Grandstream Networks, Inc.

GWN780x(P) L2+

User Manual

WELCOME

The GWN780x series are Layer 2+ managed network switches that allow 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 Snooping for network performance optimization, and comprehensive security capabilities against potential attacks. The PoE models provide smart dynamic PoE output to power IP phones, IP cameras, Wi-Fi access points, and other PoE endpoints. The GWN7800 series can be managed in a number of ways, including the local web user interface of the GWN7800 series switch. The series is also supported by GWN.Cloud, Grandstream's cloud and on-premise Wi-Fi management platform. The enterprise-grade GWN780x series are the ideal managed network switches for small-to-medium businesses.

PRODUCT OVERVIEW

Technical Specifications

	GWN7801	GWN7801P	GWN7802	GWN7802P	GWN7803	GWN7803P
Network Protocol	IPv4, IPv6, IEEE 802.3, IEEE 802.3i, IEEE 802.3u, IEEE 802.3ab, IEEE 802.3z, IEEE 802.3x, IEEE 802.3af/at, IEEE 802.1p, IEEE 802.1Q, IEEE 802.1w, IEEE 802.1d, IEEE 802.1s					
Gigabit Ethernet Ports	8		16		24	
Gigabit SFP Ports	2		4			
Console	1					
Number of PoE Ports	/	8	/	16	/	24
Integrated Power Supply	30W	150W	30W	270W	30W	400W
Max Output Power per PoE Port	/	30W	/	30W	/	30W
Max Total PoE Output Power	/	120W	/	240W	/	360W
PoE Standards	/	IEEE 802.3af/at	/	IEEE 802.3af/at	/	IEEE 802.3af/at
Auxiliary Ports	1x Reset Pinhole					
Forwarding Mode	Store-and-forward					
Total non-blocking throughput	10Gbps		20Gbps		28Gbps	

Switching Capability	20Gbps		40Gbps		56Gbps	
Forwarding Rate	14.88M packets per second		29.76M packets per second		41.66M packets per second	
Packet Buffer	4.1MB					
Switching	● 8K static, dynamic and filtering MAC addresses ● 4K VLANs, port-based VLAN, IEEE 802.1Q VLAN tagging, voice VLAN ● VLAN virtual interface ● 8 link aggregation groups ● Spanning tree, 16 instances for MSTP					
Multicast	IGMP Snooping, MLD Snooping					
QoS/ACL	● Auto detection and prioritization of voice/video/RTP/SIP/other latency-sensitive packets ● Port priority ● Priority mapping ● Queue scheduling, including SP, WRR ● Traffic shaping ● Rate limit ● 1.5K ACL for Ethernet, IPv4 and IPv6					
DHCP	Option 82, 60,160 and 43					
Maintenance	CPU and memory monitoring, SNMP, RMON, LLDP&LLDP-MED, backup and restore, syslog, alert, diagnostics including Ping, Traceroute, port mirroring					
Security	● 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 proctection ● Kensington Security Slot (Kensington Lock) support					
Mounting	Desktop, wall-mount, or rack-mount (rack-mount brackets included)					
LEDs	1x tri-color LED for device tracking and status indication					
	10x green LEDs for data ports	10x green LEDs for data ports, 8x yellow-color LEDs for PoE ports	20x green LEDs for data ports	20x green LEDs for data ports, 16x yellow-color LEDs for PoE ports	28x green LEDs for data ports	28x green LEDs for data ports, 24x yellow-color LEDs for PoE ports
Fan	/	/	/	1	/	2
Environmental	Operation: 0°Cto 45°C, humidity 10-90% RH(Non-condensing) Storage: -10°C to 60°C, humidity: 5% to 95%(Non-condensing)					
Dimensions	300mm(L)*175mm(W)*44(H)		440mm(L)*200mm(W)*44mm(H)			

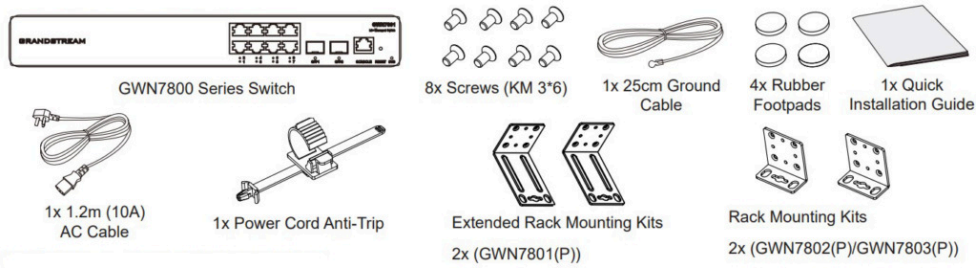
Unit Weight(TBD)	1.8Kg	2Kg	2.6Kg	3Kg	2.7Kg	3.3Kg
Package Content	Switch, 1x 1.2m(10A) AC Cable, 1x Ground Cable, 4x Rubber Feet, 2x Lug Ear		Switch, 1x 1.2m(10A) AC Cable, Rack-mounting Standard Brackets, 1x Ground Cable, 4x Rubber Feet, 2x Lug Ear			
Compliance	FCC, CE, RCM, IC, UKCA					

GWN780x Technical Specifications

INSTALLATION

Before deploying and configuring the GWN780x 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 GWN780x switch.

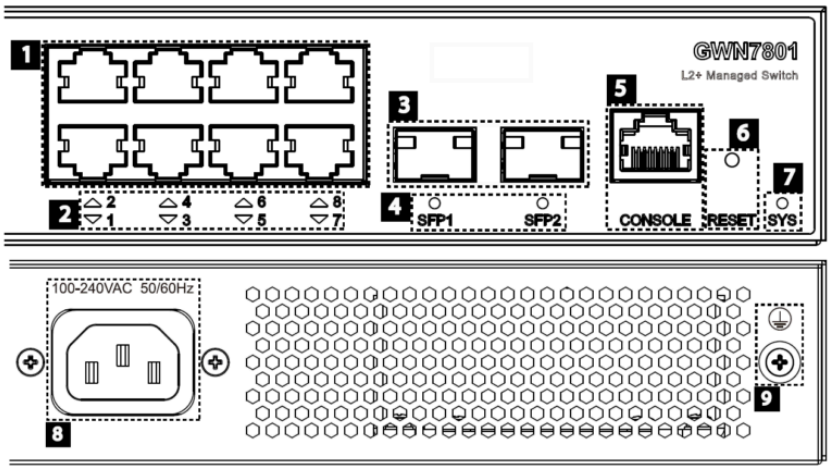
Package Contents



GWN780x Package Contents

GWN780x Ports

- **GWN7801/GWN7801P**



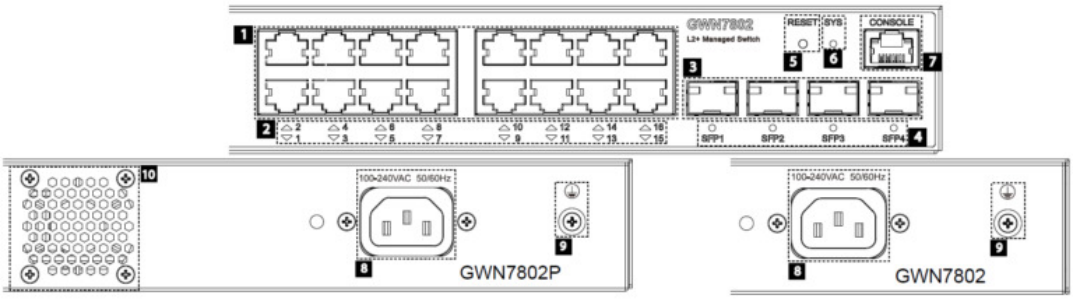
GWN7801/GWN7801P Ports

No.	Port & LED	Description
1	Port 1-8	8x Ethernet RJ45 (10/100/1000Mbps), used for connecting terminals. Note: GWN7801P Ethernet ports support PoE and PoE+.
2	1-8	Ethernet ports' LED indicators

3	**Port SFP1/2**	2x 1000Mbps SFP ports
4	**SFP 1/2**	SFP ports' LED indicators
5	**CONSOLE**	1x Console port, used for connecting managing PC
6	**RESET**	Factory Reset pinhole. Press for 5 seconds to reset factory default settings
7	**SYS**	System LED indicator
8	**100-240 VAC 50-60Hz**	Power socket
9		Lightning protection grounding post

GWN7801(P) Ports and LEDs

- **GWN7802/GWN7802P**

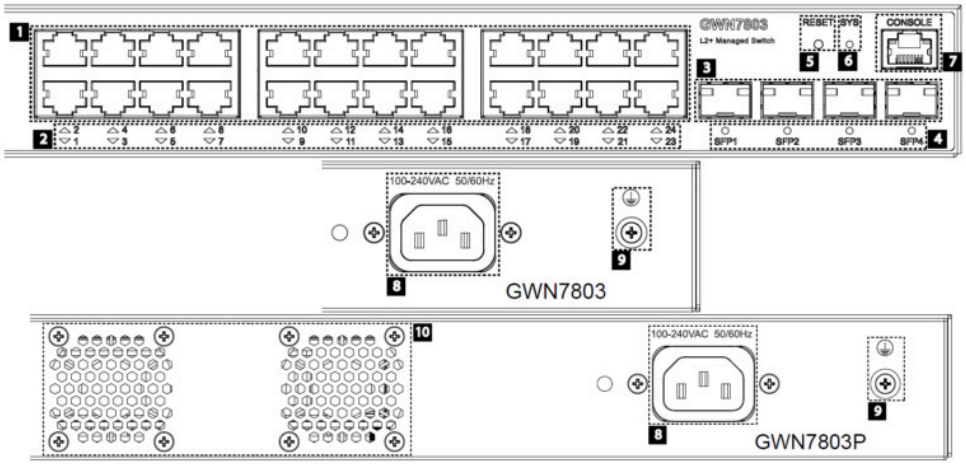


GWN7802/GWN7802P Ports

No.	Port & LED	Description
1	**Port 1-16**	16x Ethernet RJ45 (10/100/1000Mbps), used for connecting terminals. Note: GWN7802P Ethernet ports support PoE and PoE+.
2	**1-16**	Ethernet ports' LED indicators
3	**Port SFP1/2/3/4**	4x 1000Mbps SFP ports
4	**SFP 1/2/3/4**	SFP ports' LED indicators
5	**RESET**	Factory Reset pinhole. Press for 5 seconds to reset factory default settings
6	**SYS**	System LED indicator
7	**CONSOLE**	1x Console port, used for connecting managing PC
8	**100-240 VAC 50-60Hz**	Power socket
9		Lightning protection grounding post
10	**Fan**	1x Fan

GWN7802(P) Ports and LEDs

- **GWN7803/GWN7803P**

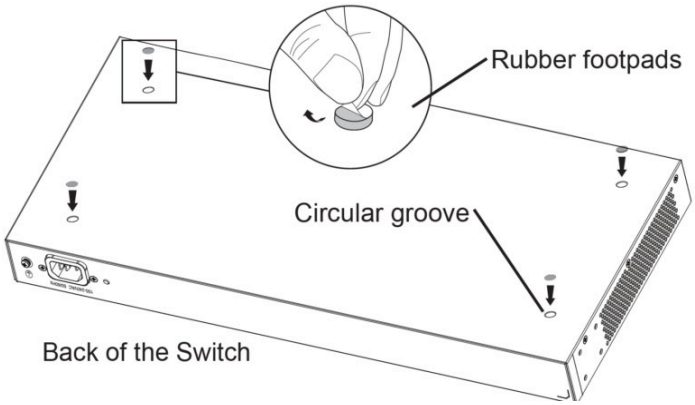


GWN7803/GWN7803P Ports

No.	Port & LED	Description
1	**Port 1-24**	24x Ethernet RJ45 (10/100/1000Mbps), used for connecting terminals. Note: GWN7803P Ethernet ports support PoE and PoE+.
2	**1-24**	Ethernet ports' LED indicators
3	**Port SFP1/2/3/4**	4x 1000Mbps SFP ports
4	**SFP 1/2/3/4**	SFP ports' LED indicators
5	**RESET**	Factory Reset pinhole. Press for 5 seconds to reset factory default settings
6	**SYS**	System LED indicator
7	**CONSOLE**	1x Console port, used for connecting managing PC
8	**100-240 VAC 50-60Hz**	Power socket
9	⏚	Lightning protection grounding post
10	**Fan**	2x Fan

GWN7803(P) Ports and LEDs

Install on the Desktop



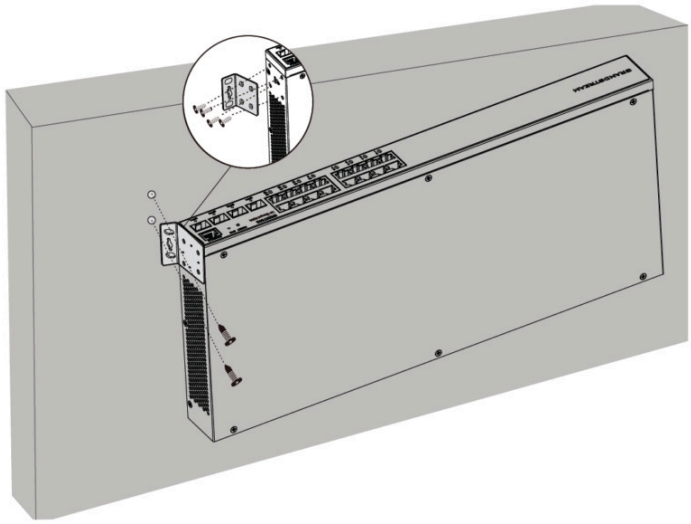
GWN780x(P) Desktop Installation

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 the Wall

Note:

GWN7801(P) require the Extended Rack Mounting Kits



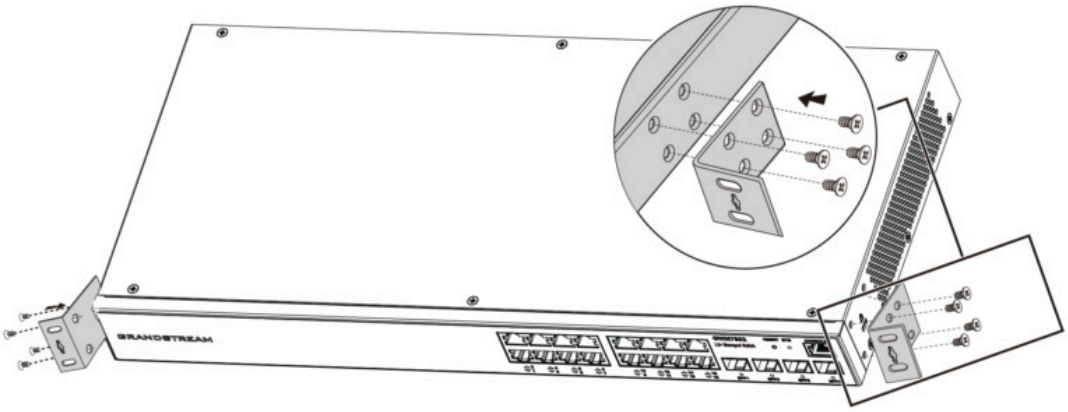
GWN780x(P) Wall Installation

1. Use the matching screws (KM 3*6) to fix the two L-shaped rack-mounting kits (rotated 90°) on both sides of switch.
2. Stick the switch port up and horizontally on the selected wall, mark the position of the screw hole on the L-shaped rack-mounting kits with a marker. Then, drill a hole at the marked position with an impact drill, and drill the expansion screws(prepared by yourself) into the drilled hole in the wall.
3. Use a screwdriver to tighten the screws (prepared by yourself) that have passed through the L-shaped rack-mounting kits to tighten the expansion solenoids to ensure that the switch is firmly installed on the wall.

Install on a 19" Standard Rack

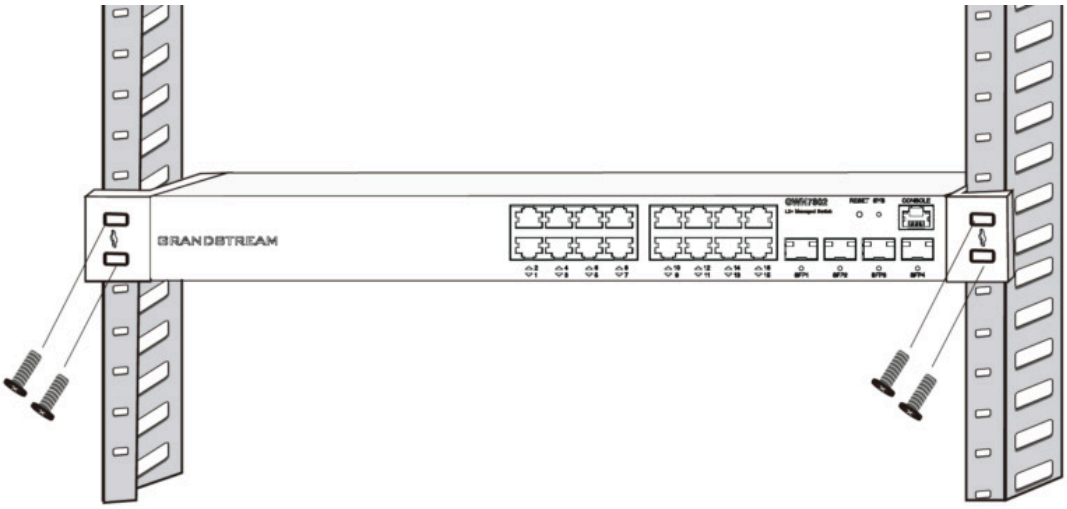
Note:

GWN7801(P) require the Extended Rack Mounting Kits



GWN780x(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).

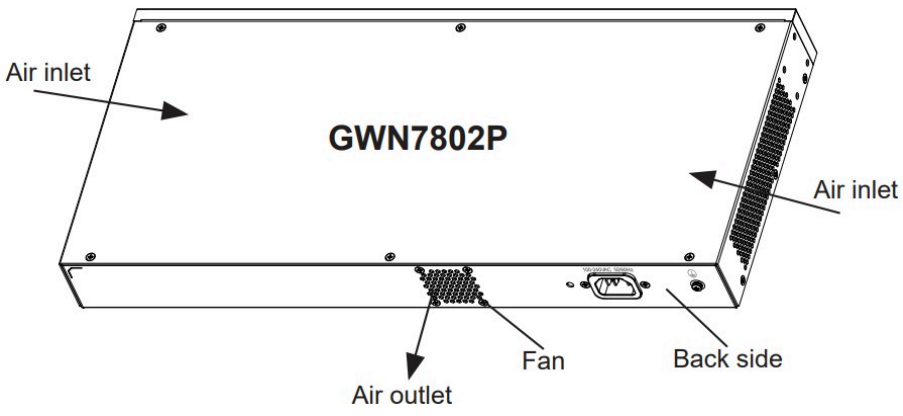


GWN780x(P) Standard Rack Installation

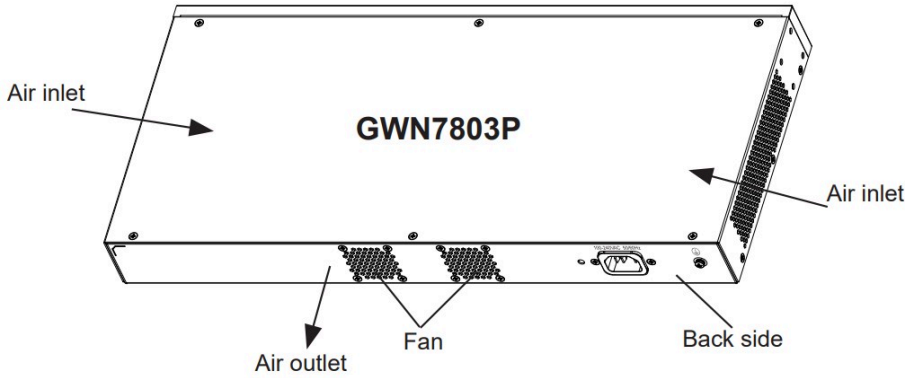
3. Place the switch in a proper position in the rack and support it by the bracket.
4. Fix the L-shaped rack-mounting to the guide grooves at both ends of the rack with screws(prepared by yourself) to ensure that the switch is stably and horizontally installed on the rack.

Note:

To avoid high temperatures and keep the device cool, sufficient space should be left around the switch for heat dissipation. The air inlet of the switch cannot face or be close to the air outlet of other devices.



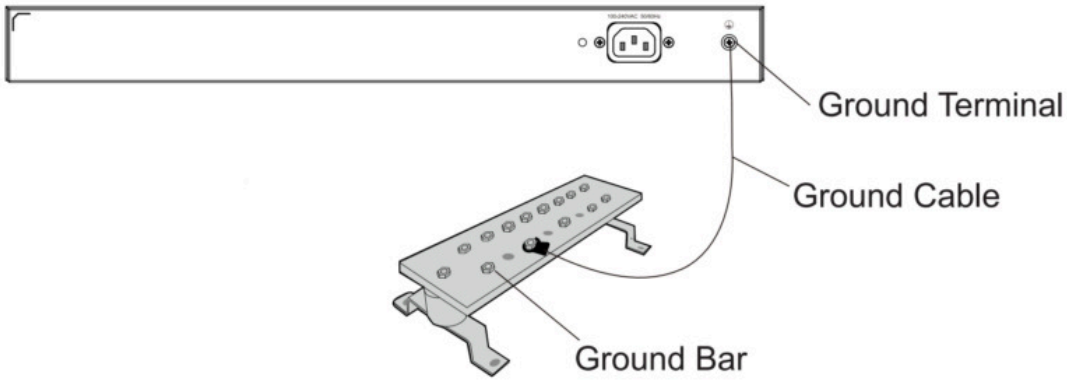
GWN7802P – Air inlet/outlet



GWN7803P – Air inlet/outlet

Powering and Connecting GWN780x(P)

- **Grounding the Switch**

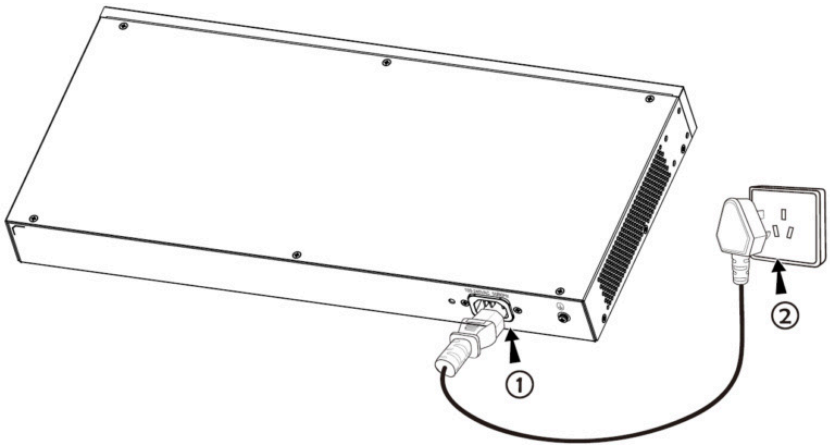


Grounding the Switch

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**

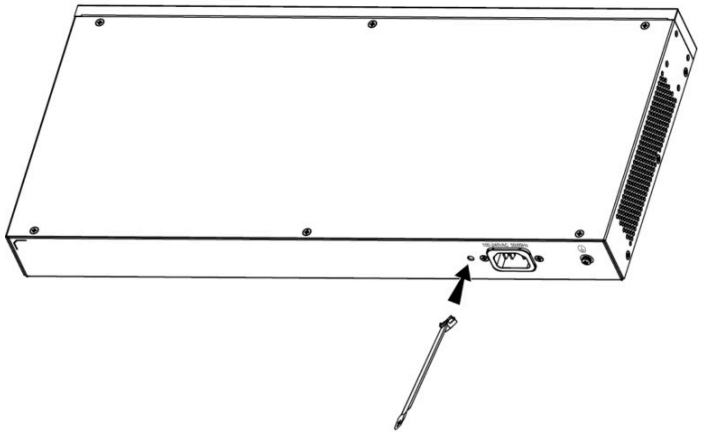
Connect the power cable and the switch first, then connect the power cable to the power supply system of the equipment room



Powering on the Switch

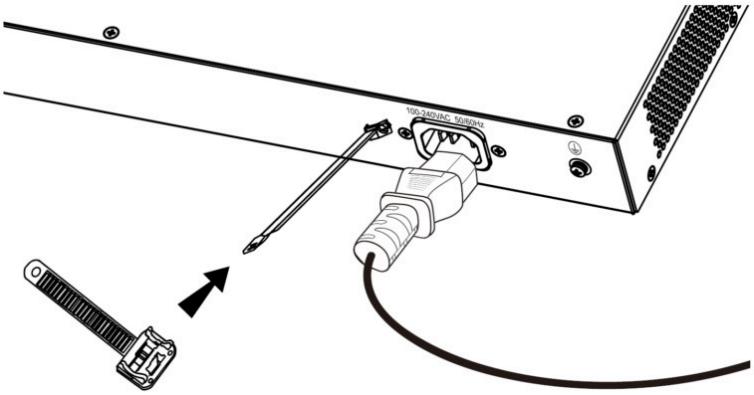
- **Connecting Power Cord Anti-Trip (Optional)**

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 (Optional) – part 1

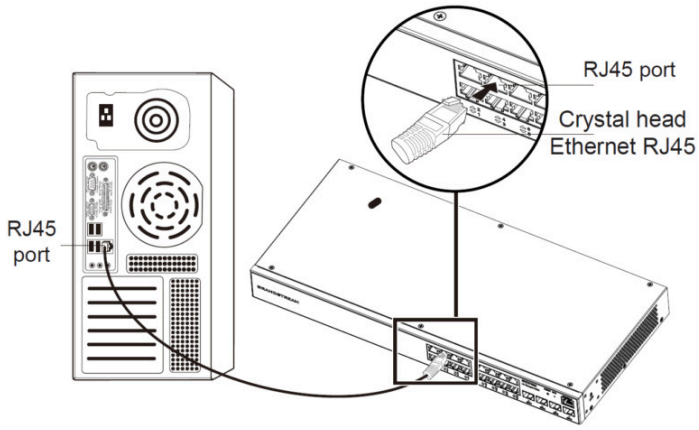
1. Place the smooth side of the fixing strap towards the power outlet and insert it into the hole on the side of it.



Connecting Power Cord Anti-Trip (Optional) – part 2

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**

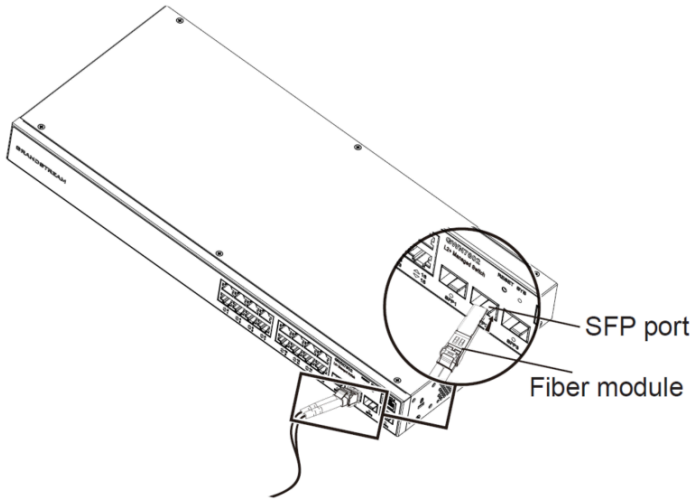


Connect to RJ45 Port

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.

- **Connect to SFP Port**

The installation process of the fiber module is as follows:



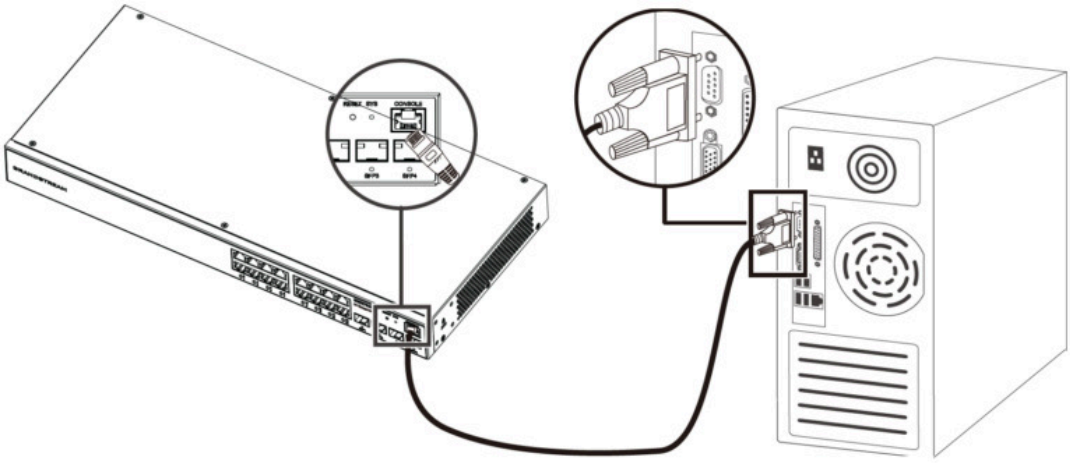
Connect to SFP Port

1. Grasp the fiber module from the side and insert it smoothly along the switch SFP port slot until the module is in close contact with the switch.
2. When connecting, pay attention to confirm the Rx and Tx ports of SFP fiber module. Insert one end of the fiber into the Rx and Tx ports correspondingly, and connect the other end to another device.
3. 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.

Notes:

- Please select the optical fiber cable according to the module type. The multi-mode module corresponds to the multi-mode optical fiber, and the single-mode module corresponds to the single-mode optical fiber.
- Please select the same wavelength optical fiber cable for connection.
- Please select an appropriate optical module according to the actual networking situation to meet different transmission distance requirements.
- The laser of the first-class laser products is harmful to eyes. Do not look directly at the optical fiber connector.

- **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 GWN780x(P) L2+ Managed Network Switch complies with FCC/CE and various safety standards. The GWN780x(P) power adapter is compliant with the UL standard. Use the universal power adapter provided with the GWN780x(P) package only. The manufacturer's warranty does not cover damages to the device caused by unsupported power adapters.

Warranty

If GWN780x(P) L2+ 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 GWN780x(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	• **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

GWN780x(P) LED Indicators

Access & Configure

Note:

If no DHCP server is available, the GWN780x(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 GWN7800 switch).

> **Note:**
>
> The baud rate needs to be set to 115200.

Login Remotely using SSH

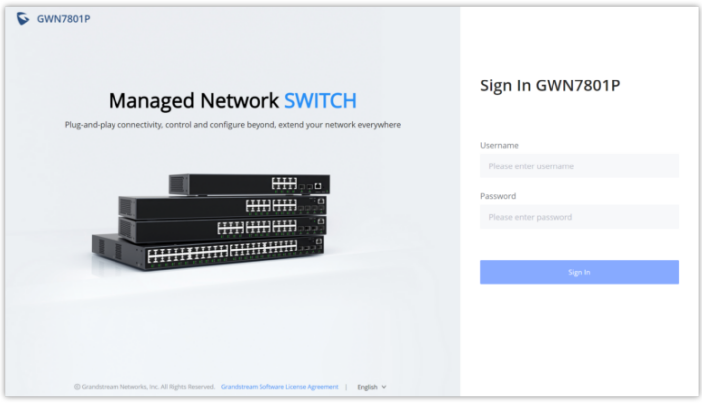
1. Enter **“cmd”** in PC/Start.
2. Enter **ssh <gwn7800_IP>** in the cmd window.
3. Enter the default username and password to login. (The default administrator username is “admin” and the default random password can be found at the sticker on the GWN7800 switch).

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 GWN780x(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 IE, Mozilla Firefox, or Google Chrome.



GWN780x(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://<gwn7800_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 GWN7800 switch).

CLI Access

In addition to the web-based configuration, the GWN780x series can also be configured using a Command Line Interface (CLI). For detailed instructions on using the CLI, please refer to the GWN78xx CLI User Guide.

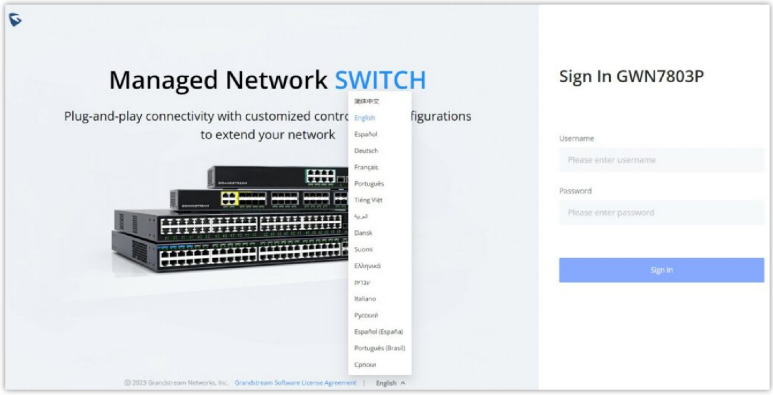
> **Note:**

The command line supports up to 2000 characters.

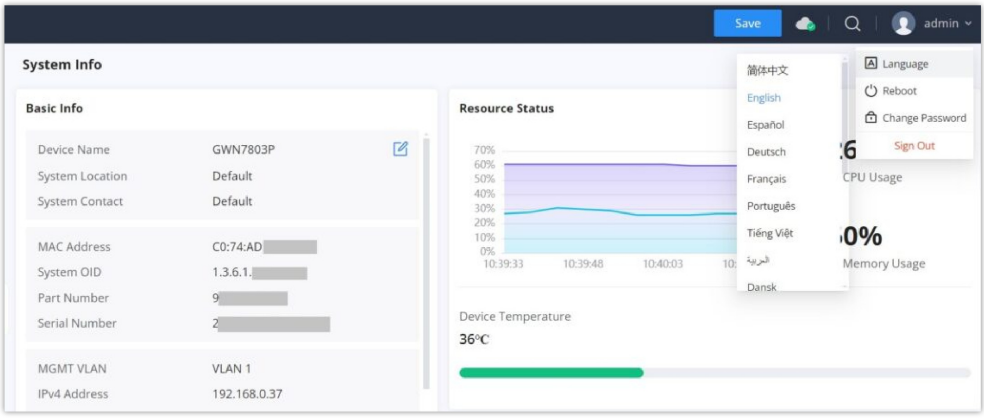
WEB GUI Languages

The GWN7800 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.



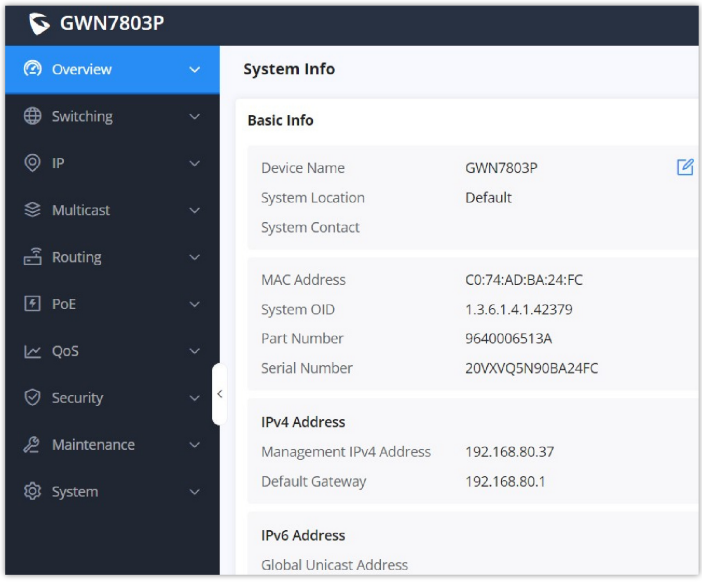
Web GUI Languages – Login Page



WEB GUI – Start page

WEB GUI Configuration

GWN780x web GUI includes 10 main sections to configure and manage the switch and check the connection status.

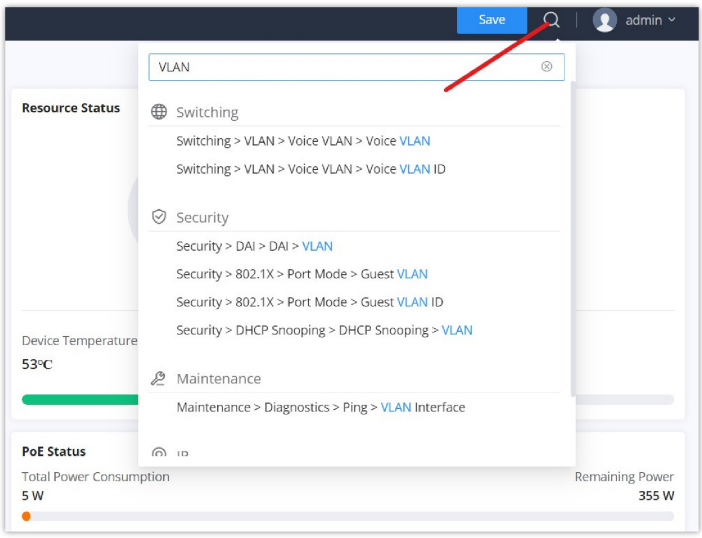


WEB GUI Configuration

Search

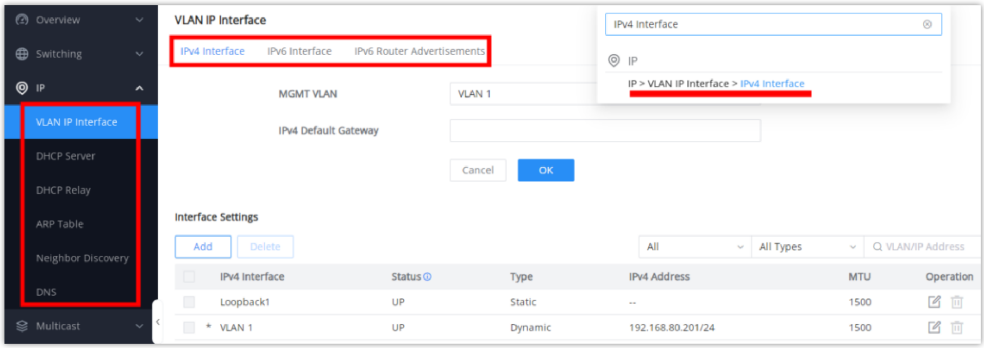
In case it's hard to go through every single section, GWN780x(P) Switches have search functionality to help the user find the right configuration, settings or parameters, etc.

On the top of the page, there is a search icon, the user can click on it and then enter the keyword relevant to his search, then he will get all the possible locations of that keyword.



Search – part 1

It's also possible to search through menus and sub-menus, and once the user clicks on the search result, they will jump directly to the specified page, please see the figure below:



Search – part 2

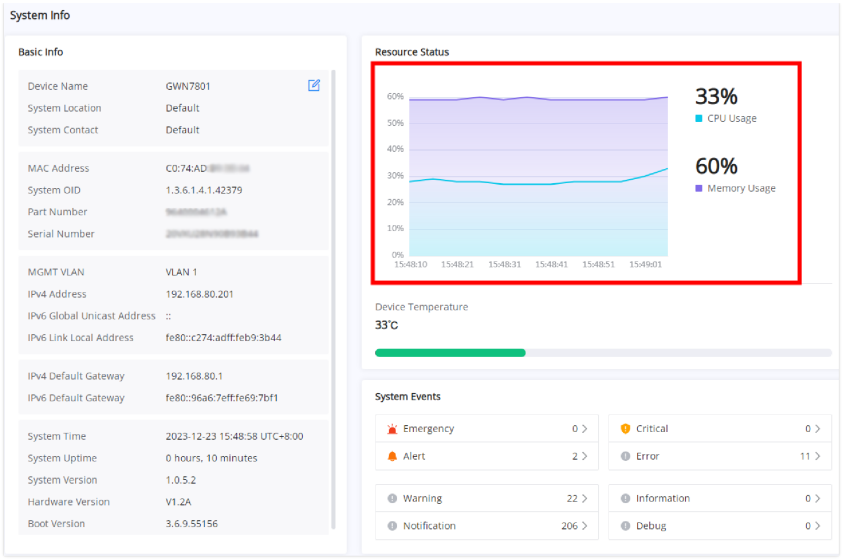
OVERVIEW

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 GWN780x(P) system and ports status for easy monitoring.

System Info

System Info is the first page after a successful login to the GWN780x(P) Web Interface. It provides an overall view of the GWN780x(P) Switch information presented in a Dashboard style for easy monitoring including basic info, Resources Status, PoE Status (only PoE models), System Events and Fan (only for supported models).

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



System Info page

Basic Info	Displays Device and System general information that includes (Device name, MAC Address, Default Gateway, System Time, System Version etc.)
Resource Status	Displays real-time CPU and memory usage also supports viewing the historical information of CPU and memory, and helps to check the problem of excessive CPU and memory usage.
PoE Status	Shows the Total Power Consumption and the remaining Power in Watt. ***Note:*** *Available only for PoE models.*
System Events	Diplays the total number of events for each category (Emergency, Alert, Warning etc). ***Note:*** *Clicking on any events category will redirect you to the Diagnostics page for further details.*
Fan	Displays the fans operation status and speed. ***Note:*** *it's only available for devices with fans like GWN7802P and GWN7803P.*

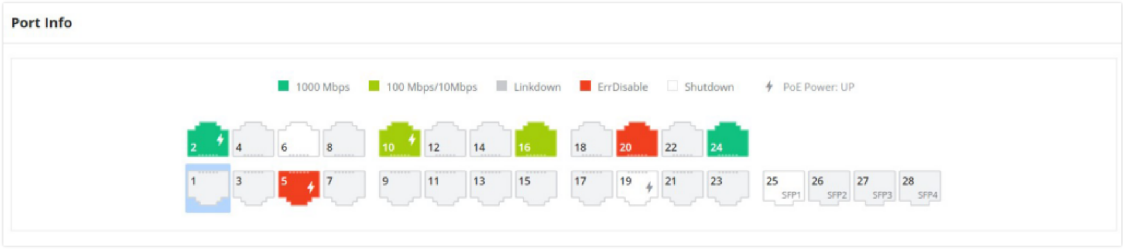
System Info page

Port Info

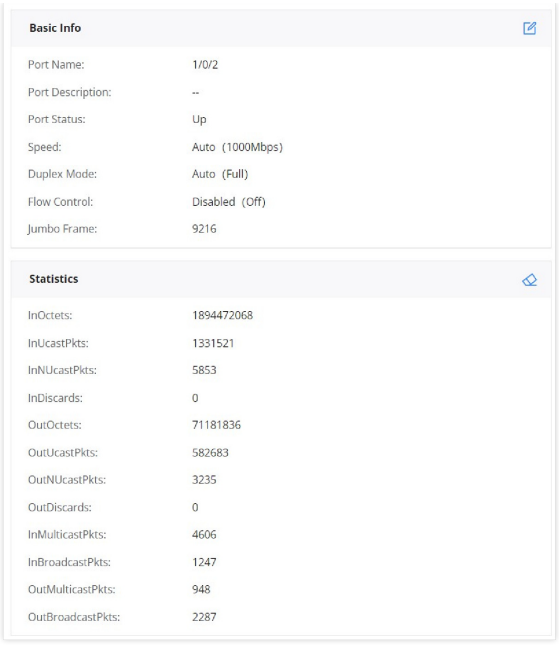
This page displays the status for each port on the GWN780x(P) switches.

- **Port Info:** indicates port status by color code (green, red, gray, white, etc.) and PoE icon.
- **Basic Info:** click on the port to see basic information like port description, speed, duplex mode, etc.
- **Statistics:** displays the port traffic statistics.
- **Neighbor Info:** displays port neighbor information, including device name, MAC address, IP address, speed, connection duration, and more.
- **PoE Power Supply:** displays the power history of PoE ports to help identify and pinpoint PoE power issues.

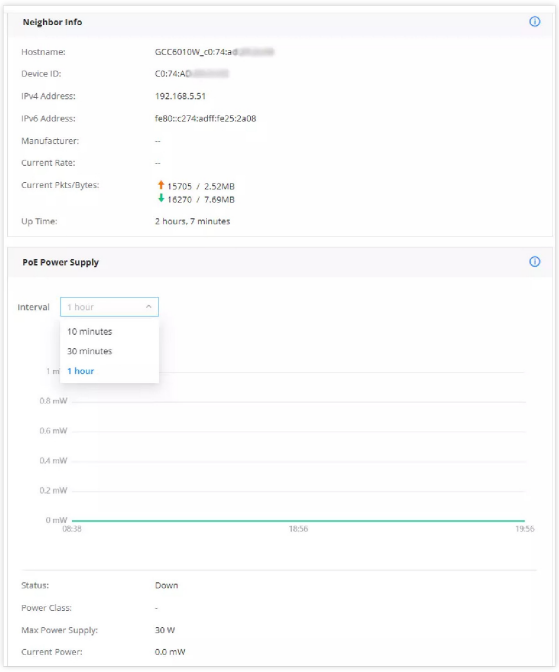
Please refer to the figures below:



Port Info



Port Info – Basic Info & Statistics



Port Info – Neighbor Info & PoE Power Supply

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

	Grey: Linkdown
	White: shutdown
	**Green:** 1000 Mbps speed
	**Light green:** 100 Mbps/10 Mbps speed
	**Red:** ErrDisable

	Symbol: PoE Power is enabled.

Ports Labels and Color code

Note: a PoE symbol and color code combination is also possible. Ex: in this case, the port is using 1000 Mbps speed and also using PoE at the same time.

There are 3 main sections for each port:

- **Basic Info:** 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, Multicast, etc).

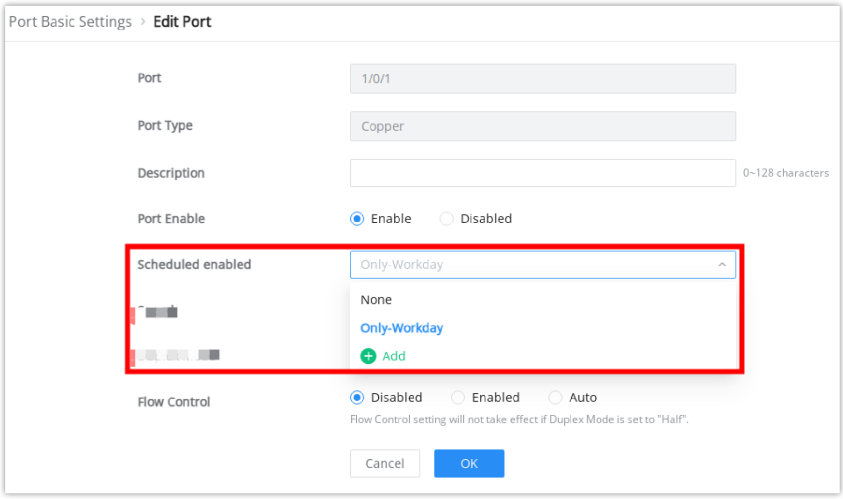
Note: *Click on to clear the statistics.*

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 GWN780x(P) Switch ports, like disabling or enabling the port or even enabling the port based on a schedule, adding Description, specifying the speed by default is Auto, Duplex Mode, and Flow Control. There is also a filter on in case you wan to edit only the Copper ports which are the Gigabit Ethernet ports or Fiber ports which are the SFP ports.



