



Grandstream Networks, Inc.

GWN780x Series

GWN7806(P) – User Manual



WELCOME

The GWN7806(P) is a layer 2+ managed switch that allows small-to-medium enterprises to build scalable, secure, high-performance and smart business networks that are fully manageable. It supports advanced VLAN for flexible and sophisticated traffic segmentation, advanced QoS for prioritization of network traffic, IGMP/MLD Snooping for network performance optimization, and comprehensive security capabilities against potential attacks. The GWN7806P provides smart dynamic PoE output to power IP phones, IP cameras, Wi-Fi access points and other PoE endpoints. GWN7806(P) is easy to deploy and manage, including managed by the local Web user interface of the GWN7806(P) switch and CLI, the command-line interface. The switch is also supported by GWN.Cloud and GWN Manager, Grandstream's cloud and on-premise network management platform. The GWN7806(P) is the best value enterprise-grade managed network switch for small-to-medium businesses.

PRODUCT OVERVIEW

Technical Specifications

	GWN7806	GWN7806(P)
Network Protocol	IPv4, IPv6, IEEE 802.3, IEEE 802.3i, IEEE 802.3u, IEEE 802.3ab, IEEE 802.3z, IEEE 802.3ae, IEEE 802.3az, IEEE 802.3ad, IEEE 802.3x, IEEE 802.3af/at, IEEE 802.1p, IEEE 802.1Q, IEEE 802.3AB, IEEE 802.1p, IEEE 802.1D, IEEE 802.1s, IEEE 802.1w, IEEE 802.1x	
Gigabit Ethernet Ports	48	
Gigabit SFP+ Ports	6	
Console	1	
Number of PoE Ports	/	48
Integrated Power Supply	60W	460W
Max Output Power per PoE Port	/	30W
Max Total PoE Output Power	/	400W
PoE Standards	/	IEEE 802.3af/at
Auxiliary Ports	1x Reset Pinhole	
Forwarding Mode	Store-and-forward	
Total non-blocking throughput	120Gbps	

Switching Capability	240Gbps
Forwarding Rate	80.352Mpps
Packet Buffer	16MB
Switching	<ul style="list-style-type: none"> ● 32K static, dynamic and filtering MAC addresses ● 4K VLANs, port-based VLAN, IEEE 802.1Q VLAN tagging, voice VLAN ● VLAN virtual interface ● GVRP (pending) ● 8 link aggregation groups ● Spanning tree, 16 instances for STP/RTSP/MSTP
Routing	<ul style="list-style-type: none"> ● Static routing
Multicast	<ul style="list-style-type: none"> ● IGMP Snooping ● MLD Snooping ● MVR (pending)
QoS/ACL	<ul style="list-style-type: none"> ● Port priority ● Priority mapping ● Queue scheduling, including SP, WRR, WFQ, SP-WRR, and SP-WFQ ● Traffic shaping ● Rate limit ● 42K ACL for Ethernet, IPv4 and IPv6
DHCP	DHCP Server, DHCP Relay, Option 82, 60,160, and 43
Maintenance	CPU and memory monitoring, SNMP, RMON, LLDP&LLDP-MED, backup and restore, syslog, diagnostics including Ping, Traceroute, port mirroring and copper test
Security	<ul style="list-style-type: none"> ● User hierarchical management and password protection, HTTPS, SSH, Telnet ● 802.1X authentication ● AAA authentication including RADIUS, TACACS+ ● Storm control ● Port isolation, port security, sticky MAC ● Filtering MAC address ● IP source guard, DoS attack prevention, ARP inspection ● DHCP Snooping ● Loop protection including BPDU protection, root protection (pending), and loopback protection (pending) ● Kensington Security Slot (Kensington Lock) support
Mounting	Desktop/ Wall-Mount Desktop, wall-mount, or rack-mount (rack-mount brackets included)
System LEDs	1x tri-color LED for device tracking and status indication
Fan	3
Environmental	Operation: 0°C to 45°C, humidity 10-90% RH (Non-condensing) Storage: -10°C to 60°C, humidity: 10% to 90% (Non-condensing)

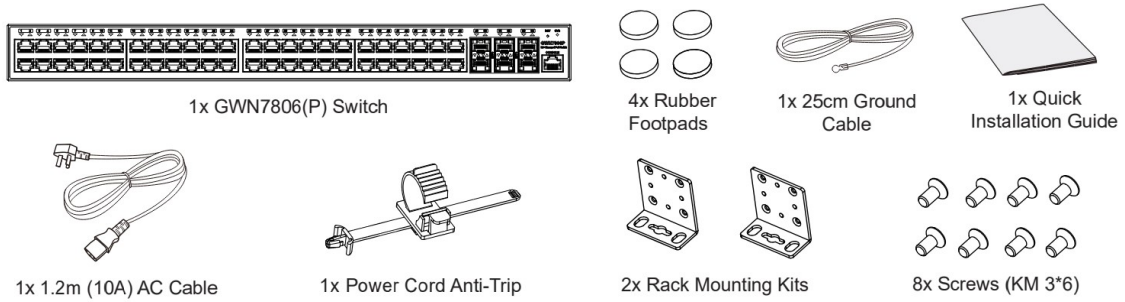
Dimensions	440mm(L)x301mm(W)x44mm(H)
Compliance	FCC, CE, RCM, IC, UKCA

Technical Specifications

INSTALLATION

Before deploying and configuring a GWN7806(P) switch, the device needs to be properly powered up and connected to the network. This section describes detailed information on the installation, connection, and warranty policy of the GWN7806(P) switch.

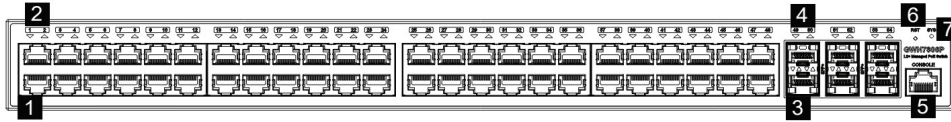
Package Content



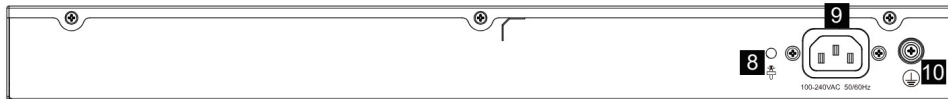
GWN7806(P) Package Contents

GWN7806(P) Ports

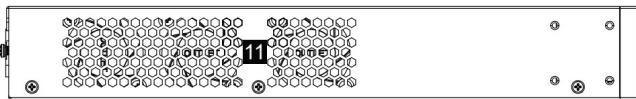
Front Panel



Back Panel





Side Panel



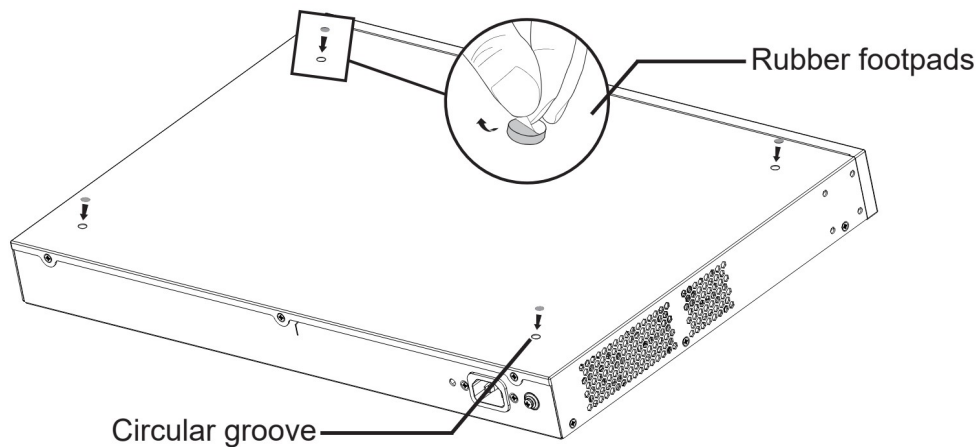
GWN7806(P) Ports

No.	Port & LED	Description
1	Port 1-48	48x Ethernet RJ45(10/100/1000Mbps), used for connecting terminals <i>Note:</i> GWN7806P Ethernet ports support PoE/PoE+
2	1-48	Ethernet ports' LED indicators
3	Port SFP+ 49-54	6x 10Gbps SFP+ ports
4	SFP+ 49-54	SFP+ ports' LED indicators

5	Console	1x Console port, used to connect a PC directly to the switch and manage it
6	RST	Factory Reset pinhole. Press for 5 seconds to reset the factory default settings
7	SYS	System LED indicator
8		Power cord anti-trip hole
9	100-240 VAC 50-60Hz	Power socket
10		Grounding terminal
11	Fan	3x Fans

GWN7806(P) Ports

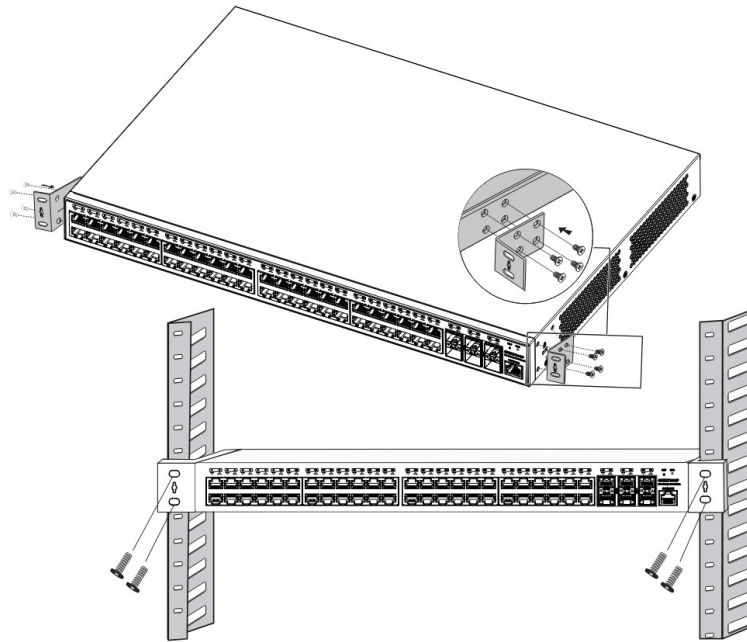
Install on the Desktop



GWN7806(P) Desktop Installation

1. Place the bottom of switch on a sufficiently large and stable table.
2. Peel off the rubber protective paper of the four footpads one by one, and stick them in the corresponding circular grooves at the four corners of the bottom of the case.
3. Flip the switch over and place it smoothly on the table.

Install on 19" Standard Rack

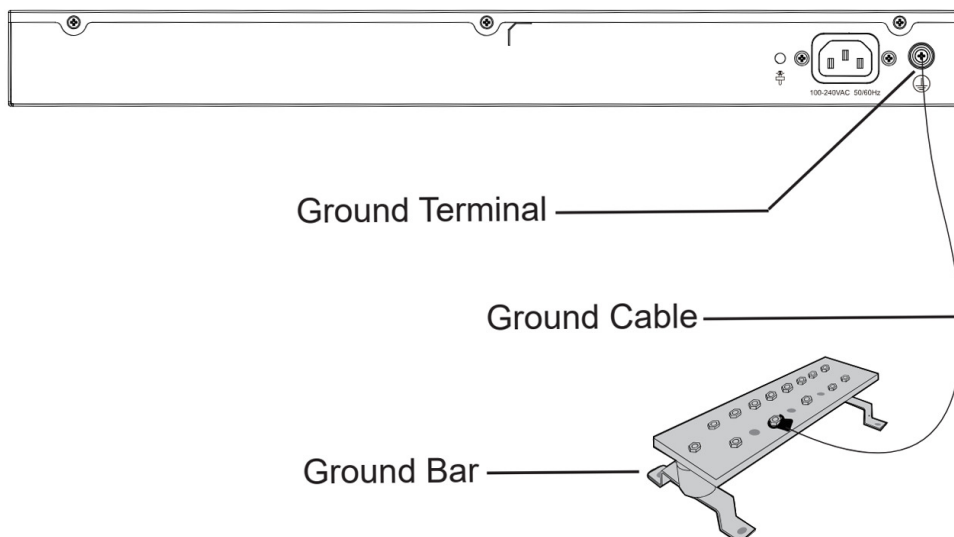


GWN7806(P) L-shaped rack-mounting Installation

1. Check the grounding and stability of the rack.
2. Install the two L-shaped rack-mounting in the accessories on both sides of switch, and fix them with the screws provided (KM 3*6).
3. Place the switch in a proper position in the rack and support it by the bracket.
4. Fix the L-shaped rack-mounting to the guide grooves at both ends of the rack with screws (prepared by yourself) to ensure that the switch is stably and horizontally installed on the rack.

Powering and Connecting GWN7806(P)

○ Grounding the Switch

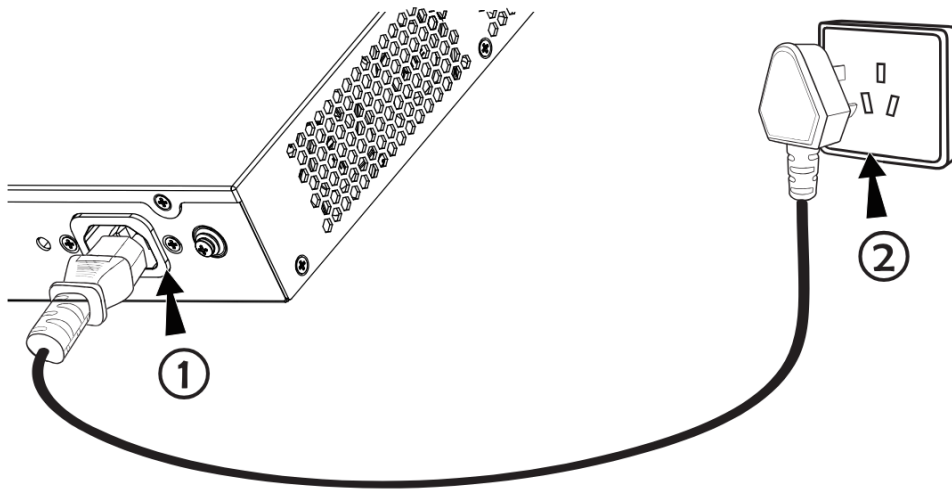


Grounding the Switch

1. Remove the ground screw from the back of switch, and connect one end of the ground cable to the wiring terminal of switch.
2. Put the ground screw back into the screw hole, and tighten it with a screwdriver.
3. Connect the other end of the ground cable to other device that has been grounded or directly to the terminal of the ground bar in the equipment room.

○ Powering on the Switch

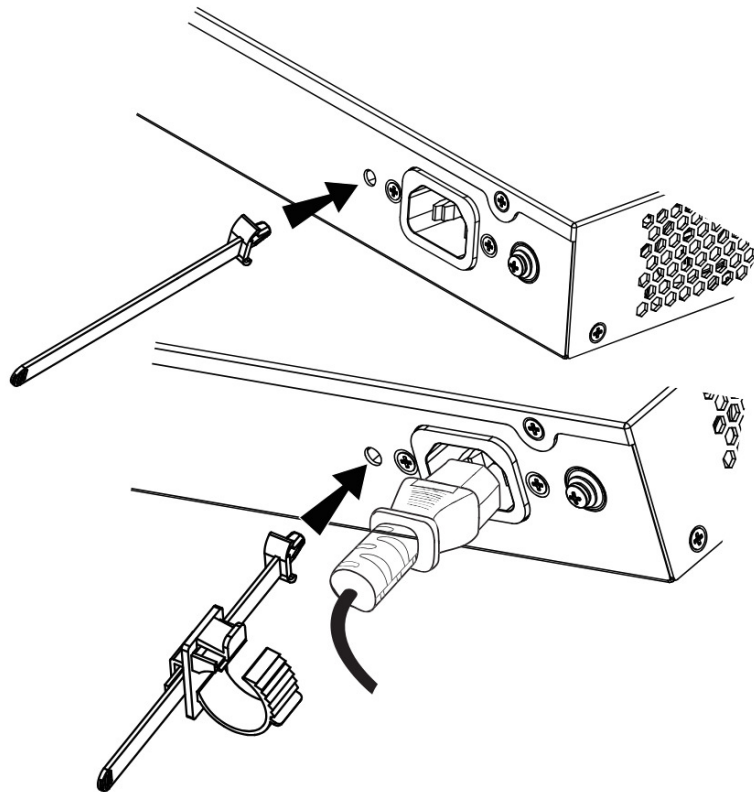
Connect the power cable and the switch first, then connect the power cable to the power supply system of the equipment room.



Powering on the Switch

○ **Connecting Power Cord Anti-trip**

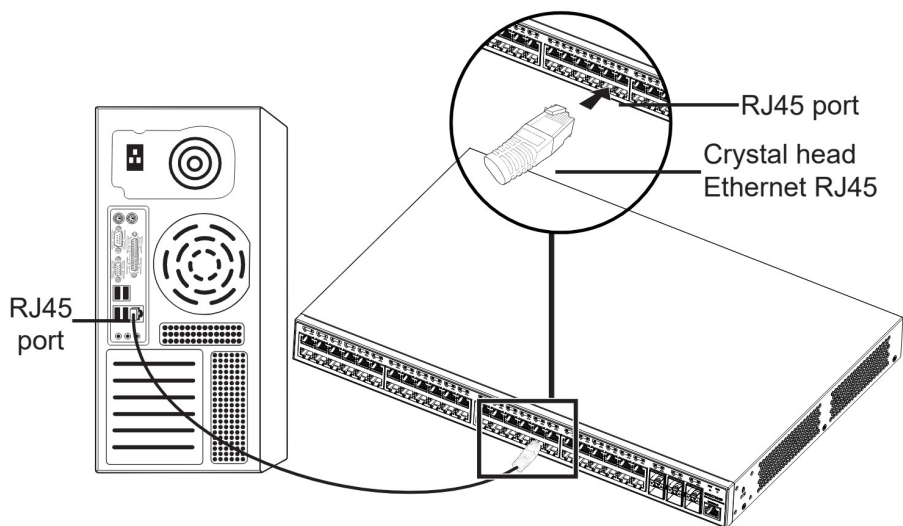
In order to protect the power supply from accidental disconnection, it's recommended to purchase a power cord anti-trip for installation.



Connecting Power Cord Anti-Trip

1. Place the smooth side of the fixing strap towards the power outlet and insert it into the hole on the side of it.
2. After plugging the power cord into the power outlet, slide the protector over the remaining strap until it slides over the end of the power cord.
3. Wrap the strap of the protective cord around the power cord and lock it tightly. Fasten the straps until the power cord is securely fastened.

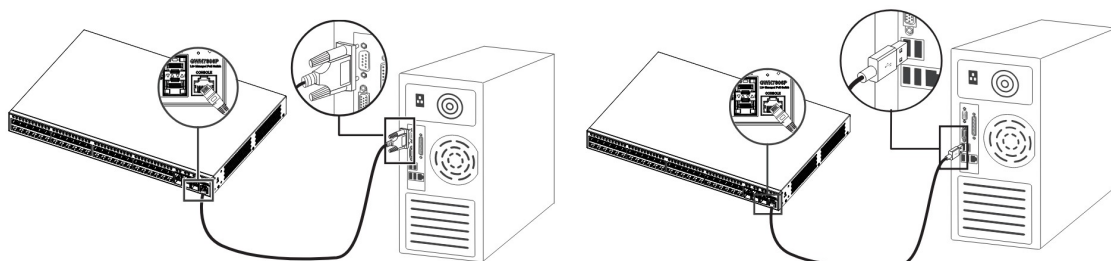
○ **Connect to RJ45 Port**



Connect to RJ45 Port

1. Connect one end of the network cable to the switch, and the other end to the peer device.
2. After powered on, check the status of the port indicator. If on, it means that the link is connected normally; if off, it means the link is disconnected, please check the cable and the peer device whether is enabled.

o **Connect to Console Port**



Connect to Console Port

1. Connect the RJ45 end of the console cable to the console port of switch.
2. Connect the other end of the console cable to the DB9 male connector or USB port to the PC.

Safety Compliances

The GWN7806(P) L3 Managed Network Switch complies with FCC/CE and various safety standards. The GWN7806(P) power adapter is compliant with the UL standard. Use the universal power adapter provided with the GWN7806(P) package only. The manufacturer’s warranty does not cover damages to the device caused by unsupported power adapters.

Warranty

If GWN7806(P) L3 Managed Network Switch was purchased from a reseller, please contact the company where the device was purchased for replacement, repair or refund. If the device was purchased directly from Grandstream, contact our Technical Support Team for an RMA (Return Materials Authorization) number before the product is returned. Grandstream reserves the right to remedy the warranty policy without prior notification.

GETTING STARTED

LED Indicators

The front panel of the GWN7806(P) has LED indicators for power and interface activities, the table below describes the LED indicators’ status.

LED Indicator	Status	Description
---------------	--------	-------------

System Indicator	Off	Power off
	Solid green	Booting
	Flashing green	Upgrade
	Solid blue	Normal use
	Flashing blue	Provisioning
	Solid red	Upgrade failed
	Flashing red	Factory reset
Port Indicator	Off	<ul style="list-style-type: none"> • For all ports: port off • For SFP ports: port failure
	Solid green	Port connected and there is no activity
	Flashing green	Port connected and data is transferring
	Solid yellow	Ethernet port connected, and there is no activity and PoE powered
	Flashing yellow	Ethernet port connected, data is transferring and PoE powered
	Alternately flashing yellow and green	Ethernet port failure

LED Indicators

Access & Configure

Note

If no DHCP server is available, the GWN7806(P) default IP address is 192.168.0.254.

Login Using the Console Port

1. Use the console cable to connect the console port of switch and the serial port of PC.
2. Open the terminal emulation program of PC (e.g. SecureCRT), enter the default username and password to login. (The default administrator username is "admin" and the default random password can be found at the sticker on the GWN7806(P) switch).

Note

The baud rate needs to be set to 115200.

Login Remotely Using SSH

1. Enter "**cmd**" in PC/Start.
2. Enter **ssh <gwn7806(P)_IP>** in the cmd window.

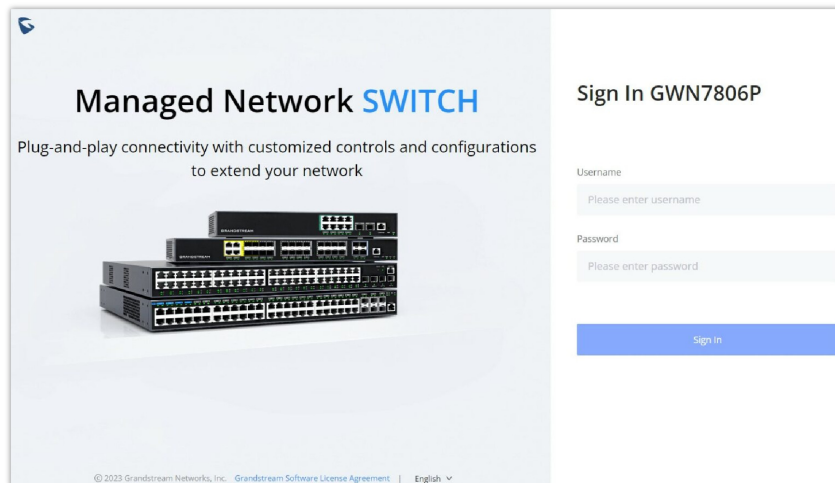
3. Enter the default username and password to login. (The default administrator username is "admin" and the default random password can be found at the sticker on the GWN7806(P) switch).

Configure Using GWN Cloud

Type <https://www.gwn.cloud> in the browser, and enter the account and password to login the cloud platform. If you don't have an account, please register first or ask the administrator to assign one for you.

Login Using the Web UI

The GWN7806(P) embedded Web server responds to HTTPS GET/POST requests. Embedded HTML pages allow users to configure the device through a Web browser such as Microsoft Edge, Mozilla Firefox, or Google Chrome.



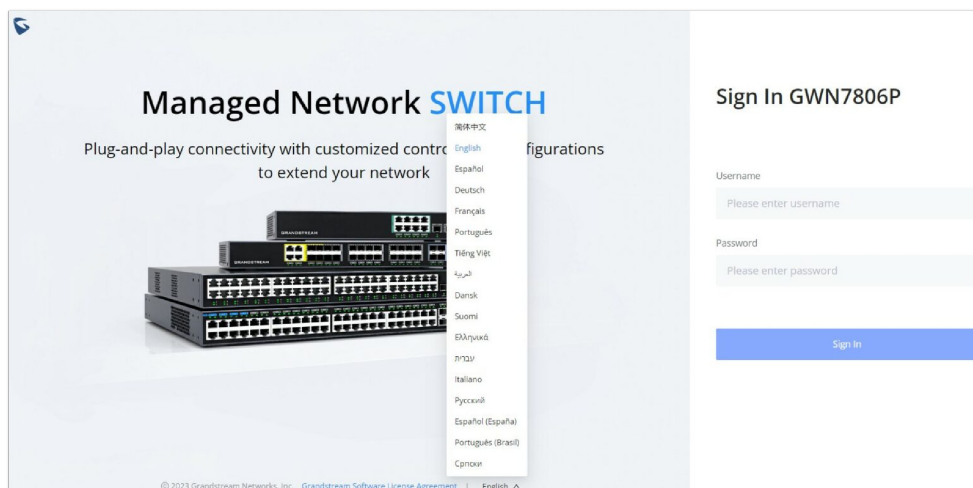
GWN7806(P) WEB GUI Page

1. A PC uses a network cable to correctly connect any RJ45 port of the switch.
2. Set the Ethernet (or local connection) IP address of the PC to 192.168.0.x ("x" is any value between 1-253), and the subnet mask to 255.255.255.0, so that it is in the same network segment with switch IP address. If DHCP is used, this step could be skipped.
3. Type the switch's default management IP address [http://<GWN7806\(P\)_IP>](http://<GWN7806(P)_IP>) in the browser, and enter username and password to login. (The default administrator username is "admin" and the default random password can be found at the sticker on the GWN7806(P) switch).

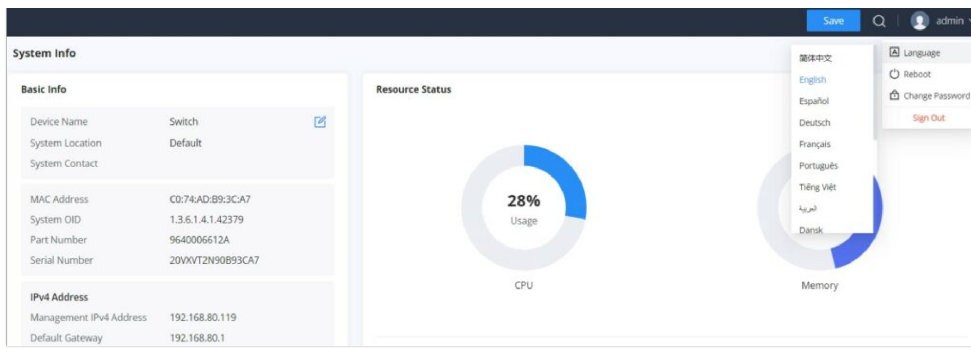
Web GUI Languages

The GWN7806(P) web GUI supports many languages including **English, Simplified Chinese, Spanish, French** etc.

To change the default language, select the displayed language at the bottom of the web GUI either before or after logging in.



