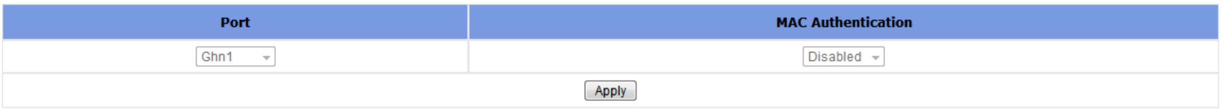
Offline Detect Time At this interval, the switch checks to see whether there is traffic from a user. Once detecting that there is no traffic from a user within this interval, the switch logs the user out and sends to the Radius server a stop accounting request. The value is in the range of 1 to 65535 seconds, and is set to 300 seconds by default.

Quiet Period Whenever a user fails MAC authentication, the switch does not perform MAC authentication of the user during such a period. The value is in the range of 1 to 3600 seconds, and is set to 60 seconds by default.

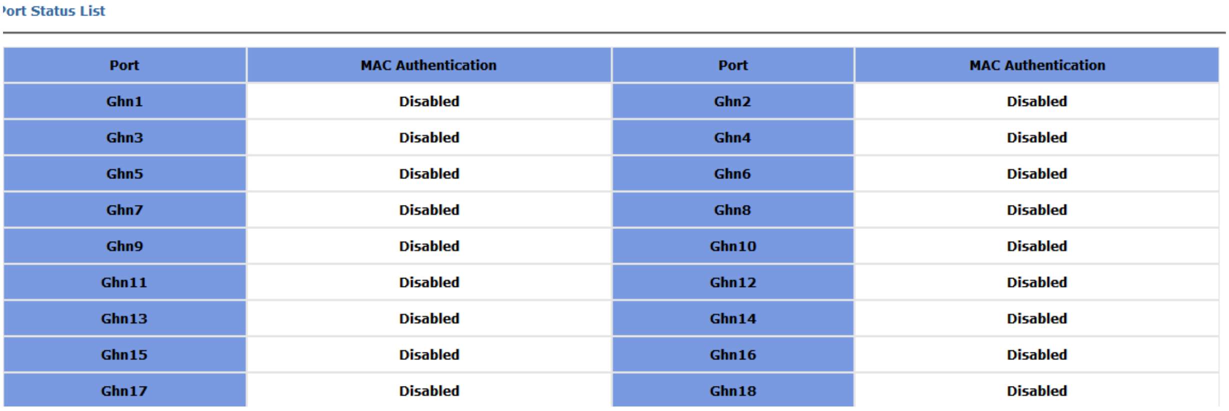
Server Timeout During authentication of a user, if the switch receives no response from the RADIUS server in this period, it assumes that its connection to the RADIUS server has timed out and forbids the user to access the network. It is in the range of 1 to 65535 seconds; the default value is 100 seconds.

3.7.3.2 Port Configuration

The following page is used to enable or disable the **MAC Authentication** function for a specific port. The lower part of the page lists the configuration status for all ports.



Port	MAC Authentication
Ghn1	Disabled

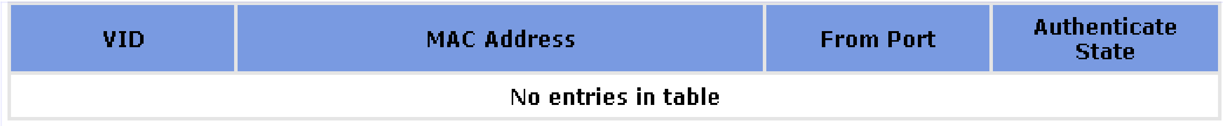


ort Status List

Port	MAC Authentication	Port	MAC Authentication
Ghn1	Disabled	Ghn2	Disabled
Ghn3	Disabled	Ghn4	Disabled
Ghn5	Disabled	Ghn6	Disabled
Ghn7	Disabled	Ghn8	Disabled
Ghn9	Disabled	Ghn10	Disabled
Ghn11	Disabled	Ghn12	Disabled
Ghn13	Disabled	Ghn14	Disabled
Ghn15	Disabled	Ghn16	Disabled
Ghn17	Disabled	Ghn18	Disabled

3.7.3.3 MAC Authentication Information

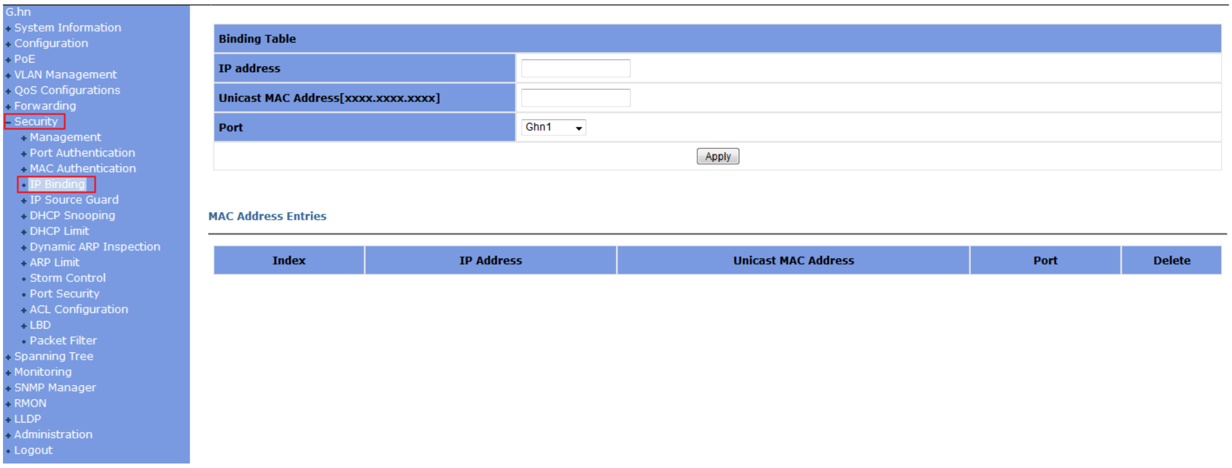
This page lists all the MAC authentication information including MAC Address, From Port, and Authenticate state.



VID	MAC Address	From Port	Authenticate State
No entries in table			

3.7.4 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[xxxx.xxxx.xxxx]	
Port	Ghn1

MAC Address Entries

Index	IP Address	Unicast MAC Address	Port	Delete

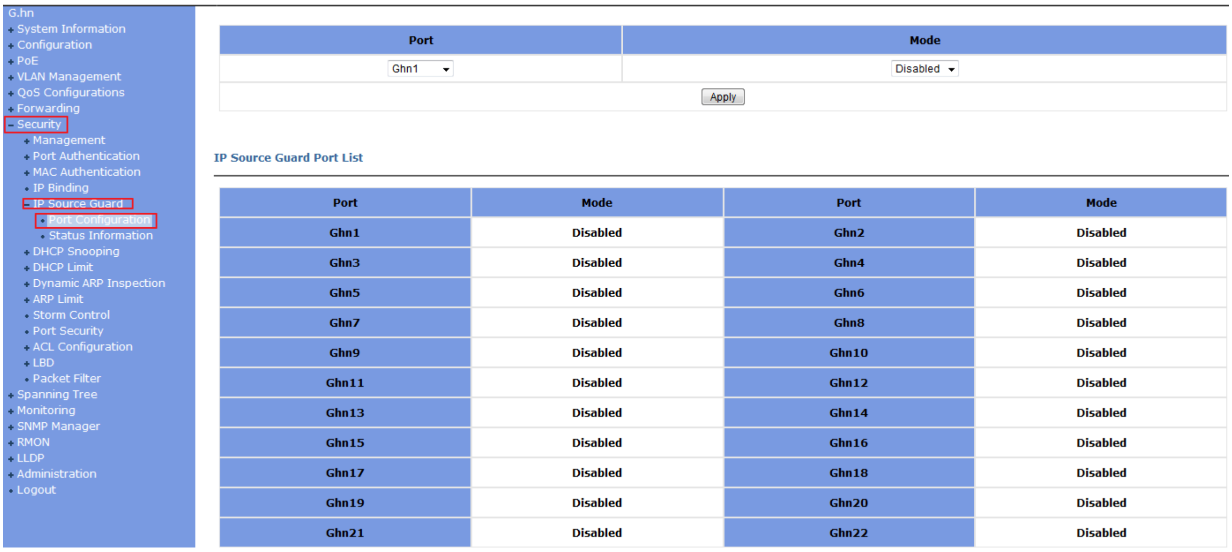
3.7.5 IP Source Guard

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.

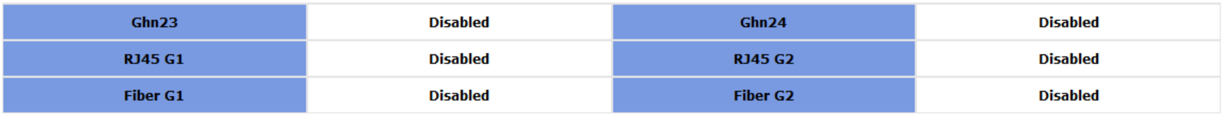
3.7.5.1 Port Configuration

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



Port	Mode
Ghn1	Disabled

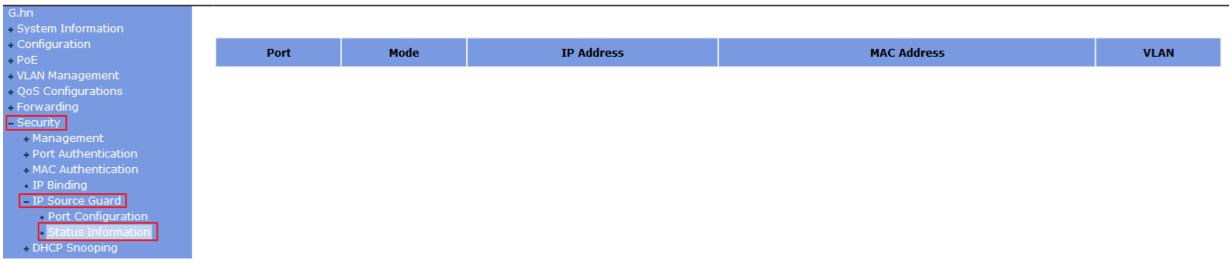
IP Source Guard Port List



Port	Mode	Port	Mode
Ghn1	Disabled	Ghn2	Disabled
Ghn3	Disabled	Ghn4	Disabled
Ghn5	Disabled	Ghn6	Disabled
Ghn7	Disabled	Ghn8	Disabled
Ghn9	Disabled	Ghn10	Disabled
Ghn11	Disabled	Ghn12	Disabled
Ghn13	Disabled	Ghn14	Disabled
Ghn15	Disabled	Ghn16	Disabled
Ghn17	Disabled	Ghn18	Disabled
Ghn19	Disabled	Ghn20	Disabled
Ghn21	Disabled	Ghn22	Disabled
Ghn23	Disabled	Ghn24	Disabled
RJ45 G1	Disabled	RJ45 G2	Disabled
Fiber G1	Disabled	Fiber G2	Disabled

3.7.5.2 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

3.7.6 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 using 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 IP addresses will be occupied by the DHCP clients permanently.

Dynamic assignment The DHCP server assigns IP addresses to DHCP clients for 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.

3.6.3.1 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.

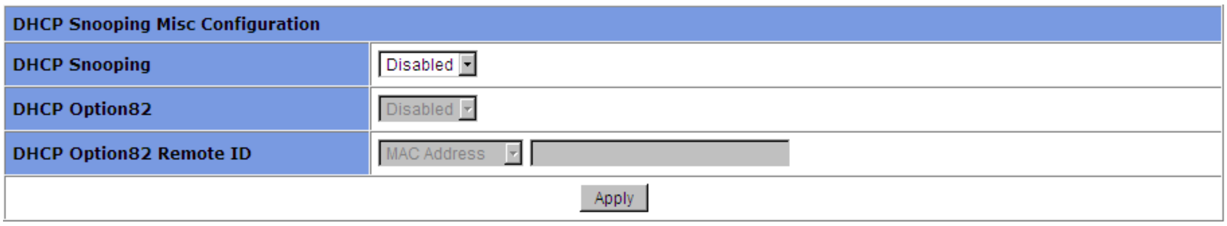
Option 82 involves at most 255 sub-options. If Option 82 is defined, at least one sub-option must be defined. Currently the DHCP relay agent supports only one sub-option: remote ID sub-option.

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 Switches (enabled with DHCP snooping) are padded as follows:

Remote ID sub-option is padded with the MAC address, system name, port remote ID 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

3.6.3.2 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 G4224 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.

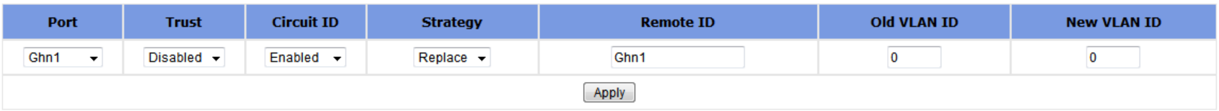
Circuit ID When Enabled the Circuit ID, it will replace the circuit to new circuit, new circuit Format: System Name ETH 0/0/port:vid ,such as *Gl8xmt ETH 0/0/2:100*

Strategy Set the Strategy as Keep/Drop/Replace

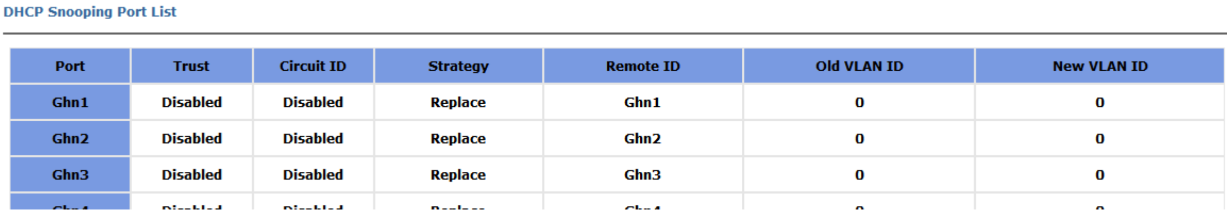
Remote ID Set port remote ID

Old VLAN ID VLAN ID in the range of 1 to 4094.This command will replace the inner VID of double tag to new VLAN

New VLAN ID VLAN ID in the range of 1 to 4094.



Port	Trust	Circuit ID	Strategy	Remote ID	Old VLAN ID	New VLAN ID
Ghn1	Disabled	Enabled	Replace	Ghn1	0	0

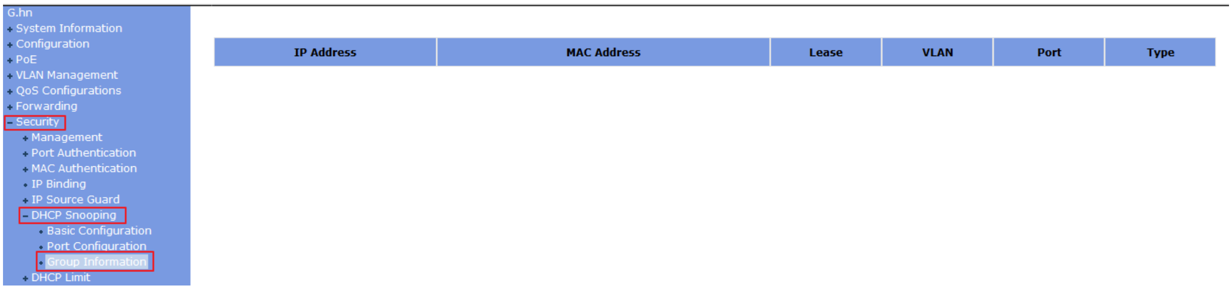


DHCP Snooping Port List

Port	Trust	Circuit ID	Strategy	Remote ID	Old VLAN ID	New VLAN ID
Ghn1	Disabled	Disabled	Replace	Ghn1	0	0
Ghn2	Disabled	Disabled	Replace	Ghn2	0	0
Ghn3	Disabled	Disabled	Replace	Ghn3	0	0
Ghn4	Disabled	Disabled	Replace	Ghn4	0	0

3.6.3.3 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 50-e5-49-e3-b6-92 of VLAN 1, connected with the Ethernet 1/1 port, successfully got an IP address 192.168.104.236 from a DHCP server, and the lease time is 259200 seconds.



IP Address	MAC Address	Lease	VLAN	Port	Type

3.7.7 DHCP Limit

To prevent attacks from unauthorized DHCP servers, DHCP packets will be processed by the switch CPU for validity checking. 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.

G4224 supports 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**.

3.7.4.1 Port Configuration

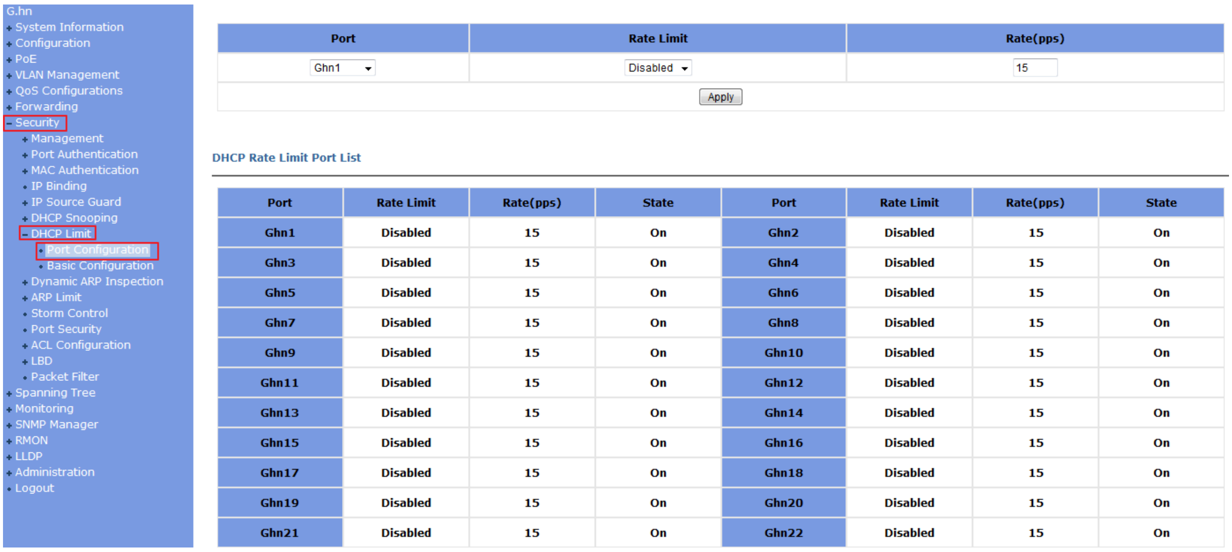
This page sets the DHCP Rate Limit for a specified Ethernet Port.

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”.

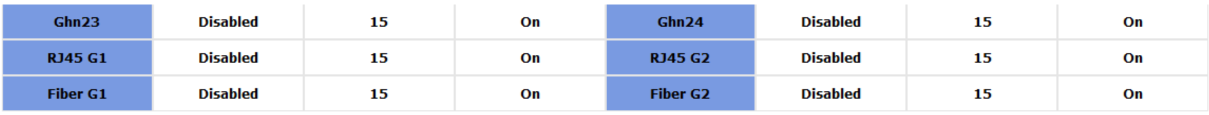
The lower part of this page lists all the DHCP Rate Limit ports.



Port	Rate Limit	Rate(pps)
Ghn1	Disabled	15

DHCP Rate Limit Port List

Port	Rate Limit	Rate(pps)	State	Port	Rate Limit	Rate(pps)	State
Ghn1	Disabled	15	On	Ghn2	Disabled	15	On
Ghn3	Disabled	15	On	Ghn4	Disabled	15	On
Ghn5	Disabled	15	On	Ghn6	Disabled	15	On
Ghn7	Disabled	15	On	Ghn8	Disabled	15	On
Ghn9	Disabled	15	On	Ghn10	Disabled	15	On
Ghn11	Disabled	15	On	Ghn12	Disabled	15	On
Ghn13	Disabled	15	On	Ghn14	Disabled	15	On
Ghn15	Disabled	15	On	Ghn16	Disabled	15	On
Ghn17	Disabled	15	On	Ghn18	Disabled	15	On
Ghn19	Disabled	15	On	Ghn20	Disabled	15	On
Ghn21	Disabled	15	On	Ghn22	Disabled	15	On
Ghn23	Disabled	15	On	Ghn24	Disabled	15	On
RJ45 G1	Disabled	15	On	RJ45 G2	Disabled	15	On
Fiber G1	Disabled	15	On	Fiber G2	Disabled	15	On

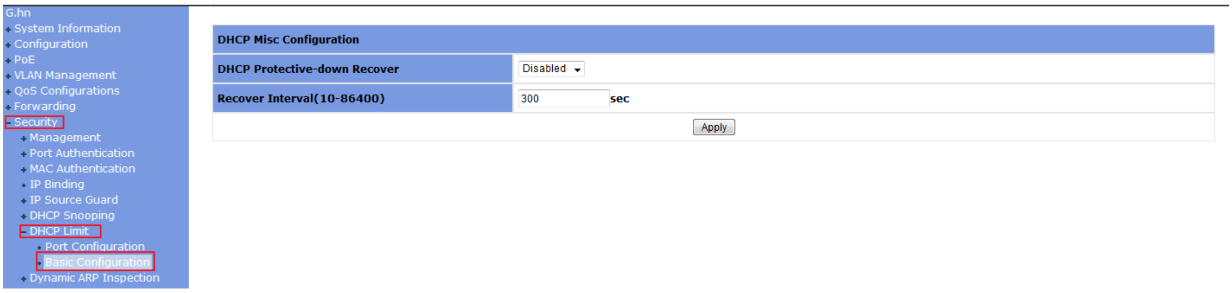


3.7.4.2 Basic Configuration

This page set 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 interval, the port will recover automatically to be enabled. 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

3.7.8 Dynamic ARP Inspection

To guard against the man-in-the-middle attacks launched by hackers or attackers, G4224 supports 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.

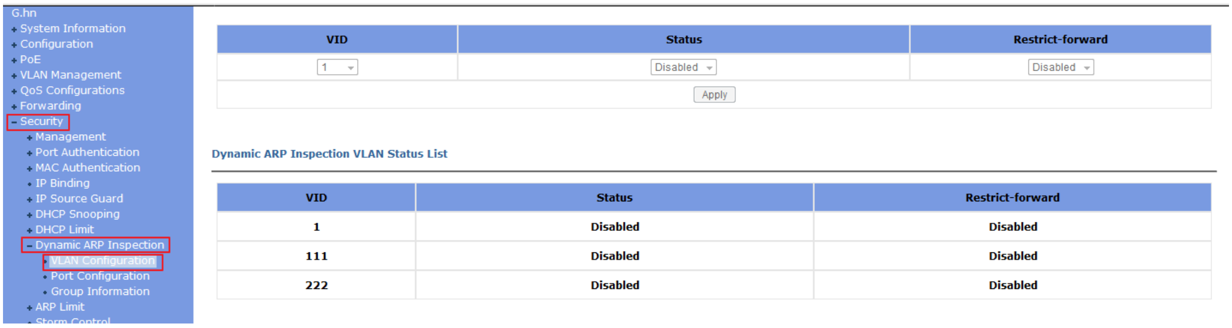
3.7.8.1 VLAN Configuration

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.



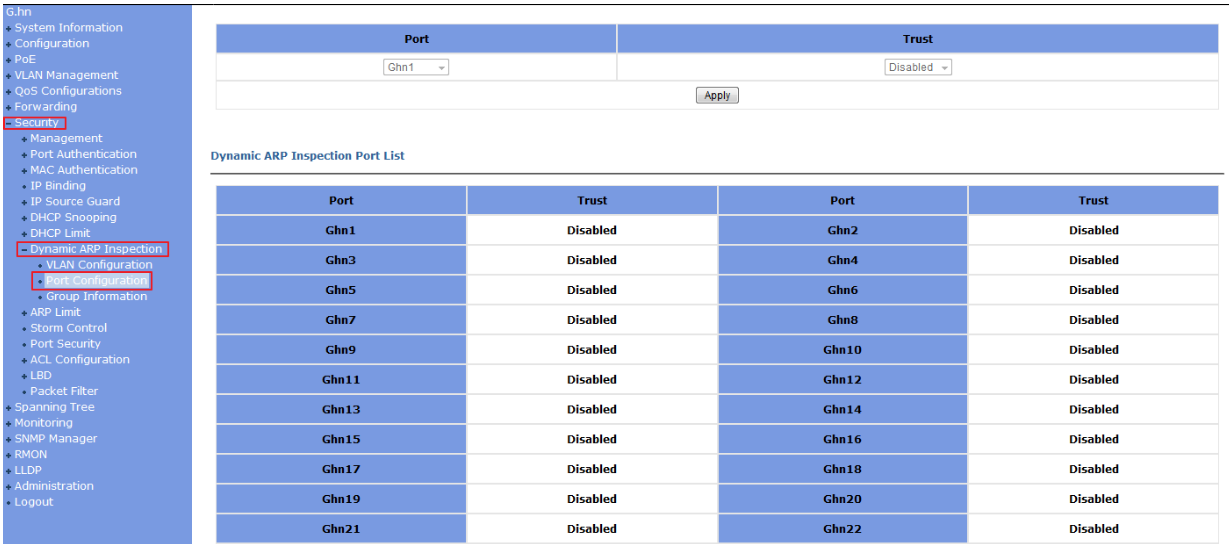
VID	Status	Restrict-forward
1	Disabled	Disabled

Dynamic ARP Inspection VLAN Status List

VID	Status	Restrict-forward
1	Disabled	Disabled
111	Disabled	Disabled
222	Disabled	Disabled

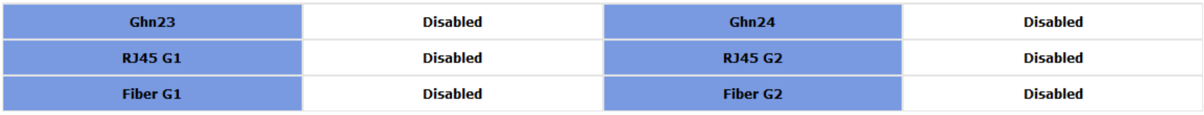
3.7.8.2 Port Configuration

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
Ghn1	Disabled

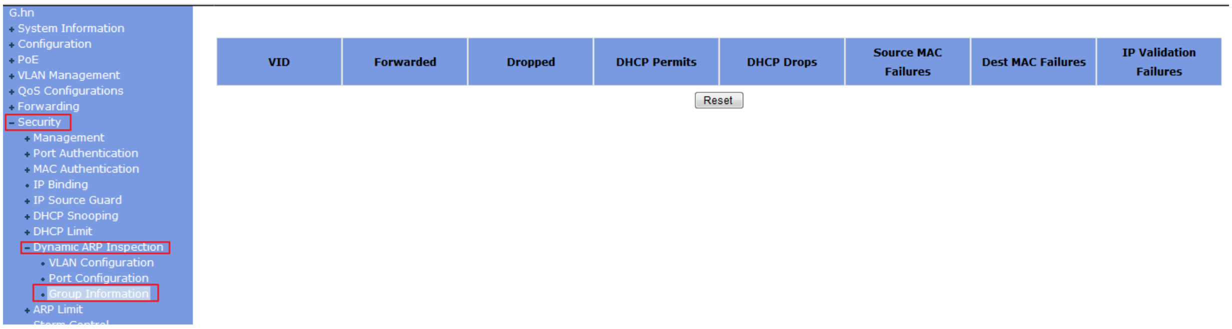
Dynamic ARP Inspection Port List



Port	Trust	Port	Trust
Ghn1	Disabled	Ghn2	Disabled
Ghn3	Disabled	Ghn4	Disabled
Ghn5	Disabled	Ghn6	Disabled
Ghn7	Disabled	Ghn8	Disabled
Ghn9	Disabled	Ghn10	Disabled
Ghn11	Disabled	Ghn12	Disabled
Ghn13	Disabled	Ghn14	Disabled
Ghn15	Disabled	Ghn16	Disabled
Ghn17	Disabled	Ghn18	Disabled
Ghn19	Disabled	Ghn20	Disabled
Ghn21	Disabled	Ghn22	Disabled
Ghn23	Disabled	Ghn24	Disabled
RJ45 G1	Disabled	RJ45 G2	Disabled
Fiber G1	Disabled	Fiber G2	Disabled

3.7.8.3 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

3.7.9 ARP Limit

To prevent ARP attacks from unauthorized DHCP servers, ARP packets will be processed by the switch CPU for validity checking. 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.