Port Basic Settings page

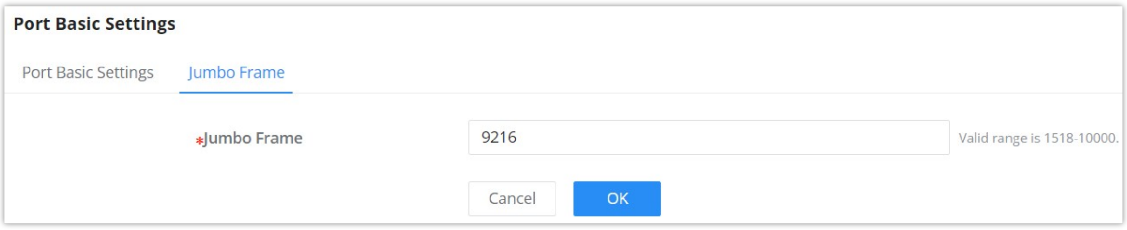
Port	The selected Port to be configured, it can be either Gigabit Ethernet port or SFP port.
Description	It is used to configure the information description of this interface , which can be a description of usage, etc., with a maximum of 128 characters, and the characters limited to input are numbers 0-9 , letters az / AZ and special characters.
Port Enable	Set whether to enable the interface. *it is enabled by default.*

Scheduled enabled	From the drop-down list, select the schedule for when the port (including physical and LAG ports) will be enabled.
Speed	Set the rate of the interface, the options are {Auto, 10Mbps, 100Mbps, 1000Mbps}. *The default is auto-negotiation.* ***Note:*** *When set to Auto, the rate of the interface is automatically negotiated between the interface and the peer port .*
Duplex Mode	Set the duplex mode of the interface. The GE ports options are { auto-negotiation, full-duplex, half-duplex}. *The default is auto-negotiation.* ***Note:*** *Optical ports only support full-duplex mode.* ● **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.
Flow Control	Set the flow control on the interface, the options are {Disabled, Enabled, Auto}. *The default is Disabled.* 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

Jumbo Frame

The maximum Transmission Payload or MTU is typically 1500 bytes, in case the user requires even a bigger MTU length for a specific scenario, there is an option on the GWN780x(P) Switch to enable Jumbo Frame, the maximum Ethernet frame size ranges from 1518 up to 10000.

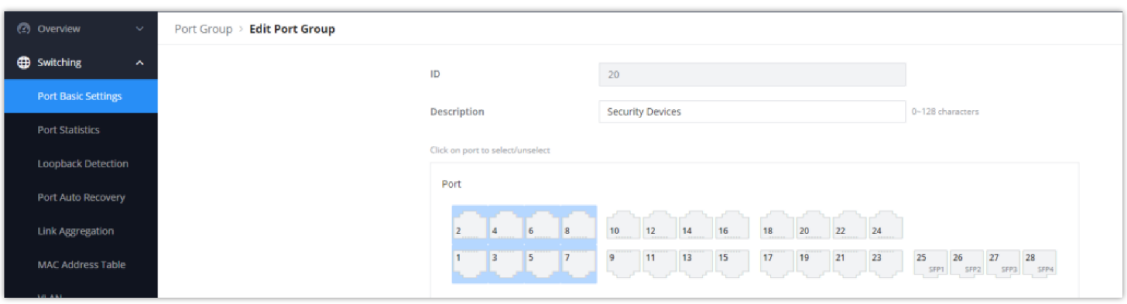


Jumbo Frame

Port Group

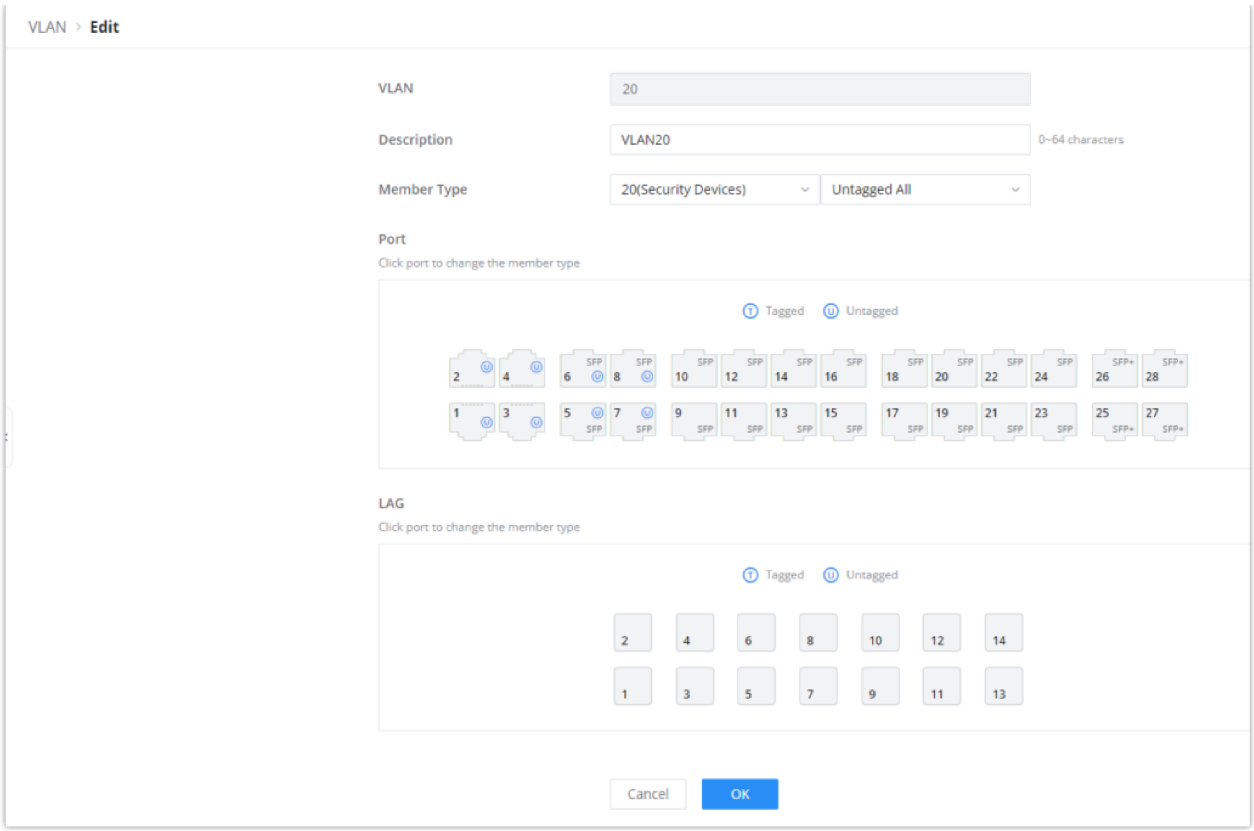
The port group feature allows administrators to logically bundle specific ports together under one group with a corresponding group ID, this can be useful when classifying the switch ports for identifying the usage of each set of ports, for example port 1 to 8 can be set with ID 20, these will be the ports connecting Security devices.

Port group settings can facilitate quick batch settings for port group ports.



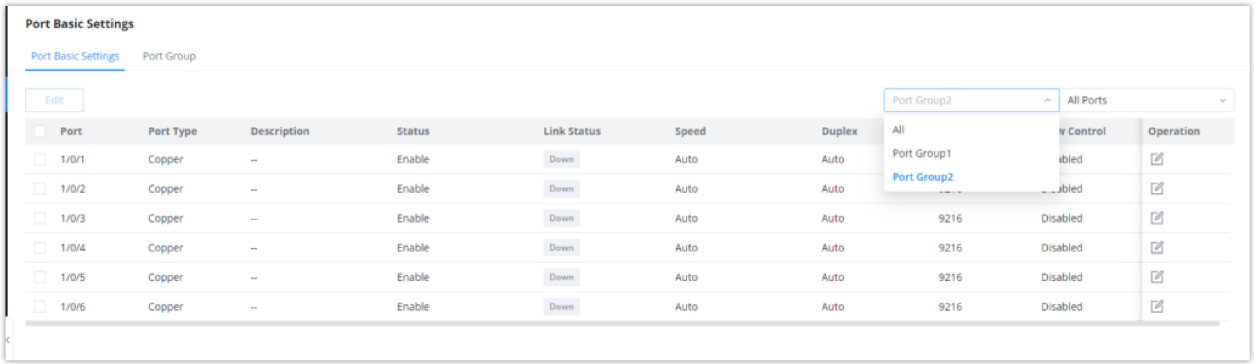
Port Group

Once the Port Group is created, it can ease up the process of selcting and tagging/untagging VLAN ports individually, Under **Switching => VLAN**, select the port group to be used for your VLAN



Port Group Selection

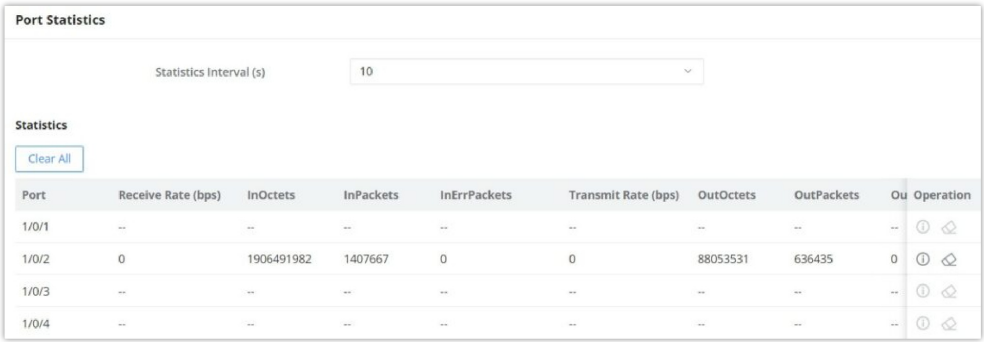
In addition, users can disable/enable specifc ports based on the port group created, instead of going through each individual port selection seperately:



Delete Port Group

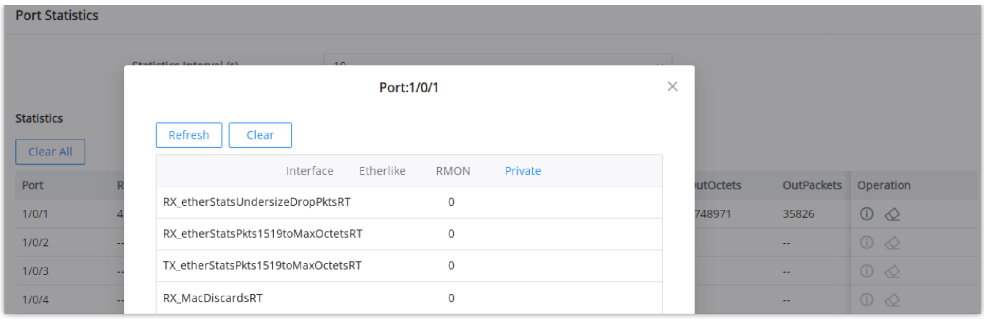
Port Statistics

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



Port Statistics – part 1

To view even more details like Etherlike (SNMP), RMON and port Private MIB information.

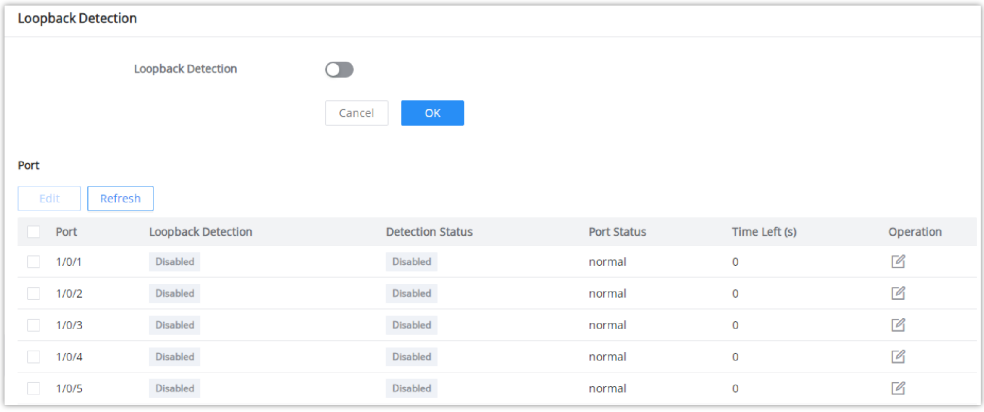


Port Statistics – part 2

Loopback Detection

By enabling the loop detection function of the interface, the interface periodically sends detection packets to check whether the packets are returned to the device, and then determines whether there is a loop in the device. If a loop is detected, the port is automatically shut down to eliminate the loop and ensure the normal operation of the network environment.

> **Note:**
>
> Interface Loopback Detection is not effective. If STP is enabled, because STP protection overrides interface Loopback Detection.



Loopback Detection

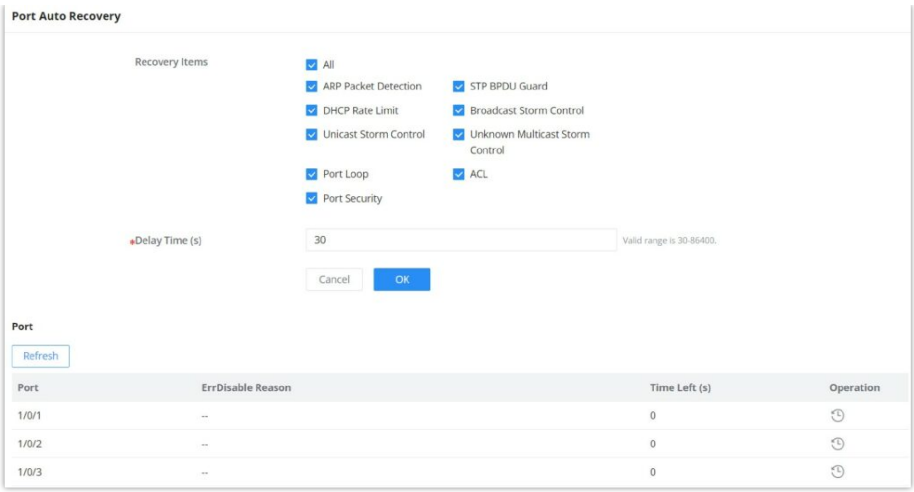
Port Auto Recovery

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.



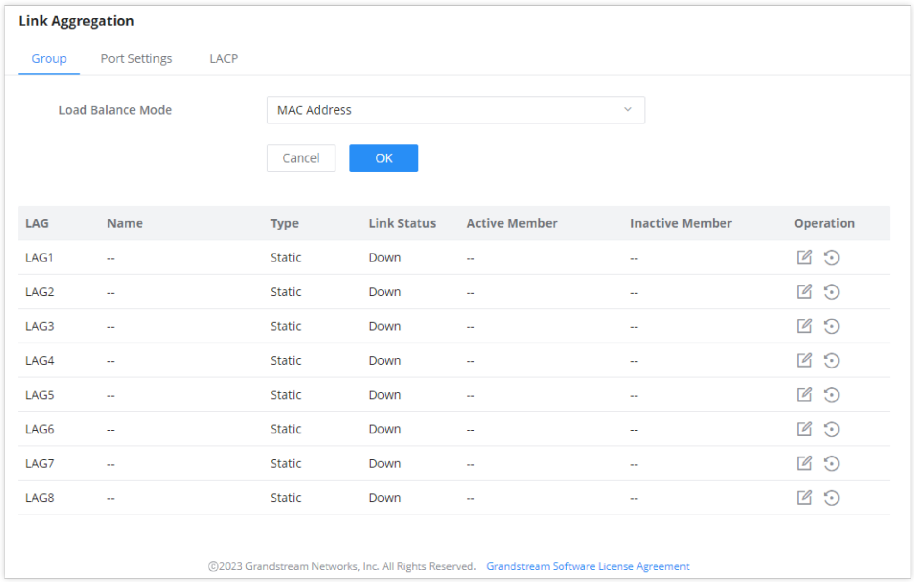
Port Auto Recovery

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 GWN780x(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

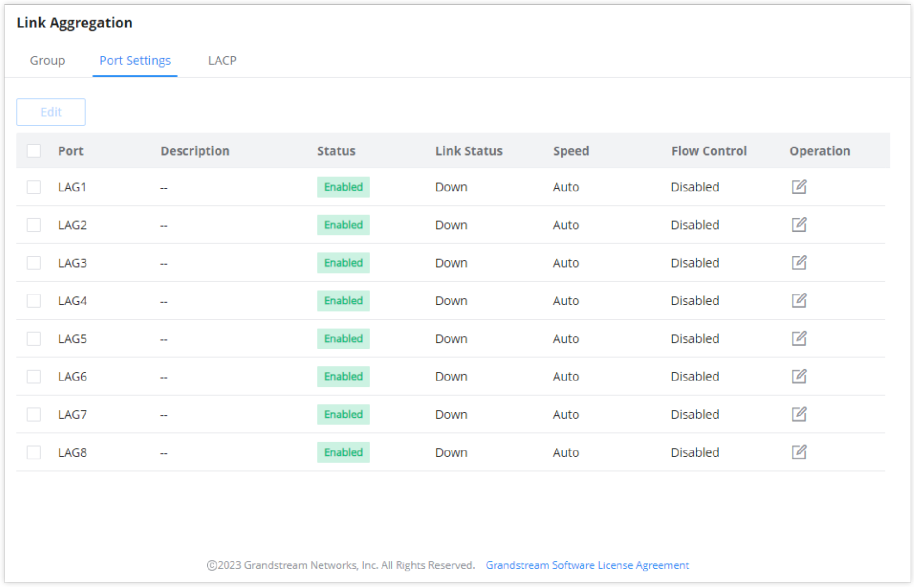
Load Balancing Mode	Select your Load balance mode. **MAC address** - Aggregated group will balance the traffic based on different MAC addresses. Therefore, the packets from different MAC addresses will be sent to different links. **IP/Mac Address** - Aggregated group will balance the traffic based on MAC addresses and IP addresses. Therefore, the packets from same MAC addresses but different IP addresses will be sent to different links.

Edit Group	**Name:** Enter the name of the LA Group. **Type:** Use the drop down menu to specify the type for LAG. ● **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. **GE**: Click on port to check / uncheck which ones will be part of this LAG.

Link Aggregation Port

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.



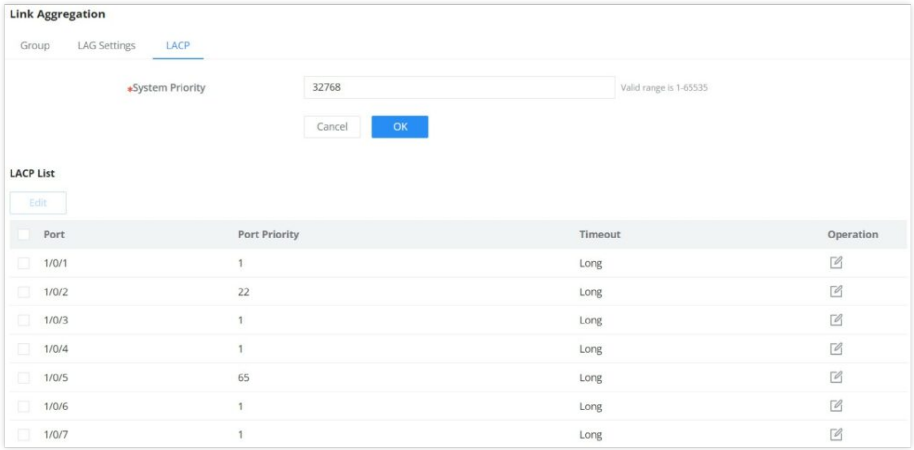
Link Aggregation Port Settings

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. *it is enabled by default.*
Speed	Set the rate of the interface, the options are {Auto, 10Mbps, 100Mbps, 1000Mbps}. *The default is auto-negotiation.* ***Note:** When set to Auto, the rate of the interface is automatically negotiated between the interface and the peer port .*
Jumbo Frame	Specify the jumpo frame, valid range is 1518-10000. Default value is 9216
Flow Control	Set the flow control on the interface, the options are { Disabled, Enabled, Auto}. *The default is Disabled* 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 – LACP

System Priority	Set the system priority of LACP, the value range is an integer from 1-65535, *the default is 32768.*
Edit LACP	**Port:** Select the switch LAG interface to be configured **Port Priority:**Set the LACP protocol priority of the port , the value range is an integer from 1 to 65535 , *the default is 1.* ***Note:** The smaller the priority value of the port , the higher the LACP priority of the port.* **Timeout:** Set the timeout time for receiving LACP packets, the options are { Short, Long} , *the default is Short.* ● **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 .

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

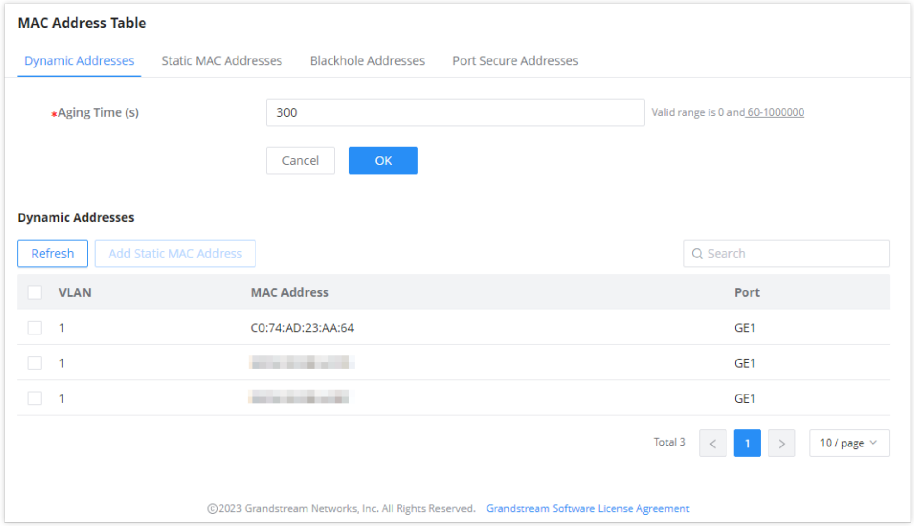
the MAC address table is established based on the automatic learning of the source MAC address in the data frame received by the device. If the MAC address entry does not exist in the MAC address table, the device adds the new MAC address and the interface and VLAN corresponding to the MAC address as a new entry into the MAC address table. GWN780x(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

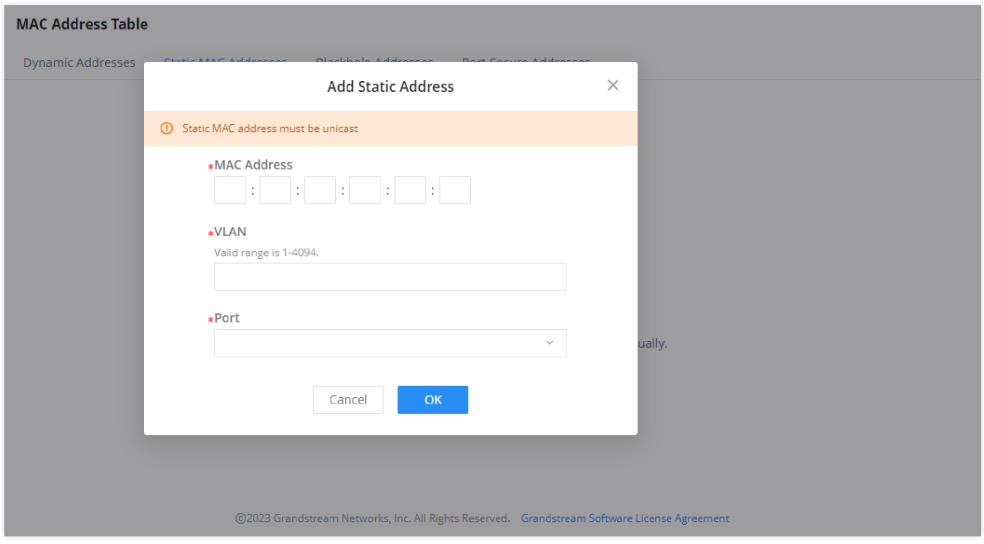
Click on **"Refresh"** button to update the table, or click on **"Add Static MAC Address"** button to add the entry to the static MAC address.

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.

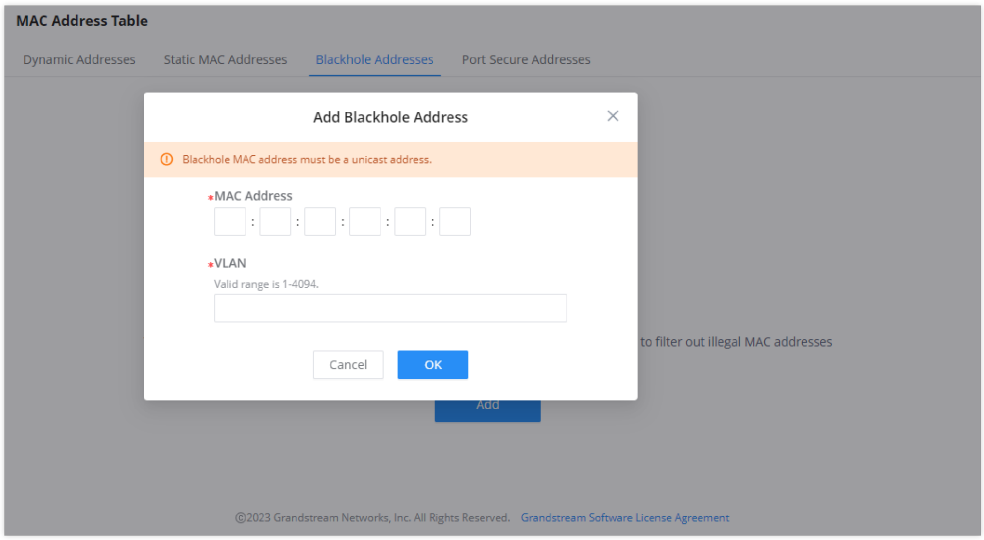
Port	Select the port where received frame of matched destination MAC address will be forwarded to.

Static MAC Address

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.



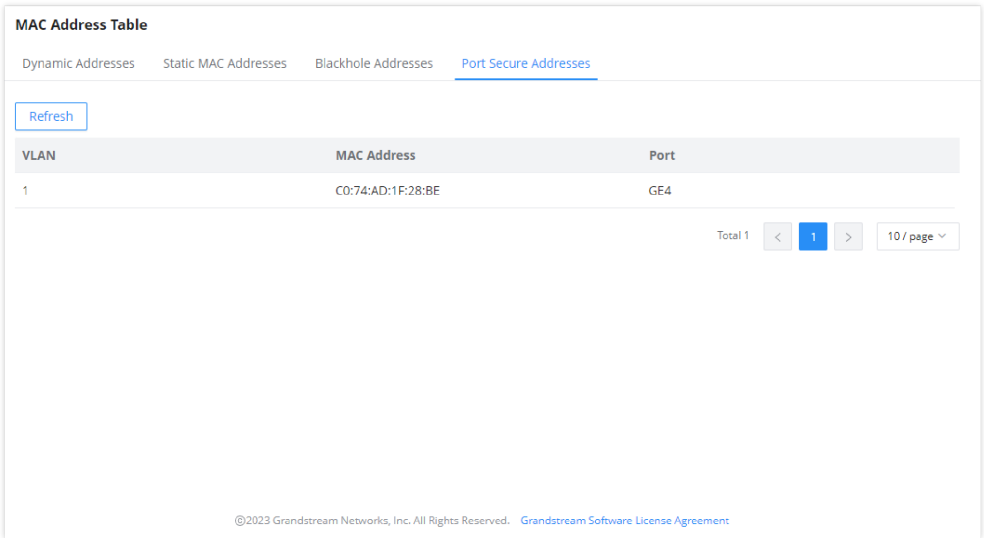
Black Hole Address

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**.



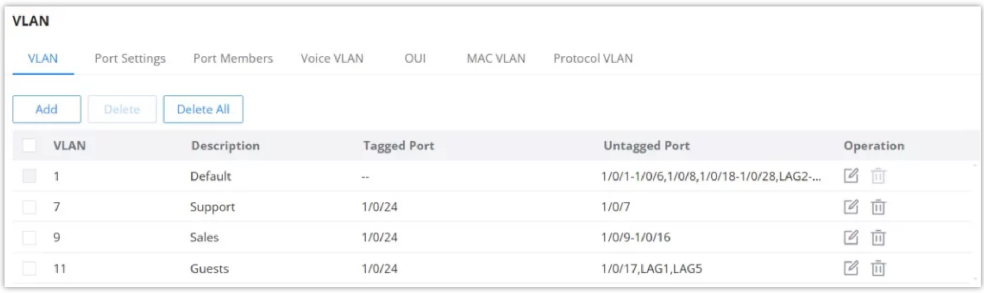
Port Security Address

VLAN

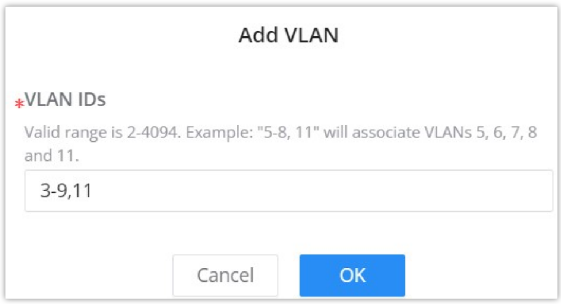
A virtual local area network, virtual LAN or VLAN, is a group of hosts with a common set of requirements that communicate as if they were attached to the same broadcast domain, regardless of their physical location. A VLAN has the same attributes as a physical local area network (LAN), but it allows 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.

> **Note:**
>
> VLAN ID valid range is from 2 to 4094. VLAN 0,1 and 4095 are reserved for the system.

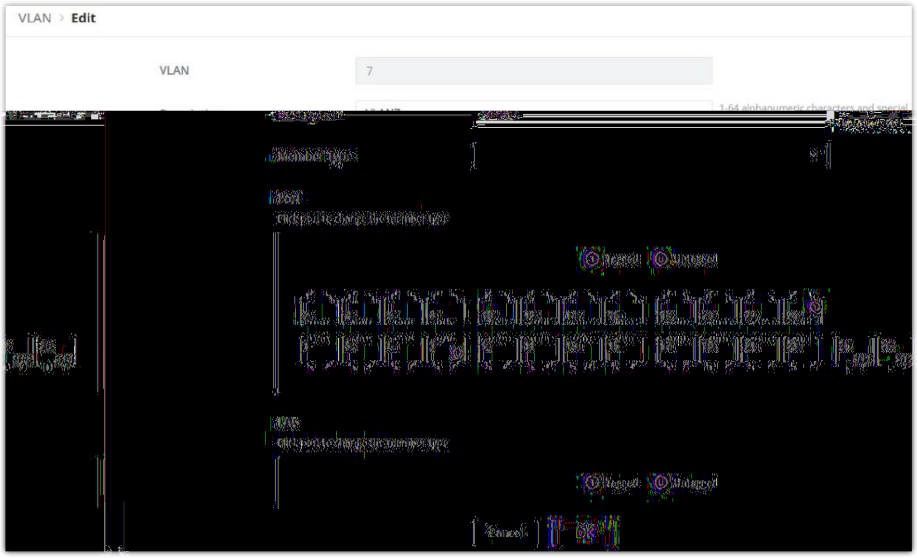


VLAN tab



Add a 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: ● **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. ***Note:*** ● 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

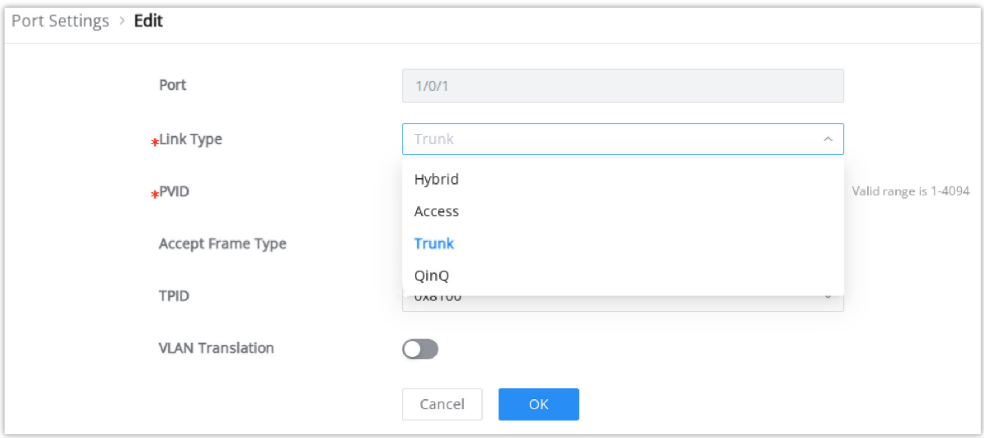
Please refer to this Table below for more details about Tagged and Untagged Ports.

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

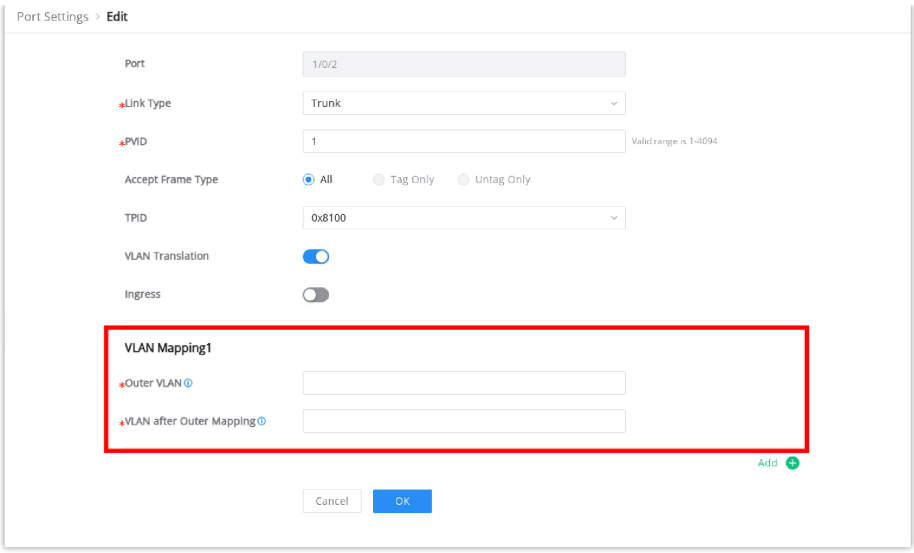
VLAN Tagged and Untagged

VLAN Port Settings

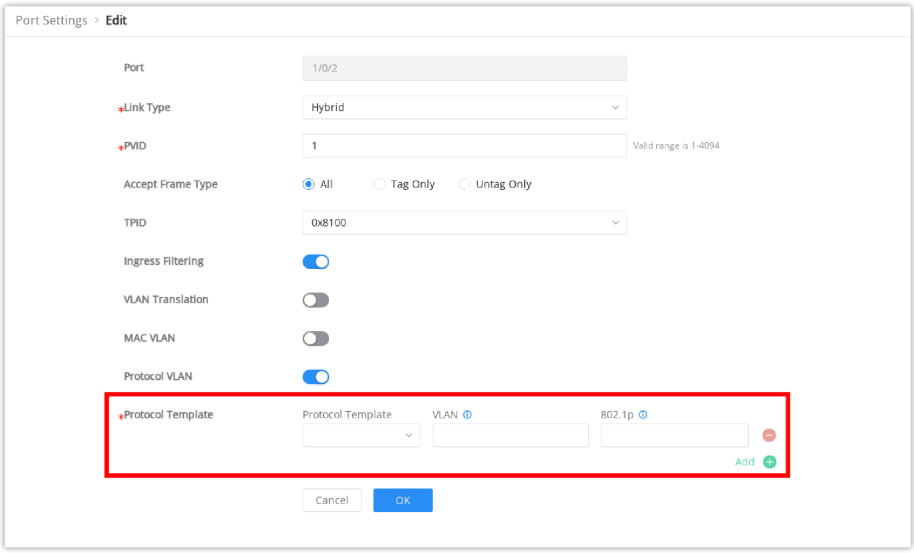
Port Settings page allows for configuring VLAN on each port and LAG by specifying the Link Type (Trunk, Access, Hybrid or QinQ) as well as the default VLAN or PVID, the user can also enable Ingress Filtering for the selected port, also the accepted Frame Type (All, Tag Only and Untag only) and more.



VLAN Port Settings – Link types



VLAN Port Settings – VLAN Translation



VLAN Port Settings – Protocol Template

Port	Shows the selected Port.
Link Type	Select the Link Type: ● **Hyprid:** 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. ● **QinQ:** This is an extended VLAN tagging technique where an additional VLAN tag is added, also known as "double tagging." It allows Layer 2 tunneling and is often used by service providers to transport customer 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. ***Note:*** *Ingress filtering is a method used by enterprises and internet service providers (ISPs) to prevent suspicious traffic from entering a network.*
VLAN Translation	Allows translating one VLAN ID to another at the port level. It's useful for scenarios where different parts of the network use different VLAN IDs but need to communicate with each other.

MAC VLAN	Allows the switch to assign VLANs based on the MAC address of the incoming traffic. It can be used for more dynamic VLAN assignment, where devices can be automatically placed into specific VLANs based on their MAC addresses.
Protocol VLAN	Allows VLAN assignments based on the protocol type in the frame, such as IP or ARP. It enables grouping traffic from certain protocols into specific VLANs for easier network management.

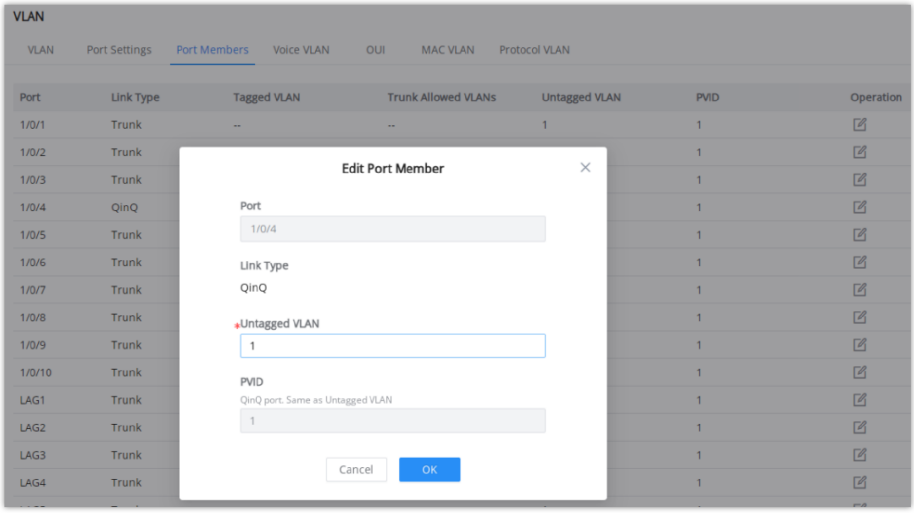
VLAN Port Settings

VLAN Port Members

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

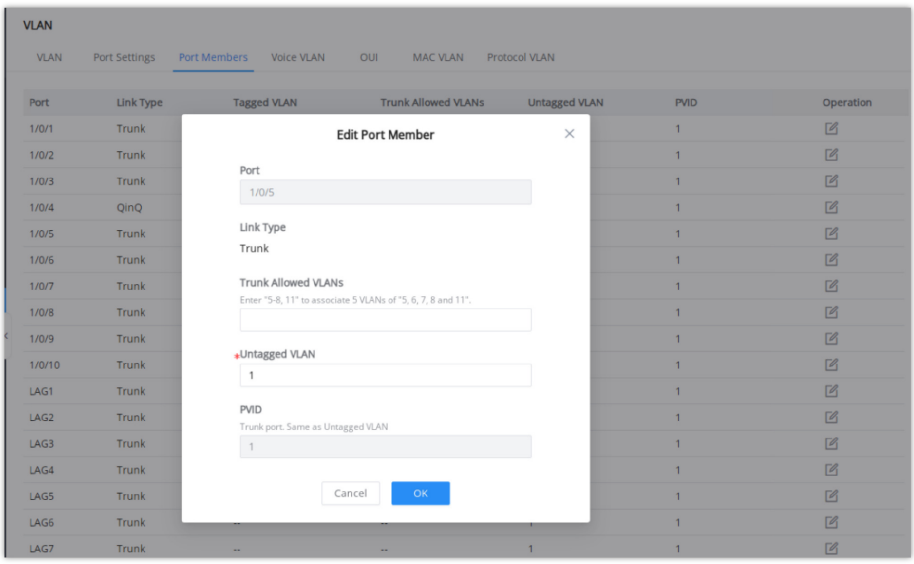
Note

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

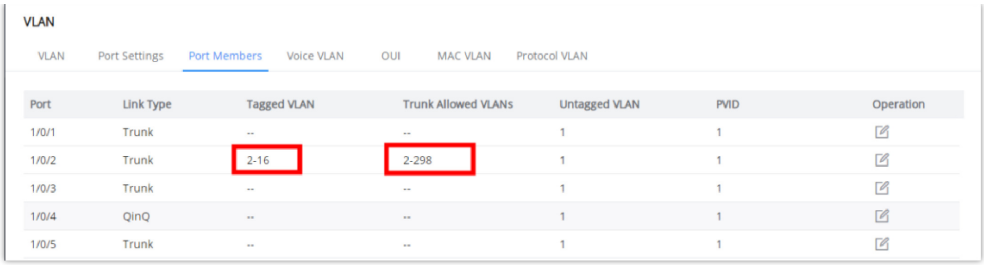


VLAN Port Members – QinQ

Trunk Allowed VLANs allows the configuration of VLANs that do not yet exist on the switch and is only effective for configured VLANs.



VLAN Port Members – Trunk



VLAN Port Members

Voice VLAN

A voice VLAN (virtual local area network) is a dedicated VLAN specifically designed to carry voice traffic, such as IP phone calls. By isolating voice traffic from other types of network traffic, voice VLANs help ensure that voice calls are prioritized and experience minimal latency or jitter. This is critical to maintaining clear and uninterrupted voice communications.

Voice VLAN advantages:

- **Improved voice quality:** By isolating voice traffic from other types of network traffic, voice VLANs help reduce the latency and jitter that can cause choppy or distorted audio during voice calls.
- **Reduced congestion:** By prioritizing voice traffic, voice VLANs help prevent other types of network traffic from interfering with voice calls, even during periods of heavy network usage.
- **Simplified network management:** Voice VLANs can simplify network management by making it easier to troubleshoot and resolve voice-related issues.

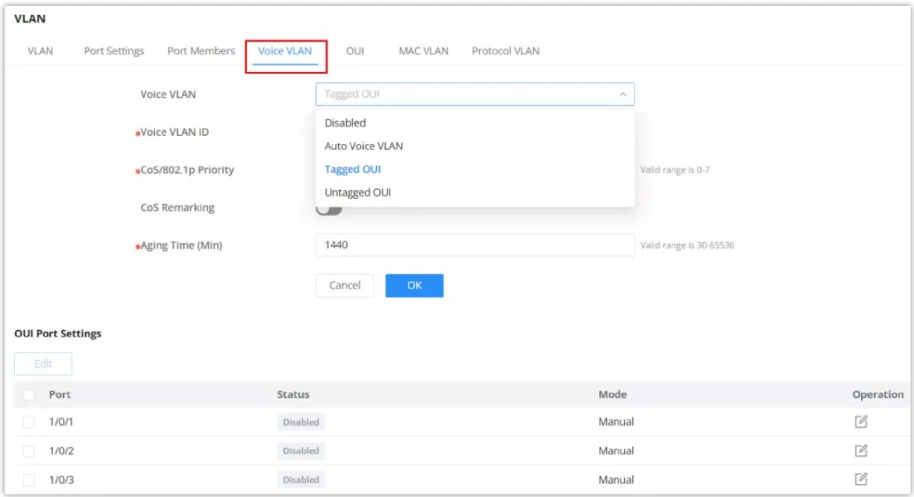
For example, when an IP phone is connected to a GWN78xx switch port, the switch prioritizes traffic in the voice VLAN, ensuring that voice packets are forwarded before other types of packets.

The user can select more than one way to set up the voice VLAN:

- Auto Voice VLAN using LLDP
- Tagged OUI using LLDP
- Tagged OUI using VLAN Tag
- Untagged OUI

For more details, please visit this guide: GWN78xx(P) – Voice VLAN Guide.

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



Voice VLAN

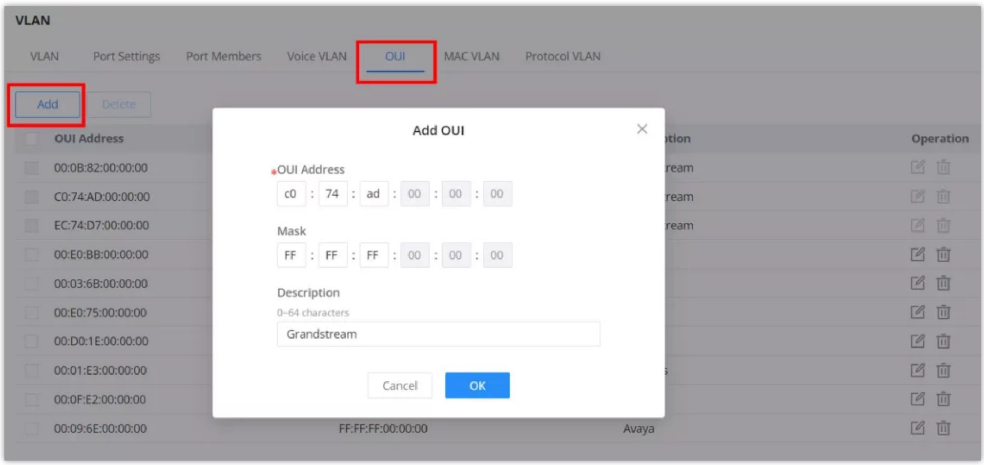
Voice VLAN	Select from the drop-down list the Voice VLAN method: • Disabled • Auto Voice VLAN • Tagged OUI

	● Untagged OUI *By default is disabled.*
Voice VLAN ID	Select a VLAN as the voice VLAN from the VLAN list. ***Note:** The default VLAN 1 cannot be used as a voice VLAN.*
CoS/802.1p Priority	Specify the CoS/802.1p Priority, Valid range is 0-7.
If Auto Voice VLAN is selected	
DSCP	Specify the DSCP priority, an integer ranging from 0 to 63.
LLDP/LLDP MED Auto Config	If Auto Voice VLAN for Voice VLAN mode is selected, then you need to go to LLDP to set network policies. LLDP automatic configuration is added to voice VLANs to make it easier and faster for users to configure them with one click.
If Tagged or Untagged OUI is selected	
CoS	Set whether to enable CoS Remarking.
Aging Time	Set the aging time of the voice VLAN. *The value range is an integer from 30 to 65536 , and the default is 1440 minutes .*
Edit Port Settings	**Port:** Displays the selected port. **Status:** Set whether to enable the voice VLAN function of the port. *it is disabled by default.* **Mode:** Set the working mode of the voice VLAN on the port. T*he default is manual.* ***Note:** When set to " Manual ", the port must be added to the voice VLAN manually, and the LLDP function needs to be used.*

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.



