

## Grandstream Networks, Inc.

### GWN783x L3 Aggregation **User Manual**



# GWN783x L3 Aggregation - User Manual

## WELCOME

The GWN7830 series are Layer 3 aggregation managed switches that allow enterprises to build scalable, secure, high performance and smart business networks that are fully manageable. It supports advanced VLAN for flexible and sophisticated traffic segmentation, advanced QoS for prioritization of network traffic, IGMP/MLD Snooping for network performance optimization, comprehensive security capabilities against potential attacks. GWN7830 series can be managed in a number of ways, including the local Web user interface of the switch and CLI, the command-line interface. And also supported by GWN.Cloud and GWN Manager, Grandstream's cloud and on-premise network management platform. With complete end-to-end quality of service and flexible security settings, the GWN7830 series are the best value enterprise-grade aggregation managed switches.

## PRODUCT OVERVIEW

### Technical Specifications

	GWN7830	GWN7831	GWN7832
<b>Network Protocol</b>	IPv4, IPv6, IEEE 802.3, IEEE 802.3i, IEEE 802.3u, IEEE 802.3ab, IEEE 802.3z, IEEE 802.3ae, IEEE 802.3az, IEEE 802.3ad, IEEE 802.3x, IEEE 802.1p, IEEE 802.1Q, IEEE 802.3AB, IEEE 802.1D, IEEE 802.1s, IEEE 802.1w, IEEE 802.1x		
<b>Gigabit Ethernet Ports</b>	2	4x Combo	/
<b>Gigabit SFP Ports</b>	6	4x Combo, 20x SFP	/
<b>10 Gigabit SFP+ Ports</b>	4		12
<b>Console</b>	1		
<b>Integrated Power Supply</b>	30W	60W	
<b>External Redundant Power Supply(RPS)</b>	/	12V/60W	
<b>Auxiliary Ports</b>	1x Reset Pinhole		
<b>Forwarding Mode</b>	Store-and-forward		
<b>Total non-blocking throughput</b>	48Gbps	64Gbps	120Gbps
<b>Switching Capability</b>	96Gbps	128Gbps	240Gbps

<b>Forwarding Rate</b>	71.424Mpps	95.232Mpps	80.352Mpps
<b>Packet Buffer</b>	12MB		16MB
<b>Switching</b>	<ul style="list-style-type: none"> <li>• 16K static, dynamic and filtering MAC addresses</li> <li>• Spanning tree, 32 instances for STP/RSTP/MSTP</li> </ul>		<ul style="list-style-type: none"> <li>• 32K static, dynamic and filtering MAC addresses</li> <li>• Spanning tree, 64 instances for STP/RSTP/MSTP</li> </ul>
	<ul style="list-style-type: none"> <li>• 4K VLANs, port-based VLAN, IEEE 802.1Q VLAN tagging, voice VLAN</li> <li>• VLAN virtual interface</li> <li>• GVRP(pending)</li> <li>• 8 link aggregation</li> </ul>		
<b>Routing</b>	<ul style="list-style-type: none"> <li>• Static routing</li> <li>• Dynamic routing, including RIP, RIPng, OSPF and OSPFv3</li> <li>• Policy routing (pending)</li> </ul>		
<b>Multicast</b>	<ul style="list-style-type: none"> <li>• IGMP Snooping with IGMPv2 and IGMPv3</li> <li>• MLD Snooping with MLDv1 and MLDv2</li> <li>• MVR (pending)</li> </ul>		
<b>QoS/ACL</b>	<ul style="list-style-type: none"> <li>• Port priority</li> <li>• Priority mapping</li> <li>• Queue scheduling, including SP, WRR, WFQ, SP-WRR and SP-WFQ</li> <li>• Traffic shaping</li> <li>• Rate limit</li> </ul>		
	2K ACL for Ethernet, IPv4 and IPv6		4K ACL for Ethernet, IPv4 and IPv6
<b>DHCP</b>	DHCP server, DHCP relay, Option 82, 60, 160 and 43		
<b>Maintenance</b>	CPU and memory monitoring, fault detection and alarm for power supply and fan, SNMP, RMON, LLDP&LLDP-MED, backup and restore, syslog, diagnostics including Ping, Traceroute, port mirroring, UDLD(TBD) and copper test		

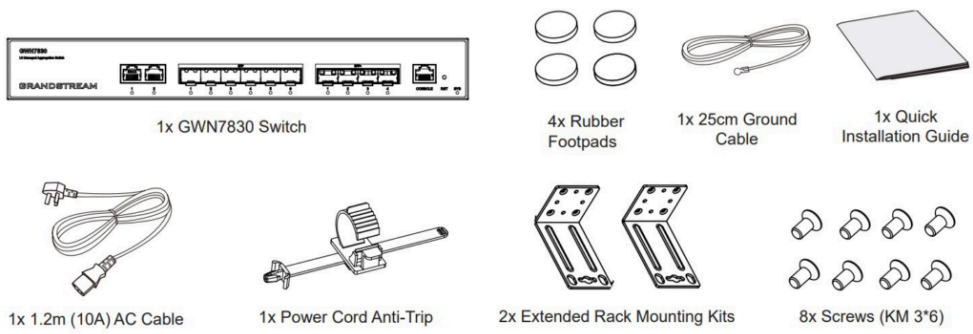
*Technical Specifications*

## INSTALLATION

Before deploying and configuring a GWN783x 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 GWN783x switch.