G4224 supports ARP packet rate limit on a port and shut down the port under attack to prevent hazardous impact on the device CPU.

After ARP packet rate limit is enabled on an Ethernet port, the switch counts the number of ARP packets received on this port per second. If the number of ARP 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.

3.7.9.1 Port Configuration

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

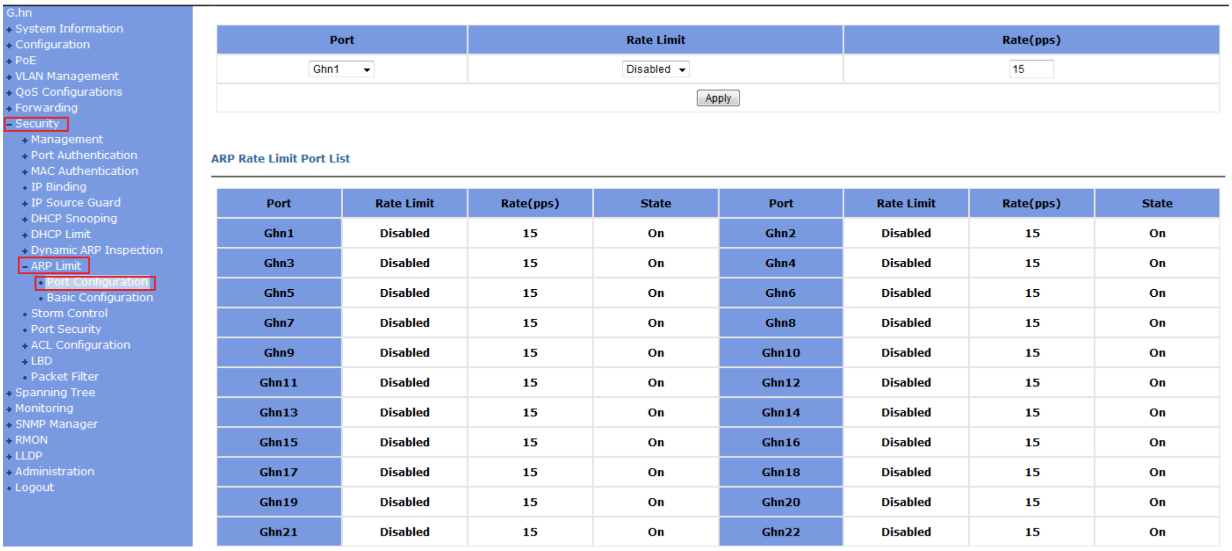
Port Specify a port to configure DHCP rate limit

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”.

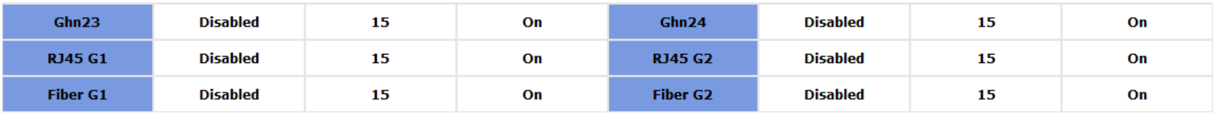
The lower part of this page lists the ARP Rate Limit of all the ports.



Port	Rate Limit	Rate(pps)
Ghn1	Disabled	15

ARP Rate Limit Port List

Port	Rate Limit	Rate(pps)	State	Port	Rate Limit	Rate(pps)	State
Ghn1	Disabled	15	On	Ghn2	Disabled	15	On
Ghn3	Disabled	15	On	Ghn4	Disabled	15	On
Ghn5	Disabled	15	On	Ghn6	Disabled	15	On
Ghn7	Disabled	15	On	Ghn8	Disabled	15	On
Ghn9	Disabled	15	On	Ghn10	Disabled	15	On
Ghn11	Disabled	15	On	Ghn12	Disabled	15	On
Ghn13	Disabled	15	On	Ghn14	Disabled	15	On
Ghn15	Disabled	15	On	Ghn16	Disabled	15	On
Ghn17	Disabled	15	On	Ghn18	Disabled	15	On
Ghn19	Disabled	15	On	Ghn20	Disabled	15	On
Ghn21	Disabled	15	On	Ghn22	Disabled	15	On



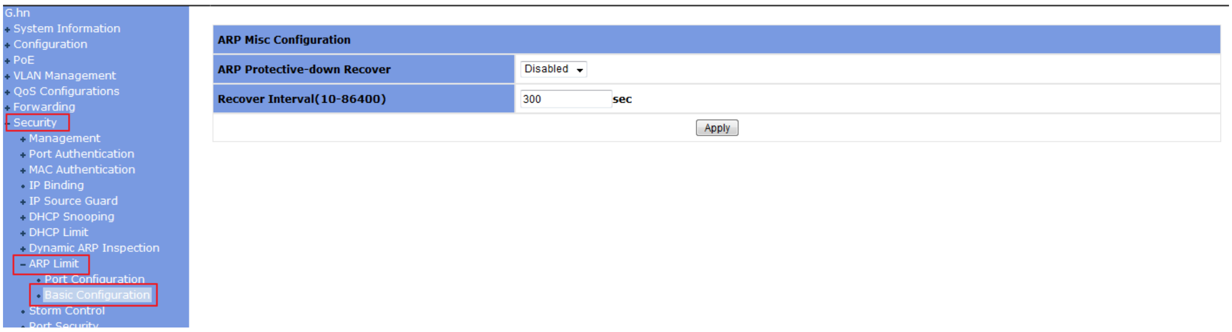
Ghn23	Disabled	15	On	Ghn24	Disabled	15	On
RJ45 G1	Disabled	15	On	RJ45 G2	Disabled	15	On
Fiber G1	Disabled	15	On	Fiber G2	Disabled	15	On

3.7.9.2 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.



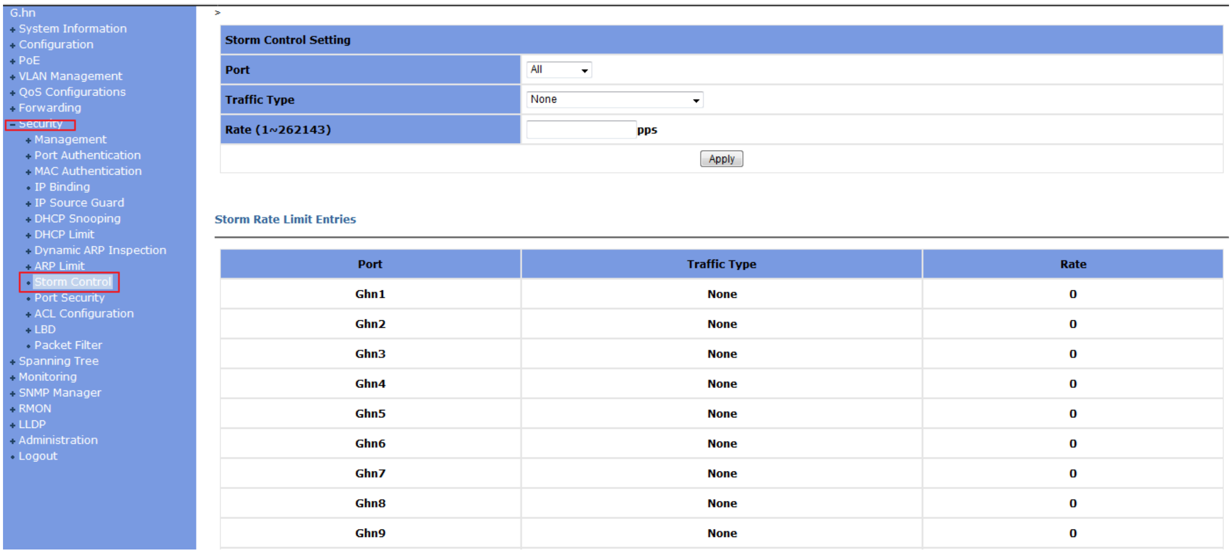
ARP Misc Configuration	
ARP Protective-down Recover	Disabled
Recover Interval(10-86400)	300 sec

3.7.10 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 be automatically 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
Ghn1	None	0
Ghn2	None	0
Ghn3	None	0
Ghn4	None	0
Ghn5	None	0
Ghn6	None	0
Ghn7	None	0
Ghn8	None	0
Ghn9	None	0

3.7.11 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

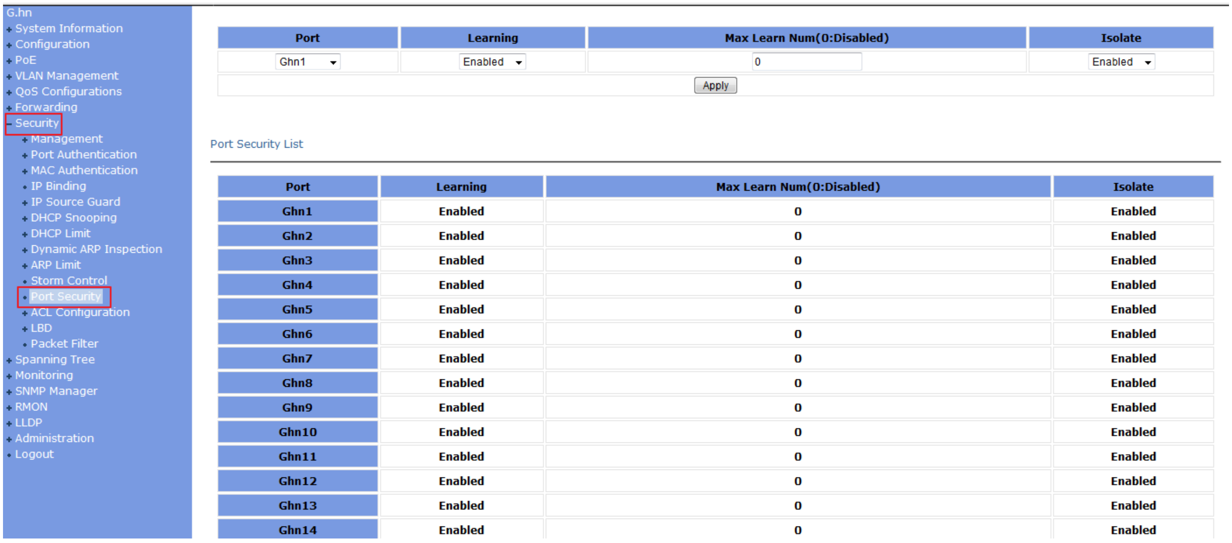
This configuration is different from that of the maximum number of MAC addresses that can be learned by a port in MAC address management.

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.

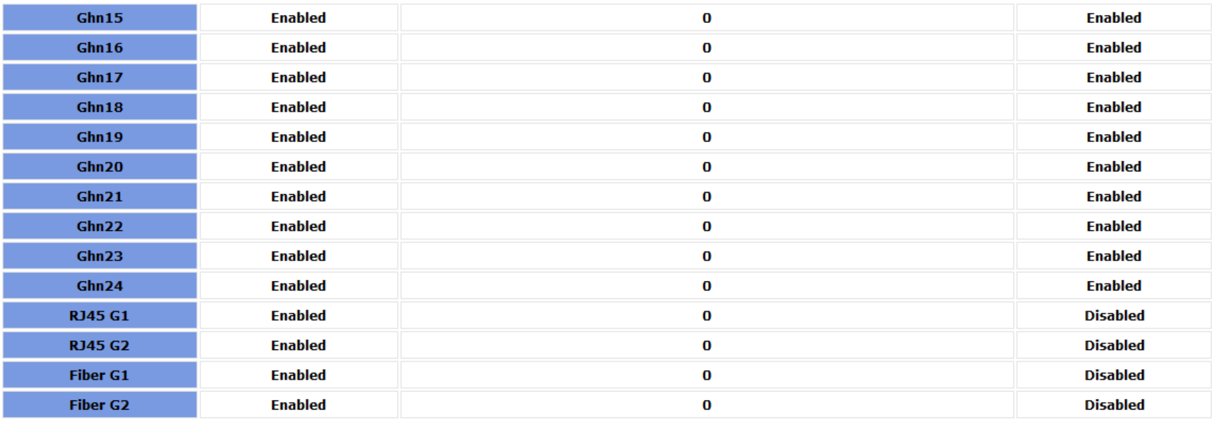
Isolate Enable/disable port isolation.

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	Learning	Max Learn Num(0:Disabled)	Isolate
Ghn1	Enabled	0	Enabled

Port Security List

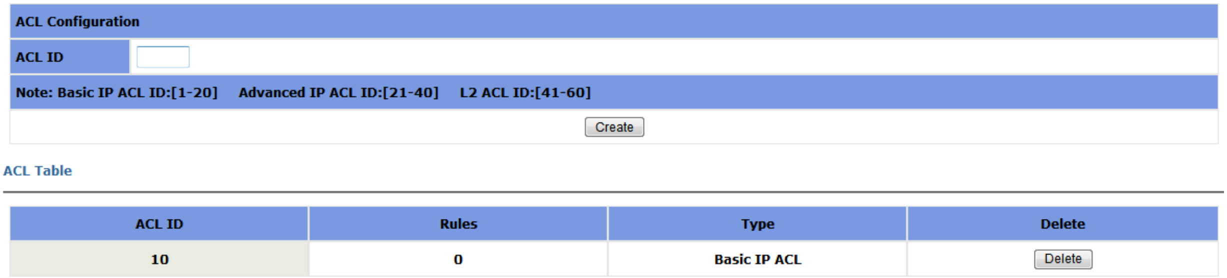


Port	Learning	Max Learn Num(0:Disabled)	Isolate
Ghn1	Enabled	0	Enabled
Ghn2	Enabled	0	Enabled
Ghn3	Enabled	0	Enabled
Ghn4	Enabled	0	Enabled
Ghn5	Enabled	0	Enabled
Ghn6	Enabled	0	Enabled
Ghn7	Enabled	0	Enabled
Ghn8	Enabled	0	Enabled
Ghn9	Enabled	0	Enabled
Ghn10	Enabled	0	Enabled
Ghn11	Enabled	0	Enabled
Ghn12	Enabled	0	Enabled
Ghn13	Enabled	0	Enabled
Ghn14	Enabled	0	Enabled
Ghn15	Enabled	0	Enabled
Ghn16	Enabled	0	Enabled
Ghn17	Enabled	0	Enabled
Ghn18	Enabled	0	Enabled
Ghn19	Enabled	0	Enabled
Ghn20	Enabled	0	Enabled
Ghn21	Enabled	0	Enabled
Ghn22	Enabled	0	Enabled
Ghn23	Enabled	0	Enabled
Ghn24	Enabled	0	Enabled
RJ45 G1	Enabled	0	Disabled
RJ45 G2	Enabled	0	Disabled
Fiber G1	Enabled	0	Disabled
Fiber G2	Enabled	0	Disabled

3.7.12 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.

3.7.12.1 ACL ID



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

ACL Table

ACL ID	Rules	Type	Delete
10	0	Basic IP 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.

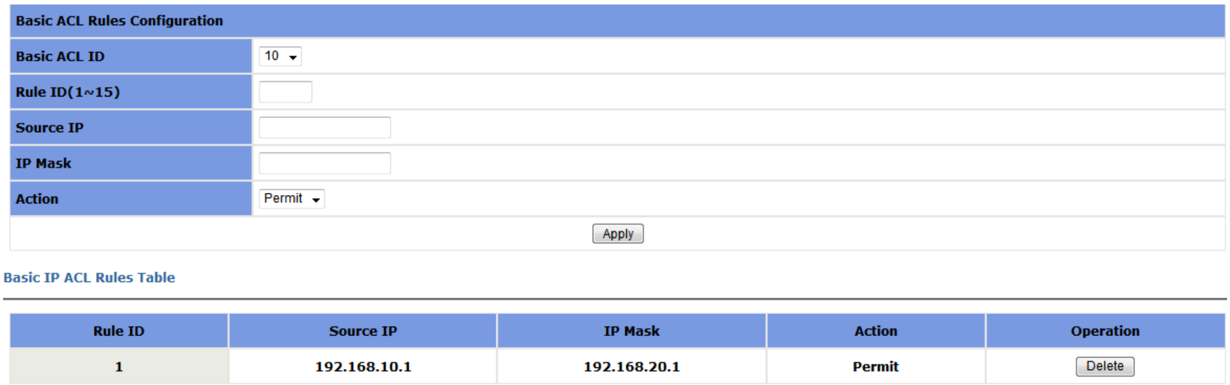
L2 ACL: The filtering packets based on source MAC address, destination MAC addresses, 802.1p priority, and L2 protocol type.

3.7.12.2 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**.**



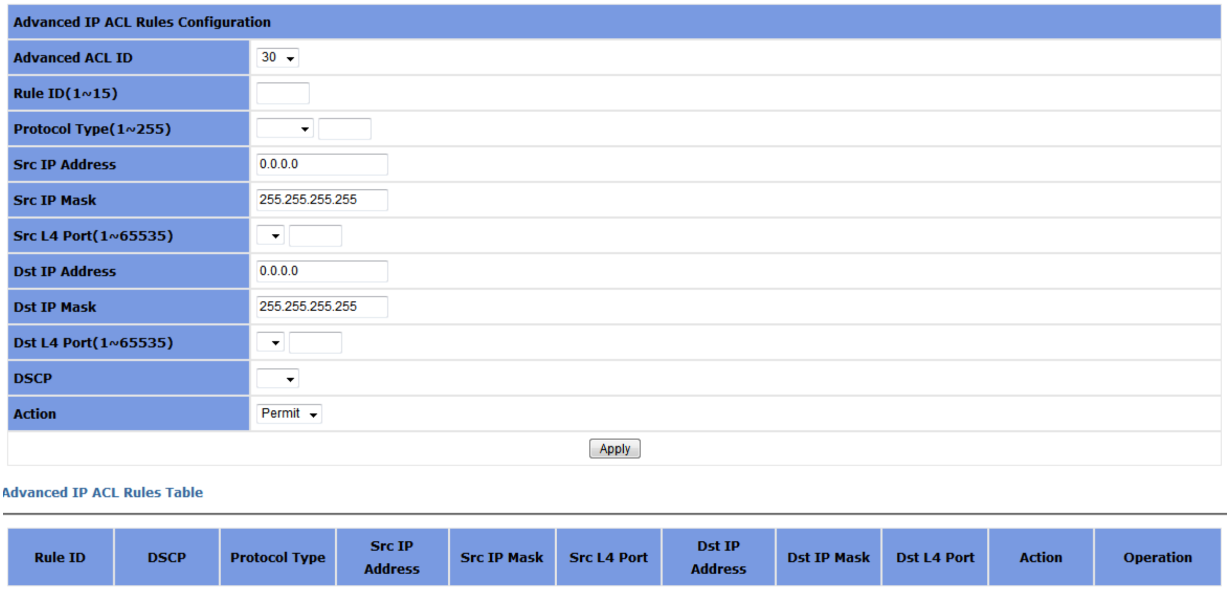
Basic ACL Rules Configuration	
Basic ACL ID	10
Rule ID(1~15)	
Source IP	
IP Mask	
Action	Permit
Apply	

Basic IP ACL Rules Table

Rule ID	Source IP	IP Mask	Action	Operation
1	192.168.10.1	192.168.20.1	Permit	Delete

3.7.12.3 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(1~15)	
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

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 from 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**.**

3.7.12.4 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.**

Rule ID: Identification of the ACL rule.

Src MAC Address: Source host mac address.

Src MAC Address Mask: Source host mac address mask.

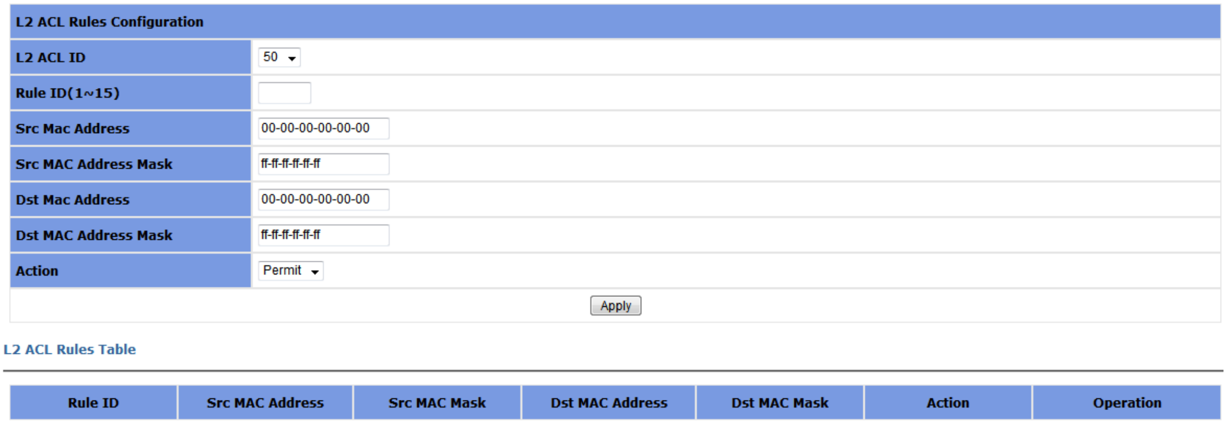
Dst MAC Address: Destination host mac address.

Dst MAC address Mask: Destination host mac address mask.

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

3.7.12.5 Traffic ACL

The page configures 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.



L2 ACL Rules Configuration

L2 ACL ID	50
Rule ID(1~15)	
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

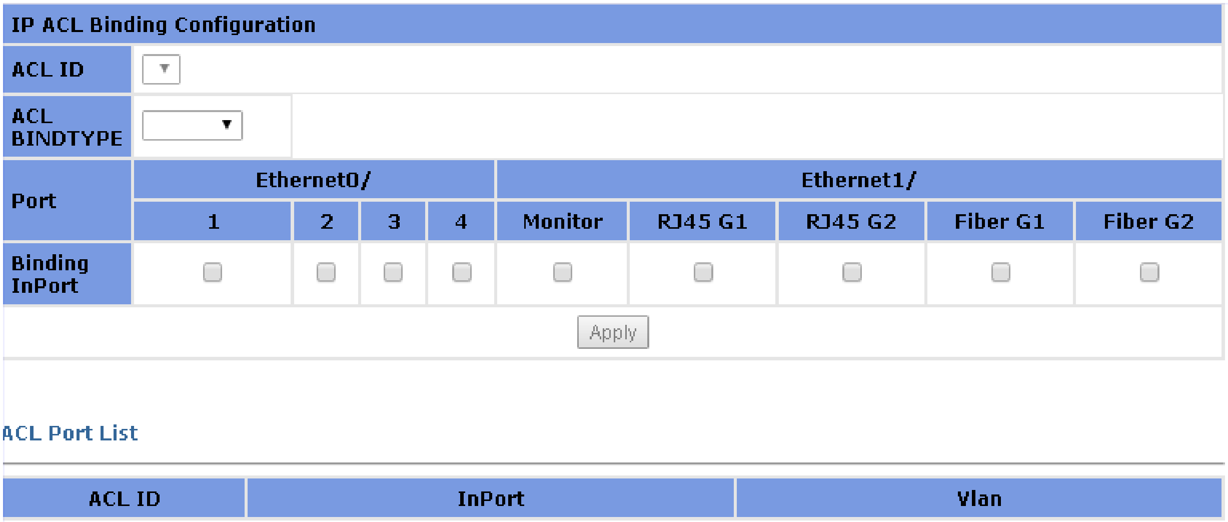
L2 ACL Rules Table

Rule ID	Src MAC Address	Src MAC Mask	Dst MAC Address	Dst MAC Mask	Action	Operation

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.

3.7.12.6 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	☐	☐	☐	☐	☐	☐	☐	☐	☐

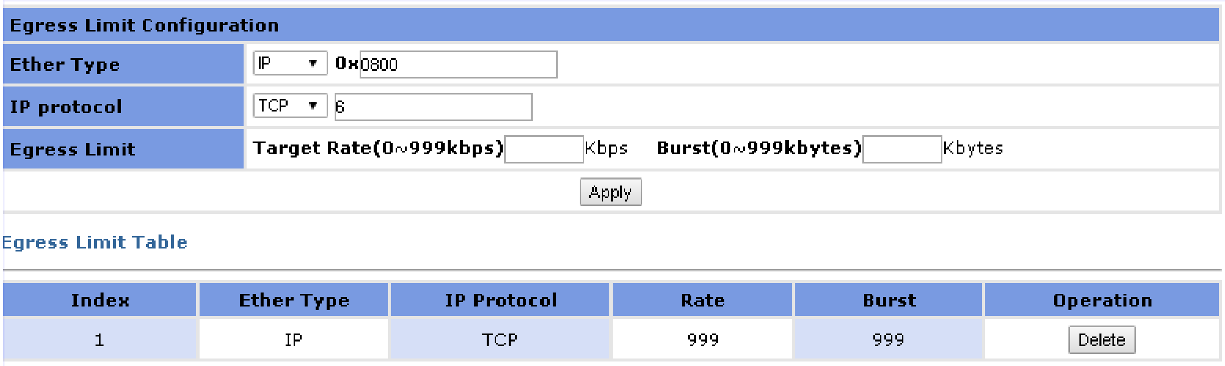
Apply

ACL Port List

ACL ID	InPort	Vlan

3.7.12.7 Egress Limit

This page sets the egress limit configuration



Egress Limit Configuration	
Ether Type	IP ▾ 0x 0800
IP protocol	TCP ▾ 6
Egress Limit	Target Rate(0~999kbps) Kbps Burst(0~999kbytes) Kbytes

Apply

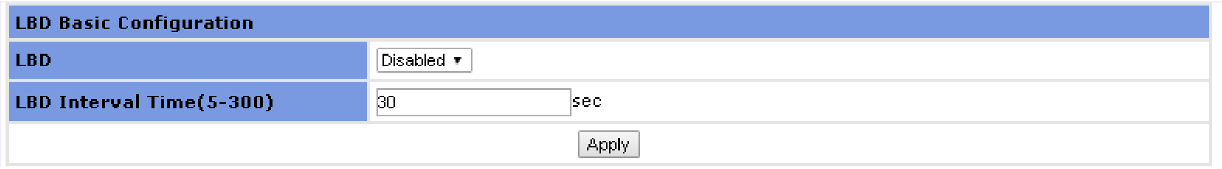
Egress Limit Table

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

3.7.13 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.