VLAN – OUI

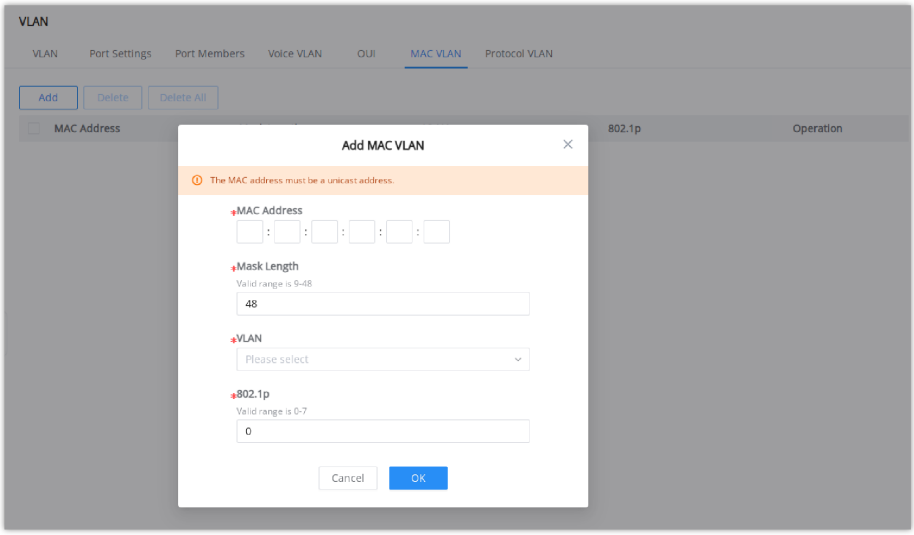
MAC VLAN

MAC VLAN is a networking technique where each VLAN is based on the source MAC address of incoming frames. Devices with the same MAC address share a VLAN. This segmentation enables isolated communication between devices within the same VLAN based on MAC addresses.

VLANs are divided according to the source MAC address of the data frame. Through the configured MAC address and VLAN mapping table, when the switch receives an untagged frame, it adds the specified VLAN Tag to the data frame based on the mapping table.

To add a MAC address to VLAN mapping, click on "**Add**" button then specify the MAC Address, Mask Length, VLAN and the priority (802.1p).

> **Note:**
>
> Only effective for Hybrid port.

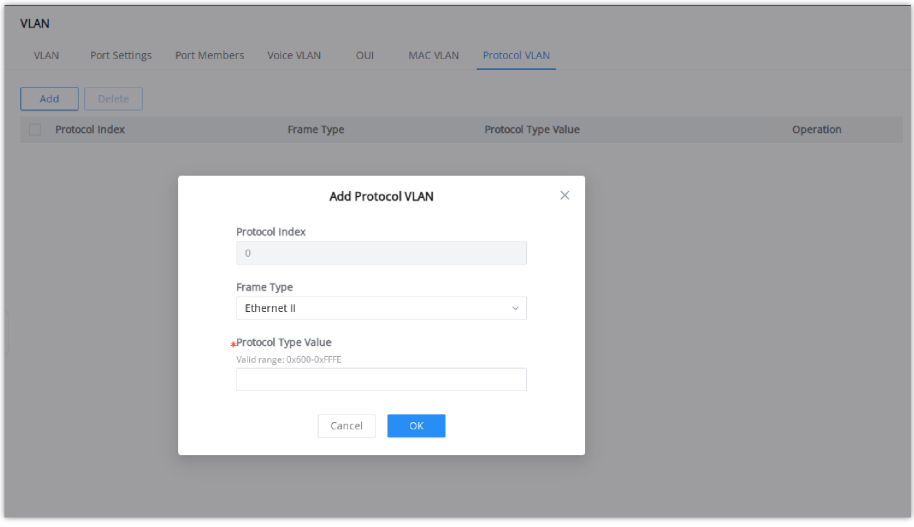


VLAN – MAC VLAN

Protocol VLAN

VLANs are divided according to the protocol (family) type and encapsulation format to which the data frame belongs. Through the configured protocol domain and VLAN mapping table in the Ethernet frame, when the switch receives an untagged frame, it adds the specified VLAN Tag based on the mapping table.

> **Note:**
>
> Only effective for Hybrid port.



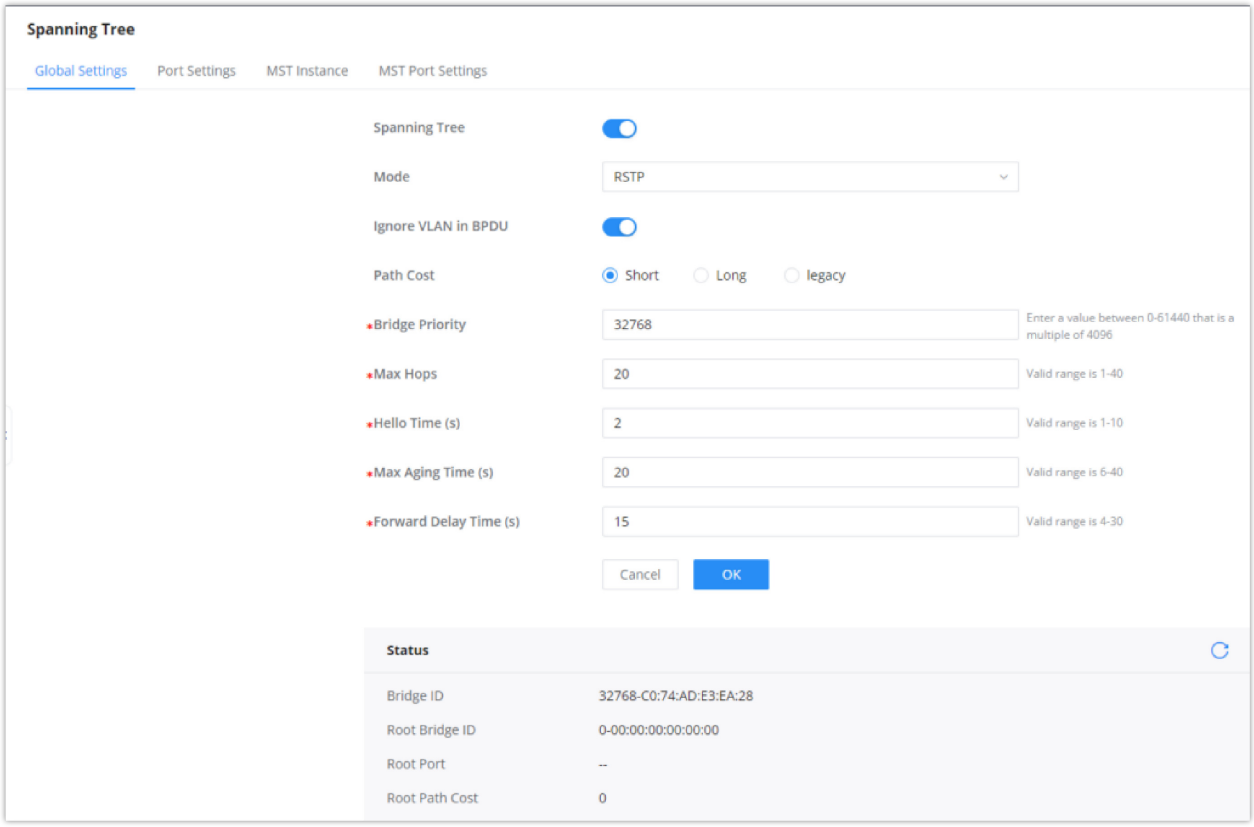
VLAN – Protocol VLAN

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

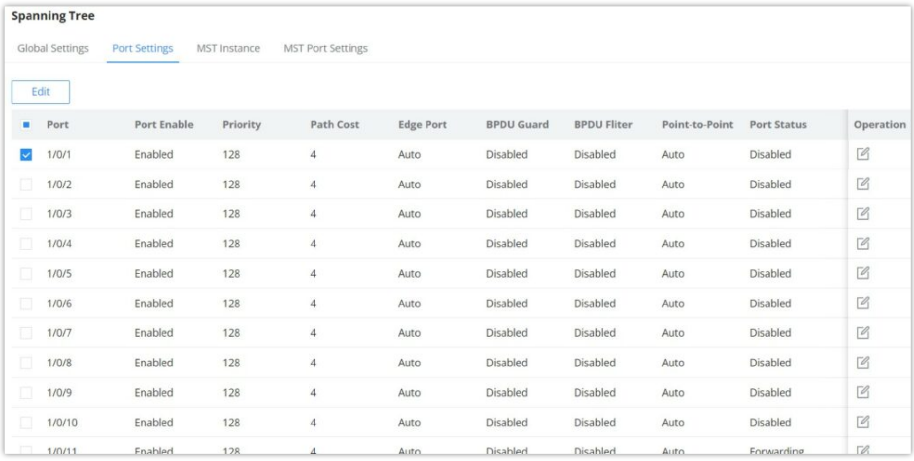
Spanning Tree	Set whether to enable Spanning Tree.
Mode	Set the operating mode of Spanning Tree (STP). ● **STP:** Enable the Spanning Tree (STP) operation. ● **RSTP:** Enable the Rapid Spanning Tree (RSTP) operation. ● **MSTP:** Enable the Multiple Spanning Tree Protocol (MSTP) operation.
Ignore VLAN in BPDU	This feature allows the switch to ignore VLAN-specific information in Bridge Protocol Data Units (BPDUs). This prevents VLAN configurations from influencing Spanning Tree Protocol (STP) decisions across multiple VLANs.
Path Cost	Specify the path cost method (Short, Long). *Default is Short.*
Bridge Priority	Select the Bridge Priority, In an STP network, the device with the smallest bridge ID is elected as the root bridge. *Default is 32768.* ***Note:** The valid range is 0~61440, which must be a multiple of 4096*

Max Hops	Select the Max Hops (the range is 1 - 40). *Default is 20*
Hello Time (s)	Specify the Hello Time in seconds (the range is 1 -10). *Default is 2.* ***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.*
Max Aging Time (s)	Select The aging time of BPDU packets of the port (the range is 6 - 40). *Default is 20.*
Forward Delay Time (s)	Specify the Forward Delay Time in seconds (the range is 4 -30). *Default is 15.*

STP Global Settings

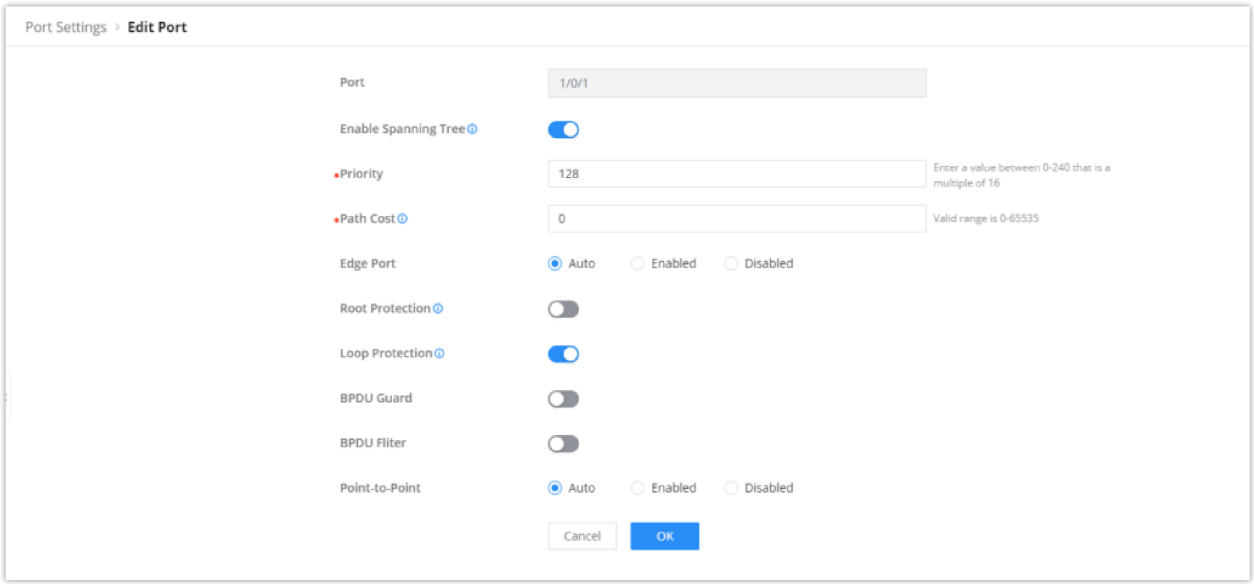
STP Port Settings

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



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.



Spanning Tree – Edit Port Settings

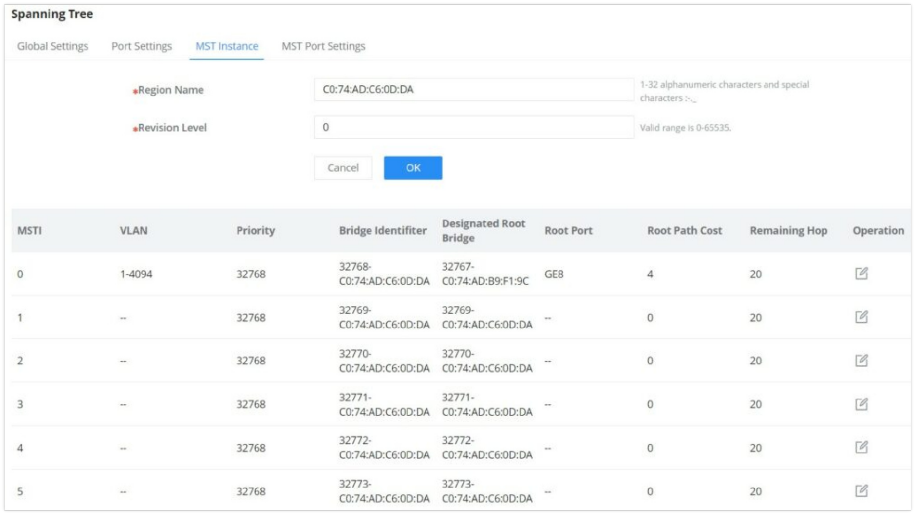
Port	Displays the selected GE/LAG Port.
Enable STP	Set whether to enable STP on this port.

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 . ***Note:*** *The valid range is 0~240, which must be a multiple of 16*
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. ***Note:*** *The valid range is 0~200000000. 0 is equal to auto*
Edge Port	Set whether to enable Edge Port or disable it, by default it's on auto. ***Notes:*** ● *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.*
Root Protection	Safeguards the root bridge by preventing designated ports from becoming the root port, thus protecting the current root bridge from being displaced by lower-priority BPDUs.
Loop Protection	Prevents Layer 2 loops by ensuring a blocking state on ports that stop receiving BPDUs, avoiding the formation of network loops.
BPDU Guard	Set whether to enable BPDU Guard. ***Note:*** *BPDU Guard further protects your switch by turning this port into error state and shutdown if any BPDU received from this port.*
BPDU Filter	Set whether to enable BPDU Filter. ***Note:*** *Drop all BPDU packets and no BPDU will be sent.*
Point-to-Point	Select Point-to-Point option (Auto, Enabled or Disabled). *Default is Auto.* ***Note:*** *determines the STP of link type for this port automatically if set to Auto.*

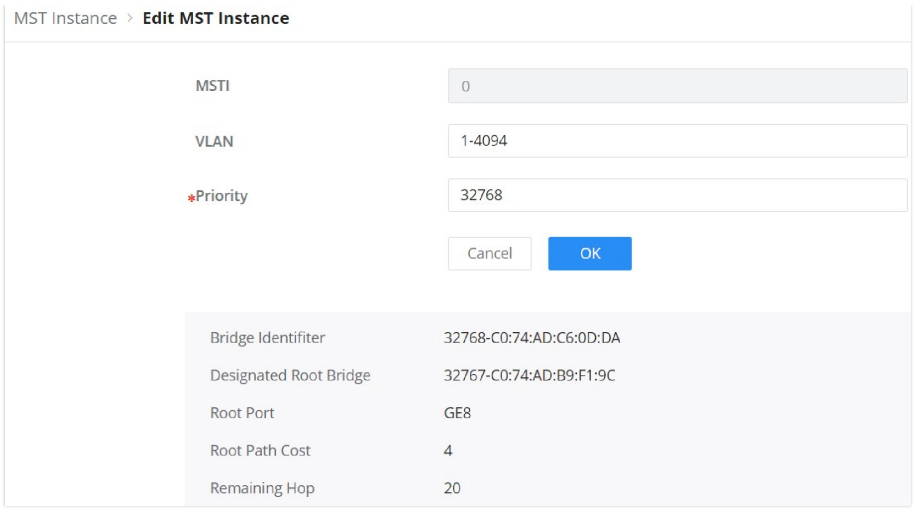
STP Port Settings

Multiple Spanning Tree Instance

MST or Multiple Spanning Tree Instance allows traffic of different VLAN to be mapped into different MST Instances. GWN780x(P) Switch supports up to 16 independent MST instances (0~15) where each instance can be associated with many VLANs.

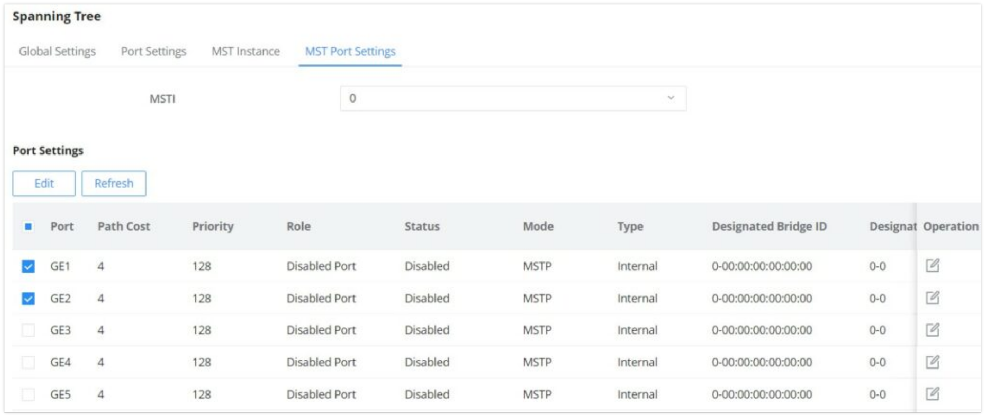


Multiple Spanning Tree Instance



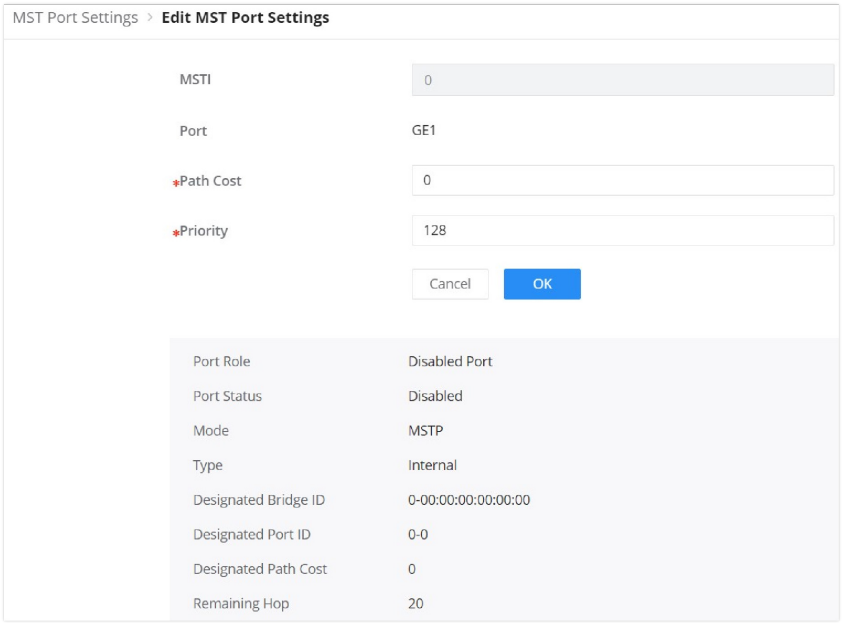
MSTP – Edit Port

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.



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 port

IP

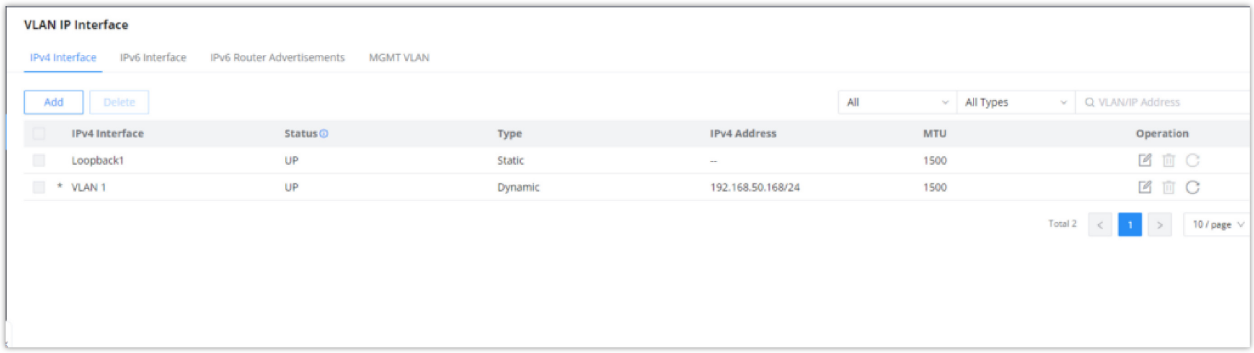
VLAN IP Interface

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.

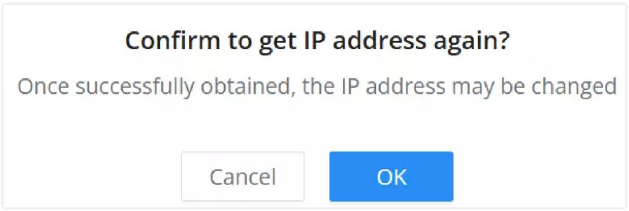
IPv4/IPv6 Interface

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



VLAN IP Interface – MGMT VLAN

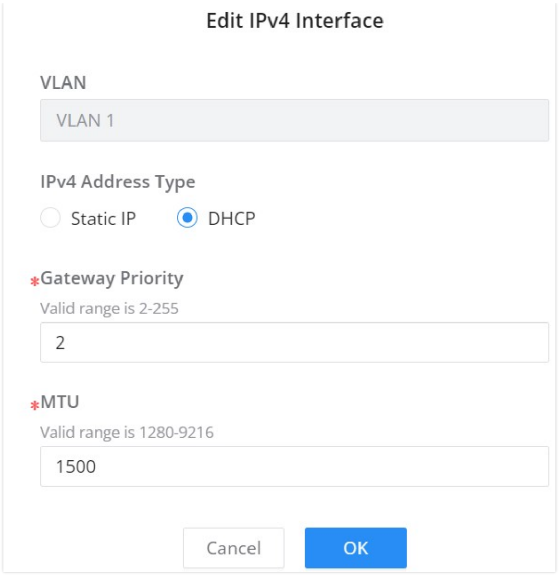
Use the "**refresh icon**" to request a new IP address from the DHCP server. This action will prompt a confirmation dialog; clicking "**OK**" will obtain a new IP address, which may change upon successful retrieval.



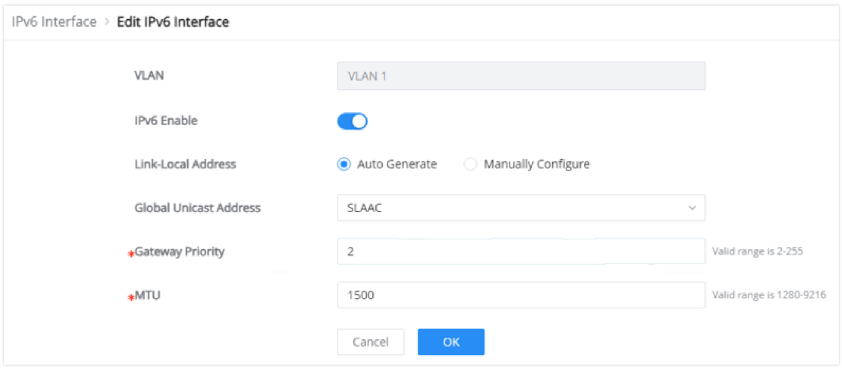
Refresh IP address

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 – IPv4

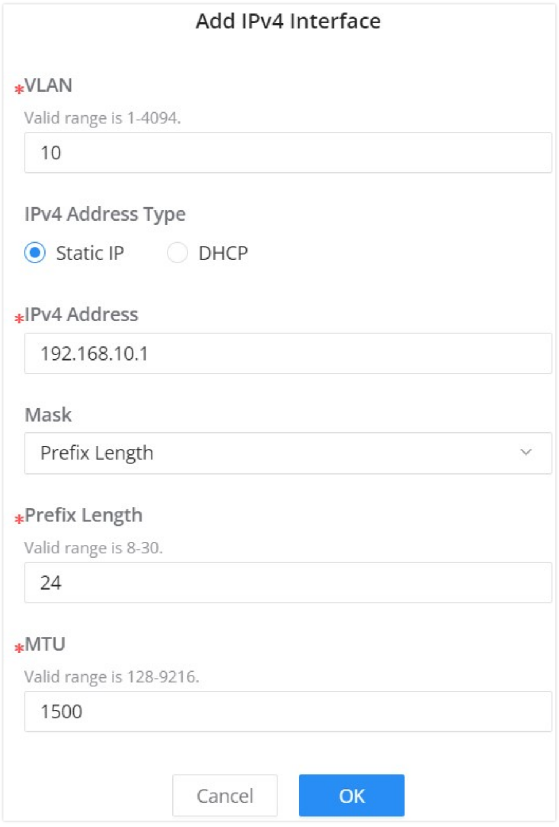


Add VLAN IP Interface – DHCP – IPv6

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**: the user can specify the IPv4 or IPv6 manually.



Add VLAN IP Interface

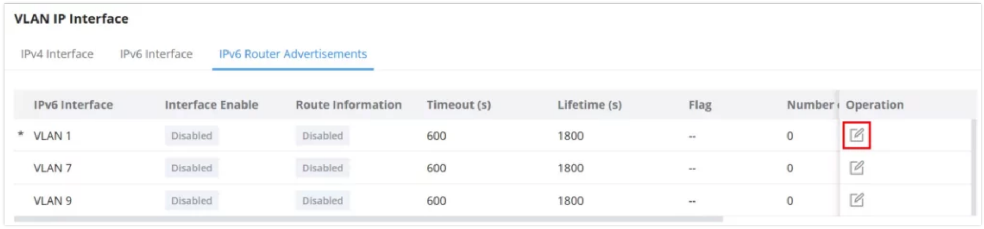
Note:

Gateway Usage Priority:

- Statically configured gateway (manually set) has the highest priority.
- Gateway with a specified priority (smaller priority value means higher priority).
- If priorities are the same, the gateway with the smaller VLAN ID will be used.

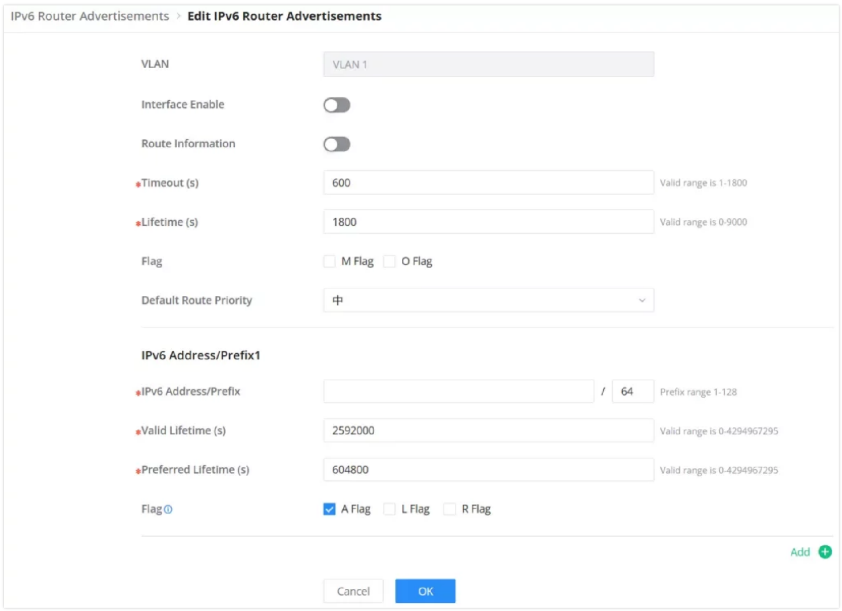
IPv6 Router Advertisements

IPv6 Router Advertisements (RAs) are messages sent by routers to provide information to devices on the network, such as the default gateway, DNS servers, and network prefixes. These advertisements help devices configure their IP addresses and routing automatically without the need for manual configuration. In the VLAN IP Interface section, you can configure RAs for each VLAN to manage IPv6 network settings.



IPv6 Router Advertisement

In the Edit IPv6 Router Advertisements screen, you can customize settings for a specific VLAN. This includes enabling or disabling the interface, setting route information, and configuring timeouts and lifetimes for the advertisements. You can also define IPv6 addresses and prefixes, adjust flags for additional configurations, and set the priority of the default route. This allows for fine-tuning the behavior of the advertisements to suit your network requirements.

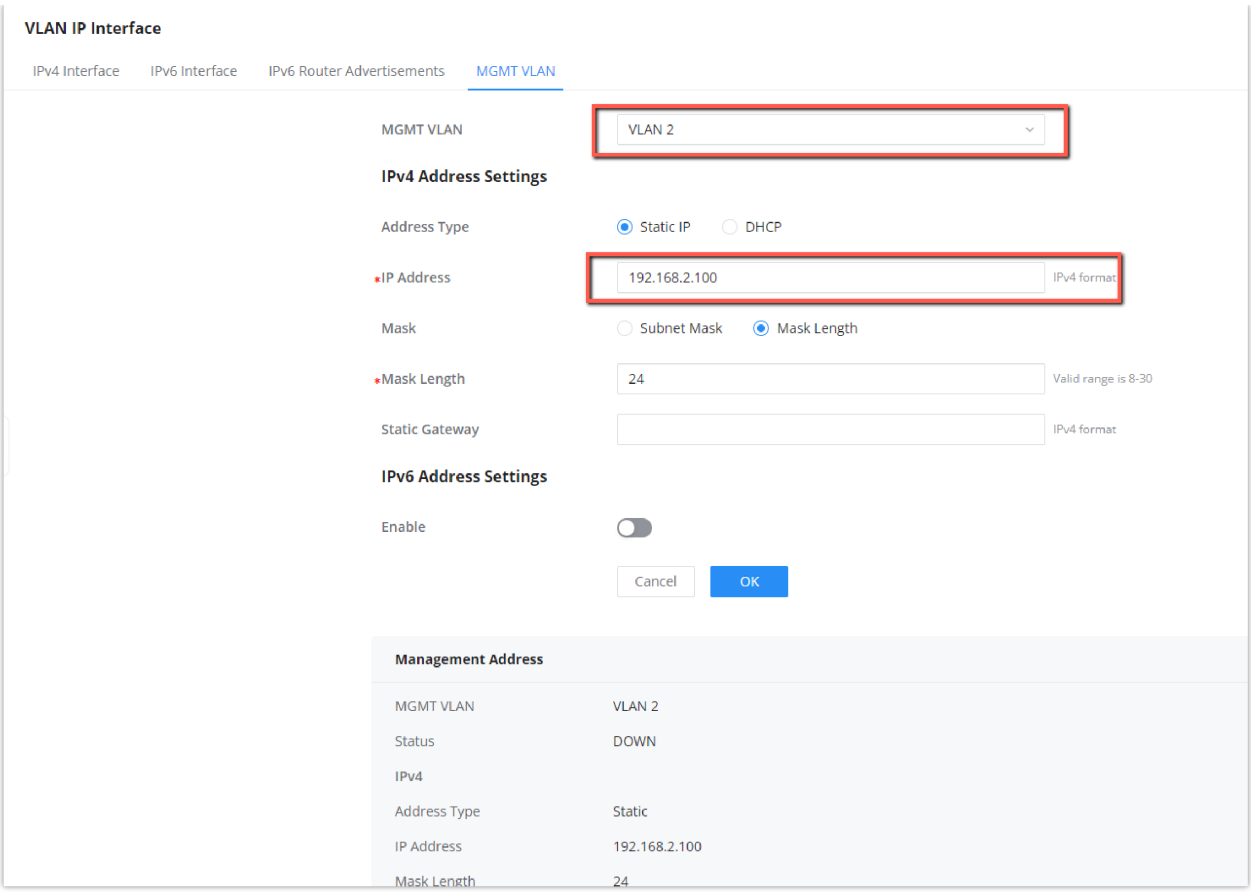


Edit IPv6 Router Advertisement

MGMT VLAN

When you assign an IP address to the management VLAN interface, the system synchronizes this IP configuration with the corresponding VLAN interface in the device's Layer 3 IP interface configuration. This ensures that the IP address used for managing the device is consistent with the VLAN's routing and switching setup.

For example, if you configure the management VLAN with IP address `192.168.2.100` on VLAN 2, this IP will also be reflected in the IP interface configuration for VLAN 2, ensuring both management and routing functions are aligned.



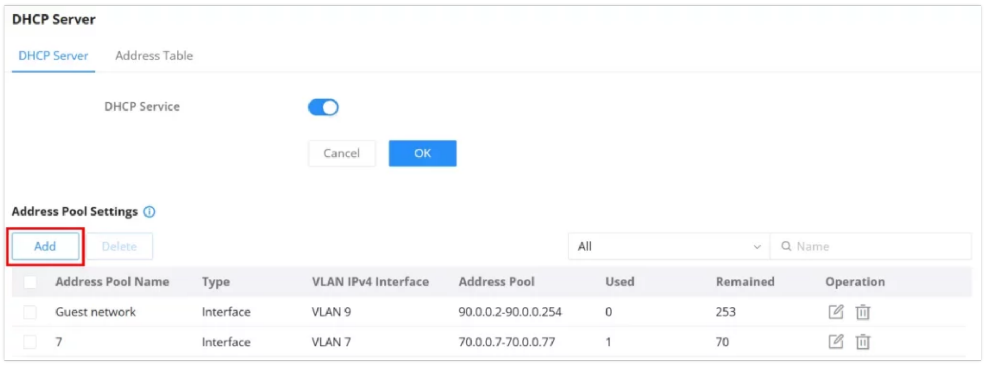
MGMT VLAN

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.

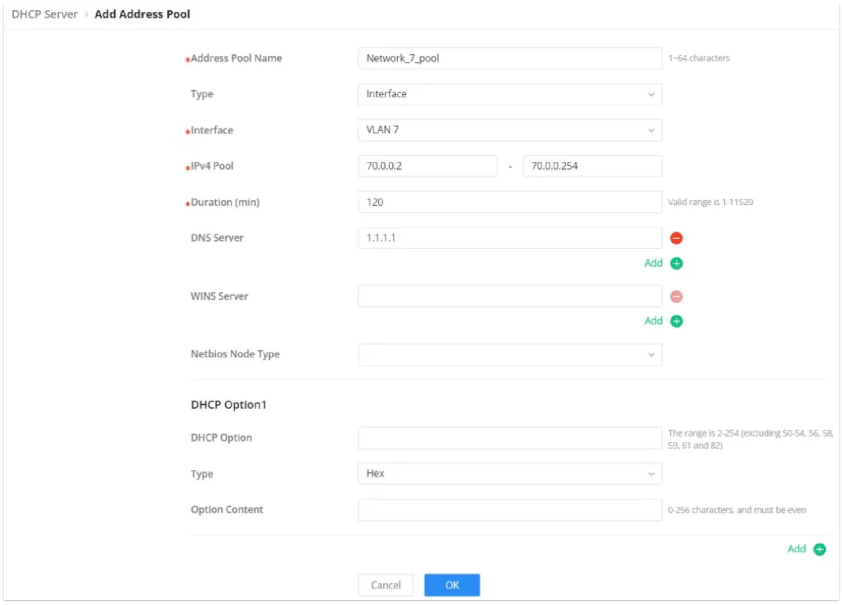


DHCP – Global Settings

Step 2: on **Address Pool Settings section**, click on "**Add**" button to add a new address pool.

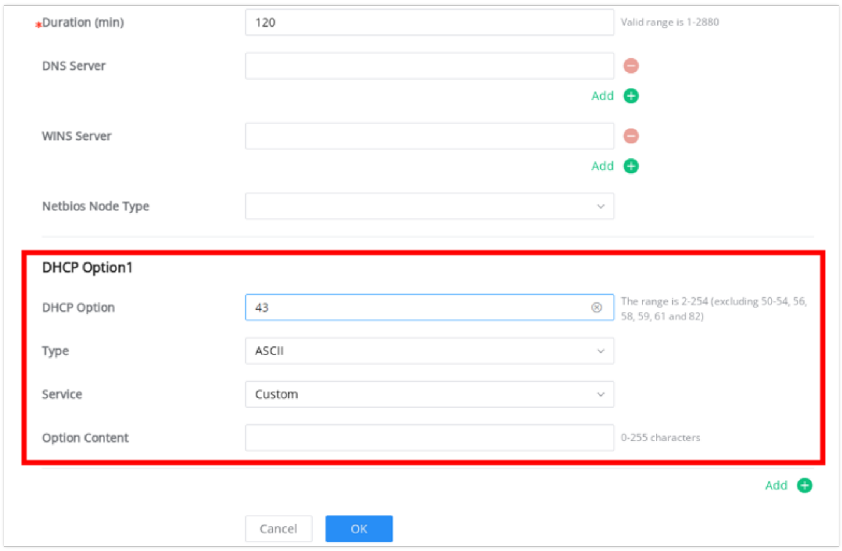
> **Note:**
>
> Global address pool is only used for IP address allocation to DHCP relay.

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



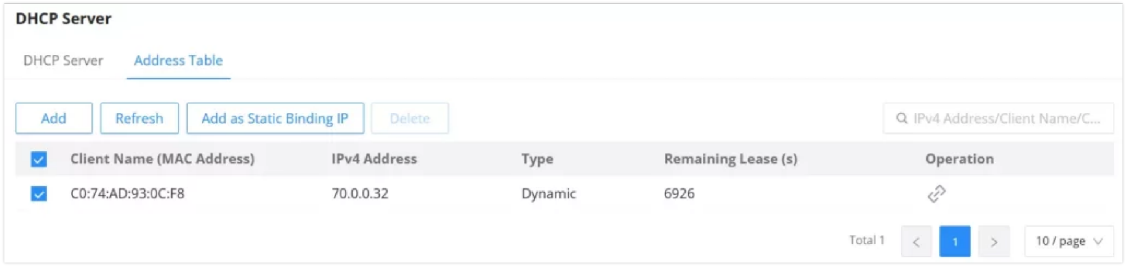
DHCP – Add Pool

On this section the user can configure DHCP Option like the type, Service (for option 43) and option content. It's also possible to add more DHCP Option by clicking on "**Add**" icon as shown below:



DHCP Server -Add Pool – DHCP Options

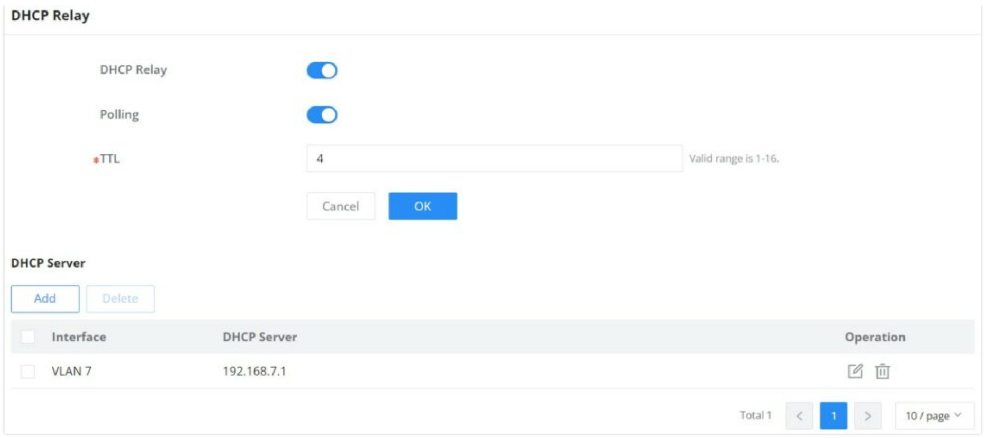
The address table will displays the hosts (devices) MAC Addresses and the IP addresses when using the DHCP Server. Also it's possible make a entry a static one by clicking on "**Add as Static Binding IP**" button.



DHCP – DHCP Server

DHCP Relay

DHCP relay on GWN780x(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.



DHCP Relay

DHCP Relay	Set whether to enable the global DHCP relay function *the default is off.*
Polling	Set whether to enable the polling function of the DHCP relay *disabled by default.*
TTL	Set the TTL value of the DHCP request message after being forwarded by the DHCP relay layer 3. *the value is an integer from 1 to 16 , and the default is 4 .*
DHCP Server	
Interface	Select from the existing VLAN interfaces.
DHCP Server	Set the address of the DHCP server. ***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.*

DHCP Relay

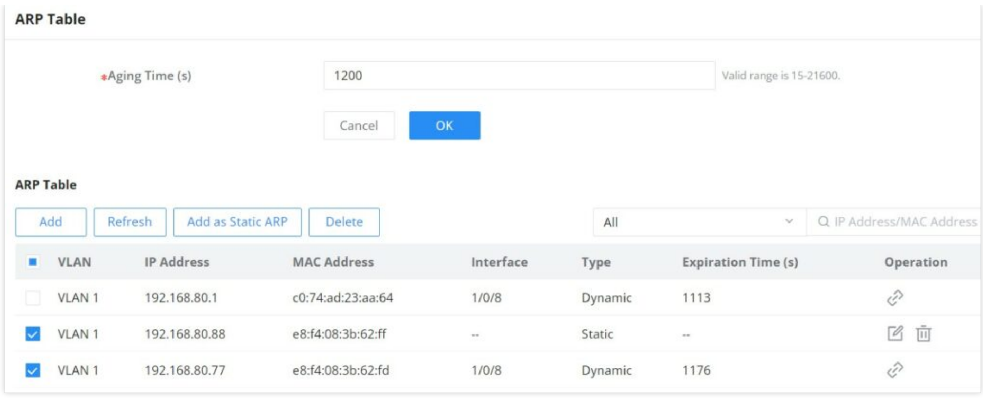
ARP Table

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**.



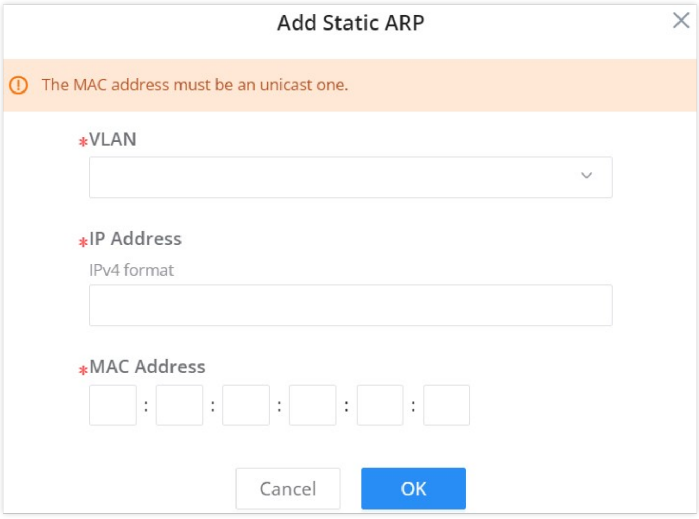
ARP Table

Aging time (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 – 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.



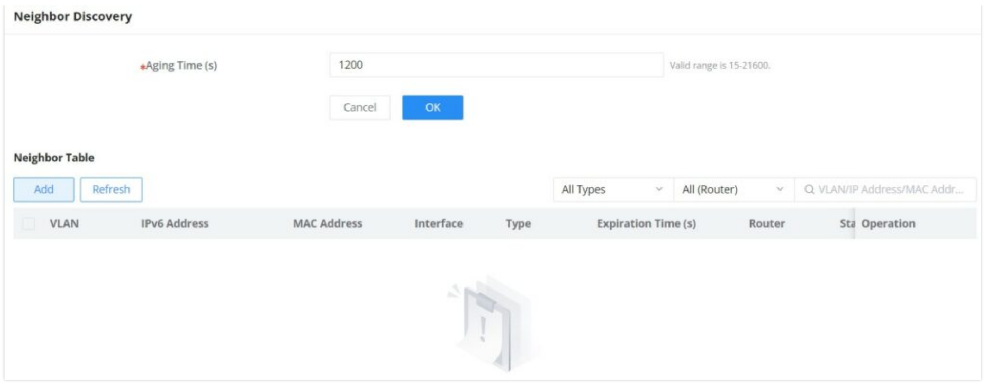
Add Static ARP

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.**

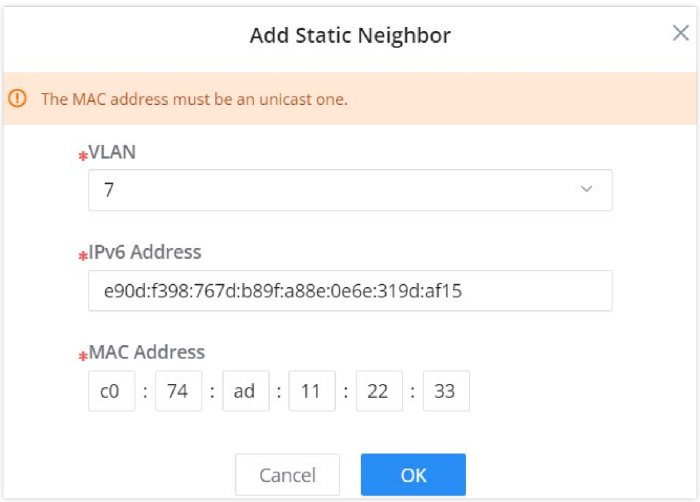


Neighbor Discovery

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

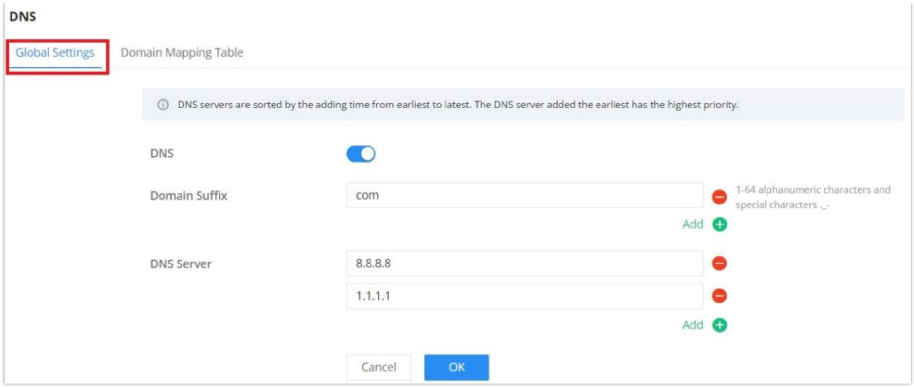
Domain Name System DNS provides translation services between domain names and IP addresses. GWN7800 Switches act as a DNS client. When users perform certain applications on the device (such as Telnet to a device or host), they can directly use a memorable and meaningful domain name, and resolve the domain 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 GWN7800 switches, navigate to **Web UI → IP → DNS**, then click on the **Global Settings** tab.