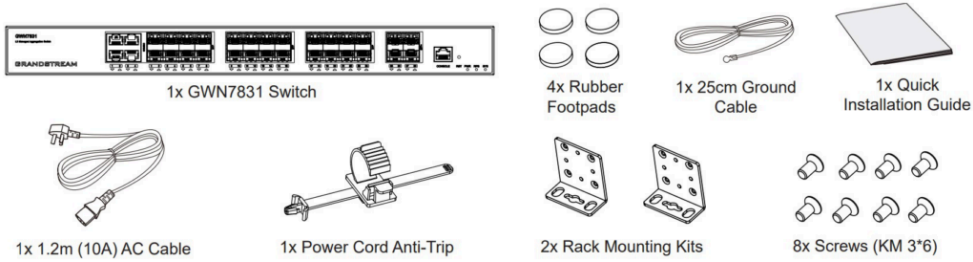
### Package Content

#### GWN7830



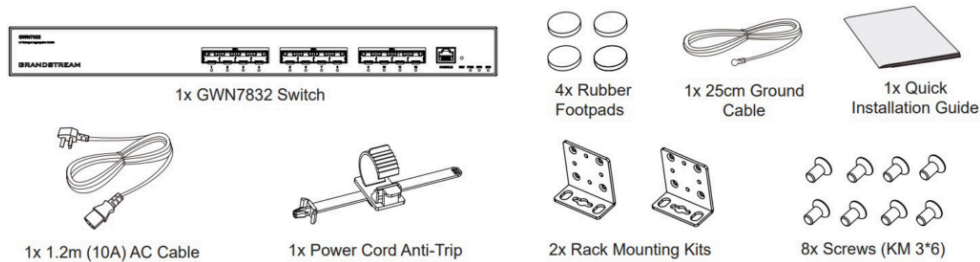
GWN7830 – Package Content

**GWN7831**



GWN7831 – Package Content

**GWN7832**

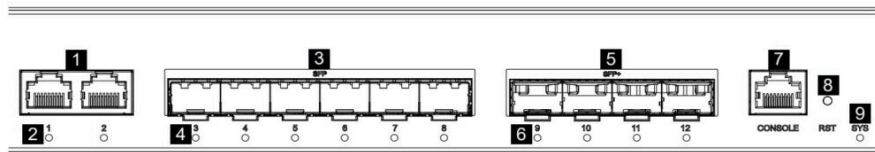


GWN7832 – Package Content

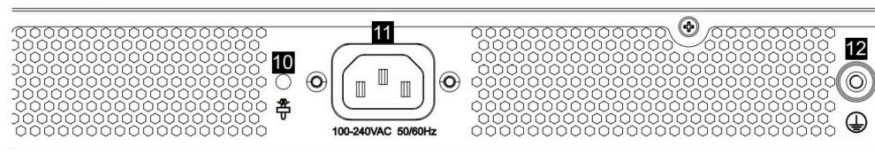
**GWN783X Ports**

**GWN7830**

**Front Panel**





**Back Panel**



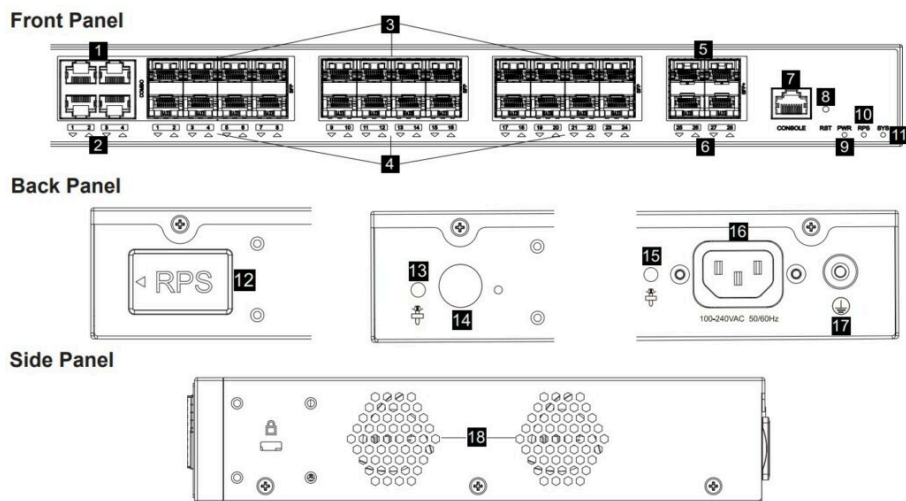
GWN7830 – Ports

No.	Port & LED	Description
1	Ports 1-2	2x 10/100/1000Mbps Ethernet ports
2	1-2	Ethernet ports' LED indicators

3	Ports 3-8	6x 1Gbps SFP ports
4	3-8	SFP ports' LED indicators
5	Ports 9-12	4x 10Gbps SFP+ ports
6	9-12	SFP+ ports' LED indicators
7	Console	1x Console port, used to connect a PC directly to the switch and manage it.
8	RST	Factory Reset pinhole, press for 5 seconds to reset factory default settings
9	SYS	System LED indicator
10		Power cord anti-trip hole
11	100-240VAC 50-60Hz	Power socket
12		Grounding terminal






GWN7830 Ports

## GWN7831



GWN7831 Ports

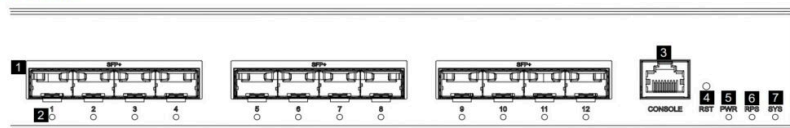
No.	Port & LED	Description
1	Ports 1-4	4x 10/100/1000Mbps Ethernet ports
2	1-4	Ethernet ports' LED indicators
3	Ports 1-24	24x 1Gbps SFP ports <b>Note:</b> SFP 1-4 and Port 1-4 combine 4 Combo ports.
4	1-24	SFP ports' LED indicators
5	Ports 25-28	4x 10Gbps SFP+ ports

6	25-28	SFP+ ports' LED indicators
7	Console	1x Console port, used to connect a PC directly to the switch and manage it.
8	RST	Factory Reset pinhole, press for 5 seconds to reset factory default settings
9	PWR	Internal power supply LED indicator
10	RPS	Secondary external power supply LED indicator
11	SYS	System LED indicator
12		External power supply rubber plug
13		Power cord anti-trip hole
14		External RPS power outlet
15		Power cord anti-trip hole
16	100-240VAC 50-60Hz	Power socket
17		Grounding terminal
18	Fan	2x Fans

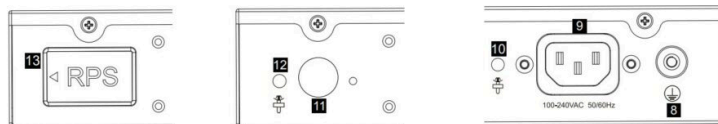
GWN7831 Ports

## GWN7832

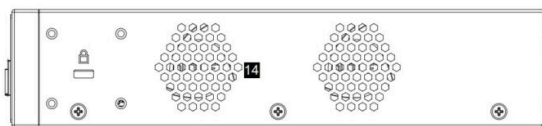
### Front Panel



### Back Panel








### Side Panel



GWN7832 Ports

No.	Port & LED	Description
1	Ports 1-12	12x 10Gbps SFP+ ports

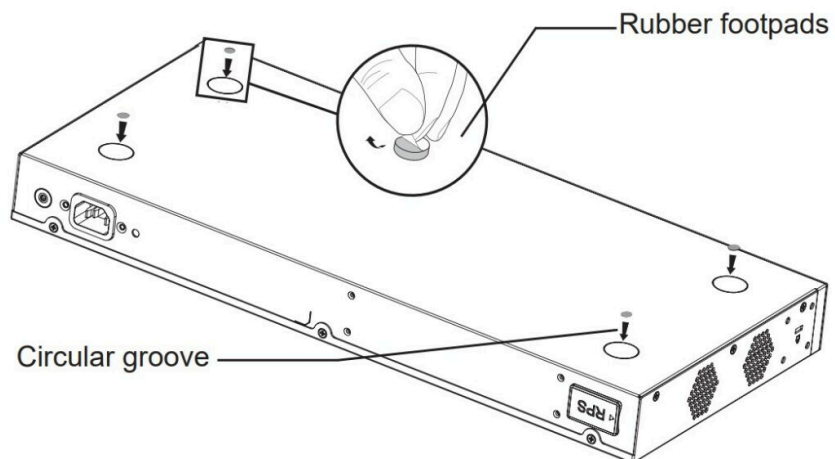
2	1-12	SFP+ ports' LED indicators
3	Console	1x Console port, used to connect a PC directly to the switch and manage it.
4	RST	Factory Reset pinhole, press for 5 seconds to reset factory default settings
5	PWR	Internal power supply LED indicator
6	RPS	Secondary external power supply LED indicator
7	SYS	System LED indicator
8		Grounding terminal
9	100-240VAC 50-60Hz	Power socket
10		Power cord anti-trip hole
11		External RPS power outlet
12		External RPS power cord anti-trip hole
13		External power supply rubber plug
14	Fan	2x Fans

GWN7832 Ports

**Note:**

External RPS (Redundant Power Supply) is sold separately.