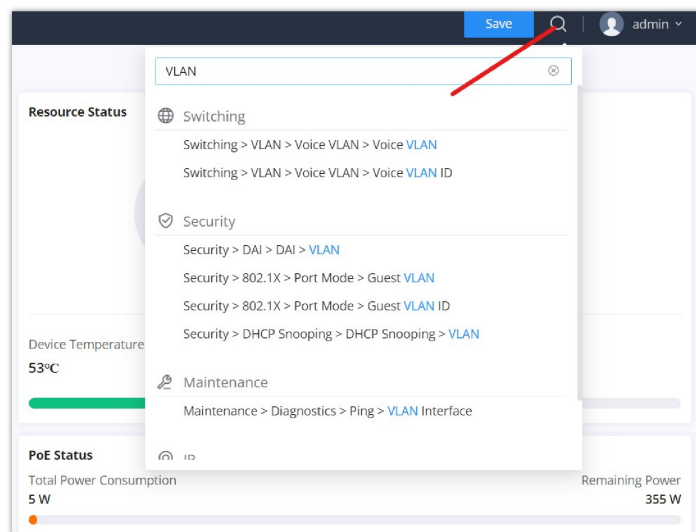
Web GUI Languages – Login Page



WEB GUI – Start page

Search

The web GUI of the GWN7806(P) switches provide a search tool to find the parameters quickly. To search for a specific parameter, please click on the magnifier icon on the top right corner of the web page.



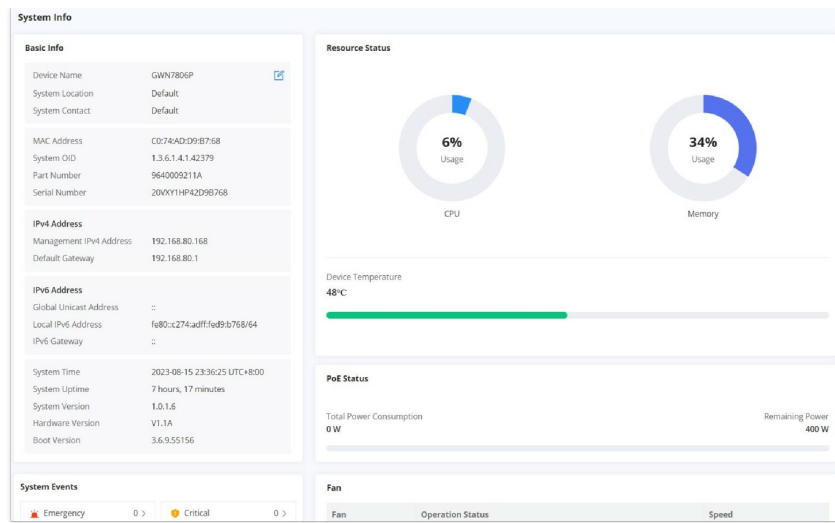
Search

OVERVIEW


Overview is the first section that displays System information in the first page “**System Info**” and Port status on the second page “**Port Info**”. This section provides the user with a general and global view about the GWN7806(P) system and ports status for easy monitoring.

System Info

System Info is the first page after a successful login to the GWN7806(P) Web Interface. It provides an overall view of the GWN7806(P) Switch information presented in a Dashboard style for easy monitoring including basic info, Resources Status, PoE Status and System Events.



System Info page

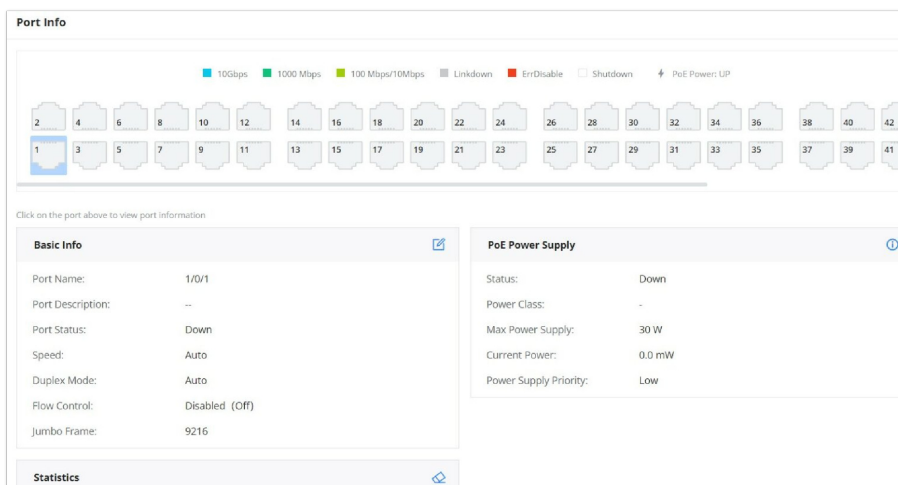
To name the device please click on , then enter the desired name.

Basic Info	Displays Device and System general information that includes (Device name, MAC Address, Default Gateway, System Time, System Version etc.)
Resource Status	Displays in real time the usage of CPU and Memory.
PoE Status	Shows the Total Power Consumption and the remaining Power in mA.
System Events	Displays the total number of events for each category (Emergency, Alert, Warning etc). <i>Note: Clicking on any events category will redirect you to the Diagnostics page for further details.</i>
Fan	Displays the fans operation status and speed.

System Info page


Port Info


This page displays the status for each port on the GWN7806(P) switches indicated by color code, in terms of connection (Up, Linkdown or Shutdown), and also in terms of PoE (Up, Disabled, Current Power, priority etc).



Port Info page




The following table explained the color mode and the symbols used:

	Ethernet Port is Down, PoE is Disabled.
---	---

	Ethernet Port is Shutdown.
	SFP Port is Down.
	Ethernet Port is Up and 1000 Mbps, PoE is Disabled
	Ethernet Port is Up and 100/10 Mbps, PoE is Enabled
	Ethernet Port is ErrDisable.
	PoE Power is enabled.

Port Info

There are 3 main sections for each port:

- Basic Port:** Displays info about the port name, speed, status etc.
Note: Click on  to modify the port settings like *Description*, *Speed*, *Duplex Mode* and *Flow Control* or to *enable* or *disable* the port.
- PoE Power Supply:** Displays *PoE Current Power* and *Priority*, *Status* etc.
Note: Click  on to change PoE settings.
- Statistics:** Displays Statistics about Octets, and different types of Packets (Broadcast and Multicast, etc.)
Note: Click  on to clear the statistics










SWITCHING

Switching section is used to configure ports settings, link Aggregation, VLAN, Spanning Tree etc.

Port Basic Settings

On this page, you can configure the basic parameters for GWN7806(P) Switch ports, like disabling or enabling the port, adding Description, specifying the speed by default is Auto, Duplex Mode, and Flow Control. There is also a filter on in case you want to edit only the Copper ports which are the Gigabit Ethernet ports or Fiber ports which are the SFP+ ports.

To configure a port, please navigate to **Web UI** → **Switching** → **Port Basic Settings**.

Port Basic Settings							
Port	Port Type	Description	Status	Link Status	Speed		
<input checked="" type="checkbox"/>	1/0/1	Copper	GWN76xx	Enabled	Down	Auto	
<input checked="" type="checkbox"/>	1/0/2	Copper	Guests	Enabled	Down	Auto	
<input checked="" type="checkbox"/>	1/0/3	Copper	--	Enabled	Down	Auto	
<input checked="" type="checkbox"/>	1/0/4	Copper	--	Enabled	Down	Auto	
<input checked="" type="checkbox"/>	1/0/5	Copper	--	Enabled	Down	Auto	
<input checked="" type="checkbox"/>	1/0/6	Copper	--	Enabled	Down	Auto	
<input checked="" type="checkbox"/>	1/0/7	Copper	--	Enabled	Down	Auto	
<input checked="" type="checkbox"/>	1/0/8	Copper	--	Enabled	Down	Auto	
<input checked="" type="checkbox"/>	1/0/9	Copper	--	Enabled	Down	Auto	

Port Basic Settings

To configure a port, click on **"Edit"** icon under operation column.

Port Basic Settings – Edit port

Port	The selected Port to be configured, it can be either Gigabit Ethernet port or SFP port.
Port Type	Displays the Port Type (Copper or SFP+).
Description	It is used to configure the information description of this interface , which can be a description of usage, etc., with a maximum of 128 characters, and the characters limited to input are numbers 0-9 , letters az / AZ and special characters.
Port Enable	Set whether to enable the interface. <i>it is enabled by default.</i>
Speed	Set the rate of the interface, the options are {Auto, 10Mbps, 100Mbps, 1000Mbps}. <i>The default is auto-negotiation.</i> Note: When set to Auto, the rate of the interface is automatically negotiated between the interface and the peer port .
Only available for SFP+ Ports	
<p>Auto Detect: toggle ON or OFF Auto Detect, if it's ON the speed and DAC cable will be selected automatically, and if it's OFF the user can select speed and DAC Cable manually.</p> <p>Speed: select from the drop-down list the speed for the SFP+ port (100Mbps, 1000 Mbps or 10Gbps)</p> <p>DAC Cable: select from the drop-down list the DAC Cable, the options are (Disable, 0.5m, 1m, 3m, 5m)</p>	
Duplex Mode	<p>Set the duplex mode of the interface. The GE ports options are { auto-negotiation, full-duplex, half-duplex}. <i>The default is auto-negotiation.</i></p> <p>Note: Optical ports only support full-duplex mode.</p> <ul style="list-style-type: none"> ● Auto-negotiation: The duplex state of an interface is determined by the auto-negotiation between the interface and the peer port. ● Duplex: the interface send and receive data packets. ● Half-duplex: interface can only send/ receive packets.
Jumbo Frame	Specify the Jumbo Frame, the valid range is 1518-10000.
Flow Control	Set the flow control on the interface, the options are {Disabled, Enabled, Auto} . <i>The default is Disabled.</i> After enabling it, if the local device is congested, it will send a message to the peer device to notify the peer device to temporarily stop sending packets, after receiving the message, the peer device will temporarily stop sending

packets to the local and vice versa. Thus, the occurrence of packet loss is avoided.

Note: The optical port does not support auto-negotiation mode.

Port Basic Settings – Edit port

Flow Statistics

For monitoring or even sometimes troubleshooting, the Flow Statistics displays in real time the flow of data with different units like Octets, Packets, Transmission Rate and OutErrPackets. The option to clear all the statistics or a specific port is supported as well.

Port	Receive Rate (bps)	InOctets	InPackets	InErrPackets	Transmit Rate (bps)	OutOctets	OutPackets	OutErrPackets	Operation
1/0/1	--	--	--	--	--	--	--	--	🔄
1/0/2	--	--	--	--	--	--	--	--	🔄
1/0/3	--	--	--	--	--	--	--	--	🔄
1/0/4	--	--	--	--	--	--	--	--	🔄
1/0/5	--	--	--	--	--	--	--	--	🔄
1/0/6	--	--	--	--	--	--	--	--	🔄
1/0/7	--	--	--	--	--	--	--	--	🔄
1/0/8	--	--	--	--	--	--	--	--	🔄
1/0/9	--	--	--	--	--	--	--	--	🔄
1/0/10	--	--	--	--	--	--	--	--	🔄
1/0/11	--	--	--	--	--	--	--	--	🔄

Flow Statistics

Port Auto Recovery

Port Auto Recovery helps recover a port after a specific delay that can be specified by the user. When the following functions of the port trigger the port down, the port automatically returns to the up state after the delay time:

Examples:

- **ARP packet detection:** If the ARP rate in DAI exceeds the set value, the current port will be shut down.
- **STP BPDU Guard:** In spanning tree, the port enables BPDU Guard. When this function is triggered, the port will be shut down.
- **Port Loop:** When the port is self-looping and spanning tree is enabled, the port will be shut down.
- **ACL:** When the ACL rule is matched and the action is shutdown, the port will be shut down.
- **Port Security:** When the number of port MAC addresses exceeds the set number, the port will be shut down.

Note

When the recovery time is up and the port is back up, if the condition that triggers the down occurs again, the port will be shut down again.

Port Auto Recovery

Recovery Items

- All
- ARP Packet Detection
- DHCP Rate Limit
- Unicast Storm Control
- Port Loop
- Port Security
- STP BPDU Guard
- Broadcast Storm Control
- Unknown Multicast Storm Control
- ACL

Delay Time (s): Valid range is 30-86400.

Port

Port	ErrDisable Reason	Time Left (s)	Operation
1/0/1	--	0	
1/0/2	--	0	
1/0/3	--	0	

Port Auto Recovery

Link Aggregation

LAG means Link Aggregation Group which groups some physical ports together to make a single high-bandwidth data path. Thus it can implement traffic load sharing among the member ports in a group to enhance the connection reliability.

Link Aggregation Group

There are two load balance modes on the GWN7806(P) Switches, either based on the MAC Address or based on the IP – MAC Address. And in terms of the type of LAG, there are either the static option or to use the LACP or Link Aggregation Control Protocol both of them are supported.

Link Aggregation

Group | LAG Settings | LACP

Load Balance Mode:

LAG	Description	Type	Link Status	Active Member	Inactive Member	Operation
LAG1	--	Static	Down	--	--	
LAG2	--	Static	Down	--	--	
LAG3	--	Static	Down	--	--	
LAG4	--	Static	Down	--	--	
LAG5	--	Static	Down	--	--	
LAG6	--	Static	Down	--	--	
LAG7	--	Static	Down	--	--	
LAG8	--	Static	Down	--	--	
LAG9	--	Static	Down	--	--	
LAG10	--	Static	Down	--	--	

Link Aggregation Group

Load Balancing Mode	<p>Select your Load balance mode.</p> <p>MAC address - Aggregated group will balance the traffic based on different MAC addresses. Therefore, the packets from different MAC addresses will be sent to different links.</p> <p>IP/Mac Address - Aggregated group will balance the traffic based on MAC addresses and IP addresses. Therefore, the packets from same MAC addresses but different IP addresses will be sent to different links.</p>
Edit Group	<p>Name: Enter the name of the LA Group.</p> <p>Type: Use the drop down menu to specify the type for LAG.</p> <ul style="list-style-type: none"> ● Static- The static aggregated port sends packets over active member without detecting or negotiating with remote aggregated port. ● LACP- The LACP aggregated ports place member into active only after negotiated with remote aggregated port for best reliability. <p>GE: Click on port to check / uncheck which ones will be part of this LAG.</p>

LAG Port Settings

In this page, the user can Enable the Link Aggregation Group and add Description as well as specifying the speed and the flow control for LAG.

Link Aggregation								
Group		LAG Settings	LACP					
<input type="button" value="Edit"/>								
<input type="checkbox"/>	Port	Description	Status	Link Status	Speed	Jumbo Frame	Flow Control	Operation
<input type="checkbox"/>	LAG1	--	Enabled	Down	Auto	9216	Disabled	<input type="checkbox"/>
<input type="checkbox"/>	LAG2	--	Enabled	Down	Auto	9216	Disabled	<input type="checkbox"/>
<input type="checkbox"/>	LAG3	--	Enabled	Down	Auto	9216	Disabled	<input type="checkbox"/>
<input type="checkbox"/>	LAG4	--	Enabled	Down	Auto	9216	Disabled	<input type="checkbox"/>
<input type="checkbox"/>	LAG5	--	Enabled	Down	Auto	9216	Disabled	<input type="checkbox"/>
<input type="checkbox"/>	LAG6	--	Enabled	Down	Auto	9216	Disabled	<input type="checkbox"/>
<input type="checkbox"/>	LAG7	--	Enabled	Down	Auto	9216	Disabled	<input type="checkbox"/>
<input type="checkbox"/>	LAG8	--	Enabled	Down	Auto	9216	Disabled	<input type="checkbox"/>
<input type="checkbox"/>	LAG9	--	Enabled	Down	Auto	9216	Disabled	<input type="checkbox"/>
<input type="checkbox"/>	LAG10	--	Enabled	Down	Auto	9216	Disabled	<input type="checkbox"/>

Link Aggregation Port Settings

Port	The selected LAG to be configured.
Description	It is used to configure the information description for this LAG , which can be a description of usage, etc., with a maximum of 128 characters, and the characters limited to input are numbers 0-9 , letters az / AZ and special characters.
Port Enable	Set whether to enable the interface. <i>it is enabled by default.</i>
Speed	Set the rate of the interface, the options are {Auto, 10Mbps, 100Mbps, 1000Mbps} . <i>The default is auto-negotiation.</i> Note: <i>When set to Auto, the rate of the interface is automatically negotiated between the interface and the peer port</i>
Flow Control	Set the flow control on the interface, the options are { Disabled, Enabled, Auto} . <i>The default is Disabled</i> After enabling it, if the local device is congested, it will send a message to the peer device to notify the peer device to temporarily stop sending packets, after receiving the message, the peer device will temporarily stop sending packets to the local and vice versa. Thus, the occurrence of packet loss is avoided.

Link Aggregation Settings

LACP

LACP or Link Aggregation Control Protocol is based on the priority, and the user can enable a system priority or even specify the the priority for each port individually.

Link Aggregation

Group LAG Settings **LACP**

System Priority: Valid range is 1-65535

LACP List

<input type="checkbox"/>	Port	Port Priority	Timeout	Operation
<input type="checkbox"/>	1/0/1	1	Long	<input type="checkbox"/>
<input type="checkbox"/>	1/0/2	1	Long	<input type="checkbox"/>
<input type="checkbox"/>	1/0/3	1	Long	<input type="checkbox"/>
<input type="checkbox"/>	1/0/4	1	Long	<input type="checkbox"/>
<input type="checkbox"/>	1/0/5	1	Long	<input type="checkbox"/>
<input type="checkbox"/>	1/0/6	1	Long	<input type="checkbox"/>
<input type="checkbox"/>	1/0/7	1	Long	<input type="checkbox"/>
<input type="checkbox"/>	1/0/8	1	Long	<input type="checkbox"/>

Link Aggregation – LACP

System Priority	Set the system priority of LACP, the value range is an integer from 1-65535, <i>the default is 32768.</i>
Edit LACP	<p>Port: Select the switch LAG interface to be configured</p> <p>Port Priority: Set the LACP protocol priority of the port, the value range is an integer from 1 to 65535, <i>the default is 1.</i></p> <p>Note: <i>The smaller the priority value of the port, the higher the LACP priority of the port.</i></p> <p>Timeout: Set the timeout time for receiving LACP packets, the options are { Short, Long }, <i>the default is Short.</i></p> <ul style="list-style-type: none"> • Short mode: the default timeout period for receiving LACP protocol packets is 3 seconds. • Long mode: the default timeout period for receiving LACP protocol packets is 90 seconds.

Link Aggregation – LACP

MAC Address Table

The MAC address table records the correspondence between the MAC addresses of other devices learned by the switch and the interfaces, as well as information such as the VLANs to which the interfaces belong. When forwarding a packet, the device queries the MAC address table according to the destination MAC address of the packet. If the MAC address table contains an entry corresponding to the destination MAC address of the packet, it directly forwards the packet through the outbound interface in the entry. If the MAC address table does not contain an entry corresponding to the destination MAC address of the packet, the device will use broadcast mode to forward the packet on all interfaces in the VLAN to which it belongs except the receiving interface.

The entries in the MAC address table are divided into **Dynamic Address**, **Static MAC Address**, **Black hole Address** and **Port Security Address**.

Dynamic Address

the MAC address table is established based on the automatic learning of the source MAC address in the data frame received by the device. If the MAC address entry does not exist in the MAC address table, the device adds the new MAC address and the interface and VLAN corresponding to the MAC address as a new entry into the MAC address table. GWN7806(P) Switch will update the entry by resetting the aging time.

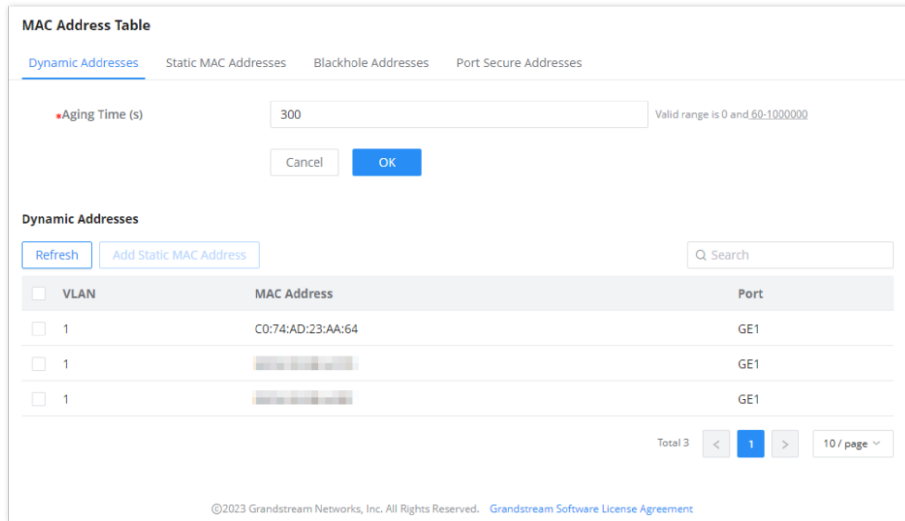
Aging Time:

Dynamic MAC address entries are not always valid. Each entry has a lifetime. The entries that cannot be updated after reaching the lifetime will be deleted. This lifetime is called the Aging Time. If the record is updated before reaching the lifetime, the aging time of the entry will be recalculated.

Notes

- The value range is 0 or 60-1 000000, **the default is 300**. If it is set to 0, it means that dynamic MAC address entries will not be aged

- Dynamic table entries are lost after system restart.



Dynamic MAC Address Table

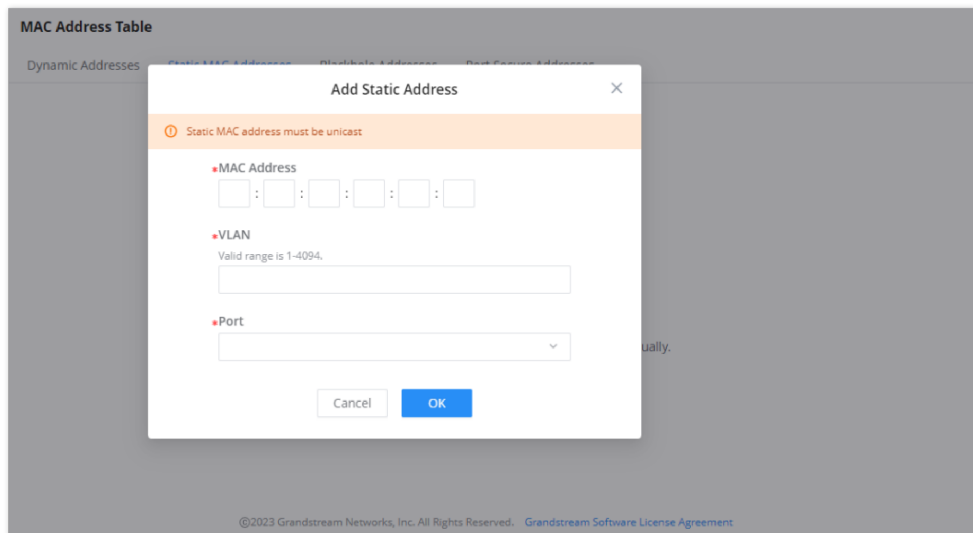
Click on **“Refresh”** button to update the table, or click on **“Add Static MAC Address”** button to add the entry to the static MAC address.

Static MAC Address

This section allows user to manually assign MAC address into MAC table. The configuration result will be displayed on the table listed on the lower side of this web page.

Note

The static MAC address must be unicast.



Static MAC Address

MAC Address	Enter the MAC address that will be forwarded
VLAN	This is the VLAN group to which the MAC address belongs.
Port	Select the port where received frame of matched destination MAC address will be forwarded to.

Black Hole Address

If a MAC address is not trusted or insecure, The user can block the traffic of certain MAC Address and discard them by adding them to the Black Hole Address Table.

Click on “**Add**” button then enter the MAC Address and the VLAN.

The screenshot shows the 'MAC Address Table' configuration page with the 'Blackhole Addresses' tab selected. A modal dialog titled 'Add Blackhole Address' is open, featuring a warning message: 'Blackhole MAC address must be a unicast address.' Below this, there are input fields for 'MAC Address' (displayed as six boxes) and 'VLAN' (with a note 'Valid range is 1-4094.'). 'Cancel' and 'OK' buttons are at the bottom of the dialog. An 'Add' button is visible below the dialog. The background interface includes tabs for 'Dynamic Addresses', 'Static MAC Addresses', 'Blackhole Addresses', and 'Port Secure Addresses'. A copyright notice at the bottom reads: '©2023 Grandstream Networks, Inc. All Rights Reserved. Grandstream Software License Agreement'.

Black Hole Address

Port Security Address

After enabling port security in **Security** → **Port Security**, the addresses will be displayed in the **MAC Address Table** → **Port Security Address** synchronously.

The list shows interface name, VLAN, MAC address.

Note

To edit, delete or add security addresses, please navigate to Security → Port Security.

The screenshot shows the 'MAC Address Table' configuration page with the 'Port Secure Addresses' tab selected. A 'Refresh' button is at the top left. Below it is a table with the following data:

VLAN	MAC Address	Port
1	CD:74:AD:1F:28:BE	GE4

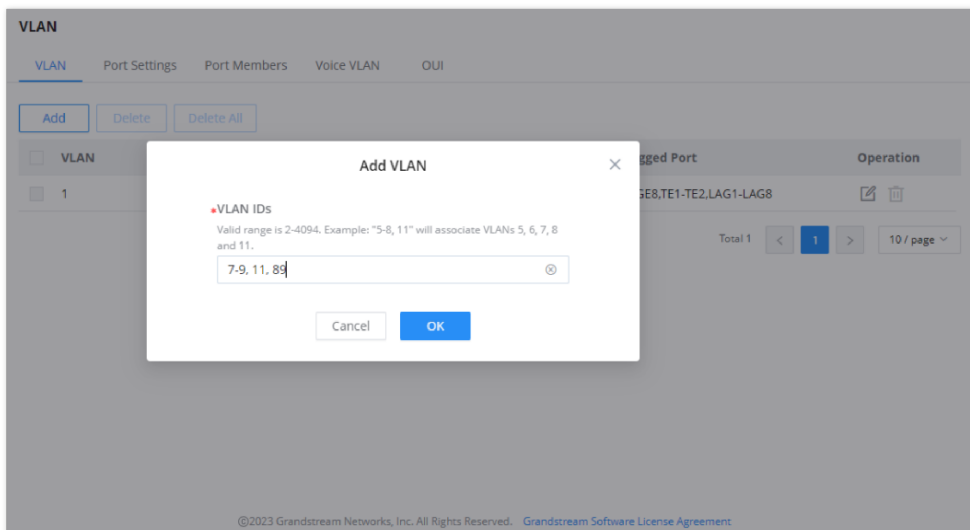
At the bottom right of the table, there is a pagination control showing 'Total 1', a page number '1' in a blue box, and '10 / page'. A copyright notice at the bottom reads: '©2023 Grandstream Networks, Inc. All Rights Reserved. Grandstream Software License Agreement'.