3.7.13.1 Basic Configuration



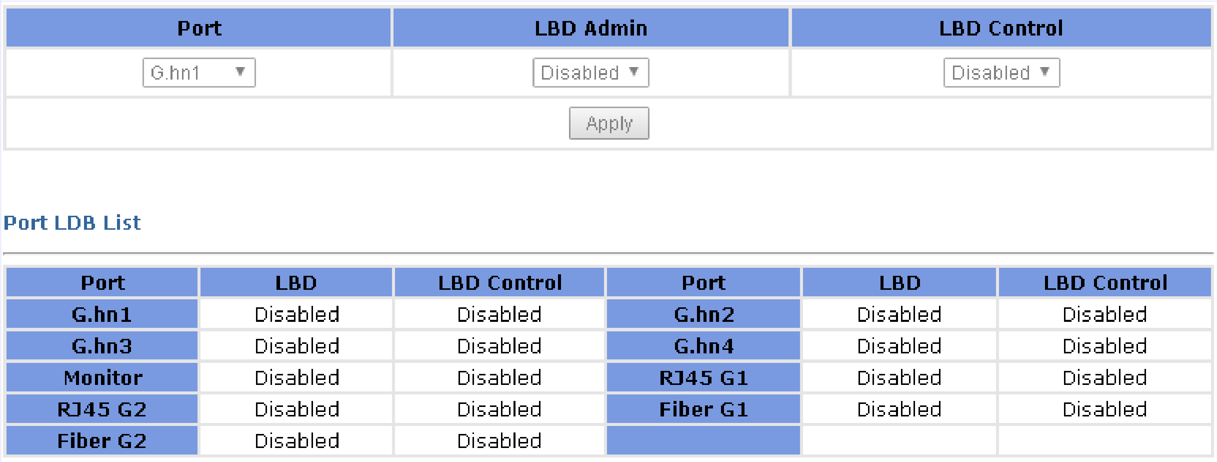
LBD Basic Configuration	
LBD	Disabled ▾
LBD Interval Time(5-300)	30 sec

Apply

LBD: enable or disabled

LBD Interval Times: configure interval time for loopback detection

3.7.13.2 Port Configuration



Port	LBD Admin	LBD Control
G.hn1 ▼	Disabled ▼	Disabled ▼

Port LDB List

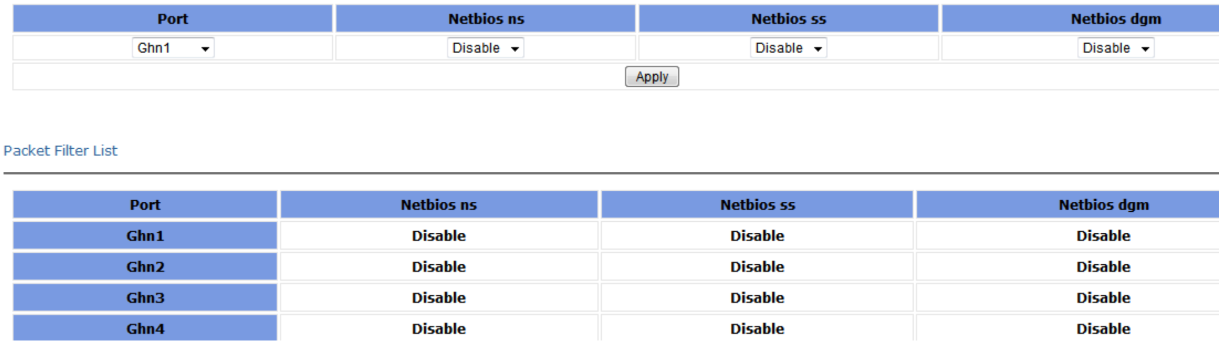
Port	LBD	LBD Control	Port	LBD	LBD Control
G.hn1	Disabled	Disabled	G.hn2	Disabled	Disabled
G.hn3	Disabled	Disabled	G.hn4	Disabled	Disabled
Monitor	Disabled	Disabled	RJ45 G1	Disabled	Disabled
RJ45 G2	Disabled	Disabled	Fiber G1	Disabled	Disabled
Fiber G2	Disabled	Disabled			

LBD Admin: enable or disable Loopback detection on this port

LBD Control: configure port loopback detection control.

3.7.14 Packet Filter

You can set filter Netbios protocol here.



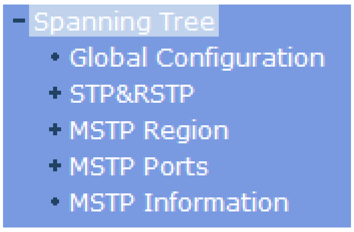
Port	Netbios ns	Netbios ss	Netbios dgm
Ghn1 ▾	Disable ▾	Disable ▾	Disable ▾

Packet Filter List

Port	Netbios ns	Netbios ss	Netbios dgm
Ghn1	Disable	Disable	Disable
Ghn2	Disable	Disable	Disable
Ghn3	Disable	Disable	Disable
Ghn4	Disable	Disable	Disable

3.8 Spanning Tree

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



3.8.1 Global Configuration

Before configuring STP, make sure STP is enabled (see section 3.3 of this manual for details). There is one tab page: **Configuration.**

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

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

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

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

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

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

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

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

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

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

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

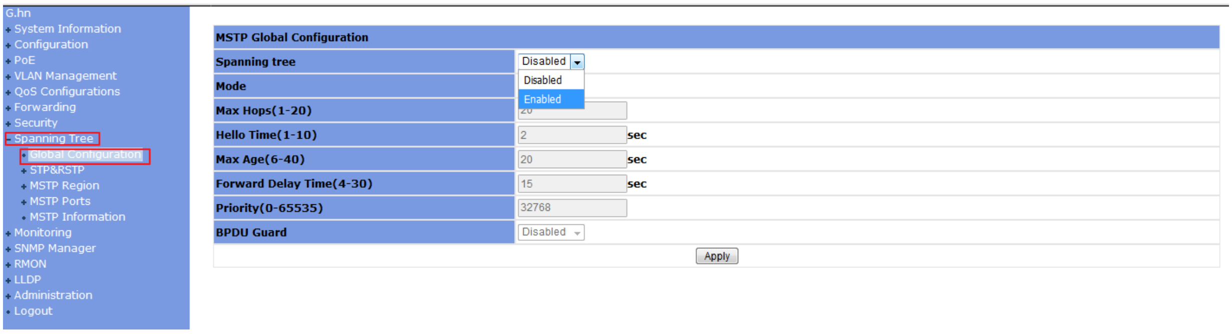
2 × (**Forward Delay Time** – 1 second) >= **Max Age**, and **Max Age** >= 2 × (**Hello Time** + 1 second).

Priority: This value is in the range of 0 to 65535, and is 32768 by default. This parameter is used in STP and RSTP modes only.

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

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

By default, the BPDU protection function is disabled.



MSTP Global Configuration	
Spanning tree	Disabled
Mode	
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

3.8.2 STP&RSTP

3.7.2.1 Ports Configuration

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

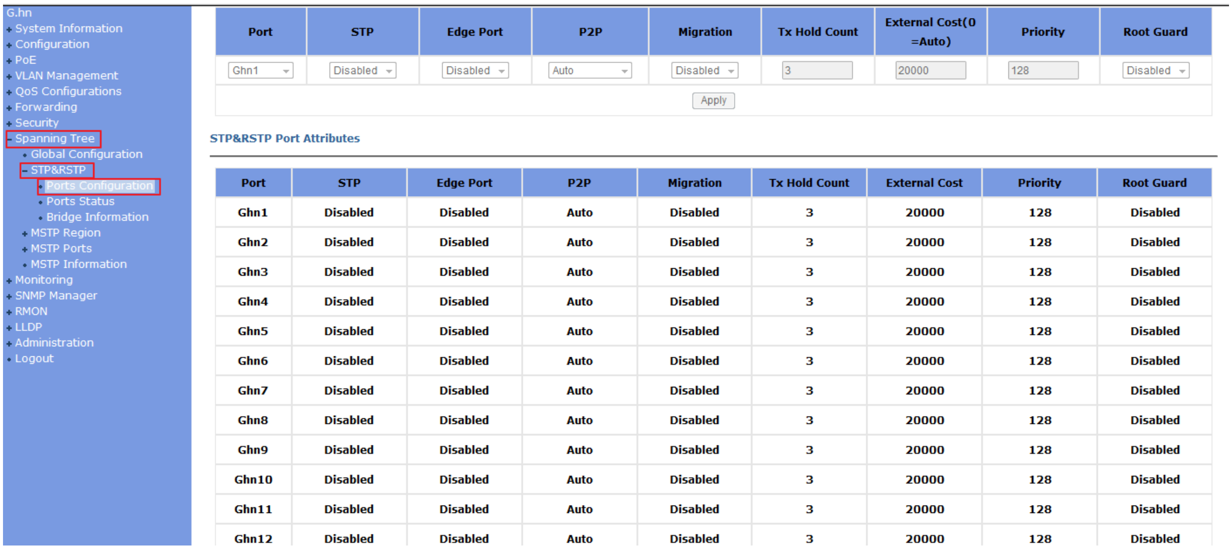
External Cost: sets the path cost of the specified port. It is in the range of 1 to 200000000, the default value is 0 (Auto).

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).



Port	STP	Edge Port	P2P	Migration	Tx Hold Count	External Cost(0 =Auto)	Priority	Root Guard
Ghn1	Disabled	Disabled	Auto	Disabled	3	20000	128	Disabled

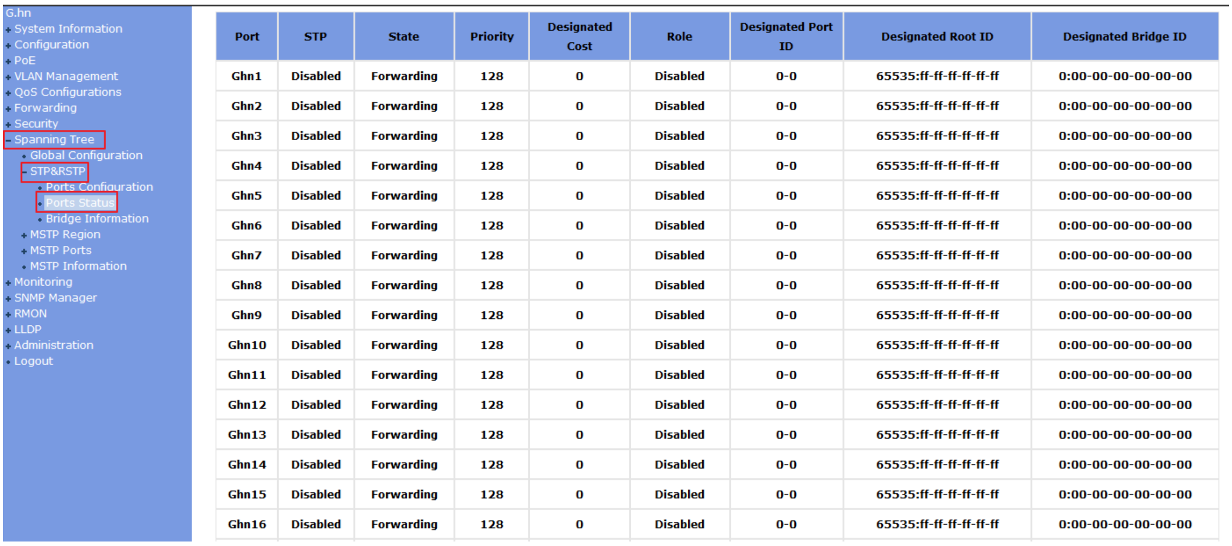
STP&RSTP Port Attributes

Port	STP	Edge Port	P2P	Migration	Tx Hold Count	External Cost	Priority	Root Guard
Ghn1	Disabled	Disabled	Auto	Disabled	3	20000	128	Disabled
Ghn2	Disabled	Disabled	Auto	Disabled	3	20000	128	Disabled
Ghn3	Disabled	Disabled	Auto	Disabled	3	20000	128	Disabled
Ghn4	Disabled	Disabled	Auto	Disabled	3	20000	128	Disabled
Ghn5	Disabled	Disabled	Auto	Disabled	3	20000	128	Disabled
Ghn6	Disabled	Disabled	Auto	Disabled	3	20000	128	Disabled
Ghn7	Disabled	Disabled	Auto	Disabled	3	20000	128	Disabled
Ghn8	Disabled	Disabled	Auto	Disabled	3	20000	128	Disabled
Ghn9	Disabled	Disabled	Auto	Disabled	3	20000	128	Disabled
Ghn10	Disabled	Disabled	Auto	Disabled	3	20000	128	Disabled
Ghn11	Disabled	Disabled	Auto	Disabled	3	20000	128	Disabled
Ghn12	Disabled	Disabled	Auto	Disabled	3	20000	128	Disabled

Ghn13	Disabled	Disabled	Auto	Disabled	3	20000	128	Disabled
Ghn14	Disabled	Disabled	Auto	Disabled	3	20000	128	Disabled
Ghn15	Disabled	Disabled	Auto	Disabled	3	20000	128	Disabled
Ghn16	Disabled	Disabled	Auto	Disabled	3	20000	128	Disabled
Ghn17	Disabled	Disabled	Auto	Disabled	3	20000	128	Disabled
Ghn18	Disabled	Disabled	Auto	Disabled	3	20000	128	Disabled
Ghn19	Disabled	Disabled	Auto	Disabled	3	20000	128	Disabled
Ghn20	Disabled	Disabled	Auto	Disabled	3	20000	128	Disabled
Ghn21	Disabled	Disabled	Auto	Disabled	3	20000	128	Disabled
Ghn22	Disabled	Disabled	Auto	Disabled	3	20000	128	Disabled
Ghn23	Disabled	Disabled	Auto	Disabled	3	20000	128	Disabled
Ghn24	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

3.8.2.2 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
Ghn1	Disabled	Forwarding	128	0	Disabled	0-0	65535:ff-ff-ff-ff-ff-ff	0:00-00-00-00-00-00
Ghn2	Disabled	Forwarding	128	0	Disabled	0-0	65535:ff-ff-ff-ff-ff-ff	0:00-00-00-00-00-00
Ghn3	Disabled	Forwarding	128	0	Disabled	0-0	65535:ff-ff-ff-ff-ff-ff	0:00-00-00-00-00-00
Ghn4	Disabled	Forwarding	128	0	Disabled	0-0	65535:ff-ff-ff-ff-ff-ff	0:00-00-00-00-00-00
Ghn5	Disabled	Forwarding	128	0	Disabled	0-0	65535:ff-ff-ff-ff-ff-ff	0:00-00-00-00-00-00
Ghn6	Disabled	Forwarding	128	0	Disabled	0-0	65535:ff-ff-ff-ff-ff-ff	0:00-00-00-00-00-00
Ghn7	Disabled	Forwarding	128	0	Disabled	0-0	65535:ff-ff-ff-ff-ff-ff	0:00-00-00-00-00-00
Ghn8	Disabled	Forwarding	128	0	Disabled	0-0	65535:ff-ff-ff-ff-ff-ff	0:00-00-00-00-00-00
Ghn9	Disabled	Forwarding	128	0	Disabled	0-0	65535:ff-ff-ff-ff-ff-ff	0:00-00-00-00-00-00
Ghn10	Disabled	Forwarding	128	0	Disabled	0-0	65535:ff-ff-ff-ff-ff-ff	0:00-00-00-00-00-00
Ghn11	Disabled	Forwarding	128	0	Disabled	0-0	65535:ff-ff-ff-ff-ff-ff	0:00-00-00-00-00-00
Ghn12	Disabled	Forwarding	128	0	Disabled	0-0	65535:ff-ff-ff-ff-ff-ff	0:00-00-00-00-00-00
Ghn13	Disabled	Forwarding	128	0	Disabled	0-0	65535:ff-ff-ff-ff-ff-ff	0:00-00-00-00-00-00
Ghn14	Disabled	Forwarding	128	0	Disabled	0-0	65535:ff-ff-ff-ff-ff-ff	0:00-00-00-00-00-00
Ghn15	Disabled	Forwarding	128	0	Disabled	0-0	65535:ff-ff-ff-ff-ff-ff	0:00-00-00-00-00-00
Ghn16	Disabled	Forwarding	128	0	Disabled	0-0	65535:ff-ff-ff-ff-ff-ff	0:00-00-00-00-00-00
Ghn17	Disabled	Forwarding	128	0	Disabled	0-0	65535:ff-ff-ff-ff-ff-ff	0:00-00-00-00-00-00
Ghn18	Disabled	Forwarding	128	0	Disabled	0-0	65535:ff-ff-ff-ff-ff-ff	0:00-00-00-00-00-00
Ghn19	Disabled	Forwarding	128	0	Disabled	0-0	65535:ff-ff-ff-ff-ff-ff	0:00-00-00-00-00-00
Ghn20	Disabled	Forwarding	128	0	Disabled	0-0	65535:ff-ff-ff-ff-ff-ff	0:00-00-00-00-00-00
Ghn21	Disabled	Forwarding	128	0	Disabled	0-0	65535:ff-ff-ff-ff-ff-ff	0:00-00-00-00-00-00
Ghn22	Disabled	Forwarding	128	0	Disabled	0-0	65535:ff-ff-ff-ff-ff-ff	0:00-00-00-00-00-00
Ghn23	Disabled	Forwarding	128	0	Disabled	0-0	65535:ff-ff-ff-ff-ff-ff	0:00-00-00-00-00-00
Ghn24	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

3.8.2.3 Bridge Information

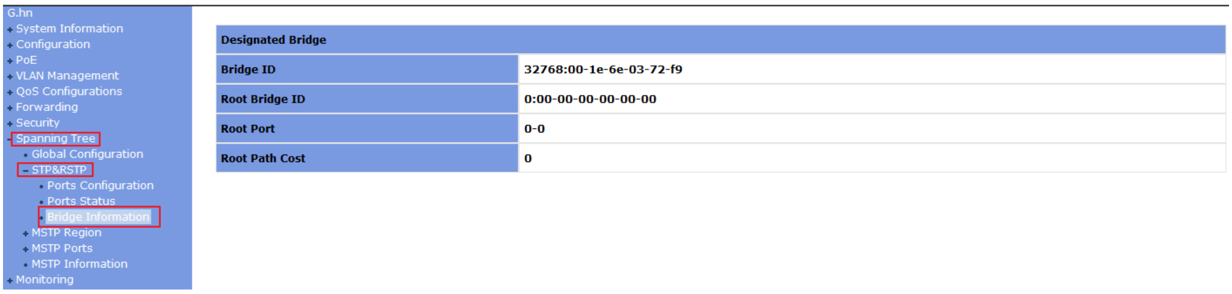
This page lists basic information of **Designated Bridge**, including Bridge ID, Root Bridge ID, Root Port, and Root Path Cost.

Bridge ID: ID of this switch.

Root Bridge ID: ID of the root bridge.

Root Port: the spanning tree root port.

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



Designated Bridge	
Bridge ID	32768:00-1e-6e-03-72-f9
Root Bridge ID	0:00-00-00-00-00-00
Root Port	0-0
Root Path Cost	0

3.8.3 MSTP Region

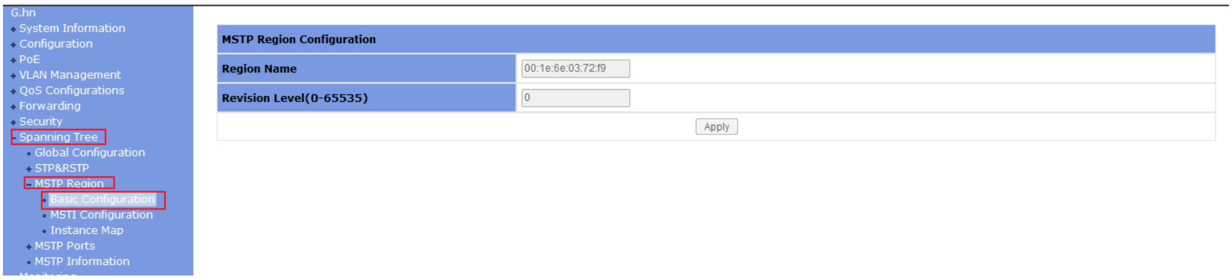
An MSTP region comprises one or more MST Bridges with the same MSTP configuration identifier.

3.8.3.1 Basic Configuration

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

Region Name: a variable length text string of up to 32 octets

Revision level: a 2-octet unsigned integer. It ranges from 0 to 65535.



MSTP Region Configuration	
Region Name	00:1e:6e:03:72:f9
Revision Level(0-65535)	0

3.8.3.2 MSTI Configuration

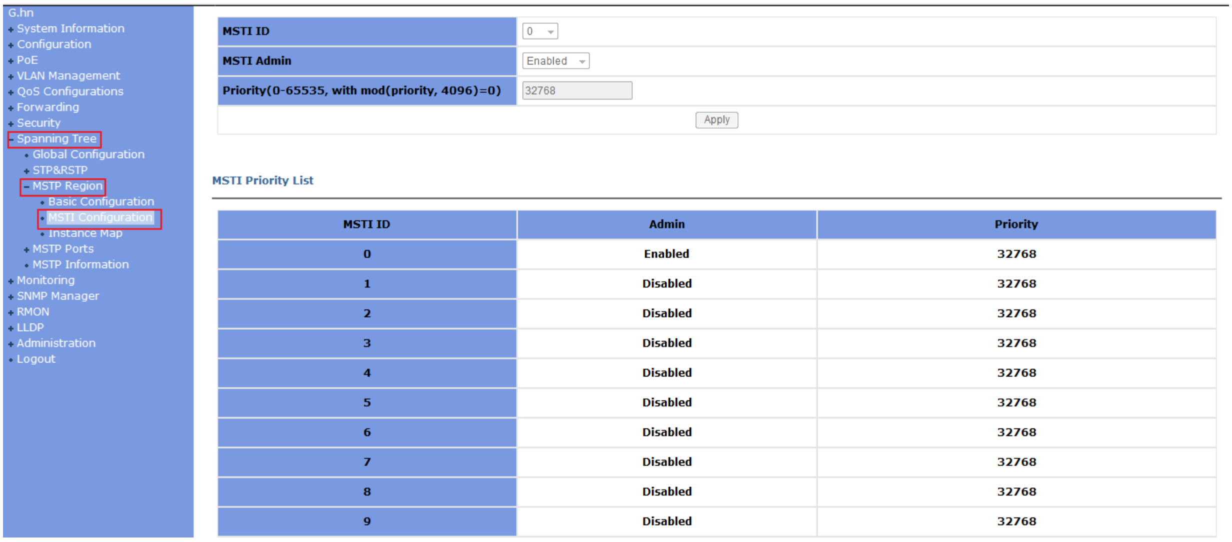
This page sets MSTI ID, MSTI Admin, and Priority for each MST instance.

MSTI ID: MSTI identification, ranging from 0 to 15

MSTI Admin: enable/disable the specified instance

Priority: sets a priority for the specified instance. It is in the range from 0 to 65535; the default value is 32768

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



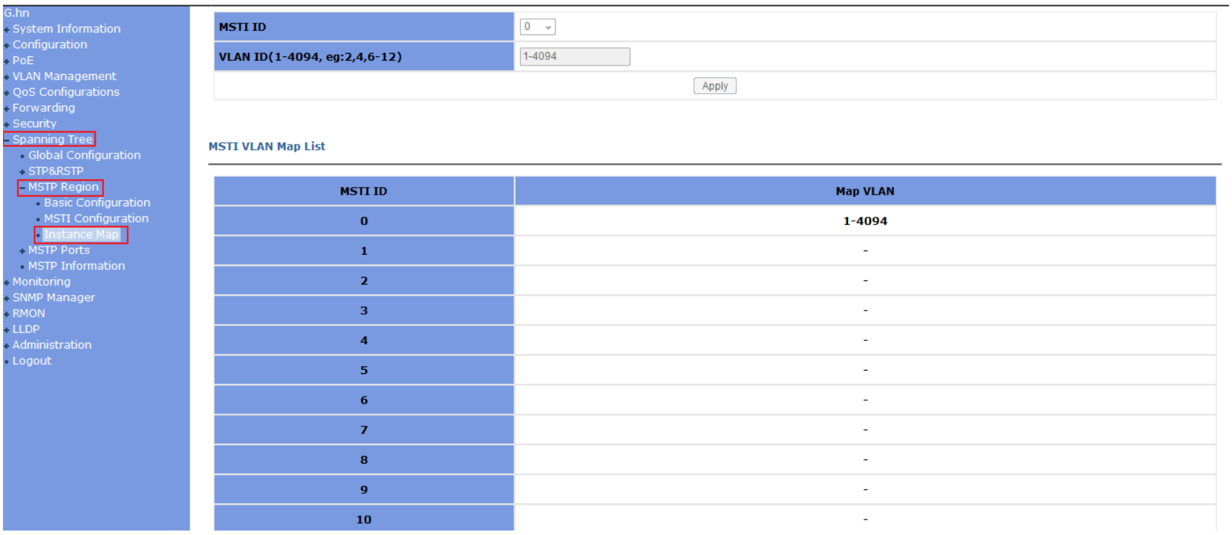
MSTI ID	0
MSTI Admin	Enabled
Priority(0-65535, with mod(priority, 4096)=0)	32768

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

3.8.3.3 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

MSTI VLAN Map List

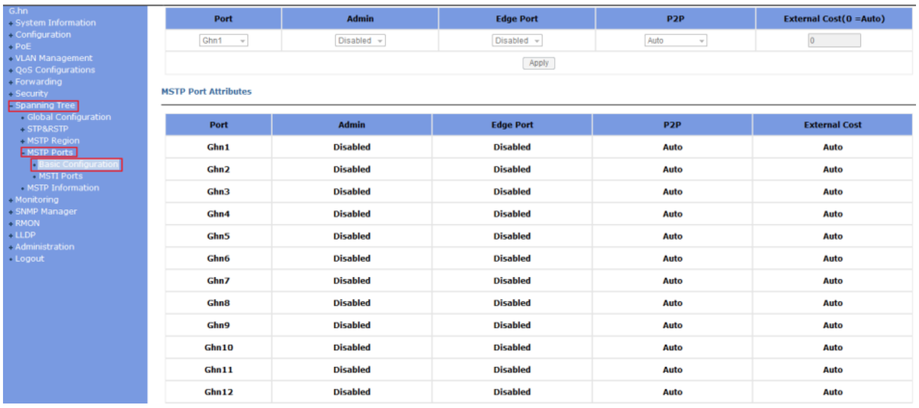
MSTI ID	Map VLAN
0	1-4094
1	-
2	-
3	-
4	-
5	-
6	-
7	-
8	-
9	-
10	-

3.8.4 MSTP Ports

3.8.4.1 Basic Configuration

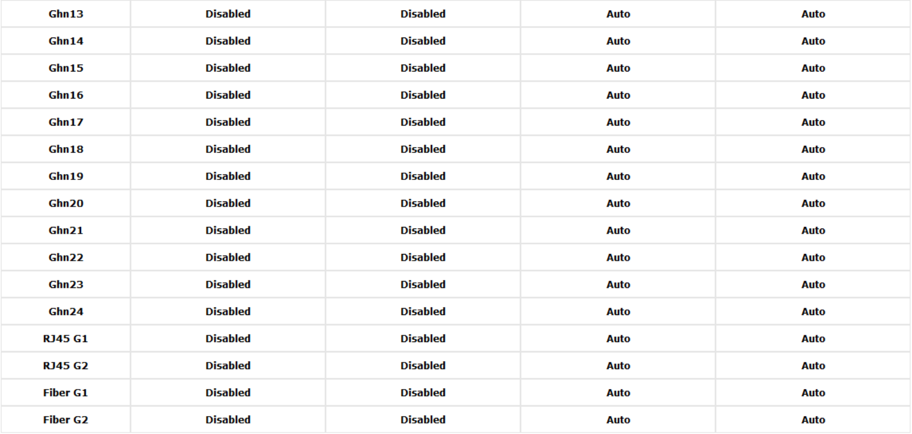
This page can set **Port**, **Admin**, **Edge Port, P2P,** and **External Cost** for each port. Similar to

STP and RSTP port configuration described in section 3.4.2 Ports Configuration, this page sets MSTP port configuration. The bottom part of this page lists the MSTP attributes for each port.