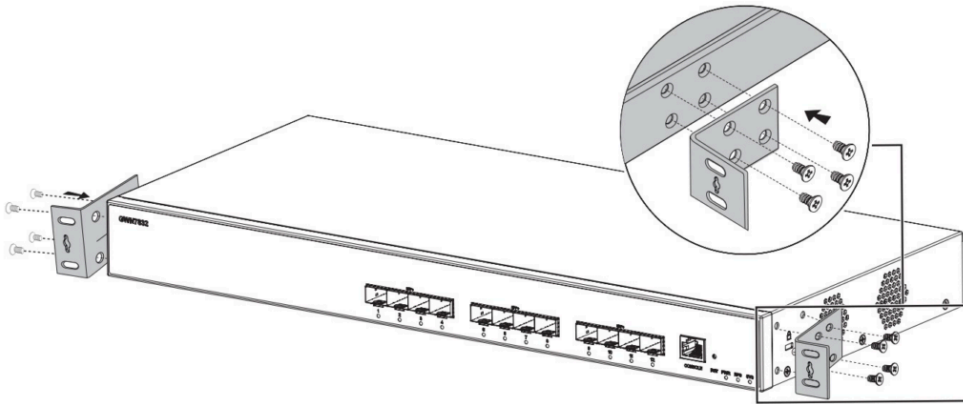
**Install on the Desktop**



Desktop Installation

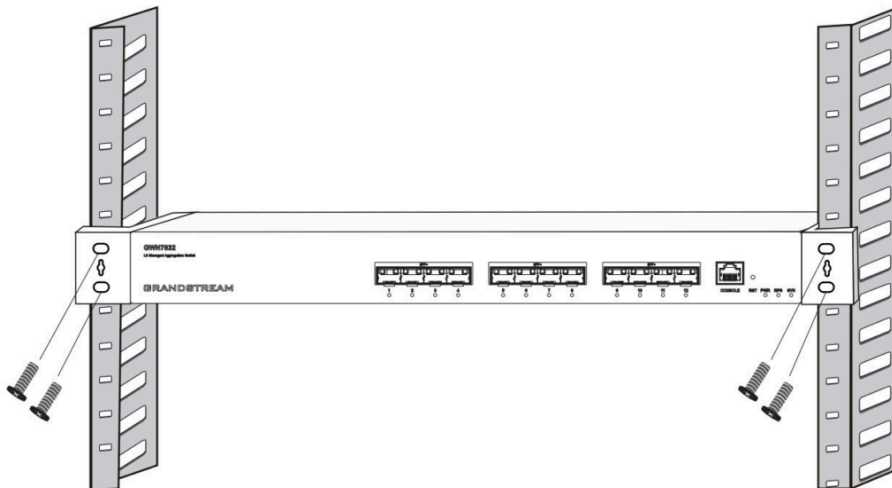
1. Place the bottom of switch on a sufficiently large and stable table.
2. Peel off the rubber protective paper of the four footpads one by one, and stick them in the corresponding circular grooves at the four corners of the bottom of the case.
3. Flip the switch over and place it smoothly on the table.

## Install on 19" Standard Rack



*Install on 19" Standard Rack*

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).



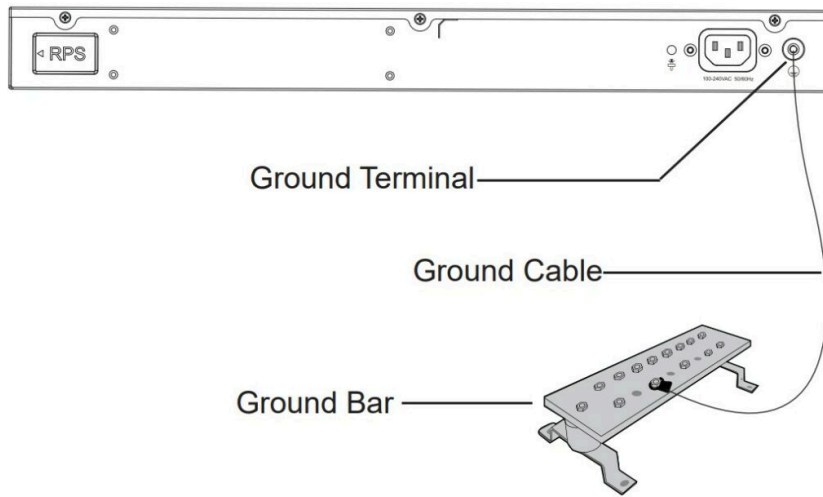
*Install on 19" Standard Rack*

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

## Powering and Connecting GWN783X

- **Grounding the Switch**



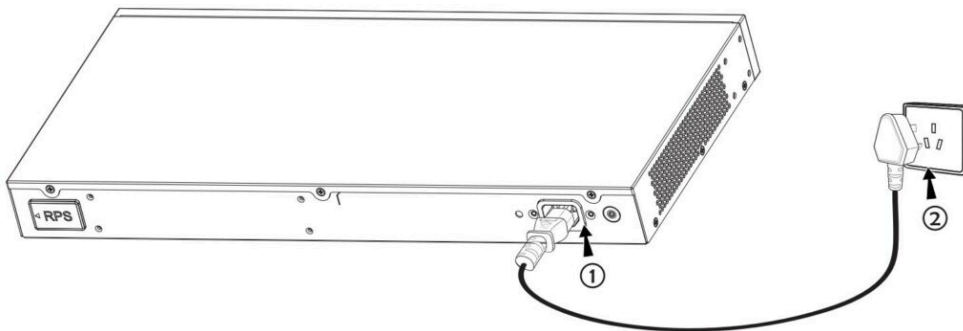


*Grounding the Switch*

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**

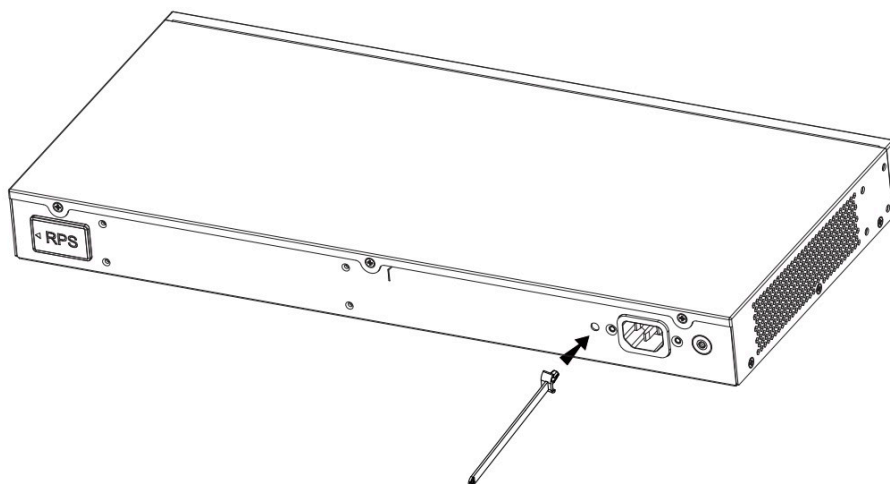
Connect the power cable and the switch first, then connect the power cable to the power supply system of the equipment room.



*Powering on the Switch*

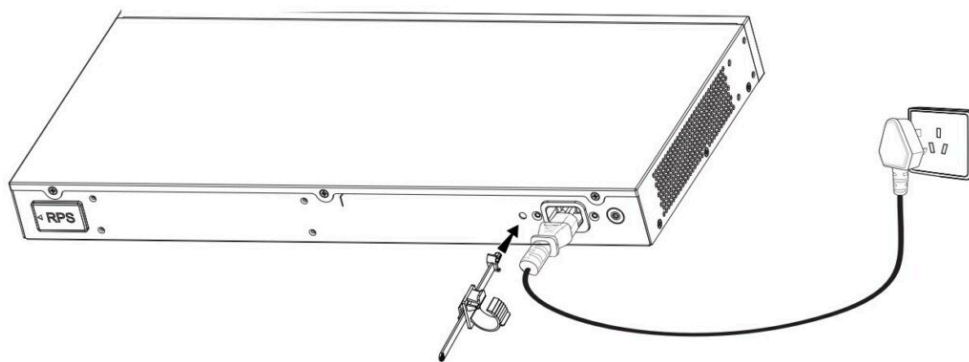
○ **Connecting Power Cord Anti-trip (Optional)**

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*

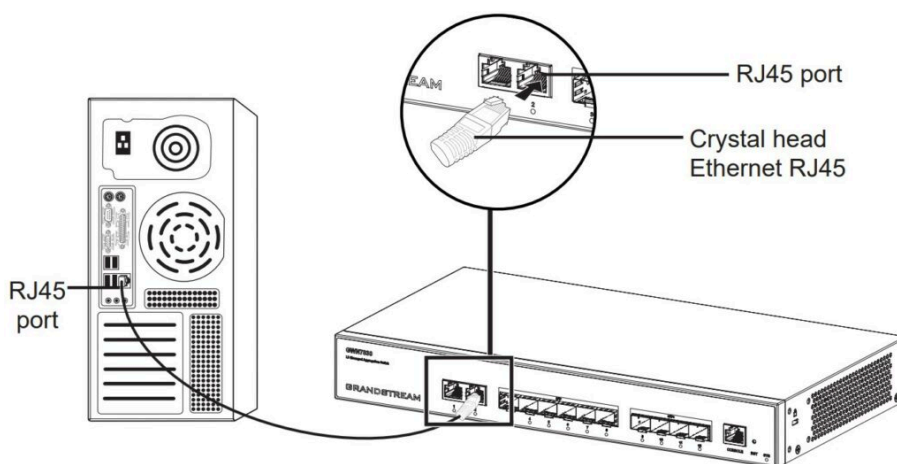
1. Place the smooth side of the fixing strap towards the power outlet and insert it into the hole on the side of it.