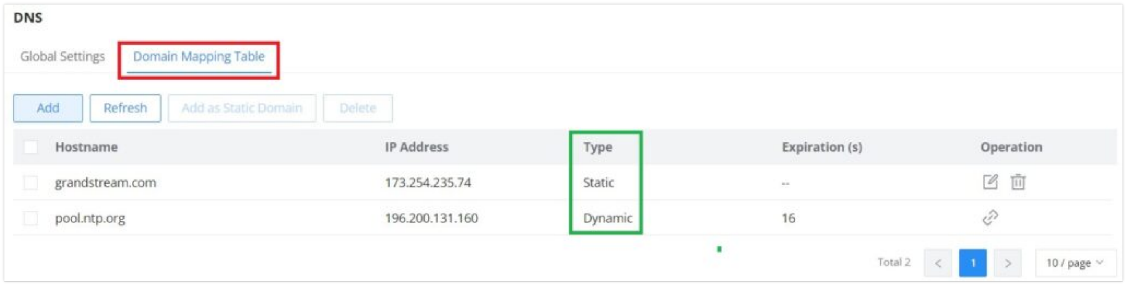
DNS – Global Settings

Up to 8 Domain Suffixes and 8 DNS Servers can be added. To add a Domain Suffex 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.

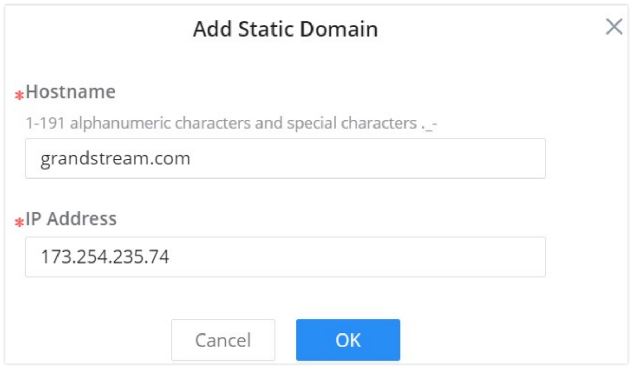
Domain Mapping Table

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



DNS – Domain Mapping Table

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



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).

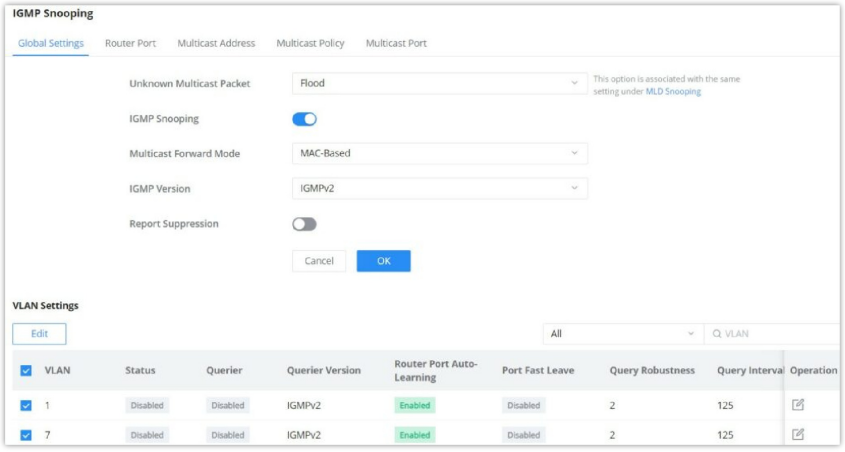
IGMP Snooping

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.



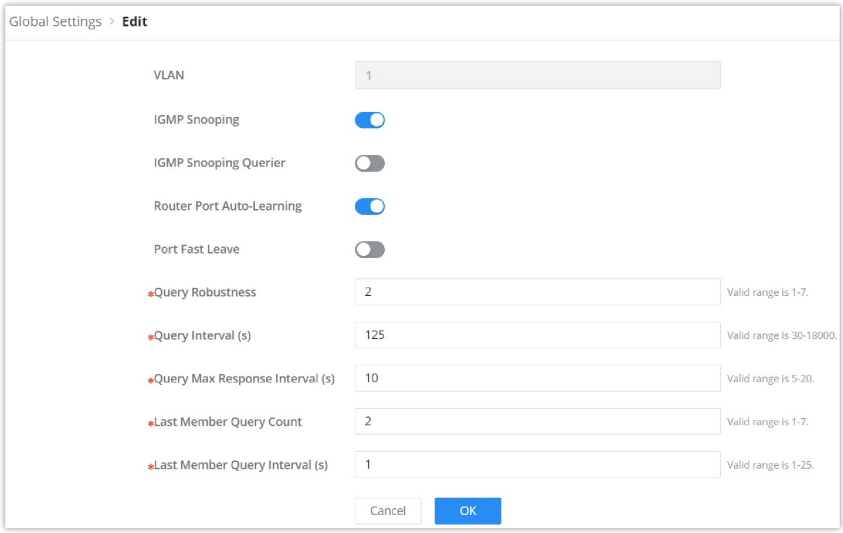
IGMP Snooping Global Settings

Unknown Multicast Packet	Select an action for switch to handle with unknown multicast packet. • **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 GlobaI IGMP Snooping
Multicast Forward Mode	Set the Multicast Forward Mode. • **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.

IGMP Snooping Global Settings

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



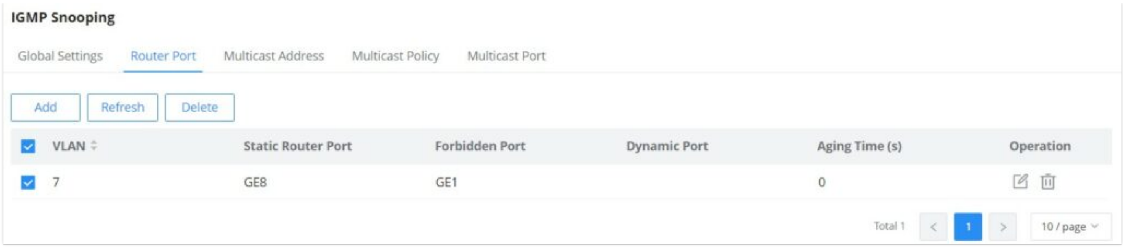
IGMP Snooping Edit VLAN

VLAN	Displays the selected VLAN
IGMP Snooping	Click on the toggle button to enable IGMP Snooping for the selected VLAN.
Router Port Auto-Learning	Click on the toggle button to learn router port by IGMP query.
Port Fast Leave	Select Enable/Disable Fast Leave feature for the desired port. ***Note:*** *If Fast Leave is enabled for a port, the switch will immediately remove this port from the multicast group upon receiving IGMP leave messages.*
Query Robustness	Set a number which allows tuning for the expected packet loss on a subnet. *The valid range is 1-7*
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. ***Note:*** *The valid range is 5-20 in seconds.*
Last Member Query Count	After quering for specified times and still not receiving any response from the subscribed member, GWN7800 series switches will stop transmitting data to the related GE port(s). ***Note:*** *The valid range is 1-7*
Last Member Query Interval (s)	The maximum time interval between counting each member query message with no responses from any subscribed member. ***Note:*** *The valid range is 1-25 in seconds*

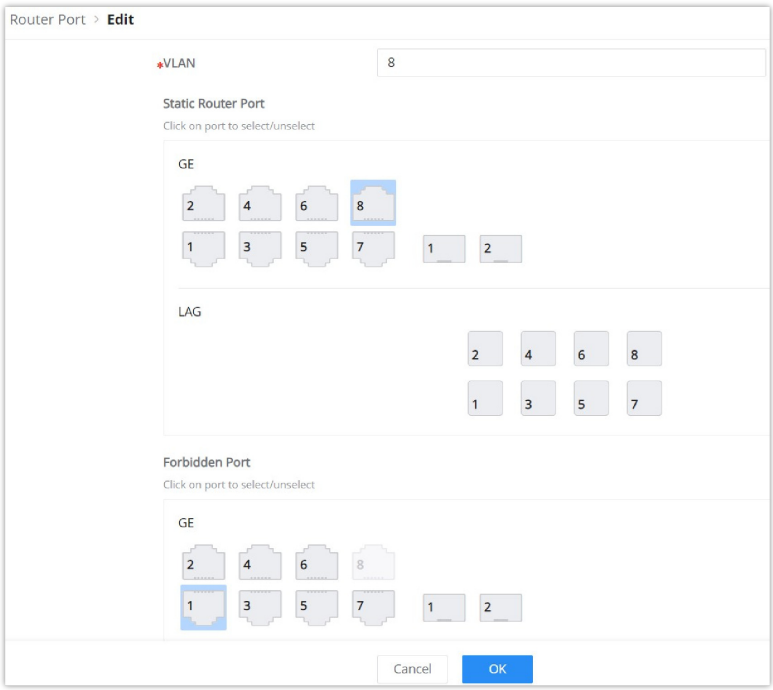
IGMP Snooping Edit VLAN

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.



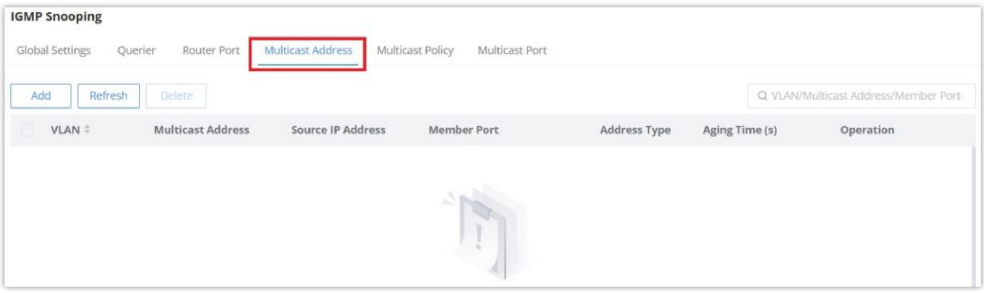
IGMP Snooping Router Port



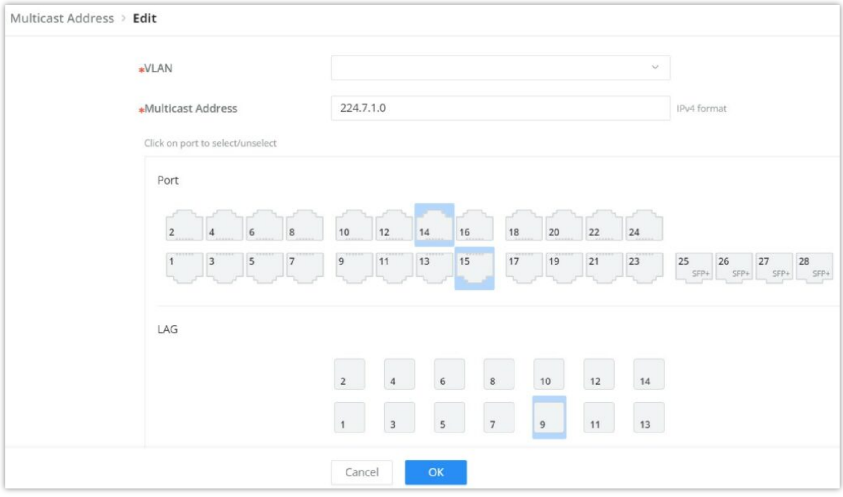
IGMP Snooping Router Port – add or edit

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" Add button or click "Edit" icon to edit.



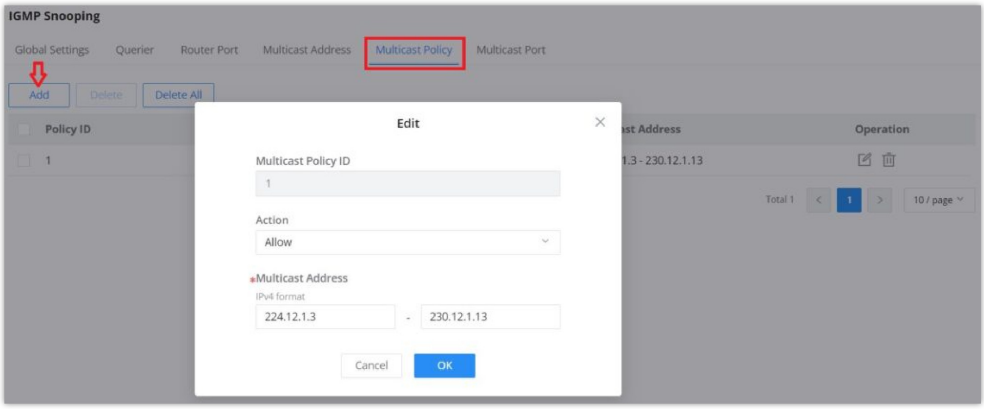
IGMP Snooping Multicast Address page



Add IGMP Snooping Multicast Address

IGMP Snooping Multicast Policy

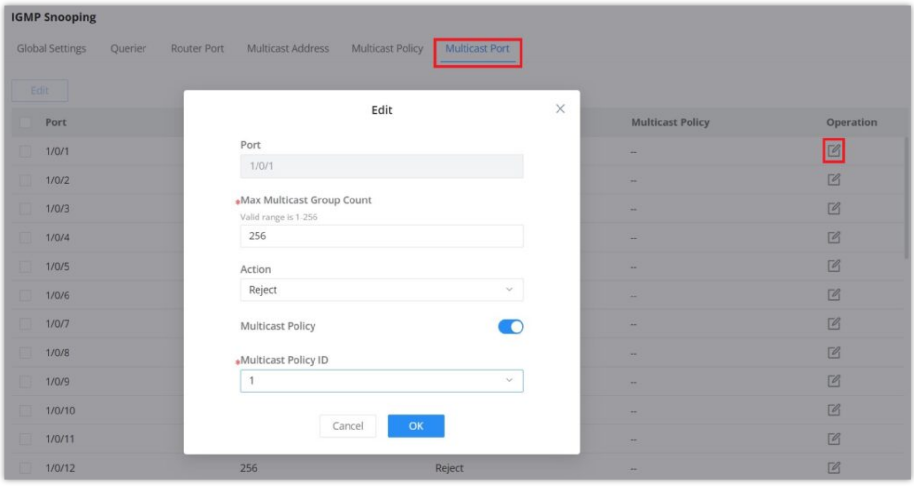
In this page, the user can add a Multicast Policy up to 128 Policy ID to Allow or Reject a range of Multicast Addresses.



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.



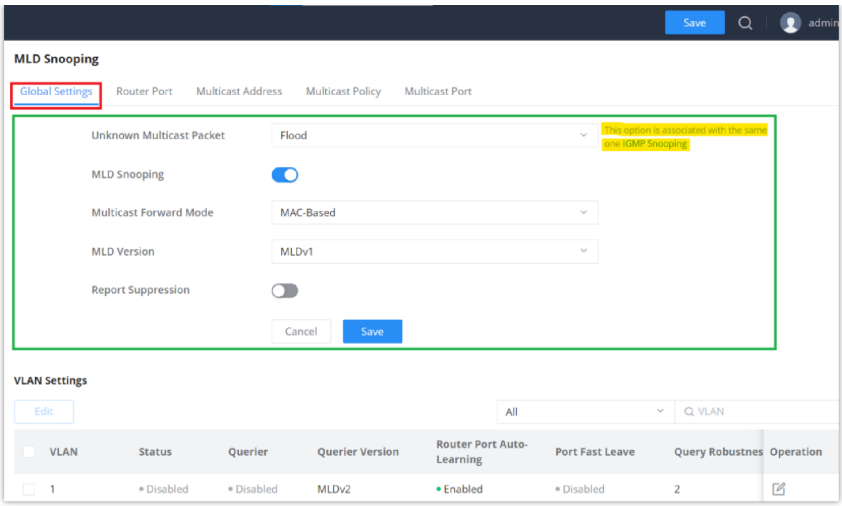
IGMP Snooping Multicast Port

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.

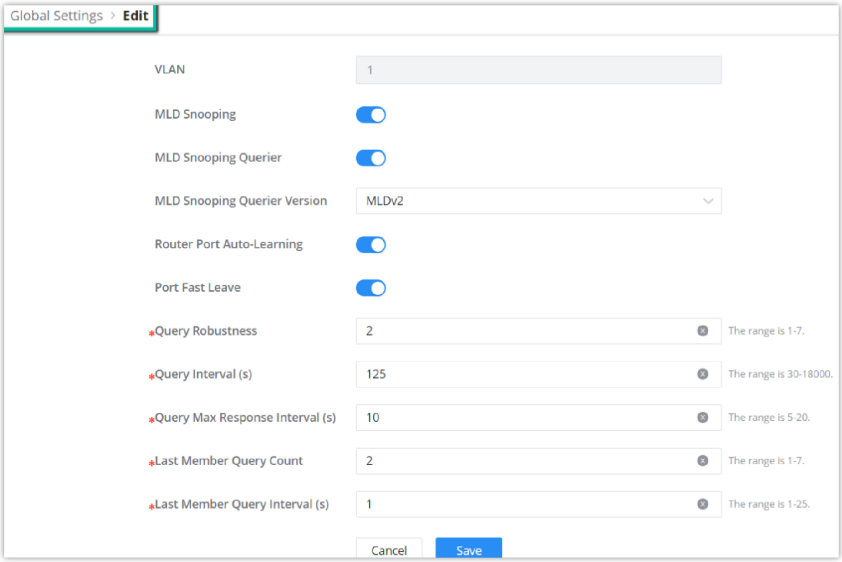


MLD Snooping Global Settings

Unknown Multicast Packet	Select an action for switch to handle with unknown multicast packet. • **Drop:** Drop the unknown multicast data. • **Flood:** Flood the unknown multicast data. • **Forward to Router port:** Forward the unknown multicast data to router port. ***Note:*** *This option is associated with the same one IGMP Snooping.*
MLD Snooping	Enable or disable GlobaI MLD Snooping
Multicast Forward Mode	Set the Multicast Forward Mode. • **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.



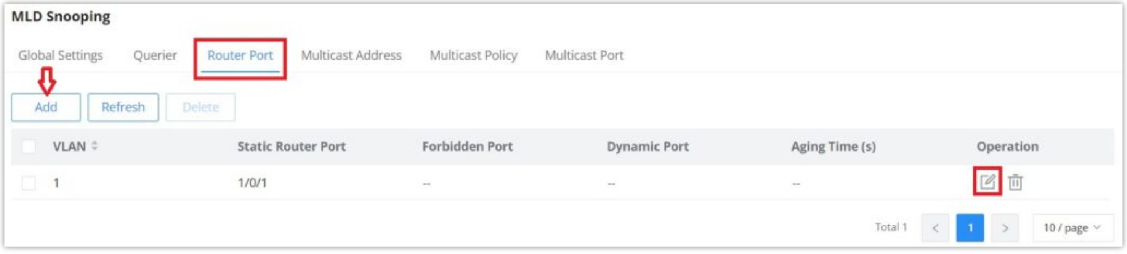
MLD Snooping – Edit VLAN

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. ***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.*
Query Robustness	Set a number which allows tuning for the expected packet loss on a subnet. *The valid range is 1-7*
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. ***Note:*** *The valid range is 5-20 in seconds.*
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). ***Note:*** *The valid range is 1-7*
Last Member Query Interval (s)	Set The maximum time interval between counting each member query message with no responses from any subscribed member. ***Note:*** *The valid range is 1-25 in seconds*

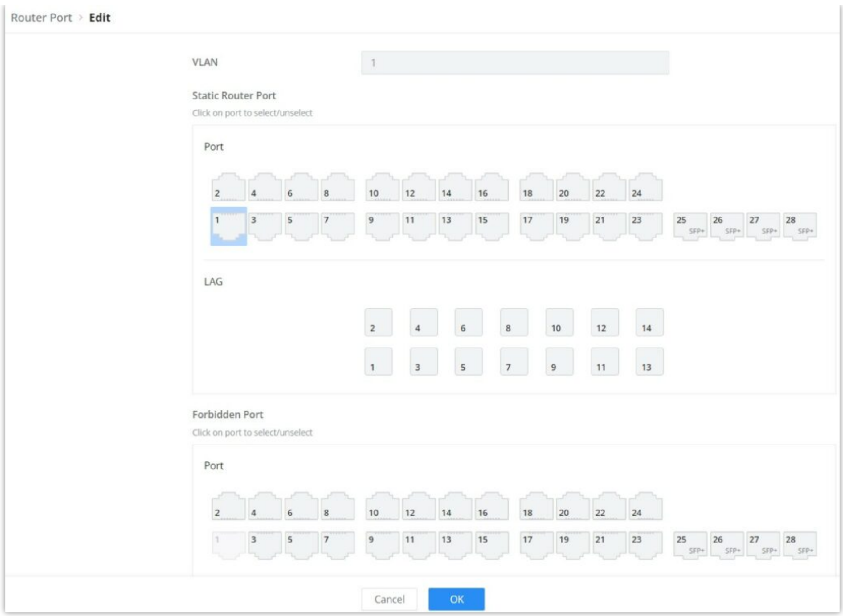
MLD Snooping – Edit VLAN

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.



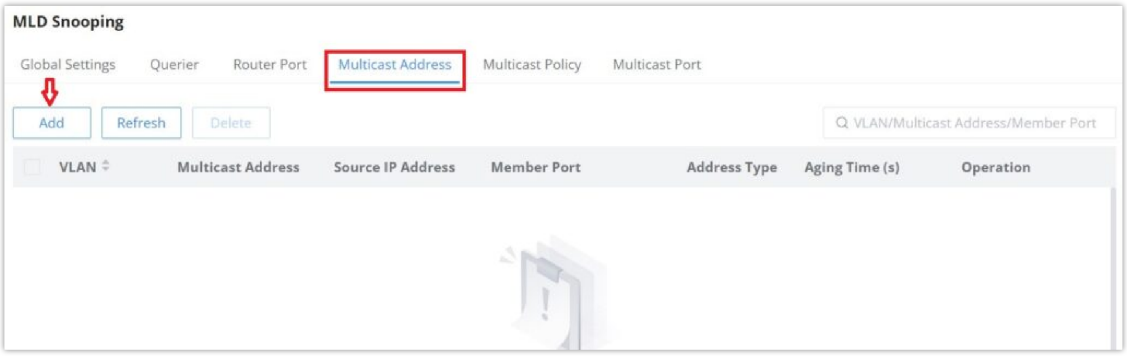
MLD Snooping Router Port page



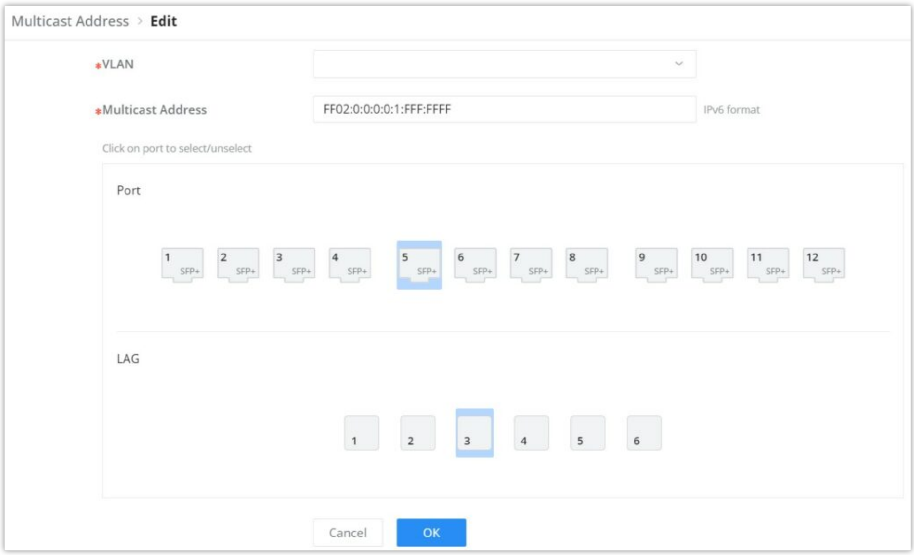
Add MLD Snooping Router Port

MLD Snooping Multicast Address

GWN780x(P) Switches do also support adding static multicast addresses by specifying the VLAN and member port.



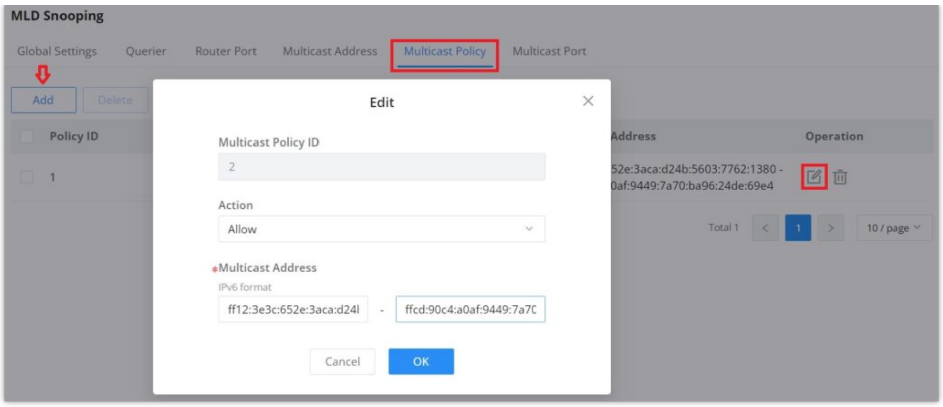
MLD Snooping Multicast Address page



Add MLD Snooping Multicast Address

MLD Snooping Multicast Policy

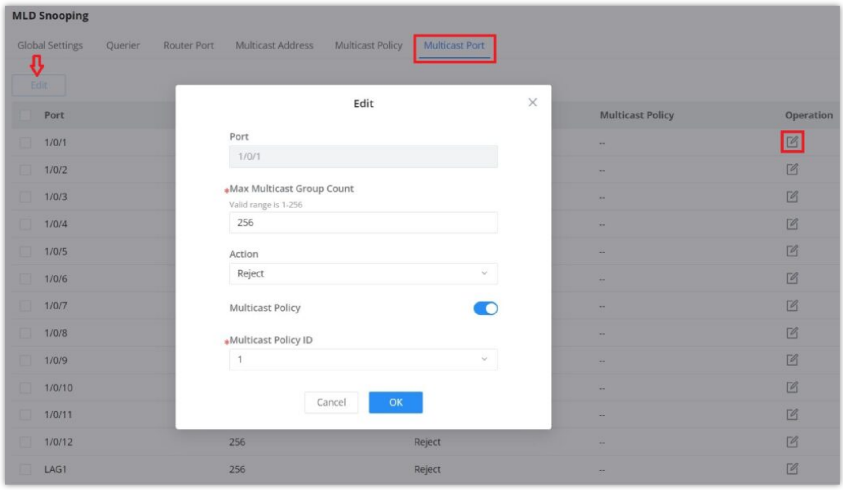
Multicast Policy can be created in this page to allow or reject a range of IPv6 Multicast Addresses. Up to 128 Policy can be created.



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 .



MLD Snooping Multicast Port

Routing

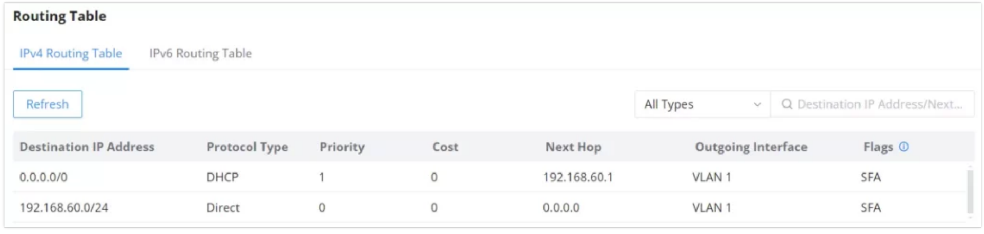
Routing is a process in which the router selects the optimal path according to the destination address of the received data packet and forwards it to the next network node leading to the target network, and the last routing node under this path forwards the data to the target host. (Router refers to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

GWN780x(P) support IPv4 and IPv6 static routing.

Routing Table

The routing table displays all the routes either the dynamic ones added automatically when the user add a VLAN IP Interface or the static ones added manually by the user. It's also possible to click on "**Refresh**" button to update the list.

Please navigate to **Web UI** → **Routing** → **Routing Table** page.



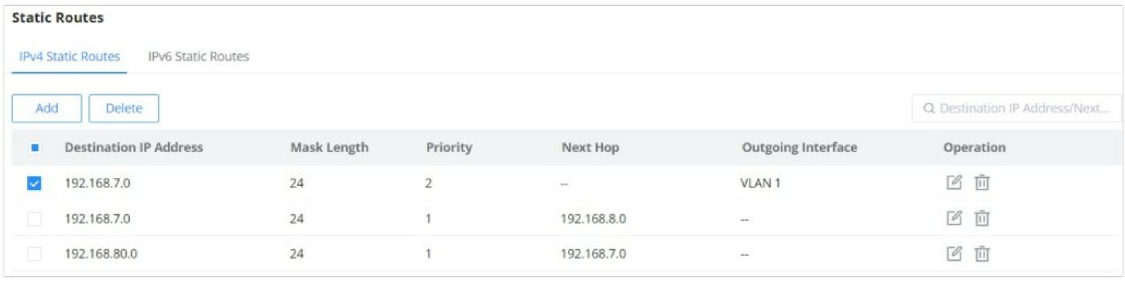
Routing table

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.

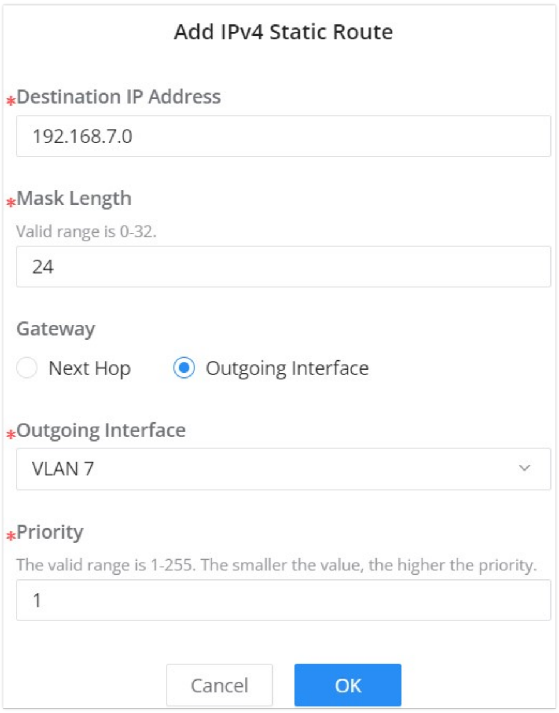
To add a static route, please navigate to **Web UI → Routing → Static Routes** page.



Static Routes

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 static route

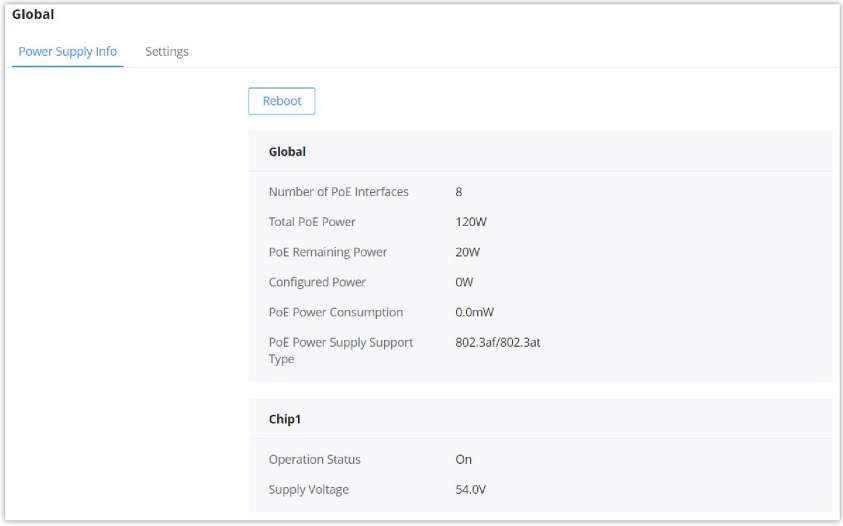
PoE

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.

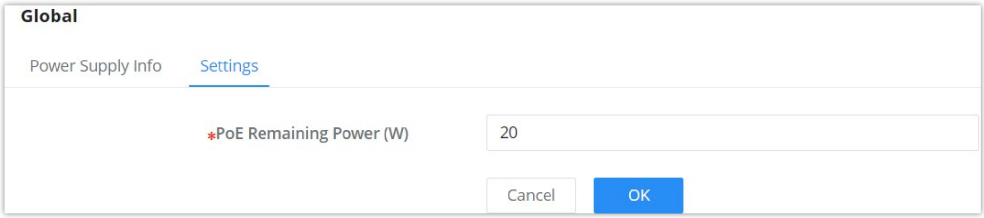


PoE Global

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

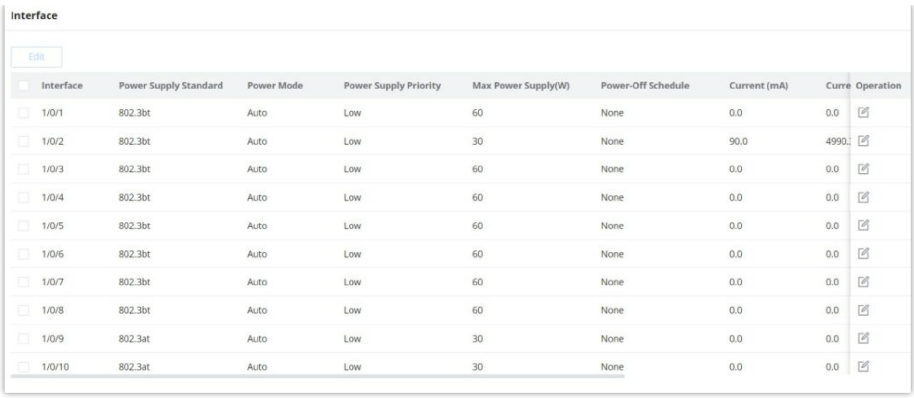
Application scenarios:

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.

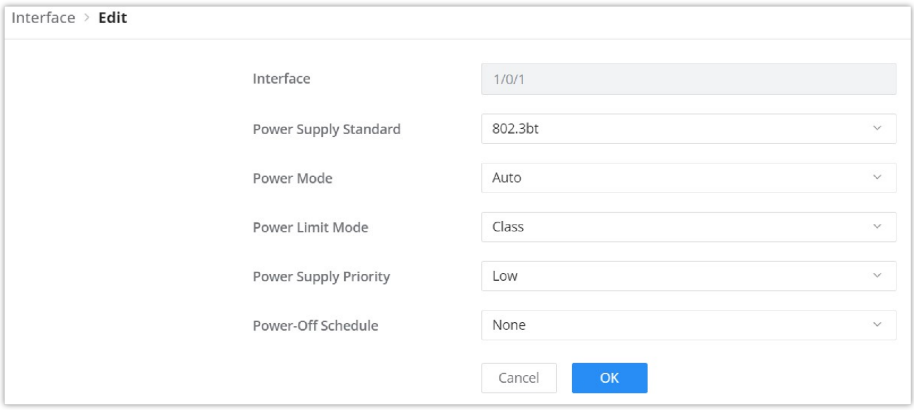
Interface PoE configuration

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 page



PoE – Interface edit port

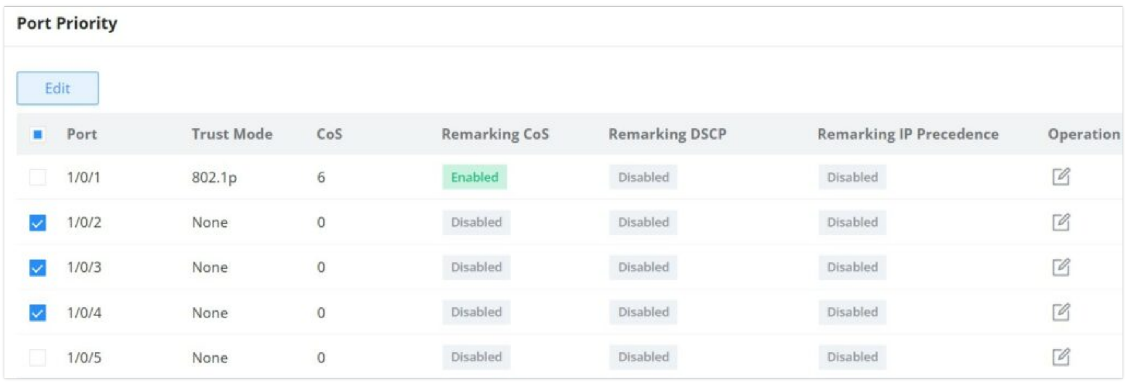
QoS

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

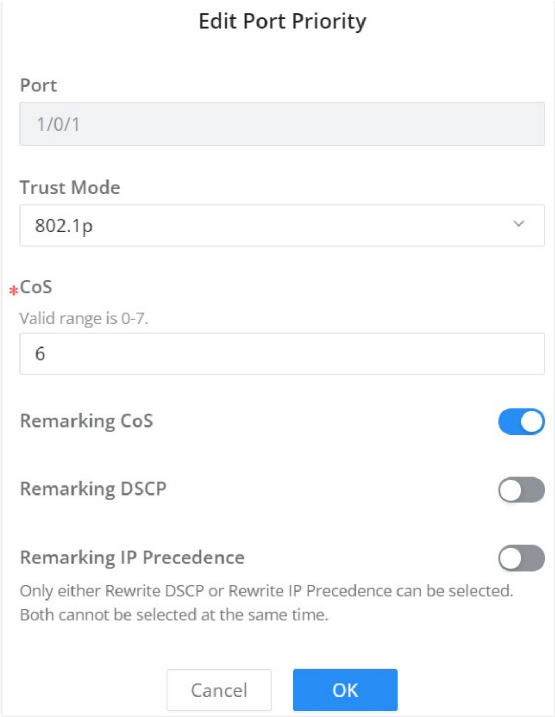
In this page, the user can enable/disable port priority for each interface (port/LAG), supported modes are (CoS, DSCP, CoS-DSCP or IP-Precedence).

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



QoS – Port Priority

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



Edit Port Priority

Port	Displays the selected port GE/LAG.
Trust Mode	Select the QoS operation mode: ● **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 Mappging 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. ● **IP-Precedence:** The IP precedence is a 3-bit field in TOS that threats 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), *the default is 0.*
Remarking CoS	Set whether to enable Remarking CoS function of outgoing packets, *which is disabled by default.*
Remarking DSCP	Set whether to enable Remarking DSCP function of outgoing packets, *and it is disabled by default.*
Re-marking IP Precedence	Set whether to enable Remarking IP Precedence function of outgoing packets, *and it is disabled by default.* ***Note** : Only one of DSCP and IP Precedence re-marking can be enabled.*

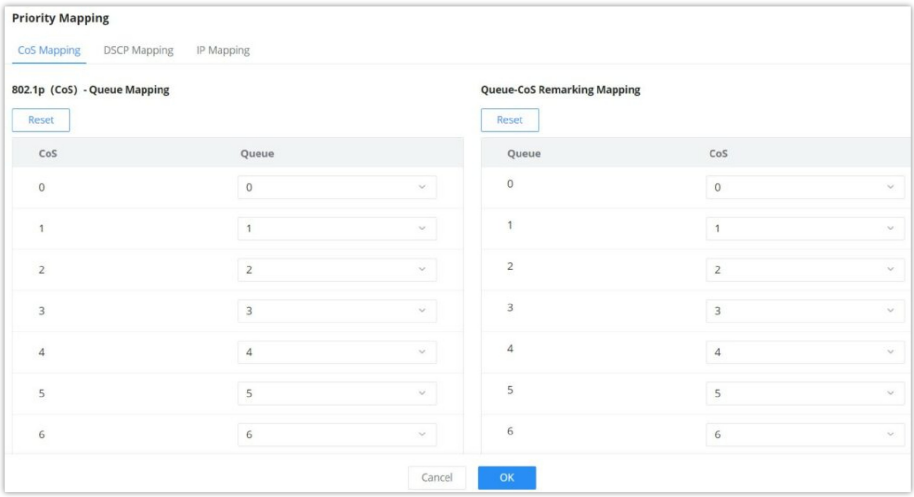
QoS Port Priority

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**

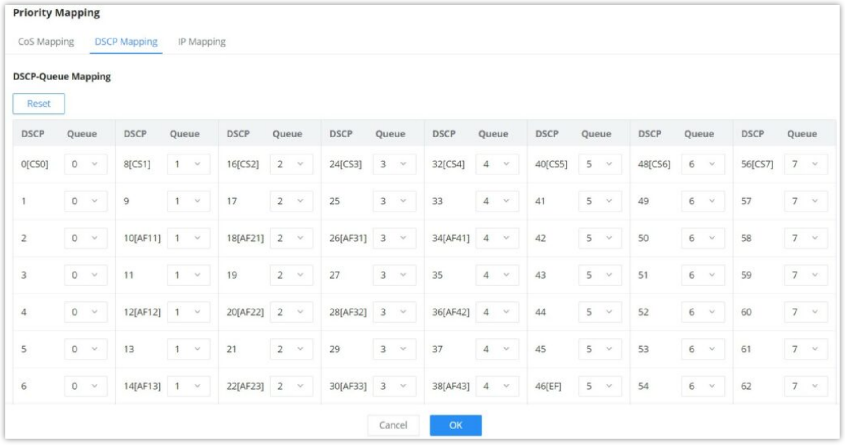
Shows the mapping relationship between queues and CoS remarking priorities.



CoS Mapping

- **DSCP Mapping**

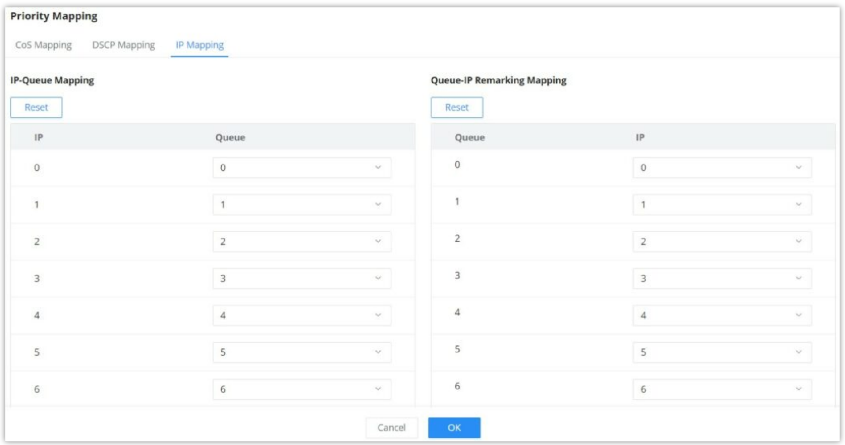
Shows the mapping relationship between DSCP values and queue priorities.



DSCP Mapping

- **IP Mapping**

Shows the mapping relationship between IP priority and queue.



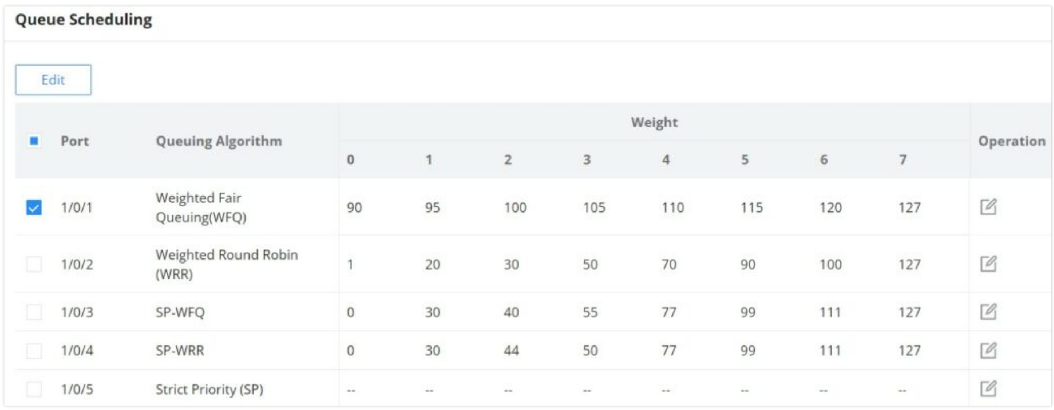
IP Mapping

Queue Scheduling

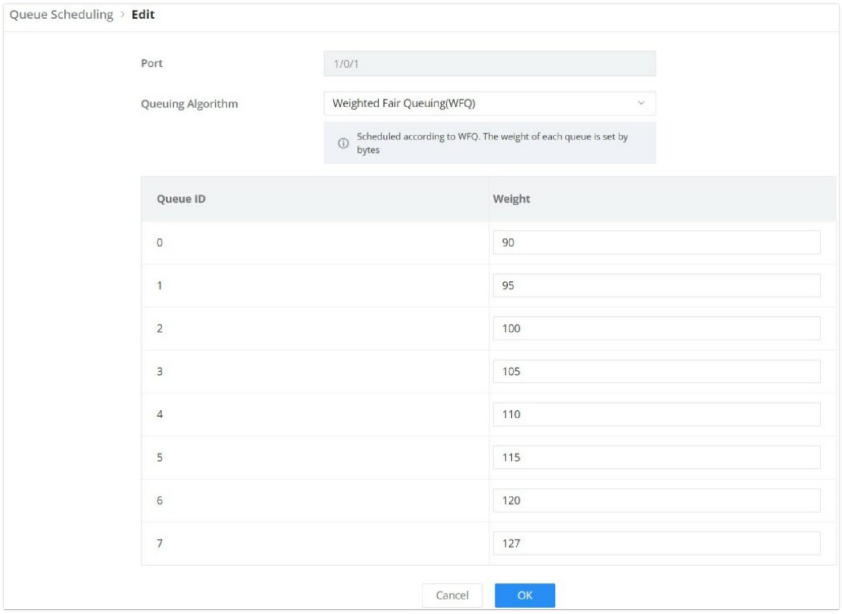
When congestion occurs in the network, the device will determine the processing order of forwarding packets according to the specified scheduling policy, so that high-priority packets are preferentially scheduled.