Port	Admin	Edge Port	P2P	External Cost(0 =Auto)
Ghn1	Disabled	Disabled	Auto	0

MSTP Port Attributes



Port	Admin	Edge Port	P2P	External Cost
Ghn1	Disabled	Disabled	Auto	Auto
Ghn2	Disabled	Disabled	Auto	Auto
Ghn3	Disabled	Disabled	Auto	Auto
Ghn4	Disabled	Disabled	Auto	Auto
Ghn5	Disabled	Disabled	Auto	Auto
Ghn6	Disabled	Disabled	Auto	Auto
Ghn7	Disabled	Disabled	Auto	Auto
Ghn8	Disabled	Disabled	Auto	Auto
Ghn9	Disabled	Disabled	Auto	Auto
Ghn10	Disabled	Disabled	Auto	Auto
Ghn11	Disabled	Disabled	Auto	Auto
Ghn12	Disabled	Disabled	Auto	Auto
Ghn13	Disabled	Disabled	Auto	Auto
Ghn14	Disabled	Disabled	Auto	Auto
Ghn15	Disabled	Disabled	Auto	Auto
Ghn16	Disabled	Disabled	Auto	Auto
Ghn17	Disabled	Disabled	Auto	Auto
Ghn18	Disabled	Disabled	Auto	Auto
Ghn19	Disabled	Disabled	Auto	Auto
Ghn20	Disabled	Disabled	Auto	Auto
Ghn21	Disabled	Disabled	Auto	Auto
Ghn22	Disabled	Disabled	Auto	Auto
Ghn23	Disabled	Disabled	Auto	Auto
Ghn24	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

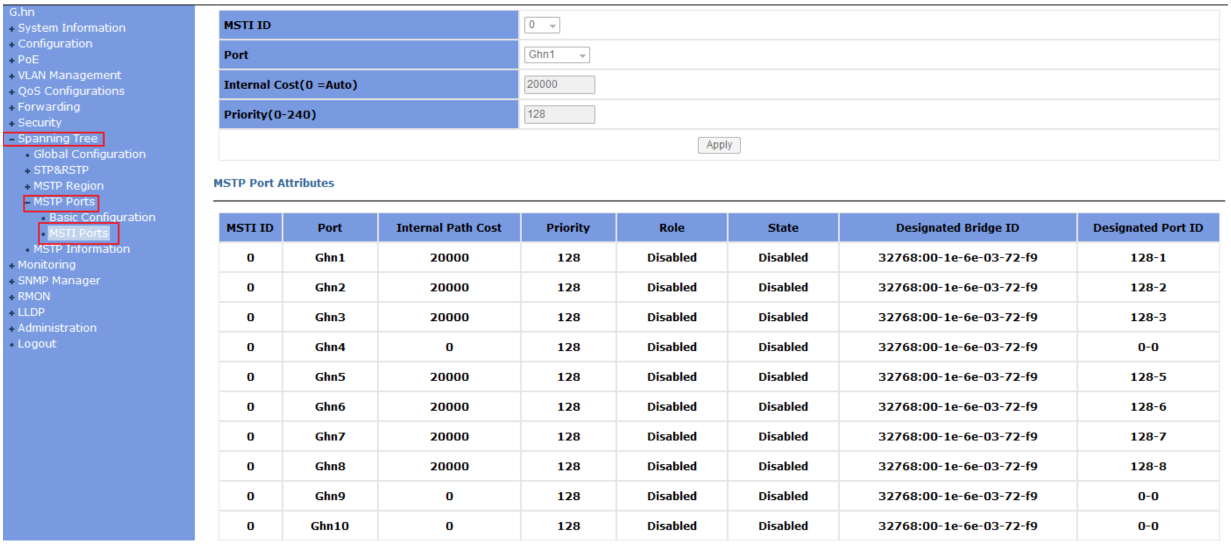
3.8.4.2 MSTI Ports

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

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

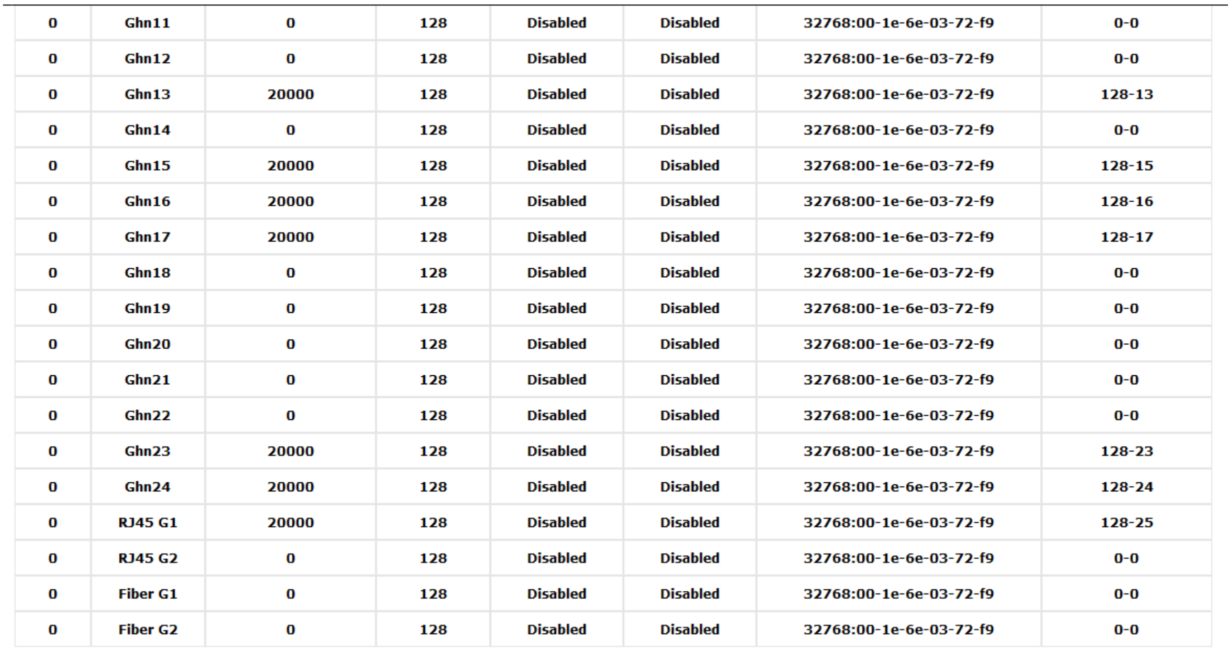
Priority: sets the port priority for the specified port in a specified MST instance. It is in the range from 0 to 240, and the default value is 128.

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



MSTI ID	0
Port	Ghn1
Internal Cost(0 =Auto)	20000
Priority(0-240)	128

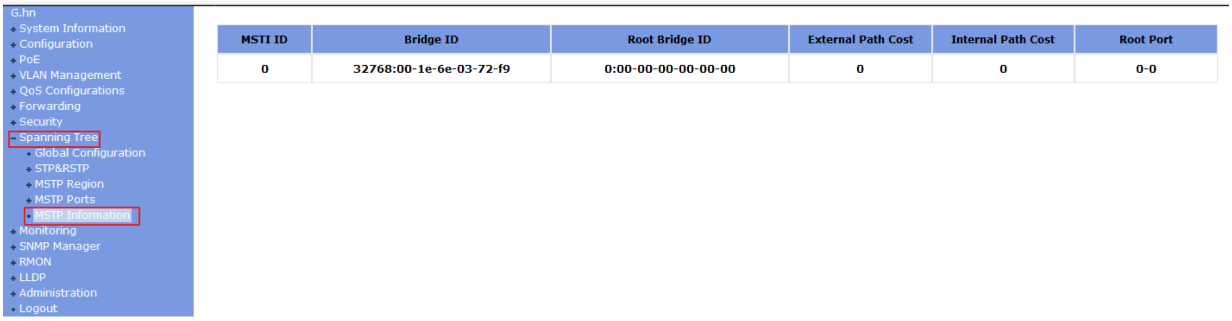
MSTP Port Attributes



MSTI ID	Port	Internal Path Cost	Priority	Role	State	Designated Bridge ID	Designated Port ID
0	Ghn1	20000	128	Disabled	Disabled	32768:00-1e-6e-03-72-f9	128-1
0	Ghn2	20000	128	Disabled	Disabled	32768:00-1e-6e-03-72-f9	128-2
0	Ghn3	20000	128	Disabled	Disabled	32768:00-1e-6e-03-72-f9	128-3
0	Ghn4	0	128	Disabled	Disabled	32768:00-1e-6e-03-72-f9	0-0
0	Ghn5	20000	128	Disabled	Disabled	32768:00-1e-6e-03-72-f9	128-5
0	Ghn6	20000	128	Disabled	Disabled	32768:00-1e-6e-03-72-f9	128-6
0	Ghn7	20000	128	Disabled	Disabled	32768:00-1e-6e-03-72-f9	128-7
0	Ghn8	20000	128	Disabled	Disabled	32768:00-1e-6e-03-72-f9	128-8
0	Ghn9	0	128	Disabled	Disabled	32768:00-1e-6e-03-72-f9	0-0
0	Ghn10	0	128	Disabled	Disabled	32768:00-1e-6e-03-72-f9	0-0
0	Ghn11	0	128	Disabled	Disabled	32768:00-1e-6e-03-72-f9	0-0
0	Ghn12	0	128	Disabled	Disabled	32768:00-1e-6e-03-72-f9	0-0
0	Ghn13	20000	128	Disabled	Disabled	32768:00-1e-6e-03-72-f9	128-13
0	Ghn14	0	128	Disabled	Disabled	32768:00-1e-6e-03-72-f9	0-0
0	Ghn15	20000	128	Disabled	Disabled	32768:00-1e-6e-03-72-f9	128-15
0	Ghn16	20000	128	Disabled	Disabled	32768:00-1e-6e-03-72-f9	128-16
0	Ghn17	20000	128	Disabled	Disabled	32768:00-1e-6e-03-72-f9	128-17
0	Ghn18	0	128	Disabled	Disabled	32768:00-1e-6e-03-72-f9	0-0
0	Ghn19	0	128	Disabled	Disabled	32768:00-1e-6e-03-72-f9	0-0
0	Ghn20	0	128	Disabled	Disabled	32768:00-1e-6e-03-72-f9	0-0
0	Ghn21	0	128	Disabled	Disabled	32768:00-1e-6e-03-72-f9	0-0
0	Ghn22	0	128	Disabled	Disabled	32768:00-1e-6e-03-72-f9	0-0
0	Ghn23	20000	128	Disabled	Disabled	32768:00-1e-6e-03-72-f9	128-23
0	Ghn24	20000	128	Disabled	Disabled	32768:00-1e-6e-03-72-f9	128-24
0	RJ45 G1	20000	128	Disabled	Disabled	32768:00-1e-6e-03-72-f9	128-25
0	RJ45 G2	0	128	Disabled	Disabled	32768:00-1e-6e-03-72-f9	0-0
0	Fiber G1	0	128	Disabled	Disabled	32768:00-1e-6e-03-72-f9	0-0
0	Fiber G2	0	128	Disabled	Disabled	32768:00-1e-6e-03-72-f9	0-0

3.8.5 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-03-72-f9	0:00-00-00-00-00-00	0	0	0-0

3.9 Monitoring

3.9.1 Port Statistics

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

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

TxBadPkts The total byte number of outgoing error frames

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

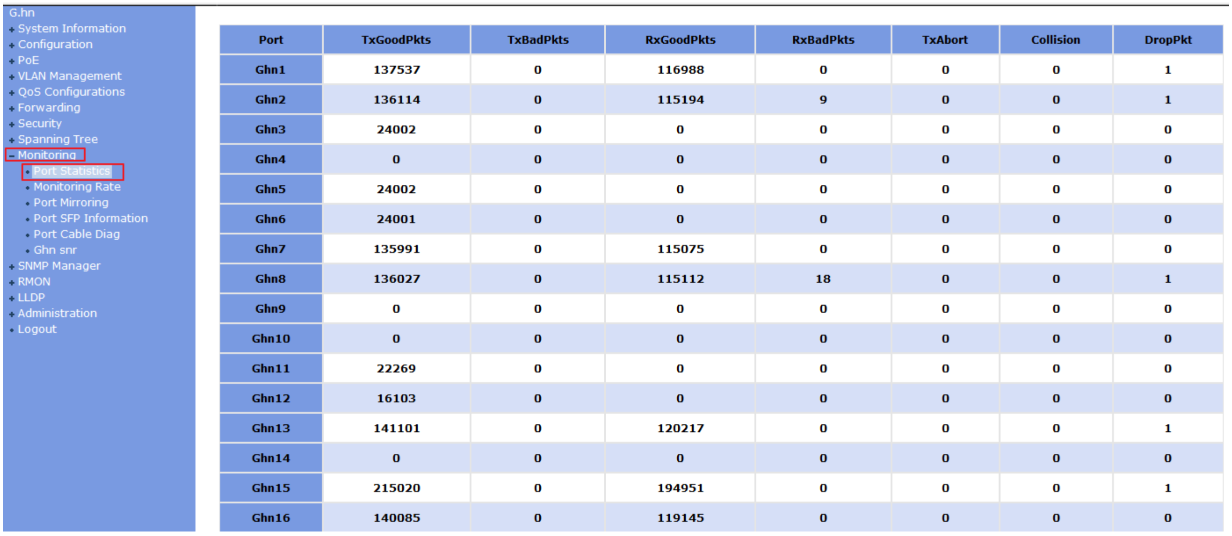
RxBadPkts The total number of incoming error frames

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

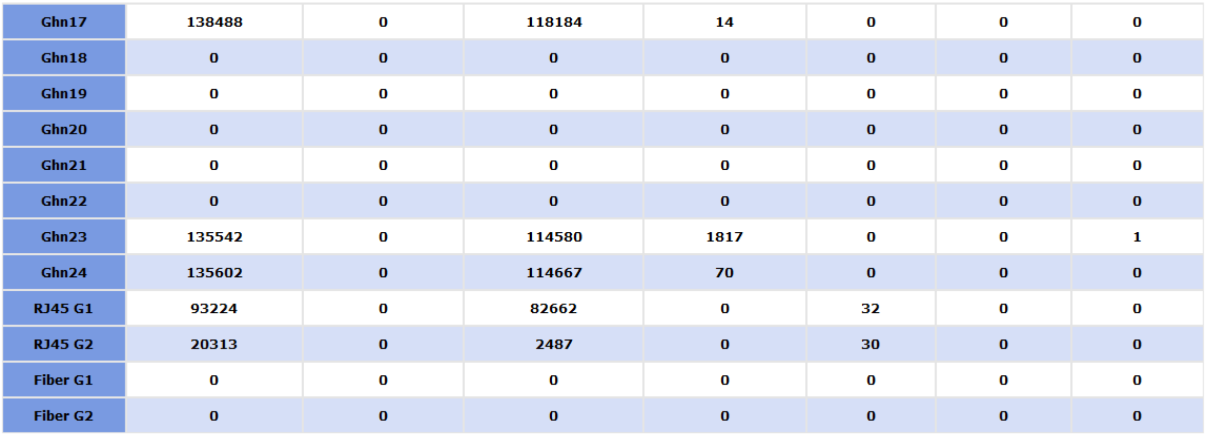
Collision The number of detected collisions

DropPkt The number of packets dropped for various reasons

Reset Clear the number of all ports



Port	TxGoodPkts	TxBadPkts	RxGoodPkts	RxBadPkts	TxAbort	Collision	DropPkt
Ghn1	137537	0	116988	0	0	0	1
Ghn2	136114	0	115194	9	0	0	1
Ghn3	24002	0	0	0	0	0	0
Ghn4	0	0	0	0	0	0	0
Ghn5	24002	0	0	0	0	0	0
Ghn6	24001	0	0	0	0	0	0
Ghn7	135991	0	115075	0	0	0	0
Ghn8	136027	0	115112	18	0	0	1
Ghn9	0	0	0	0	0	0	0
Ghn10	0	0	0	0	0	0	0
Ghn11	22269	0	0	0	0	0	0
Ghn12	16103	0	0	0	0	0	0
Ghn13	141101	0	120217	0	0	0	1
Ghn14	0	0	0	0	0	0	0
Ghn15	215020	0	194951	0	0	0	1
Ghn16	140085	0	119145	0	0	0	0



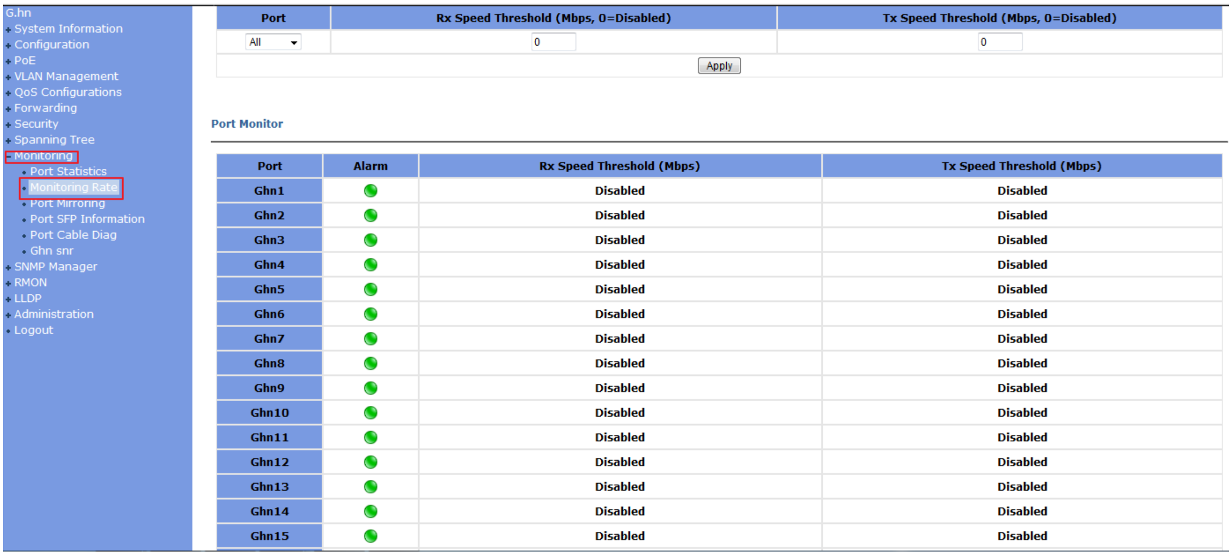
Ghn17	138488	0	118184	14	0	0	0
Ghn18	0	0	0	0	0	0	0
Ghn19	0	0	0	0	0	0	0
Ghn20	0	0	0	0	0	0	0
Ghn21	0	0	0	0	0	0	0
Ghn22	0	0	0	0	0	0	0
Ghn23	135542	0	114580	1817	0	0	1
Ghn24	135602	0	114667	70	0	0	0
RJ45 G1	93224	0	82662	0	32	0	0
RJ45 G2	20313	0	2487	0	30	0	0
Fiber G1	0	0	0	0	0	0	0
Fiber G2	0	0	0	0	0	0	0

3.9.2 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 the syslog server.

Note: You need to configure syslog configuration in advance.

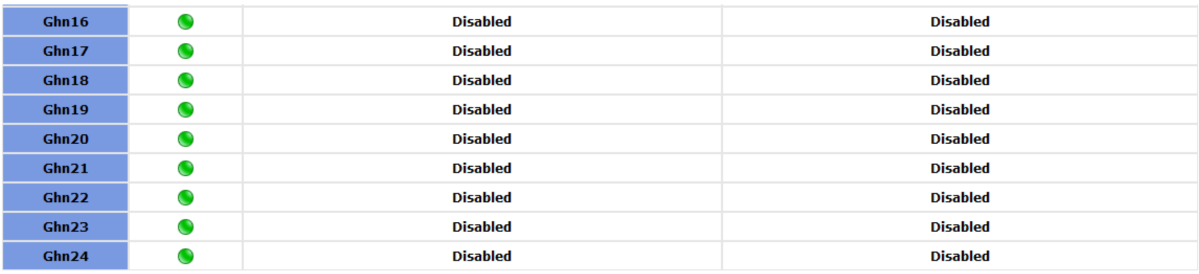
Port：Port number
Rx Speed Threshold：Rx Speed Threshold（0=Disable）
Tx Speed Threshold：Tx Speed Threshold（0=Disable）
Alarm：Red is on if alarm occurs; Green is on if there is no alarm.



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

Port Monitor

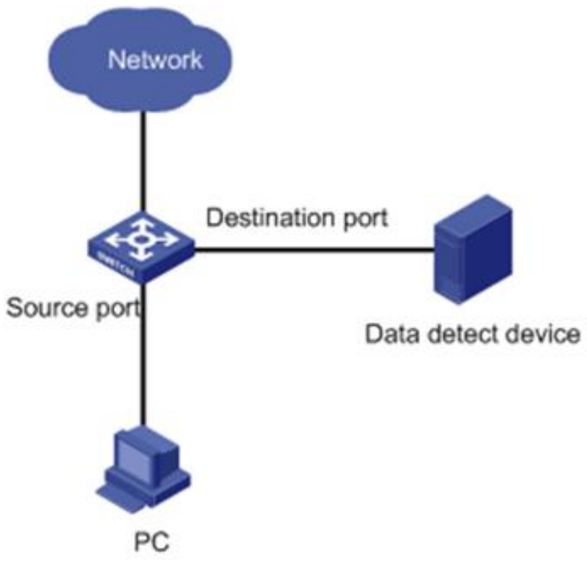
Port	Alarm	Rx Speed Threshold (Mbps)	Tx Speed Threshold (Mbps)
Ghn1	●	Disabled	Disabled
Ghn2	●	Disabled	Disabled
Ghn3	●	Disabled	Disabled
Ghn4	●	Disabled	Disabled
Ghn5	●	Disabled	Disabled
Ghn6	●	Disabled	Disabled
Ghn7	●	Disabled	Disabled
Ghn8	●	Disabled	Disabled
Ghn9	●	Disabled	Disabled
Ghn10	●	Disabled	Disabled
Ghn11	●	Disabled	Disabled
Ghn12	●	Disabled	Disabled
Ghn13	●	Disabled	Disabled
Ghn14	●	Disabled	Disabled
Ghn15	●	Disabled	Disabled



Ghn16	●	Disabled	Disabled
Ghn17	●	Disabled	Disabled
Ghn18	●	Disabled	Disabled
Ghn19	●	Disabled	Disabled
Ghn20	●	Disabled	Disabled
Ghn21	●	Disabled	Disabled
Ghn22	●	Disabled	Disabled
Ghn23	●	Disabled	Disabled
Ghn24	●	Disabled	Disabled

3.9.3 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-aggregation 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.

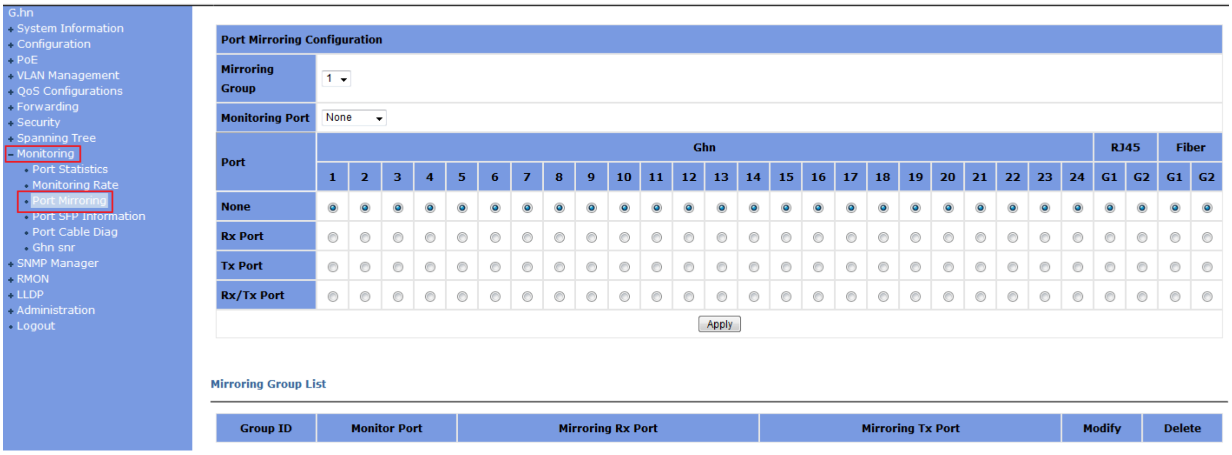
None: Means to mirror none packets on the port;

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

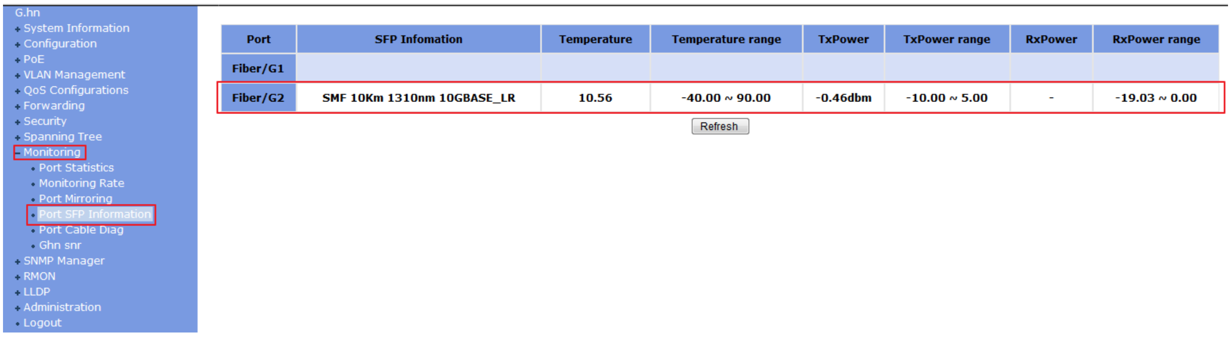
Port	Ghn																								RJ45		Fiber	
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	G1	G2	G1	G2
None	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Rx Port	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Tx Port	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Rx/Tx Port	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○

Mirroring Group List

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

3.9.4 Port SFP Information

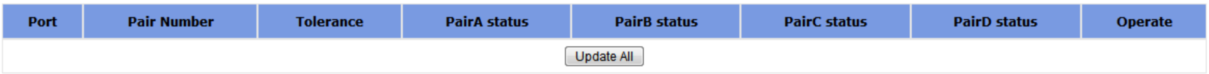
You can check the SFP model information (like Temperature, Tx/Rx Power) as below



Port	SFP Infomation	Temperature	Temperature range	TxPower	TxPower range	RxPower	RxPower range
Fiber/G1							
Fiber/G2	SMF 10Km 1310nm 10GBASE_LR	10.56	-40.00 ~ 90.00	-0.46dbm	-10.00 ~ 5.00	-	-19.03 ~ 0.00

3.9.5 Port Cable Diag

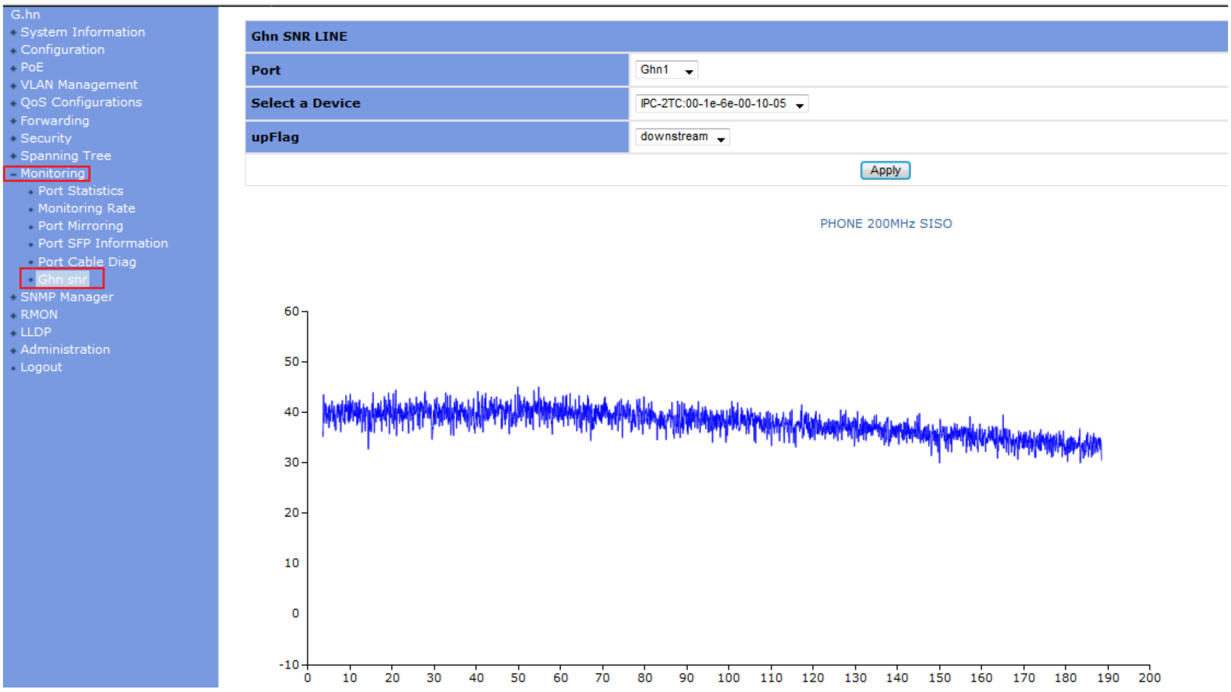
This page shows the port cable diagnosis information



Port	Pair Number	Tolerance	PairA status	PairB status	PairC status	PairD status	Operate

3.9.5 Ghn SNR

You can check the node upstream and downstream SNR information in this page as below:



Ghn SNR LINE

Port	Ghn1
Select a Device	IPC-2TC:00-1e-6e-00-10-05
upFlag	downstream

Note: in order to get the SNR information, the PC needs to have IP connectivity with the RX node, for example, if the RX node IP address is 192.168.10.253, netmask 255.255.255.0, the IP of this PC should be 192.168.10.xxx

3.10 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 written 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.