Connecting Power Cord Anti-trip

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.

o **Connect to RJ45 Port**



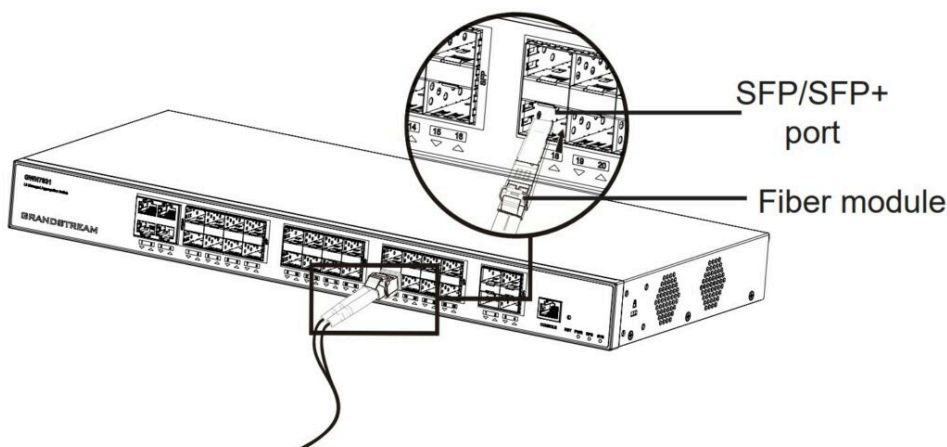
Connect to RJ45 Port

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.

**Note:**

For GWN7832 use a SFP+ to RJ45 transceiver module (not provided).

o **Connect to SFP/SFP+ Port**



Connect to SFP/SFP+ port

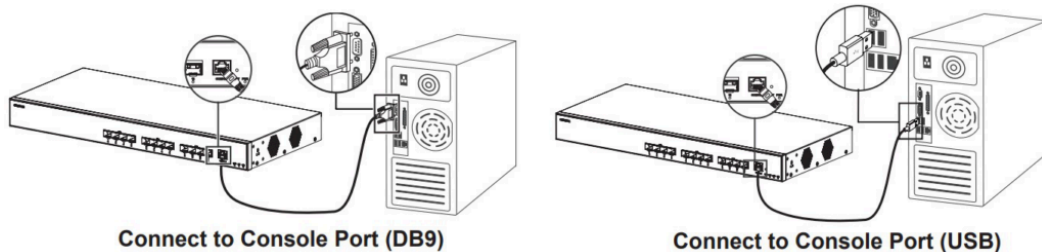
The installation process of the fiber module is as follows:

1. Grasp the fiber module from the side and insert it smoothly along the switch SFP/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/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 console cable (prepared by yourself) to the DB9 male connector or USB port to the PC.
2. Connect the other end of the RJ45 end of the console cable to the console port of switch.

**Notes:**

- To connect, the steps order (1 -> 2) must be respected.
- To disconnect, the steps order is reversed (2 -> 1).

**Safety Compliances**

The GWN783x L3 Aggregation Managed Network Switch complies with FCC/CE and various safety standards. The GWN783x power adapter is compliant with the UL standard. Use the universal power adapter provided with the GWN783x package only. The manufacturer's warranty does not cover damages to the device caused by unsupported power adapters.

**Warranty**

If GWN783x L3 Aggregation 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 GWN783x 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	Port off
	Solid green	Port with 10Gbps connected and there is no activity
	Flashing green	Port with 10Gbps connected and data is transferring
	Solid yellow	Port with 1Gbps connected and there is no activity
	Flashing yellow	Port with 1Gbps connected and data is transferring
PWR/RPS Indicator	Off	Unused or failure
	Solid Green	In use
	Solid Red	Overvoltage or undervoltage

*LED Indicators*

## Access & Configure

### Note

If no DHCP server is available, the GWN783x 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 GWN783x switch).

#### Note

The baud rate needs to be set to 115200.

## Login Remotely Using SSH

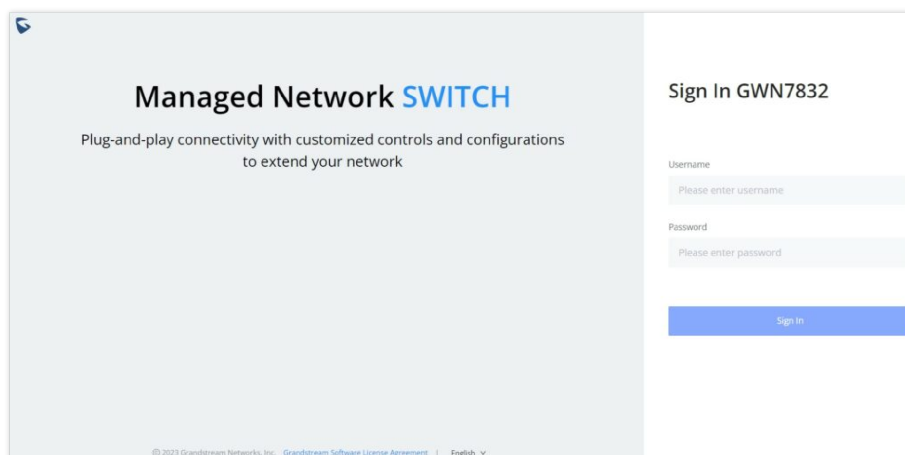
1. Enter "cmd" in PC/Start.
2. Enter `ssh <gwn783x_IP>` in the cmd window.
3. Enter the default username and password to login. (The default administrator username is "admin" and the default random password can be found at the sticker on the GWN783x switch).

## 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 GWN783x embedded Web server responds to HTTPS GET/POST requests. Embedded HTML pages allow users to configure the device through a Web browser such as Microsoft Edge, Mozilla Firefox, or Google Chrome.



*Login Using the Web UI*

1. A PC uses a network cable to correctly connect any RJ45 port of the switch (or SFP/SFP+ using SFP+ to RJ45 transceiver module).
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://<gwn783x_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 GWN783x switch).

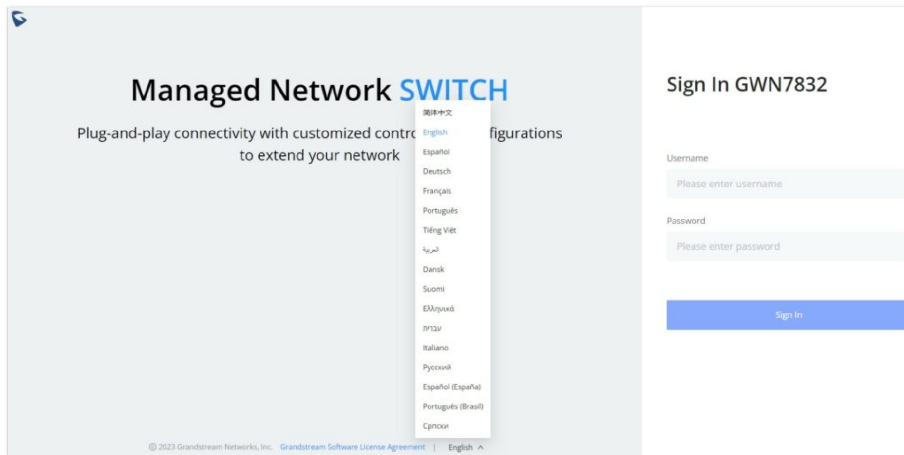
## CLI Access

In addition to the web-based configuration, the GWN783x 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](#).

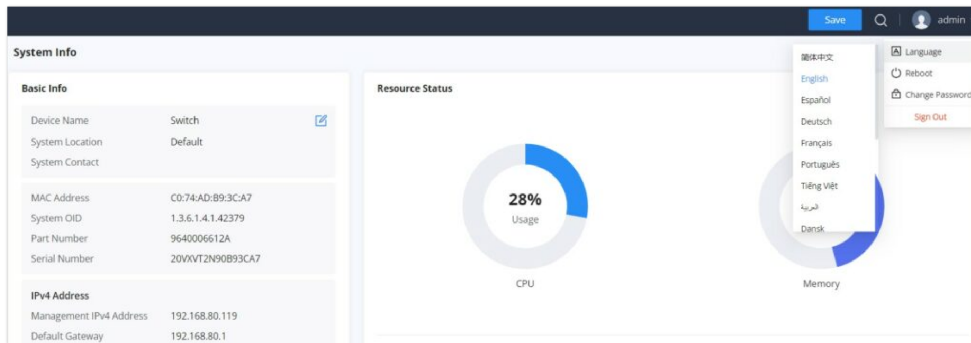
## Web GUI Languages

The GWN783x web GUI supports many languages including **English, Simplified Chinese, Spanish, French** etc.