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

- **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.*
- **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.
- **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.
- **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.
- **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

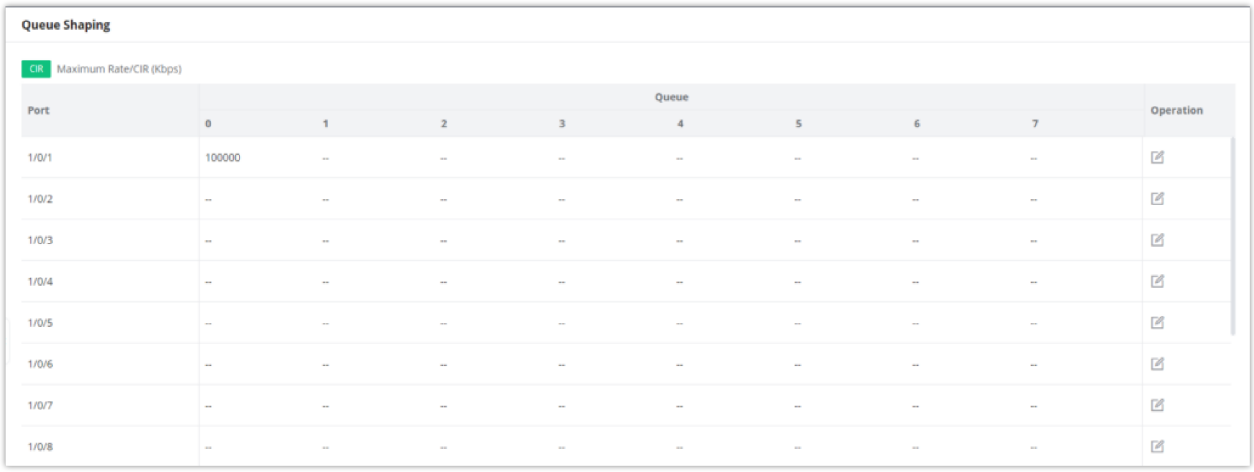


Queue Scheduling – Edit port

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

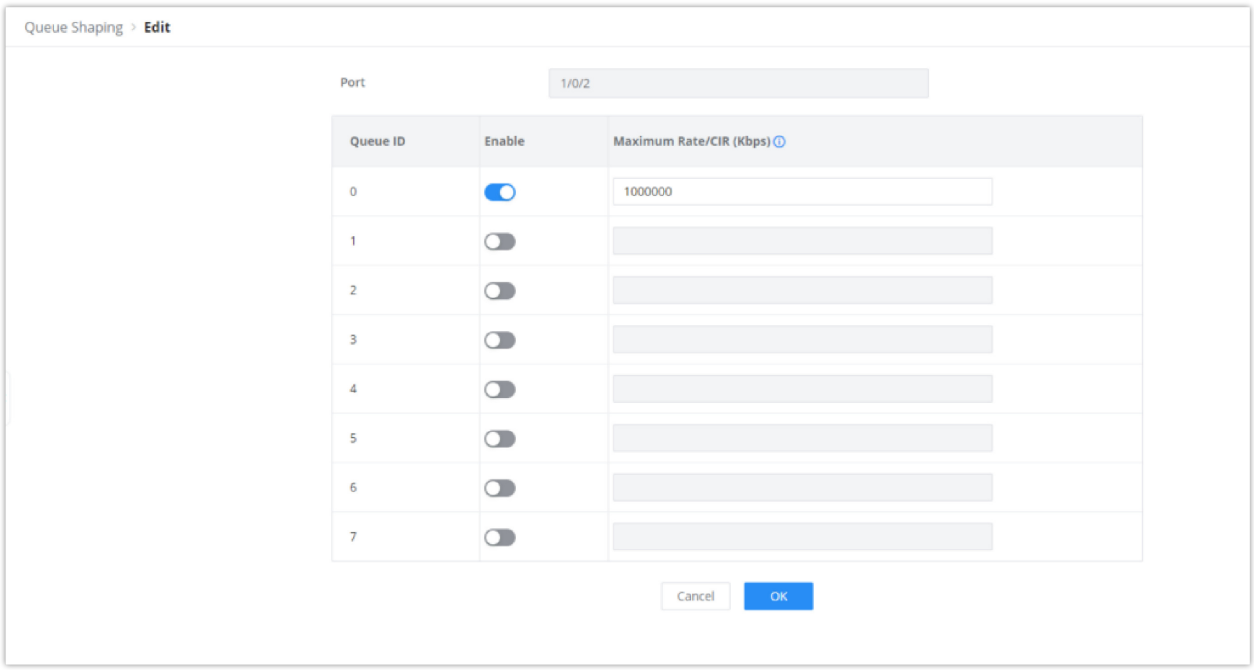
make the limited network resources serve users more effectively, it is necessary to restrict the service flow of users.



Queue Shaping

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

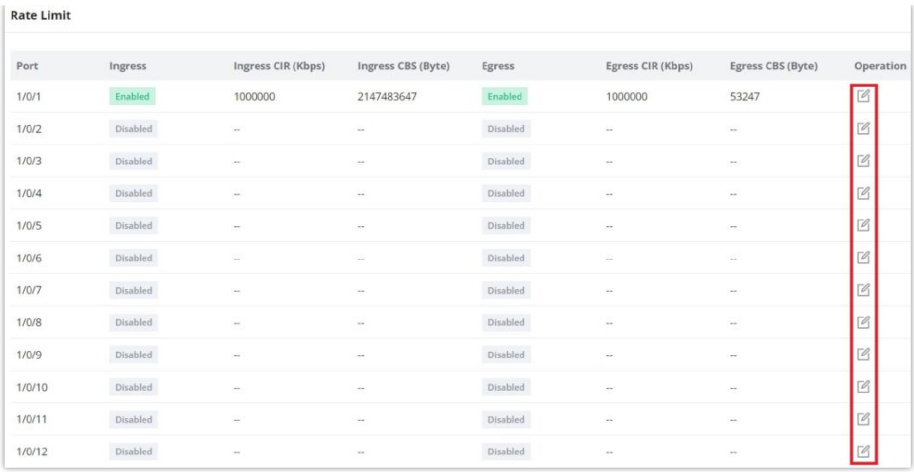
Maximum Rate/CIR (Kbps): Configures the maximum rate of shaping. The value must be an integer between 16-1000000 Kbps, and must be multiples of 16. By default it's the port rate.



Configuration of Maximum Rate

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.

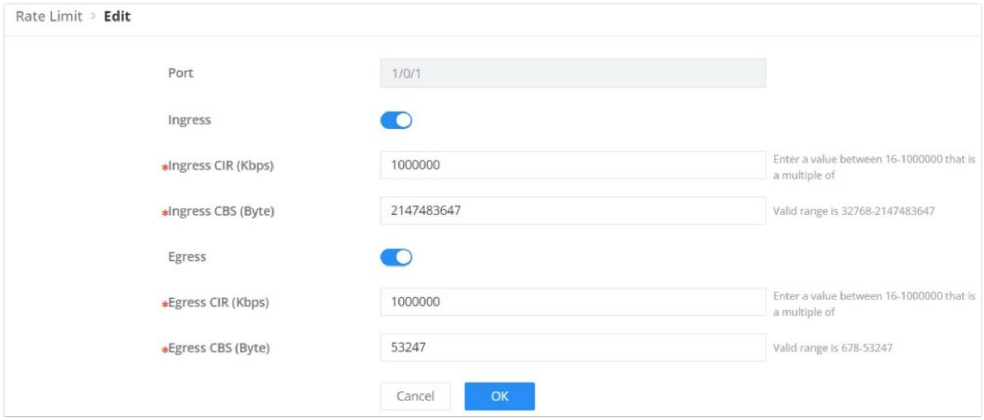


Rate Limit

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 a port

SECURITY

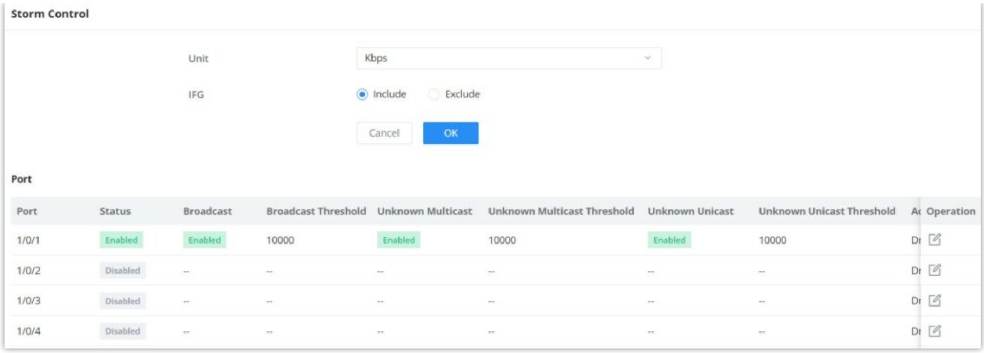
GWN780x(P) Switches series support many tools and features to enhance the security of the device against misconfiguration or attacks.

Storm Control

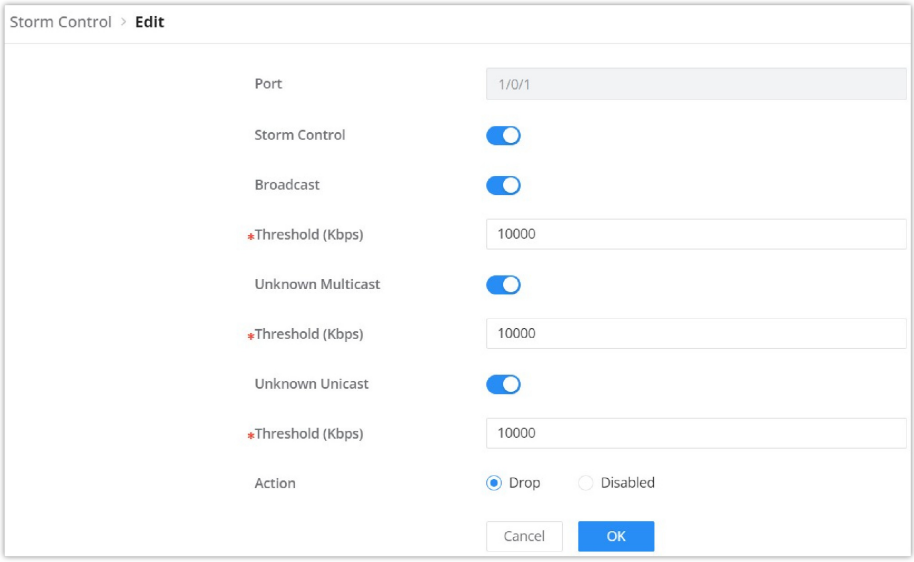
Traffic suppression can limit the rate of broadcast, unknown multicast , unknown unicast, known multicast, and known unicast packets by configuring thresholds , preventing broadcast, unknown multicast packets, and unknown unicast packets from generating broadcast storms. Large traffic impact of known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



Storm Control edit port

Unit	Select Unit: ● kbps: Storm control rate will be calculated by octet-based. ● **pps**: Storm control rate will be calculated by packet-based.
IFG	Select IFG (Inter Frame Gap): ● **Excluded:** Exclude IFG when count ingress storm control rate. ● **Included:** Include IFG when count ingress storm control rate.
Storm Control → Edit	
Port	Displays the selected port.
Storm Control	Select whether to enable Storm Control on the selected port or not.
Broadcast	Set whether to enable the storm threshold setting for broadcast packets. If Enabled Please enter a Treshhold (Kbps). ***Note:*** *The valid range is 16~1000000, which must be a multiple of 16. Default is 10000.*
Unknown Multicast	Set whether to enable the storm threshold setting for the Unknown Multicast packets If Enabled Please enter a Treshhold (Kbps). ***Note:*** *The valid range is 16~1000000, which must be a multiple of 16. Default is 10000.*
Unknown Unicast	Set whether to enable the storm threshold setting for the Unknown Unicast packets. If Enabled Please enter a Treshhold (Kbps). ***Note:*** *The valid range is 16~1000000, which must be a multiple of 16. Default is 10000.*

Action	Select the state of setting • **Drop:** Packets exceed storm control rate will be dropped. • **Shutdown:** Port exceeds storm control rate will be shutdown.

Storm Control

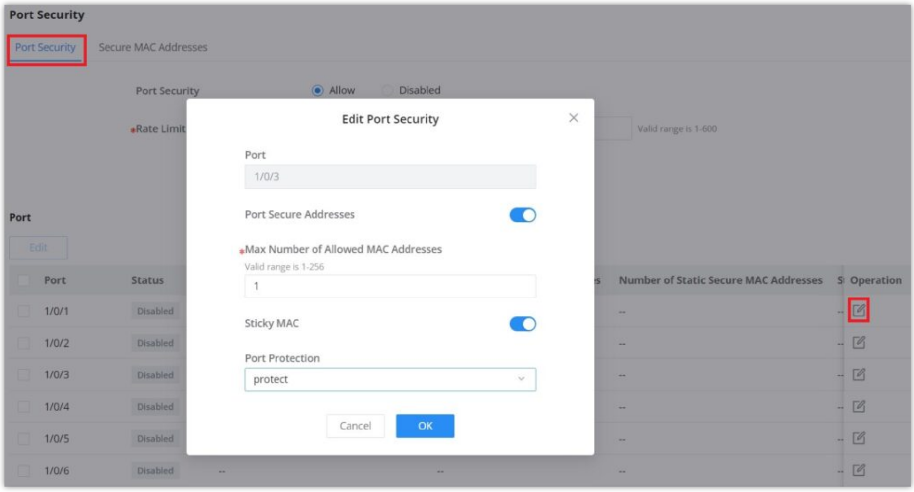
Port Security

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

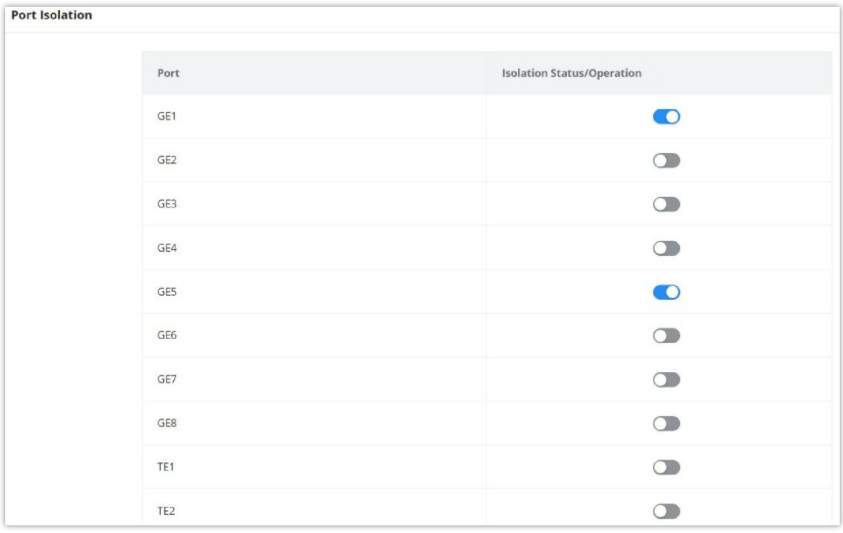
	address exists, the switch considers that there is an attack by an illegal user, and will protect the interface according to the port protection configuration (Protect, Restrict or Shutdown).
Sticky MAC	When the port security is enabled, the Sticky MAC function can be enabled, by default it's disabled . 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	Set the protection action when the number of MAC addresses learned by the interface reaches the maximum number or static MAC address flapping occurs . There are three modes **(Protect, Restrict or Shutdown)**, the default is Protect. ● **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. ***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.*

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

ACL

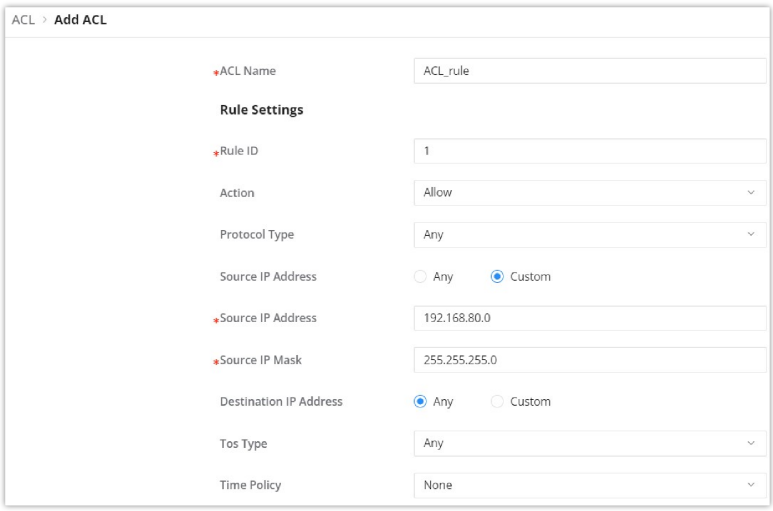
Access control list (ACL) is a collection of one or more rules. A rule is a judgment statement that describes the matching conditions of a packet. These conditions can be the source address, destination address, port number, etc. of the packet. ACL is essentially a packet filter, and the rule is the 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/IPv6 ACL

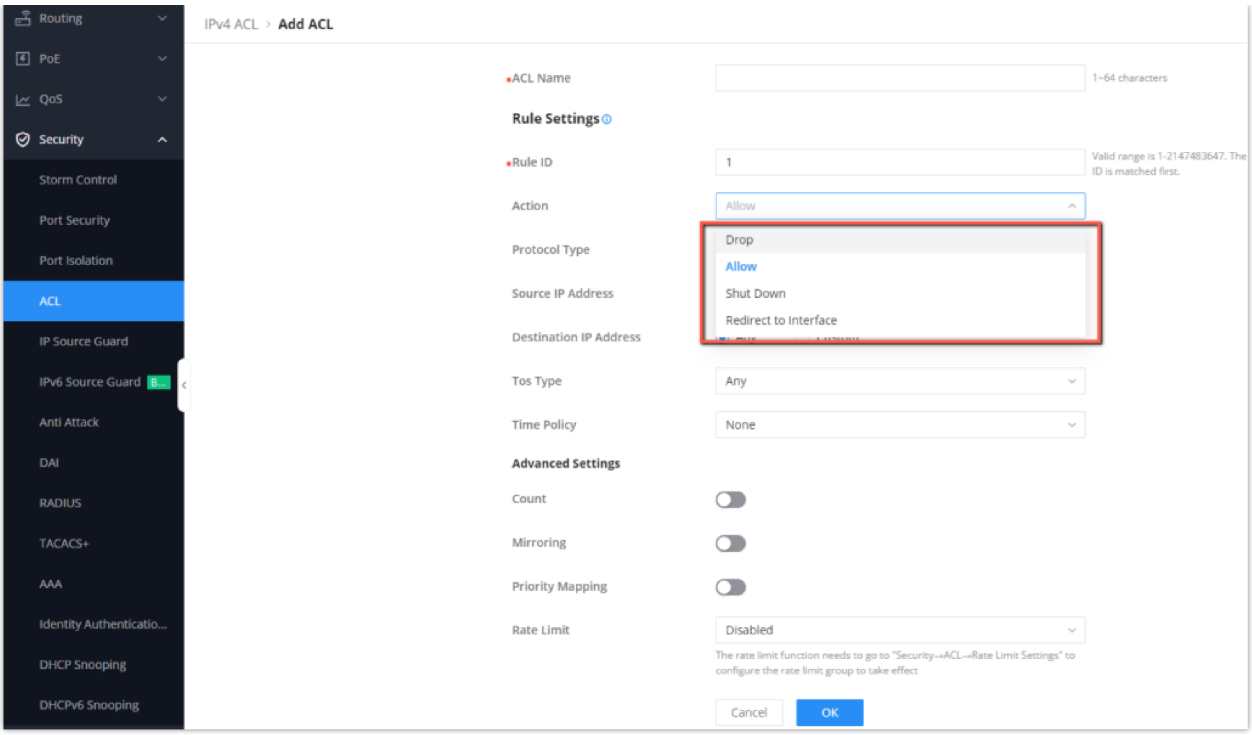
To add an IPv4 or IPv6 ACL rule, navigate to **Security → ACL → IPv4 tab or IPv6 tab**, then click on "**Add**" button to add an IPv4/IPv6 based ACL rule.



ACL – IPv4/IPv6

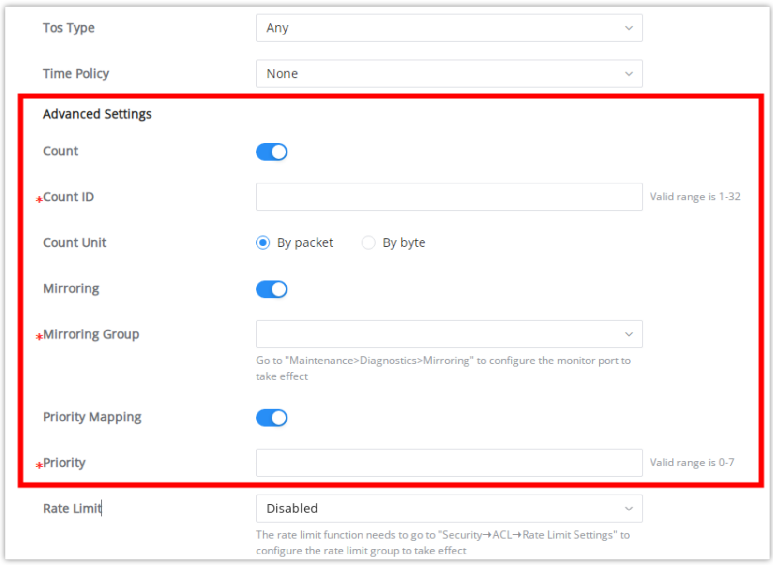
The rules action can be defined in one of the four ways below:

- **Drop**: This action denies or blocks traffic that matches the specified ACL rule, which prevents the packet from being forwarded through the network.
- **Allow**: This action permits traffic that matches the ACL rule, allowing the packet to pass through and continue to its destination.
- **Shut Down**: This action disables the interface or port that the traffic is passing through if the ACL rule is triggered, effectively stopping all traffic on that interface.
- **Redirect to Interface**: This action forwards the traffic matching the ACL rule to a different interface than it was originally destined for, often used for traffic monitoring, load balancing, or security purposes.

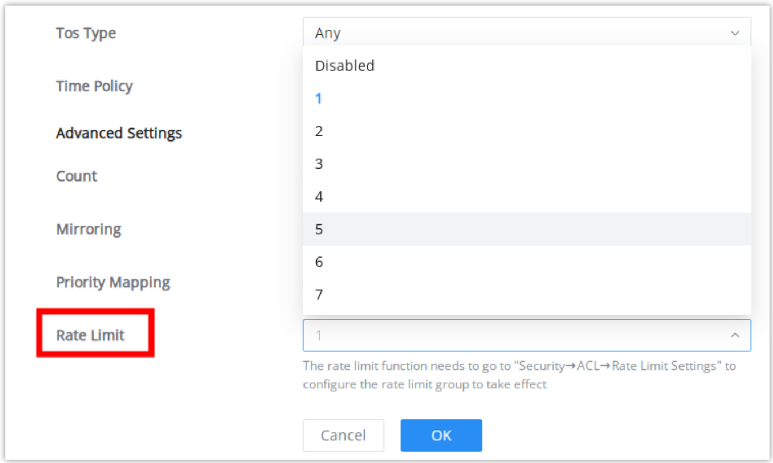


Action Taken by ACL Rule

Some more advanced settings can be defined below:



ACL IPv4/IPv6 – Advanced Settings



ACL IPv4/IPv6 – Rate Limit

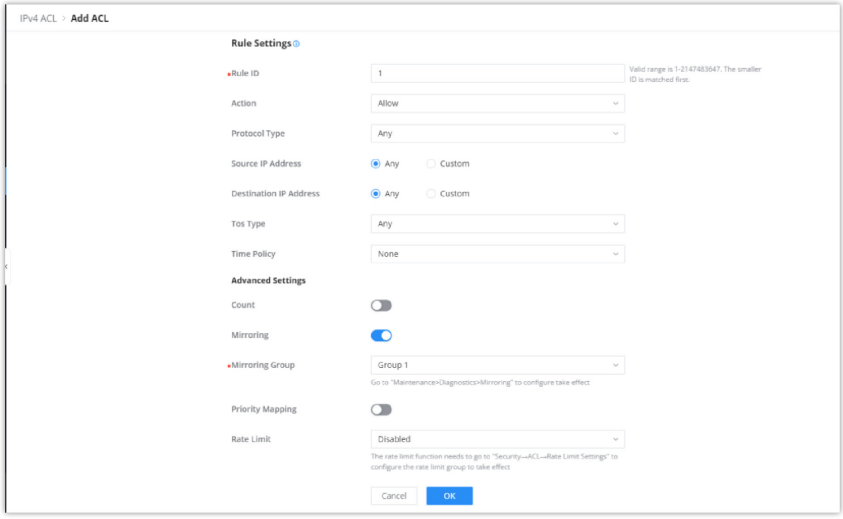
Note

The rate limit function needs to go to "**Security → ACL → Rate Limit Settings**" to configure the rate limit group to take effect.

Configuring an ACL based RSPAN

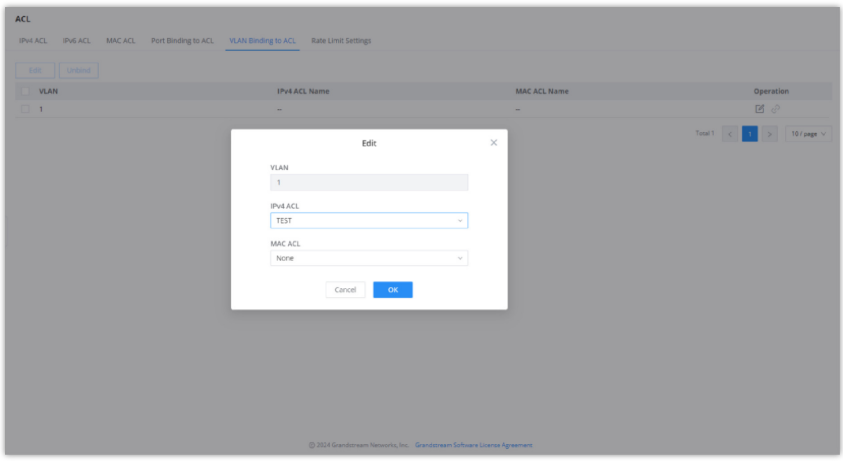
To perform an ACL-based RSPAN, please follow the below steps:

- Select an image group in ACL Image



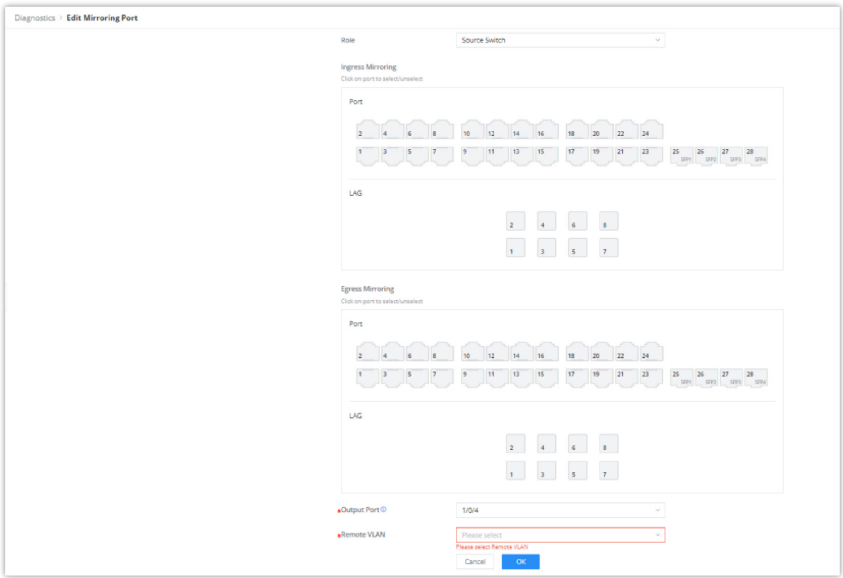
ACL Based RSPAN

- Then,Under **ACL=>VLAN Binding ACL,** select the corresponding port/VLAN binding ACL.



IPv4 ACL VLAN

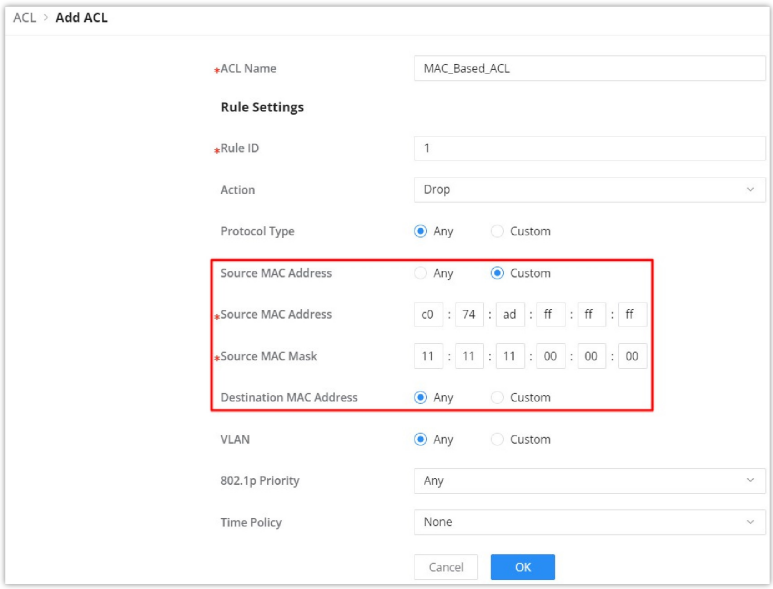
- Then go to **Diagnostics => Mirroring => Setup Mirroring Group**. If you select RSPAN, you can only use it as a source switch and you need to set the output port and remote VLAN.



Setup Mirroring Group

MAC ACL

To add an ACL based on MAC address, on the MAC ACL tab, click on "**Add**" button to add an ACL rule, then configure the **Source MAC Address** and the **Destination MAC Address** accordingly. Please refer to the figure below:



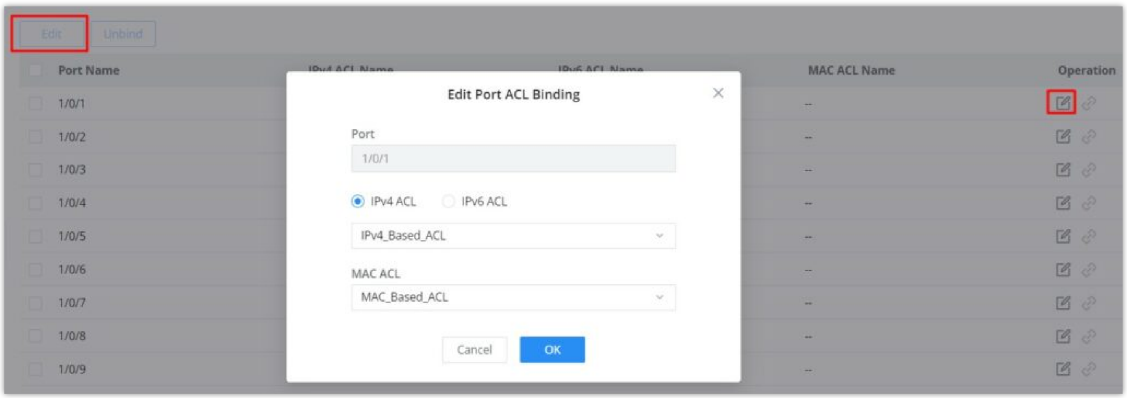
MAC address based ACL

Port Binding to ACL

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

To apply IP/MAC ACL rules on multiple ports, select the ports first then click on "**Edit**" button, then select the IP and MAC ACL rule from the drop-down list.

To apply the ACL rule on a specific port, click on "**Edit icon**" on the right side of the page as shown below:



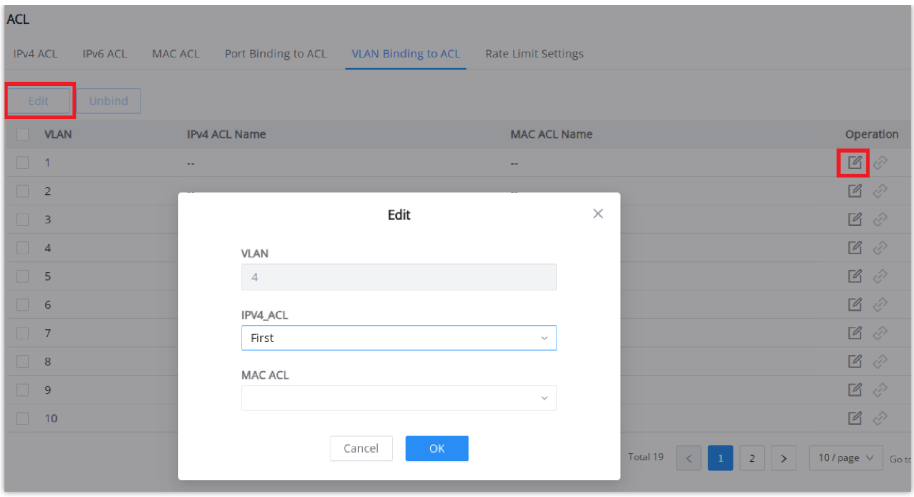
ACL Binding

VLAN Binding to ACL

On this page, the users can bind the IP/MAC ACL rule to a VLAN(s), to apply the ACL rules to multiple VLANs, first check the VLANs from the list then click on "**Edit**" button, select the ACL rule from the drop-down list under IP/MAC ACL.

For example: if the IP/MAC ACL rule is configured with rate limit, and then bound to a VLAN, the bandwidth limit will be applied to the specified VLAN.

refer to the figure below:

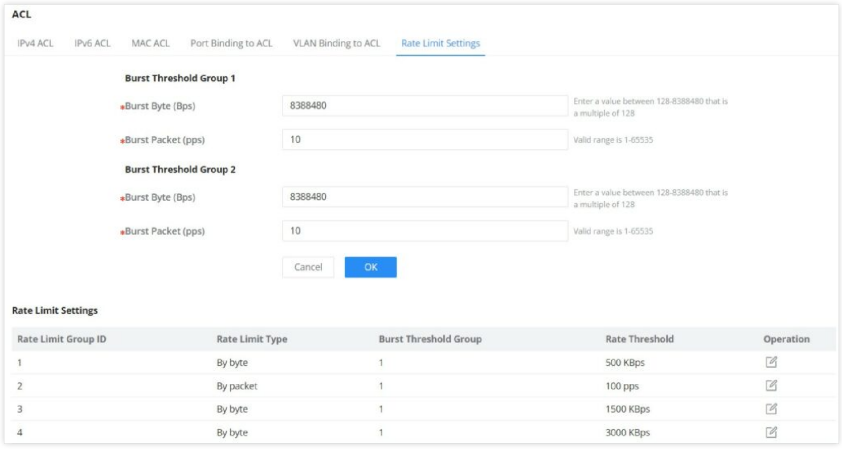


VLAN Binding to ACL

Rate Limit Settings

On this page, the users can configure the rate limit settings.

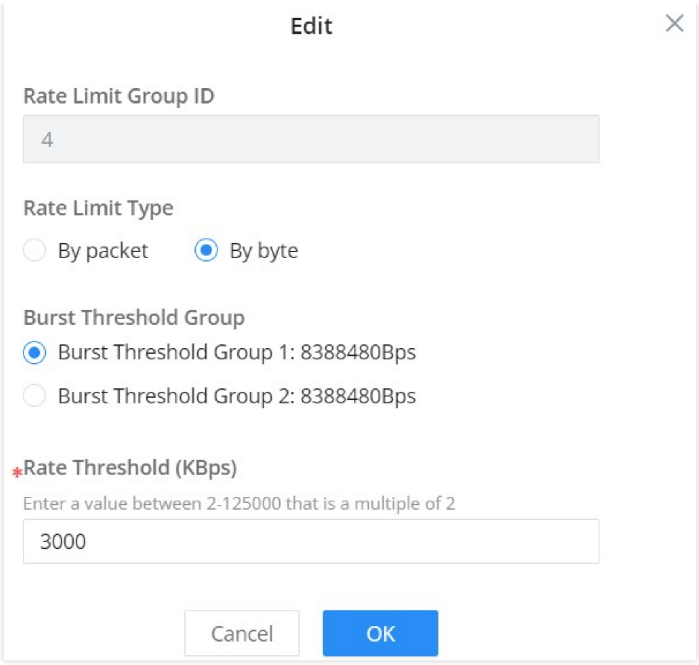
The **Burst Threshold Group 1 and Group 2** are two groups (preset) to limit the traffic burst (initial maximum bandwidth) before the Rate Limit configuration takes effect, using either Bps (Byte per second) or pps (Packet per second), then one of them can be selected when the user wants to configure the Rate Limit group. See the figures below:



ACL – Rate Limit Settings

The users can configure up to 128 groups, click on the “Edit icon” under operation column.

1. Select the **Rate Limit Type** either the limit will be by packet or byte.
2. Select the **Burst Threshold Group 1 or 2**.
3. Finally, specify the rate limit accordingly.



ACL – Edit Rate Limit Group

IP Source Guard

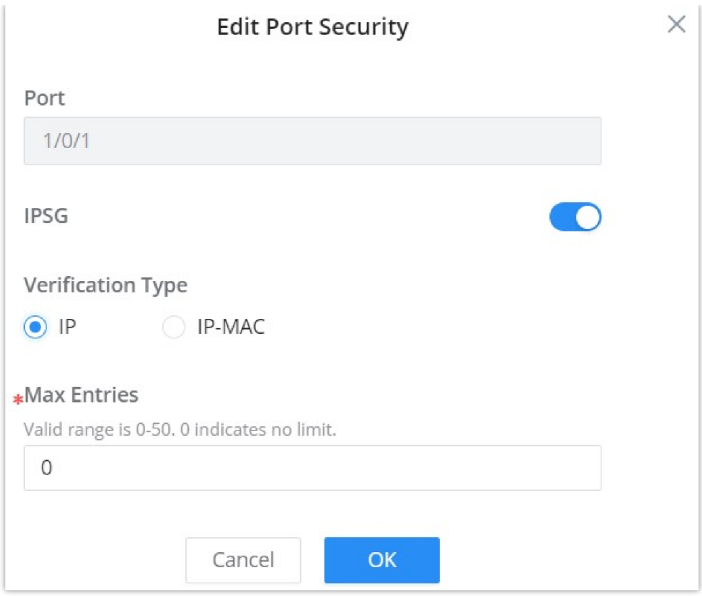
IP source guard is a source IP address filtering technology based on Layer 2 interface. It can prevent malicious hosts from forging IP addresses of legitimate hosts to impersonate legitimate hosts, and also ensure that unauthorized hosts cannot access by specifying their own IP addresses. network or 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.

> **Note:**
>
> It's recommended to enable first DHCP Snooping by navigating to **Security → DHCP Snooping**.

To enable IP Source Guard, first navigate to **Security → IP Source Guard** page, then select the port and click on "**Edit**" to configure the port.

IP Source Guard

Then, select the **Verification Type** where either the verification will be based on IP addresses or both IP and MAC addresses. **Max Entries** limits the number of IP/MAC addresses (e.g. devices) where 0 indicates no limit.

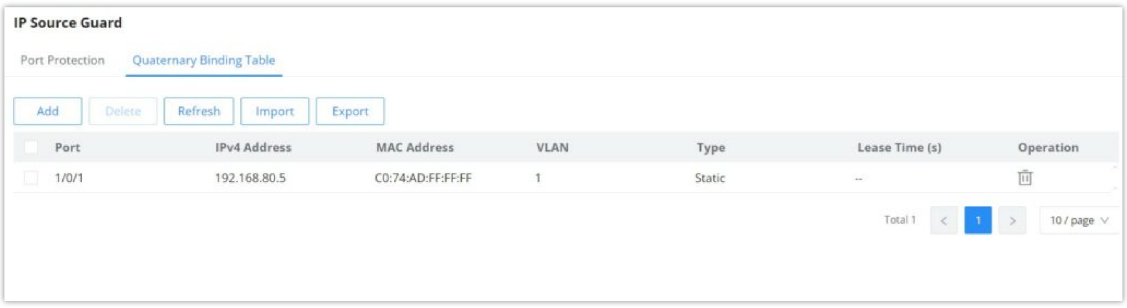


IP Source Guard – Edit port

In this page displays the dynamic binding (port, IP, MAC, VLAN) generated when DHCP Snooping is enabled on the GWN78xx switches, also the user can add static binding by clicking on "**Add**" button as shown below:

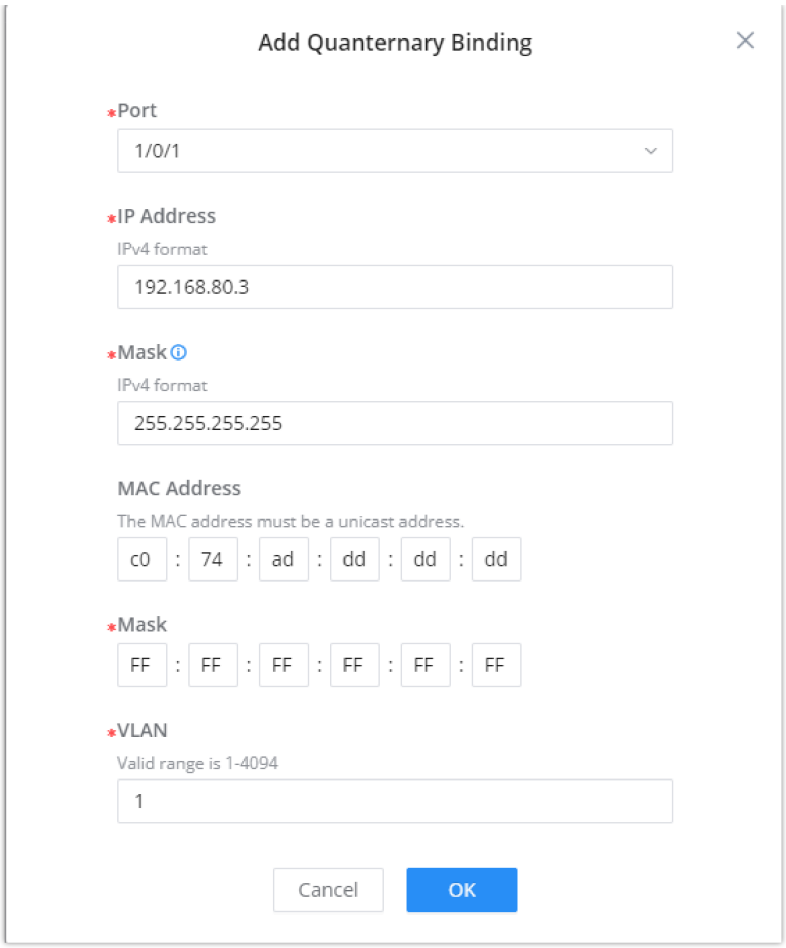
> **Note:**
>
> Dynamic entries require enabling **DHCP Snooping**.

To import or export the list click on **import or export button** respectively.



Quaternary Binding Table

The binding requires to specify the port, IP Address and its mask, MAC address and its mask, and the VLAN ID . These information will be used to verify the traffic and make sure all the traffic is generated by legitimate users.



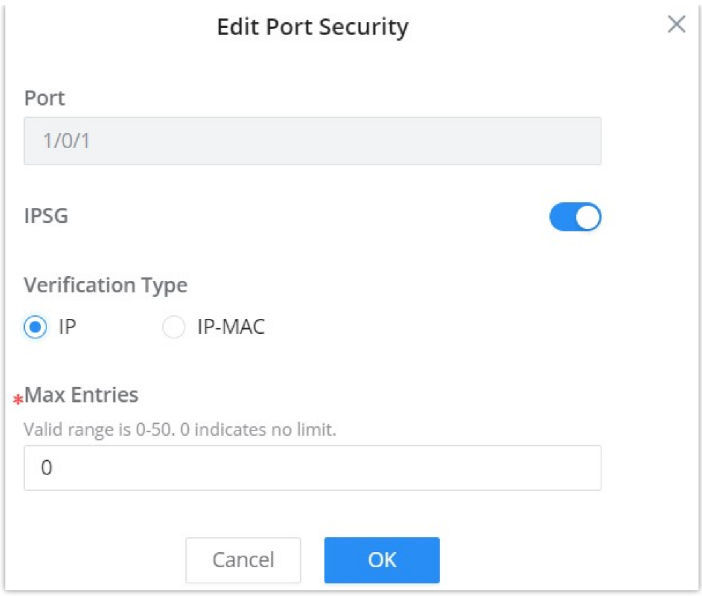
Add Quaternary Binding

IPv6 Source Guard

IPv6 Source Guard is similar to IP Source Guard (based on IPv4), the only difference is that IPv6 Source Guard filters IPv6 addresses.

IPv6 Source Guard

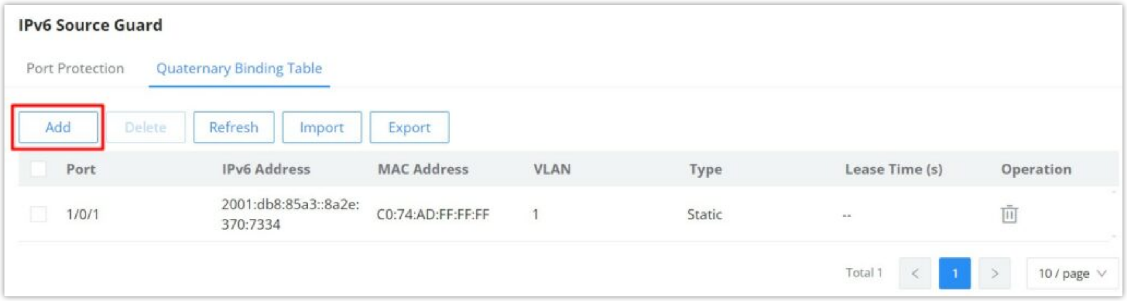
To enable IPv6 Source Guard on a port, select the port then click on “Edit” button to under operation column, then select the **Verification Type** and specify the **Max Entries**.



IPv6 Source Guard – Edit port

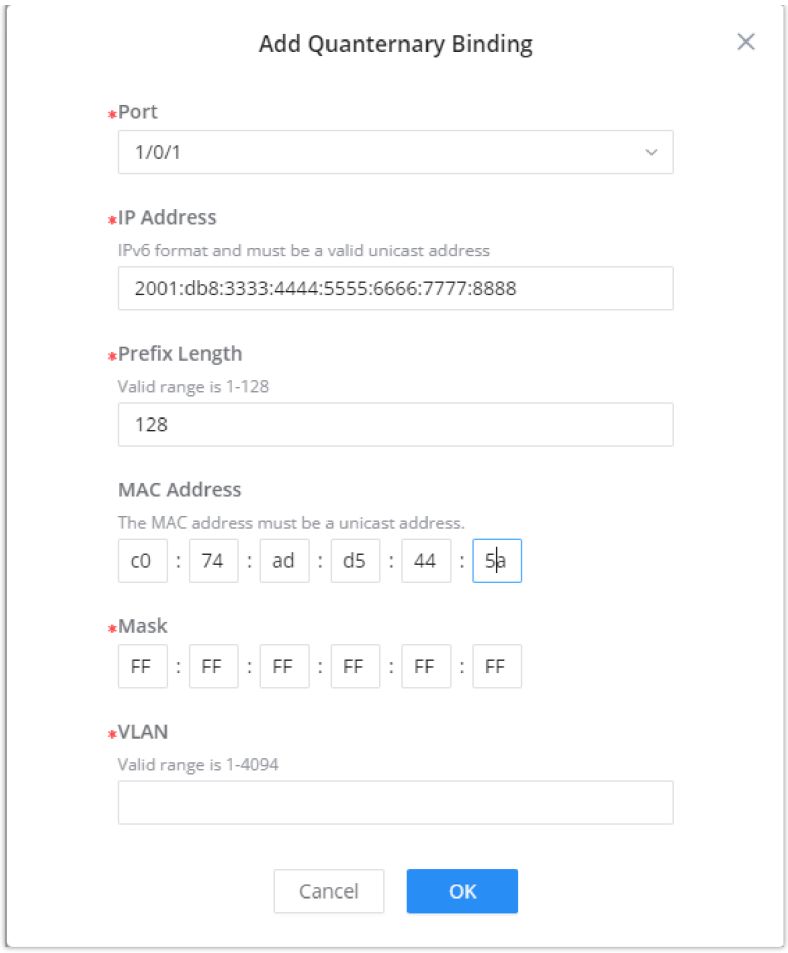
On this tab, the user can see the list of binding both static and dynamic (DHCP Snooping must enabled).