3.10.1 SNMP Community

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

SNMP Version

v1 To create an SNMPv1 user.

v2c To create an SNMPv2c user.

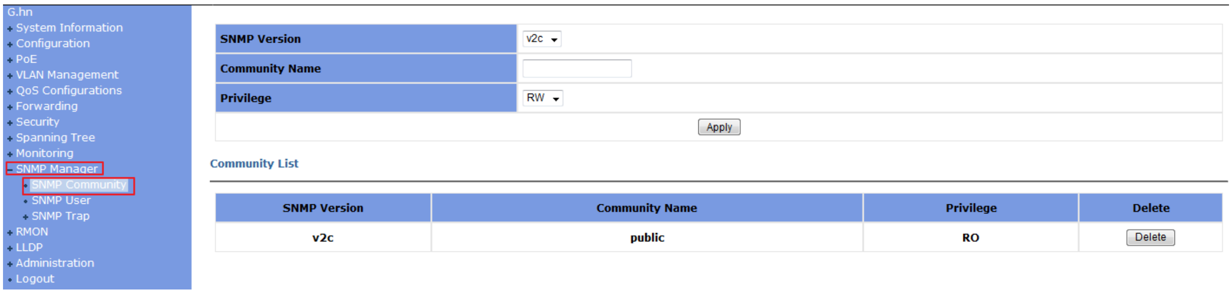
Community Name The name of the community. It is a string with 3 to 16 characters

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.



SNMP Version	v2c
Community Name	
Privilege	RW

Community List

SNMP Version	Community Name	Privilege	Delete
v2c	public	RO	Delete

3.10.2 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 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.

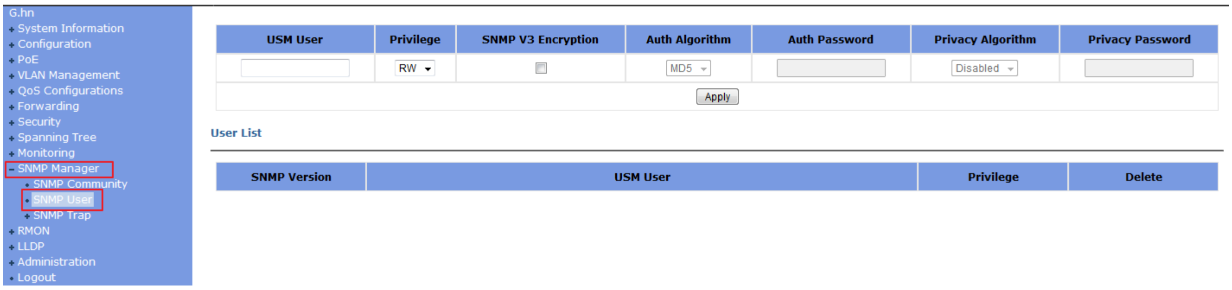
Privacy Algorithm: Select the Privacy Algorithm for the SNMP v3 User.

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.



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

User List

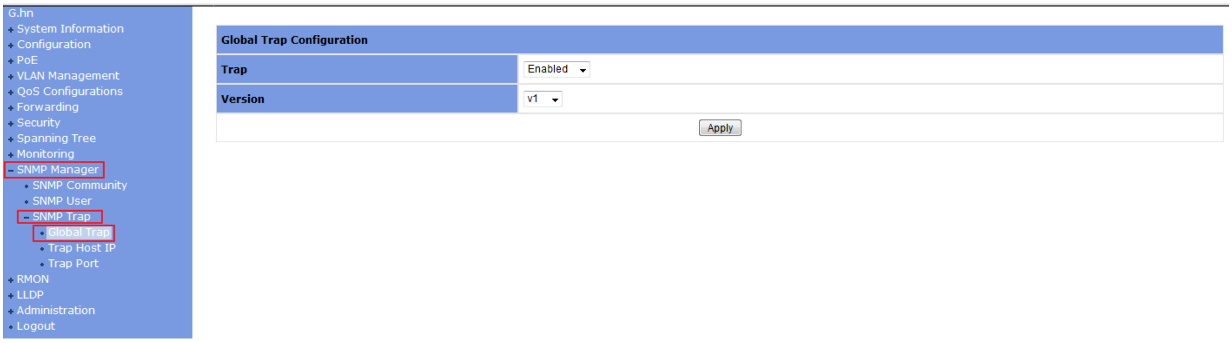
SNMP Version	USM User	Privilege	Delete

3.10.3 SNMP Trap

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

3.10.3.1 Global Trap

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

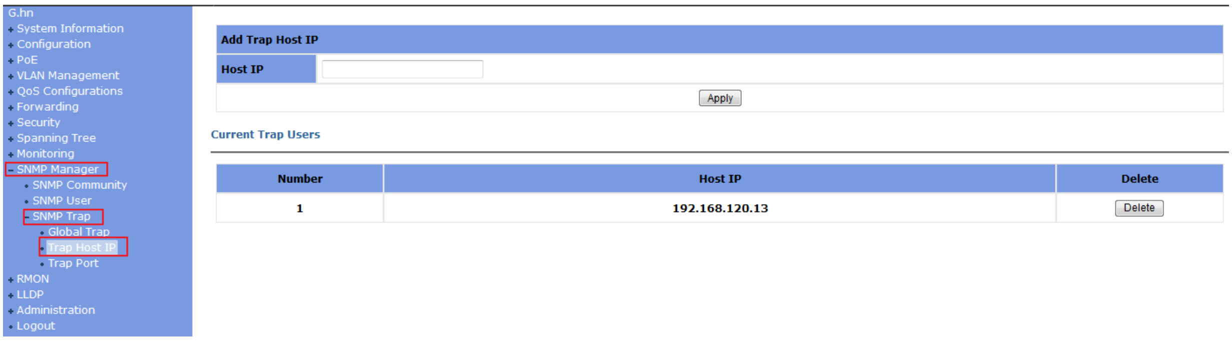


Global Trap Configuration	
Trap	Enabled
Version	v1

3.10.3.2 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	

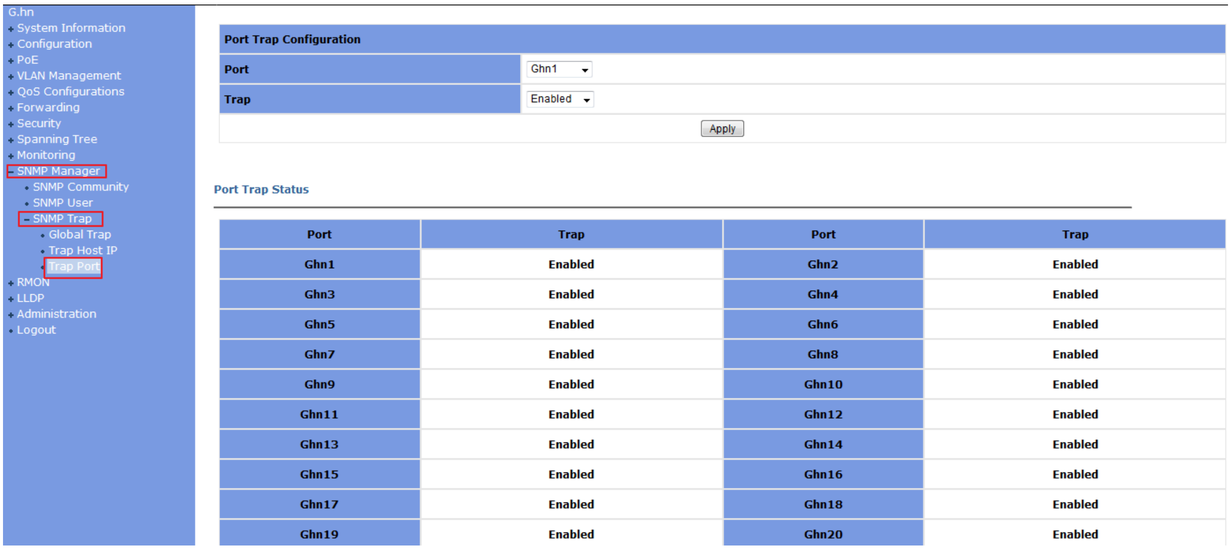
Current Trap Users

Number	Host IP	Delete
1	192.168.120.13	Delete

3.10.3.3 Trap Port

Enable or disable the trap function for each port.

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

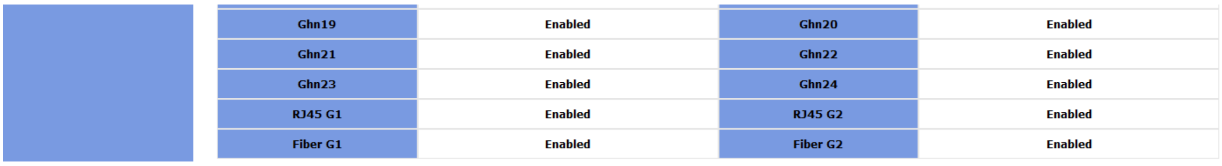


Port Trap Configuration

Port	Ghn1
Trap	Enabled

Port Trap Status

Port	Trap	Port	Trap
Ghn1	Enabled	Ghn2	Enabled
Ghn3	Enabled	Ghn4	Enabled
Ghn5	Enabled	Ghn6	Enabled
Ghn7	Enabled	Ghn8	Enabled
Ghn9	Enabled	Ghn10	Enabled
Ghn11	Enabled	Ghn12	Enabled
Ghn13	Enabled	Ghn14	Enabled
Ghn15	Enabled	Ghn16	Enabled
Ghn17	Enabled	Ghn18	Enabled
Ghn19	Enabled	Ghn20	Enabled



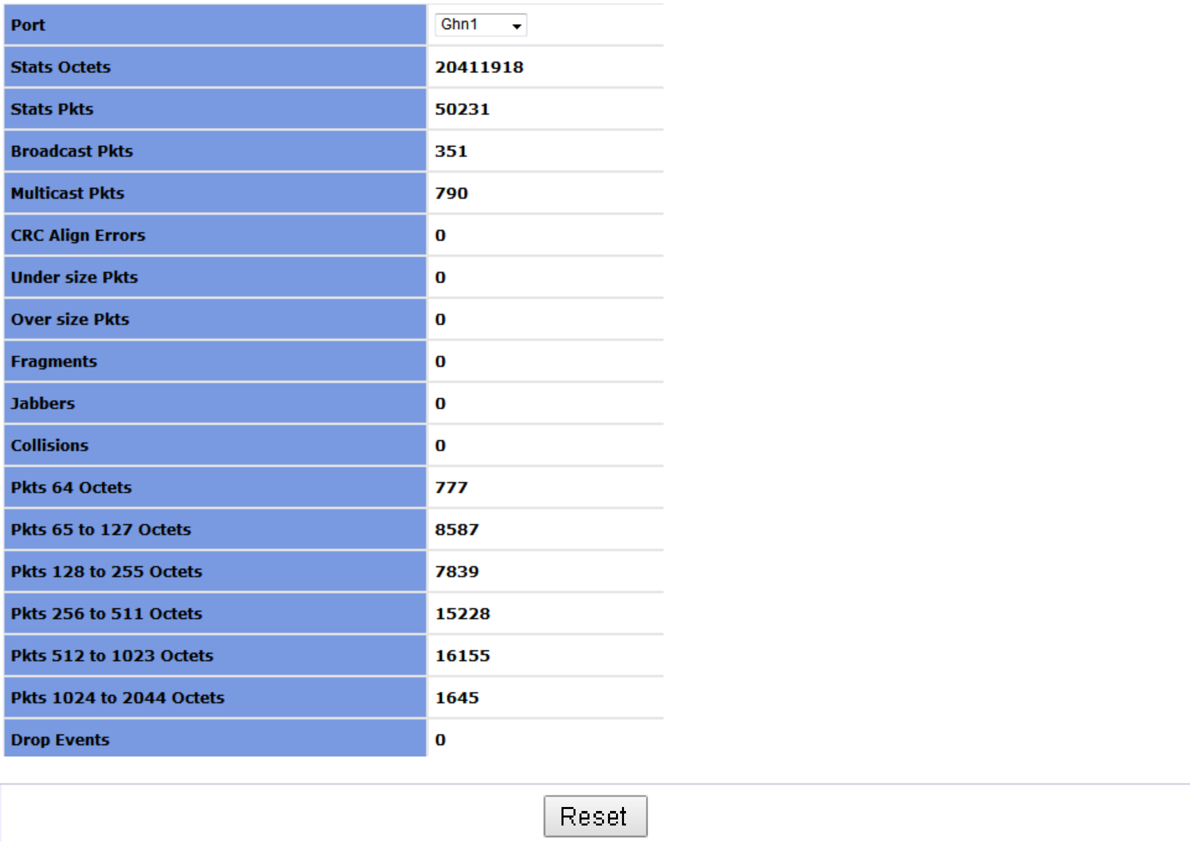
Ghn19	Enabled	Ghn20	Enabled
Ghn21	Enabled	Ghn22	Enabled
Ghn23	Enabled	Ghn24	Enabled
RJ45 G1	Enabled	RJ45 G2	Enabled
Fiber G1	Enabled	Fiber G2	Enabled

3.11 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.

3.11.1 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	Ghn1
Stats Octets	20411918
Stats Pkts	50231
Broadcast Pkts	351
Multicast Pkts	790
CRC Align Errors	0
Under size Pkts	0
Over size Pkts	0
Fragments	0
Jabbers	0
Collisions	0
Pkts 64 Octets	777
Pkts 65 to 127 Octets	8587
Pkts 128 to 255 Octets	7839
Pkts 256 to 511 Octets	15228
Pkts 512 to 1023 Octets	16155
Pkts 1024 to 2044 Octets	1645
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 received packets which 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.

3.11.2 History

3.11.2.1 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.

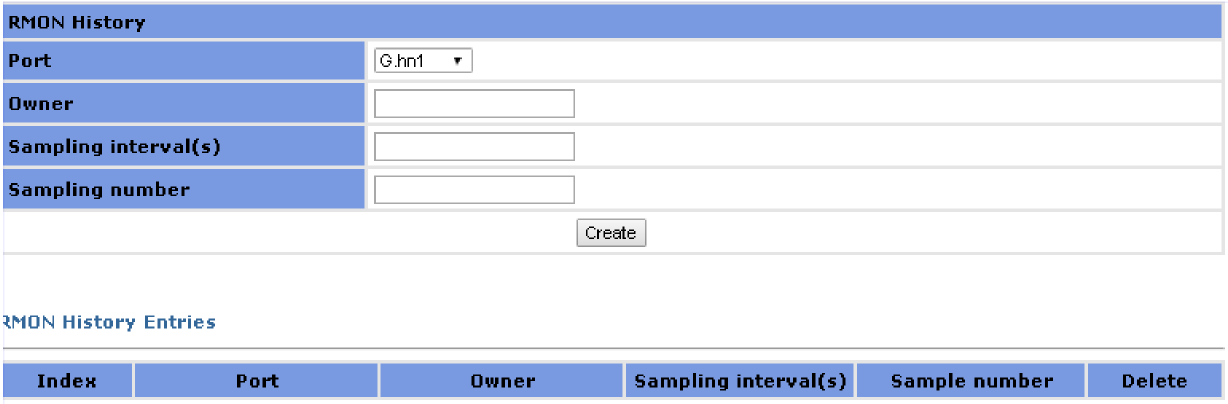
Port The Ethernet port for collecting statistics.

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	

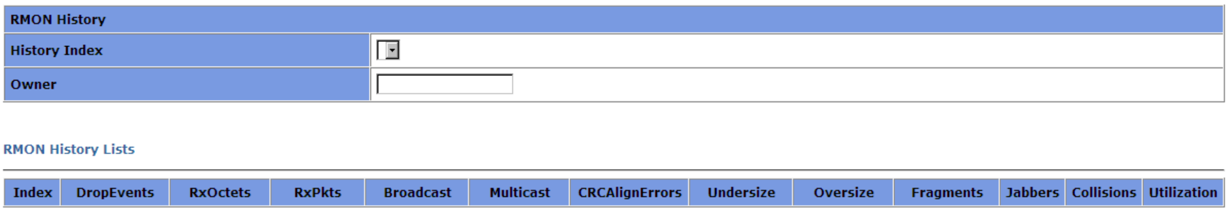
RMON History Entries

Index	Port	Owner	Sampling interval(s)	Sample number	Delete

3.11.2.2 History List

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

g



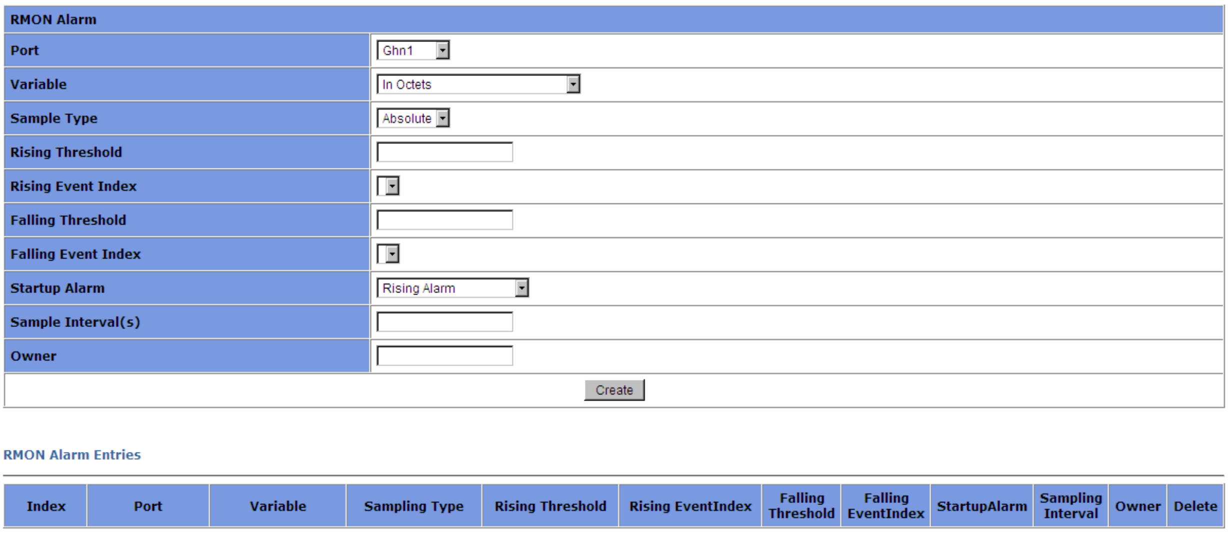
RMON History	
History Index	▾
Owner	

RMON History Lists

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

3.11.3 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	
Create	

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,

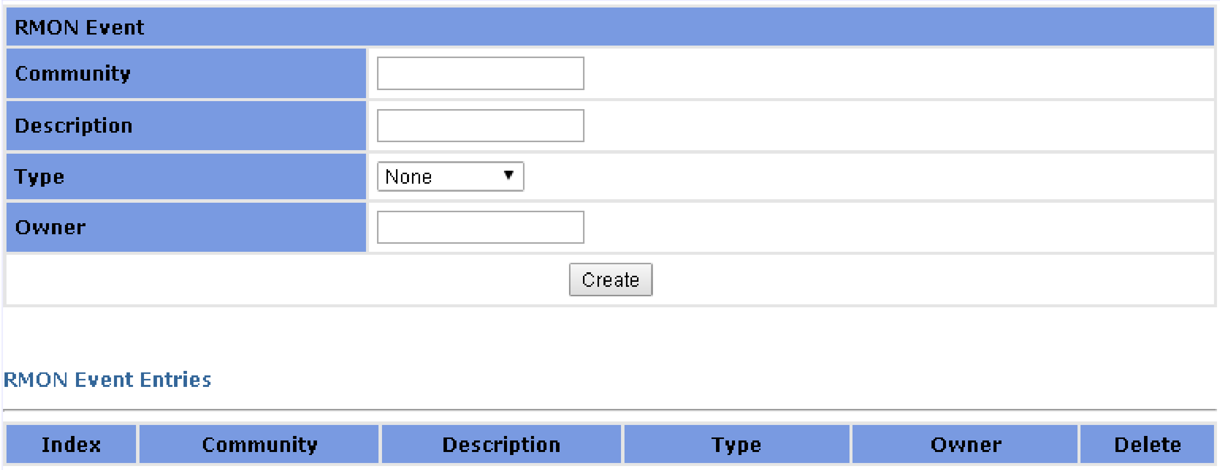
In Discarded Pks, In Error Pks, In Unknown Protocol Pks, Out Octets, Out Unicast Pks, Out None Unicast Pks, Out Discarded Pks, Out Error Pks, RMON Drop Events, RMON Received Octets, RMON Received Pks, RMON Broadcast Pks, RMON Multicast Pks, RMON CRC Align Pks, RMON Undersize Pks, RMON Oversize Pks, RMON 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 absolute Value (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 delta Value (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.

3.11.4 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.

3.11.4.1 Event



RMON Event	
Community	
Description	
Type	None ▼
Owner	
Create	

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.

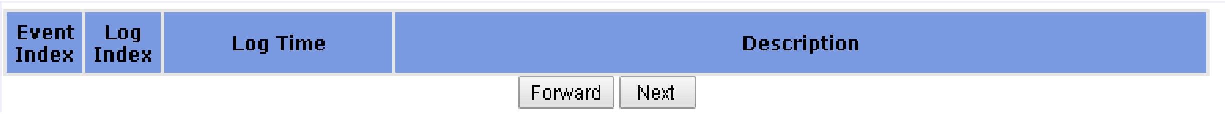
- **None**: No action;
- **Log** : The result will be shown in Event Log;
- **Trap**: The switch will send trap to the specified trap host
- **Log and trap**: The trap will be shown in Event Log and sent to the specified trap host.

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.

3.11.4.2 Event Log

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



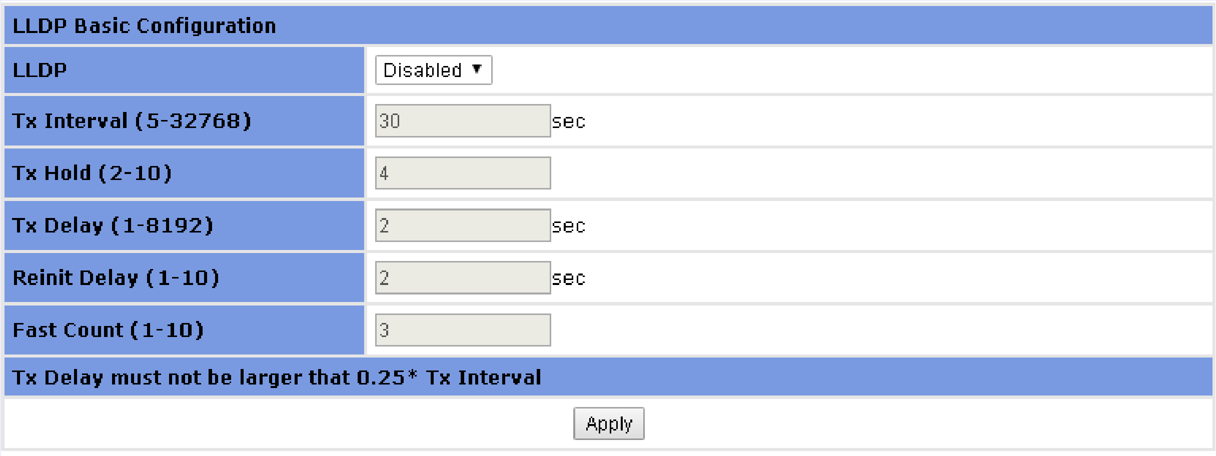
Event Index	Log Index	Log Time	Description

3.12 LLDP

3.12.1 Configuration

3.12.1.1 Basic

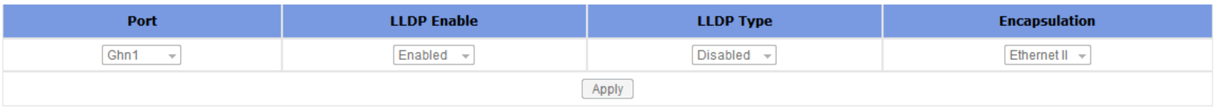
This page sets lldp enable or disabled



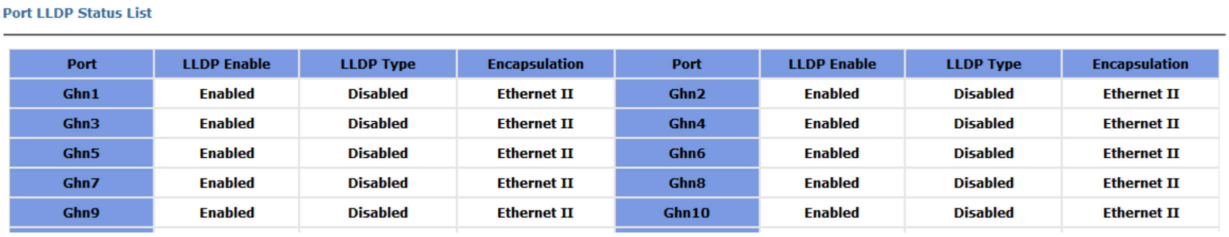
LLDP Basic Configuration	
LLDP	Disabled
Tx Interval (5-32768)	30 sec
Tx Hold (2-10)	4
Tx Delay (1-8192)	2 sec
Reinit Delay (1-10)	2 sec
Fast Count (1-10)	3
Tx Delay must not be larger that 0.25* Tx Interval	

3.12.1.2 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
Ghn1	Enabled	Disabled	Ethernet II



Port LLDP Status List

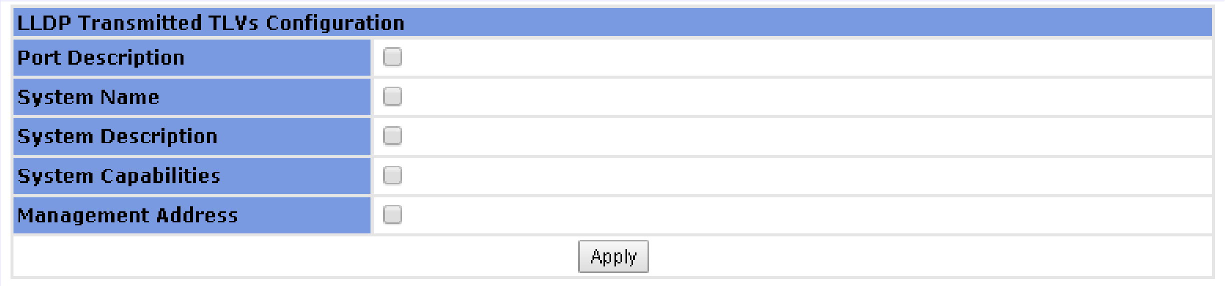
Port	LLDP Enable	LLDP Type	Encapsulation	Port	LLDP Enable	LLDP Type	Encapsulation
Ghn1	Enabled	Disabled	Ethernet II	Ghn2	Enabled	Disabled	Ethernet II
Ghn3	Enabled	Disabled	Ethernet II	Ghn4	Enabled	Disabled	Ethernet II
Ghn5	Enabled	Disabled	Ethernet II	Ghn6	Enabled	Disabled	Ethernet II
Ghn7	Enabled	Disabled	Ethernet II	Ghn8	Enabled	Disabled	Ethernet II
Ghn9	Enabled	Disabled	Ethernet II	Ghn10	Enabled	Disabled	Ethernet II

EthernetII: the Ethernet frame of type 0x88cc.