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



Web GUI Languages – Login Page

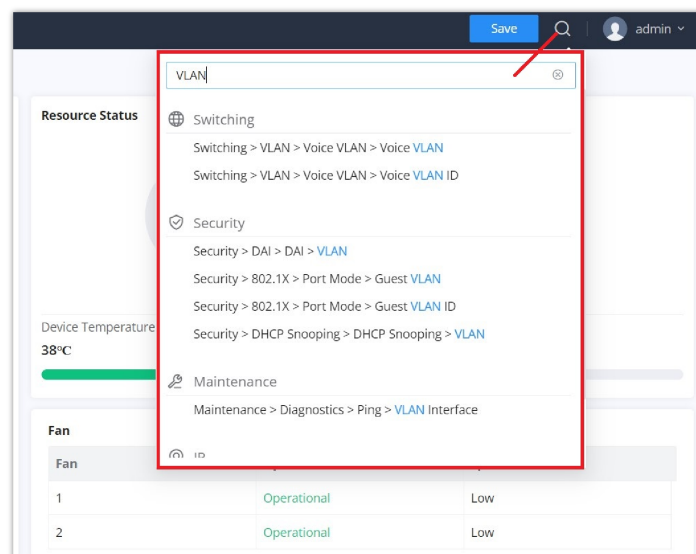


WEB GUI – Start page

## Search

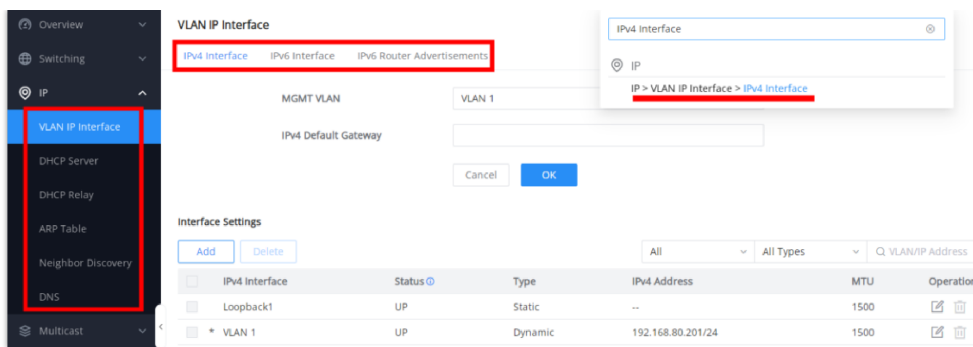
In case it's hard to go through every single section, GWN783x Switches have search functionality to help the user find the right configuration, settings or parameters, etc.

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:



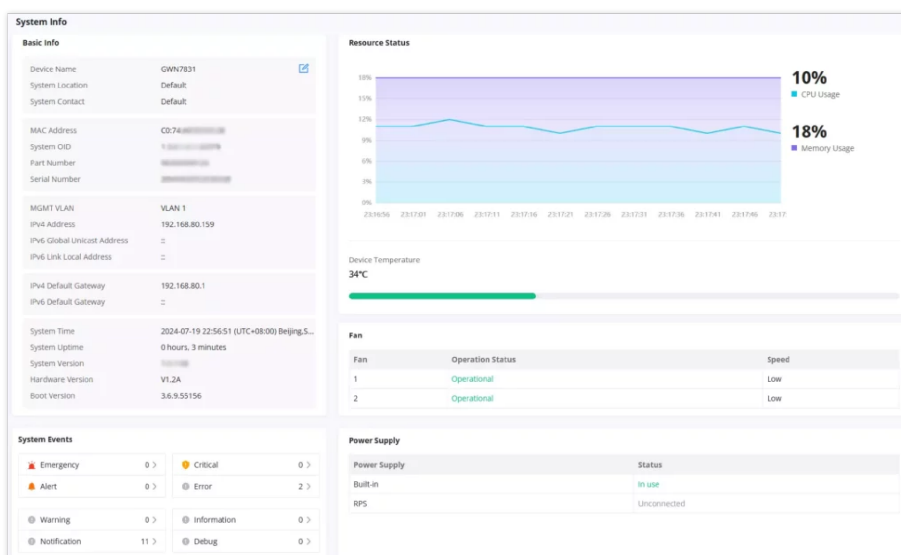
Search – part 2

## 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 GWN783x system and ports status for easy monitoring.

### System Info

System Info is the first page after a successful login to the GWN783x Web Interface. It provides an overall view of the GWN783x Switch information presented in a Dashboard style for easy monitoring including basic info, Resources Status, FAN Status and System Events.



System Info page

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

<b>Basic Info</b>	Displays Device and System general information that includes (Device name, MAC Address, Default Gateway, System Time, System Version etc.)
<b>Resource Status</b>	Displays in real time the usage of CPU and Memory.
<b>Fan</b>	Displays the fans operation status and speed.
<b>System Events</b>	Displays the total number of events for each category (Emergency, Alert, Warning etc). <b>Note:</b> Clicking on any events category will redirect you to the Diagnostics page for further details.
<b>Power Supply</b>	Shows the status of Built-in and RPS power supply either in use or unconnected.

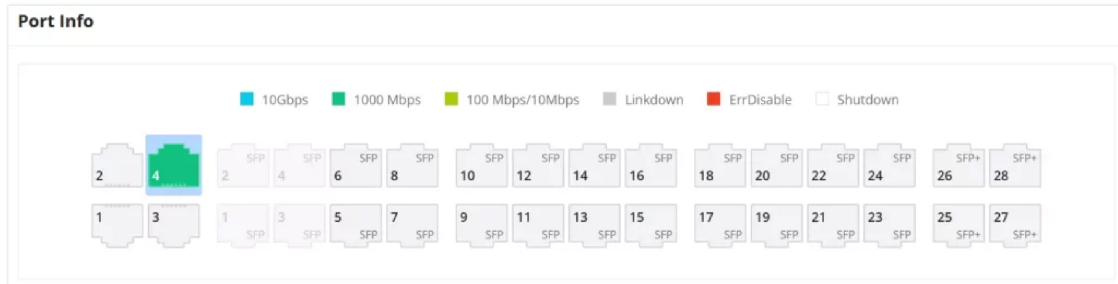
System Info page

## Port Info

This page on the GWN switches provides comprehensive port statistics, PoE power supply information, and detailed port and neighbor information. It helps users monitor network performance and manage connected devices efficiently.

- o **Port Info**

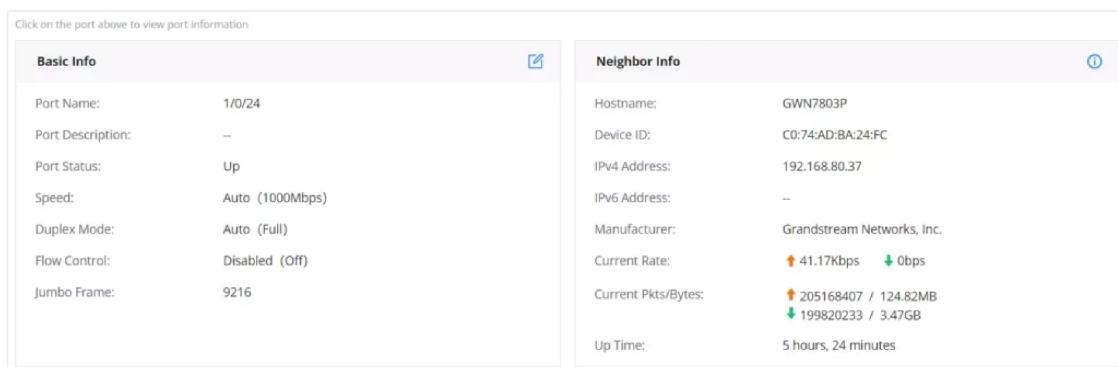
The **"Port Info"** section visually displays the status and speed of each port, using different colors for speeds and states. Users can quickly identify active, inactive, or problematic ports and their PoE power status.