To add a static entry, click on "**Add**" button, it's also possible to import or export the list as shown below:



IPv6 Quaternary Binding Table

Specify the binding (port, IP address, MAC Address and VLAN), then click on "**OK**" button to save.



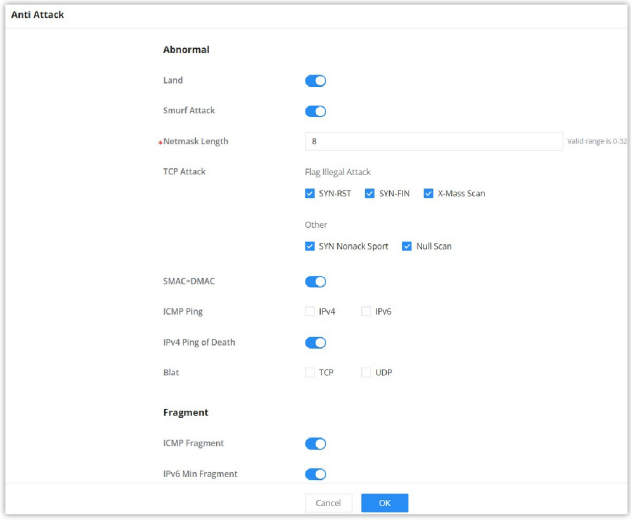
IPv6 Quaternary Binding – edit port

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.



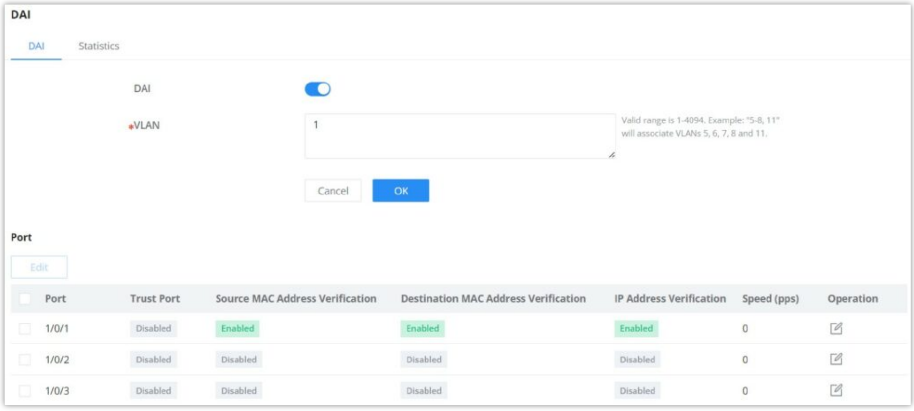
Anti Attack

Dynamic ARP Inspection (DAI)

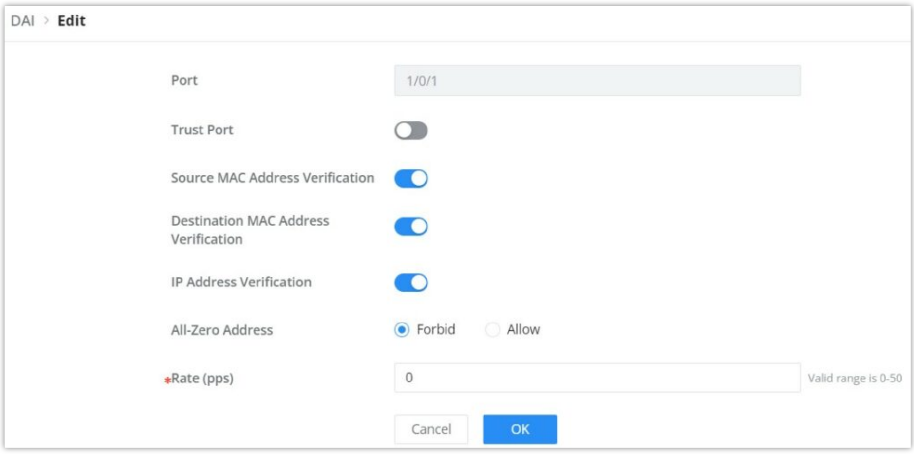
To defend against man-in-the-middle attacks and prevent data of legitimate users from being stolen by the man-in-the-middle, you can enable dynamic ARP inspection. The device compares the source IP, source MAC, interface, and VLAN information corresponding to the ARP packet with the information in the 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 . Then, 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.

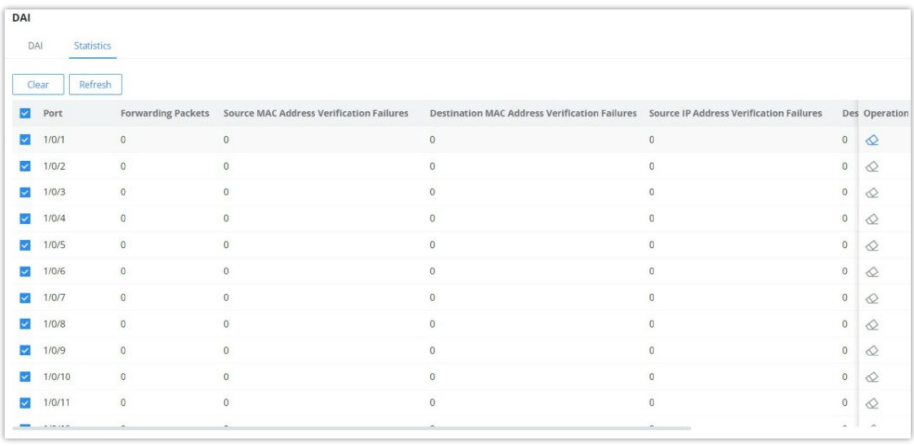


DAI page



DAI – Edit port

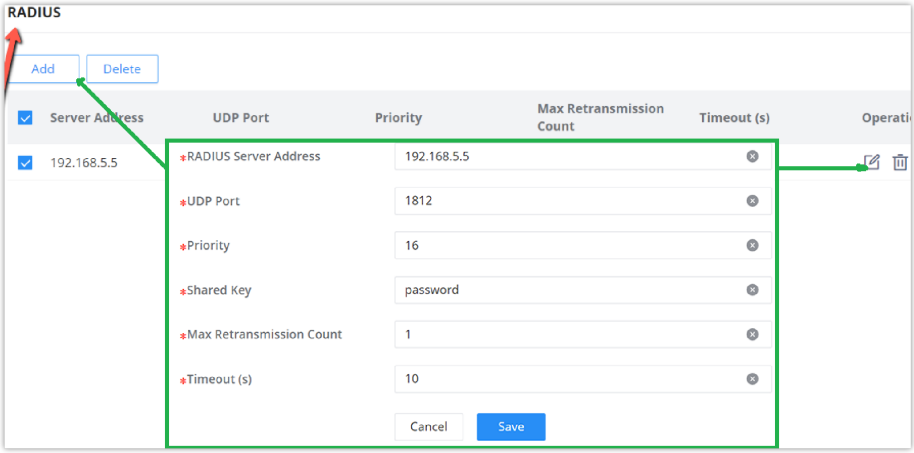
The statistics about DAI activities will be listed here for each port GE/LAG with the options of refreshing the statistics or clearing specified port data.



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.



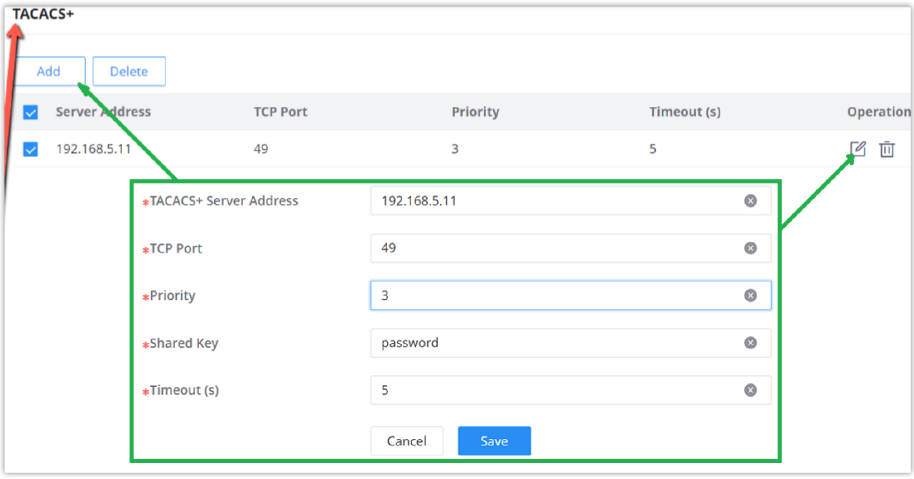
RADIUS

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.



TACACS+

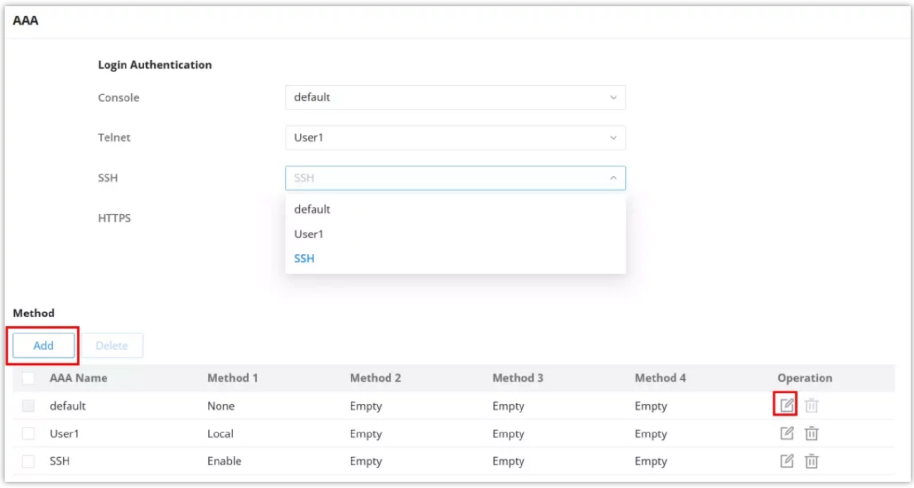
AAA

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:

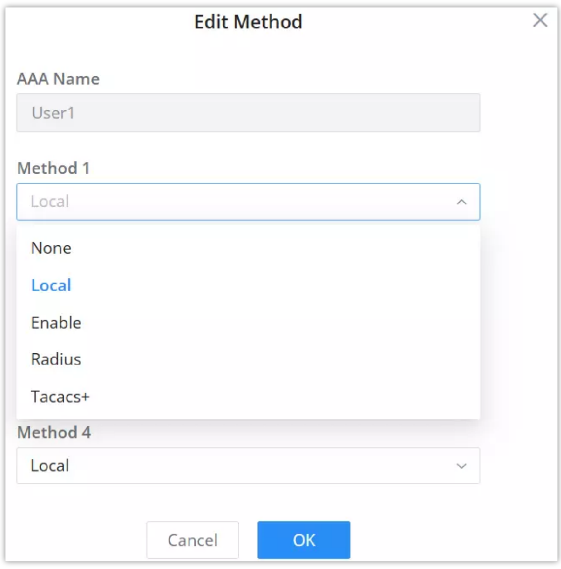
- Authentication , confirming the identity of users accessing the network , and judging whether the visitor is a legitimate network user;
- Authorization , giving different users Different permissions limit the services that the user can use;
- Billing , record all operations during the user's use of 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.



AAA

To add a method click on "**Add**" button and modify a method click on "**modify icon**" as shown above:



Add/Edit a method

Method	Description	Applicability

None	No authentication is performed. Users can log in without a username or password. This setting should generally be avoided due to security risks.	Console, Telnet, SSH, Web UI
Local	Uses the local user database on the switch for authentication. User credentials are stored directly on the switch.	Console, Telnet, SSH, Web UI
Enable	Requires users to enter an enable password to gain elevated privileges (admin access). This provides an additional layer of security after initial authentication. **Note:** *The password for user mode to enter privileged mode must be set using CLI.*	Console, Telnet, SSH
RADIUS	Utilizes a RADIUS server for authentication. RADIUS (Remote Authentication Dial-In User Service) is used for centralized Authentication, Authorization, and Accounting management.	Console, Telnet, SSH, Web UI
TACACS+	Utilizes a TACACS+ server for authentication. TACACS+ (Terminal Access Controller Access-Control System Plus) offers more granular control over authorization and is used for centralized AAA management.	Console, Telnet, SSH, Web UI

AAA Methods

Identity Authentication Management

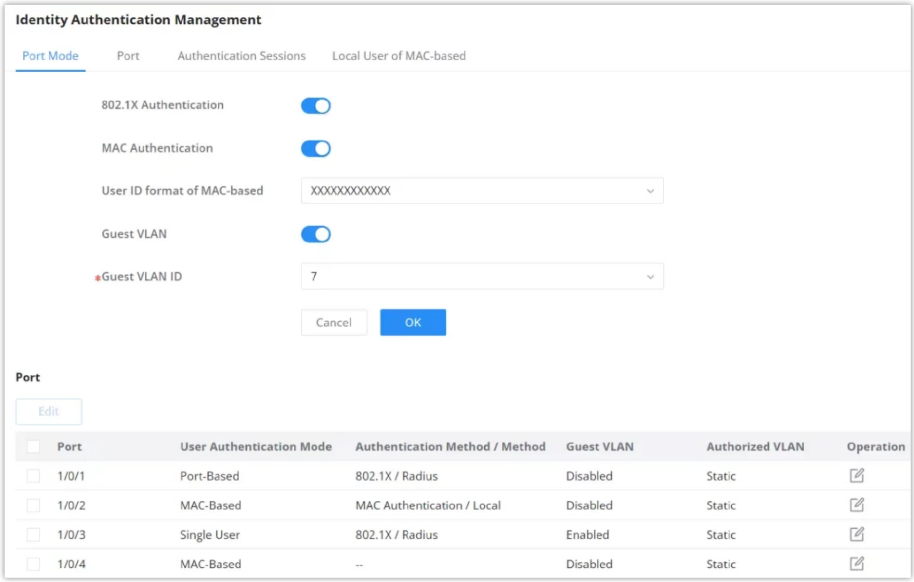
The Identity Authentication Management feature on Grandstream GWN switches provides a robust method for securing network access through 802.1X and MAC-based authentication. It allows administrators to configure and manage user authentication settings, ensuring only authorized devices can connect to the network, thereby enhancing overall network security and control.

The 802.1X protocol is a port-based network access 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 by logical interfaces to improve security.

Port Mode

To enable 802.1x and MAC authentication, please navigate to **Security → Identity Authentication Management**, then Toggle on "**802.1X Authentication**" and "**MAC Authentication**", click on "**OK**" button to save.

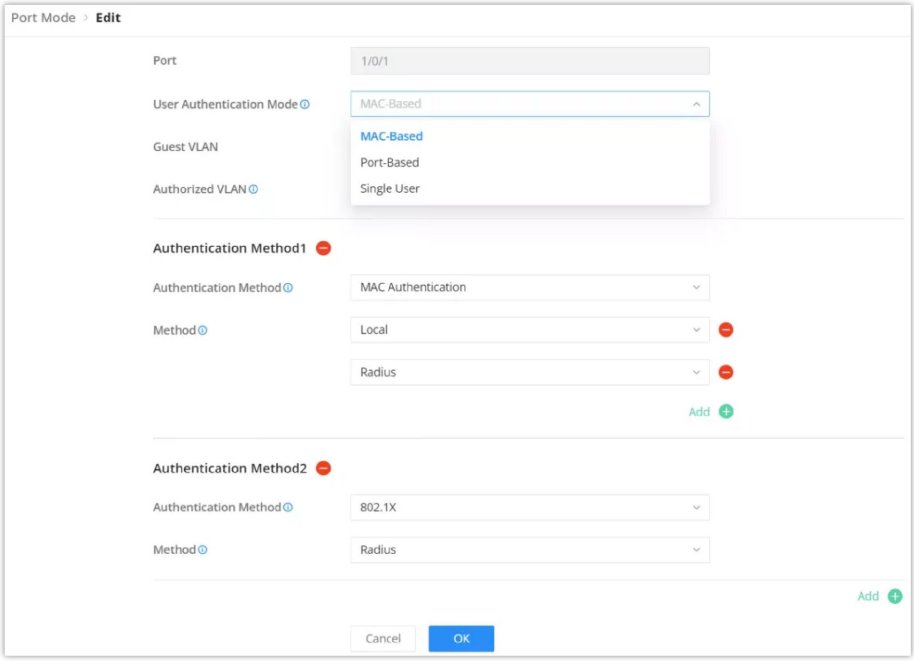
On this page also, you can specify a **user ID format for MAC-based** and enable a **Guest VLAN**. This ensures these devices remain isolated from the main network while still maintaining limited network connectivity through the Guest VLAN. The Guest VLAN ID directs unauthenticated users to a designated network segment, providing controlled and secure access.



Identity Authentication Management – Port Mode

To enable it on a port, select port(s) from the list then click on "**Edit**" button or click on "**Edit icon**" on the right side under operation column.

Note: *a RADIUS server must first be added under Security → RADIUS.*



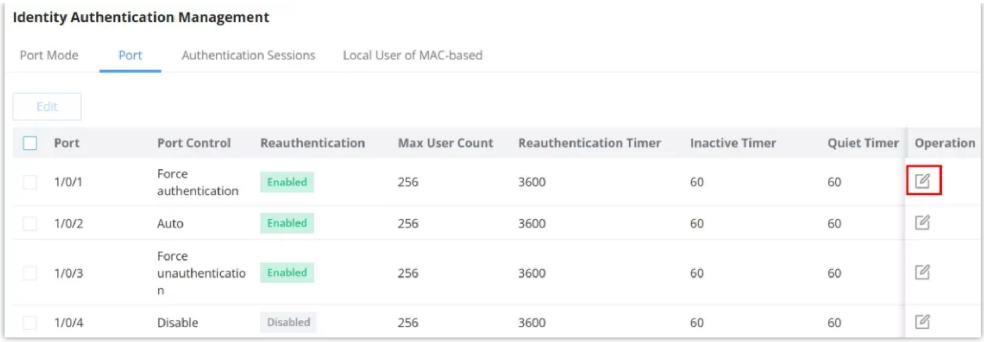
Port Mode – Edit port

Port	The specific port being configured. This field shows the port number (e.g.
User Authentication Mode	The mode of user authentication to be used on this port. Options include: MAC-Based
Guest VLAN	Enables or disables the Guest VLAN for this port. If enabled
Authorized VLAN	Specifies the VLAN ID that authenticated users will be assigned to. This ensures that authorized devices are placed in the correct network segment.
Authentication Methods(x) ***Note:*** *click on "Add+" to add another method.*	
Authentication Method1	Select the authentication method, two options: ● **802.1X**: it will use 802.1x authentication, RADIUS must be first added. ● **MAC Authentication**: it will use local MAC Addresses under Security → Identity Authentication Management page → Local User of MAC-based or RADIUS depending on the seleted method.
Method	• If **MAC Authentication** is selected, the user can add two methods: Radius and Local. • If **802.1x** is selected, the user can only select radius.

Port Mode – Edit port

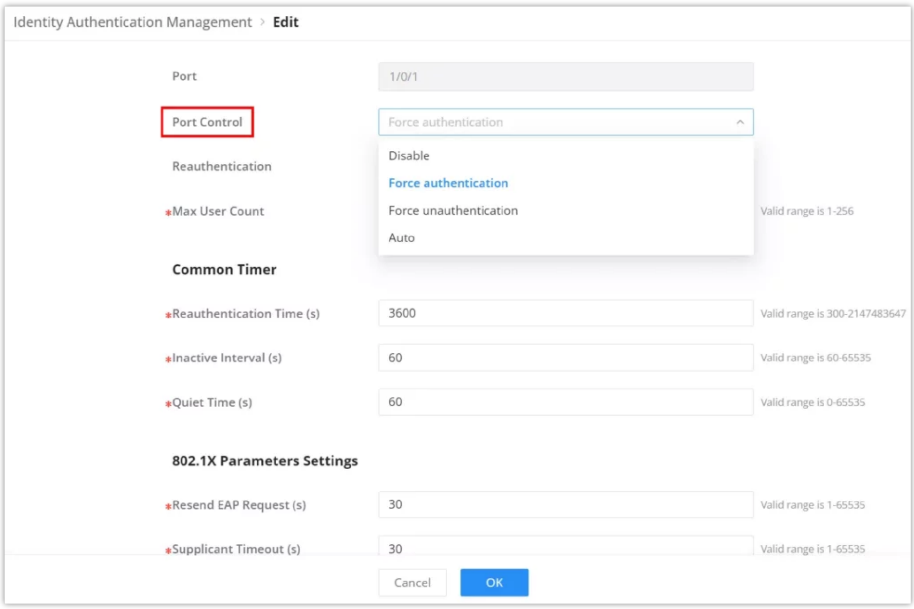
Port

On this tab, the users can enable on which ports the authentication will take effect, select the port(s) and then click on "**Edit**" button or icon to configure the port(s) as shown below:



Identity Authentication Management – port page

To enable the authentication on the port(s), under Port Control (Disable, Force authentication, Force unauthentication, Auto) select Auto or Force authentication and then save the configuration.



Identity Authentication Management – port – edit port

Note:

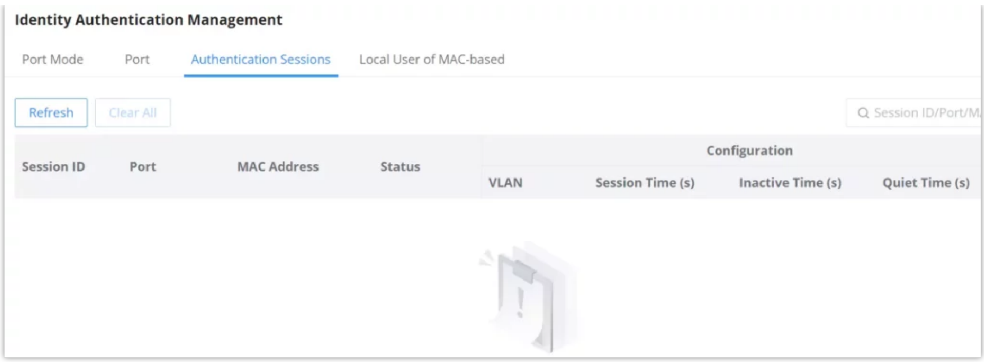
The 802.1X must be also configured on the device connected to the GWN780x(P) switch port.

Example of 802.1X configuration on GXV3480 IP Video phone.

802.1X Mode on GXV3480

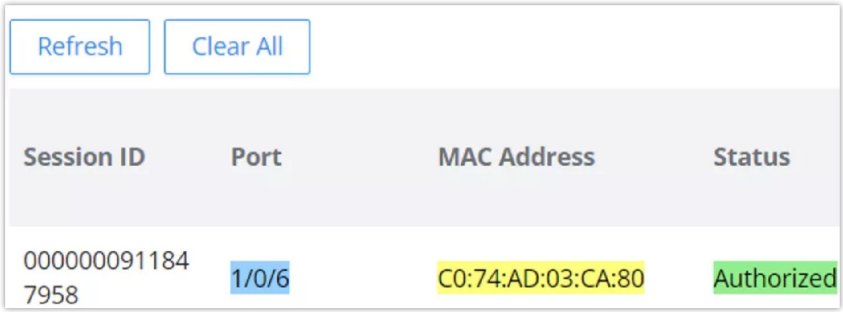
Authentication Sessions

On this tab, the authenticated devices will be listed here with more details. Please refer to the figures below:



Authentication Sessions

There are three status (Authorized, Locked, Guest):



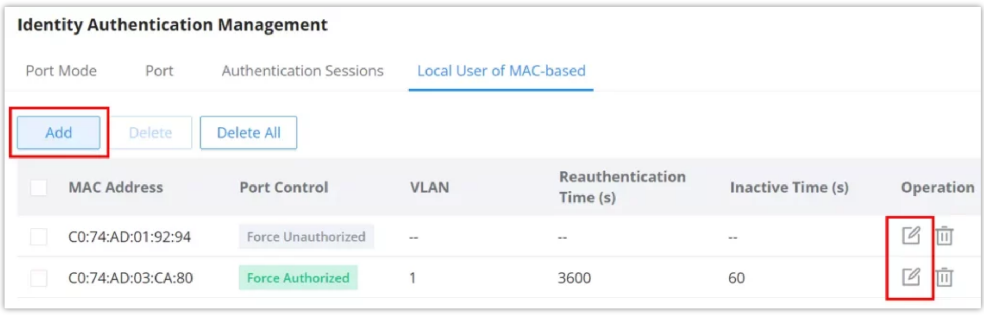
Authentication Sessions – Status Authorized

Authentication Sessions – Status Locked

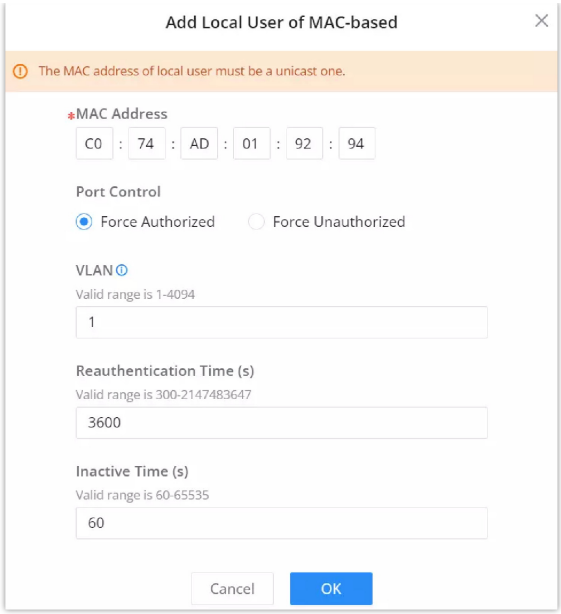
Authentication Sessions – Status Guest

Local User of MAC-based

The "**Local User of MAC-based**" feature in Grandstream GWN switches provides a way to add and manage users based on their MAC addresses. This feature ensures that only devices with specified MAC addresses are granted network access, enhancing security and control over network resources.



Local User of MAC-based



Add local User of MAC-based

MAC Address	The MAC address of the local user must be a unicast one.
Port Control	• **Force Authorized:** Forces the port to authorize the device with the specified MAC address, allowing it access to the network. • **Force Unauthorized:** Forces the port to not authorize the device, preventing it from accessing the network.
VLAN	Valid range is 1-4094.
Reauthentication Time (s)	Valid range is 300-2147483647.
Inactive Time (s)	Valid range is 60-65535.

Add *local User of MAC-based*

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.

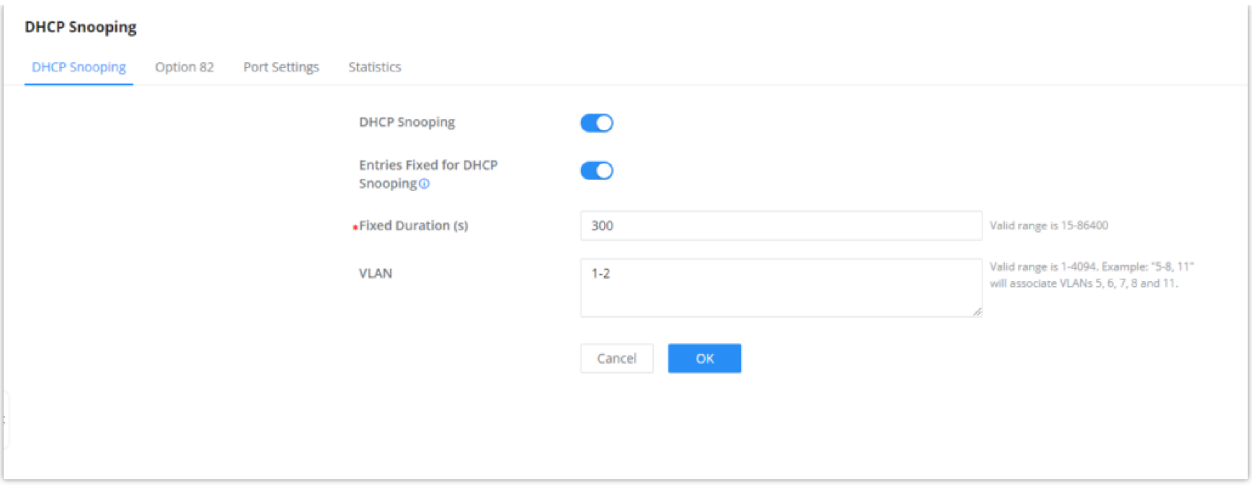
In order to ensure the security of network communication services, the DHCP Snooping technology is introduced, and a firewall is established between the DHCP Client and the DHCP Server to defend against various attacks against DHCP in the network.

When the device reboots, the dynamic binding table for IP source guard is automatically restored.

Note: Associated with the "Entries Fixed for DHCPv6 Snooping" option of DHCPv6 Snooping.

Users can configure fixed entries for DHCP Snooping, ensuring that when the device reboots, the dynamic binding table for IP source guard is automatically restored after a fixed duration defined in seconds. Note that this is linked to the 'Entries Fixed for DHCPv6 Snooping' option in DHCPv6 Snooping.

To enable DHCP Snooping feature on GWN78xx switches, navigate to **Security → DHCP Snooping**, then enable DHCP Snooping, to make the DHCP snooping enabled on a VLAN, specify the VLANs or a VLAN range for example 5-8 that means VLANs from 5 to 8, click "**OK**" button to save. Please refer to the figure below:



DHCP Snooping – General page

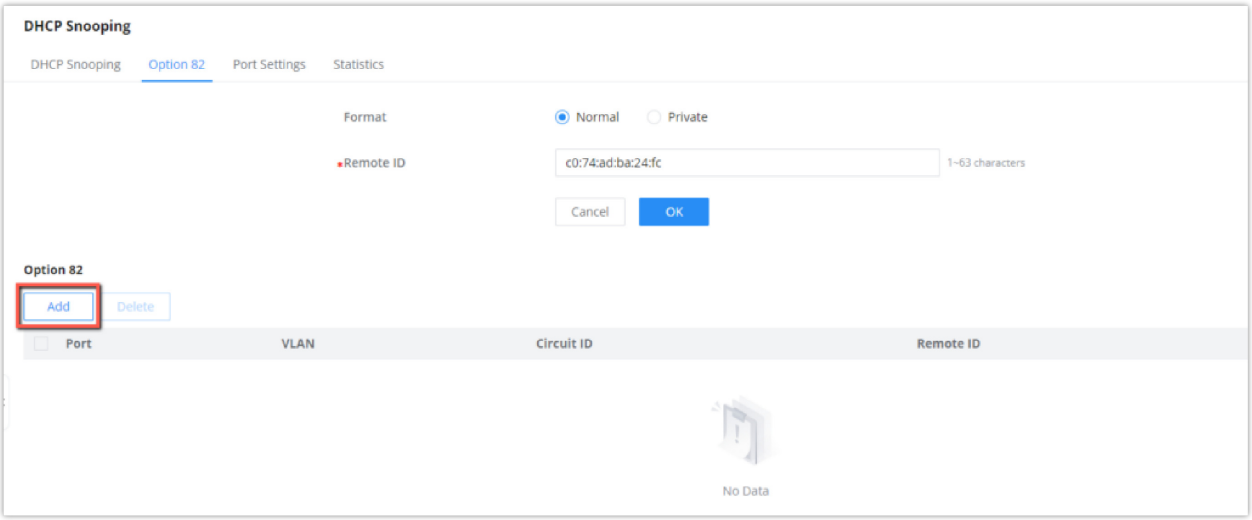
DHCP Snooping Option 82

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 specify the **Remote ID**, the format can be either **Normal** (standard) or a **Private**:

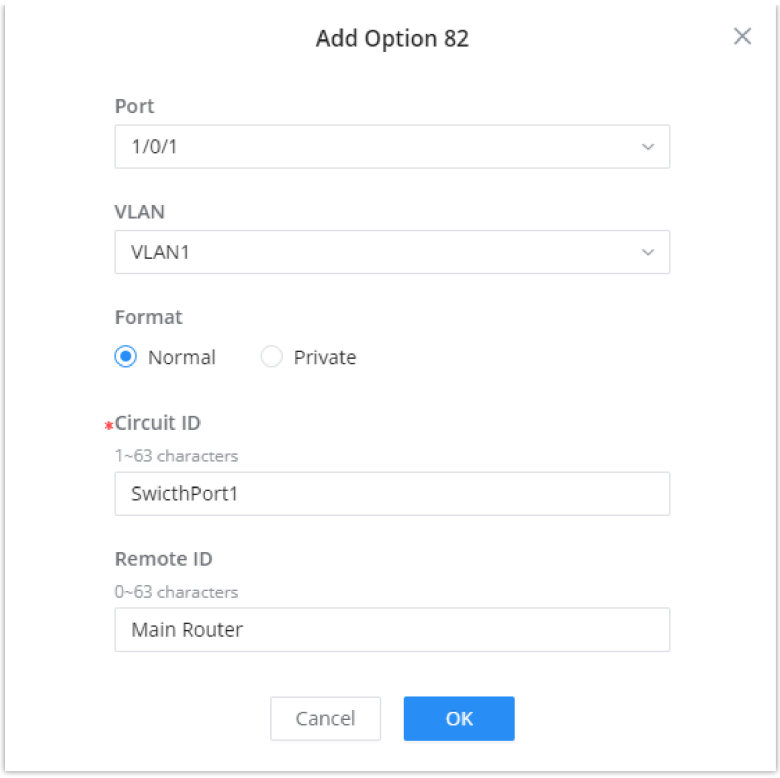
- **Normal Format:** is generally used when interoperability between different vendors' equipment is required, for GWN78xx switches by default the MAC Address of the switch will be used, but any other characters in the range of 1-63 can be used.
- **Private Format:** is specific to the vendor's ecosystem and may not be compatible with other vendors' equipment (check the vendor specific format).

Option 82 is used to identify both the Circuit ID and Remote ID of the specific port, this can be used to identify the VLAN, interface and other information where the client is located. To define these information, go to **DHCP Snooping => Option 82**, Choose a specifc port:



DHCP Snooping – Option 82

Then, select a port, VLAN and Format, and specify the Circuit ID and Remote ID of the specfic port:



DHCP Snooping – Option 82 – Add Circuit

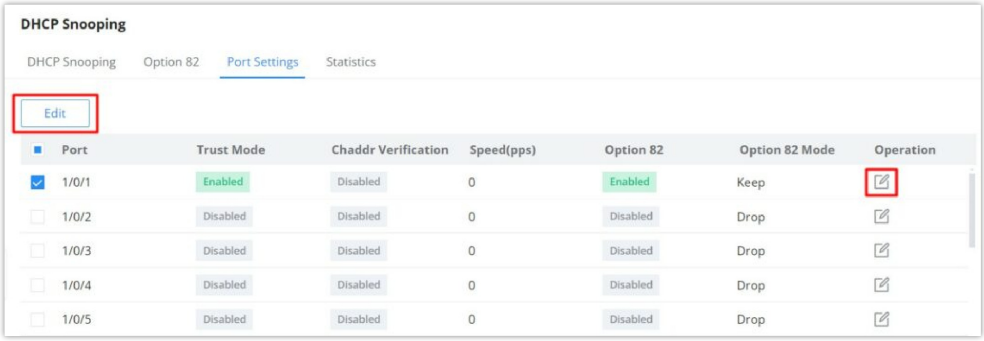
Note

Please note that the Remote ID per port is different from the global remote ID of the switch.

DHCP Snooping Port Settings

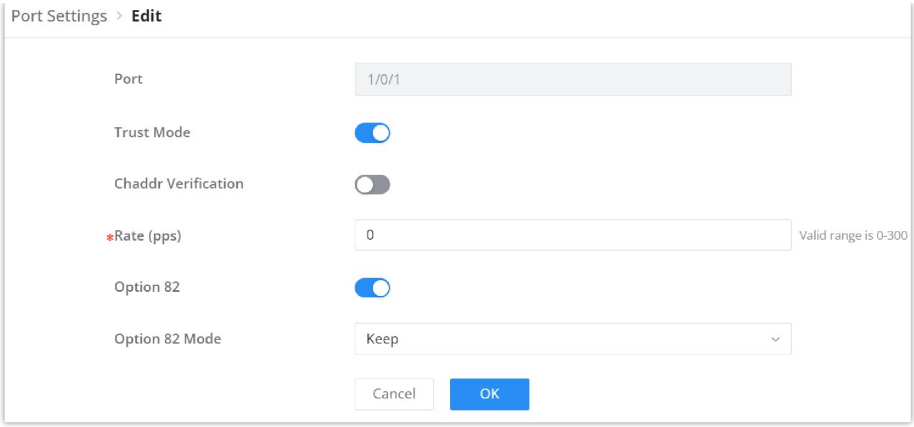
On this page, the use can configure the trusted port(s) that will allow DHCP messages, all other ports that are not trusted will discard the DHCP messages, this way GWN78xx will protect users from rogue DHCP servers that are plugged on untrusted ports.

To configure a port(s), either select the port(s) and click on "**Edit**" button or click on "**Edit icon**" under operation column as seen below:



DHCP Snooping – Port Settings

To make a port trusted, Toggle ON **Trust Mode**, more security parameters can be enabled too like **Chaddr Verification**, **Rate** (**pps** = packet per seconds) to limit the number of DHCP packets, and enable Option 82 for this port with three modes (keep, drop, replace). Please refer to the figure below:

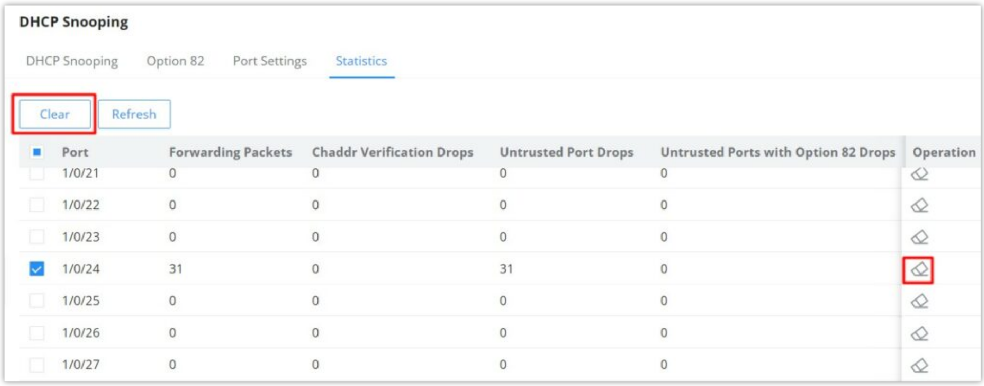


DHCP Snooping – Port Settings – Edit

DHCP Snooping Statistics

This page displays all statistics recorded by DHCP snooping function including Forwarding packets, Untrusted Port Drops, etc.

To clear the statistics, select the ports and click on "**Clear**" button as shown below:



DHCP Snooping – Statistics

DHCPv6 Snooping

DHCPv6 snooping is a security feature in IPv6 networks that safeguards against unauthorized DHCPv6 server messages and controls IPv6 address assignments, similar to how DHCPv4 snooping operates in IPv4 networks.

To enable DHCPv6 Snooping feature on GWN78xx switches, navigate to **Security → DHCPv6 Snooping**, then enable DHCPv6 Snooping, to make the DHCPv6 snooping enabled on a VLAN, specify the VLANs or a VLAN range for example 5-8 that means VLANs from 5 to 8, click "**OK**" button to save. Please refer to the figure below:

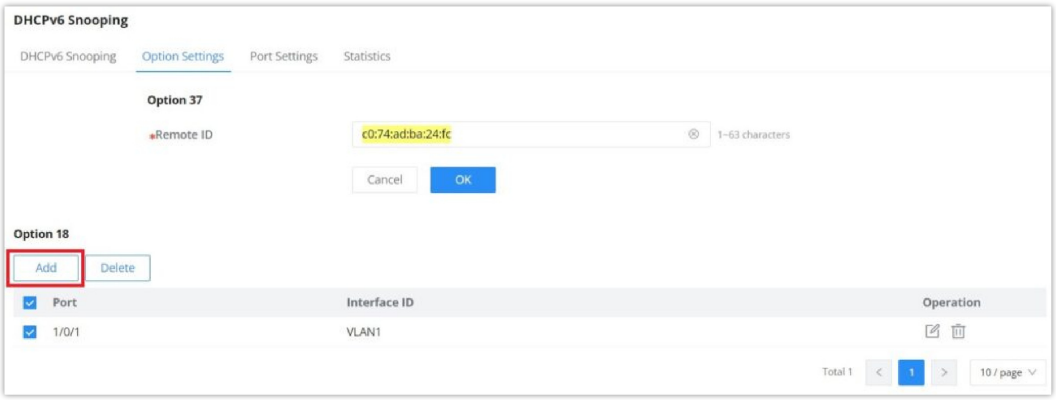
DHCPv6 Snooping

DHCPv6 Snooping Option 18

On this page, the user can configure the Remote ID (Option 37), by default GWN78xx switches uses the GWN78xx switches MAC Address.

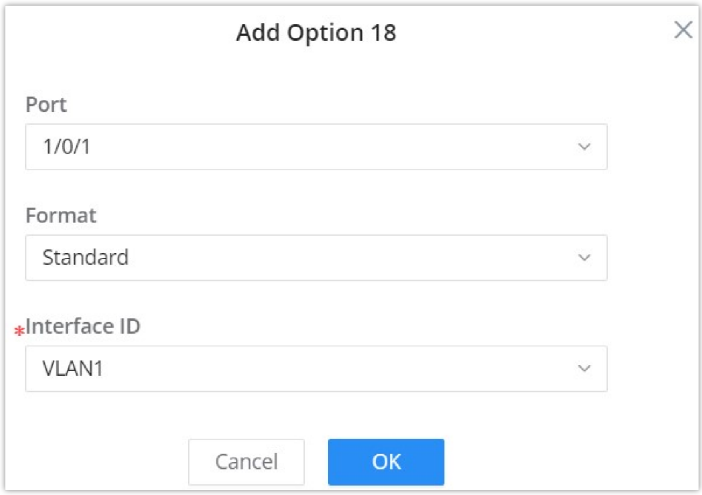
The DHCPv6 Relay-Option, encompassing Option 18 and Option 37, enables a DHCPv6 relay agent to embed circuit-specific and remote information as a TLV (type-length-value) within the relay message sent to the DHCPv6 server. In this scenario, the managed device functions as a DHCPv6 relay agent.

To add an option 18 for a port, click on "**Add**" button as shown below:



DHCPv6 Snooping – Option Settings

Then, select the port, Format (Standard, Extended), when the Standard format is selected then the user can select the VLAN and if the Extended Format is selected the user can interface ID (3~63 characters), click on "**OK**" to save.

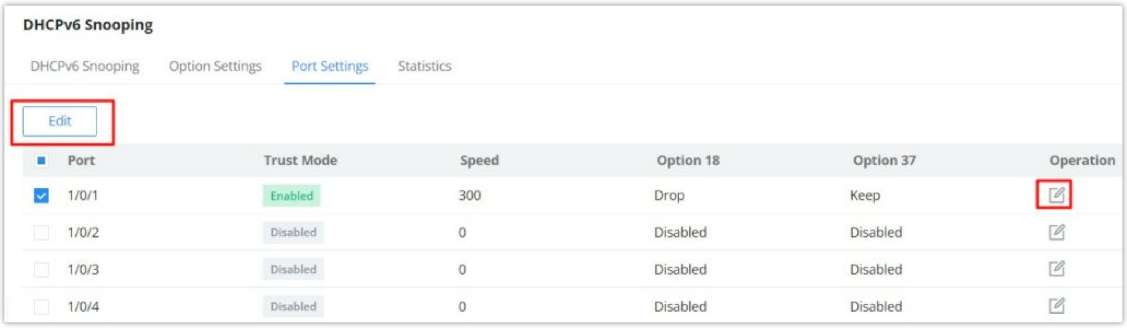


DHCPv6 Snooping – Add option 18

DHCPv6 Snooping Port Settings

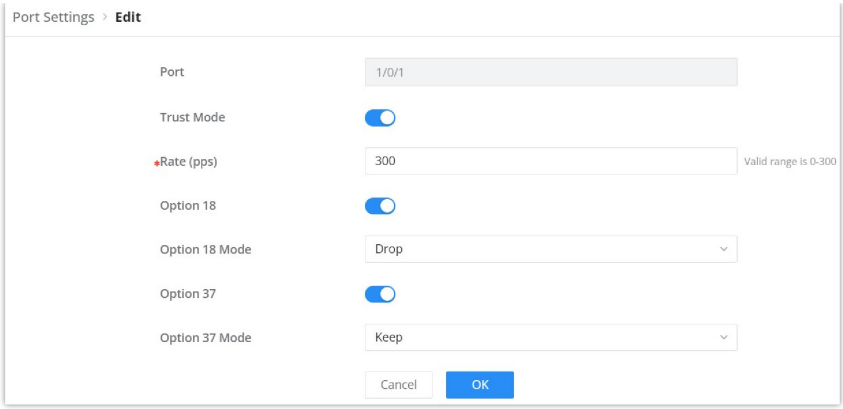
On this page, the use can configure the trusted port(s) that will allow DHCP messages, all other ports that are not trusted will discard the DHCP messages, this way GWN78xx will protect users from rogue DHCP servers that are plugged on untrusted ports.

To configure a port(s), either select the port(s) and click on "**Edit**" button or click on "**Edit icon**" under operation column as seen below:



DHCPv6 Snooping – Port Settings

To make a port trusted, Toggle ON **Trust Mode**, more security parameters can be enabled too like **Rate** (**pps** = packet per seconds) to limit the number of DHCPv6 packets, and enable Option 18 and 37 for this port with three modes (keep, drop, replace). Please refer to the figure below:

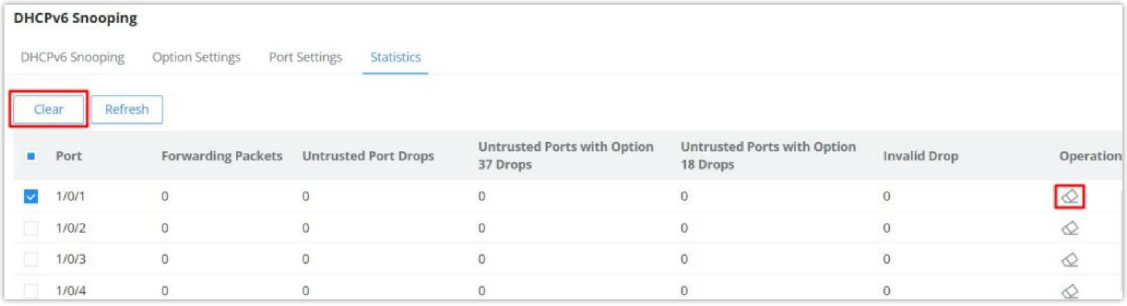


DHCPv6 Snooping – Port Settings – Edit

DHCPv6 Snooping Statistics

This page displays all statistics recorded by DHCPv6 snooping function including Forwarding packets, Untrusted Port Drops, etc.