Port Security Address


VLAN

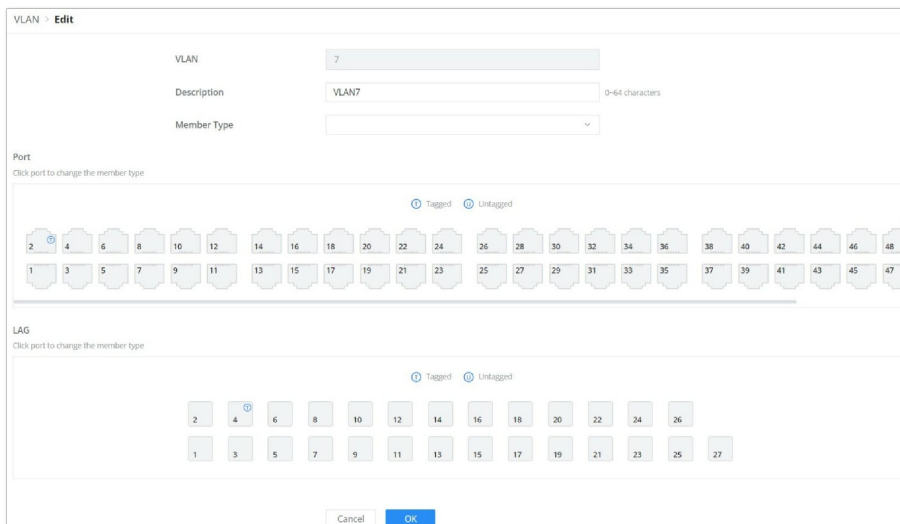
A virtual local area network, virtual LAN or VLAN, is a group of hosts with a common set of requirements that communicate as if they were attached to the same broadcast domain, regardless of their physical location. A VLAN has the same attributes as a physical local area network (LAN), but it allows for end stations to be grouped together even if they are not located on the same network switch. VLAN membership can be configured through software instead of physically relocating devices or connections.

A user can click on "Add" button to add a new VLAN, also it's possible to create many VLANs at the same time by specifying a range, for example (7-9) will create VLAN 7,8 and 9, or create different separated VLANs, for example (11,89) will create VLAN 11 and 89.



Add VLAN

If the VLAN is already created there is also the option to modify it by clicking on modify button  for more options and settings like Description, Tagged and Untagged ports and LAGs.



Edit VLAN

VLAN	The specified VLAN ID
Description	Enter a brief comment for the VLAN ID.
Member Type	Select from the drop-down list: <ul style="list-style-type: none"> ● Remove All: remove all ports GE/LAG from this VLAN ● Tagged All: Tag all ports GE/LAG to this VLAN ● Untagged All: Untag all ports GE/LAG from this VLAN
GE	Select individually which ports are tagged, untagged or unselected. <i>Note:</i> <ul style="list-style-type: none"> ● Unselected ports will not be part of the VLAN ● Tagged ports expects tagged frames (Trunk port) like connecting a switch with another switch. ● Untagged ports expects non-tagged frames (Access port) like connecting a switch with end device.
LAG	Select individually which LAGs are tagged, untagged or unselected.

Edit VLAN

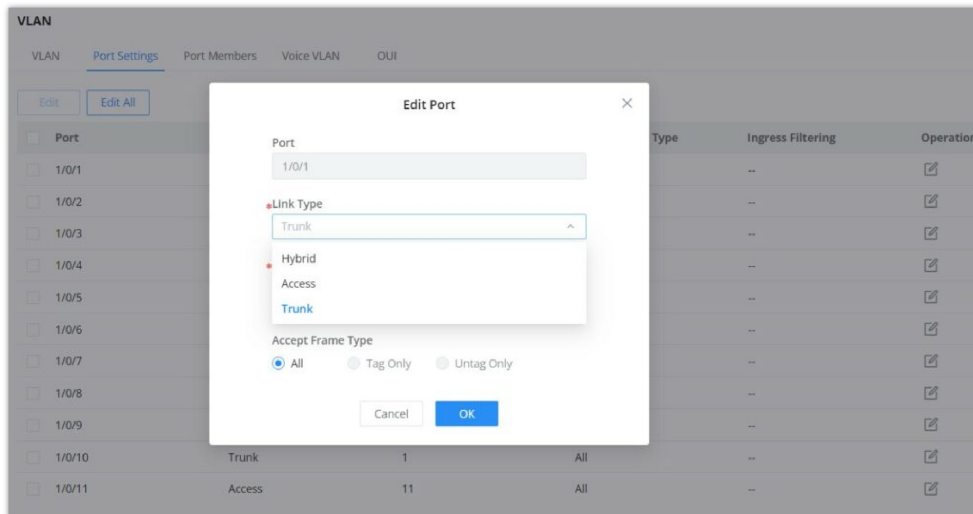
Please refer to this Table below for more details about Tagged and Untagged Ports.

Port Type	Receiving Packets		Forwarding Packets
	Untagged Packets	Tagged Packets	Tagged Packets
Untagged	When untagged packets are received, the port will add the default VLAN tag, i.e. the PVID of the ingress port, to the packets.	If the VID of packet is allowed by the port, the packet will be received. If the VID of packet is forbidden by the port, the packet will be dropped.	The packet will be forwarded after removing its VLAN tag
Tagged			The packet will be forwarded with its current VLAN tag

Tagged and Untagged Ports

VLAN Port Settings

Port Settings page allows for configuring VLAN on each port and LAG by specifying the Link Type (Trunk, Access and Hybrid) as well as the default VLAN or PVID, the user can also enable Ingress Filtering for the selected port, also the accepted Frame Type (All, Tag Only and Untag only).



VLAN Port Settings

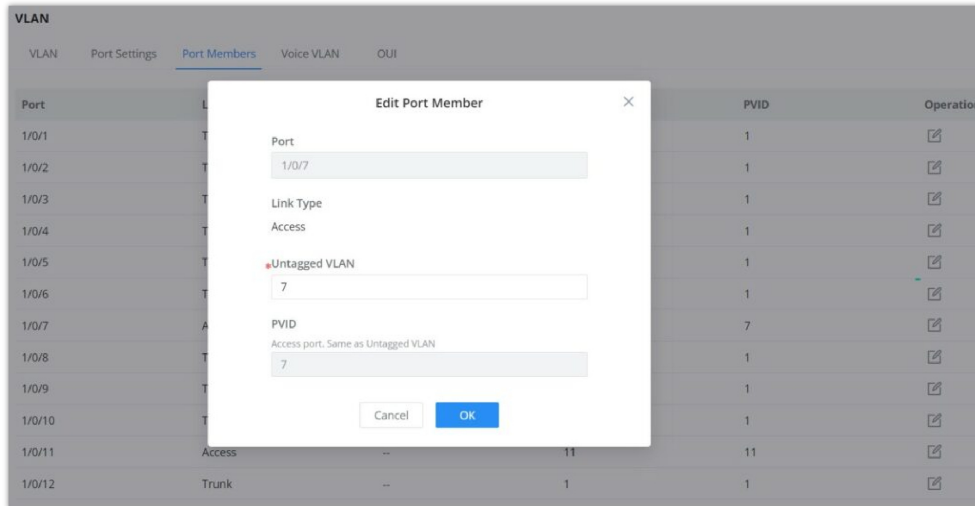
Port	Shows the selected Port.
Link Type	Select the Link Type: <ul style="list-style-type: none"> ● Hybrid: Used for connection between switches, or switch and computer. ● Access: used to connect the switch and the user terminal. ● Trunk: used for interconnecting switches or connecting switches and routers, and can carry data frames of multiple different VLANs.
PVID	Enter the default VLAN ID.
Accept Frame Type	Select the Frame type (Tag Only, Untag Only or All).
Ingress Filtering	Set whether to enable the inbound filtering function of the interface. Ingress Filtering is only available for Hybrid port, and it's enabled by default. <i>Note: Ingress filtering is a method used by enterprises and internet service providers (ISPs) to prevent suspicious traffic from entering a network.</i>

VLAN Port Members

On this page, the user can define both Tagged and Untagged VLANs (members) for each port individually.

Note

Example: Enter "5-8, 11" to associate 5 VLANs of "5, 6, 7, 8 and 11".

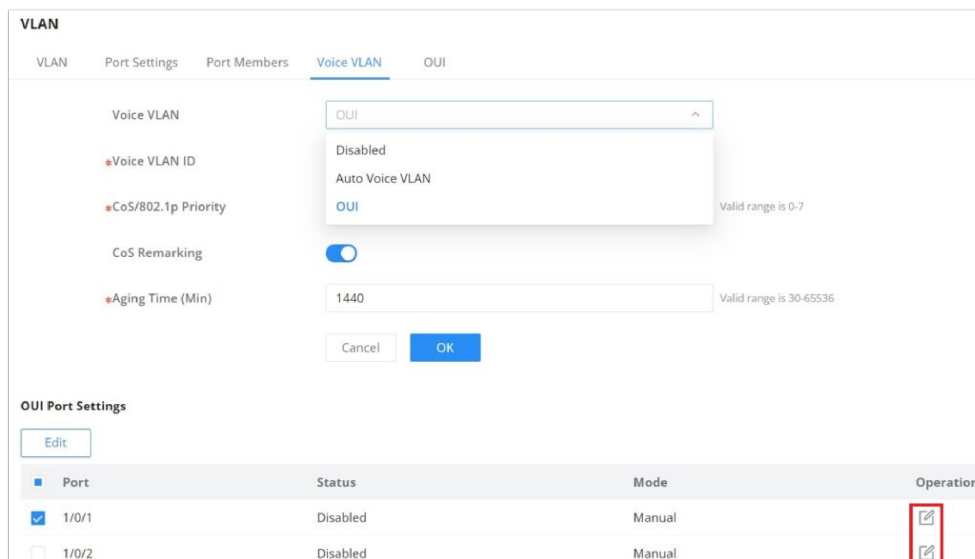


VLAN Port Members

Voice VLAN

Voice VLANs are configured specially for voice data stream. By configuring Voice VLANs and adding the ports with voice devices attached to voice VLANs, you can perform QoS-related configuration for voice data, ensuring the transmission priority of voice data stream and voice quality.

To configure Voice VLAN, please navigate to **Web UI → Switching → VLAN page → Voice VLAN tab**.



Voice VLAN

- **If Auto Voice VLAN is selected:** Enable **LLDP/LLDP-MED** and **Auto Voice Network Policy** or configure a network policy.
- **OUI:** click on "Edit" icon under operation column to configure the port.

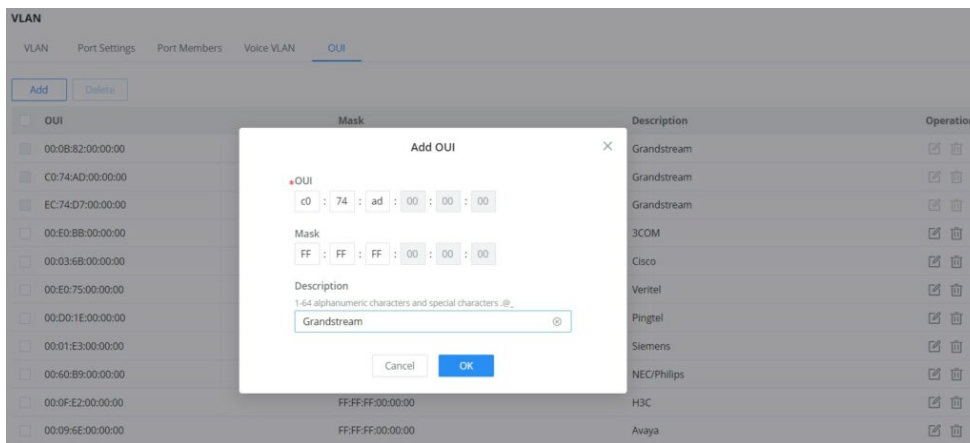
Voice VLAN (OUI) – Edit Port Settings

Voice VLAN	<p>Select from the drop-down list the Voice VLAN:</p> <ul style="list-style-type: none"> • Disabled • Auto Voice VLAN • OUI <p><i>it is disabled by default.</i></p>
Voice VLAN ID	<p>Select a VLAN as the voice VLAN from the VLAN list. <i>Note: The default VLAN 1 cannot be used as a voice VLAN.</i></p>
CoS/802.1p Priority	<p>Set whether to enable CoS Remarking.</p>
If Auto Voice VLAN is selected	
DSCP	<p>Specify the DSCP priority, an integer ranging from 0 to 63.</p>
If OUI is selected	
CoS	<p>Specify the CoS priority, an integer ranging from 0 to 7. <i>The default is 6. The higher the value, the higher the priority.</i></p>
Aging Time	<p>Set the aging time of the voice VLAN. <i>The value range is an integer from 30 to 65536 , and the default is 1440 minutes .</i></p>
Edit Port Settings	<p>Port: Displays the selected port.</p> <p>Status: Set whether to enable the voice VLAN function of the port. <i>it is disabled by default.</i></p> <p>Mode: Set the working mode of the voice VLAN on the port. <i>The default is manual.</i></p> <p>Note: <i>When set to " Manual ", the port must be added to the voice VLAN manually, and the LLDP function needs to be used.</i></p>

Voice VLAN

OUI

An OUI address is a unique identifier assigned by IEEE (Institute of Electrical and Electronics Engineers) to a device vendor. It comprises the first 24 bits of a MAC address. You can recognize which vendor a device belongs to according to the OUI address. The following table shows the OUI addresses of several manufacturers. There is also the option to add a custom one based on user needs.



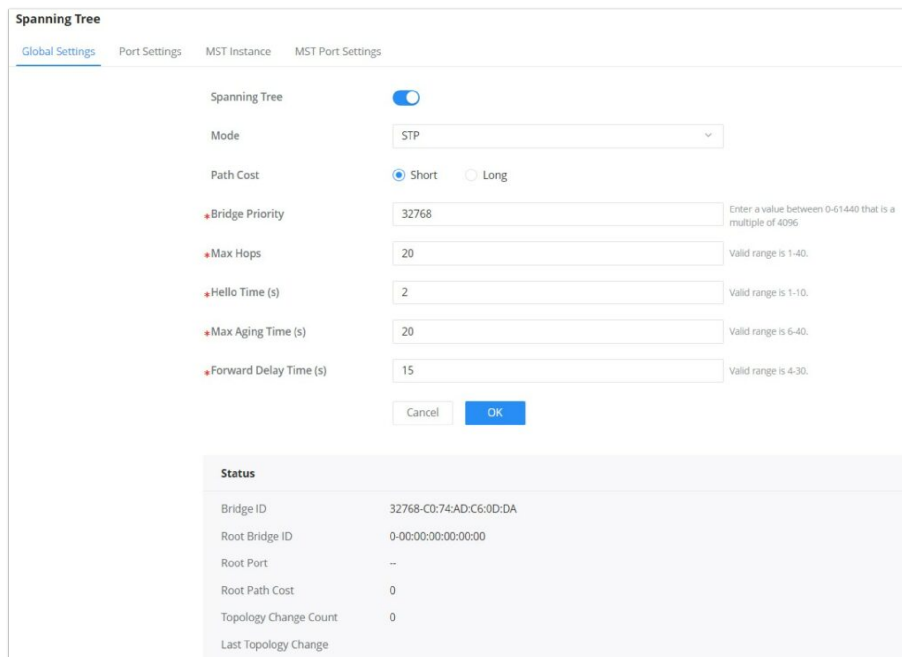
OUI

SPANNING TREE

STP (Spanning Tree Protocol), Devices running STP discover loops in the network and block ports by exchanging information, in that way, a ring network can be disbranched to form a tree-topological ring-free network to prevent packets from being duplicated and forwarded endlessly in the network.

BPDU (Bridge Protocol Data Unit) is the protocol data that STP, RSTP and MSTP use. Enough information is carried in BPDU to ensure the spanning tree generation. STP is to determine the topology of the network via transferring BPDUs between devices.

This page allows a user to configure and display Spanning Tree Protocol (STP) property configuration including the STP Mode (STP, RSTP or MSTP), Path Cost, Bridge Priority, Max Hops, Hello and Max Aging time and Forward Delay Time.



Spanning Tree – Global Settings

Spanning Tree	Set whether to enable Spanning Tree.
Mode	Set the operating mode of Spanning Tree (STP). <ul style="list-style-type: none"> ● STP: Enable the Spanning Tree (STP) operation. ● RSTP: Enable the Rapid Spanning Tree (RSTP) operation. ● MSTP: Enable the Multiple Spanning Tree Protocol (MSTP) operation.
Path Cost	Specify the path cost method (Short, Long). <i>Default is Short.</i>

Bridge Priority	Select the Bridge Priority, In an STP network, the device with the smallest bridge ID is elected as the root bridge. <i>Default is 32768.</i> <i>Note: The valid range is 0~61440, which must be a multiple of 4096</i>
Max Hops	Select the Max Hops (the range is 1 - 40). <i>Default is 20</i>
Hello Time (s)	Specify the Hello Time in seconds (the range is 1 -10). <i>Default is 2.</i> <i>Note: The time interval at which the device running the STP protocol sends the configuration message BPDU , which is used by the device to detect whether the link is faulty.</i>
Max Aging Time (s)	Select The aging time of BPDU packets of the port (the range is 6 - 40). <i>Default is 20.</i>
Forward Delay Time (s)	Specify the Forward Delay Time in seconds (the range is 4 -30). <i>Default is 15.</i>

STP Global Settings

STP Port Settings

To configure STP on each port and LAG then navigate to **WEB UI → Spanning Tree → Port Settings**, then click on “Edit” button.

Port	Port Enable	Priority	Path Cost	Edge Port	BPDU Guard	BPDU Filter	Point-to-Point	Port Status	Operation
<input checked="" type="checkbox"/> 1/0/1	Enabled	128	4	Auto	Disabled	Disabled	Auto	Disabled	
<input type="checkbox"/> 1/0/2	Enabled	128	4	Auto	Disabled	Disabled	Auto	Disabled	
<input type="checkbox"/> 1/0/3	Enabled	128	4	Auto	Disabled	Disabled	Auto	Disabled	
<input type="checkbox"/> 1/0/4	Enabled	128	4	Auto	Disabled	Disabled	Auto	Disabled	
<input type="checkbox"/> 1/0/5	Enabled	128	4	Auto	Disabled	Disabled	Auto	Disabled	
<input type="checkbox"/> 1/0/6	Enabled	128	4	Auto	Disabled	Disabled	Auto	Disabled	
<input type="checkbox"/> 1/0/7	Enabled	128	4	Auto	Disabled	Disabled	Auto	Disabled	
<input type="checkbox"/> 1/0/8	Enabled	128	4	Auto	Disabled	Disabled	Auto	Disabled	
<input type="checkbox"/> 1/0/9	Enabled	128	4	Auto	Disabled	Disabled	Auto	Disabled	
<input type="checkbox"/> 1/0/10	Enabled	128	4	Auto	Disabled	Disabled	Auto	Disabled	
<input type="checkbox"/> 1/0/11	Enabled	128	4	Auto	Disabled	Disabled	Auto	Forwarding	

Spanning Tree – Port Settings

For each port or LAG, the user can enable STP and specify the priority, Path Cost, Edge port, BPDU Guard and Filter and Point-To-Point.

Port Settings > **Edit Port**

Port	GE1
Enable STP	<input checked="" type="checkbox"/>
*Priority	128
*Path Cost	0
Edge Port	<input checked="" type="radio"/> Auto <input type="radio"/> Enabled <input type="radio"/> Disabled
BPDU Guard	<input checked="" type="checkbox"/>
BPDU Filter	<input checked="" type="checkbox"/>
Point-to-Point	<input checked="" type="radio"/> Auto <input type="radio"/> Enabled <input type="radio"/> Disabled
	<input type="button" value="Cancel"/> <input type="button" value="OK"/>

Port Status	Disabled
Designated Bridge ID	0-00:00:00:00:00:00
Designated Port ID	0-0
Path Cost	4
Operational Edge	Disabled
Operational Point-to-Point	Disabled

Spanning Tree – Edit Port Settings

Port	Displays the selected GE/LAG Port.
Enable STP	Set whether to enable STP on this port.
Priority	Priority is an important basis for determining whether the port will be selected as the root port. The port with higher priority under the same conditions will be selected as the root port . The smaller the value , the higher the priority . An integer in the range of 0-240, with a step size of 16, and a default of 128 . <i>Note: The valid range is 0~240, which must be a multiple of 16</i>
Path Cost	Set the path cost of the port on the specified spanning tree. The default value is 0, which means that path cost calculation is performed automatically. <i>Note: The valid range is 0~200000000. 0 is equal to auto</i>
Edge Port	Set whether to enable Edge Port or disable it, by default it's on auto. <i>Notes:</i> <ul style="list-style-type: none"> • A port is considered as an edge port when it is directly connected to the user terminal or server, instead of any other switches or shared network segments. The edge port will not cause a loop upon network topology changes. • In the edge mode, the interface would be put into the Forwarding state immediately upon link up. While in auto mode it will detect if the port is an edge or not.
BPDU Guard	Set whether to enable BPDU Guard. <i>Note: BPDU Guard further protects your switch by turning this port into error state and shutdown if any BPDU received from this port.</i>
BPDU Filter	Set whether to enable BPDU Filter. <i>Note: Drop all BPDU packets and no BPDU will be sent.</i>
Point-to-Point	Select Point-to-Point option (Auto, Enabled or Disabled). <i>Default is Auto.</i> <i>Note: determines the STP of link type for this port automatically if set to Auto.</i>

Multiple Spanning Tree Instance

MST or Multiple Spanning Tree Instance allows traffic of different VLAN to be mapped into different MST Instances. GWN7806(P)(P) Switch supports up to 16 independent MST instances (0~15) where each instance can be associated with many VLANs.

Spanning Tree

Global Settings Port Settings **MST Instance** MST Port Settings

Region Name: C0:74:AD:C6:0D:DA (1-32 alphanumeric characters and special characters >_)

Revision Level: 0 (Valid range is 0-65535)

Cancel OK

MSTI	VLAN	Priority	Bridge Identifier	Designated Root Bridge	Root Port	Root Path Cost	Remaining Hop	Operation
0	1-4094	32768	32768-C0:74:AD:C6:0D:DA	32767-C0:74:AD:B9:F1:9C	GE8	4	20	
1	--	32768	32769-C0:74:AD:C6:0D:DA	32769-C0:74:AD:C6:0D:DA	--	0	20	
2	--	32768	32770-C0:74:AD:C6:0D:DA	32770-C0:74:AD:C6:0D:DA	--	0	20	
3	--	32768	32771-C0:74:AD:C6:0D:DA	32771-C0:74:AD:C6:0D:DA	--	0	20	
4	--	32768	32772-C0:74:AD:C6:0D:DA	32772-C0:74:AD:C6:0D:DA	--	0	20	
5	--	32768	32773-C0:74:AD:C6:0D:DA	32773-C0:74:AD:C6:0D:DA	--	0	20	

Multiple Spanning Tree Instance

MST Instance > **Edit MST Instance**

MSTI: 0

VLAN: 1-4094

Priority: 32768

Cancel OK

Bridge Identifier: 32768-C0:74:AD:C6:0D:DA

Designated Root Bridge: 32767-C0:74:AD:B9:F1:9C

Root Port: GE8

Root Path Cost: 4

Remaining Hop: 20

MST – Edit Port

MST Port Settings is used to configure the GE port / LAG group settings for each MST instance. The table displays the MST parameters for each port.

Spanning Tree

Global Settings Port Settings MST Instance **MST Port Settings**

MSTI: 0

Port Settings

Edit Refresh

Port	Path Cost	Priority	Role	Status	Mode	Type	Designated Bridge ID	Designat	Operation
<input checked="" type="checkbox"/> GE1	4	128	Disabled Port	Disabled	MSTP	Internal	0-00:00:00:00:00:00	0-0	
<input checked="" type="checkbox"/> GE2	4	128	Disabled Port	Disabled	MSTP	Internal	0-00:00:00:00:00:00	0-0	
<input type="checkbox"/> GE3	4	128	Disabled Port	Disabled	MSTP	Internal	0-00:00:00:00:00:00	0-0	
<input type="checkbox"/> GE4	4	128	Disabled Port	Disabled	MSTP	Internal	0-00:00:00:00:00:00	0-0	
<input type="checkbox"/> GE5	4	128	Disabled Port	Disabled	MSTP	Internal	0-00:00:00:00:00:00	0-0	

MST Port Settings

Click on "Edit" button to edit the MST Port Settings for each Port/LAG individually and also the user can even specify the Path Cost and Priority per Port/LAG as well.

MST Port Settings > **Edit MST Port Settings**

MSTI: 0

Port: GE1

*Path Cost: 0

*Priority: 128

Cancel OK

Port Role: Disabled Port

Port Status: Disabled

Mode: MSTP

Type: Internal

Designated Bridge ID: 0-00:00:00:00:00:00

Designated Port ID: 0-0

Designated Path Cost: 0

Remaining Hop: 20

MST Port Settings – Edit port

IP

VLAN IP Interface

Hosts in different VLANs cannot communicate directly and need to be forwarded through routers or layer 3 switching protocols.

A VLAN interface is a virtual interface in Layer 3 mode and is mainly used to implement Layer 3 communication between VLANs, it does not exist on the device as a physical entity. Each VLAN corresponds to an interface by configuring an IP address for it, it can be used as the gateway address of each port in the VLAN so that packets between different VLANs can be forwarded to each other on Layer 3 routing through the VLAN interfaces. GWN switches support IPv4 interfaces as well as IPv6.

To configure a VLAN IP Interface, please navigate to **Web UI** → **IP** → **VLAN IP Interface** page.

MGMT VLAN (Management VLAN): as the name suggests it's the VLAN used to manage the switch, for example when using remote location with protocols like telnet, SSH, syslog etc. the default MGMT VLAN is VLAN 1 and the user have to choice to change it by selecting another VLAN from the drop-down list.

VLAN IP Interface

IPv4 Interface | IPv6 Interface | IPv6 Router Advertise

MGMT VLAN: VLAN 1

Cancel OK

Interface Settings

Add Delete All All Types Q VLAN/IP Address

IPv4 Interface	Status	Type	IPv4 Address	Mask Length	MTU	Operation
<input type="checkbox"/> Loopback1	DOWN	Static	--	--	1500	
<input type="checkbox"/> * VLAN 1	UP	Dynamic	192.168.80.120	24	1500	
<input checked="" type="checkbox"/> VLAN 7	UP	Dynamic	192.168.7.35	24	1500	
<input type="checkbox"/> VLAN 9	UP	Static	192.168.9.1	24	1500	
<input type="checkbox"/> VLAN 11	UP	Static	192.168.11.1	24	1500	

VLAN IP Interface

To add an IP Interface, please click on **"Add"** button, refer to the figure above:

IPv4 Address Type:

- **If DHCP is selected:** hosts will obtain IP addresses automatically from whatever DHCP pool configured from example like a router.

Add VLAN IP Interface – DHCP

Gateway Priority: valid range from 2 [very important] to 255 [least important].

MTU (Maximum Transmission Unit): valid range is 1280-9216.

- **If Static IP is selected:** for hosts to obtain IP addresses, the user must configure [DHCP Server](#) with the same VLAN.

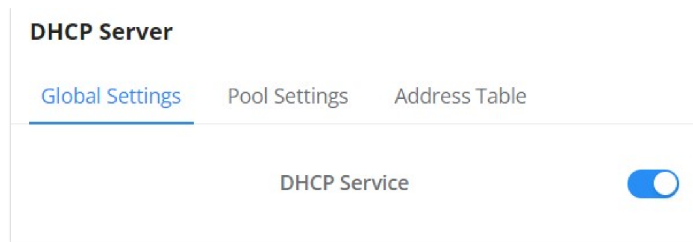
Add VLAN IP Interface – Static IP

DHCP Server

When creating VLAN IP Interface with a static IP, the user can link it with a DHCP Server for hosts to obtain IP addresses.