Port Info page 1

- o **Basic Info and Neighbor Info**

The **"Basic Info"** section shows specific details for a selected port, including its status and settings. The **"Neighbor Info"** section provides information about the device connected to the port, such as hostname and current traffic rates.



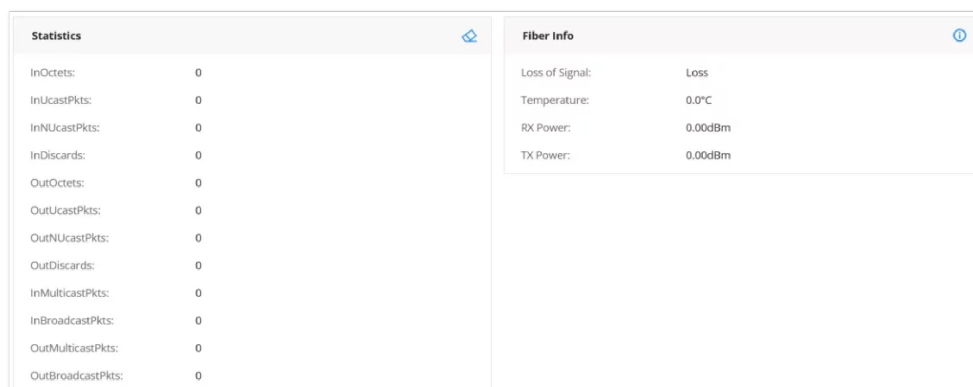
Port Info page 2

- o **Statistics**

The **"Statistics"** section offers detailed metrics on network traffic through the switch. It includes data on octets, packets, and discards, which is crucial for monitoring performance and troubleshooting.

- o **Fiber Info**

The **"Fiber Info"** section displays details like signal loss, temperature, RX, and TX power.



Port Info page 3

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



	<b>Grey:</b> Linkdown
	<b>White:</b> shutdown
	<b>Blue:</b> 10Gbps
	<b>Green:</b> 1000 Mbps speed
	<b>Light green:</b> 100 Mbps/10 Mbps speed
	<b>Red:</b> ErrDisable

### Port Info

#### Icons Description:

- **Basic Info:** The edit icon forwards users to the Port Basic Settings page, where they can modify the port settings such as Description, Speed, Duplex Mode, and Flow Control, or enable/disable the port.
- **Neighbor Info:** The details icon forwards users to the LLDP/LLDP-MED Neighbor Info page. Here, users can view additional information about the connected devices, including chassis ID, port ID, device name, system description, and survival time.
- **Fiber Info:** Fiber, it forwards to the Fiber Module page, displaying comprehensive fiber details such as signal loss, temperature, RX, and TX power.
- **Statistics:** The clear icon clears the displayed 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 GWN783x Switch ports, like disabling or enabling the port, adding Description, specifying the speed by default is Auto, Duplex Mode, and Flow Control. There is also a filter on in case you want to edit only the Copper ports which are the Gigabit Ethernet ports or Fiber ports which are the SFP+ ports.

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

Port Basic Settings										
Edit 										
Port	Port Type	Description	Status	Link Status	Speed	Duplex	Jumbo Frame	Flow Con	Operation	
<input checked="" type="checkbox"/>	1/0/1	SFP+	Uplink	Enabled	Up	Auto Detect (10Gbps)	Full (Full)	9216	Disabled	
<input type="checkbox"/>	1/0/2	SFP+	--	Enabled	Down	Auto Detect	Full	9216	Disabled	
<input type="checkbox"/>	1/0/3	SFP+	--	Enabled	Down	Auto Detect	Full	9216	Disabled	
<input type="checkbox"/>	1/0/4	SFP+	--	Enabled	Down	Auto Detect	Full	9216	Disabled	
<input type="checkbox"/>	1/0/5	SFP+	--	Enabled	Down	Auto Detect	Full	9216	Disabled	
<input type="checkbox"/>	1/0/6	SFP+	--	Enabled	Down	Auto Detect	Full	9216	Disabled	
<input type="checkbox"/>	1/0/7	SFP+	--	Enabled	Down	Auto Detect	Full	9216	Disabled	
<input type="checkbox"/>	1/0/8	SFP+	--	Enabled	Down	Auto Detect	Full	9216	Disabled	
<input type="checkbox"/>	1/0/9	SFP+	--	Enabled	Down	Auto Detect	Full	9216	Disabled	
<input type="checkbox"/>	1/0/10	SFP+	--	Enabled	Down	Auto Detect	Full	9216	Disabled	
<input type="checkbox"/>	1/0/11	SFP+	--	Enabled	Down	Auto Detect	Full	9216	Disabled	
<input type="checkbox"/>	1/0/12	SFP+	--	Enabled	Down	Auto Detect	Full	9216	Disabled	

Port Basic Settings

To configure a port, click on **"Edit"** button or icon under operation column as shown above.

*Port Basic Settings – Edit port*

<b>Port</b>	The selected Port to be configured, it can be either Gigabit Ethernet, SFP/SFP+ or Combo port.
<b>Port Type</b>	Displays the Port Type (Copper, SFP/SFP+ and Combo port).
<b>Description</b>	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.
<b>Mode</b>	<p>This option is only available when the selected port is a Combo port.</p> <ul style="list-style-type: none"> <li>● <b>Auto:</b> If set to "Auto", fiber mode will be used when both ports are connected.</li> <li>● <b>Fiber Mode:</b> Fiber will be used.</li> <li>● <b>Ethernet Mode:</b> Ethernet will be used.</li> </ul>
<b>Port Enable</b>	Set whether to enable the interface. <i>it is enabled by default.</i>
<b>Scheduled enabled</b>	From the drop-down list, select the schedule for when the port (including physical and LAG ports) will be enabled.
<b>Speed</b>	<p>Set the rate of the interface:</p> <ul style="list-style-type: none"> <li>● <b>Ethernet port (Copper):</b> the options are {Auto, 10Mbps, 100Mbps, 1000Mbps}, The default is auto-negotiation.</li> <li>● <b>SFP port:</b> the options are (auto, 100Mbps, 1000 Mbps).</li> <li>● <b>SFP+ port:</b> the options are (100Mbps, 1000 Mbps or 10Gbps), only available when Auto Detect is disabled.</li> </ul> <p><b>Note:</b> When set to Auto, the rate of the interface is automatically negotiated between the interface and the peer port .</p>
<b>Auto Detect</b>	toggle ON or OFF Auto Detect, if it's ON the speed and DAC cable will be selected automatically, and if it's OFF the user can select speed and DAC Cable manually. <b>Note:</b> Only available for SFP+ Ports.
<b>DAC Cable</b>	Select from the drop-down list the DAC Cable, the options are (Disable, 0.5m, 1m, 3m, 5m) <b>Note:</b> Only available for SFP+ Ports and when Auto Detect is disabled.
<b>Duplex Mode</b>	Set the duplex mode of the interface. The GE ports options are { auto-negotiation, full-duplex, half-duplex}. <i>The default is auto-negotiation.</i>

	<p><b>Note:</b> Optical ports only support full-duplex mode.</p> <ul style="list-style-type: none"> <li>• <b>Auto-negotiation:</b> The duplex state of an interface is determined by the auto-negotiation between the interface and the peer port.</li> <li>• <b>Duplex:</b> the interface send and receive data packets.</li> <li>• <b>Half-duplex:</b> interface can only send/ receive packets.</li> </ul>
<b>Jumbo Frame</b>	Specify the Jumbo Frame, the valid range is 1518-10000. Default is 9216
<b>Flow Control</b>	<p>Set the flow control on the interface, the options are {Disabled, Enabled, Auto}. <i>The default is Disabled.</i> After enabling it, if the local device is congested, it will send a message to the peer device to notify the peer device to temporarily stop sending packets, after receiving the message, the peer device will temporarily stop sending packets to the local and vice versa. Thus, the occurrence of packet loss is avoided.</p> <p><b>Note:</b> The optical port does not support auto-negotiation mode.</p>