To clear the statistics, select the ports and click on "**Clear**" button as shown below:



DHCPv6 Snooping – Statistics

MAINTENANCE

Upgrade

GWN78xx Switches support manual upload firmware upgrade via a BIN file that can downloaded from Grandstream Firmware page: https://www.grandstream.com/support/firmware.

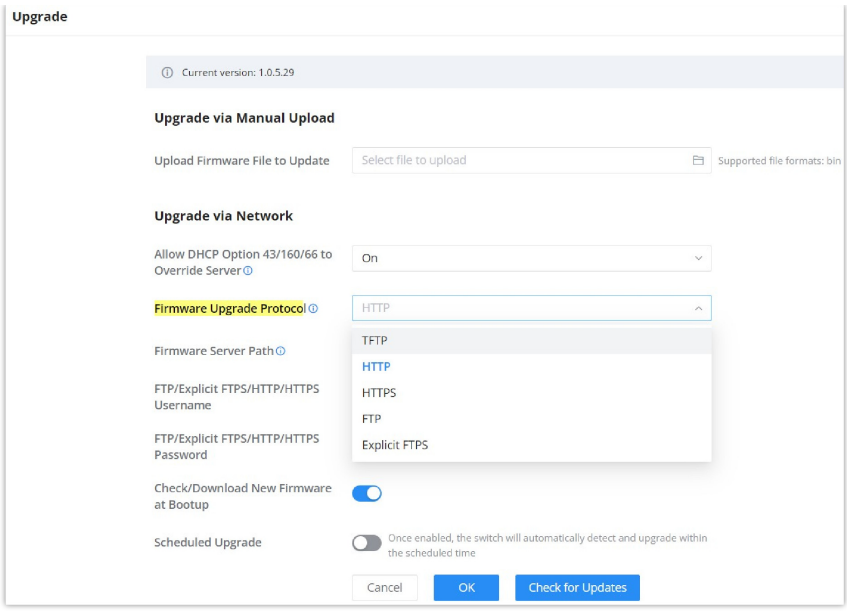
Upgrading via network is also possible using 5 these protocols:

- TFTP
- HTTP
- HTTPS
- FTP
- Explicit FTPS

Once the protocol is selected, then the user needs to specify the firmware Server Path (For example: firmware.grandstream.com).

Note:

- Username and Password must be specified if the Server requires it.
- For FTP protocol use the header "**ftp://**" and for FTPS use "**ftps://**"
- Considering the memory problem of the device, the upload upgrade supports streaming upgrade, and the upgrade is carried out while uploading.



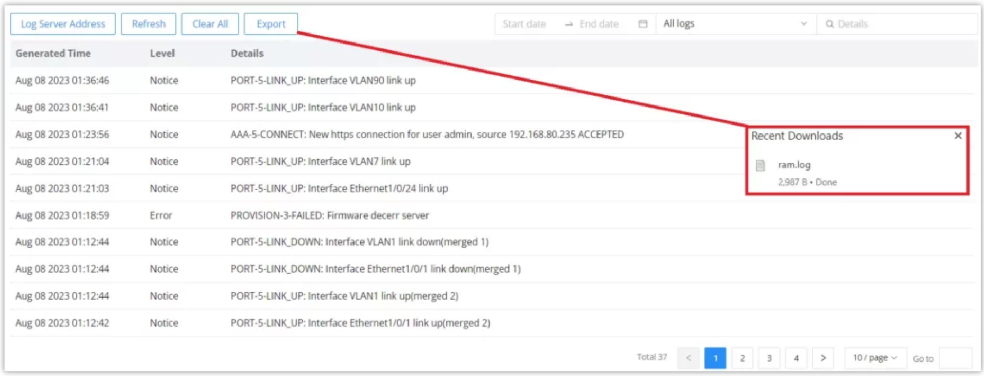
Upgrade

Diagnostics

GWN78xx Switches support many diagnostics tools that can help the user troubleshoot the issue and resolve it. These tools include Logs, Ping, Traceroute, Mirroring, Fiber Module, Copper Test and One-Click Debugging.

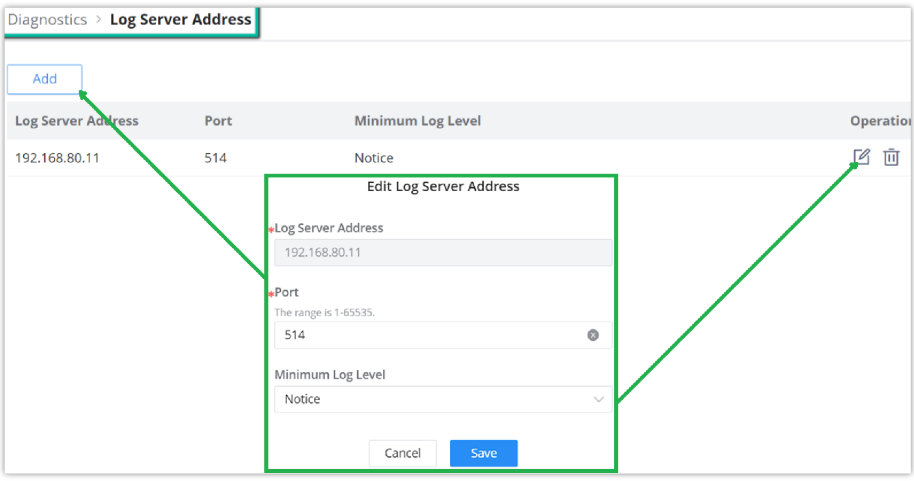
Logs

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



Diagnostics – Logs

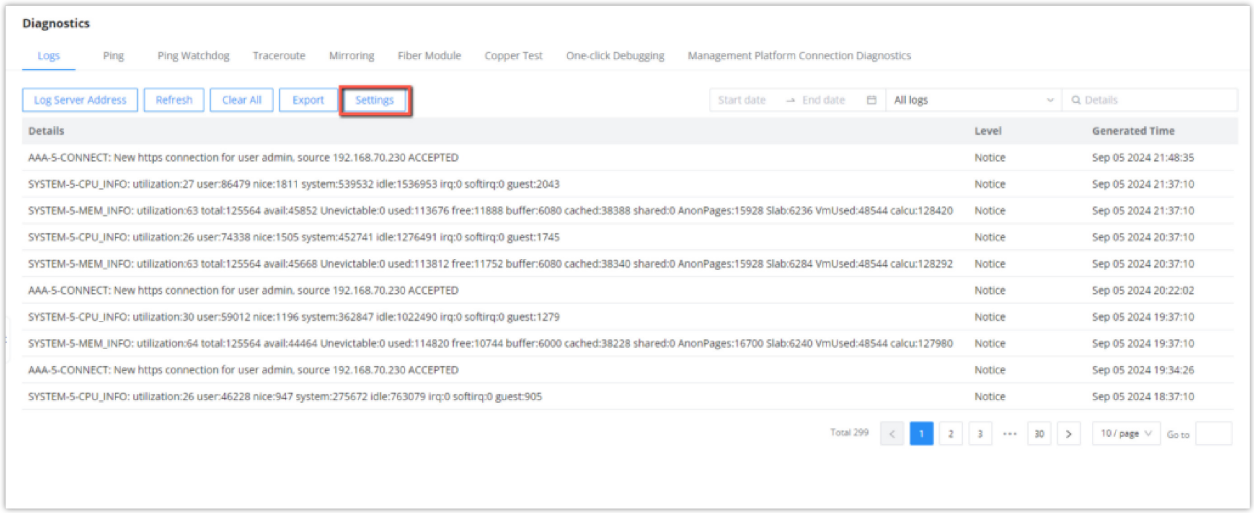
Adding a Log Server Address to the logs to be sent to is also supported on the GWN78xx Switches.



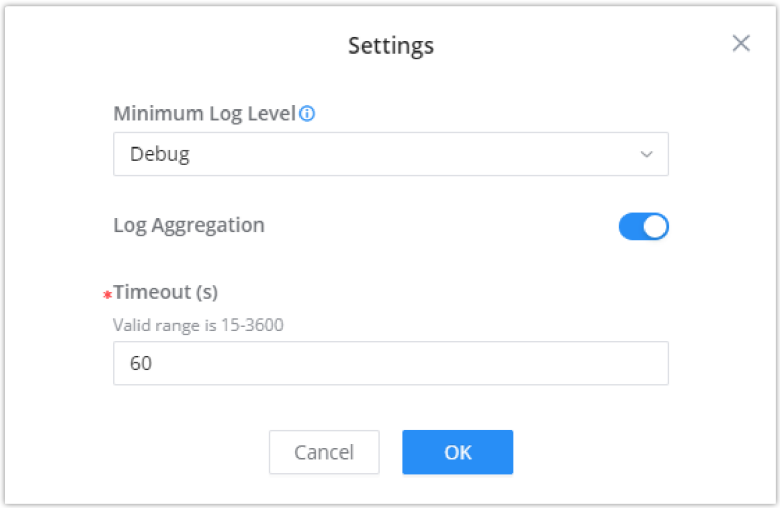
Log Server Address

Users can Configure the following elements in the logs settings:

- **Minimum log level:** This defines the lowest severity of events that will be logged. “Debug” means all messages, including detailed diagnostic information, will be recorded. Other log levels (e.g., Info, Warning, Error) would filter out lower-priority messages.
- **Log Aggregation:** This option allows you to merge multiple logs from various sources or components into a centralized location for easier monitoring, analysis, and management.
- **Timeout:** This setting defines the time, in seconds, before the logging operation times out. In the example shown, the timeout is set to 60 seconds. The valid range for the timeout is between 15 and 3600 seconds.



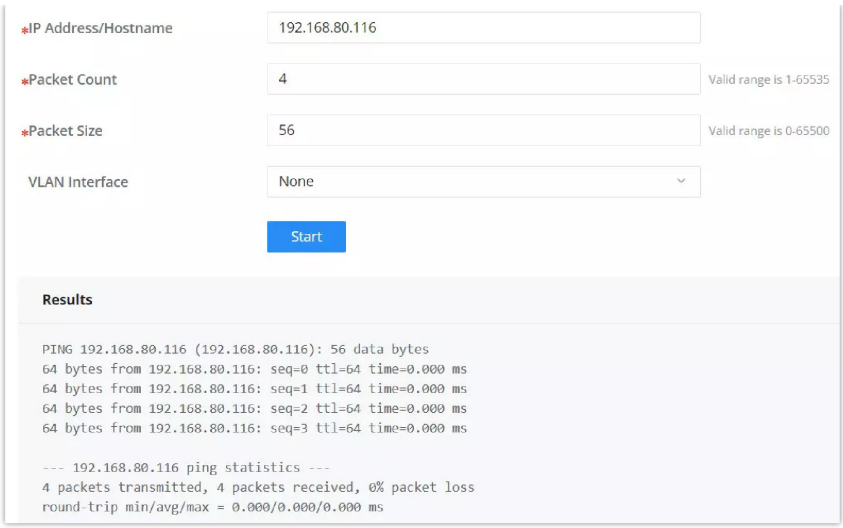
Log Diagnostics



Log Diagnostics

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

Ping Watchdog

Ping Watchdog is a feature designed to monitor the connectivity of a device by continuously pinging a specified IP address. If the device becomes unresponsive to pings, then corrective actions can be triggered based on the configuration settings.

Port: Specifies the port on the device that will be monitored or managed by Ping Watchdog.

Enable: Toggles the Ping Watchdog feature on or off for the selected port.

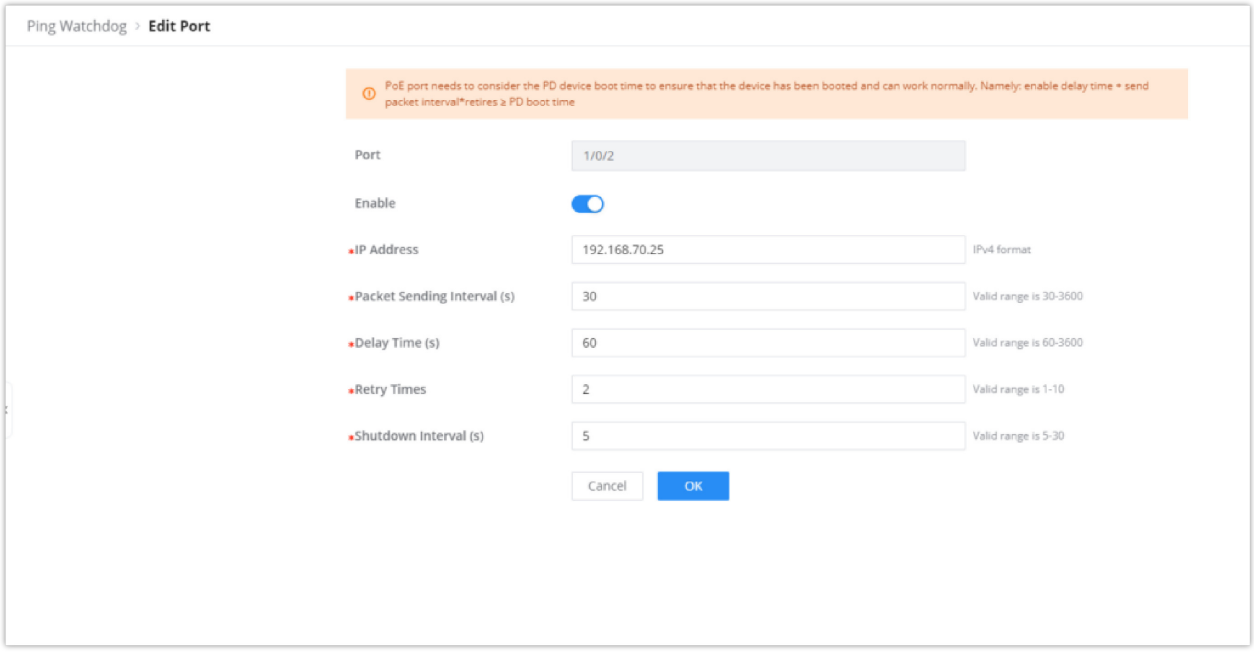
IP Address: The target IP address to which the device will send ping requests.

Packet Sending Interval (s): Defines how frequently (in seconds) ping packets are sent to the specified IP address.

Delay Time (s): This sets a delay before the Ping Watchdog starts monitoring the device after it's enabled or after a reboot.

Retry Times: Specifies how many failed ping attempts are allowed before the watchdog takes action.

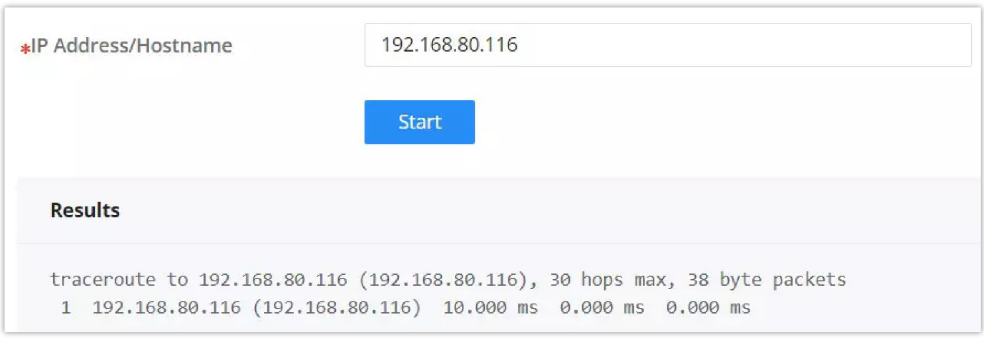
Shutdown Interval (s): The time period (in seconds) for which the monitored PoE port will remain shut down after failing the ping test and triggering the shutdown action.



Ping watchdog

Traceroute

Another tool is Traceroute that shows the number of hops, and GWN78xx Switches enables the user to run Traceroute commands right from the Switches WEB UI.



Traceroute

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.

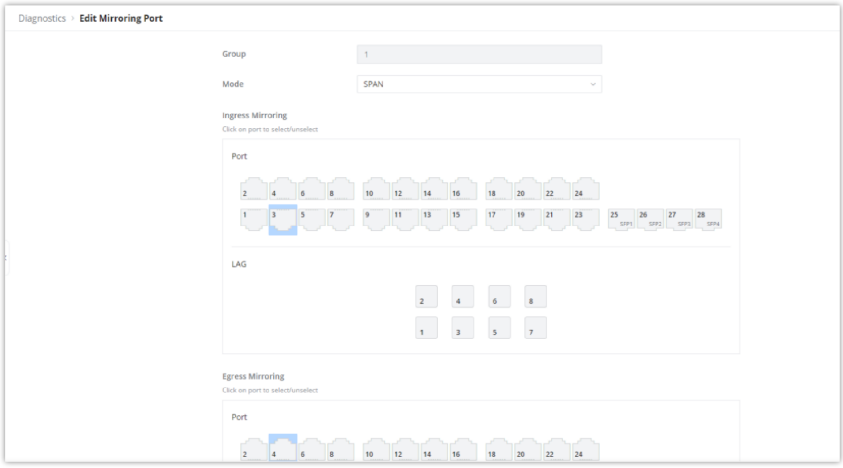
The GWN78xx switches supports two modes of Port Mirroring: SPAN and RSPAN:

- **SPAN (Local)**: Traffic is mirrored locally within the same switch.
- **RSPAN (Remote)**: Traffic is mirrored remotely across a network using a Remote VLAN.

SPAN

The traffic mirroring occurs locally within the same switch. SPAN allows you to capture traffic from one or more ports and send a copy of it to another port, typically connected to a network analyzer or monitoring tool.

- **Ingress Mirroring**: Captures incoming traffic on the source port(s).
- **Egress Mirroring**: Captures outgoing traffic from the source port(s).
- **Source Port**: Where the traffic originates (the port being monitored).
- **Tx/Rx Regular Data Messages:** defines what type of traffic (transmit, receive, or both) is monitored on the destination switch.



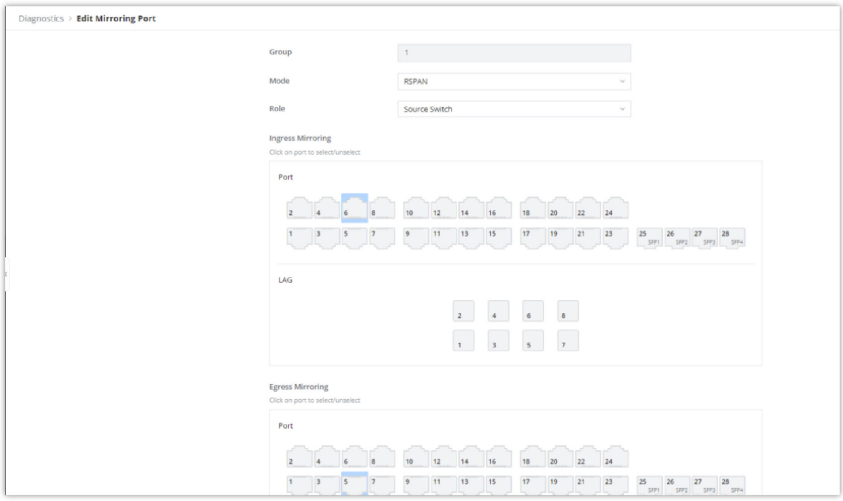
Port Mirroring

RSPAN

RSPAN (Remote Switched Port Analyzer) allows traffic to be mirrored from one switch to another over a network. Unlike SPAN, which is limited to mirroring traffic locally within the same switch, RSPAN uses a **Remote VLAN** to transport mirrored traffic across multiple switches, enabling centralized monitoring.

Source Switch Role (RSPAN)

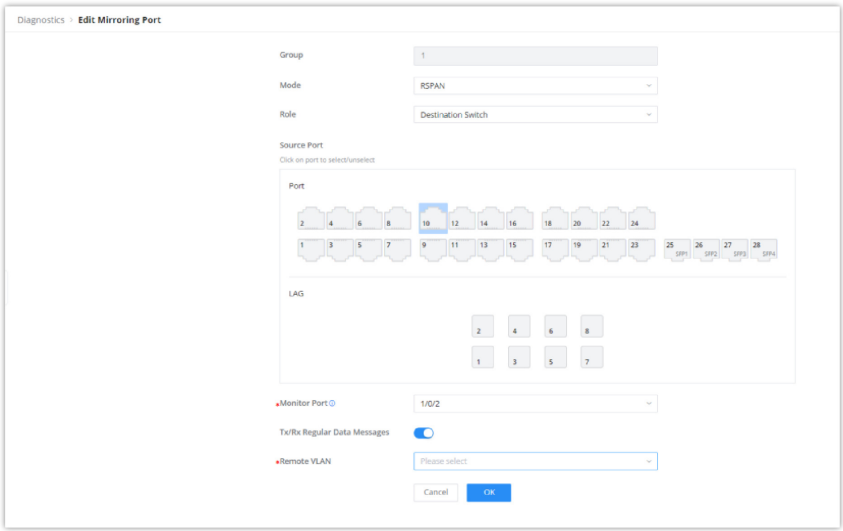
- **Ingress Mirroring**: This captures incoming traffic on the specified source port(s). It mirrors the packets received by the port before they are processed by the switch, forwarding them to the designated destination for monitoring or analysis.
- **Egress Mirroring**: This captures outgoing traffic from the specified source port(s). It mirrors the packets leaving the port after the switch processes them, forwarding these packets to the monitoring destination.
- **Output Port**: This is the port on the source switch where the mirrored traffic is sent. In SPAN, it's usually a local port that connects to the monitoring device, but in RSPAN, this traffic is forwarded across a network using the Remote VLAN to the destination switch.
- **Remote VLAN**: This is the VLAN used to transport mirrored traffic between the source switch and the destination switch in an RSPAN configuration. The source switch forwards mirrored traffic to this VLAN, which allows it to be sent across the network to the destination switch for analysis.



Source Switch Role

Destination Switch Role (RSPAN)

- **Source Port**: This is the remote VLAN where the mirrored traffic from the source switch arrives. The destination switch receives the mirrored packets via this VLAN and forwards them to the appropriate monitoring port.
- **Monitor Port TX/RX**: This defines what type of traffic (transmit, receive, or both) is monitored on the destination switch.
- **Remote VLAN**: The VLAN used to receive mirrored traffic from the source switch. It's the same VLAN that the source switch uses to forward the mirrored traffic over the network to the destination switch.

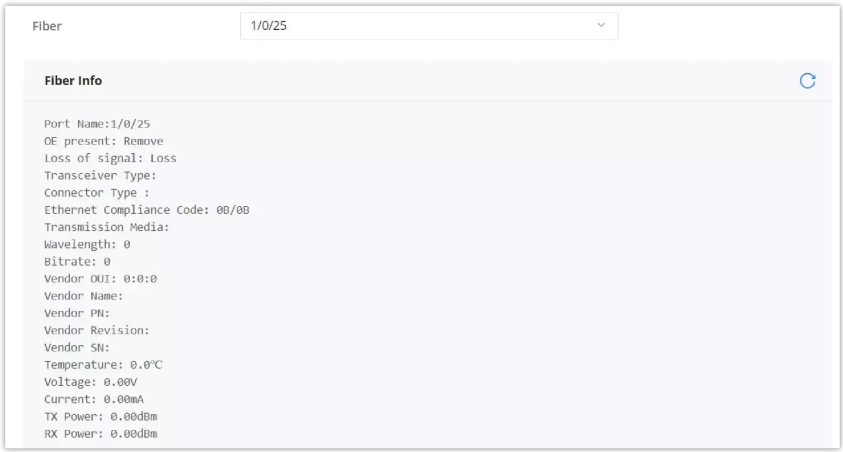


Destination Switch Role (RSPAN)

Fiber Module

This pages 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

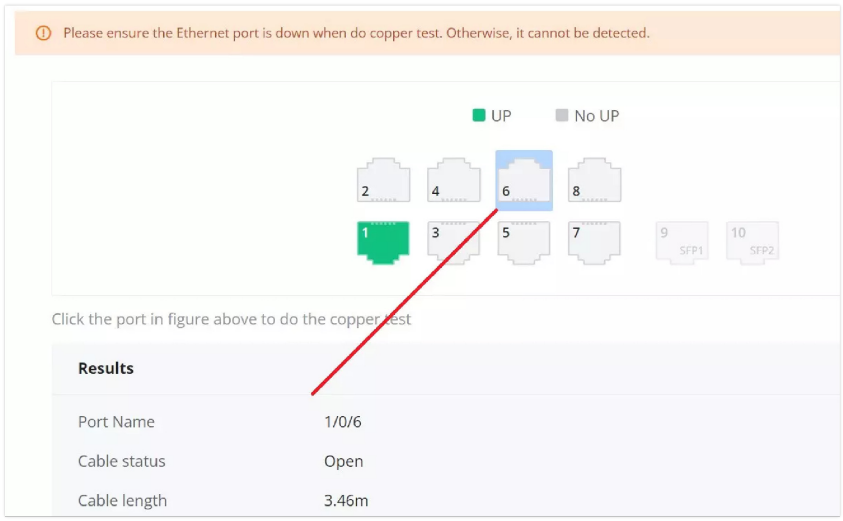
Copper Test

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:

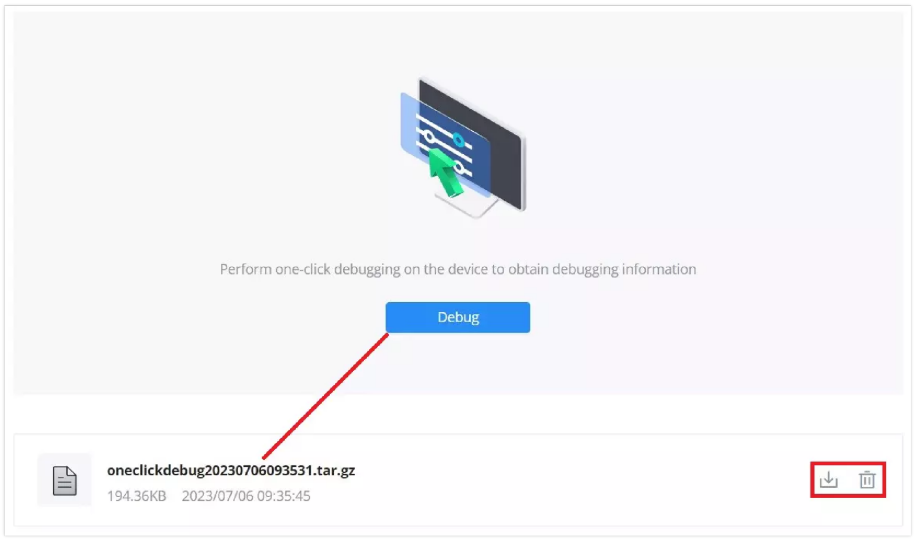
- When there is a fault: it is the length from the port to the fault location.

- When there is no fault: it is the actual length of the cable.

One-click Debugging

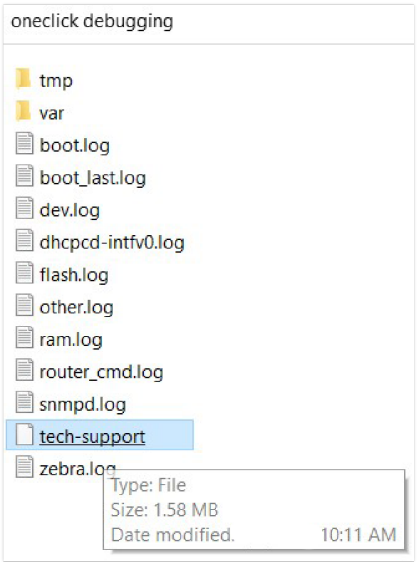
On GWN78xx switches, One-click debugging feature can help administrators or tech-support to quickly and easily get debugging information about the GWN switch in a matter of few minutes.

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.

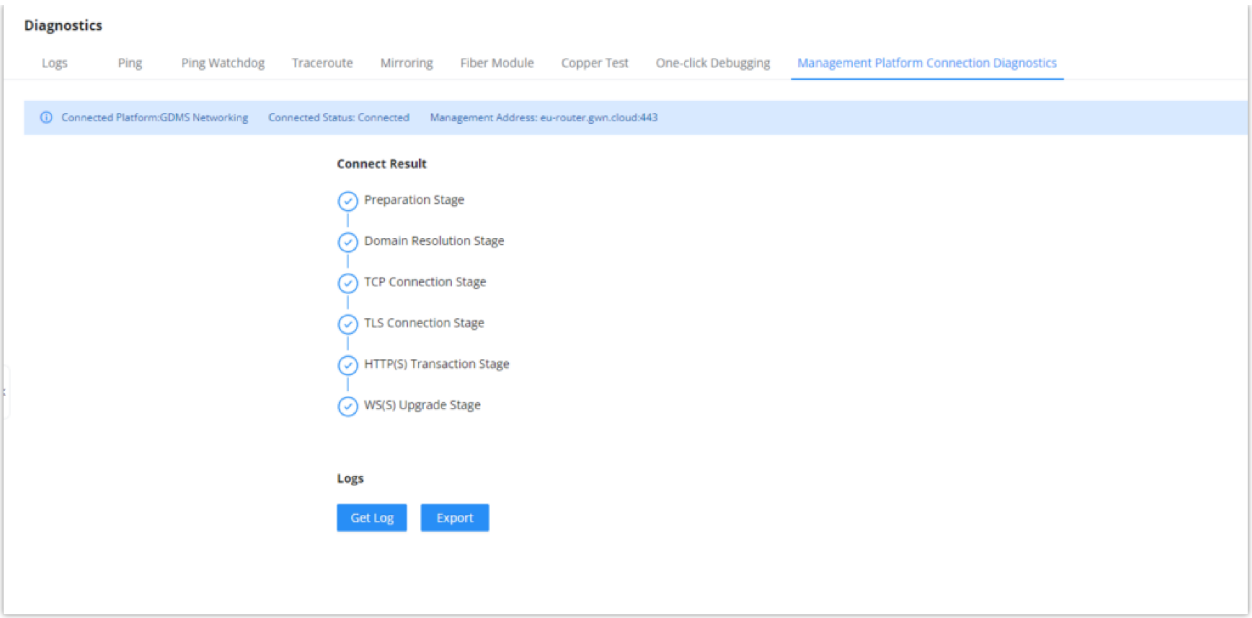


One-click Debugging Folder

Management Platform Connection Diagnostics

If the GWN78xx switch is added to the GDMS networking ,GWN Manager, or a GWN Router, it will display a Cloud icon with a green check mark (as shown in the figure below) indicating it's added to a GDMS Networking account, GWN Manage, or to a GWN Router.

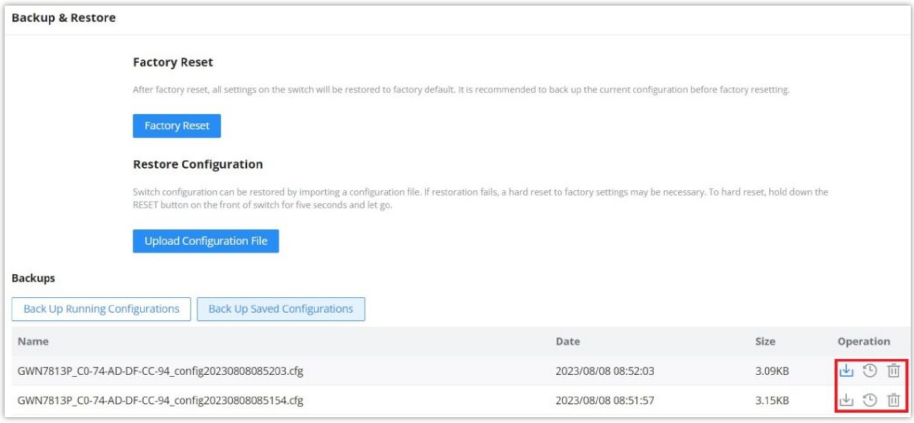
In case there is an issue with the connection, then the user can navigate to **Maintenance** → **System Diagnosis** → **Cloud/Manager Connection Diagnostics** and then click on "**Detection**" or "**Redetection**" button to see in what stage/step the connection has failed. Refer to the figure below:



Cloud/Manager Connection Diagnostics

Backup and Restore

Click on "Factory Reset" button to reset the GWN78xx 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

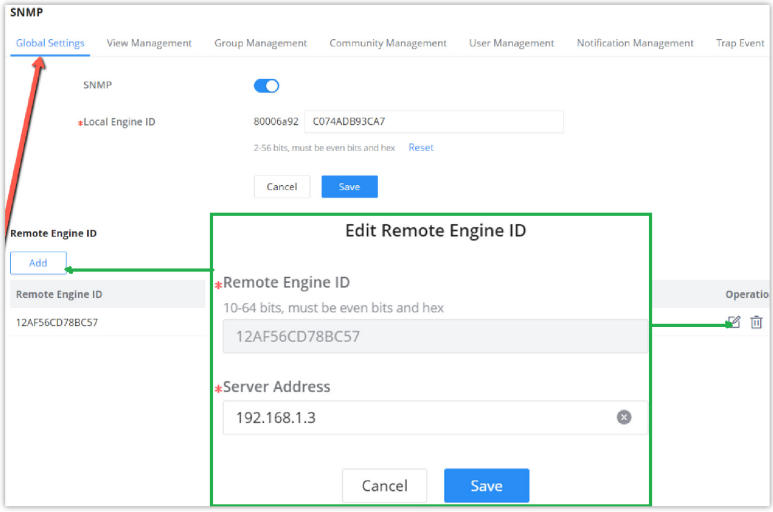
Network Management Protocol (SNMP) is an "Internet-standard protocol for managing devices on IP networks". Devices that typically support SNMP include routers, switches, servers, workstations, printers, modem racks and more. SNMP is used mostly in network management systems to monitor network-attached 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.



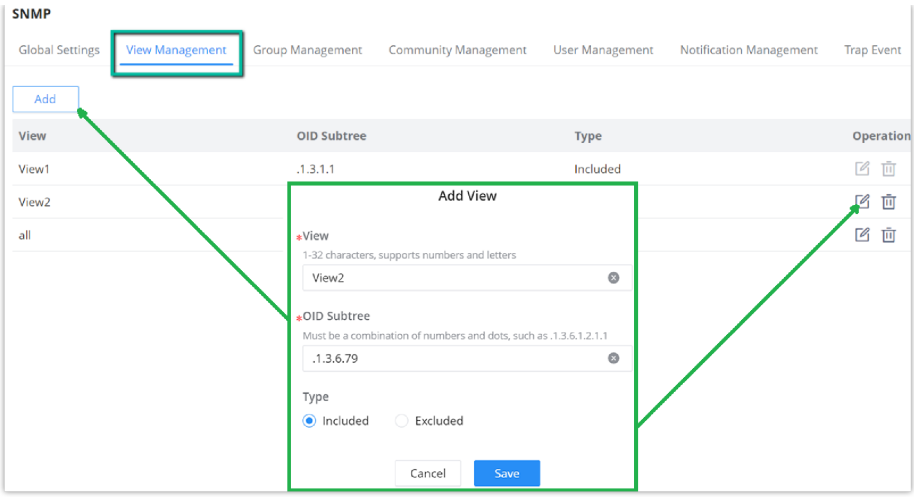
SNMP -Global Settings

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. ***Note:*** *The default is 8000 A59Dxxxxxxxx, 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 characters. The number of characters must be an even number .*
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

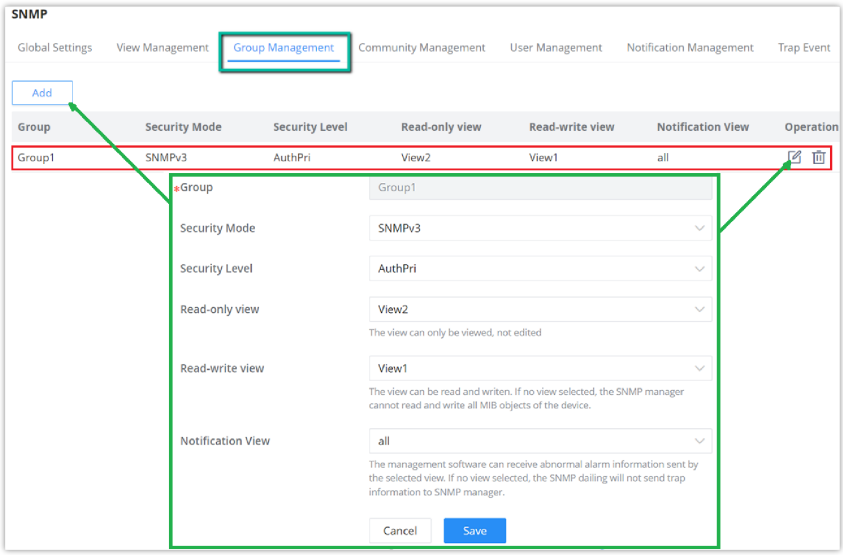
This page allows the network administrator to create MIB views (Management information base) and then include or exclude OID (Object Identifier) in a view.



SNMP – View Management

Group Management

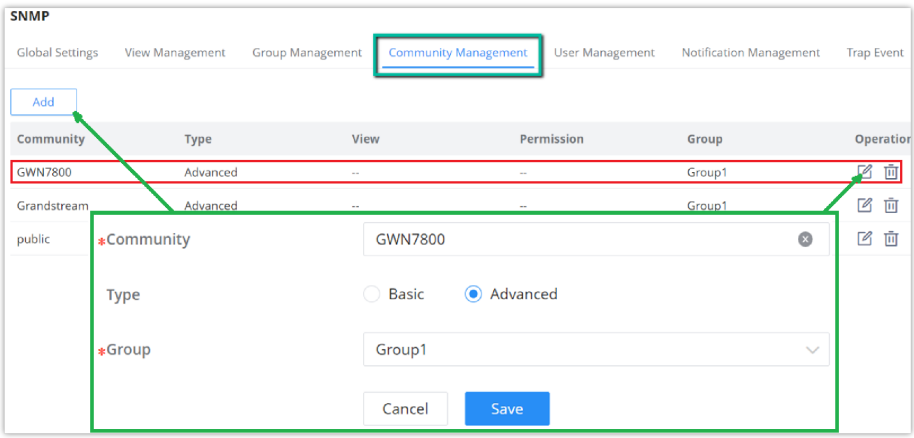
This page allows the network administrator to group SNMP users and assign different authorization and access privileges.



SNMP – Group Management

Community Management

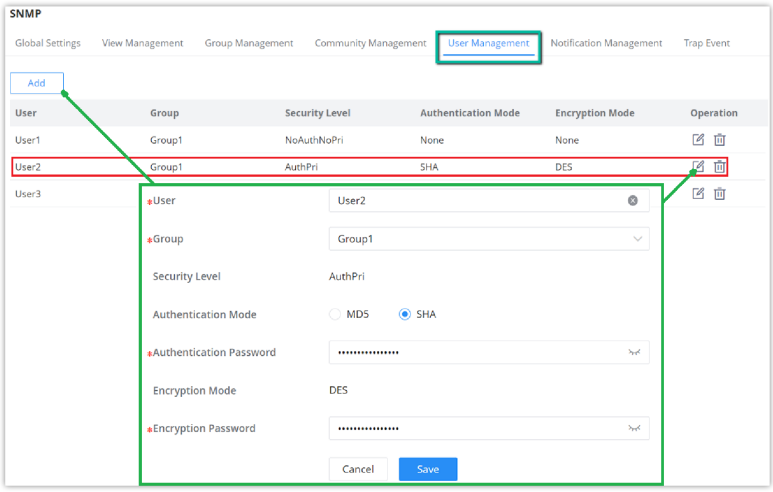
This page allows a user to add/remove multiple communities of SNMP.



SNMP – Community Management

SNMP User Management

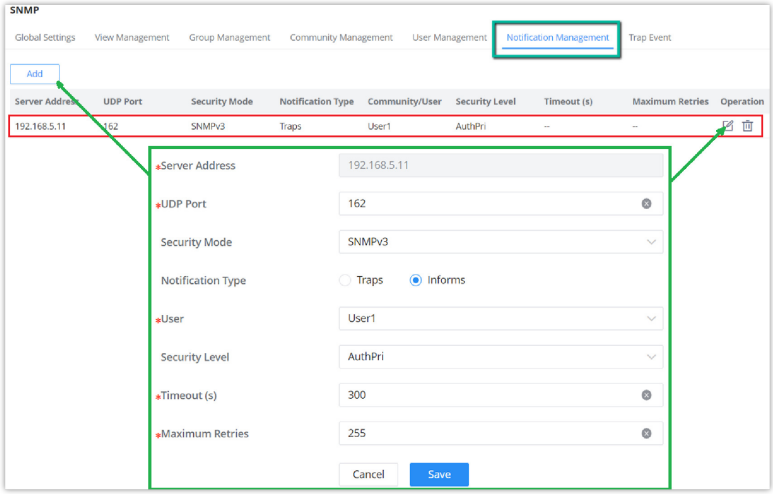
This page allows a user to configure SNMPv3 user profile.



SNMP – User Management

Notification Management

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

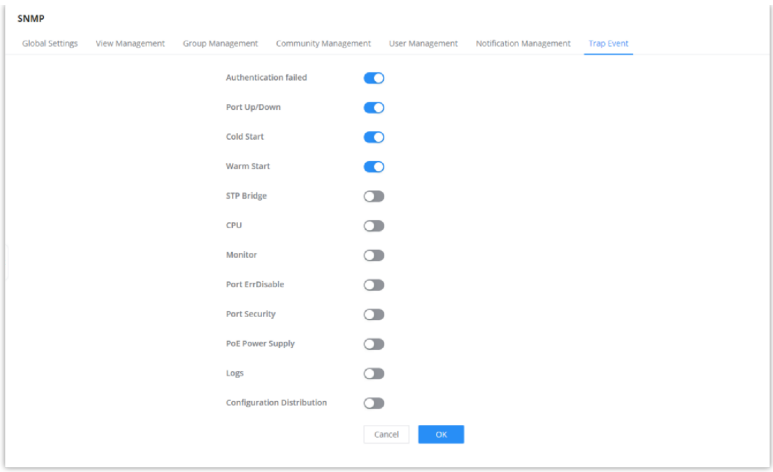


SNMP – Notification Management

Trap Event

a **Trap event** refers to an alert or notification that is automatically sent by a device or system when a specific event occurs. These events, shown in the SNMP configuration, are various types of conditions that the system is monitoring. When enabled, the device sends a trap to the SNMP manager, notifying it of occurrences like:

- **Authentication failed**: When there is an unauthorized login attempt.
- **Port Up/Down**: When a network port goes offline or comes online.
- **Cold Start/Warm Start**: When the system or device reboots (cold or warm restart).



SNMP – Trap Event

RMON

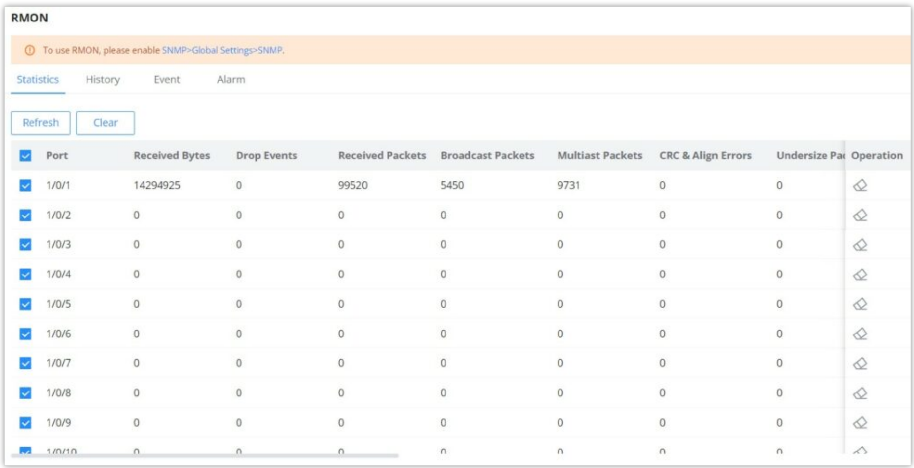
RMON (Remote Monitoring) based on SNMP (Simple Network Management Protocol) architecture, functions to monitor the network. RMON is currently a commonly used network management standard defined by Internet Engineering Task Force (IETF), which is mainly used to monitor the data traffic across a network 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.

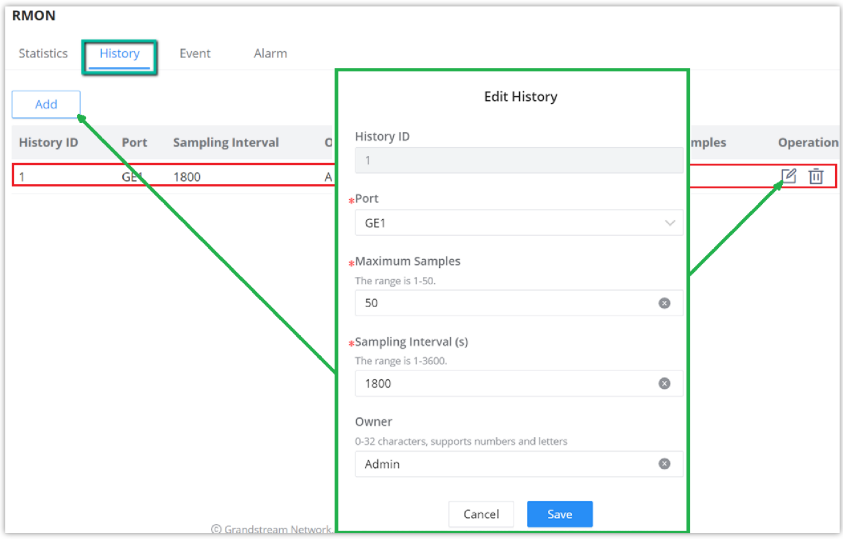


RMON – Statistics

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.

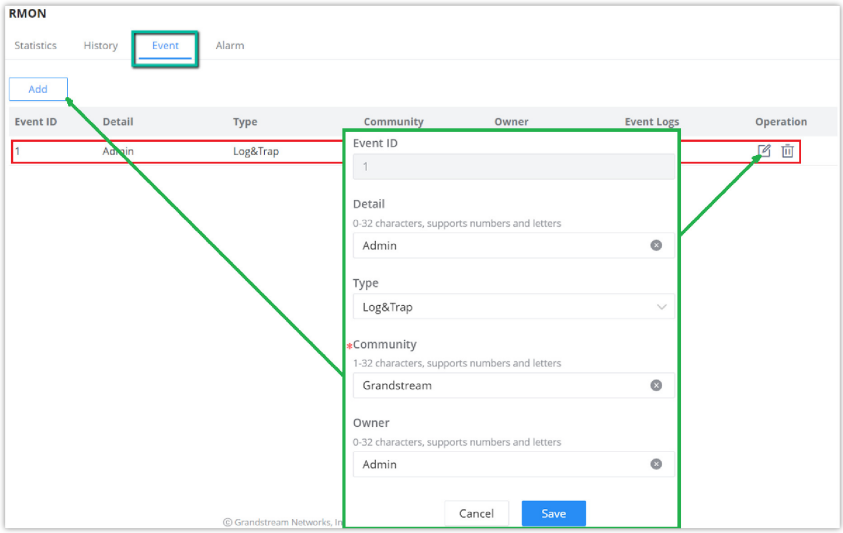
Click on “Add” button to create a History ID specifying the Port as well.