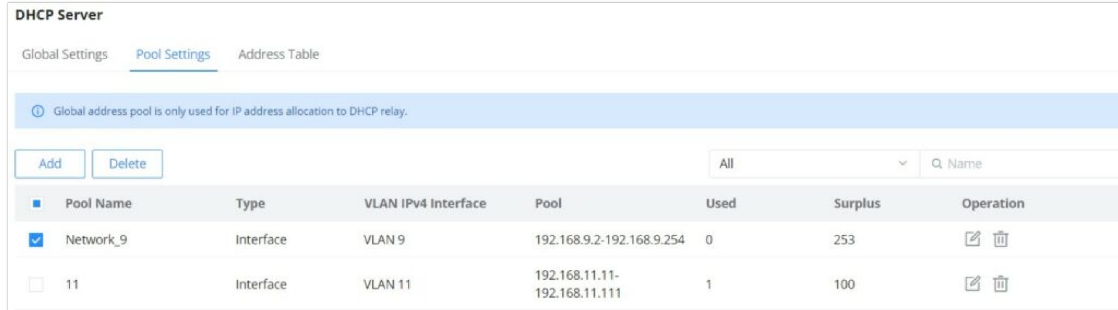
Please navigate to **Web UI** → **IP** → **DHCP Server** page.

Step 1: Enable DHCP Server.



DHCP – Global Settings

Step 2: on Pool Settings tab, click on “Add” button to add a new DHCP Server.

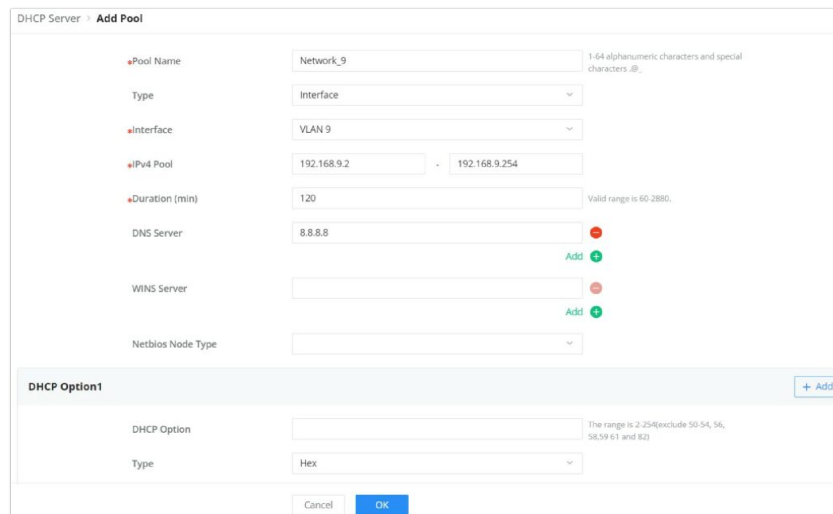


DHCP – Pool Settings

Note:

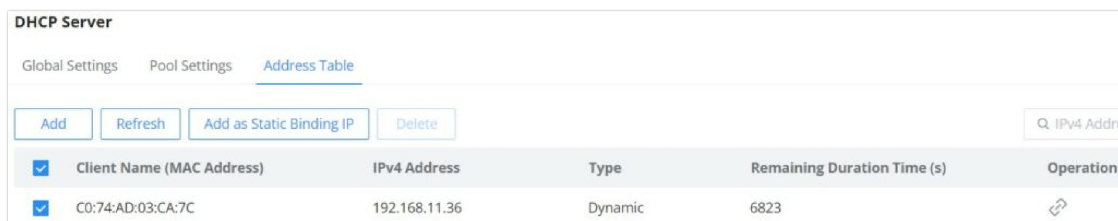
Global address pool is only used for IP address allocation to DHCP relay.

Add a pool range for the DHCP Server, then select the interface (VLAN).



DHCP – Add Pool

The address table will displays the hosts (devices) MAC Addresses and the IP addresses when using the DHCP Server. Also it's possible make a entry a static one by clicking on “Add as Static Binding IP” button.



DHCP – DHCP Server

DHCP Relay

DHCP relay on GWN7806(P) switch helps a network device pass DHCP messages between clients and servers that are on a completely different networks. When you have a DHCP server that needs to serve clients on different subnets (or VLANs). A DHCP relay agent is a network device that can route between the client's subnet and the server's subnet. The relay agent gets

the broadcast request from the client and sends it to the server, putting its own interface address as the gateway address (giaddr) field in the packet. This way, the server can tell which subnet the client is on and assign a suitable IP address. The server then sends the reply back to the relay agent, which passes it to the client.

The screenshot shows the DHCP Relay configuration page. Under 'DHCP Relay', the 'DHCP Relay' and 'Polling' options are enabled (toggles are on), and the 'TTL' is set to 4. Below this is the 'DHCP Server' section, which contains a table with one entry: 'VLAN 7' as the interface and '192.168.7.1' as the DHCP server address. There are 'Add' and 'Delete' buttons above the table, and a pagination control at the bottom right showing 'Total 1' and '1 / page'.

DHCP Relay

DHCP Relay	Set whether to enable the global DHCP relay function <i>the default is off.</i>
Polling	Set whether to enable the polling function of the DHCP relay <i>disabled by default.</i>
TTL	Set the TTL value of the DHCP request message after being forwarded by the DHCP relay layer 3. <i>the value is an integer from 1 to 16 , and the default is 4 .</i>
DHCP Server	
Interface	Select from the existing VLAN interfaces.
DHCP Server	Set the address of the DHCP server. <i>Note: The DHCP server address cannot be the interface IP address of the DHCP relay gateway , otherwise the DHCP client cannot obtain an IP address.</i>

DHCP Relay

ARP Table

Address Resolution Protocol ARP is a protocol used to resolve IP addresses to MAC addresses. In a local area network, when a host or three-layer network device has data to send to another host or three-layer network device, it needs to know the other party's network layer address (IP address) because IP addresses must be encapsulated into frames to be sent over the physical network, the sender also needs to know the receiver's actual physical address (MAC address), which requires a mapping from IP to MAC address. ARP implements the resolution of IP addresses into MAC addresses. A host or Layer 3 network device maintains an ARP table to store the relationship between IP addresses and MAC addresses. ARP entries include dynamic ARP entries and static ARP entries.

Dynamic ARP entry: It is automatically generated and maintained by the ARP protocol through ARP packets , can be aged out, can be updated by new ARP packets, and can be overwritten by static ARP entries . When the aging time is reached and the interface is down, the device immediately deletes the dynamic ARP entry in response .

Static ARP entry: A fixed mapping relationship between IP addresses and MAC addresses manually established by the network administrator, which will not be aged out and will not be overwritten by dynamic ARP entries, which can ensure the security of network communication. Static ARP entries can restrict the local device to use only the specified MAC address when communicating with the peer device with the specified IP address, in this case, the attack packet cannot modify the mapping relationship between the IP address and the MAC address in the ARP table of the local device thus the normal communication between the local device and the peer device is protected.

To configure ARP Table, please navigate to **Web UI → IP → ARP Table**.

ARP Table

*Aging Time (s) Valid range is 15-21600.

ARP Table

All

VLAN	IP Address	MAC Address	Interface	Type	Expiration Time (s)	Operation
<input type="checkbox"/> VLAN 1	192.168.80.1	c0:74:ad:23:aa:64	1/0/8	Dynamic	1113	
<input checked="" type="checkbox"/> VLAN 1	192.168.80.88	e8:f4:08:3b:62:ff	--	Static	--	
<input checked="" type="checkbox"/> VLAN 1	192.168.80.77	e8:f4:08:3b:62:fd	1/0/8	Dynamic	1176	

ARP Table

Aging time (seconds): Set the aging time of dynamic ARP entries. After the aging time expires, dynamic ARP entries are automatically deleted. The value range is an integer from 15 to 21600, and the default is 1200 seconds.

ARP Table

All

VLAN	IP Address	MAC Address	Interface	Type	Expiration Time (s)	Operation
<input type="checkbox"/> VLAN 1	192.168.80.1	c0:74:ad:23:aa:64	1/0/8	Dynamic	1073	
<input type="checkbox"/> VLAN 1	192.168.80.88	e8:f4:08:3b:62:ff	--	Static	--	
<input type="checkbox"/> VLAN 1	192.168.80.77	e8:f4:08:3b:62:fd	1/0/8	Dynamic	1127	

ARP Table – Operation

- Click on **“Link”** icon to make the dynamic entry as a static entry.
- Click on **“Delete”** icon to delete the static entry.
- Click on **“Modify”** icon to modify the static entry

It's also possible to add a static ARP entry manually by clicking on **“Add”** button, then specify the VLAN, IP Address and MAC Address combination.

Add Static ARP

The MAC address must be an unicast one.

*VLAN

*IP Address
IPv4 format

*MAC Address
 : : : : :

Add Static ARP

Neighbor Discovery

Neighbor Discovery Protocol (NDP) is an important basic protocol in the IPv6 protocol system it replaces the ARP and ICMP router discovery of IPv4. It defines the use of ICMPv6 packets to achieve address resolution, neighbor unreachability detection, duplicate address detection, router discovery, redirection, ND proxy, and other functions.

IPv6 address autoconfiguration and router discovery rely on two kinds of ICMPv6 messages: RS (Router Solicitation) and RA (Router Advertisement). Hosts send RS messages to ask routers on the same link to send RA messages right away. Routers send RA messages to let hosts know they are there and give them information like IPv6 prefixes, hop limit, MTU, and configuration flags.

To configure ND please navigate to **Web UI → IP → Neighbor Discovery**.

Neighbor Discovery

Aging time (seconds): Set the aging time of dynamic neighbor entries. After the aging time expires, the dynamic neighbor entry is automatically deleted. The value range is an integer from 15 to 21600, and the default is 1200 seconds.

Note:

Aging time applies only to dynamic entries.

Click on **Refresh** button to refresh the list for dynamic entries or click on **Add** button to add a static entry, refer to the figure below:

Add Static Neighbor

Select the VLAN from the drop-down list then enter the unicast IPv6 address and MAC address then click on **OK** button.

DNS

Domain Name System DNS provides translation services between domain names and IP addresses. GWN7806(P) Switches act as a DNS client. When users perform certain applications on the device (such as Telnet to a device or host), they can directly use a memorable and meaningful domain name, and resolve the domain name to the correct address through the domain name system.

DNS domain name resolution is divided into static domain name resolution and dynamic domain name resolution which can be used together when parsing domain names. If the static domain name resolution is unsuccessful, then dynamic domain name resolution will be used, since dynamic domain name resolution may take a certain amount of time and requires the cooperation of the domain name server, some commonly used domain names can be put into the static domain name resolution table, which can greatly improve the effect of domain name resolution.

Global Settings

On this page, the user can designate the switch as a DNS client to resolve DNS names to IP addresses through one or more configured DNS servers. It's enabled by default.

To configure DNS on GWN7806(P) switches, navigate to **Web UI** → **IP** → **DNS**, then click on the **Global Settings** tab.

DNS

Global Settings Domain Mapping Table

ⓘ DNS servers are sorted by the adding time from earliest to latest. The DNS server added the earliest has the highest priority.

DNS

Domain Suffix 1-64 alphanumeric characters and special characters _- Add +

DNS Server Add +

DNS – Global Settings

Up to 8 Domain Suffixes and 8 DNS Servers can be added. To add a Domain Suffix or DNS Server click on “+” icon and to delete click on “-” icon.

Note:

DNS servers are sorted from far to near according to the adding time, and the earliest added servers have the highest priority.

Domain Mapping Table

To add a static DNS or to view the Dynamic ones, click on the **Domain Mapping Table** tab.

DNS

Global Settings **Domain Mapping Table**

<input type="checkbox"/>	Hostname	IP Address	Type	Expiration Time (s)	Operation
<input type="checkbox"/>	grandstream.com	173.254.235.74	Static	--	<input type="button" value="edit"/> <input type="button" value="delete"/>
<input checked="" type="checkbox"/>	router.gwn.cloud	44.230.213.222	Dynamic	55	<input type="button" value="edit"/>

DNS – Domain Mapping Table

Click on “**Add**” button to add a new static DNS entry.

Add Static Domain

*Hostname
1-191 alphanumeric characters and special characters _-

*IP Address

Add Static Domain

Note:

Up to 32 static domain names can be added.

The user can also select the dynamic domains and then click on “**Add as a static domain**” button or icon to make them as static ones.

MULTICAST

IP multicast is a technique for one-to-many communication over an IP infrastructure in a network. To avoid the incoming data broadcasting to all GE/LAG ports, multicast is useful to transfer the data/message to specified GE/LAG ports for IGMP snooping or MLD Snooping. When the Switch receives a message "subscribed" by the client, it must decide to transfer the data to specified GE/LAG ports according to the location of the client (subscribed member).

IGMP Snooping

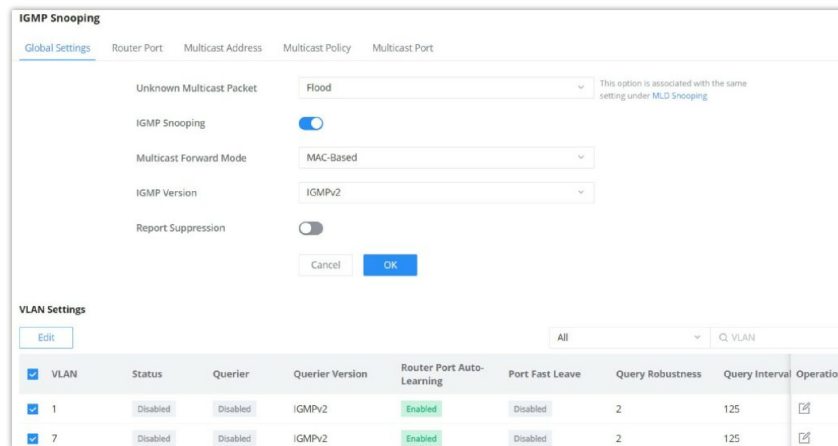
As an IPv4 Layer 2 multicast protocol, IGMP snooping is the process of listening to Internet Group Management Protocol (IGMP) network traffic. The feature allows a network switch to listen in on the IGMP conversation between hosts and routers. By listening to these conversations the switch maintains a map of which links need which IP multicast streams. Multicasts may be filtered from the links which do not need them and thus controls which ports receive specific multicast traffic.

IGMP Snooping Global Settings

This page allows the user to enable/disable IGMP Snooping function, select snooping version, and enable/disable snooping report suppression also select the Multicast Forward Mode and what to do with Unknown Multicast Packet.

Note:

Unknown Multicast Packet: This option is associated with the same one MLD Snooping. Whatever option selected here will be the same as MLD Snooping and vice versa.



IGMP Snooping Global Settings

Unknown Multicast Packet	<p>Select an action for switch to handle with unknown multicast packet.</p> <ul style="list-style-type: none"> ● Drop: Drop the unknown multicast data. ● Flood: Flood the unknown multicast data. ● Forward to Router port: Forward the unknown multicast data to router port.
IGMP Snooping	Enable or disable Global IGMP Snooping
Multicast Forward Mode	<p>Set the Multicast Forward Mode.</p> <ul style="list-style-type: none"> ● MAC-Based: Forward using MAC address. ● IP-Based: Forward using IP address
IGMP Version	Select the IGMP Version.
Report Suppression	Enable or disable the switch to handle IGMP reports between router and host, suppressing bandwidth used by

IGMP Snooping Global Settings

The user can also Enable/Disable IGMP Snooping and IGMP Snooping Querier per VLAN and much more.

IGMP Snooping Edit VLAN

VLAN	Displays the selected VLAN
MLD Snooping	Click on the toggle button to enable MLD Snooping for the selected VLAN.
MLD Snooping Querier	Click the toggle button to enable the MLD Snooping Querier.
MLD Snooping Querier Version	Select from the drop-down list the MLD Snooping Querier Version.
Router Port Auto-Learning	Click on the toggle button to learn router port by MLD query.
Port Fast Leave	Select Enable/Disable Fast Leave feature for the desired port. <i>Note: If Fast Leave is enabled for a port, the switch will immediately remove this port from the multicast group upon receiving MLD leave messages.</i>
Query Robustness	Set a number which allows tuning for the expected packet loss on a subnet. <i>The valid range is 1-7</i>
Query Interval (s)	Set the interval of querier send general query.
Query Max Response Interval (s)	It specifies the maximum allowed time before sending a responding report. <i>Note: The valid range is 5-20 in seconds.</i>
Last Member Query Count	After querying for specified times and still not receiving any response from the subscribed member, GWN7806(P) series switches will stop transmitting data to the related GE port(s). <i>Note: The valid range is 1-7</i>
Last Member Query Interval (s)	Set The maximum time interval between counting each member query message with no responses from any subscribed member. <i>Note: The valid range is 1-25 in seconds</i>

IGMP Snooping Edit VLAN

IGMP Snooping Router Port

This page shows the IGMP querier router known to this switch. Click on "Add" to add another one or Click on "Edit" icon to modify already created one.

IGMP Snooping

Global Settings Router Port Multicast Address Multicast Policy Multicast Port

Add Refresh Delete

<input checked="" type="checkbox"/> VLAN	Static Router Port	Forbidden Port	Dynamic Port	Aging Time (s)	Operation
<input checked="" type="checkbox"/> 7	GE8	GE1		0	

Total 1 < 1 > 10 / page

IGMP Snooping Router Port

Router Port > Edit

VLAN Enter "5-8, 11" to create 5 VLANs of "5, 6, 7, 8 and 11".

Static Router Port
Click on port to select/unselect

Port

2 4 6 8 10 12 14 16 18 20 22 24 26 28 30 32 34 36 38 40 42
 1 3 5 7 9 11 13 15 17 19 21 23 25 27 29 31 33 35 37 39 41

LAG

2 4 6 8 10 12 14 16 18 20 22 24 26
 1 3 5 7 9 11 13 15 17 19 21 23 25 27

Forbidden Port
Click on port to select/unselect

Cancel OK

IGMP Snooping Router Port – add or edit

IGMP Snooping Multicast Address

Dynamic multicast addresses will be listed here and the user can also add static multicast address entries based on VLAN by clicking on "Add" button or click "Edit" icon to edit.

Multicast Address > Edit

VLAN

Multicast Address IPv4 format

Click on port to select/unselect

Port

2 4 6 8 10 12 14 16 18 20 22 24 26 28 30 32 34 36 38 40 42
 1 3 5 7 9 11 13 15 17 19 21 23 25 27 29 31 33 35 37 39 41

LAG

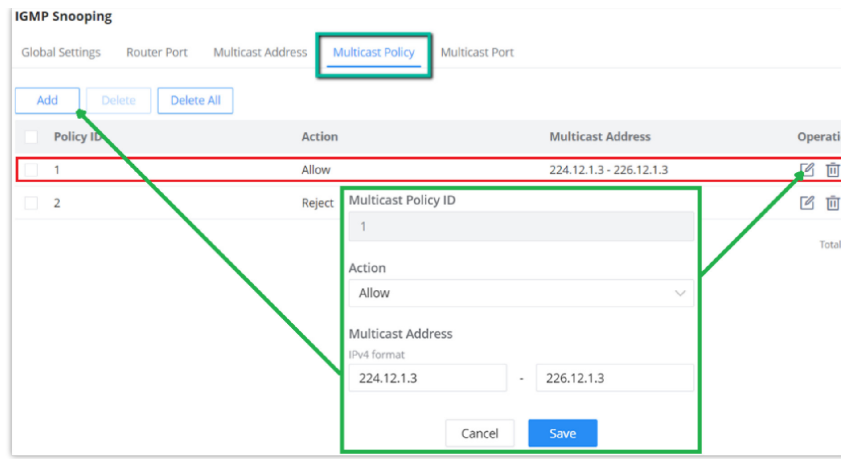
2 4 6 8 10 12 14 16 18 20 22 24 26
 1 3 5 7 9 11 13 15 17 19 21 23 25 27

Cancel OK

IGMP Snooping Multicast Address

IGMP Snooping Multicast Policy

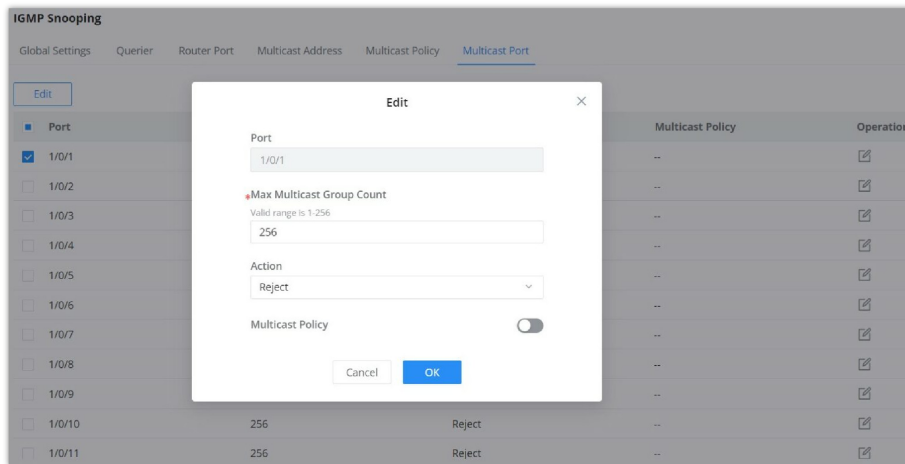
In this page, the user can add a Multicast Policy up to 128 Policy ID to Allow or Reject a range of Multicast Addresses.



IGMP Snooping Multicast Policy

IGMP Snooping Multicast Port

Once the Multicast Policy is created, the user is able to apply this policy on a port.



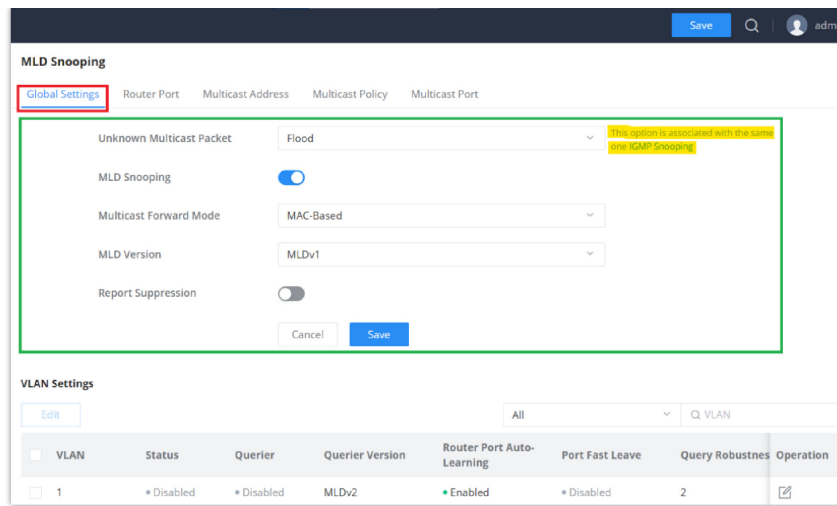
IGMP Snooping Multicast Port

MLD Snooping

MLD Snooping Global Settings

As an IPv6 Layer 2 multicast protocol, MLD Snooping maintains the outgoing port information of multicast packets by listening to the multicast protocol packets sent between Layer 3 multicast devices and user hosts, so as to manage and control multicast data . Forwarding of packets at the data link layer. When an MLD protocol packet transmitted between a host and an upstream Layer 3 device passes through a Layer 2 device, MLD Snooping analyzes the information carried in the packet, establishes and maintains a Layer 2 multicast forwarding table based on the information, and guides multicast data in the data stream.

Global Settings page give the user the ability to enable MLD Snooping as well as selecting Multicast Forward Mode etc.

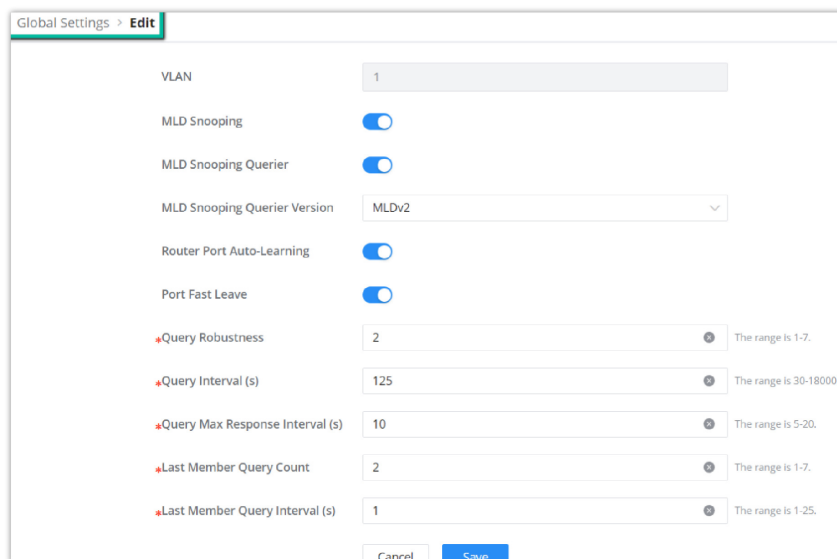


MLD Snooping Global Settings

Unknown Multicast Packet	<p>Select an action for switch to handle with unknown multicast packet.</p> <ul style="list-style-type: none"> • Drop: Drop the unknown multicast data. • Flood: Flood the unknown multicast data. • Forward to Router port: Forward the unknown multicast data to router port. <p><i>Note: This option is associated with the same one IGMP Snooping.</i></p>
MLD Snooping	Enable or disable Global MLD Snooping
Multicast Forward Mode	<p>Set the Multicast Forward Mode.</p> <ul style="list-style-type: none"> • MAC-Based: Forward using MAC address. • IP-Based: Forward using IP address
MLD Version	Select the MLD Version.
Report Suppression	Enable or disable the switch to handle MLD reports between router and host, suppressing bandwidth used by MLD.

MLD Snooping Global Settings

Once Global MLD Snooping is enabled, then the user can enable more settings per VLAN.