Port Basic Settings – Edit port

## Port Statistics

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

Port	Receive Rate (bps)	InOctets	InPackets	InErrPackets	Transmit Rate (bps)	OutOctets	OutPackets	OutErrPackets	Operation
1/0/1	--	--	--	--	--	--	--	--	🔄 🗑️
1/0/2	0	1906491982	1407667	0	0	88053531	636435	0	🔄 🗑️
1/0/3	--	--	--	--	--	--	--	--	🔄 🗑️
1/0/4	--	--	--	--	--	--	--	--	🔄 🗑️

Port Statistics – part 1

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

Interface	Etherlike	RMON	Private
RX_etherStatsUndersizeDropPktsRT		0	
RX_etherStatsPkts1519toMaxOctetsRT		0	
TX_etherStatsPkts1519toMaxOctetsRT		0	
RX_MacDiscardsRT		0	

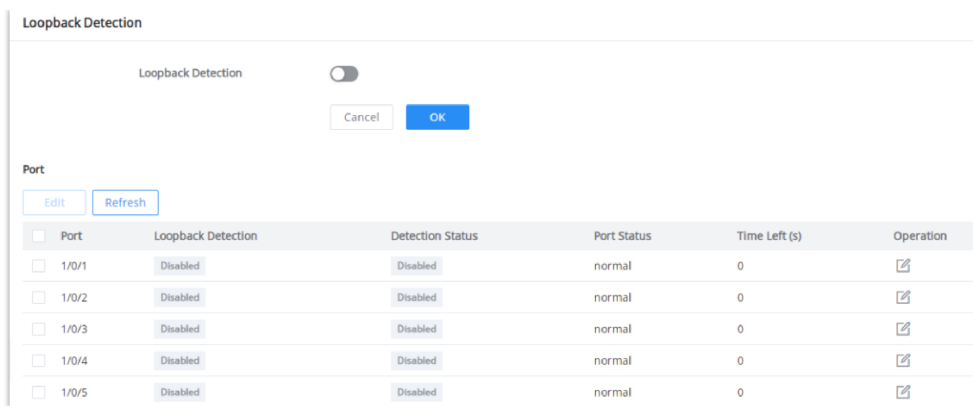
Port Statistics – part 2

## 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

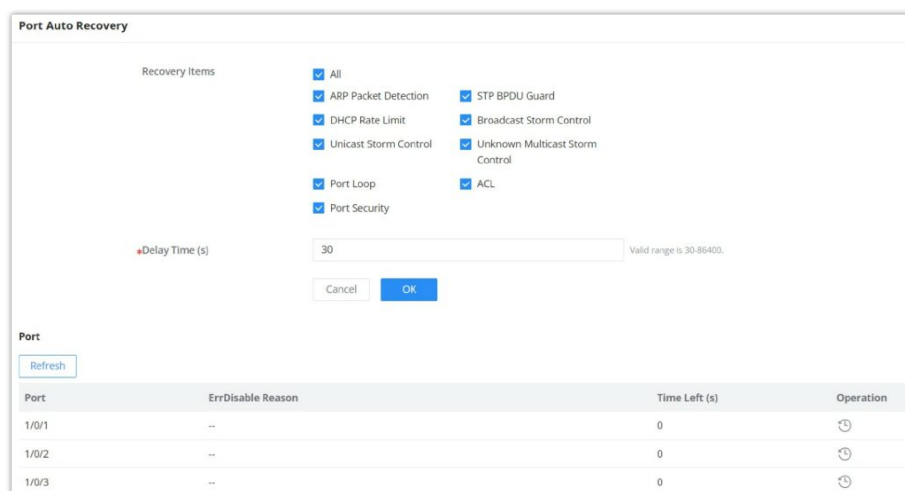
Port Auto Recovery helps recover a port after a specific delay that can be specified by the user. When the following functions of the port trigger the port down, the port automatically returns to the up state after the delay time:

### 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.



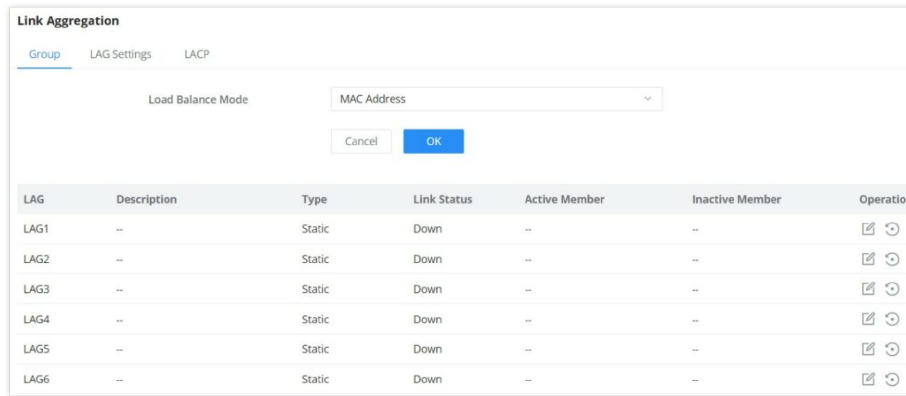
Port Auto Recovery

## 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 GWN783x 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.



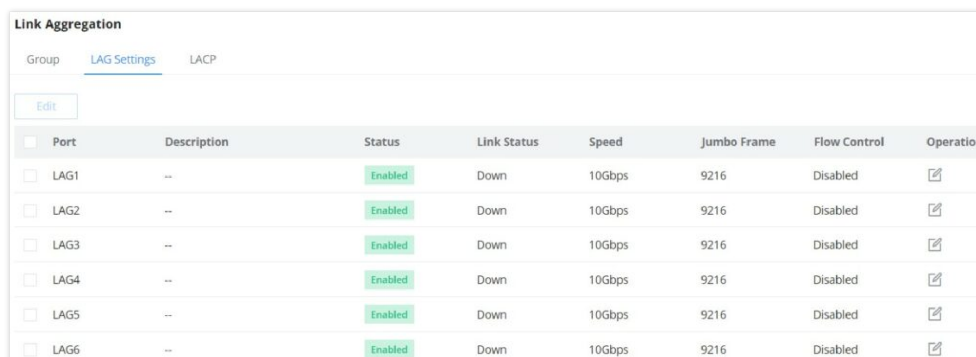
Link Aggregation Group

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

Link Aggregation Group

## 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

Click on "**Edit**" icon under operation column to edit a LAG.

Port Settings > **Edit Port**

Port	LAG1
Description	main link
Port Enable	<input checked="" type="checkbox"/>
Speed	10Gbps
Jumbo Frame	9216
Flow Control	<input checked="" type="radio"/> Disabled <input type="radio"/> Enabled <input type="radio"/> Auto <small>Flow Control setting will not take effect if Duplex Mode is set to "Half".</small>
<input type="button" value="Cancel"/> <input type="button" value="OK"/>	

Edit a LAG

<b>Port</b>	The selected LAG to be configured.
<b>Description</b>	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.
<b>Port Enable</b>	Set whether to enable the interface. <i>it is enabled by default.</i>
<b>Speed</b>	Set the rate of the interface, the options are {Auto, 10Mbps, 100Mbps, 1000Mbps}. <i>The default is auto-negotiation.</i> <b>Note:</b> When set to Auto, the rate of the interface is automatically negotiated between the interface and the peer port .
<b>Jumbo Frame</b>	Specify the jumbo frame, valid range is 1518-10000. Default value is 9216
<b>Flow Control</b>	Set the flow control on the interface, the options are { Disabled, Enabled, Auto}. <i>The default is Disabled</i> After enabling it, if the local device is congested, it will send a message to the peer device to notify the peer device to temporarily stop sending packets, after receiving the message, the peer device will temporarily stop sending packets to the local and vice versa. Thus, the occurrence of packet loss is avoided.