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

3.12.1.3 TLVs

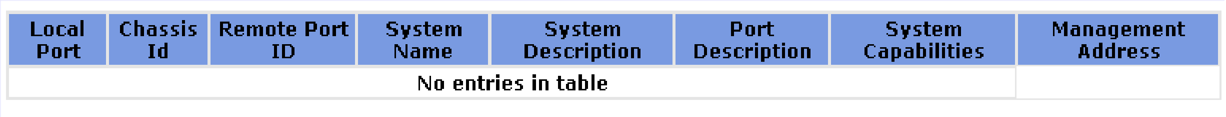
This page sets the type of transmitting information: **Port Description, System Name, System Description, System Capability,** and **Management Address**.



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

3.12.2 Neighbor

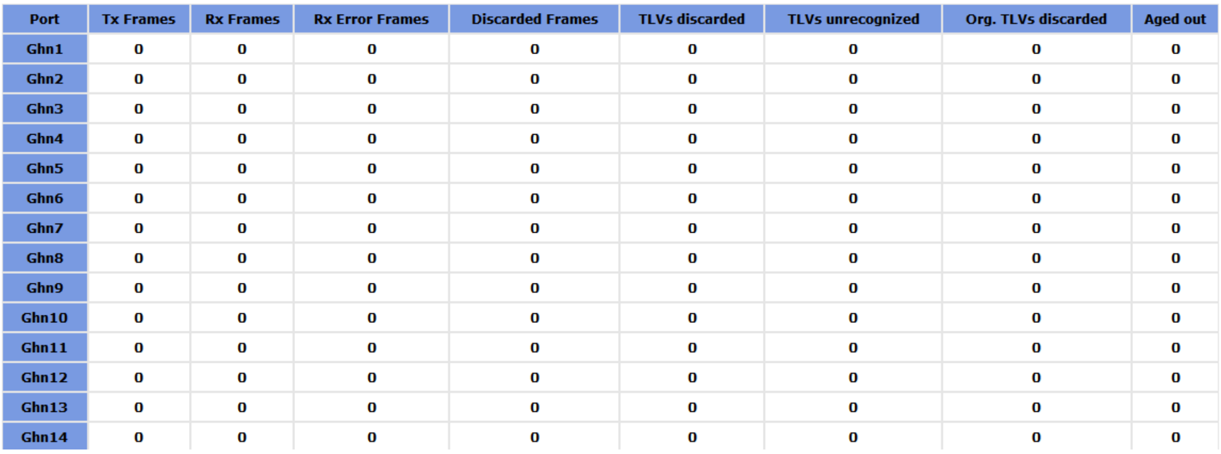
This page shows the **Local Port, Chassis Id** of a local device**,** and the **Remote Port ID, System name, Port description, System Capabilities**, and **Management Address** of a neighbor device.



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

3.12.3 Statistics

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

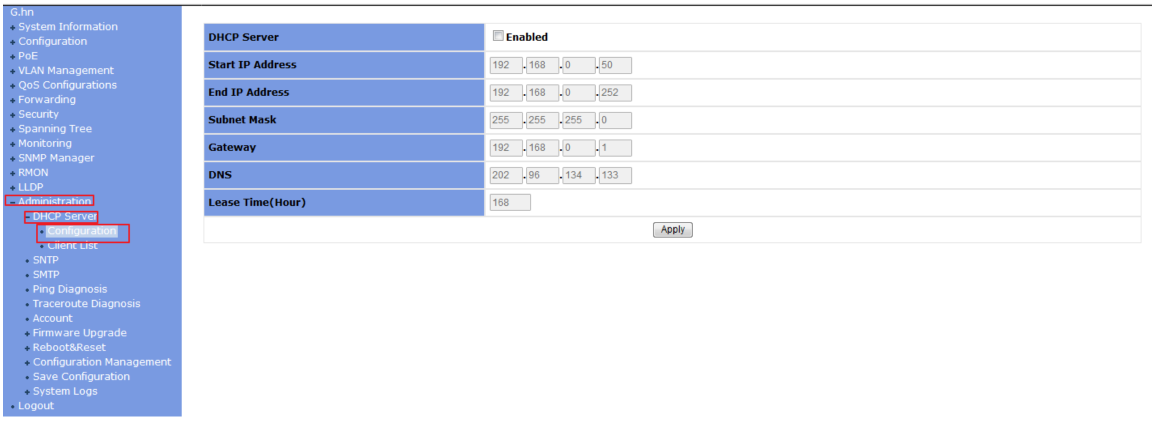


Port	Tx Frames	Rx Frames	Rx Error Frames	Discarded Frames	TLVs discarded	TLVs unrecognized	Org. TLVs discarded	Aged out
Ghn1	0	0	0	0	0	0	0	0
Ghn2	0	0	0	0	0	0	0	0
Ghn3	0	0	0	0	0	0	0	0
Ghn4	0	0	0	0	0	0	0	0
Ghn5	0	0	0	0	0	0	0	0
Ghn6	0	0	0	0	0	0	0	0
Ghn7	0	0	0	0	0	0	0	0
Ghn8	0	0	0	0	0	0	0	0
Ghn9	0	0	0	0	0	0	0	0
Ghn10	0	0	0	0	0	0	0	0
Ghn11	0	0	0	0	0	0	0	0
Ghn12	0	0	0	0	0	0	0	0
Ghn13	0	0	0	0	0	0	0	0
Ghn14	0	0	0	0	0	0	0	0

3.13 Administration

3.13.1 DHCP Server

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 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

3.13.2 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.

You can configure the SNTP on this page.

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.

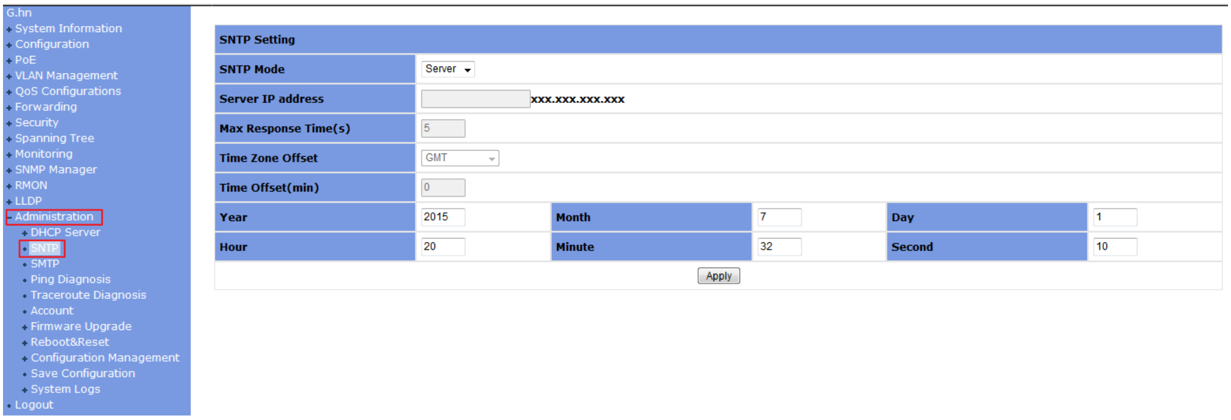
Service IP address IP address of the SNTP server

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.



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	1
Hour	20	Minute	32	Second	10

3.13.3 SMTP

This page sets SMTP configuration. When a pre-defined event occurs, an e-mail will be sent to the following destination mail address.

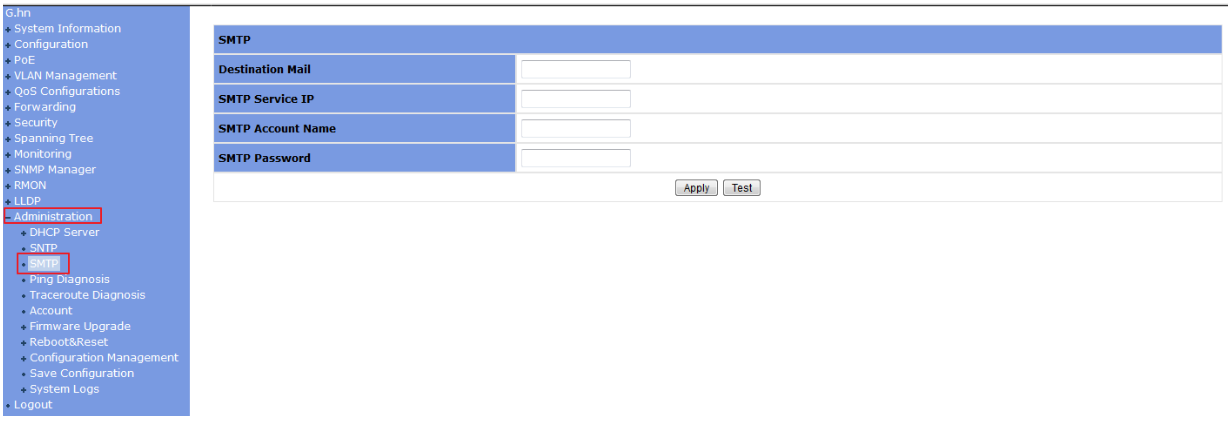
Destination Mail The e-mail address to receive the event information.

SMTP Service IP The IP address of SMTP server.

Source Account Name Source e-mail account on SMTP server.

SMTP Password The password for source e-mail account.

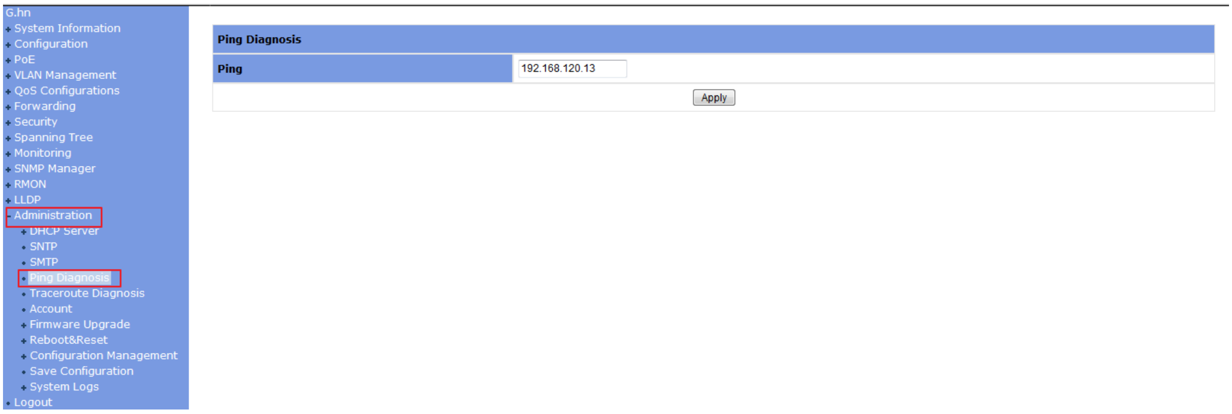
Click <Test> to check whether the configuration is correct. If it is correct, the destination mail will receive an e-mail.



SMTP	
Destination Mail	
SMTP Service IP	
SMTP Account Name	
SMTP Password	

3.13.4 Ping Diagnosis

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

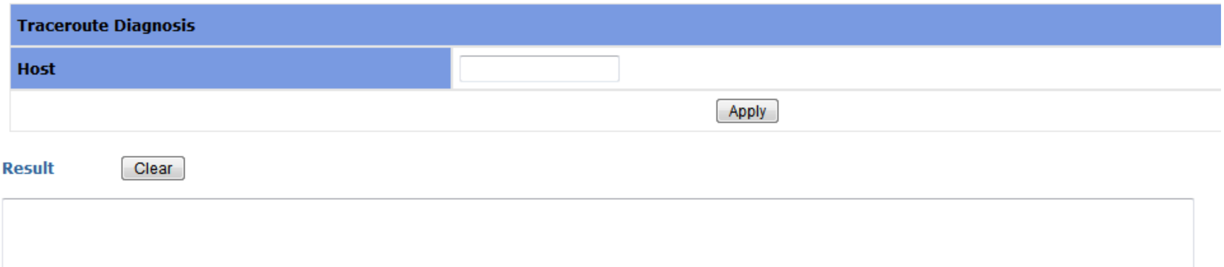


Ping Diagnosis

Ping	192.168.120.13

3.13.5 Traceroute Diagnosis

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



Traceroute Diagnosis

Host	

3.13.6 Account

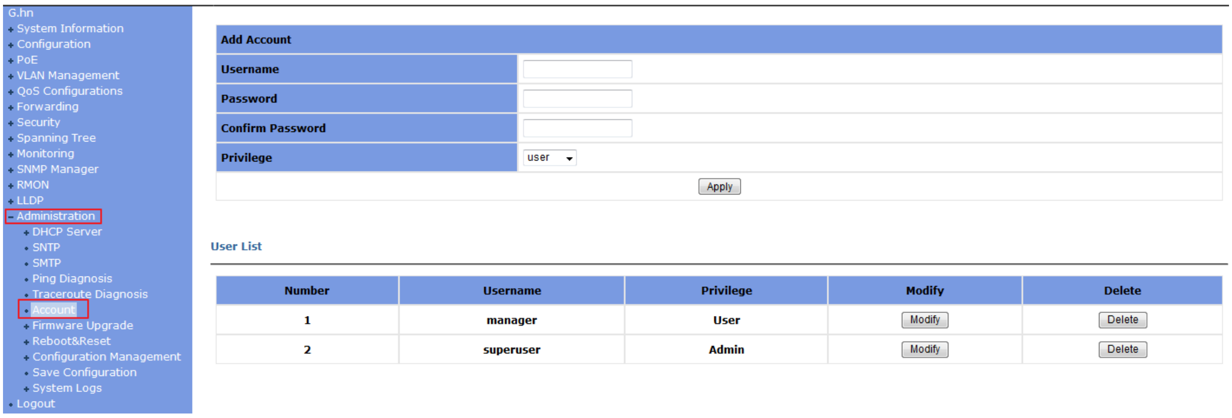
On this page, **Add Account** is used to add a new account. A set of specified **Username**, **Password** and **Privilege** for the new account shall be assigned.

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	user
	Apply

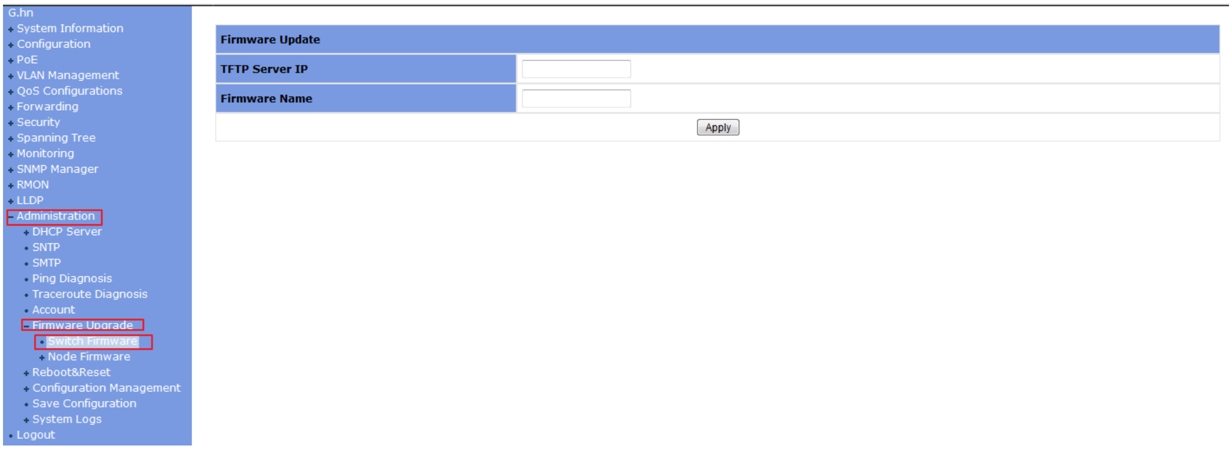
User List

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

3.13.7 Firmware Upgrade

3.13.7.1 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.

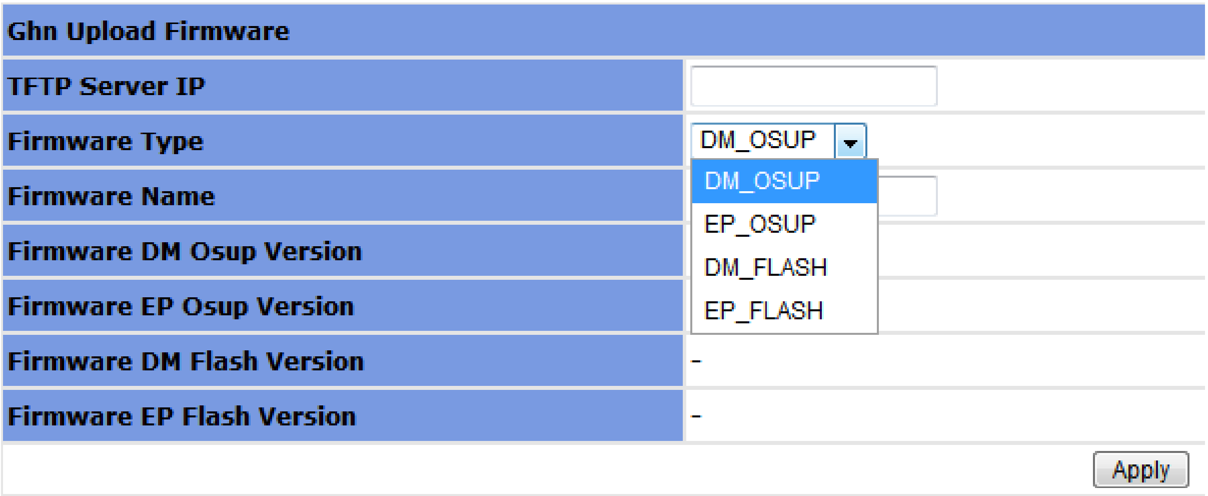


Firmware Update	
TFTP Server IP	
Firmware Name	
	Apply

3.13.7.2 Node Firmware

1) Firmware Loader

Before upgrade for nodes, you need to upload the node firmware first. If you use osup file to upload local/remote node software, you must choose the Firmware Type ‘DM_OSUP’/’EP_OSUP’, if you use flash file to upload local/remote node software, you must choose Firmware Type ‘DM_FLASH’/’EP_FLASH’. Please make sure that the TFTP Server IP and Node Name is correct, then you can you can start the node firmware upgrade. If you choose incorrectly or load wrong software, system will inform “Firmware Upload failed”



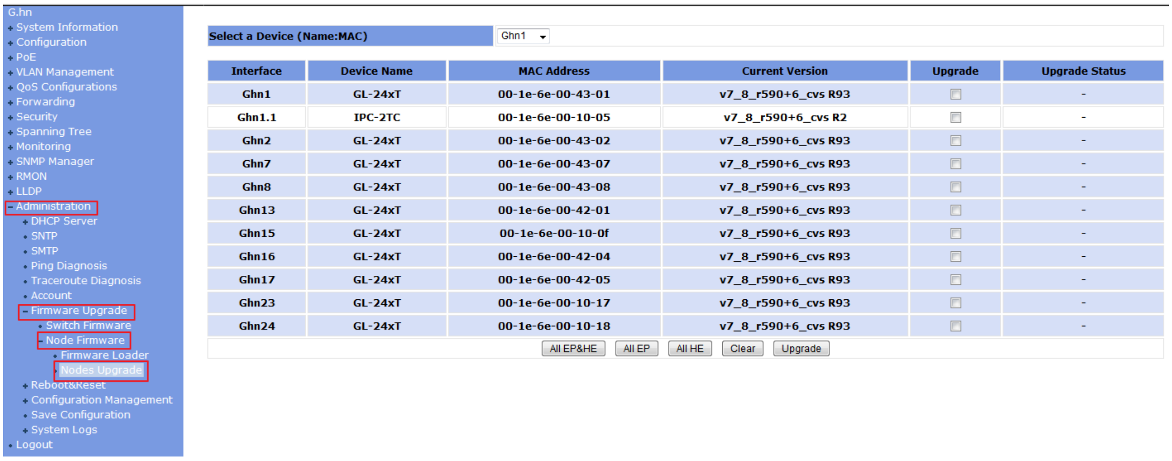
Ghn Upload Firmware	
TFTP Server IP	
Firmware Type	DM_OSUP
Firmware Name	
Firmware DM Osup Version	
Firmware EP Osup Version	
Firmware DM Flash Version	-
Firmware EP Flash Version	-

Note: Sometimes you have checked and ensure that the TFTP Server IP, Firmware Type and Firmware are all correct, but when you click “Apply” to upload firmware, it still show you “Firmware Upload Failed”. In this case, it may be caused by the firmware name(firmware name is too long), you can try to shorten the firmware name and try again. For example, the original firmware name is “Ghn HE_nologo-P2MP_web-SPIRIT.v7_6_r589+11_cvs_2.85.ftp”, then change it to “Ghn HE_web. v7_6_r589+11.ftp”, and try upload it again.

2) Node Upgrade

The selected devices will be upgraded firmware by this page.

For Node Upgrade batch, local and remote can be operated at the same time.
Don’t cut off power or restart during upgrading, otherwise the system can’t be stated.
After upgrading, remote will restart automatically and make the new software take effect. Local will be restarted by manually to make the new software take effect.



Select a Device (Name:MAC): Ghn1

Interface	Device Name	MAC Address	Current Version	Upgrade	Upgrade Status
Ghn1	GL-24xT	00-1e-6e-00-43-01	v7_8_r590+6_cvs R93	□	-
Ghn1.1	IPC-2TC	00-1e-6e-00-10-05	v7_8_r590+6_cvs R2	□	-
Ghn2	GL-24xT	00-1e-6e-00-43-02	v7_8_r590+6_cvs R93	□	-
Ghn7	GL-24xT	00-1e-6e-00-43-07	v7_8_r590+6_cvs R93	□	-
Ghn8	GL-24xT	00-1e-6e-00-43-08	v7_8_r590+6_cvs R93	□	-
Ghn13	GL-24xT	00-1e-6e-00-42-01	v7_8_r590+6_cvs R93	□	-
Ghn15	GL-24xT	00-1e-6e-00-10-0f	v7_8_r590+6_cvs R93	□	-
Ghn16	GL-24xT	00-1e-6e-00-42-04	v7_8_r590+6_cvs R93	□	-
Ghn17	GL-24xT	00-1e-6e-00-42-05	v7_8_r590+6_cvs R93	□	-
Ghn23	GL-24xT	00-1e-6e-00-10-17	v7_8_r590+6_cvs R93	□	-
Ghn24	GL-24xT	00-1e-6e-00-10-18	v7_8_r590+6_cvs R93	□	-

Note: If use osup file to upload node software, please choose the ‘Nodes Osup Upgrade ‘page. if use flash file to upload node software, please choose the' Nodes Flash Upgrade' page.

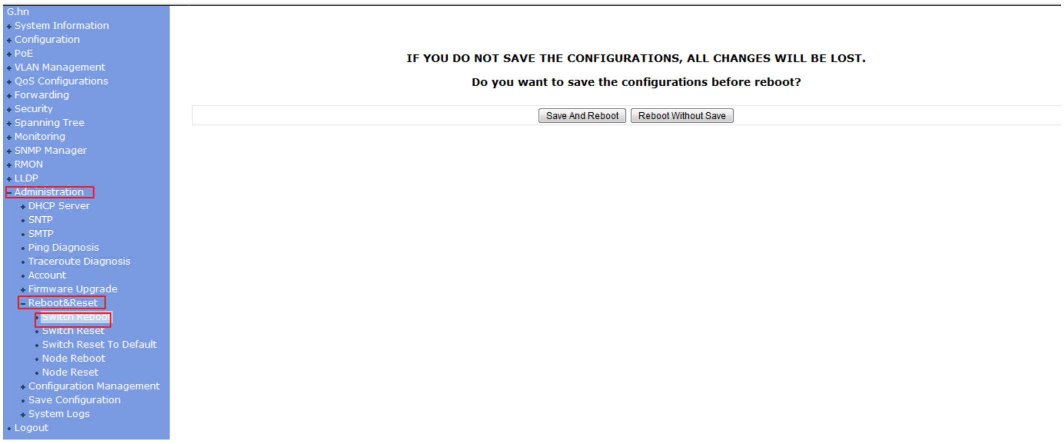
3.13.8 Reboot & Reset

3.13.8.1 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.

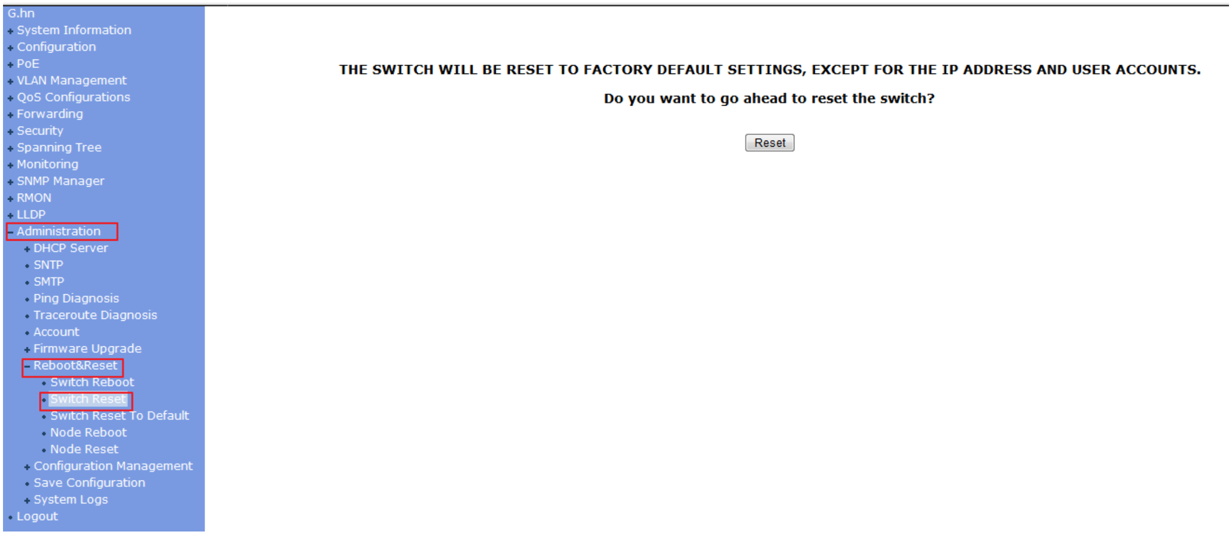


IF YOU DO NOT SAVE THE CONFIGURATIONS, ALL CHANGES WILL BE LOST.