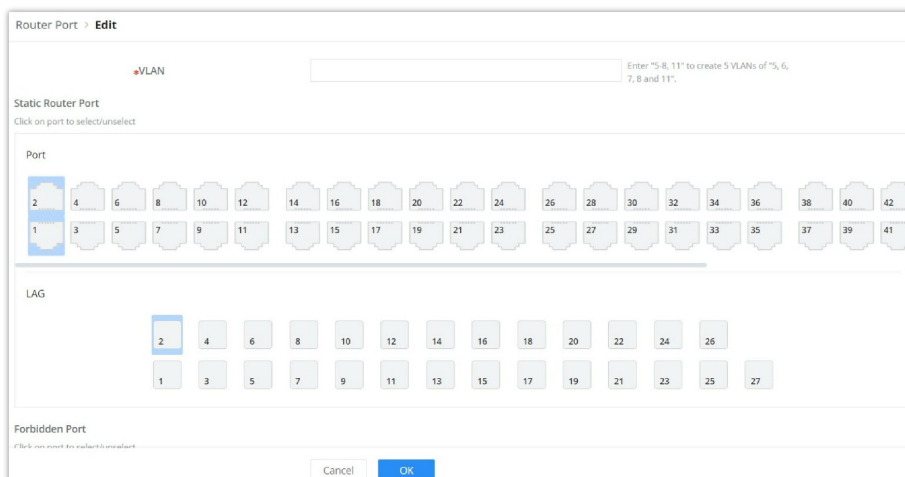
MLD Snooping – Edit VLAN

VLAN	Displays the selected VLAN
MLD Snooping	Click on the toggle button to enable MLD Snooping for the selected VLAN.
MLD Snooping Querier	Click the toggle button to enable the MLD Snooping Querier.
MLD Snooping Querier Version	Select from the drop-down list the MLD Snooping Querier Version.
Router Port Auto-Learning	Click on the toggle button to learn router port by MLD query.
Port Fast Leave	Select Enable/Disable Fast Leave feature for the desired port. <i>Note: If Fast Leave is enabled for a port, the switch will immediately remove this port from the multicast group upon receiving MLD leave messages.</i>
Query Robustness	Set a number which allows tuning for the expected packet loss on a subnet. <i>The valid range is 1-7</i>
Query Interval (s)	Set the interval of querier send general query.
Query Max Response Interval (s)	It specifies the maximum allowed time before sending a responding report. <i>Note: The valid range is 5-20 in seconds.</i>
Last Member Query Count	After quering for specified times and still not receiving any response from the subscribed member, GWN7806(P) series switches will stop transmitting data to the related GE port(s). <i>Note: The valid range is 1-7</i>
Last Member Query Interval (s)	Set The maximum time interval between counting each member query message with no responses from any subscribed member. <i>Note: The valid range is 1-25 in seconds</i>

MLD Snooping – Edit VLAN

MLD Snooping Router Port

If the router port is statically configured, the Layer 2 device will also forward the MLD report and leave message to the static router port. If a static member port is configured, the interface will be added as the outgoing interface in the forwarding table. After a Layer 2 multicast forwarding table entry is established on a Layer 2 device, when the Layer 2 device receives a multicast data packet, it searches for the forwarding table according to the VLAN to which the packet belongs and the destination address of the packet (that is, the IPv6 multicast group address). Whether the item has the corresponding "outbound interface information". If it exists, the packet is sent to all multicast group member ports; if it does not exist, the packet is discarded or broadcast in the VLAN.



MLD Snooping Multicast Address

GWN7806(P) Switches do also support adding static multicast addresses by specifying the VLAN and member port.

The screenshot shows the 'Multicast Address' configuration page. At the top, there are dropdown menus for 'VLAN' and 'Multicast Address' (with a note 'IPv6 format'). Below these is a section titled 'Click on port to select/unselect' containing two grids of port numbers. The first grid is for individual ports (1-42) and the second is for LAGs (1-27). At the bottom, there are 'Cancel' and 'OK' buttons.

MLD Snooping Multicast Address

MLD Snooping Multicast Policy

Multicast Policy can be created in this page to allow or reject a range of IPv6 Multicast Addresses. Up to 128 Policy can be created.

The screenshot shows the 'MLD Snooping' configuration page with the 'Multicast Policy' tab selected. It features a table with columns: Policy ID, Action, Multicast Address, and Operation. A modal window titled 'Edit' is open, showing fields for 'Multicast Policy ID' (set to 1), 'Action' (set to Allow), and 'Multicast Address' (IPv6 format range: ff12:3e3c:652e:3ac:d241 - ffcd:3e3c:652e:3ac:d241). The modal also has 'Cancel' and 'Save' buttons.

MLD Snooping Multicast Policy

MLD Snooping Multicast Port

The multicast policy can be applied to Gigabit Ethernet/LAG port, the user can also set the maximum number of multicast groups that the port is allowed to join and set the action when the port multicast exceeds the limit, the default is rejected .

The screenshot shows the 'MLD Snooping' configuration page with the 'Multicast Port' tab selected. It features a table with columns: Port, Multicast Policy, and Operation. A modal window titled 'Edit' is open, showing fields for 'Port' (set to 1/0/1), 'Max Multicast Group Count' (set to 256, with a note 'Valid range is 1-256'), 'Action' (set to Reject), and a 'Multicast Policy' checkbox which is checked. The modal also has 'Cancel' and 'OK' buttons.

Routing

Routing is a process in which the router selects the optimal path according to the destination address of the received data packet and forwards it to the next network node leading to the target network, and the last routing node under this path forwards the data to the target host. (Router refers to both a router in the traditional sense and an Ethernet switch running a routing protocol).

GWN7806(P) support IPv4 and IPv6 static routing.

Routing Table

A routing table is like a map of the network that shows the best routes to each destination. It achieves this by storing information on how to reach different destinations on a network and with this table the router can decide where to forward packets that it receives from other devices.

To get to the Routing Table, please navigate to **Web UI** → **Routing** → **Routing Table**.

Destination IP Address	Mask Length	Protocol Type	Priority	Next Hop	Flags
0.0.0.0	0	DHCP	1	192.168.80.1	SFA
192.168.80.0	24	Direct	0	0.0.0.0	SFA
192.168.7.0	24	Static	1	0.0.0.0	SFA
192.162.7.0	24	Direct	0	0.0.0.0	VLAN 7 SFA
90.0.0.0	24	OSPF	110	192.168.80.211	VLAN 1 SFA
80.0.0.0	16	Static	1	0.0.0.0	VLAN 1 SFA
70.0.0.0	24	OSPF	110	192.168.80.211	VLAN 1 SFA
10.0.0.0	24	OSPF	110	192.168.80.211	VLAN 1 SFA

Routing Table

A routing table contains the following information for each entry: Destination IP address, Mask Length, Protocol Type, Priority, Next Hop, outgoing Interface and Flags.

A routing table get populated over time with dynamic routing protocol like OSPF and RIP or static entries (manually configured by an administrator) or directly connected networks.

Static Routes

Static route is a special route that requires manual configuration by an administrator. Static routes have different purposes in different network environments:

- When the network structure is relatively simple, the network can work normally only by configuring static routes.
- In complex network environments, configuring static routes can improve network performance and ensure bandwidth for important applications, however, when the network fails or the topology changes, the static routes are not automatically updated and must be reconfigured manually.

To add a static route, please navigate to **Web UI** → **Routing** → **Static Routes** page.

Destination IP Address	Mask Length	Priority	Next Hop	Outgoing Interface	Operation
<input checked="" type="checkbox"/> 192.168.7.0	24	2	--	VLAN 1	
<input type="checkbox"/> 192.168.7.0	24	1	192.168.8.0	--	
<input type="checkbox"/> 192.168.80.0	24	1	192.168.7.0	--	

Click on "Add" button to add a new static route. then fill in the Destination IP Address with the mask length then select the next hop or the outgoing interface (VLAN) with specifying the priority.

Please refer to the figure below:

Add IPv4 Static Route

***Destination IP Address**

***Mask Length**

Valid range is 0-32.

Gateway

Next Hop Outgoing Interface

***Outgoing Interface**

***Priority**

The valid range is 1-255. The smaller the value, the higher the priority.

Add static route

PoE

Power Over Ethernet (PoE) refers to supplying power over an Ethernet network , also known as a local area network-based power supply system PoL or Active Ethernet.

Usually , the terminal devices of the access point need to use DC power supply , but due to insufficient wiring , these devices need unified power management . At this time , the switch interface provides the power supply function, which can solve the above problems and realize the precise control of the port PoE power supply.

Global

This page Displays the Power Supply Info like number of PoE, Total and Remaining PoE Power etc and even the Supply Voltage.

Global

[Power Supply Info](#) [Settings](#)

Global	
Number of PoE Interfaces	48
Total PoE Power	400W
PoE Reserved Power	0W
Configured Power	0W
PoE Power Consumption	0.0mW
PoE Power Supply Support Type	802.3 af/at

Chip1	
Operation Status	On
Supply Voltage	55.3V

Click on [Reboot](#) button to soft restart the PoE module function.

PoE Remaining power

PoE Remaining power(W) : specify the total reserved power of PoE power supply, the default is 20 W.

PoE – Global – Settings

Application scenarios:

The device will dynamically allocate power to each interface according to the power actually consumed by each interface. During the running process of each PD device, its power consumption will continue to change, and the system will periodically calculate the total power required by all currently connected PDs. Whether the upper limit of the available PoE power is exceeded, if it exceeds, the system will automatically power off the PD device on the interface with lower priority to ensure the normal operation of other devices. However, sometimes there will be a sudden surge in power consumption, the remaining available power of the system cannot support this surge in demand, and the system has not yet had time to calculate the total power consumption exceeding the limit, so as to disconnect the power supply of the interface with lower priority. When the PoE power supply is overloaded, the overload protection will be powered off, and all PD devices will be powered off. Use the PoE power-reserved command to reasonably set the reserved power of the system. In the event of a sudden surge in power demand, the reserved power of the system can support the sudden demand and ensure that the system has time to power off the devices on the interfaces with low priority. method to ensure the stable operation of other equipment.

Interface PoE configuration

Select the switch interface that supports PoE power supply to be configured . Multiple choices are possible.

Click on "Edit" button or icon to change the configuration per port including Power Supply Standard, Power Mode, Power Limit Mode and Power Supply Priority.

PoE – Interface

QoS

Popularity of the network and the diversification of services have led to a surge in Internet traffic, resulting in network congestion, increased forwarding delay, and even packet loss in severe cases, resulting in reduced service quality or even unavailability. Therefore , in order to carry out these real-time services on the network, it is necessary to solve the problem of network congestion . The best way is to increase the bandwidth of the network, but considering the cost of operation and maintenance, this is not realistic . The most effective solution is to apply a " Guaranteed " policies govern network traffic. QoS technology is developed under this background . QoS is quality of service , and its purpose is to provide end-to-end service

quality assurance for various business needs . QoS is a tool for effectively utilizing network resources. It allows different traffic flows to compete for network resources unequally. Voice, video and important data applications can be prioritized in network equipment.

Port Priority

In this page, the user can enable/disable port priority for each interface (port/LAG), supported modes are (CoS, DSCP, CoS-DSCP or IP-Precedence).

Please navigate to **Web UI** → **QoS** → **Port Priority** page.

Port Priority							
Edit							
<input type="checkbox"/>	Port	Trust Mode	CoS	Remarking CoS	Remarking DSCP	Remarking IP Precedence	Operation
<input type="checkbox"/>	1/0/1	802.1p	6	Enabled	Disabled	Disabled	
<input checked="" type="checkbox"/>	1/0/2	None	0	Disabled	Disabled	Disabled	
<input checked="" type="checkbox"/>	1/0/3	None	0	Disabled	Disabled	Disabled	
<input checked="" type="checkbox"/>	1/0/4	None	0	Disabled	Disabled	Disabled	
<input type="checkbox"/>	1/0/5	None	0	Disabled	Disabled	Disabled	

QoS – Port Priority

Then the user can click on **“Edit”** button for further configuration per Port/LAG.

Edit Port Priority

Port
1/0/1

Trust Mode
802.1p

*CoS
Valid range is 0-7.
6

Remarking CoS

Remarking DSCP

Remarking IP Precedence

Only either Rewrite DSCP or Rewrite IP Precedence can be selected. Both cannot be selected at the same time.

Edit Port Priority

Port	Displays the selected port GE/LAG.
Trust Mode	<p>Select the QoS operation mode:</p> <ul style="list-style-type: none"> ● None: no packet priority is trusted, and the interface default priority is used. ● CoS: Traffic is mapped to queues based on the CoS Queue Mapping, it can configured in QoS → Priority Mapping → CoS Mapping page. ● DSCP: All IP traffic is mapped to queues based on the DSCP field in the IP header. If the traffic is not IP traffic, it is mapped to the lowest priority queue. ● CoS-DSCP: All IP traffic is mapped to queues based on the DSCP field in the IP header. If the traffic is not IP traffic but has VLAN tag, mapped to queues based on the CoS value in the VLAN tag. it can configured in QoS → Priority Mapping → DSCP Mapping page.

	<ul style="list-style-type: none"> ● IP-Precedence: The IP precedence is a 3-bit field in TOS that treats high priority packets as more important than other packets. it can configured in QoS → Priority Mapping → IP Mapping page.
CoS	Set the CoS value of the interface, the value range is an integer from 0 to 7 (7 is the highest priority), <i>the default is 0.</i>
Remarking CoS	Set whether to enable Remarking CoS function of outgoing packets, <i>which is disabled by default.</i>
Remarking DSCP	Set whether to enable Remarking DSCP function of outgoing packets, <i>and it is disabled by default.</i>
Re-marking IP Precedence	Set whether to enable Remarking IP Precedence function of outgoing packets, <i>and it is disabled by default.</i> <i>Note : Only one of DSCP and IP Precedence re-marking can be enabled.</i>

QoS Port Priority

Priority Mapping

Priority mapping is used to realize the conversion between the QoS priority carried in the packet and the internal priority of the device (also known as the local priority, which is the priority used by the device to differentiate the service level of the packet) so that the device provides the Differentiated QoS service quality. Users can use different QoS priority fields in different networks according to network planning.

○ CoS Mapping

Shows the mapping relationship between queues and CoS remarking priorities.

The screenshot shows the 'Priority Mapping' configuration page for interface 802.1p (CoS). It has two tabs: 'CoS Mapping' and 'Queue-CoS Remarking Mapping'. The 'CoS Mapping' tab is active, showing a table with 'CoS' values from 0 to 6 and corresponding 'Queue' values from 0 to 6. The 'Queue-CoS Remarking Mapping' tab is also visible, showing a similar mapping. There are 'Reset', 'Cancel', and 'OK' buttons at the bottom.

CoS Mapping

○ DSCP Mapping

Shows the mapping relationship between DSCP values and queue priorities.

The screenshot shows the 'Priority Mapping' configuration page for interface 802.1p (CoS), specifically the 'DSCP-Queue Mapping' tab. It displays a grid of DSCP values (e.g., 0[CS0], 1, 2, 3, 4, 5, 6) and their corresponding Queue values (e.g., 0, 1, 2, 3, 4, 5, 6, 7). Each cell contains a dropdown menu for selecting the queue. There are 'Reset', 'Cancel', and 'OK' buttons at the bottom.

DSCP Mapping

- o **IP Mapping**

Shows the mapping relationship between IP priority and queue.

IP Mapping

Queue Scheduling

When congestion occurs in the network, the device will determine the processing order of forwarding packets according to the specified scheduling policy, so that high-priority packets are preferentially scheduled.

Queue scheduling algorithm : queue scheduling according to the switch interface.

- o **Strict priority (SP, Strict Priority) scheduling:** The flow with the highest priority is served first, and the flow with the second highest priority is served until there is no flow at that priority. Each interface of the switch supports 8 queues (queues 0-7), queue 7 is the highest priority queue, and queue 0 is the lowest priority queue. **Disadvantage :** *When congestion occurs, if there are packets in the high-priority queue for a long time, the packets in the low-priority queue cannot be scheduled, and data cannot be transmitted.*
- o **Weighted Round Robin (WRR, Weighted Round Robin) scheduling:** each priority queue is allocated a certain bandwidth, and provides services for each priority queue according to the priority from high to low. When the high-priority queue has used up all the allocated bandwidth, it is automatically switched to the next priority queue to serve it.
- o **Weighted Fair Queuing (WFQ):** On the basis of ensuring fairness (bandwidth , delay) as much as possible, priority considerations are added , so that high-priority packets have more opportunities for priority scheduling than low- priority packets . WFQ can automatically classify flows by their "session" information (protocol type , source and destination IP addresses , source and destination TCP or UDP ports, priority bits in the ToS field, etc.) Place each flow evenly into different queues, thus balancing the latency of the individual flows as a whole. When dequeuing , WFQ allocates the bandwidth that each flow should occupy at the egress according to the flow priority (Precedence) . The smaller the priority value is, the less bandwidth is obtained ; otherwise, the more bandwidth is obtained.
- o **SP-WRR:** the switch schedules packets in the SP scheduling group preferentially, and when the SP scheduling group is empty, schedules the packets in the WRR scheduling group. Queues in the SP scheduling group are scheduled with the SP queue scheduling algorithm. Queues in the WRR scheduling group are scheduled with WRR.
- o **SP-WFQ:** the switch schedules packets of queues in the WFQ group based on their minimum guaranteed bandwidth settings, then uses SP queuing to schedule the queues in the SP scheduling group, then uses WFQ to schedule the queues in the WFQ scheduling group in a round robin fashion according to their weights.

Queue Scheduling											
<input type="button" value="Edit"/>											
Port	Queuing Algorithm	Weight								Operation	
		0	1	2	3	4	5	6	7		
<input checked="" type="checkbox"/>	1/0/1	Weighted Fair Queuing(WFQ)	90	95	100	105	110	115	120	127	
<input type="checkbox"/>	1/0/2	Weighted Round Robin (WRR)	1	20	30	50	70	90	100	127	
<input type="checkbox"/>	1/0/3	SP-WFQ	0	30	40	55	77	99	111	127	
<input type="checkbox"/>	1/0/4	SP-WRR	0	30	44	50	77	99	111	127	
<input type="checkbox"/>	1/0/5	Strict Priority (SP)	--	--	--	--	--	--	--	--	

Queue Scheduling

Queue Scheduling > **Edit**

Port: 1/0/1

Queuing Algorithm: Weighted Fair Queuing(WFQ)

Scheduled according to WFQ. The weight of each queue is set by bytes

Queue ID	Weight
0	90
1	95
2	100
3	105
4	110
5	115
6	120
7	127

Cancel OK

Queue Scheduling – Edit port

Queue Shaping

When the packet sending rate is higher than the receiving rate, or the interface rate of the downstream device is lower than the interface rate of the upstream device, network congestion may occur. If the size of the service traffic sent by users is not limited, the continuous burst of service data from a large number of users will make the network more congested. In order to make the limited network resources serve users more effectively, it is necessary to restrict the service flow of users.

To configure Queue Shaping, please navigate to **Web UI → QoS → Queue Shaping**.

Queue Shaping

CIR Maximum Rate/CIR (Kbps) **CBS** Committed Burst/CBS (Bytes)

Port	Queue								Operation
	0	1	2	3	4	5	6	7	
1/0/1	--	1000000	1000000	--	--	--	--	--	
	--	53247	50000	--	--	--	--	--	
1/0/2	--	--	--	--	--	--	--	--	
	--	--	--	--	--	--	--	--	
1/0/3	--	--	--	--	--	--	--	--	
	--	--	--	--	--	--	--	--	
1/0/4	--	--	--	--	--	--	--	--	
	--	--	--	--	--	--	--	--	

Queue Shaping

To configure a port, click on **"Edit"** icon under operation column.

Maximum Rate/CIR (Kbps): Configures the maximum rate of shaping. The value must be an integer between 16-1000000 Kbps, and must be multiples of 16. By default it's the port rate.

Committed Burst/CBS (Bytes): Configures the committed burst traffic that can transmit instantly. The valid range is 678-53247 bytes. The default value is 53247 bytes.

Queue Shaping > **Edit**

Port: 1/0/1

Queue ID	Enable	Maximum Rate/CIR (Kbps)	Committed Burst/CBS (Bytes)
0	<input type="checkbox"/>		
1	<input checked="" type="checkbox"/>	1000000	53247
2	<input checked="" type="checkbox"/>	1000000	50000
3	<input type="checkbox"/>		
4	<input type="checkbox"/>		
5	<input type="checkbox"/>		
6	<input type="checkbox"/>		
7	<input type="checkbox"/>		

Cancel OK

Queue Shaping – Edit port

Rate Limit

Interface rate limit can limit the total rate of all packets sent or received on an interface. The interface rate limit also uses the token bucket to control the flow. If an interface rate limit is configured on an interface of the device, all packets sent through this interface must first be processed through the token bucket of the interface rate limiter. If there are enough tokens in the token bucket, the packet can be sent; otherwise, the packet will be discarded or cached.

To configure Rate Limit, please navigate to **Web UI → QoS → Rate Limit**.

Rate Limit

Port	Ingress	Ingress CIR (Kbps)	Ingress CBS (Byte)	Egress	Egress CIR (Kbps)	Egress CBS (Byte)	Operation
1/0/1	Enabled	1000000	2147483647	Enabled	1000000	53247	
1/0/2	Disabled	--	--	Disabled	--	--	
1/0/3	Disabled	--	--	Disabled	--	--	
1/0/4	Disabled	--	--	Disabled	--	--	
1/0/5	Disabled	--	--	Disabled	--	--	
1/0/6	Disabled	--	--	Disabled	--	--	
1/0/7	Disabled	--	--	Disabled	--	--	
1/0/8	Disabled	--	--	Disabled	--	--	
1/0/9	Disabled	--	--	Disabled	--	--	
1/0/10	Disabled	--	--	Disabled	--	--	
1/0/11	Disabled	--	--	Disabled	--	--	
1/0/12	Disabled	--	--	Disabled	--	--	

Rate Limit

To configure a port, click on “**Edit**” icon under operation column, then set the CIR and CBS for both Ingress and Egress.

CIR (Committed Information Rate): the guaranteed average transmission rate or the minimum guaranteed traffic delivered in the network.

CBS (Committed Burst Size): the average volume of burst traffic that can pass through an interface.

Rate Limit > **Edit**

Port: 1/0/1

Ingress:

• Ingress CIR (Kbps): 1000000 Enter a value between 16-1000000 that is a multiple of

• Ingress CBS (Byte): 2147483647 Valid range is 32768-2147483647

Egress:

• Egress CIR (Kbps): 1000000 Enter a value between 16-1000000 that is a multiple of

• Egress CBS (Byte): 53247 Valid range is 678-53247

Cancel OK

SECURITY

GWN7806(P) Switches series support many tools and features to enhance the security of the device against misconfiguration or attacks.

Storm Control

Traffic suppression can limit the rate of broadcast, unknown multicast, unknown unicast, known multicast, and known unicast packets by configuring thresholds, preventing broadcast, unknown multicast packets, and unknown unicast packets from generating broadcast storms. Large traffic impact of known multicast packets and known unicast packets.

Storm control can block the traffic of broadcast, unknown multicast and unknown unicast packets by blocking packets or shutting down ports. The device supports storm control for the above three types of packets on the interface according to the packet rate, byte rate, and percentage. During a detection interval, the device monitors the average rate of three types of packets received on the interface and compares it with the configured maximum threshold. When the packet rate is greater than the configured maximum threshold, the device performs storm control on the interface and executes the Configured storm control actions. Storm control actions include blocking packets and shutting down / shutdown interfaces.

- If packets are blocked, when the average rate of receiving packets on the interface is less than the specified minimum threshold, storm control will release the blocking of the packets on the interface.
- If the action is to shut down / shutdown the interface, you need to manually run the command to bring up the interface, or enable the interface state to automatically return to UP, it's also possible to use the **Auto Recovery** function to bring up the interface automatically.

Storm Control > Edit

Port: 1/0/1

Storm Control:

Broadcast:

Threshold (Kbps): 10000 Enter a value between 16-1000000 that is a multiple of 16

Unknown Multicast:

Threshold (Kbps): 10000 Enter a value between 16-1000000 that is a multiple of 16

Unknown Unicast:

Threshold (Kbps): 10000 Enter a value between 16-1000000 that is a multiple of 16

Action: Drop Disabled

Buttons: Cancel, OK

Storm Control

Secure Dynamic MAC Address	If enabled but the Sticky MAC function is not enabled.	If the device is restarted, the entries will be lost and need to be relearned.
Secure Static MAC Address	Static MAC address manually configured when port security is enabled.	The entries will not be aged, and will not be lost after a reboot.
Sticky MAC Address	The MAC address converted after the port security is enabled and the Sticky MAC function is enabled at the same time	The entries will not be aged, and the addresses will not be lost after restarting the device.

Storm Control

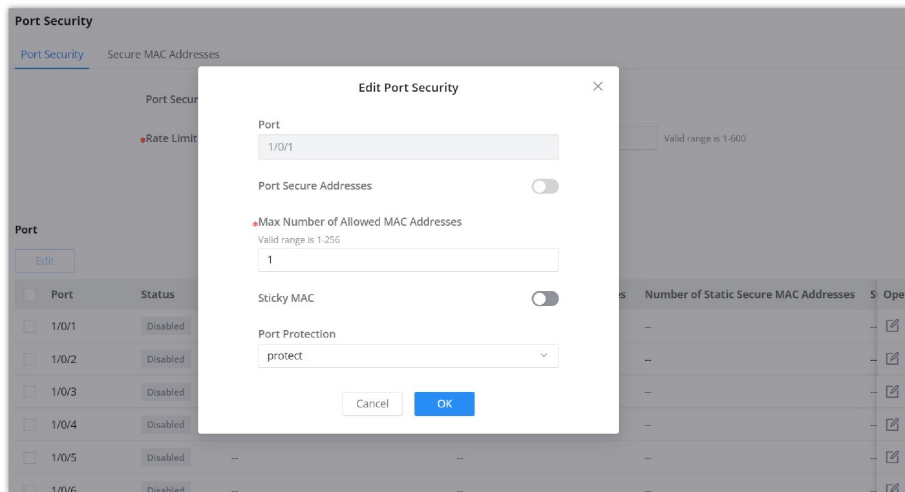
Port Security

By converting the MAC address learned by the interface into secure MAC addresses (including secure dynamic MAC address, secure static MAC address and Sticky MAC) , port security prevents illegal users from communicating with the switch through this interface, thereby enhancing the security of the device.

Security MAC addresses are divided into: Secure Dynamic MAC, Secure Static MAC and Sticky MAC.

Secure Dynamic MAC Address	If enabled but the Sticky MAC function is not enabled.	If the device is restarted, the entries will be lost and need to be relearned.
Secure Static MAC Address	Static MAC address manually configured when port security is enabled.	The entries will not be aged, and will not be lost after a reboot.
Sticky MAC Address	The MAC address converted after the port security is enabled and the Sticky MAC function is enabled at the same time	The entries will not be aged , and the addresses will not be lost after restarting the device.

Secure MAC Address Types



Port Security

Port Security	Click Allow to set the port security function to be enabled globally , by default is disabled.
Rate Limit (packet/s)	Set the rate at which the port MAC address is learned. The value is an integer from 1 to 600, the default is 100.
Edit Port Security	
Port	Displays the selected ports.
Port Security Address	Click to enable Port Security Address, by default is disabled.
Maximum MAC Number	Set the maximum number of MAC addresses to be learned by the interface , the value range is an integer from 1 to 256 , and the default is 1 . After the maximum number is reached , if the switch receives a packet whose source MAC address does not exist, regardless of whether the destination MAC address exists, the switch considers that there is an attack by an illegal user, and will protect the interface according to the port protection configuration (Protect, Restrict or Shutdown).
Sticky MAC	When the port security is enabled, the Sticky MAC function can be enabled, by default it's disabled . When enabled, the interface will convert the learned secure dynamic MAC address into a Sticky MAC. If the maximum number of MAC addresses has been reached, the MAC address in the non-sticky MAC

	entry learned by the interface will be discarded , and a trap alarm will be reported according to the interface protection mode configuration.
Port Protection	<p>Set the protection action when the number of MAC addresses learned by the interface reaches the maximum number or static MAC address flapping occurs .</p> <p>There are three modes (Protect, Restrict or Shutdown), the default is Protect.</p> <ul style="list-style-type: none"> ● Protect: Only discard the packets whose source MAC address does not exist, and does not report an alarm. ● Restrict: Discard packets with nonexistent source MAC addresses and report an alarm. ● Shutdown: The interface state is set to error-down and an alarm is reported. <p><i>Note: By default, an interface will not automatically recover after being shut down, and the interface can only be enabled by the network administrator under the interface. If you want the shut down interface to be restored automatically , you can enable Port Auto Recovery function to automatically restore the interface status to Up.</i></p>

Port Security

Port Isolation

With the port isolation function, the isolation between ports in the same VLAN can be realized. As long as the user adds the port to the isolation group, the Layer 2 data isolation between the ports in the isolation group can be realized. The port isolation function provides users with a safer and more flexible networking solution.