RMON – History

RMON Event

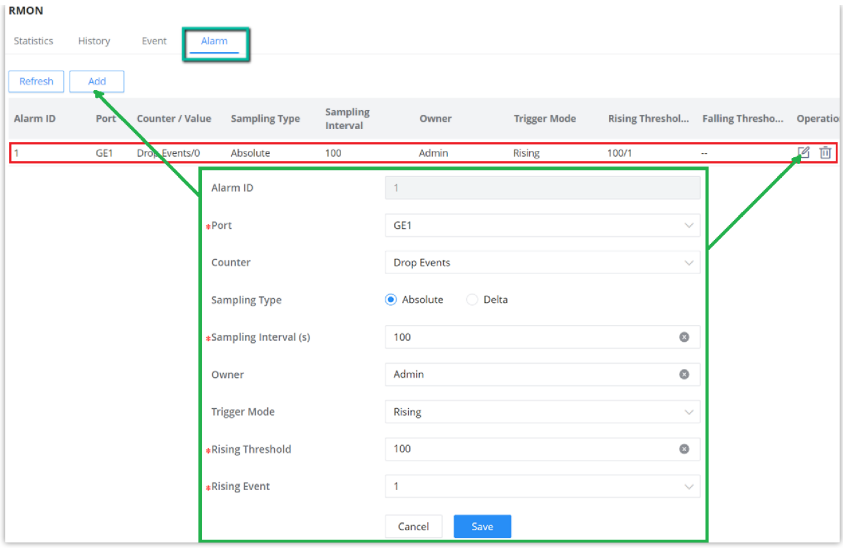
The event group controls the events and prompts from the device, and provides all events generated by the RMON Agent. When an event occurs, it can record logs or send Trap to the network management station.



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

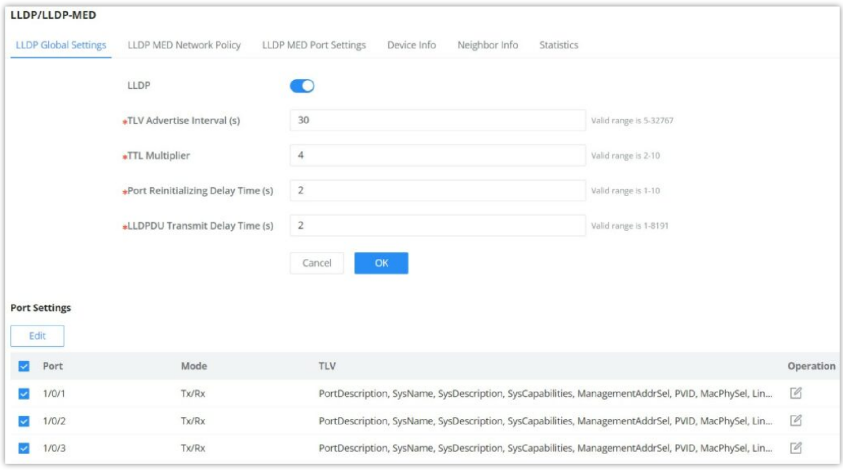
LLDP/LLDP MED

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);

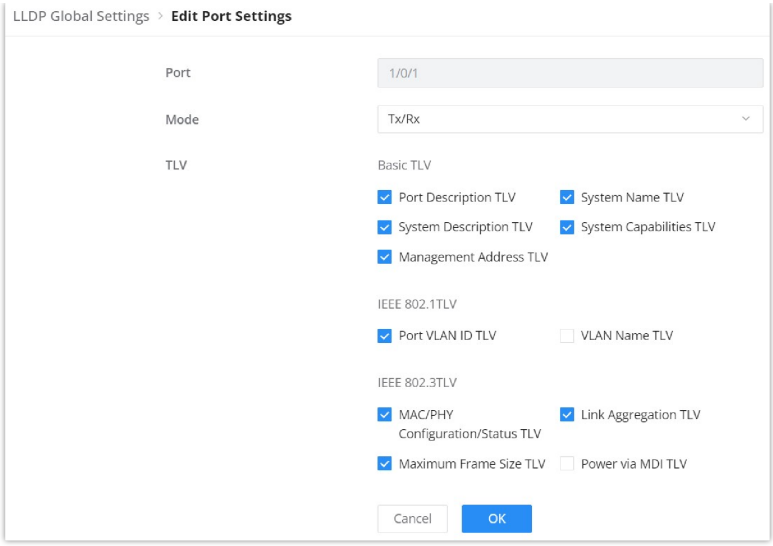
LLDP Global Settings

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



LLDP Global Settings

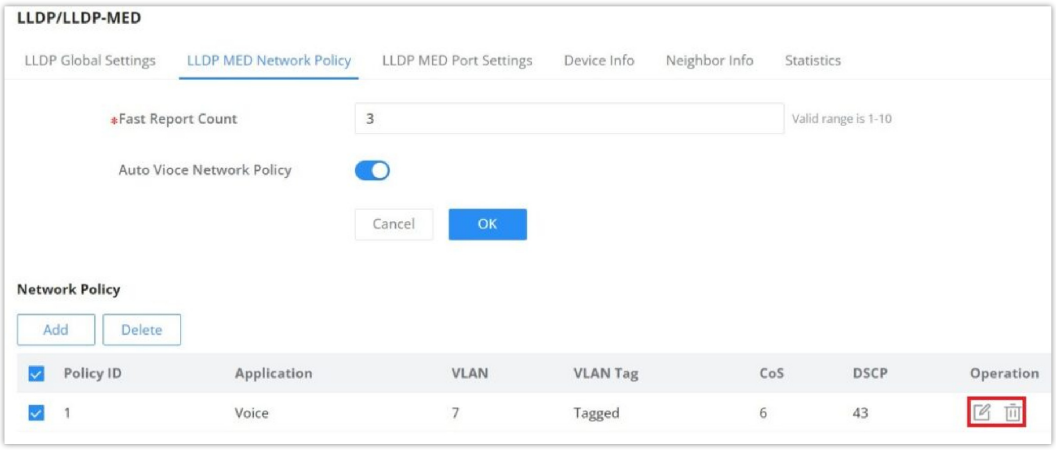
More configuration can adjusted per port (GE1 to GE10).



LLDP Port Settings

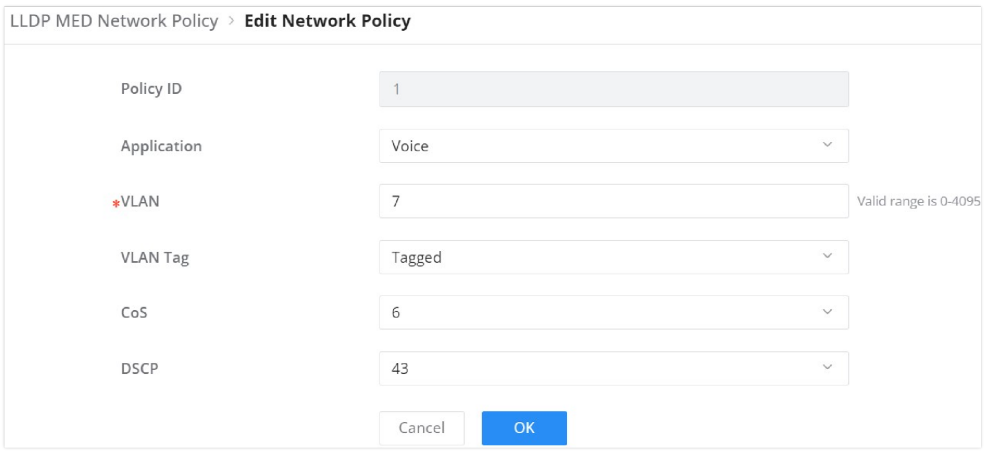
LLDP MED Network Policy

This page allows the network administrator to set MED (Media Endpoint Discovery) network policy. Click on "Add" button to add a Network Policy.



LLDP MED Network Policy

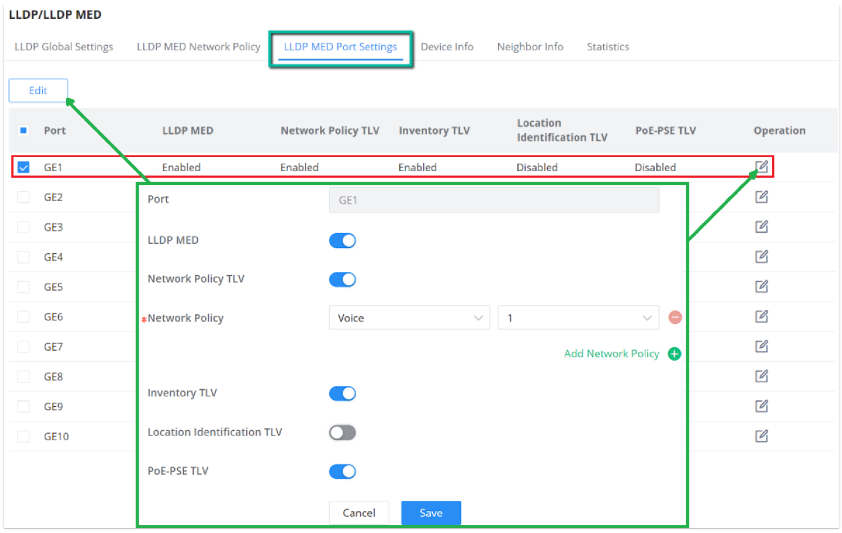
To add a Network Policy, click on "**Add**" button or click on "**Edit**" icon under Operation column to edit.



Add/Edit Network Policy

LLDP MED Port Settings

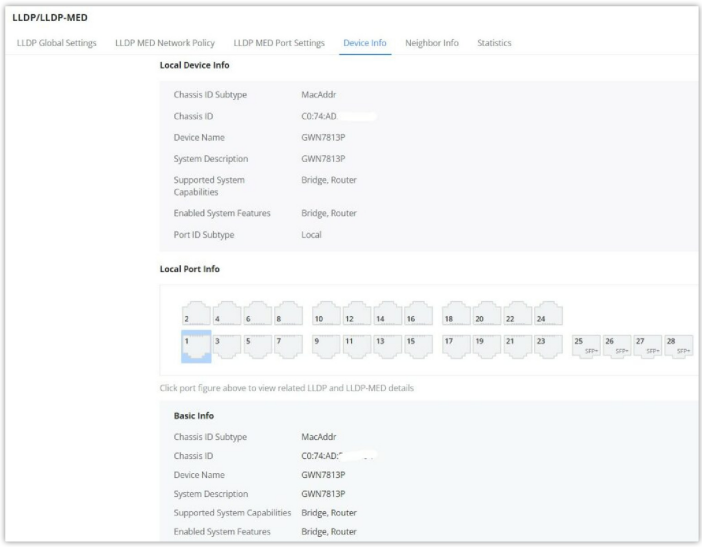
The user can configure LLDP MED Settings for each port in this page.



LLDP MED Port Settings

LLDP Device Info

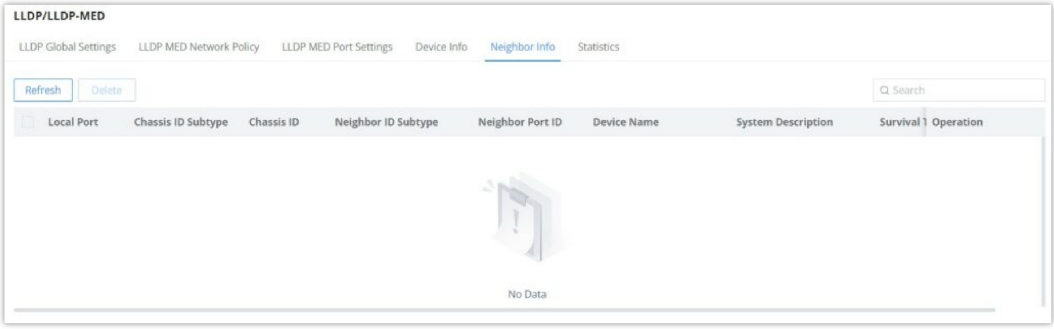
This page displays information for LLDP Local Device connected to each port. Click on the port to view related LLDP information about that port, the information include: Basic Info, **IEEE 802.1 TLVs** information, **IEEE 802.3 TLVs (802.3 bt)** information, **MED Details**, **Network Policy**...



LLDP Device Info

Neighbor Info

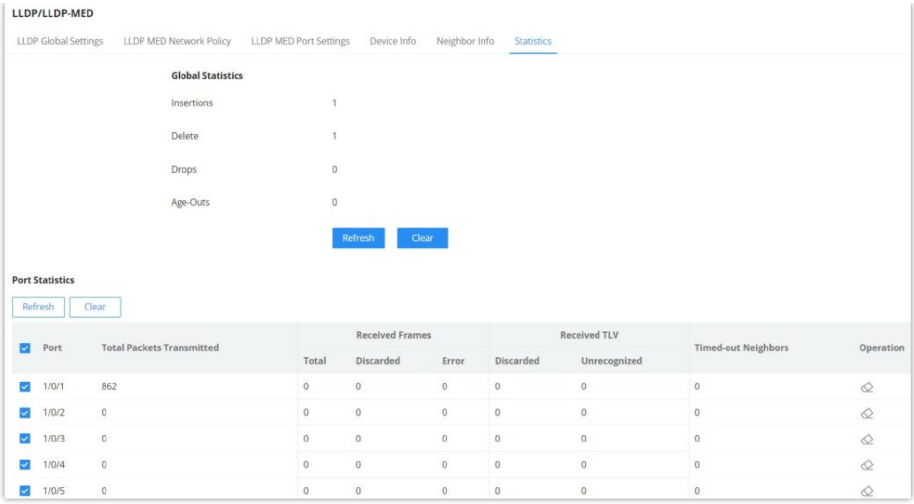
This page lists the neighbors obtained on the switch ports. Click on "Refresh" button to update the list.



LLDP Neighbor Info

LLDP Statistics

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



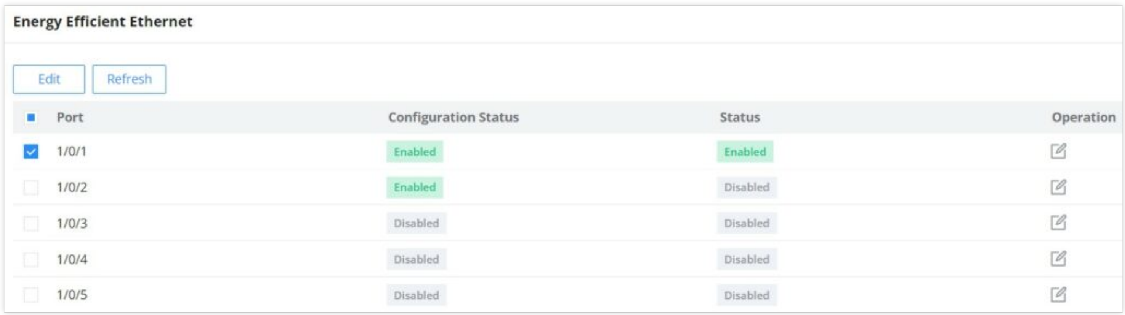
LLDP Statistics

Energy Efficient Ethernet

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.

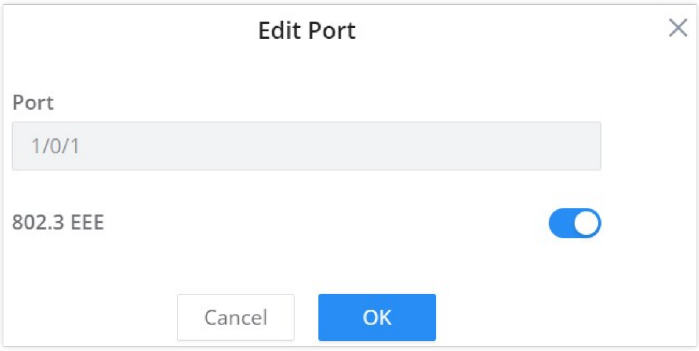
Navigate to **Maintenance** → **Energy Saving Management**, select a port to edit then enable 802.3 EEE.

- **Configuration Status:** shows if the configuration is enabled.
- **Status:** if a supported device is connected to the GWN78xx switch, it will show if it's enabled or not.



Energy Efficient Ethernet

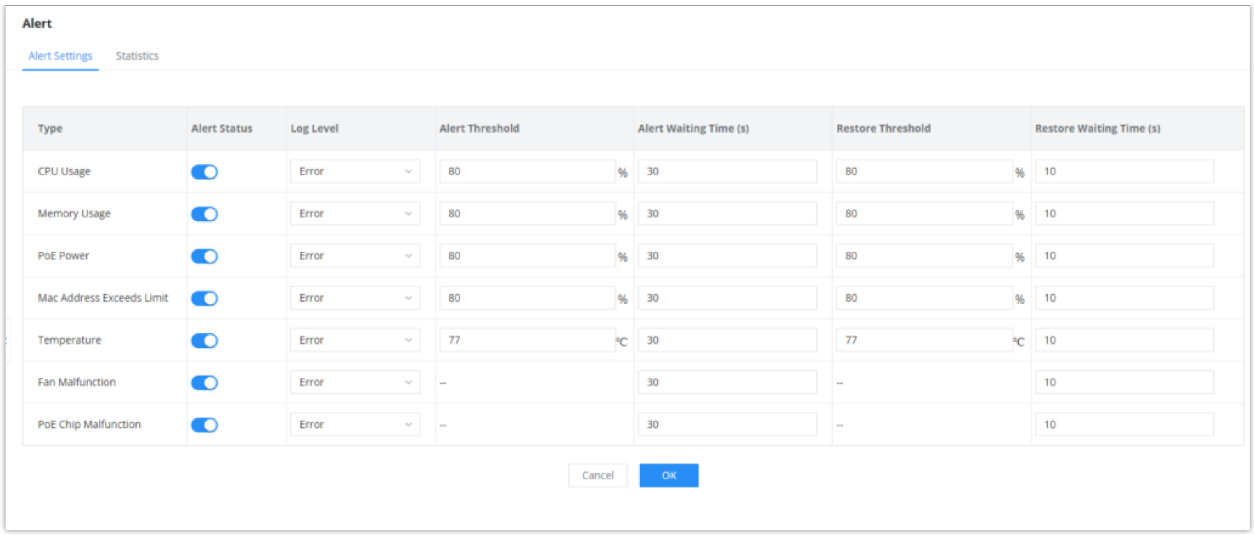
To enable EEE on a port, select a port then click on "**Edit"** button then toggle ON 802.3 EEE as shown below:



Energy Efficient Ethernet

Alert

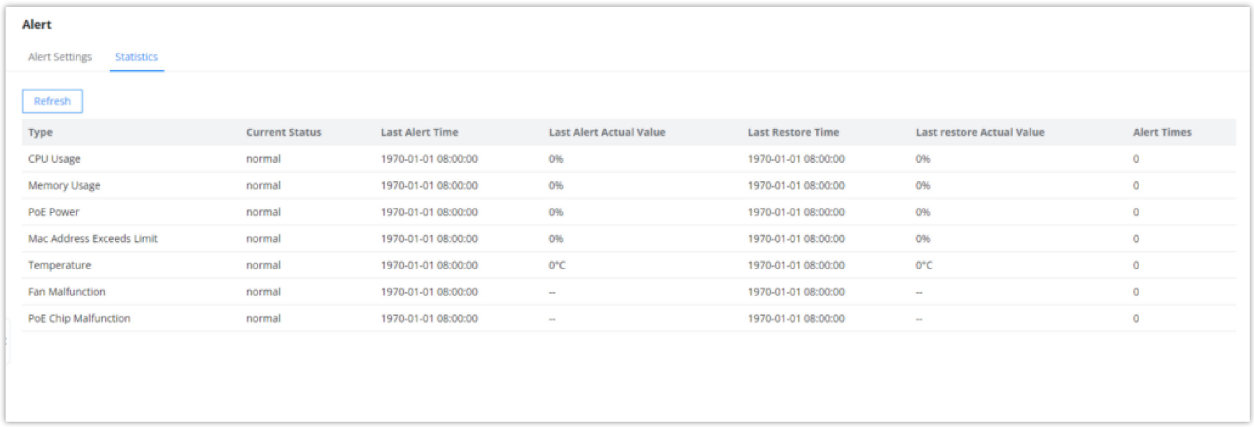
The Alerts section allows administartors to set up alert statuses for different types of system reactions for hardware components, this can be configured based on the component's performance, this can include factors such as CPU Usage, Memory Usage, PoE Power, MAC Address Exceeds Limit, Temperature, Fan Malfunctioning, PoE Chip Malfunctioning...



Alert Settings to Webp

Alert Statistics

The statistics section shows the current status of the Hardware components, in addition to some other hardware information, it alo displays the last alert time and last restore time of the service



Alert Statistics

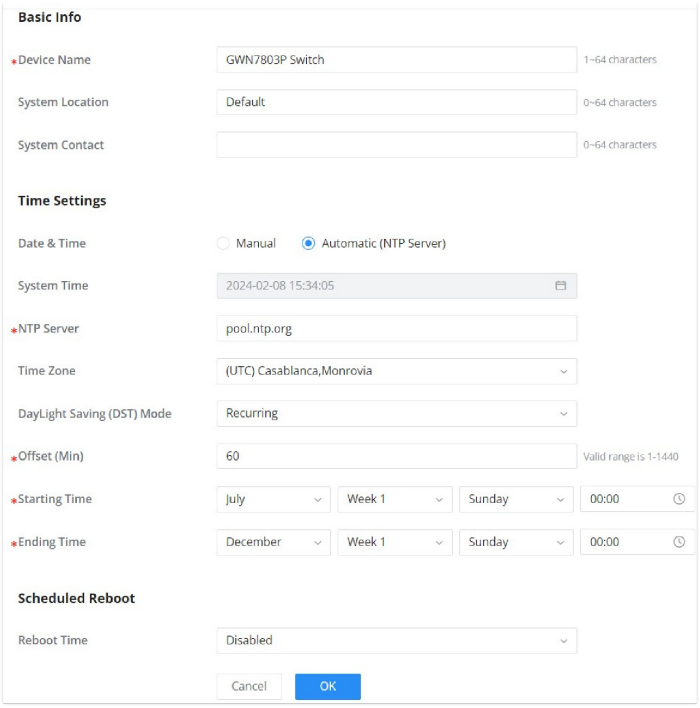
SYSTEM

Basic Settings

The basic settings page is split into three categories:

- **Basic Info:** first section, the user can specify a name for GWN78xx switch with a system location and contact.
- **Time Settings:** on this section, the users can configure the time either manually, or using a NTP Server, it's also possible to configure DayLight Saving (DST) Mode accordingly to the location or recurrence.
- **Scheduled Reboot:** the users can enabled scheduled reboot by adding a schedule under Time Policy.

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



Basic Settings

Basic Info	
Device Name	Specify a name for the device.
System Location	Enter system location.
System Contact	Specify the system contact.
Time Settings	
Date & Time	Select time synchronization method: Manual or Automatic (NTP Server). ● **Manual**: specify the time manually. ● **Automatic (NTP Server)**: time will be synced automatically with NTP Server. ***Note:*** *if the device is added to the GWN.Cloud and Auto Sync Time feature (under Settings → System) is enabled then the local NTP setting on the device will be disabled. All managed devices will synchronize the time from GWN.Cloud.*
System Time	● **If Manual is selected**, the user can specify the date and time. ● **If Automatic (NTP Server) is selected**, the current time and time will be displayed,
NTP Server	If Date & Time is set to Automatic (NTP Server), please specify the NTP Server address, by default is set to "pool.ntp.org" .
Time Zone	Select the time zone from the drop-down list.
DayLight Saving (DST) Mode	● **Disabled:** DayLight Saving mode will be disabled. ● **Recurring:** if the Daylight saving is recurring (repetitive). ● **Non Recurring:** if selected the user can specify the offset (min) and daylight saving time start date and end date. ● **Recurring USA:** for USA region. ● **Recurring EU:** for EU region
Offset (Min)	Specify the Offset by minutes, range from 1 to 1440.

Starting Time	Specify the starting date and time.
Ending Time	Specify the ending date and time.
Scheduled Reboot	
Reboot Time	Select a reboot time from the drop-down list or click on "+" button to add a schedule. By default is disabled.

Basic Settings

Access Control

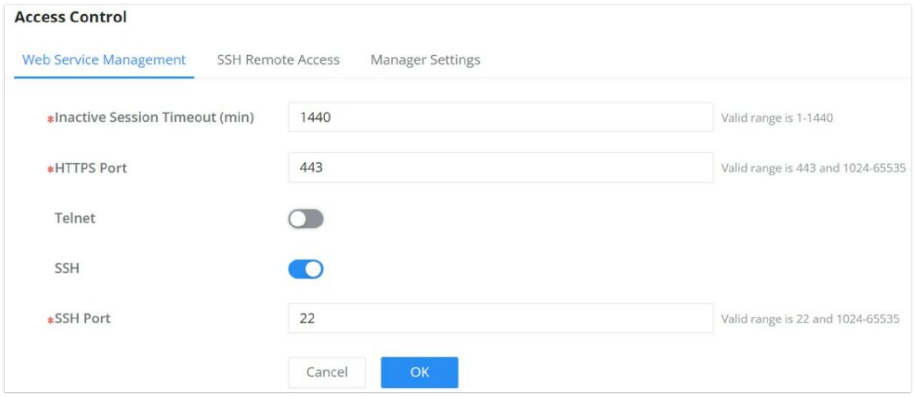
On this section, the user can configure the access to GWN78xx switches.

Please navigate to **System** → **Access Control**.

Web Service Management

On the first tab, the user can configure the following:

- **Inactive Session Timeout (min):** (the range is from 15 seconds to 1440) which is how much time before the GWN78xx switch will logout automatically.
- **HTTPS:** the HTTPS port, by default is 443, It can be changed if necessary. (it's recommended to keep it 443).
- **Telnet:** can be enabled, by default is disabled (it's recommended to keep disabled, it's not secure, and use instead SSH).
- **SSH:** SSH is enabled by default, and it's better alternative to Telnet, the default port is 22, It can be changed if necessary. (it's recommended to keep it 22)

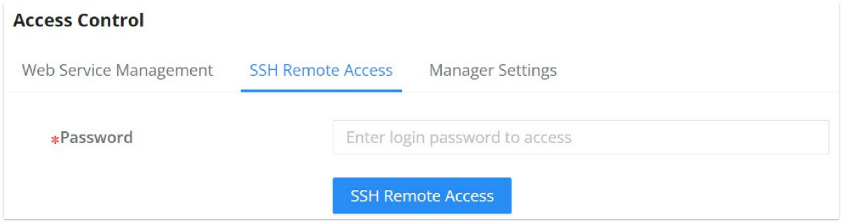


Access Control – Web Service Management

> **Note:**
>
> VTY (Virtual Teletype) sessions allow remote management of network devices through a command-line interface. GWN781x switches now support up to 12 simultaneous VTY sessions, enabling concurrent SSH or Telnet access for administrators.

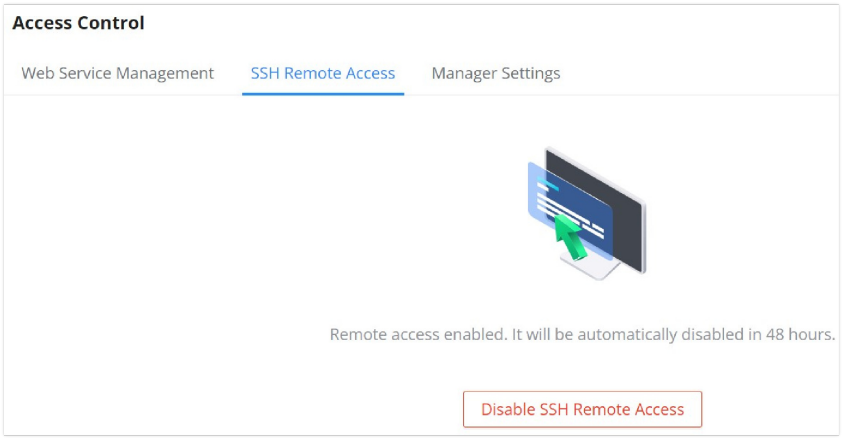
SSH Remote Access

> **Note:**
>
> This feature is exclusively used for troubleshooting purposes by our developers and support engineers. When remote access is requested by either party, please enter the current user's password to grant permission to access to the device.



Access Control – SSH Remote Access disabled

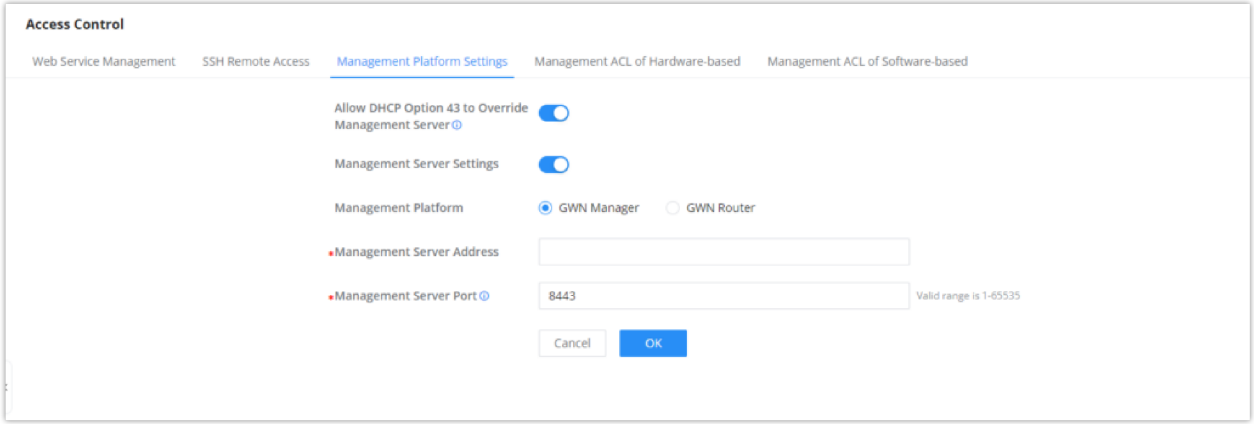
Enter the password, then click on "**SSH Remote Access**" button, it will be automatically disabled in 48 hours.



Access Control – SSH Remote Access enabled

Management Platform Settings

Manager Settings tab allows the users to configure GWN Manager or GWN Router access parameters (Server address and port). It's also possible to allow DHCP option 43 and if it's enabled If enabled, the server address assigned by DHCP Option 43 will be preferred.

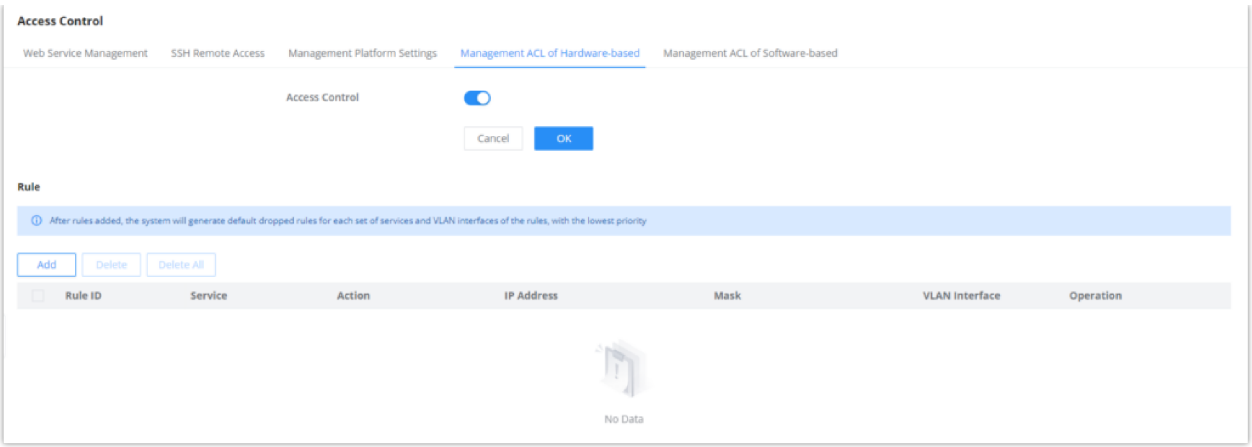


Access Control – Manager Settings

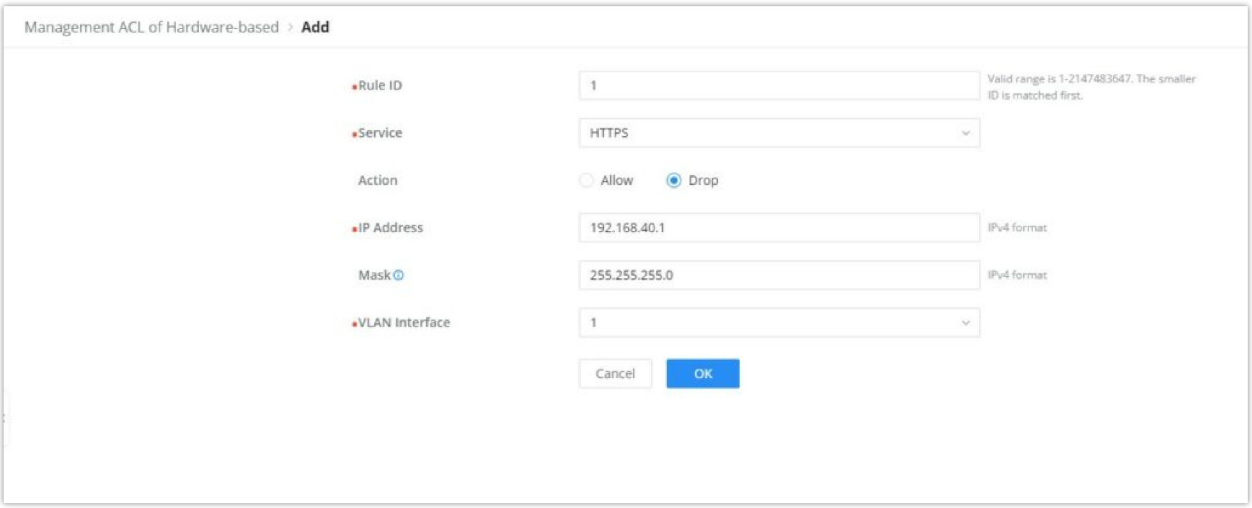
> **Note:**
>
> When GWN Manager wants to take over a managed switch, it can force the takeover by entering the switch current password.

Management ACL of Hardware-based

On a GWN78xx Layer 3 switch, the hardware management Access Control List (ACL) is designed to optimize resource efficiency by filtering traffic directly at the hardware level before it reaches the CPU. This pre-processing step ensures that only traffic matching the defined security rules is forwarded for further handling, effectively reducing unnecessary CPU load and enhancing overall performance. By offloading the initial traffic validation to the switch hardware, the GWN78xx improves both network efficiency and security.



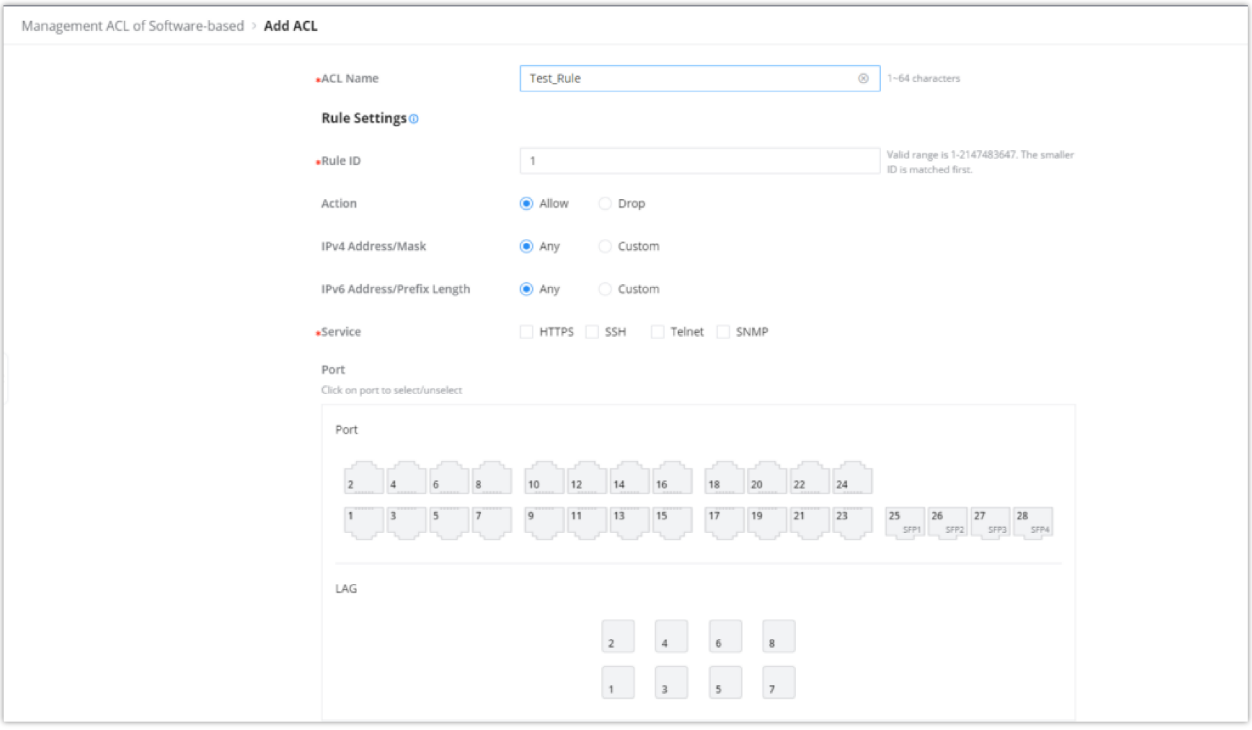
Management ACL of Hardware-based



Add a Hardware-based ACL Rule

Management ACL of Software-based

On the GWN78xx Layer 3 switch, the software-based Management ACL uses firewall-like rules to control who can access the network and its management features. This means it sets up restrictions to make sure that only authorized users and devices can access important parts of the switch, helping to keep the network secure and well-managed.



Management ACL of Software-based

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.

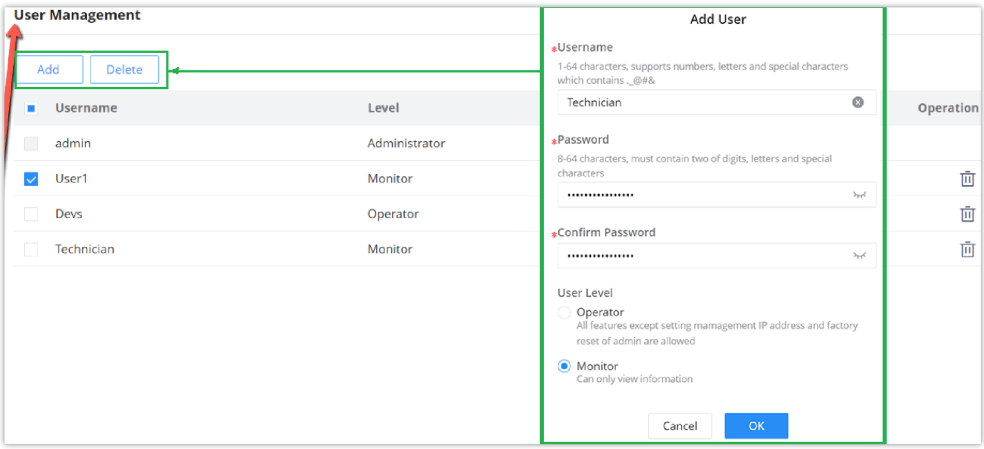
> **Note:**
>
> All features of admin are allowed except setting management IP address and factory reset.

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).

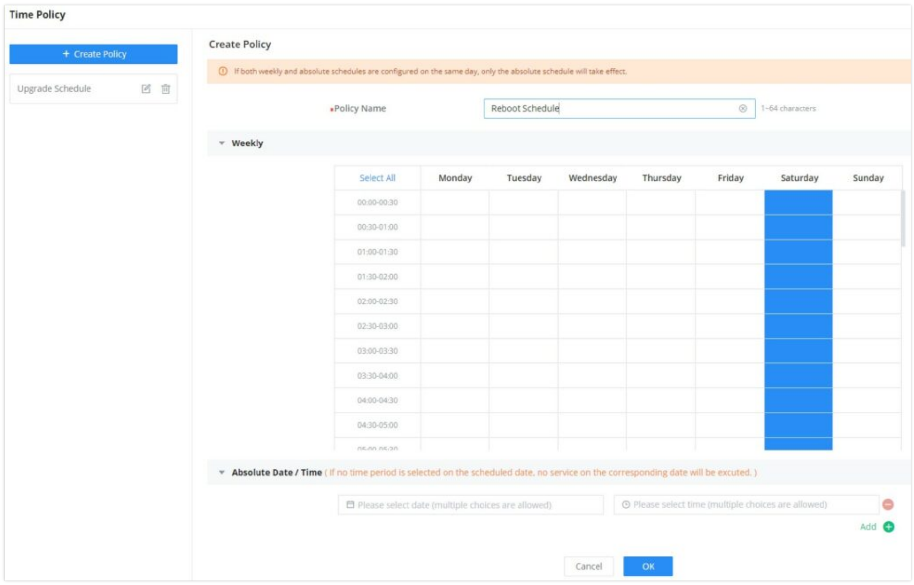


User Management

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.

CHANGE LOG

This section documents significant changes from previous versions of the GWN780x(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.

Firmware Version 1.0.9.15

- Added port groups. [Port Group]
- Added LLDP auto-config for Auto Voice VLAN mode. [LLDP/LLDP MED Auto Config]
- Added more features for STP, including ignore VLAN in BPDU, root protection and loopback protection. [Ignore VLAN in BPDU] [Root Protection] [Loop Protection]
- Added more OUI in Voice VLAN. [OUI]
- Added IP configuration for MGMT VLAN. [MGMT VLAN]
- Added redirect to interface for ACL. [Redirect to Interface]
- Added VLAN binding to ACL function.[VLAN Binding to ACL]
- Optimized the rate limit groups from 32 to128 in ACL. [Rate Limit Settings]
- Added mask for IPSG/IPv6SG. [IP Source Guard]
- Added remote-ID configuration based on port for DHCP Snooping. [DHCP Option 82]
- Changed DHCP's Option 82 Circuit ID/Remote ID. [DHCP Option 82]
- Added entries fixed for DHCP/DHCPv6 Snooping. [DHCP Snooping]
- Added flow upgrade via manual upgrade. [Upgrade Flow]
- Added more settings for logs, including minimum log level and log aggregation. [Log Aggregation]
- Added Ping watchdog in diagnostics. [Ping Watchdog]
- Added connection diagnostics of GWN router. [GWN Router]

- Added RSPAN, including port-based and ACL-based remotely mirroring. [RSPAN] [Configuring an ACL based RSPAN]
- Added new SNMP Traps. [Trap Event]
- Added 802.3bt info in LLDP. [IEEE 802.3 TLV]
- Added Maintenance Alerts. [Alert]
- Added management ACL, including hardware-based and software-based management ACL. [Management ACL of Hardware-based] [Management ACL of Software-based]
- Added Layer 3 discovery and management by GWN router.[Management Platform Settings]
- Added ACL for VTY (SSH and telnet). [Web Service Management]
- Added additional Radius Access-Request Attributes. [Identity Authentication Management]
- Removed Commited Burst Configuration from Queue Shaping. [Queue Shaping]

Firmware Version 1.0.5.61

- Optimized search for Web GUI. [Search]
- Optimized CPU and memory usage in Web GUI. [System Info]
- Optimized device IP address display [System Info]
- Added more port details such as neighbor, PoE power history info. [Port Info]
- Added port scheduled enabling feature. [Port Basic Settings]
- Added more port statistics info. [Port Statistics]
- Added loopback detection feature. [Loopback Detection]
- Added QinQ. [VLAN]
- Optimized trunk port settings. [VLAN Port Members]
- Added MAC-based VLAN. [MAC VLAN]
- Added protocol-based VLAN. [Protocol VLAN]
- Added VLAN translation. [VLAN Port Settings]
- Added default gateway configuration under MGMT VLAN. [VLAN IP Interface]
- Added gateway priority when using DHCP to get VLAN IP address. [VLAN IP Interface]
- Optimized DHCP option 43 configuration for DHCP server. [DHCP Server]
- Added advanced ACL settings, including mirroring, statistics, and priority remapping for a rule. [ACL]
- Added import/export IPSG binding table for IP Source Guard. [IP Source Guard]
- Added IPv6 Source Guard. [IPv6 Source Guard]
- Optimized remote ID and Circuit ID for DHCP Snooping. [DHCP Snooping option 82]
- Added DHCPv6 Snooping. [DHCPv6 Snooping]
- Added upgrade by FTP and Explicit FTPS. [Upgrade]
- Added connection diagnostics with GWN.Cloud/Manager. [Cloud/Manager Connection Diagnostics]
- Optimized EEE. [Energy Efficient Ethernet]
- Added DST mode for time settings. [Basic Settings]
- Added HTTPS/SSH port customization. [Web Service Management]
- Optimized Manager settings. [Manager Settings]
- Added rate limit by ACL binding to VLAN. [VLAN Binding to ACL]
- Added MAC bypass authentication. [Local User of MAC-based]
- Add GWN Manager takeover function. [Manager Settings]
- Expanded DHCP leases range up to 11520 min. [DHCP Server]
- Adjust the maximum length of the command line to 2000. [CLI Access]
- Added support to see switch clients and other information. [Port Info]

Firmware Version 1.0.3.37

- Added support for GWN Cloud 1.1.25.23. [GWN.Cloud]
- Added support of SSH and TELNET in # mode. [Login Remotely using SSH]
- Added support of Dynamic Voice VLAN. [Voice VLAN]
- Added support of voice VLAN OUI Untagged mode. [Voice VLAN]
- Added support of backspace when using CLI. [Login Remotely using SSH]

Firmware Version 1.0.3.19

- Added support of EEE [Energy Efficient Ethernet]
- Added feature of ARP table [ARP table]
- Added support of neighbor discovery [Neighbor Discovery]
- Added feature of IPv6 RA, RS [Neighbor Discovery]
- Added feature of copper test [Copper test]
- Added feature of one key debugging [One-click Debugging]
- Added feature of VLAN IP Interface [VLAN IP Interface]
- Added feature of DHCP server [DHCP Server]
- Added feature of time scheduling [Time Policy]
- Added support of Layer 2 and Layer 3 GWN Manager discovery [Access Control]
- Added support of ErrDisable status to port information [Port Info]
- Added support of SSH/Telnet client [Access Control]
- Added support of fan status to system information [System Info]
- Added support of SSH remote access [SSH remote access]
- Added support of switch IP interface DNS configuration [DNS]
- Added support of port based enable/disable in QoS port priority [Port Priority]
- Added support of SP-WRR and SP-WFQ to queue policy of QoS [Queue Scheduling]
- Added feature of routing table [Routing Table].
- Added feature of static routing [Static Routes].
- Added feature of DHCP relay [DHCP Relay]

Firmware Version 1.0.1.36

- Added DNS configurations for switch IP service. [DNS]

Firmware Version 1.0.1.30

- No major changes

Firmware Version 1.0.1.20

- This is the initial version.