Do you want to save the configurations before reboot?

3.13.8.2 Switch Reset

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

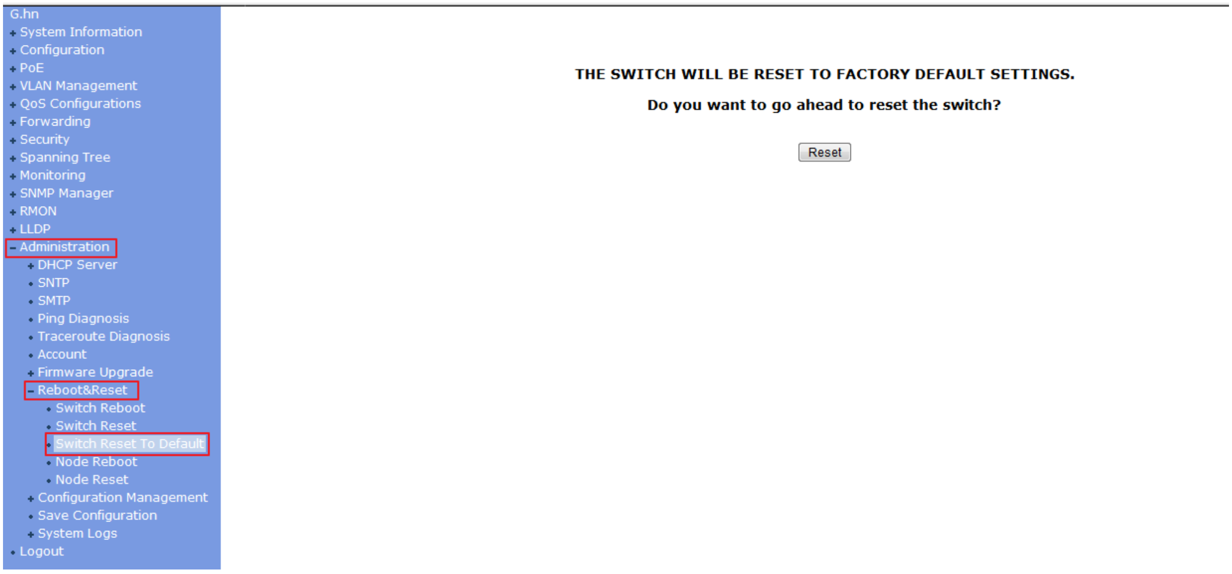


THE SWITCH WILL BE RESET TO FACTORY DEFAULT SETTINGS, EXCEPT FOR THE IP ADDRESS AND USER ACCOUNTS.

Do you want to go ahead to reset the switch?

3.13.8.3 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?

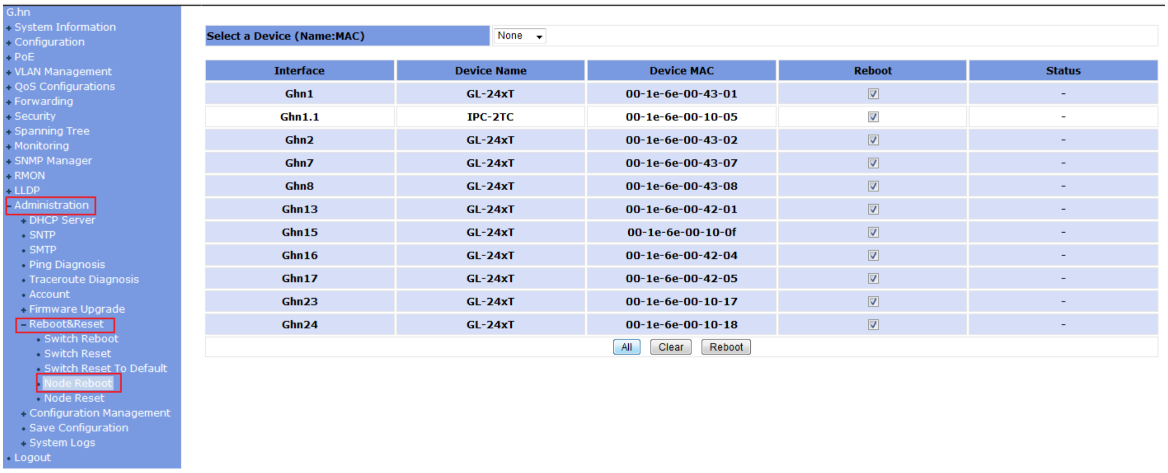
Reset

3.13.8.4 Node Reboot & Reset

For Node factory batch reset，local and remote cannot be operated at the same time. After finish remote operation, then local can be operated.

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

Node Reboot:

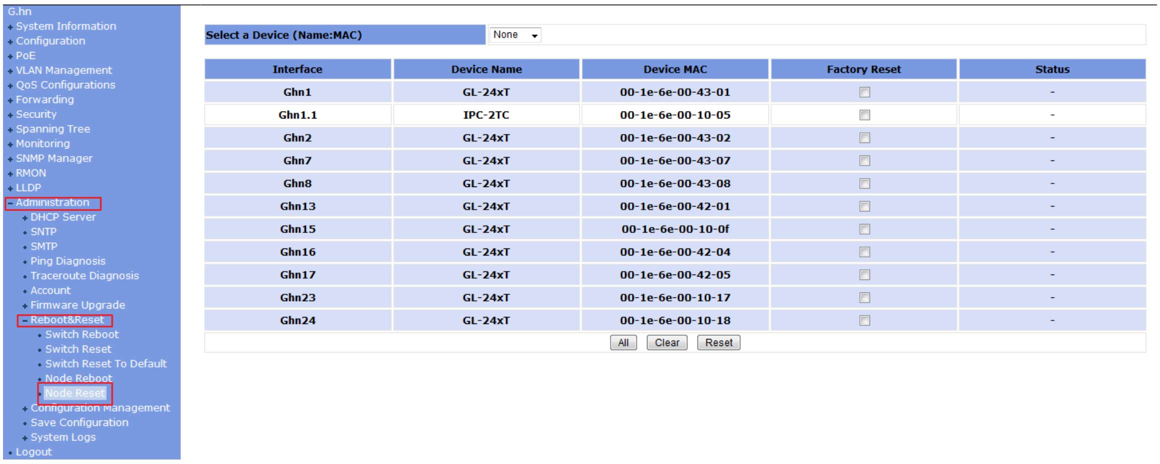


Select a Device (Name:MAC) None

Interface	Device Name	Device MAC	Reboot	Status
Ghn1	GL-24xT	00-1e-6e-00-43-01	☑	-
Ghn1.1	IPC-2TC	00-1e-6e-00-10-05	☑	-
Ghn2	GL-24xT	00-1e-6e-00-43-02	☑	-
Ghn7	GL-24xT	00-1e-6e-00-43-07	☑	-
Ghn8	GL-24xT	00-1e-6e-00-43-08	☑	-
Ghn13	GL-24xT	00-1e-6e-00-42-01	☑	-
Ghn15	GL-24xT	00-1e-6e-00-10-0f	☑	-
Ghn16	GL-24xT	00-1e-6e-00-42-04	☑	-
Ghn17	GL-24xT	00-1e-6e-00-42-05	☑	-
Ghn23	GL-24xT	00-1e-6e-00-10-17	☑	-
Ghn24	GL-24xT	00-1e-6e-00-10-18	☑	-

All Clear Reboot

Node Reset:



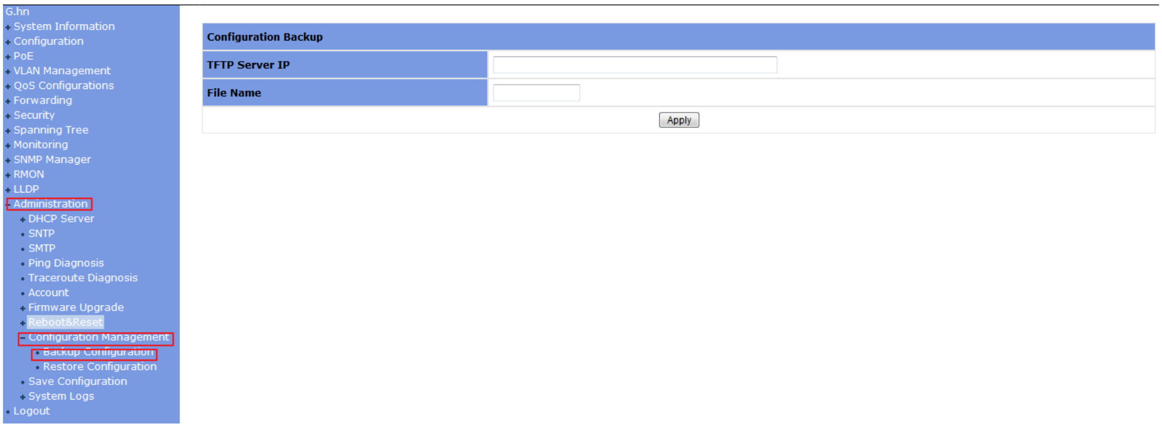
Select a Device (Name:MAC) None

Interface	Device Name	Device MAC	Factory Reset	Status
Ghn1	GL-24xT	00-1e-6e-00-43-01	□	-
Ghn1.1	IPC-2TC	00-1e-6e-00-10-05	□	-
Ghn2	GL-24xT	00-1e-6e-00-43-02	□	-
Ghn7	GL-24xT	00-1e-6e-00-43-07	□	-
Ghn8	GL-24xT	00-1e-6e-00-43-08	□	-
Ghn13	GL-24xT	00-1e-6e-00-42-01	□	-
Ghn15	GL-24xT	00-1e-6e-00-10-0f	□	-
Ghn16	GL-24xT	00-1e-6e-00-42-04	□	-
Ghn17	GL-24xT	00-1e-6e-00-42-05	□	-
Ghn23	GL-24xT	00-1e-6e-00-10-17	□	-
Ghn24	GL-24xT	00-1e-6e-00-10-18	□	-

3.13.9 Configuration Management

3.13.9.1 Backup Configuration

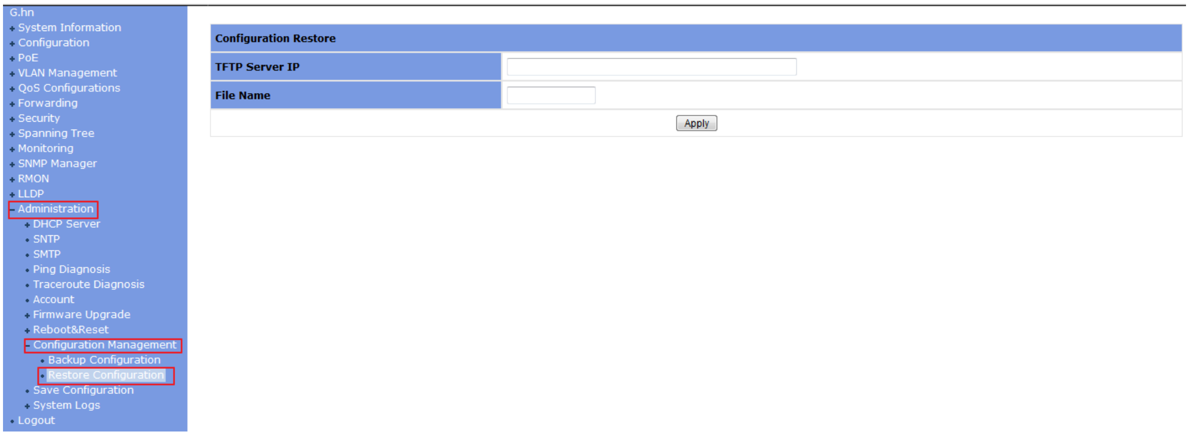
This page sets **TFTP Server IP** and **File Name**. Make sure the switch is connected to the TFTP server before clicking <Apply> to upload the switch configuration file specified in "**File Name**" to TFTP server.



Configuration Backup	
TFTP Server IP	
File Name	

3.13.9.2 Restore Configuration

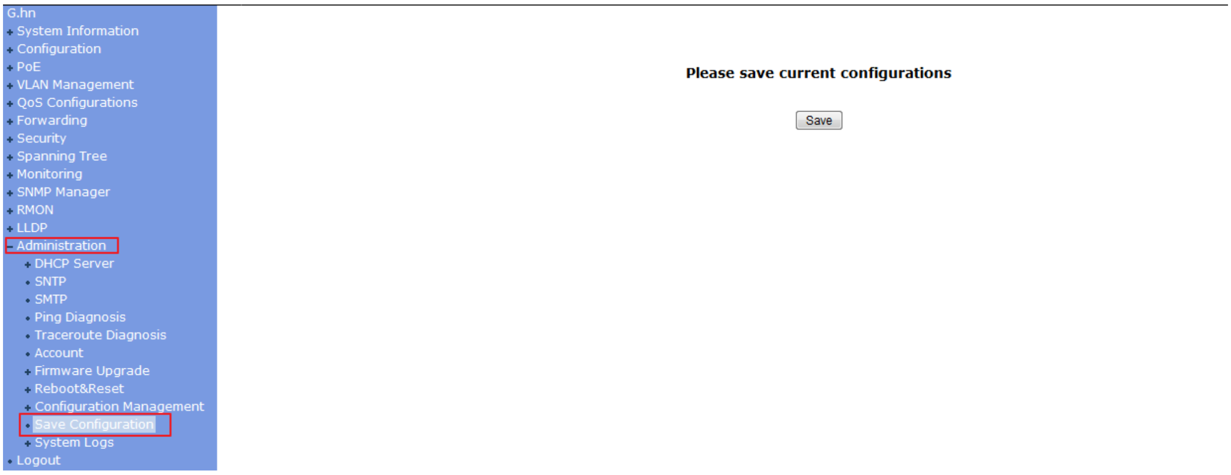
This page sets **TFTP Server IP** and **File Name**. Make sure the switch is connected to the TFTP server, and next click <Apply> to download the file specified in "**File Name**" from the TFTP server and use it as the configuration file for the switch.



Configuration Restore	
TFTP Server IP	
File Name	

3.13.10 Save Configuration

This page saves current configurations.

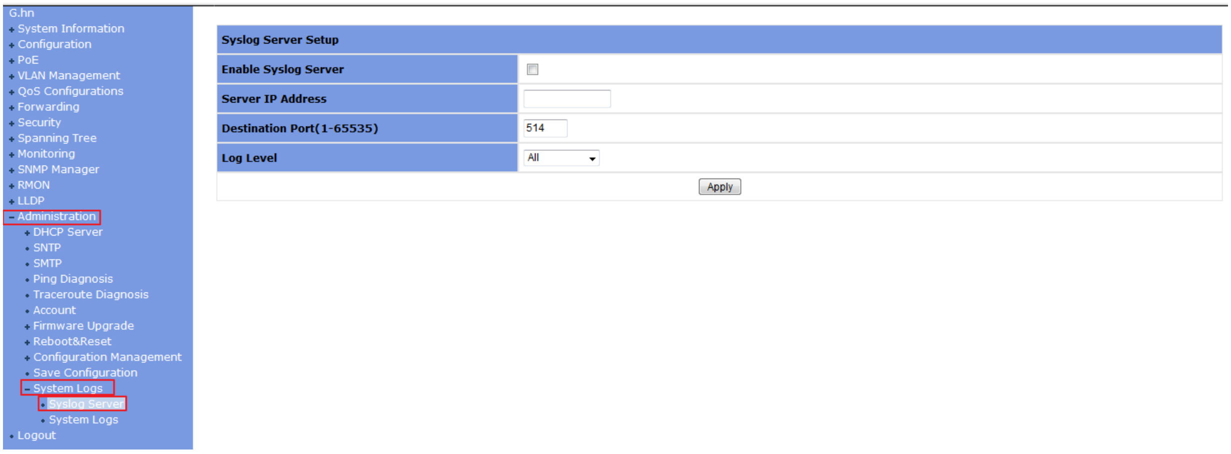


Please save current configurations

3.13.11 System Logs

3.13.11.1 Syslog Server

This page sets sys log server



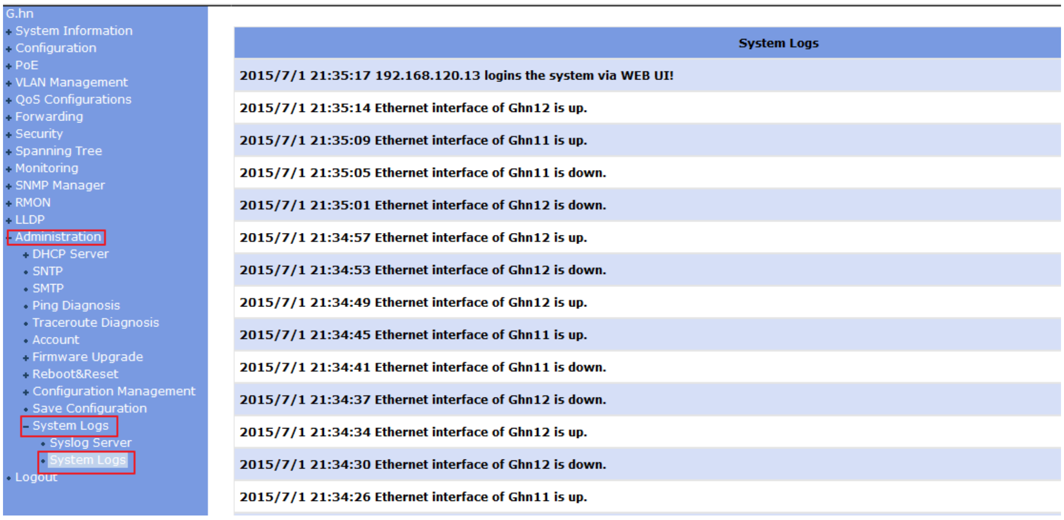
Syslog Server Setup	
Enable Syslog Server	☐
Server IP Address	
Destination Port(1-65535)	514
Log Level	All

3.13.11.2 System Logs

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

The main type of log:

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

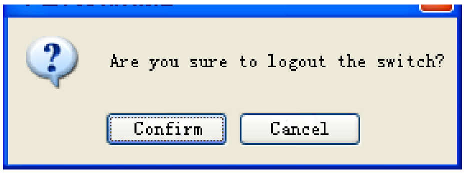


System Logs

```
2015/7/1 21:35:17 192.168.120.13 logins the system via WEB UI!
2015/7/1 21:35:14 Ethernet interface of Ghn12 is up.
2015/7/1 21:35:09 Ethernet interface of Ghn11 is up.
2015/7/1 21:35:05 Ethernet interface of Ghn11 is down.
2015/7/1 21:35:01 Ethernet interface of Ghn12 is down.
2015/7/1 21:34:57 Ethernet interface of Ghn12 is up.
2015/7/1 21:34:53 Ethernet interface of Ghn12 is down.
2015/7/1 21:34:49 Ethernet interface of Ghn12 is up.
2015/7/1 21:34:45 Ethernet interface of Ghn11 is up.
2015/7/1 21:34:41 Ethernet interface of Ghn11 is down.
2015/7/1 21:34:37 Ethernet interface of Ghn12 is down.
2015/7/1 21:34:34 Ethernet interface of Ghn12 is up.
2015/7/1 21:34:30 Ethernet interface of Ghn12 is down.
2015/7/1 21:34:26 Ethernet interface of Ghn11 is up.
```

3.14 Logout

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



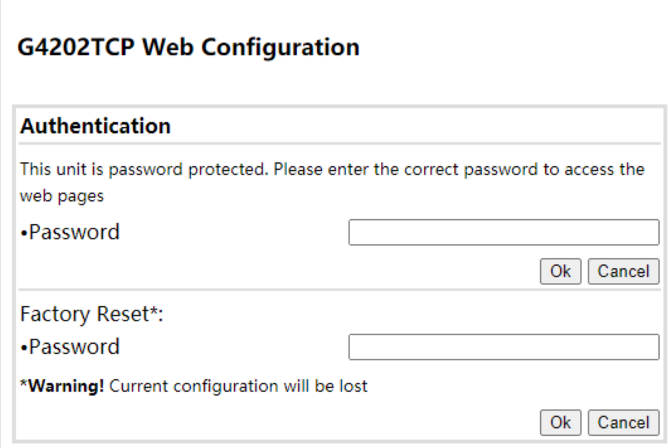
Are you sure to logout the switch?

4 G4202TCP Web-based Management

If you have not made any change to the network setting of G4202TCP. You can browse http://192.168.10.253 to access G4202TCP web management page, default login password is “paterna”, If you have not made any change to the network setting.

4.1 G.hn

After login, the Information page is shown as below, displaying the basic settings, and Encryption configuration.



G4202TCP Web Configuration

Authentication

This unit is password protected. Please enter the correct password to access the web pages

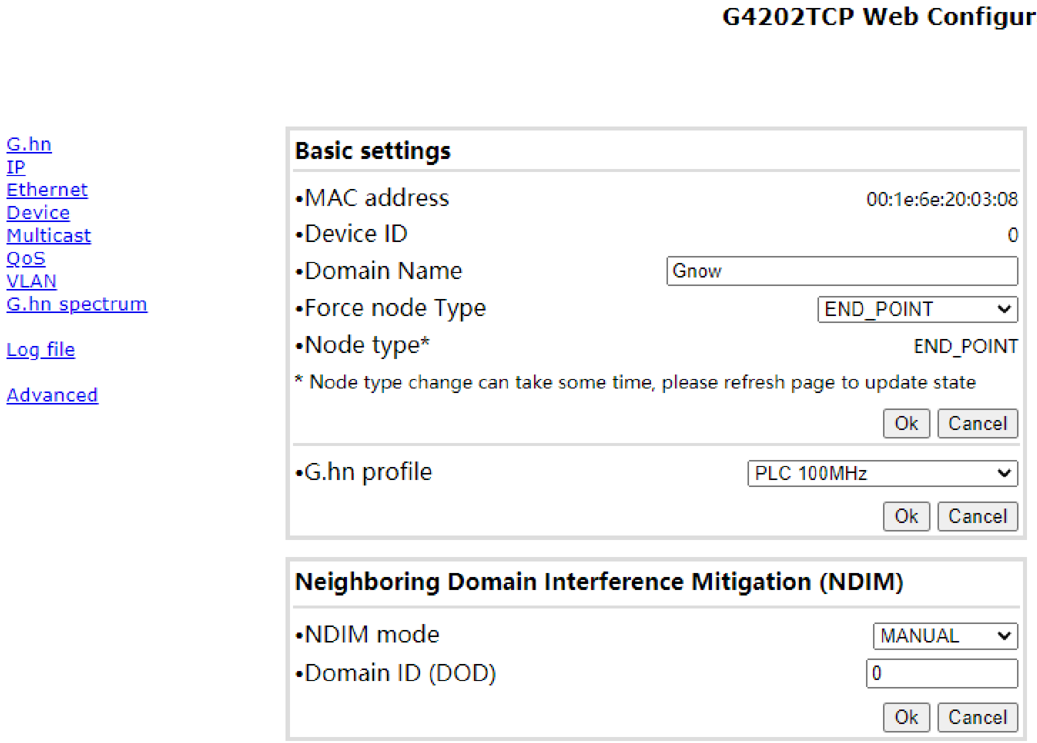
•Password

Factory Reset*:

•Password

***Warning!** Current configuration will be lost

Home Page:



G4202TCP Web Configuration

Basic settings

•MAC address 00:1e:6e:20:03:08

•Device ID 0

•Domain Name Gnow

•Force node Type END_POINT

•Node type* END_POINT

* Node type change can take some time, please refresh page to update state

•G.hn profile PLC 100MHz

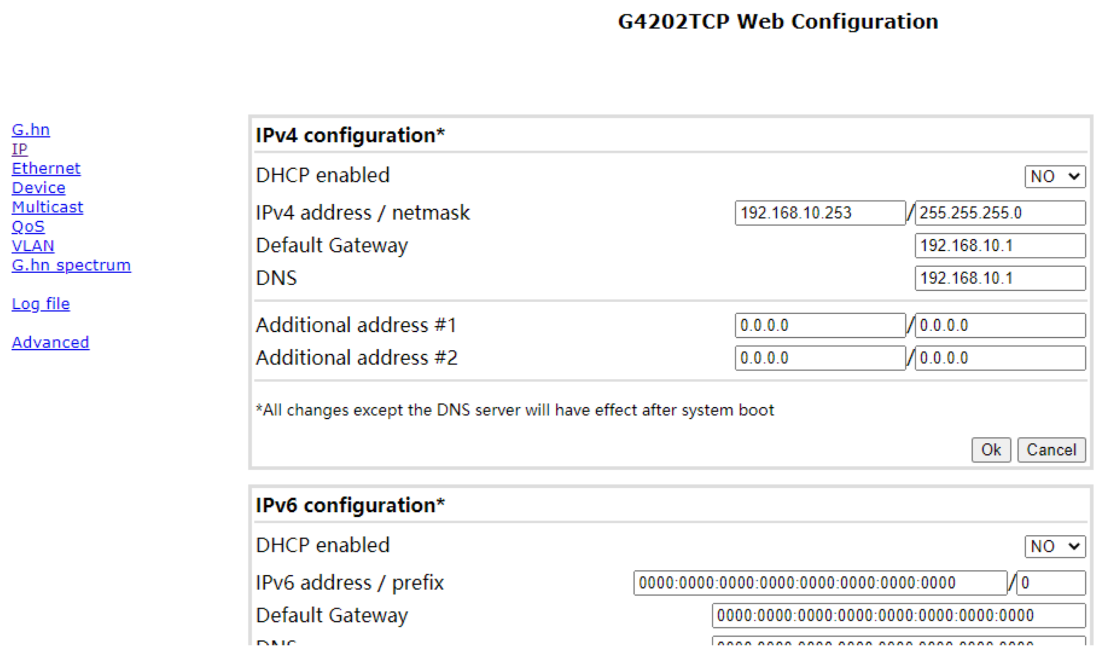
Neighboring Domain Interference Mitigation (NDIM)

•NDIM mode MANUAL

•Domain ID (DOD) 0

4.2 IP

The switch supports IPV4 and IPV6. DHCPV4/DHCPV6 can be enabled by selecting “YES”, the switch gets IP address from DHCP server. If static IP is used by selecting “NO”, IP Address, Subnet Mask, and Gateway IP address shall be specified, after clicking <OK>, you will be asked to re-login with the new IP.