Note:

Due to software limitations, only one isolation group is currently supported, and the port isolation function is disabled by default, that is, the port is added to the default isolation group . After joining , two-way isolation is performed between ports .

Port Isolation	
Port	Isolation Status/Operation
1/0/1	<input type="checkbox"/>
1/0/2	<input type="checkbox"/>
1/0/3	<input type="checkbox"/>
1/0/4	<input type="checkbox"/>
1/0/5	<input type="checkbox"/>
1/0/6	<input type="checkbox"/>
1/0/7	<input type="checkbox"/>
1/0/8	<input type="checkbox"/>
1/0/9	<input type="checkbox"/>
1/0/10	<input type="checkbox"/>
1/0/11	<input type="checkbox"/>

Port Isolation

ACL

Access control list (ACL) is a collection of one or more rules. A rule is a judgment statement that describes the matching conditions of a packet. These conditions can be the source address, destination address, port number, etc. of the packet. ACL is essentially a packet filter, and the rule is the filter element of the filter. The device matches packets based on these rules, filters out specific packets , and allows or organizes the packets to pass through according to the processing policy of the service module that applies the ACL.

Notes:

- One ACL supports setting multiple rules . When the rule settings (except the rule number) are identical, it will prompt " This rule already exists"
- If there is no match after all the rules are traversed , the Deny message will be sent directly .

IPv4 ACL

This page displays the list of IPv4 ACL and the number of rules.

ACL Name	Port	Rule Number	Operation
IPv4_ACL	GE1	1	

Total 1 | 1 | 10 / page

Rule Settings

- Rule ID: 1
- Action: Drop
- Protocol Type: ICMP
- Source IP Address: Any Custom
- Destination IP Address: Any Custom
- ICMP Type: Router Advertisement
- ICMP Code: Any Custom
- Tos Type: DSCP
- DSCP: 7

Cancel Save

ACL – IPv4

IPv6 ACL

The same as the IPv4 ACL, there is also a list for IPv6 ACL, and the same applies here.

ACL Name	Port	Rule Number	Operation
IPv6_ACL		7	

Total 1 | 1 | 10 / page

Rule Settings

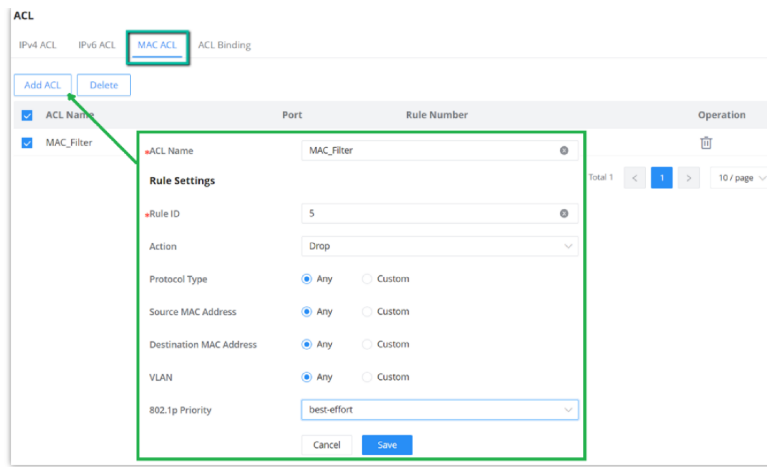
- Rule ID: 7
- Action: Drop
- Protocol Type: ICMP
- Source IP Address: Any Custom
- Destination IP Address: Any Custom
- ICMP Type: Time Exceeded
- ICMP Code: Any Custom
- Tos Type: DSCP
- DSCP: 8

Cancel Save

ACL – IPv6

MAC ACL

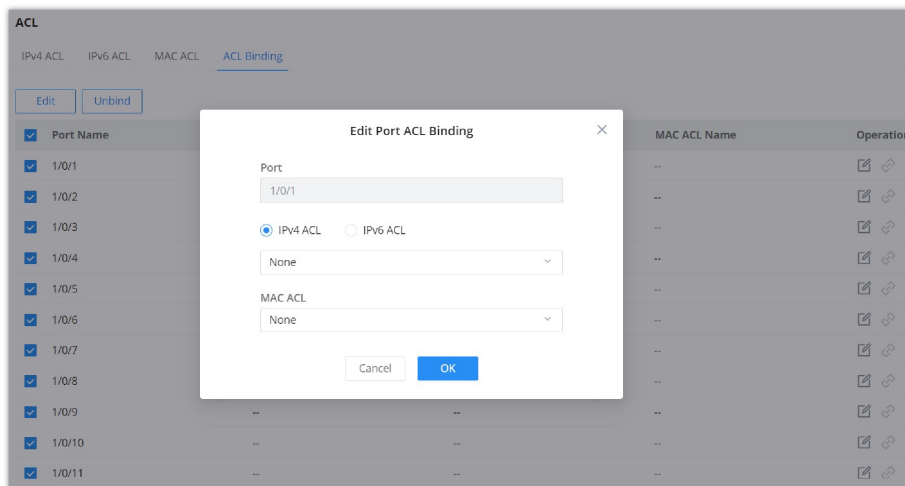
A MAC access control list (ACL) **lets you permit or deny WiFi access to individual devices based on their MAC addresses.** For example, if you notice a guest device that is using too much bandwidth, you can deny WiFi access to it without affecting other guest devices.



MAC ACL

ACL Binding

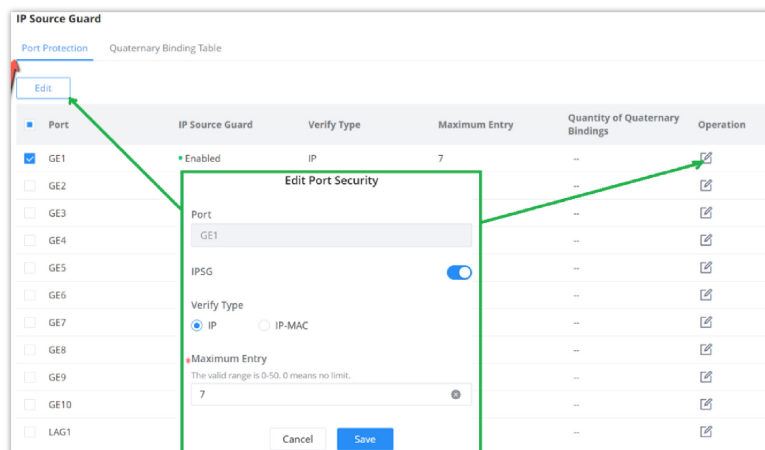
ACL Binding lets the user bind MAC ACL or IP ACL to a certain ports GE/LAG.



ACL Binding

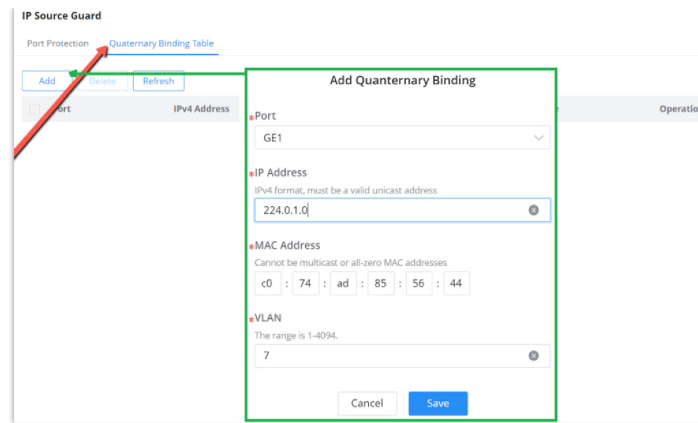
IP Source Guard

IP source guard attack is a source IP address filtering technology based on Layer 2 interface. It can prevent malicious hosts from forging IP addresses of legitimate hosts to impersonate legitimate hosts, and also ensure that unauthorized hosts cannot access by specifying their own IP addresses. network or attack the network. IPSG uses the binding table (source IP address, source MAC address, VLAN to which it belongs, and the binding of the inbound interface) to match and check the IP packets received on the Layer 2 interface. Only the packets matching the binding table are allowed to pass through.



IP Source Guard

In this page the user can specify the IP and MAC addresses as well as the VLAN for a port LAN/LAG.



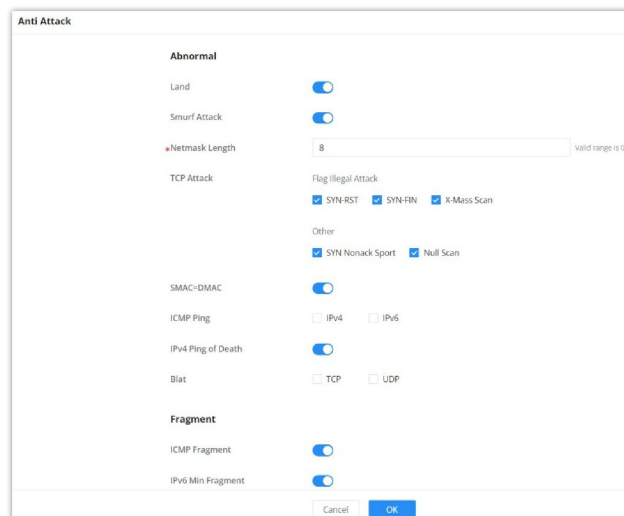
Quanternary Binding Table

Anti Attack

In the network, there are a large number of malicious attack packets targeting the CPU and various types of packets that need to be normally sent to the CPU. Malicious attack packets targeting the CPU will cause the CPU to be busy processing attack packets for a long time, thereby causing interruption of other services or even system interruption; a large number of normal packets will also lead to high CPU usage and performance degradation, thus affecting the normal business.

In order to protect the CPU and ensure that the CPU can process and respond to normal services, the switch provides a local attack defense function, which is aimed at the packets sent to the CPU. It operates normally to avoid the mutual influence of various services when the device is attacked.

Attack defense is an important network security feature. It analyzes the content and behavior of the packets sent to the CPU for processing, determines whether the packets have attack characteristics, and configures certain preventive measures against the packets with attack characteristics. Defense attacks are mainly divided into malformed packet attack defense, fragmented packet attack defense, and flood attack defense.



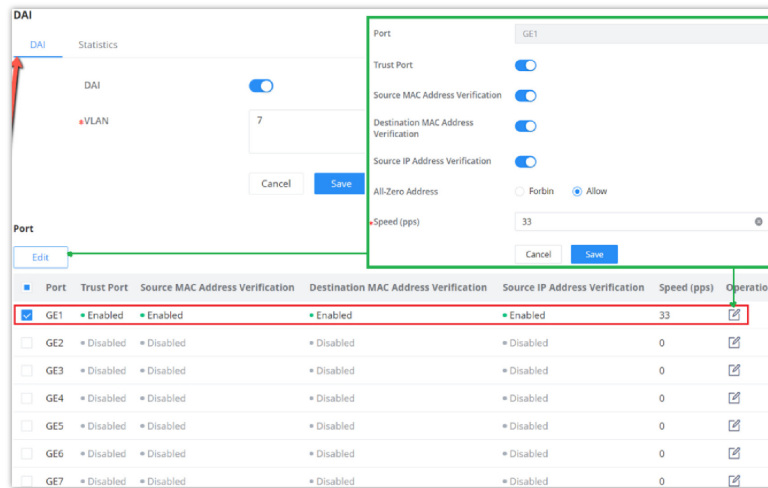
Anti Attack

Dynamic ARP Inspection (DAI)

To defend against man-in-the-middle attacks and prevent data of legitimate users from being stolen by the man-in-the-middle, you can enable dynamic ARP inspection. The device compares the source IP, source MAC, interface, and VLAN information corresponding to the ARP packet with the information in the binding table. If the information matches, it means that the user who sent the ARP packet is a legitimate user, and the user is allowed. If the ARP packet passes, otherwise it is considered an attack and the ARP packet is discarded.

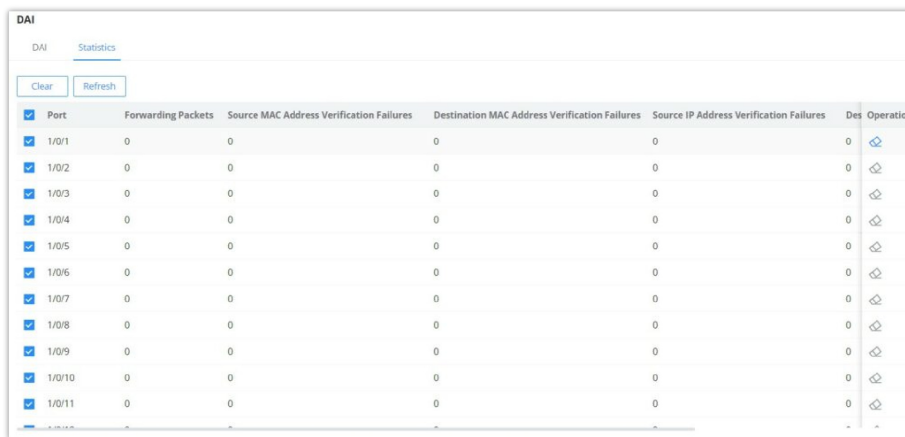
Dynamic ARP inspection can be enabled in the interface view, or VLAN view. When enabled in the interface view, the binding table matching check is performed on all ARP packets received by the interface; when enabled in the VLAN view, the binding table matching check is performed on the ARP packets belonging to the VLAN received by the interface that joins the VLAN.

When the device discards a large number of ARP packets that do not match the binding table, if you want the device to alert the network administrator in the form of an alarm , you can enable the dynamic ARP inspection discarded packet alarm function. When the number of discarded ARP packets exceeds the alarm threshold , the device generates an alarm.



DAI

The statistics about DAI activities will be listed here for each port GE/LAG with the options of refreshing the statistics or clearing specified port data.

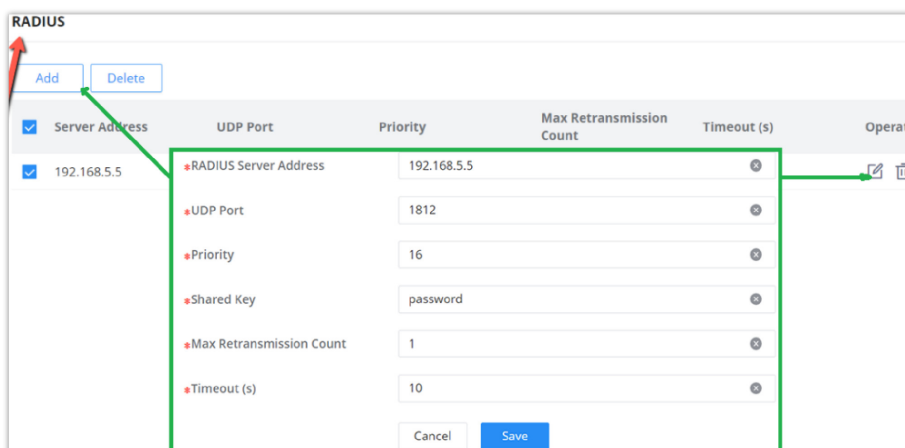


DAI Statistics

RADIUS

RADIUS is a distributed, client /server information exchange protocol that can protect the network from unauthorized access. It is often used in various network environments that require high security and allow remote users to access. This protocol defines the UDP-based RADIUS packet format and its transmission mechanism, and specifies destination UDP ports 1812 and 1813 as the default authentication and accounting port numbers, respectively.

Radius provides access services through authentication and authorization, and collects and records the use of network resources by users through accounting . The main features of RADIUS protocol are: client/server mode, secure message exchange mechanism and good expansibility.



TACACS+

TACACS+ (Terminal Access Controller Control System Protocol) is a security protocol with enhanced functions based on the TACACS protocol. This protocol is similar in function to the RADIUS protocol, and uses the client/server mode to implement the communication between the NAS and the TACACS+ server.

TACACS+ is a centralized, client /server structure information exchange protocol, which uses TCP protocol for transmission, and the TCP port number is 49. The authentication , authorization and accounting servers provided by TACACS+ are independent of each other and can be implemented on different servers. It is mainly used for authentication, authorization and accounting of access users who access the Internet by means of point-to-point protocol PPP or virtual private dial-up network VPDN and management users who perform operations.

TACACS+ is similar to RADIUS protocol : (1) both adopt client /server mode in structure; (2) both use shared key to encrypt the transmitted user information ; (3) both have better flexibility and expansibility. TACACS+ has more reliable transmission and encryption characteristics, and is more suitable for security control.

Server Address	TCP Port	Priority	Timeout (s)	Operation
192.168.5.11	49	3	5	[Edit] [Delete]

*TACACS+ Server Address	192.168.5.11
*TCP Port	49
*Priority	3
*Shared Key	password
*Timeout (s)	5
[Cancel] [Save]	

TACACS+

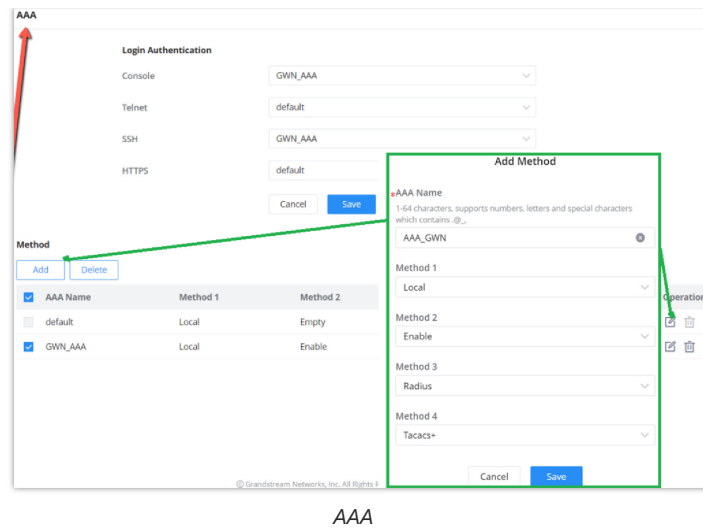
AAA

Access control is used to control which users can access the network and which network resources can be accessed. AAA is short for Authentication , Authorization , and Accounting , and provides a management framework for configuring access control on NAS (Network Access Server) devices .

As a management mechanism of network security , AAA provides services in a modular manner:

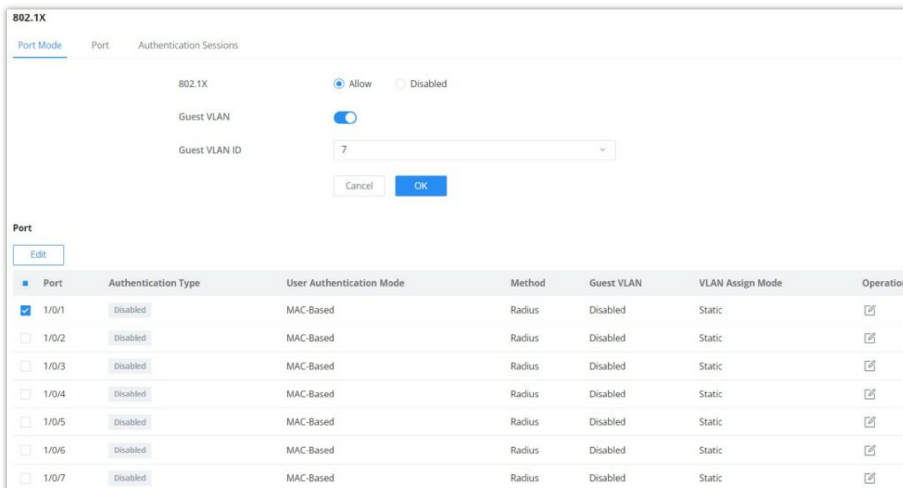
- Authentication , confirming the identity of users accessing the network , and judging whether the visitor is a legitimate network user;
- Authorization , giving different users Different permissions limit the services that the user can use;
- Billing , record all operations during the user's use of network services, including the type of service used, start time, data flow, etc., to collect and record the user's The usage of network resources, and can realize the charging requirements for events and traffic, and also monitor the network.

AAA adopts a client /server structure. The AAA client runs on the access device, usually referred to as a NAS device, and is responsible for verifying user identity and managing user access; AAA server is a collective name for authentication server, authorization server and accounting server. Responsible for centralized management of user information. AAA can be implemented through a variety of protocols. Currently, devices support AAA based on RADIUS or TACACS + protocol. In practical applications, RADIUS protocol is most commonly used.



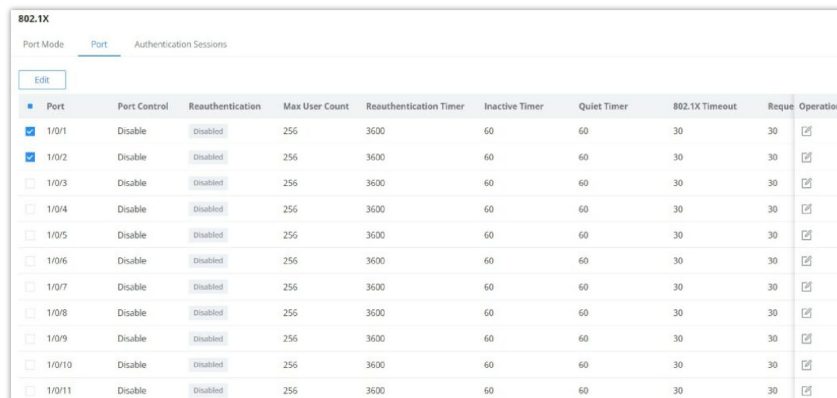
802.1X

802.1X protocol is a port – based network control protocol . Port – based network access control refers to verifying user identities and controlling their access rights at the port level of LAN access devices. The 802.1X protocol is a Layer 2 protocol and does not need to reach Layer 3. It does not require high overall performance of the access device , which can effectively reduce network construction costs. Authentication packets and data packets are separated through logical interfaces to improve security.



802.1X Port Mode

802.1X Port

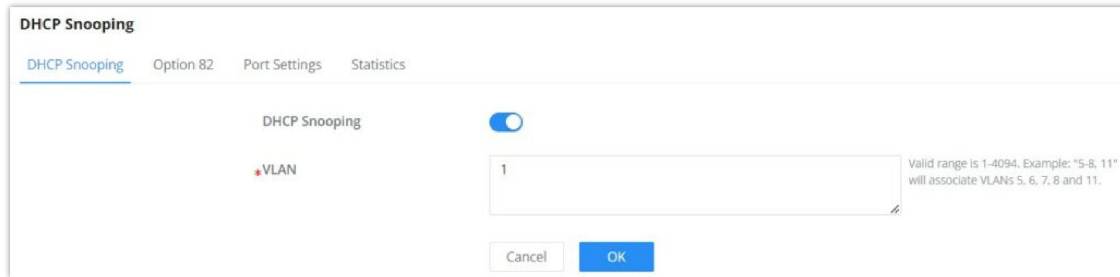


802.1X Port

DHCP Snooping

DHCP snooping ensures that DHCP clients obtain IP addresses from legitimate DHCP servers, and records the correspondence between IP addresses and MAC addresses of DHCP clients to prevent DHCP attacks on the network.

In order to ensure the security of network communication services, the DHCP Snooping technology is introduced, and a firewall is established between the DHCP Client and the DHCP Server to defend against various attacks against DHCP in the network.



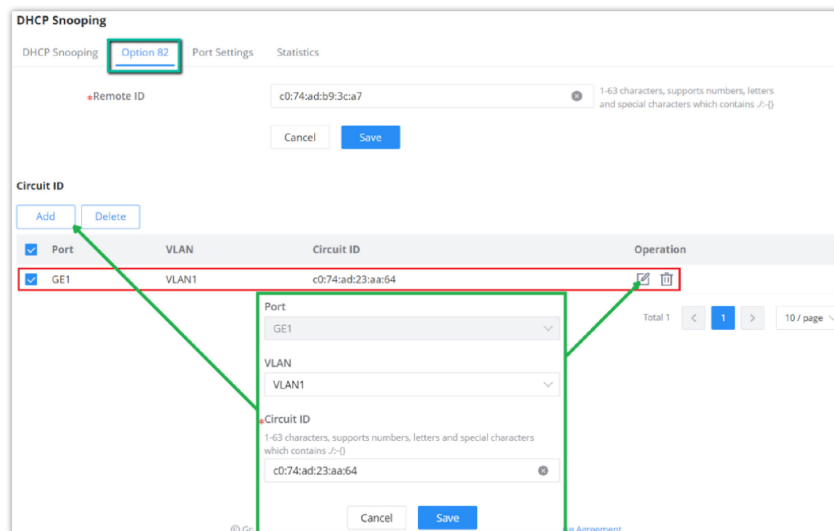
DHCP Snooping

DHCP Option 82

Option 82 is called the relay agent information option and is inserted by the DHCP relay agent when forwarding client-originated DHCP packets to a DHCP server.

To identify the device accessed by the client, the user can enter his MAC address in the remote ID.

Circuit id is used to identify the VLAN, interface and other ID information where the client is located.



DHCP Option 82

DHCP Port Settings

This page allows a user to configure detailed settings of DHCP Snooping for each port (GE/LAG).

Any device that is not in the service provider network will be regarded as an entrusted source (such as a customer switch).

DHCP Snooping

DHCP Snooping Option 82 **Port Settings** Statistics

[Edit](#)

Port	Trust Mode	Chaddr Verification	Speed(pps)	Option 82	Option 82 Mode	Operation
<input checked="" type="checkbox"/> GE1	Enabled	Enabled	0	Enabled	Drop	
<input type="checkbox"/> GE2	Enabled	Enabled	100	Enabled	Keep	
<input type="checkbox"/> GE3						
<input type="checkbox"/> GE4						
<input type="checkbox"/> GE5						
<input type="checkbox"/> GE6						
<input type="checkbox"/> GE7						
<input type="checkbox"/> GE8						
<input type="checkbox"/> GE9						

Port: GE2

Trust Mode:

Chaddr Verification:

Speed (pps): 100

Option 82:

Option 82 Mode: Keep

[Cancel](#) [Save](#)

DHCP Port Settings

DHCP Statistics

This page displays all statistics recorded by DHCP snooping function.

DHCP Snooping

DHCP Snooping Option 82 Port Settings **Statistics**

[Clear](#) [Refresh](#)

Port	Forwarding Packets	Chaddr Verification Drops	Untrusted Port Drops	Untrusted Ports with Option 82 Drops	Invalid Drop	Operation
<input checked="" type="checkbox"/> 1/0/1	0	0	0	0	0	
<input type="checkbox"/> 1/0/2	0	0	0	0	0	
<input type="checkbox"/> 1/0/3	0	0	0	0	0	
<input type="checkbox"/> 1/0/4	0	0	0	0	0	
<input type="checkbox"/> 1/0/5	0	0	0	0	0	
<input type="checkbox"/> 1/0/6	0	0	0	0	0	
<input type="checkbox"/> 1/0/7	0	0	0	0	0	
<input type="checkbox"/> 1/0/8	0	0	0	0	0	

DHCP Statistics

MAINTENANCE

Upgrade

GWN7806(P) Switches support manual upload firmware upgrade via a BIN file that can be downloaded from Grandstream Firmware page: <https://www.grandstream.com/support/firmware>

Upgrade Via Network is also supported by specifying the Firmware Server Path (For example: firmware.grandstream.com).

Upgrade

Current version: 1.0.1.6

Upgrade via Manual Upload

Upload Firmware File to Update: Supported file formats: bin

Upgrade via Network

Allow DHCP Option 43/160/66 to Override Server:

Firmware Upgrade Protocol:

Firmware Server Path:

HTTP/HTTPS Username:

HTTP/HTTPS Password:

Check/Download New Firmware at Bootup:

Scheduled Upgrade: Once enabled, the switch will automatically detect and upgrade within the scheduled time.

[Cancel](#) [OK](#) [Check for Updates](#)

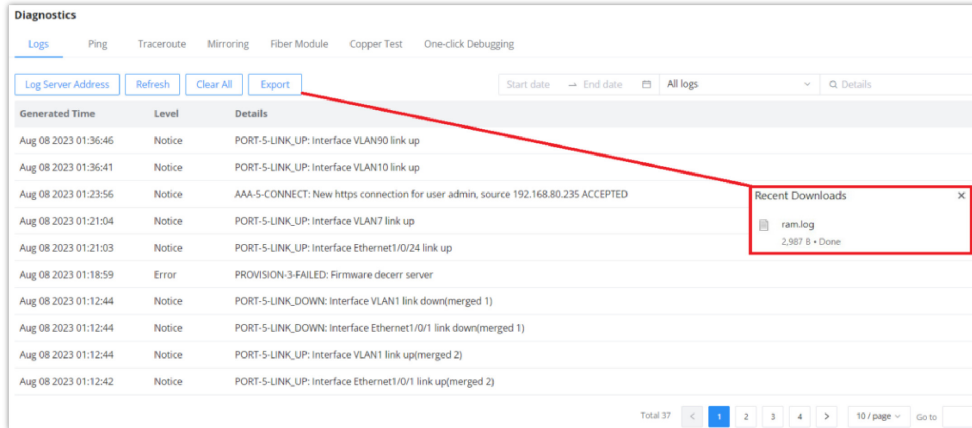
Upgrade

Diagnostics

GWN7806(P) Switches support many diagnostics tools that can help the user troubleshoot the issue and resolve it. These tools include Logs, Ping, Traceroute, Mirroring and Fiber Module.

Logs

This page lists all the generated Logs with details and level and generated time, also an option to export the list is available.

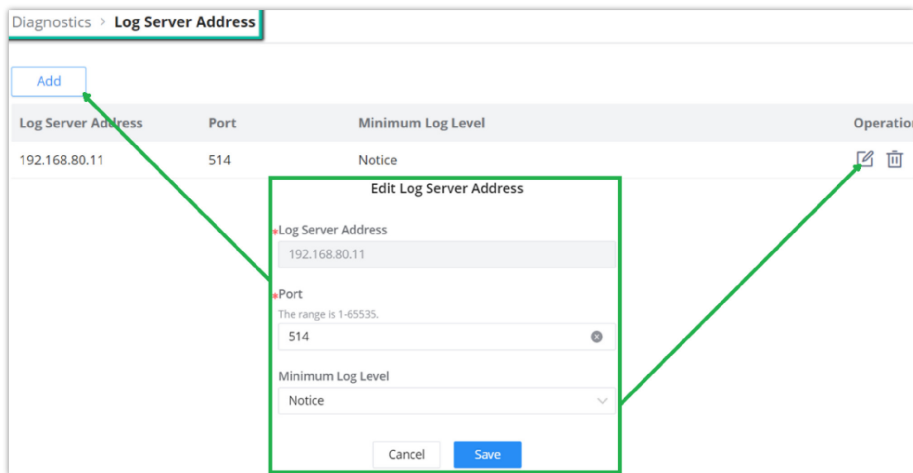


The screenshot shows the 'Diagnostics' interface with the 'Logs' tab selected. At the top, there are navigation tabs for 'Logs', 'Ping', 'Traceroute', 'Mirroring', 'Fiber Module', 'Copper Test', and 'One-click Debugging'. Below these are buttons for 'Log Server Address', 'Refresh', 'Clear All', and 'Export'. A search bar contains 'All logs' and a 'Details' search icon. The main area is a table with columns 'Generated Time', 'Level', and 'Details'. The table contains 11 log entries. A red box highlights the 'Export' button and a 'Recent Downloads' popup window showing a file named 'ram.log' (2,987 B) with a 'Done' status. A red arrow points from the 'Export' button to the popup.

Generated Time	Level	Details
Aug 08 2023 01:36:46	Notice	PORT-5-LINK_UP: Interface VLAN90 link up
Aug 08 2023 01:36:41	Notice	PORT-5-LINK_UP: Interface VLAN10 link up
Aug 08 2023 01:23:56	Notice	AAA-5-CONNECT: New https connection for user admin, source 192.168.80.235 ACCEPTED
Aug 08 2023 01:21:04	Notice	PORT-5-LINK_UP: Interface VLAN7 link up
Aug 08 2023 01:21:03	Notice	PORT-5-LINK_UP: Interface Ethernet1/0/24 link up
Aug 08 2023 01:18:59	Error	PROVISION-3-FAILED: Firmware decerr server
Aug 08 2023 01:12:44	Notice	PORT-5-LINK_DOWN: Interface VLAN1 link down(merged 1)
Aug 08 2023 01:12:44	Notice	PORT-5-LINK_DOWN: Interface Ethernet1/0/1 link down(merged 1)
Aug 08 2023 01:12:44	Notice	PORT-5-LINK_UP: Interface VLAN1 link up(merged 2)
Aug 08 2023 01:12:42	Notice	PORT-5-LINK_UP: Interface Ethernet1/0/1 link up(merged 2)

Diagnostics – Logs

Adding a Log Server Address to the logs to be sent to is also supported on the GWN7806(P) Switches.

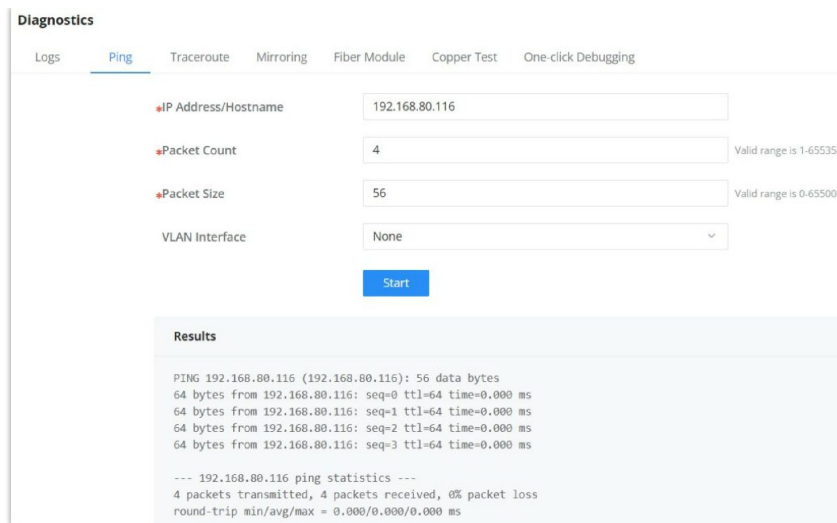


The screenshot shows the 'Diagnostics > Log Server Address' configuration page. It features an 'Add' button and a table with columns 'Log Server Address', 'Port', 'Minimum Log Level', and 'Operation'. The table contains one entry: '192.168.80.11', '514', and 'Notice'. A green box highlights the 'Add' button and the 'Edit Log Server Address' modal window. The modal window has fields for 'Log Server Address' (192.168.80.11), 'Port' (514), and 'Minimum Log Level' (Notice). A green arrow points from the 'Add' button to the modal, and another green arrow points from the 'Operation' column of the table to the modal's 'Save' button.

Log Server Address

Ping

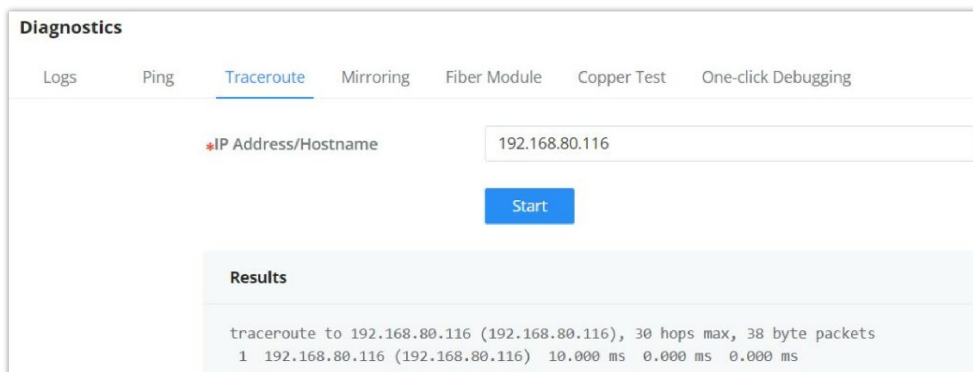
The user in this page can enter the IP Address or Hostname then click "Start", the results of the ping command will be shown below.



Ping

Traceroute

Another tool is Traceroute that shows the number of hops, and GWN7806(P) Switches enables the user to run Traceroute commands right from the Switches WEB UI.

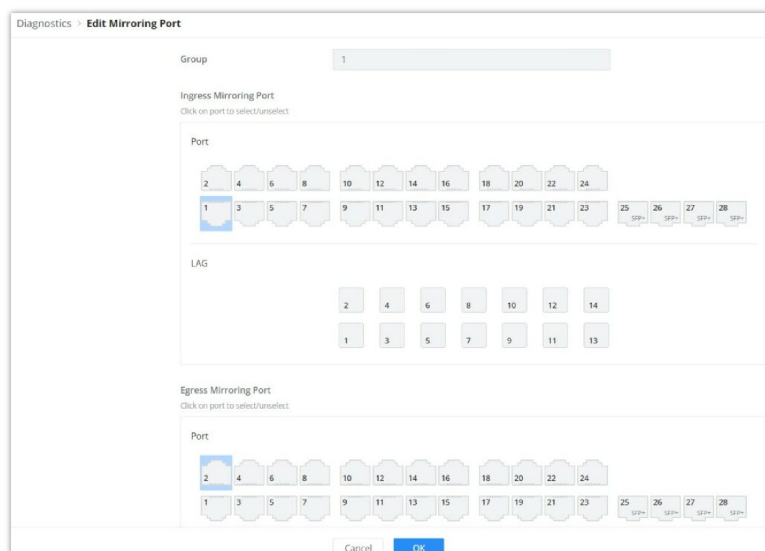


Traceroute

Port Mirroring

Mirroring refers to copying the packets from the specified source to the destination port. The specified source is called the mirroring source, the destination port is called the observing port, and the copied packet is called the mirroring packet.

Mirroring can make a copy of the original packet without affecting the normal processing of the original packet by the device, and send it to the monitoring device through the observation port to determine whether the service running on the network is normal.

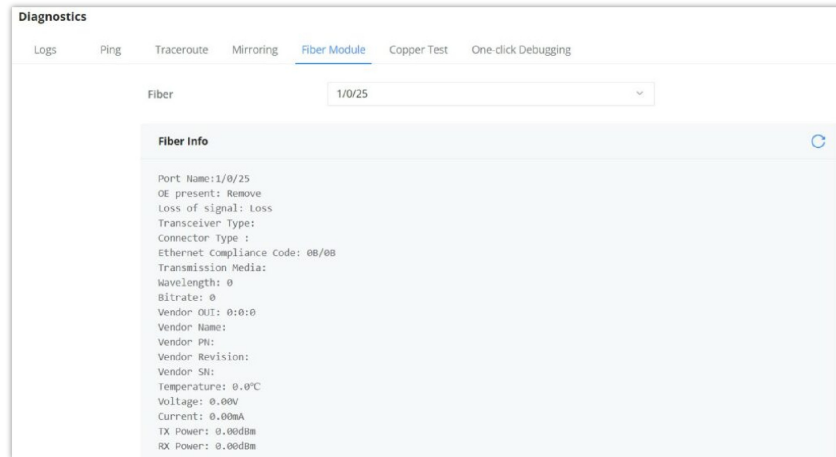


Port Mirroring

Fiber Module

This page provides the user with the information about the fiber module for each Port that supports it. Select the port from the drop-down list and click refresh icon.

Note: The information displayed on the optical module of each manufacturer is different.



Fiber Module

Copper Test

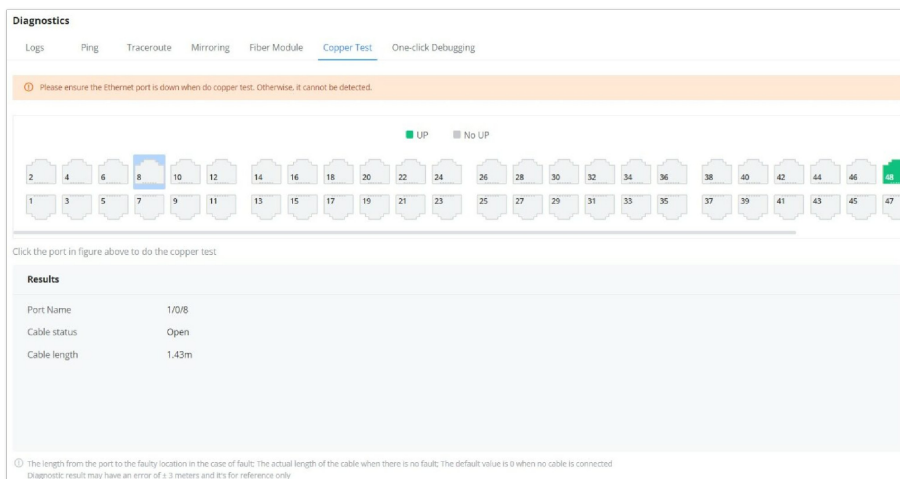
Copper test can detect whether the cable connected to the switch is faulty and the location of the fault. Using this function can assist in the daily engineering installation diagnosis .

Please navigate to **Web UI** → **Maintenance** → **Diagnostics page** → **Copper Test Tab**.

Note:

When performing cable detection, please ensure that the electrical port is not in the UP state, otherwise the detection result will not be available.

To perform the test simply click on the port, please refer to the figure below:



Copper Test

After the detection , the cable detection result is displayed as follows:

Cable Status: OK (normal), Open (open circuit), Short (short circuit) , Crosstalk (crosstalk) , Unknown (unknown).

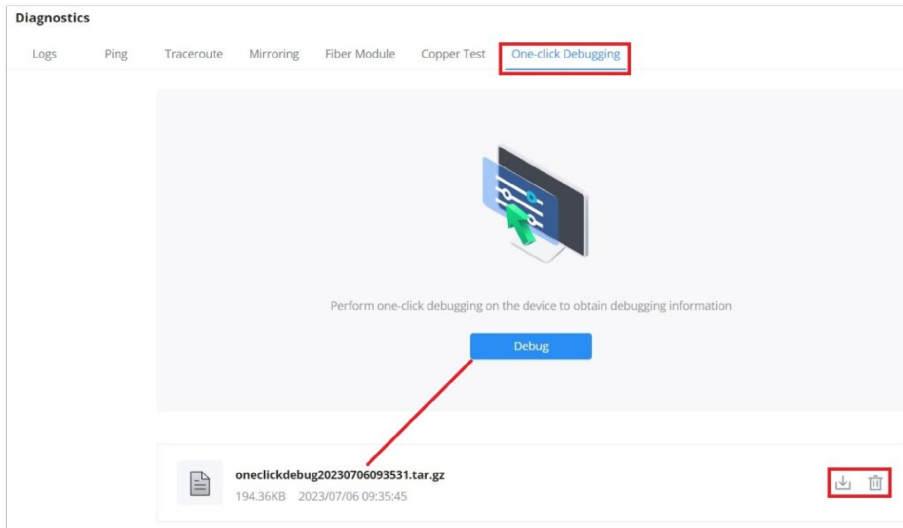
Cable Length:

- When there is a fault: it is the length from the port to the fault location.
- When there is no fault: it is the actual length of the cable.

One-click Debugging

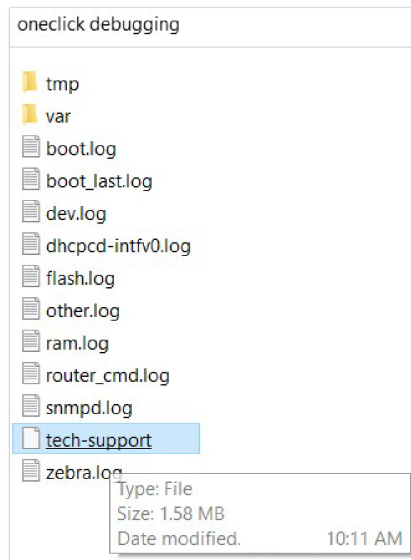
On GWN78xx switches, One-click debugging feature can help administrators or tech-support to quickly and easily get debugging information about the GWN switch in a matter of few minutes.

Please navigate to **Web UI** → **Maintenance** → **Diagnostics page** → **One-click Debugging tab**, then click on **"Debug"** button to start the debugging process.



One-click Debugging

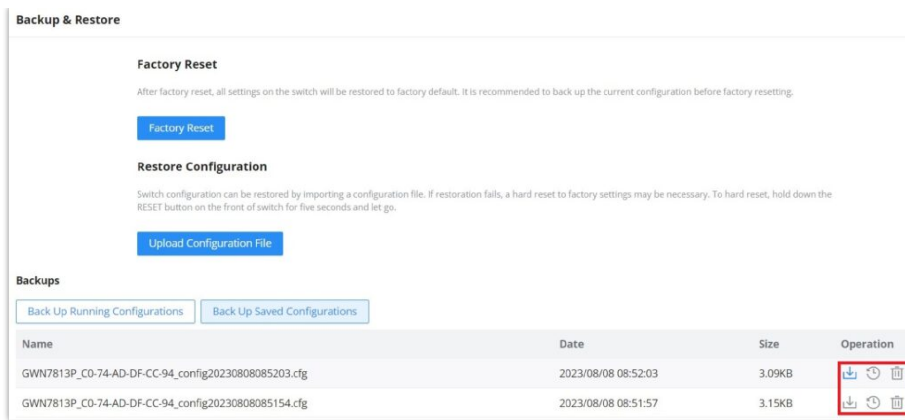
It's also possible to delete the generated file or download it locally to share it with tech-support for example. The folder contains many logs files and even a tech-support file that containing valuable information like the switch configuration etc.



One-click Debugging Folder

Backup and Restore

Click on "Factory Reset" button to reset the GWN7806(P) Switch back to default settings, or restore to previously saved backup by uploading a configuration file, these configuration files can be used as a way to back up the device running configuration or saved configuration.



Backup and Restore

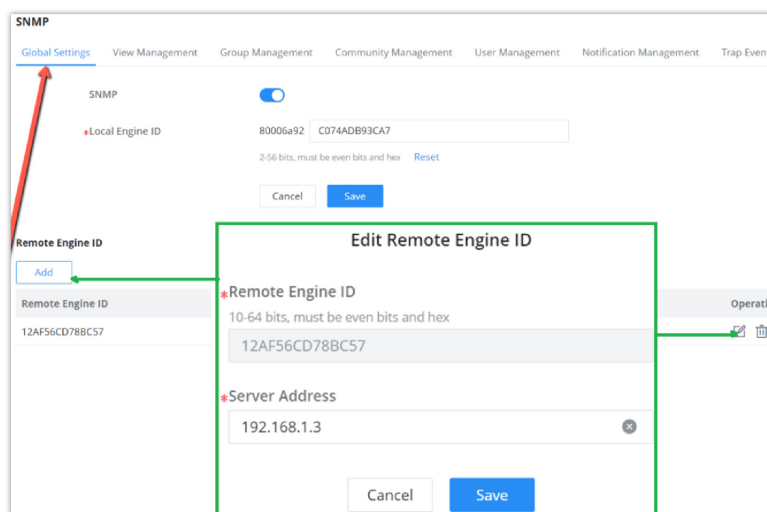
SNMP

Network Management Protocol (SNMP) is an "Internet-standard protocol for managing devices on IP networks". Devices that typically support SNMP include routers, switches, servers, workstations, printers, modem racks and more. SNMP is used mostly in network management systems to monitor network-attached devices for conditions that warrant administrative attention. SNMP is a component of the Internet Protocol Suite as defined by the Internet Engineering Task Force (IETF). It consists of a set of standards for network management, including an application layer protocol, a database schema, and a set of data objects. An SNMP-managed network consists of three key components:

- Managed device
- Agent – software which runs on managed devices
- Network management station (NMS) – software which runs on the manager

A managed device is a network node that implements an SNMP interface that allows unidirectional (read-only) or bidirectional (read and write) access to node-specific information. Managed devices exchange node-specific information with the NMSs. Sometimes called network elements, the managed devices can be any type of device, including, but not limited to, routers, access servers, switches, bridges, hubs, IP telephones, IP video cameras, computer hosts, and printers. An agent is a network-management software module that resides on a managed device. An agent has local knowledge of management information and translates that information to or from an SNMP-specific form. A network management station (NMS) executes applications that monitor and control managed devices. NMSs provide the bulk of the processing and memory resources required for network management. One or more NMSs may exist on any managed network.

Global settings page allows the user to enable the SNMP function with the Local Engine ID or add a Remote Engine ID.



SNMP -Global Settings

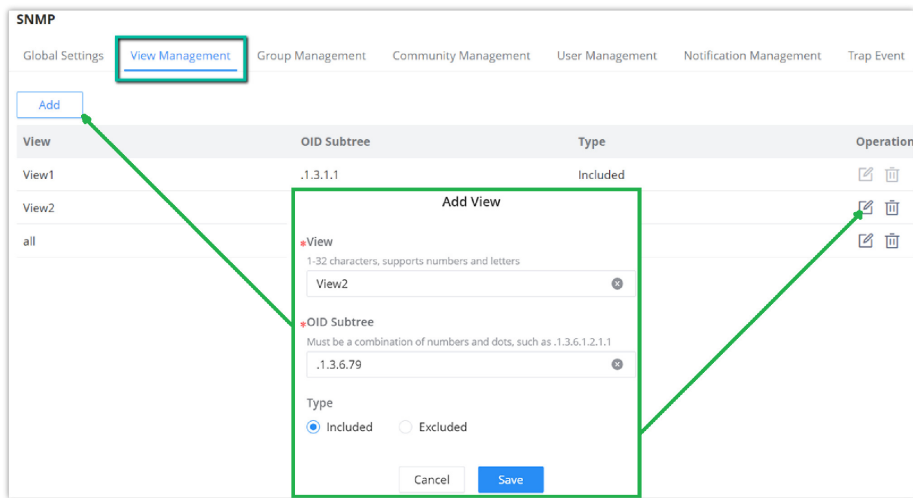
SNMP	Select whether to enable SNMP.
Local Engine ID	Set the engine ID of the local SNMP entity or click "Reset" to restore to the initial value. <i>Note: The default is 8000 A59Dxxxxxxx, where xxxxxxxx is the device MAC address by default, which can be modified by the user . It is expressed in hexadecimal , and the length is limited between 2 and 56</i>

	<i>characters. The number of characters must be an even number .</i>
Edit Remote Engine ID	
Remote Engine ID	Set the engine ID of the SNMP management side , and the remote user is established under the remote engine. The input length is limited to 10-64 characters, expressed in hexadecimal , and the number of characters must be an even number.
Server Address	Set the address of the network management station server, support input of Hostname and IP address (including IPv4 and IPv6), and need to meet the requirements of various types of address formats, otherwise an error message is required.

SNMP Global Settings

View Management

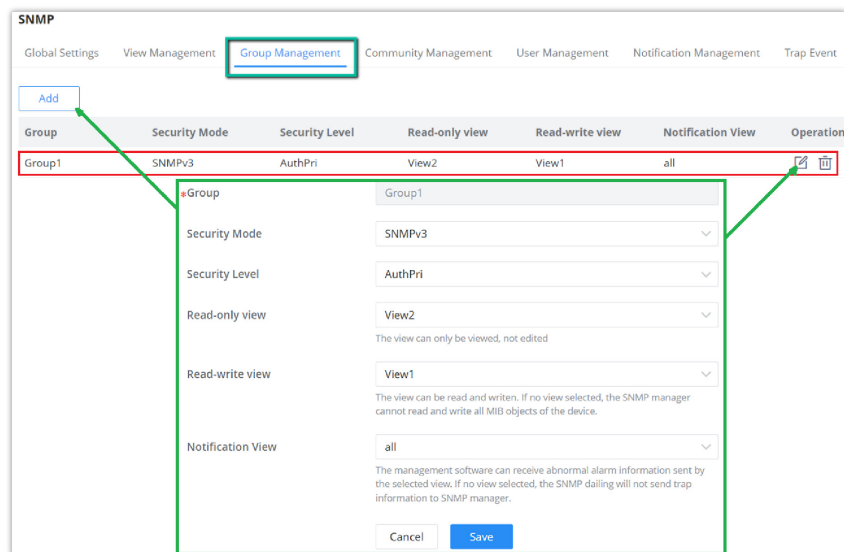
This page allows the network administrator to create MIB views (Management information base) and then include or exclude OID (Object Identifier) in a view.



SNMP – View Management

Group Management

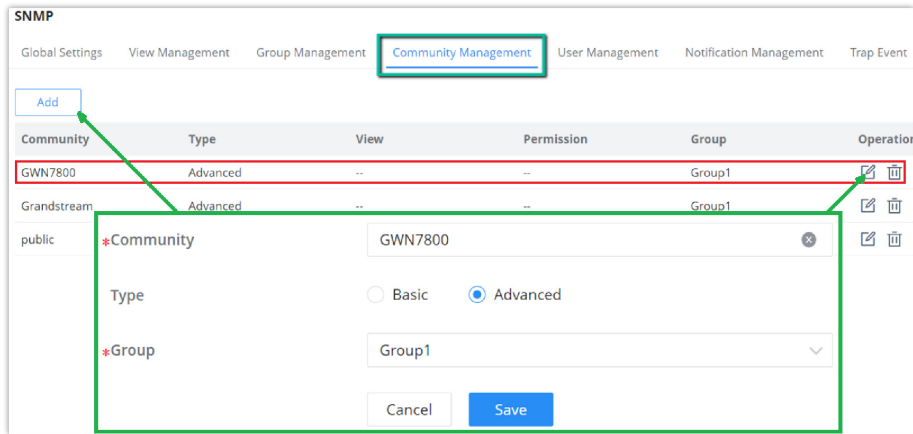
This page allows the network administrator to group SNMP users and assign different authorization and access privileges.