G4202TCP Web Configuration

IPv4 configuration*

DHCP enabled	NO
IPv4 address / netmask	192.168.10.253 / 255.255.255.0
Default Gateway	192.168.10.1
DNS	192.168.10.1
Additional address #1	0.0.0.0 / 0.0.0.0
Additional address #2	0.0.0.0 / 0.0.0.0

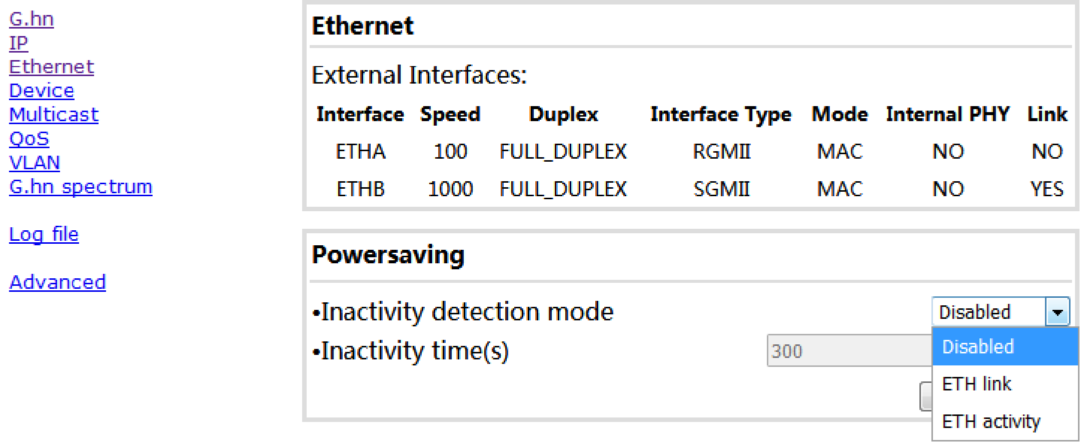
*All changes except the DNS server will have effect after system boot

IPv6 configuration*

DHCP enabled	NO
IPv6 address / prefix	0000:0000:0000:0000:0000:0000:0000:0000 / 0
Default Gateway	0000:0000:0000:0000:0000:0000:0000:0000

4.3 Ethernet

The Ethernet page is shown as below.



Ethernet

External Interfaces:

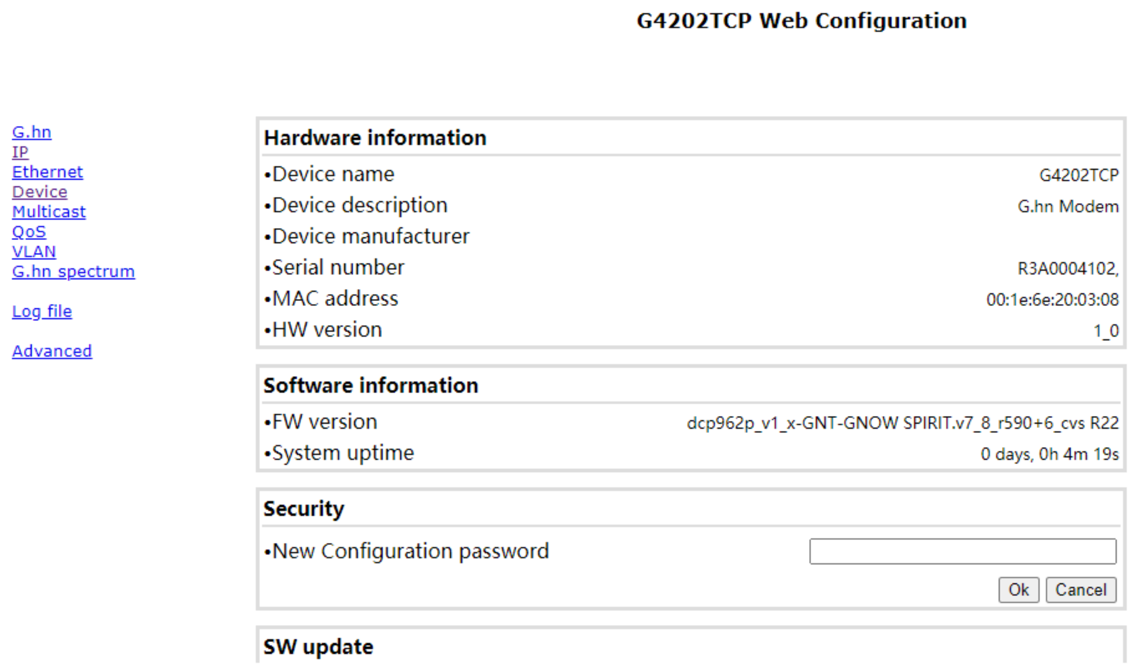
Interface	Speed	Duplex	Interface Type	Mode	Internal PHY	Link
ETHA	100	FULL_DUPLEX	RGMII	MAC	NO	NO
ETHB	1000	FULL_DUPLEX	SGMII	MAC	NO	YES

Powersaving

- Inactivity detection mode: Disabled
- Inactivity time(s): 300

4.4 Device

You can see the hardware information and software information of the system, the page is shown as below.



G4202TCP Web Configuration

Hardware information

•Device name	G4202TCP
•Device description	G.hn Modem
•Device manufacturer	
•Serial number	R3A0004102,
•MAC address	00:1e:6e:20:03:08
•HW version	1_0

Software information

•FW version	dcp962p_v1_x-GNT-GNOW SPIRIT.v7_8_r590+6_cvs R22
•System uptime	0 days, 0h 4m 19s

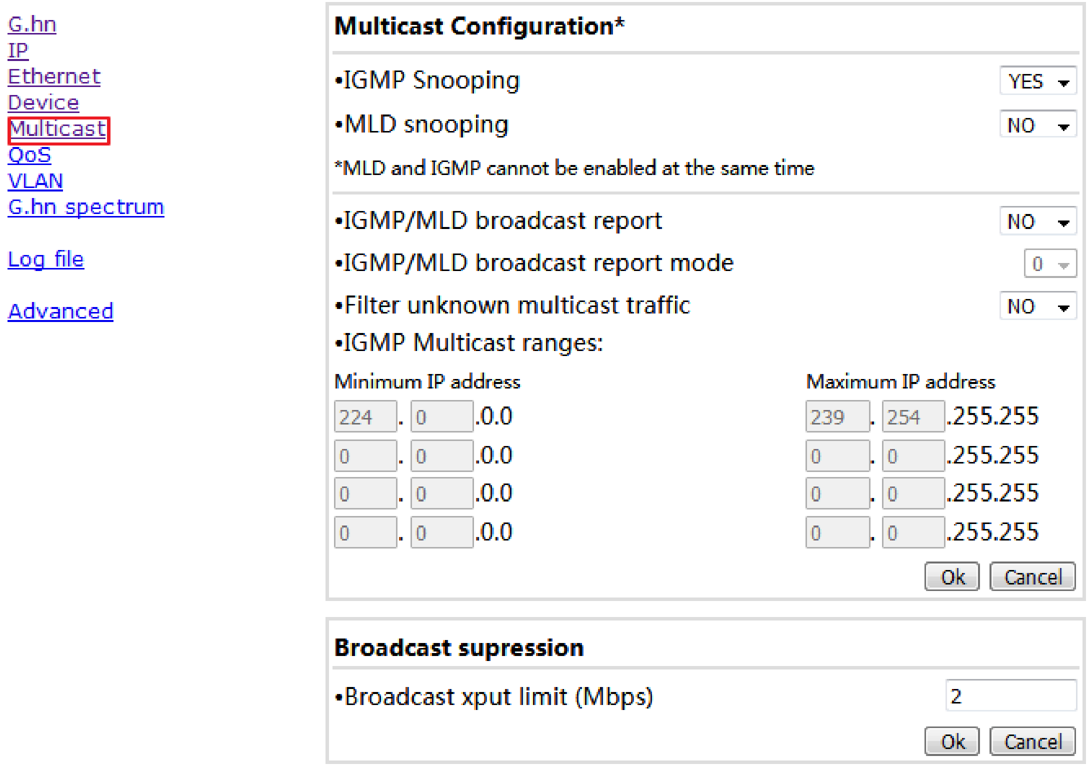
Security

•New Configuration password

SW update

4.5 Multicast

This page is shown as below.



Multicast Configuration*

- IGMP Snooping: YES
- MLD snooping: NO

*MLD and IGMP cannot be enabled at the same time

- IGMP/MLD broadcast report: NO
- IGMP/MLD broadcast report mode: 0
- Filter unknown multicast traffic: NO
- IGMP Multicast ranges:

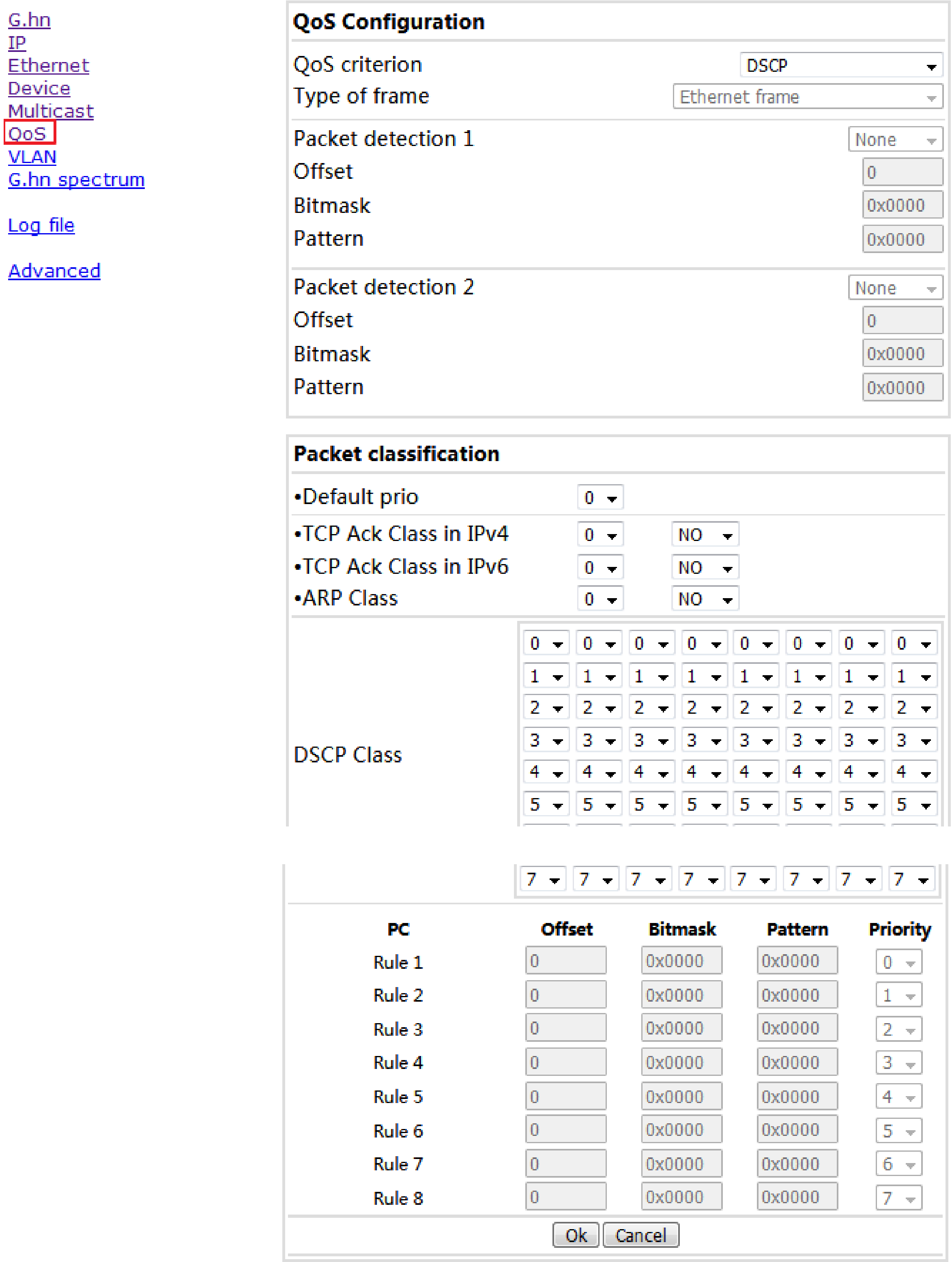
Minimum IP address	Maximum IP address
224 . 0 .0.0	239 . 254 .255.255
0 . 0 .0.0	0 . 0 .255.255
0 . 0 .0.0	0 . 0 .255.255
0 . 0 .0.0	0 . 0 .255.255

Broadcast supression

- Broadcast xput limit (Mbps): 2

4.6 Qos

This tab page sets QoS parameters of each port, the page is shown as below.



QoS Configuration

QoS criterion	DSCP
Type of frame	Ethernet frame
Packet detection 1	None
Offset	0
Bitmask	0x0000
Pattern	0x0000
Packet detection 2	None
Offset	0
Bitmask	0x0000
Pattern	0x0000

Packet classification

•Default prio	0	
•TCP Ack Class in IPv4	0	NO
•TCP Ack Class in IPv6	0	NO
•ARP Class	0	NO

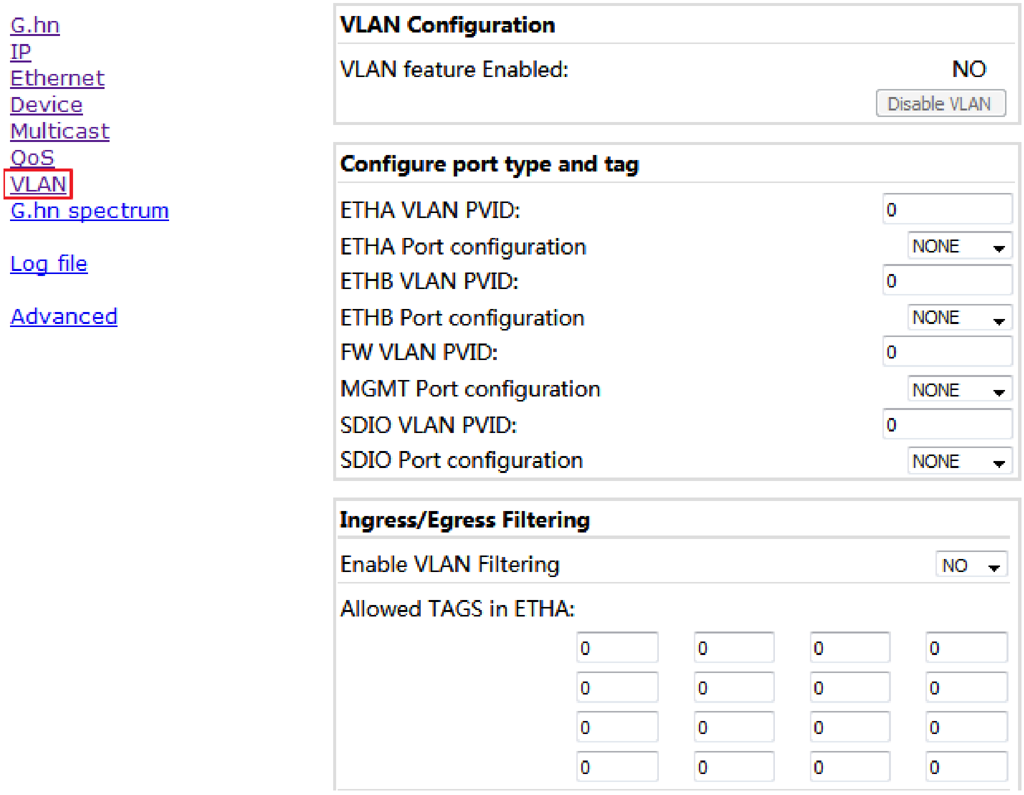
DSCP Class

0	0	0	0	0	0	0	0
1	1	1	1	1	1	1	1
2	2	2	2	2	2	2	2
3	3	3	3	3	3	3	3
4	4	4	4	4	4	4	4
5	5	5	5	5	5	5	5
7	7	7	7	7	7	7	7

PC	Offset	Bitmask	Pattern	Priority
Rule 1	0	0x0000	0x0000	0
Rule 2	0	0x0000	0x0000	1
Rule 3	0	0x0000	0x0000	2
Rule 4	0	0x0000	0x0000	3
Rule 5	0	0x0000	0x0000	4
Rule 6	0	0x0000	0x0000	5
Rule 7	0	0x0000	0x0000	6
Rule 8	0	0x0000	0x0000	7

4.7 VLAN

You can set VLAN parameters by enabling the VLAN function.



VLAN Configuration

VLAN feature Enabled: NO

Configure port type and tag

ETHA VLAN PVID: 0

ETHA Port configuration: NONE

ETHB VLAN PVID: 0

ETHB Port configuration: NONE

FW VLAN PVID: 0

MGMT Port configuration: NONE

SDIO VLAN PVID: 0

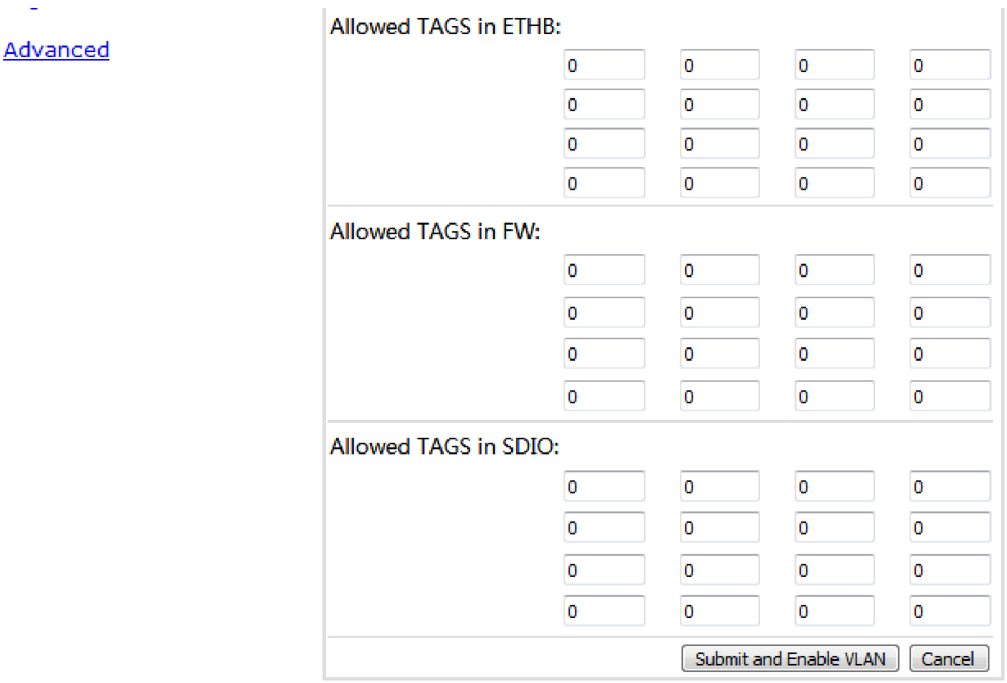
SDIO Port configuration: NONE

Ingress/Egress Filtering

Enable VLAN Filtering: NO

Allowed TAGS in ETHA:

0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	0



Allowed TAGS in ETHB:

0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	0

Allowed TAGS in FW:

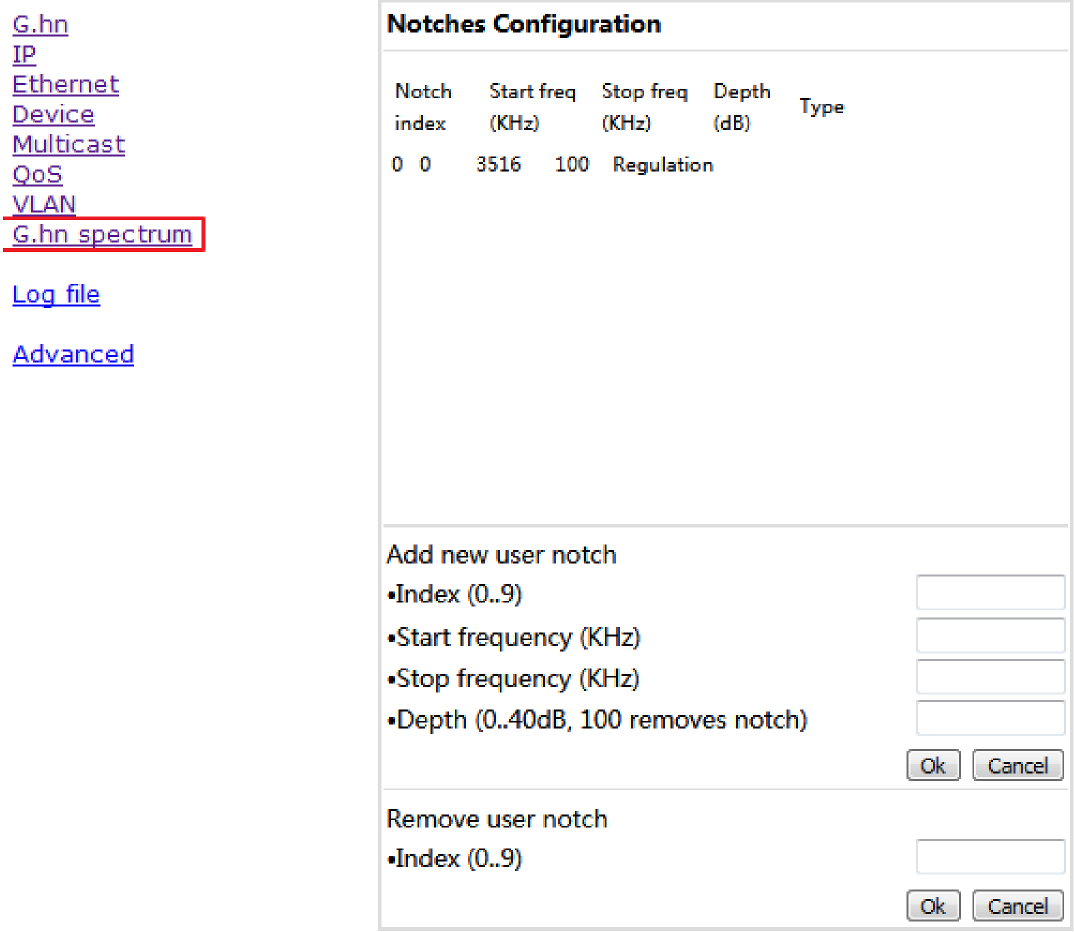
0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	0

Allowed TAGS in SDIO:

0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	0

4.8 G.hn spectrum

You can see detailed information of notch and add new user notch on this page.



Notches Configuration

Notch index	Start freq (KHz)	Stop freq (KHz)	Depth (dB)	Type
0	0	3516	100	Regulation

Add new user notch

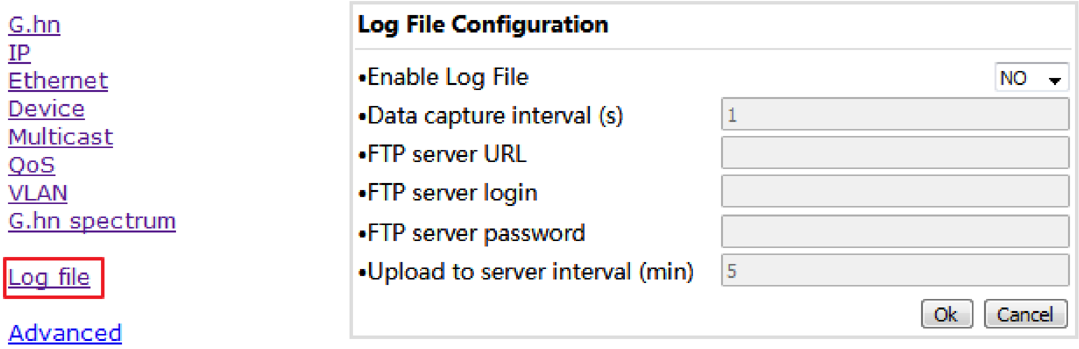
•Index (0..9)	
•Start frequency (KHz)	
•Stop frequency (KHz)	
•Depth (0..40dB, 100 removes notch)	

Remove user notch

•Index (0..9)	

4.9 Log file

This page is shown as below.

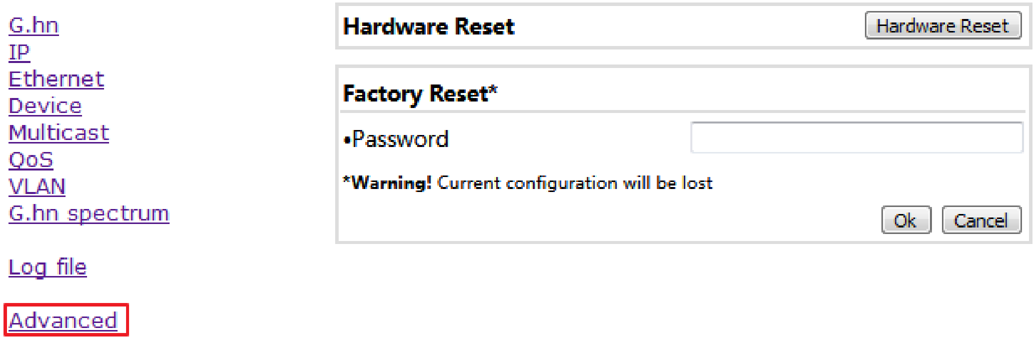


Log File Configuration

•Enable Log File	NO
•Data capture interval (s)	1
•FTP server URL	
•FTP server login	
•FTP server password	
•Upload to server interval (min)	5

4.10 Advanced

On this page, you can set the password for login system before restoring factory default settings.



*Warning! Current configuration will be lost

5. Appendix

5.1 Appendix A: G4224 Performance

Test condition

Items	Description
UTP Cable	0.5mm 25pair F/S cable
Coaxial Cable	SYV 75-4 100m, SYV 75-5 200m
Test Tool	Big Tao 200 Tester

Performance

Table1: Performance and PoE output capability test results in different coaxial cable length

Coaxial Performance	Distance(m)	Throughput (Download/Upload): Mb/s Package Length:512Bytes		802.3af/at/bt PoE Output Capability	
		Remote power through F-type coax connector	Local DC power through USB Type-C connector	Remote power through F-type coax connector	Local DC power through USB Type-C connector
	1	990/440	990/440	30w	30w
	100	990/440	990/430	30W	30w
	200	860/390	740/320	18W	30w
	300	560/290	540/270	11W	30w
	400	370/220	220/140	9W	30w

	500	170/130	160/130	7W	30w

Table2: Performance and PoE output capability test results in different UTP cable length (MIMO mode)

UTP Performance(MIMO)	Distance(m)	Throughput (Download/Upload): Mb/s Package Length:512Bytes		802.3af/at/bt PoE Output Capability	
		Remote power through UTP connector	Local DC power through USB Type-C connector	Remote power through UTP connector	Local DC power through USB Type-C connector
	1	990/440	990/440	30w	30w
	100	990/440	990/440	30w	30w
	200	980/410	980/410	21w	30w
	300	760/250	740/190	13w	30w
	400	500/150	490/140	9w	30w
	500	310/80	300/80	6w	30w
	600	210/40	200/40	4w	30w

Table3: Performance and PoE output capability test results in different UTP cable length (SISO mode)

UTP Performance(SISO)	Distance(m)	Throughput(Download/Upload): Mb/s Package Length:512Bytes		802.3af/at/bt PoE Output Capability	
		Remote power through UTP connector	Local DC power through USB Type-C connector	Remote power through UTP connector	Local DC power through USB Type-C connector

	1	990/450	990/450	30w	30w
	100	990/430	990/430	18w	30w
	200	650/250	630/250	9w	30w
	300	270/130	250/130	5w	30w
	400		140/80		30w
	500		80/50		30w
	600		40/30		30w

The above performance results is measured on Ghn11/Ghn12 or Ghn23/Ghn24 of the G4224 which support 802.3bt PoE output, also the G4202TCP support 802.3bt PoE input.

Note: The actual data rate will vary on the quality of the copper wire or UTP cable and environment factors.

Depending on what the DC/PoE Power Input and the length of coaxial/UTP cable

5.2 Appendix B: RJ45 Pin Assignments

RJ45 Pin Assignments	
Contact	POE
1	Positive(VCC+)
2	Positive(VCC+)
3	Positive(VCC+)
4	Positive(VCC+)
5	Negative(VCC-)
6	Negative(VCC-)
7	Negative(VCC-)
8	Negative(VCC-)