SNMP – Group Management

Community Management

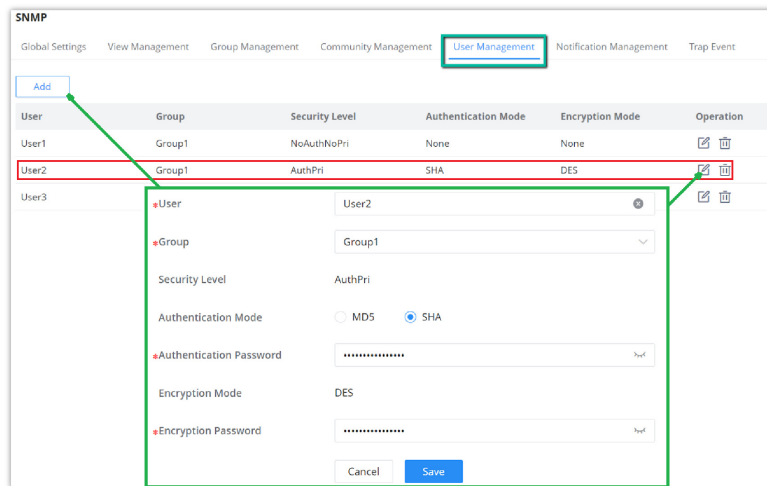
This page allows a user to add/remove multiple communities of SNMP.



SNMP – Community Management

SNMP User Management

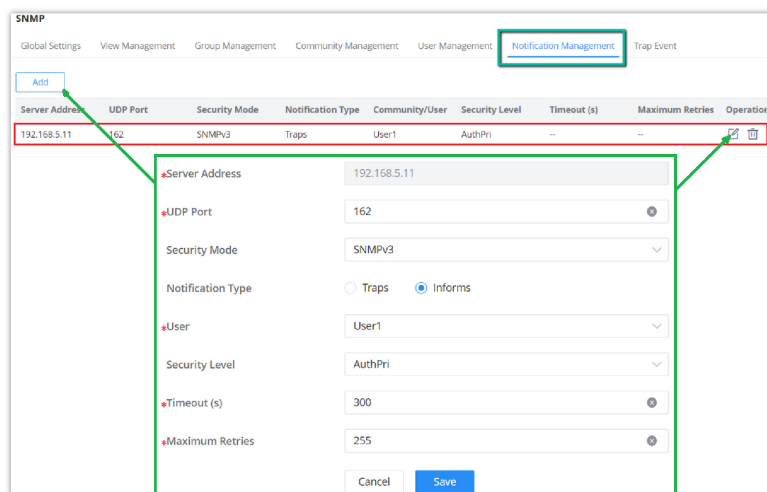
This page allows a user to configure SNMPv3 user profile.



SNMP – User Management

Notification Management

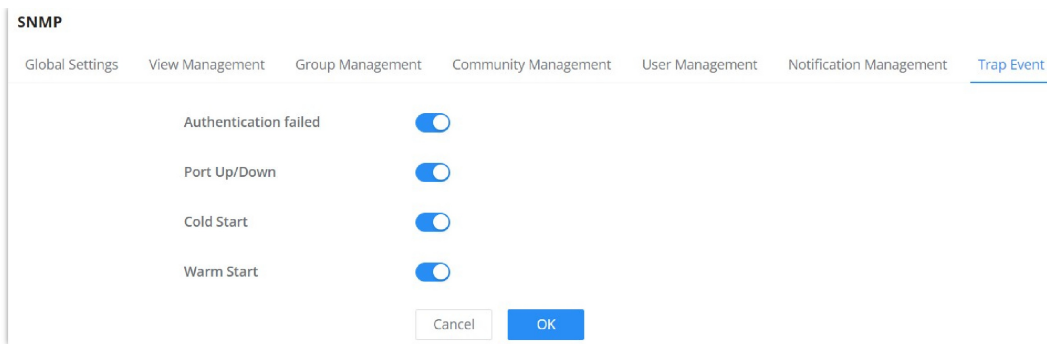
This page allows a user to configure a host to receive SNMPv1/v2/v3 notification.



SNMP – Notification Management

Trap Event

This page allows a user to add or delete SNMP trap receiver IP address and community name.



SNMP – Trap Event

RMON

RMON (Remote Monitoring) based on SNMP (Simple Network Management Protocol) architecture, functions to monitor the network. RMON is currently a commonly used network management standard defined by Internet Engineering Task Force (IETF), which is mainly used to monitor the data traffic across a network segment or even the entire network so as to enable the network administrator to take the protection measures in time to avoid any network malfunction. In addition, RMON MIB records network statistics information of network performance and malfunction periodically, based on which the management station can monitor network at any time effectively. RMON is helpful for network administrator to manage the large-scale network since it reduces the communication traffic between management station and managed agent.

Note:

 Please enable [SNMP>Global Settings>SNMP](#) first before RMON takes effect

RMON Statistics

Ethernet statistics function (corresponding to the statistics group in the RMON MIB) : The system collects basic statistics of each network being monitored. The system will continuously count the traffic of a certain network segment and the distribution of various types of packets, or the number of error frames of various types , the number of collisions , etc. The number of data packets , the number of broadcast and multicast packets, the number of received bytes, the number of received packets, etc.

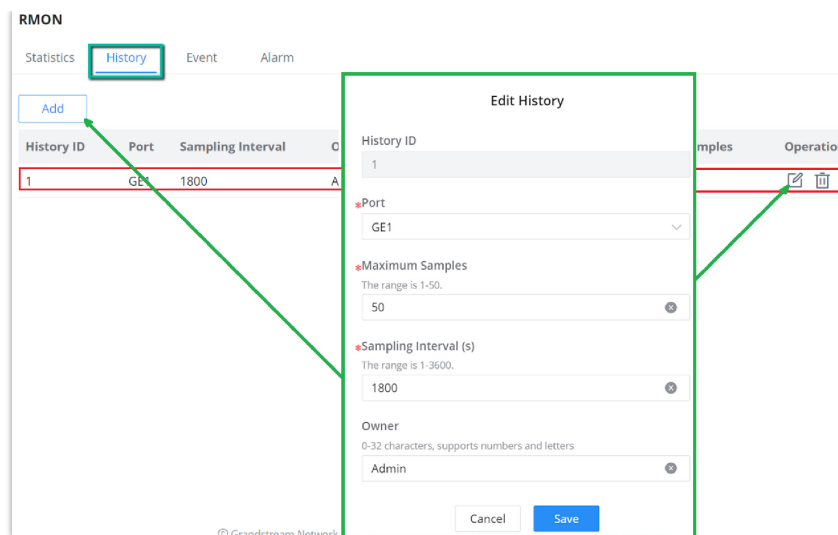
Port	Received Bytes	Drop Events	Received Packets	Broadcast Packets	Multicast Packets	CRC & Align Errors	Undersize Packets	Operation
1/0/1	14294925	0	99520	5450	9731	0	0	
1/0/2	0	0	0	0	0	0	0	
1/0/3	0	0	0	0	0	0	0	
1/0/4	0	0	0	0	0	0	0	
1/0/5	0	0	0	0	0	0	0	
1/0/6	0	0	0	0	0	0	0	
1/0/7	0	0	0	0	0	0	0	
1/0/8	0	0	0	0	0	0	0	
1/0/9	0	0	0	0	0	0	0	
1/0/10	0	0	0	0	0	0	0	

RMON – Statistics

RMON History

The system will periodically collect statistics on various traffic information , including bandwidth utilization, number of error packets and total number of packets based on the History ID.

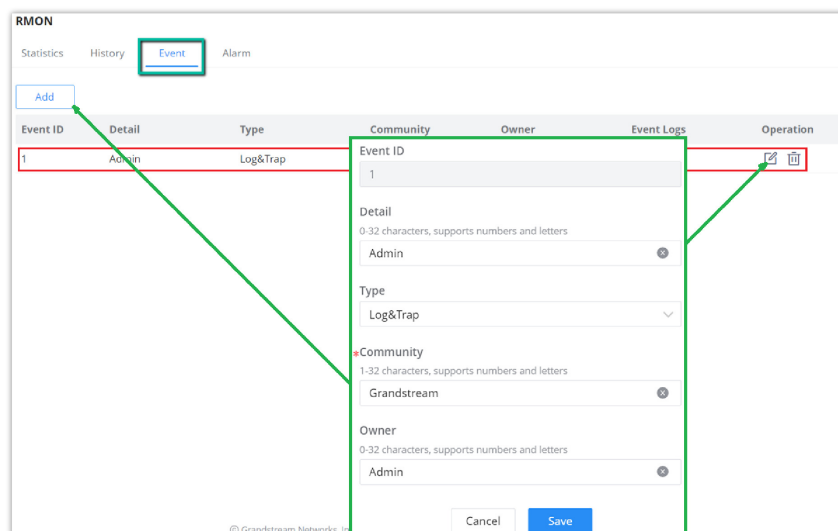
Click on “Add” button to create a History ID specifying the Port as well.



RMON – History

RMON Event

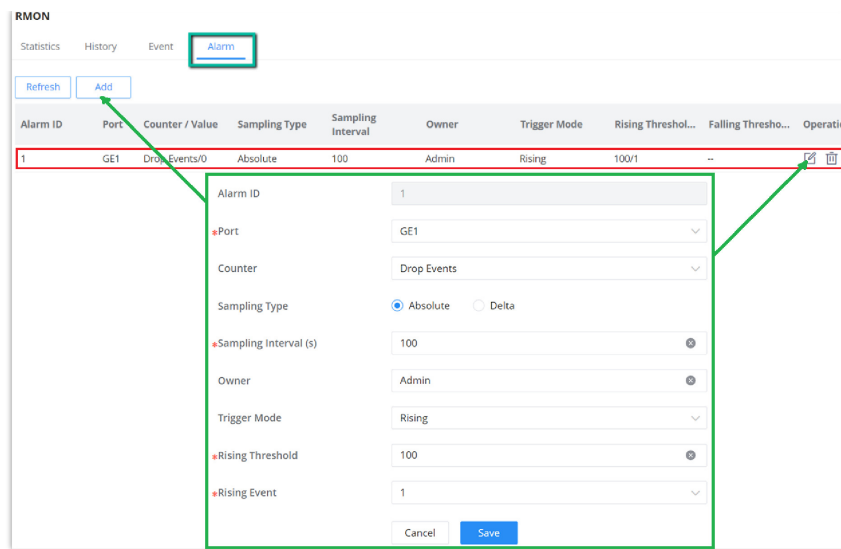
The event group controls the events and prompts from the device, and provides all events generated by the RMON Agent. When an event occurs, it can record logs or send Trap to the network management station.



RMON Event

RMON Alarm

The system monitors the specified alarm variable. After pre-defining a set of thresholds and sampling time for the specified alarm, the system will obtain the value of the specified alarm variable according to the defined time period. When the value of the alarm variable is greater than or equal to the upper threshold, an upper alarm event will be triggered. When the value of the alarm variable is less than or equal to the lower threshold, a lower alarm event is triggered.



RMON – Alarm

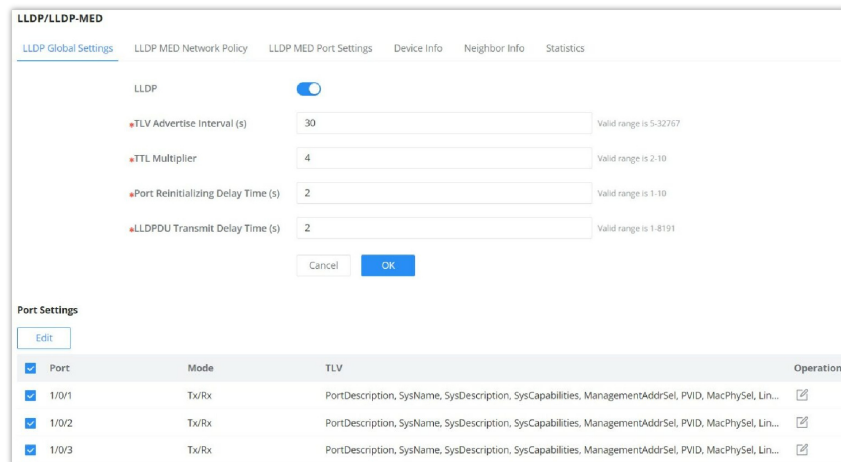
LLDP/LLDP MED

LLDP/LLDP MED is a one-way protocol, there are no request/response sequences. Information is advertised by stations implementing the transmit function, and is received and processed by stations implementing the receive function.

LLDP MED is an enhancement to LLDP that provides additional functionality to support media devices. LLDP MED features include: enabling network policy advertisement and discovery for real-time applications (such as voice and/or video);

LLDP Global Settings

This page allows a user to set general settings for LLDP including enabling LLDP and other parameters .



LLDP Global Settings

More configuration can adjusted per port (GE1 to GE10).

LLDP Global Settings > **Edit Port Settings**

Port: 1/0/1

Mode: Tx/Rx

TLV

Basic TLV

Port Description TLV System Name TLV

System Description TLV System Capabilities TLV

Management Address TLV

IEEE 802.1TLV

Port VLAN ID TLV VLAN Name TLV

IEEE 802.3TLV

MAC/PHY Configuration/Status TLV Link Aggregation TLV

Maximum Frame Size TLV Power via MDI TLV

Cancel **OK**

LLDP Port Settings

LLDP MED Network Policy

This page allows the network administrator to set MED (Media Endpoint Discovery) network policy. Click on **"Add"** button to add a Network Policy or toggle ON **Auto Voice Network Policy** (Voice VLAN has to be configured as well).

LLDP/LLDP-MED

LLDP Global Settings **LLDP MED Network Policy** LLDP MED Port Settings Device Info Neighbor Info Statistics



*Fast Report Count: 3 Valid range is 1-10

Auto Voice Network Policy:

Cancel **OK**

Network Policy

Add **Delete**

<input checked="" type="checkbox"/>	Policy ID	Application	VLAN	VLAN Tag	CoS	DSCP	Operation
<input checked="" type="checkbox"/>	1	Voice	7	Tagged	6	43	 

LLDP MED Network Policy

To add a Network Policy, click on **"Add"** button or click on **"Edit"** icon under Operation column to edit.

LLDP MED Network Policy > **Edit Network Policy**

Policy ID: 1

Application: Voice

*VLAN: 7 Valid range is 0-4095

VLAN Tag: Tagged

CoS: 6

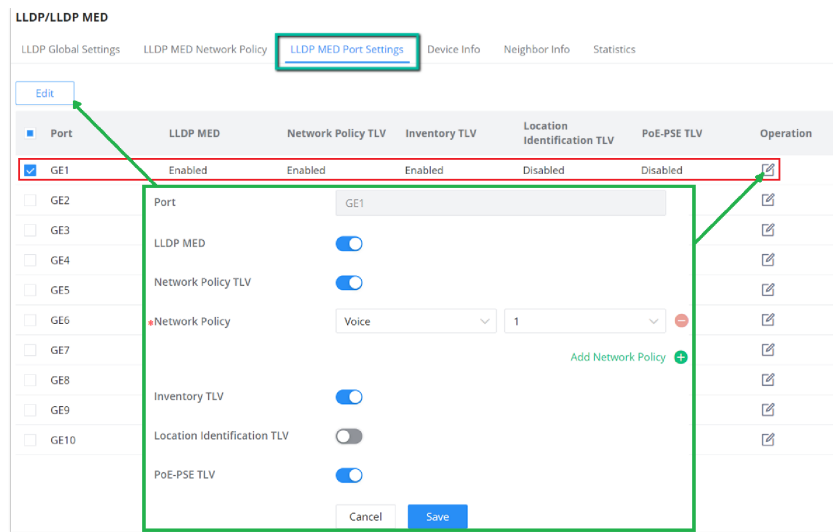
DSCP: 43

Cancel **OK**

Add/Edit Network Policy

LLDP MED Port Settings

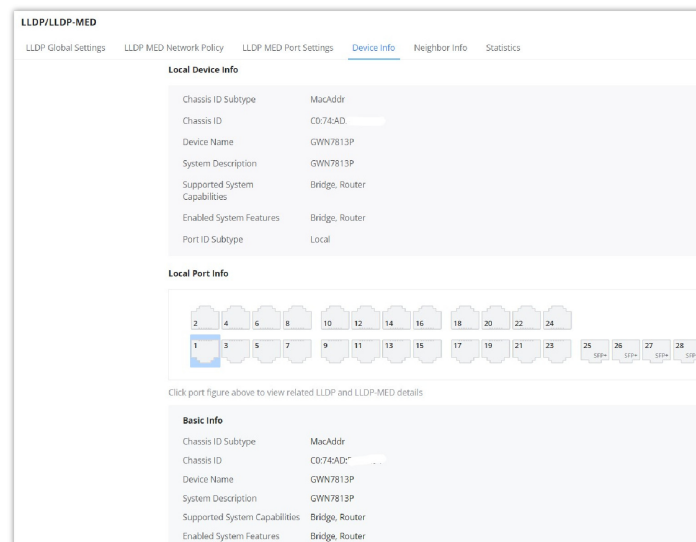
The user can configure LLDP MED Settings for each port in this page.



LLDP MED Port Settings

LLDP Device Info

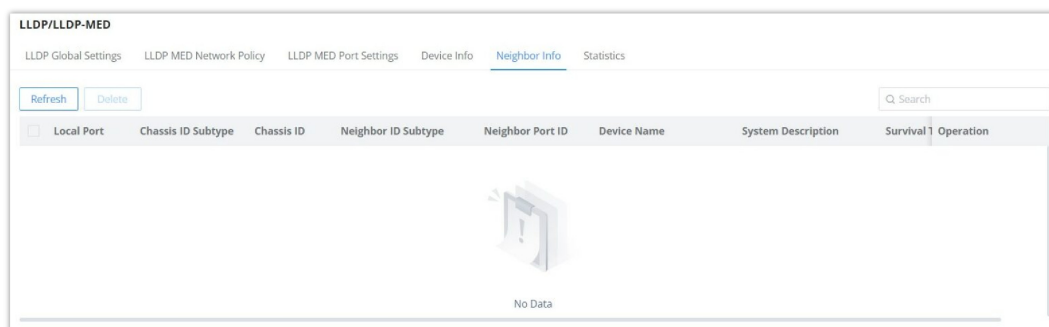
This page displays information for LLDP Local Device connected to each port. Click on the port to view related LLDP information about that port.



LLDP Device Info

Neighbor Info

This page lists the neighbors obtained on the switch ports. Click on "Refresh" button to update the list.



LLDP Neighbor Info

LLDP Statistics

View the LLDP statistics of the local device through this feature. Click on "Refresh" to update the list.

LLDP/LLDP-MED

LLDP Global Settings LLDP MED Network Policy LLDP MED Port Settings Device Info Neighbor Info **Statistics**

Global Statistics

Insertions	1
Delete	1
Drops	0
Age-Outs	0

[Refresh](#) [Clear](#)

Port Statistics

[Refresh](#) [Clear](#)

Port	Total Packets Transmitted	Received Frames			Received TLV		Timed-out Neighbors	Operation
		Total	Discarded	Error	Discarded	Unrecognized		
<input checked="" type="checkbox"/> 1/0/1	862	0	0	0	0	0	0	
<input checked="" type="checkbox"/> 1/0/2	0	0	0	0	0	0	0	
<input checked="" type="checkbox"/> 1/0/3	0	0	0	0	0	0	0	
<input checked="" type="checkbox"/> 1/0/4	0	0	0	0	0	0	0	
<input checked="" type="checkbox"/> 1/0/5	0	0	0	0	0	0	0	

LLDP Statistics

Energy Efficient Ethernet (EEE)

EEE or Energy Efficient Ethernet helps on reducing the power consumption on interfaces like GWN78xx switches Ethernet port, it achieves this by using power only during data transmission.

Navigate to **Web UI** → **Maintenance** → **Energy Saving Management**, select a port to edit then enable 802.3 EEE.

Edit Port ✕

Port

1/0/1

802.3 EEE

Cancel
OK

Energy Efficient Ethernet

SYSTEM

Basic Settings

Basic settings page allows the user to configure the name of the switch, location and also configure time settings like the NTP Server and time zone, it's also possible to configure a reboot time schedule.

Please navigate to **Web UI** → **System** → **Basic Settings** page.

Basic Settings

Basic Info

*Device Name: GWN7801P Switch 1-64 alphanumeric characters and special characters .@_

System Location: Default 1-64, support Chinese, numbers, letters and special characters .@_

System Contact: Default 1-64, support Chinese, numbers, letters and special characters .@_

Time Settings

Date & Time: Manual Automatic (NTP Server)

System Time: 2023-07-08 04:58:46

*NTP Server: pool.ntp.org

Time Zone: (UTC+08:00) Beijing, Chongqing, Hong Kong, Urumqi

Scheduled Reboot

Reboot Time: Disabled

Cancel OK

Basic Settings

Access Control

In this page we can enable/disable SSH, Telnet and SSH Remote Access, and also configure the inactive session timeout (the range is from 15 seconds to 1440) which is how much time before the GWN78xx switch will logout automatically. Also we can configure here the GWN Manager server address and port manually.

Please navigate to **Web UI** → **System** → **Access Control** page.

Access Control

Web Service Management

*Inactive Session Timeout (min): 15

Telnet:

SSH:

Cancel OK

Manager Settings

Manager Settings:

*Manager Server Address: 192.168.5.58

*Manager Server Port: 8443

Allow DHCP Option 43 to Override:

Cancel OK

SSH Remote Access

*Password: login Enter the password to access

SSH Remote Access

Access Control

User Management

There are three levels of users, namely administrator, operator and monitor. The administrator authenticates and authorizes users who log in to the switch according to management need where each user has different permissions and passwords.

1. Administrator

- Each device has one and only one administrator.
- The highest privileges, can execute any command.
- The username admin cannot be changed, only the password can be changed.

- Support adding, deleting operator and monitor.

2. Operator

- Added by administrator, there can be multiple accounts as Operators.
- The second highest authority, can execute all commands except the administrator’s key operations and important mandatory commands
- Can’t change the username, only password.
- Support adding, deleting Monitor users.

Note:

All features of admin are allowed except setting management IP address and factory reset.

3. Monitor

- Multiple Monitors are possible with the permission of an Administrator or Operator.
- The lowest authority, can only view switch status and statistics without any execution and configuration authority.
- Can’t change the username, only password.

Note:

Can only view information.

Click on “Add” button to add new user then specify the password the user level (Operator or Monitor).

The screenshot displays the 'User Management' interface. On the left, a table lists existing users:

Username	Level
<input type="checkbox"/> admin	Administrator
<input checked="" type="checkbox"/> User1	Monitor
<input type="checkbox"/> Devs	Operator
<input type="checkbox"/> Technician	Monitor

On the right, the 'Add User' dialog box is open, showing the following fields:

- Username:** 1-64 characters, supports numbers, letters and special characters which contains _@#&. Value: Technician
- Password:** 8-64 characters, must contain two of digits, letters and special characters. Value: [Redacted]
- Confirm Password:** 8-64 characters, must contain two of digits, letters and special characters. Value: [Redacted]
- User Level:**
 - Operator: All features except setting management IP address and factory reset of admin are allowed.
 - Monitor: Can only view information.

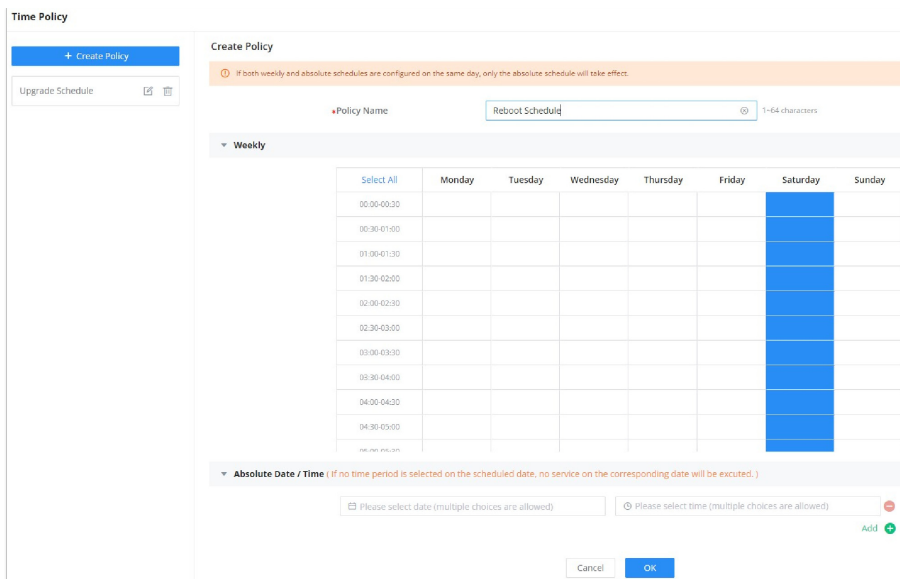
Buttons for 'Cancel' and 'OK' are at the bottom of the dialog.

User Management

Time Policy

Time policy page helps to create schedules, for example Office working hours, Upgrade schedule or Reboot schedule.

To create a schedule, Please navigate to **Web UI** → **System** → **Time Policy** page, then click on “**Create Policy**” button, there are weekly schedules or absolute Date/Time schedules, for weekly schedules please select from the table the hours and days and as for absolute Date/Time select the days from the drop-down calendars and times from the drop-down menu. Please refer to the figure below.



Time Policy

Note:

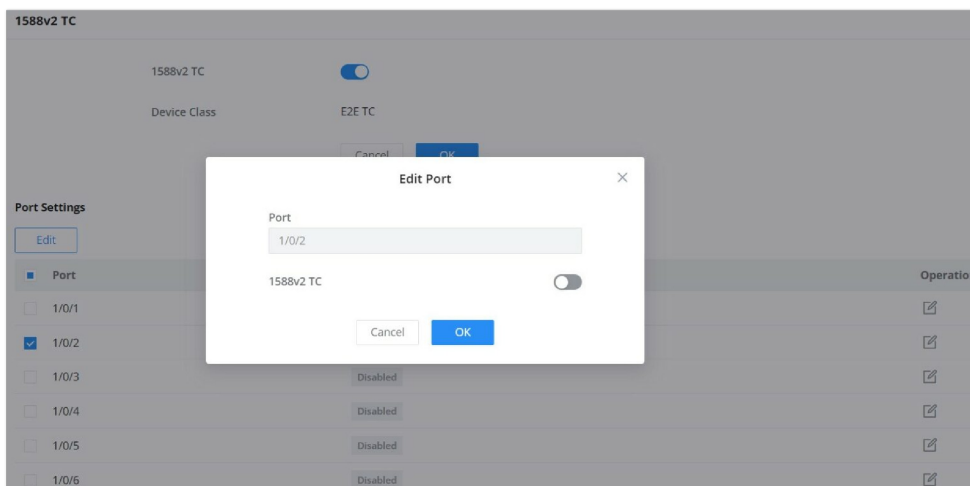
- If both weekly and absolute schedules are configured on the same day, only the absolute schedule will take effect.
- If no time period is selected on the scheduled date, no service on the corresponding date will be executed.

1588v2 TC

IEEE 1588v2 is a protocol for synchronizing clocks, enabling accurate time between nodes in a network.

A transparent clock or TC is a type of clock used in IEEE 1588v2 networks and it uses a Precision Time Protocol (PTP) messages to accurately calculate the time.

E2E or (End-to-End) transparent clock measures the delay at each network element between the master and slave clocks.



1588v2 TC

Note:

This feature is still in Beta, Web only supports E2T TC.

CHANGE LOG

This section documents significant changes from previous versions of the GWN7806(P) switches user manuals. Only major new features or major document updates are listed here. Minor updates for corrections or editing are not documented here.

Version 1.0.1.6

- This is the initial release.