Edit a LAG

## LACP

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

Link Aggregation

Group LAG Settings **LACP**

System Priority:  Valid range is 1-65535

**LACP List**

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

Link Aggregation – LACP

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

## Link Aggregation – LACP

### MAC Address Table

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

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

### Dynamic Address

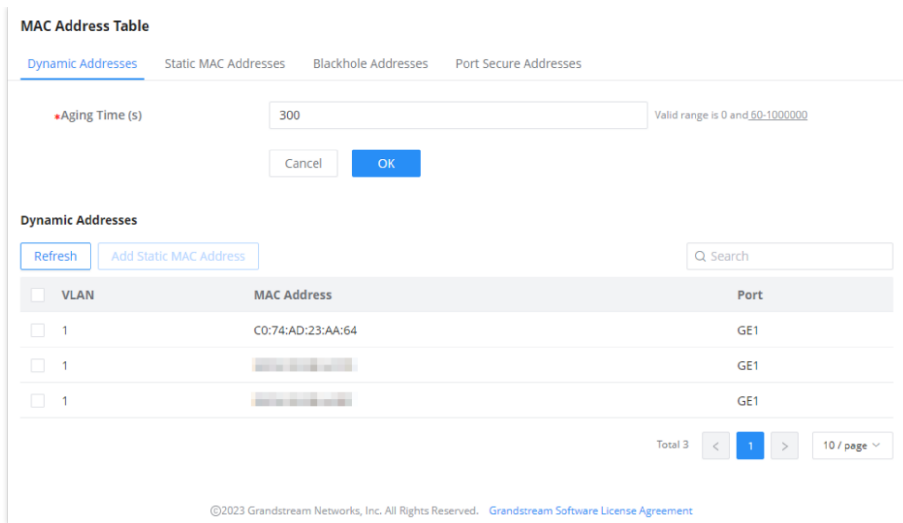
the MAC address table is established based on the automatic learning of the source MAC address in the data frame received by the device. If the MAC address entry does not exist in the MAC address table, the device adds the new MAC address and the interface and VLAN corresponding to the MAC address as a new entry into the MAC address table. GWN783x 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

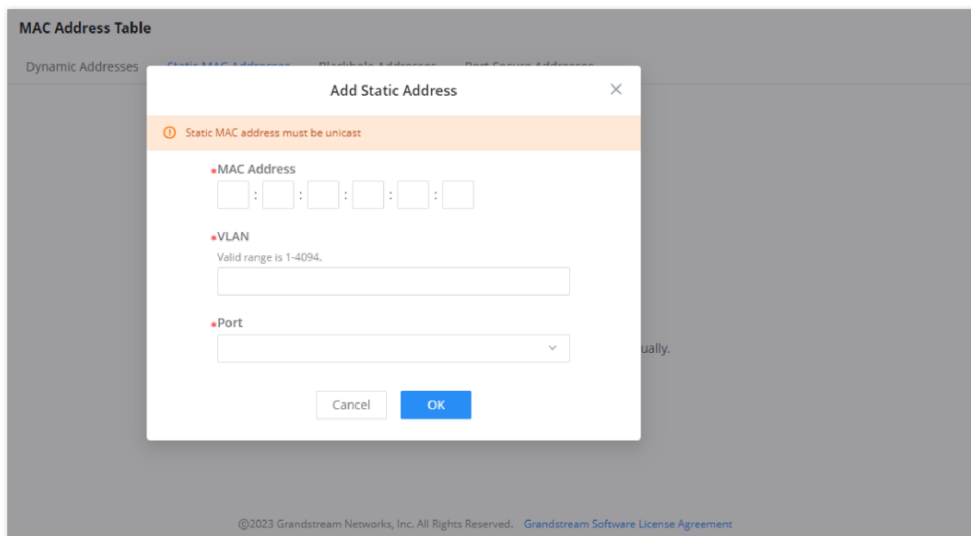
Click on **“Refresh”** button to update the table, or click on **“Add Static MAC Address”** button to add the entry to the static MAC address.

## 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

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

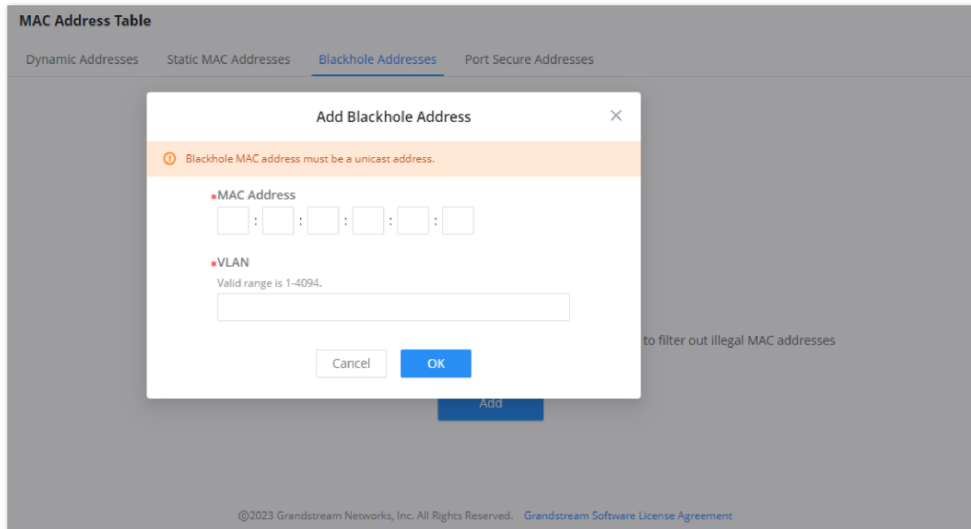
Static MAC Address

## 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*

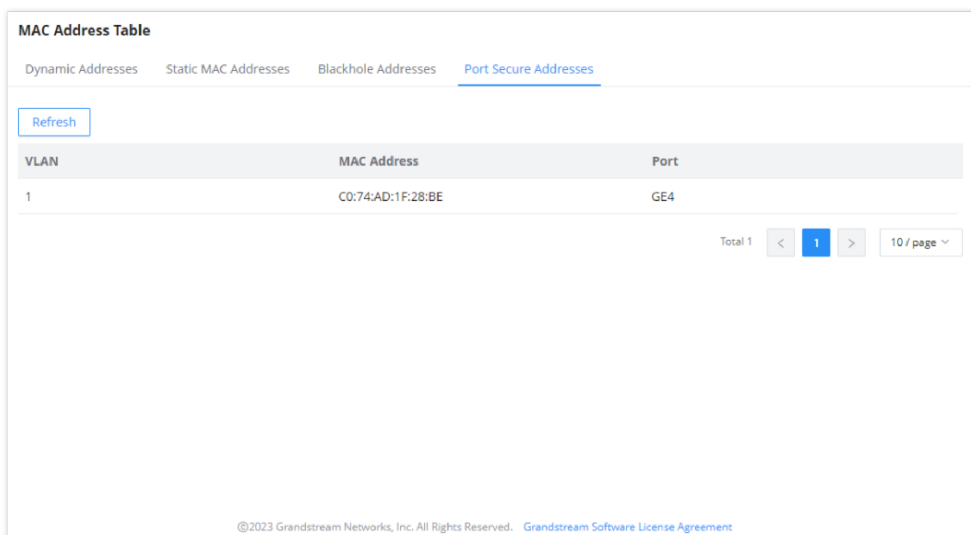
## Port Security Address

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	Description	Tagged Port	Untagged Port	Operation
1	Default	--	1/0/1-1/0/6,1/0/8,1/0/18-1/0/28,LAG2...	
7	Support	1/0/24	1/0/7	
9	Sales	1/0/24	1/0/9-1/0/16	
11	Guests	1/0/24	1/0/17,LAG1,LAG5	

VLAN tab

**Add VLAN**

**\*VLAN IDs**  
Valid range is 2-4094. Example: "5-8, 11" will associate VLANs 5, 6, 7, 8 and 11.

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.

VLAN > **Edit**

VLAN:

Description:  1-64 alphanumeric characters and special characters .@\_

Member Type:

Port  
Click port to change the member type

Tagged
  Untagged

LAG  
Click port to change the member type

Tagged
  Untagged

Edit VLAN

<b>Port</b>	Shows the selected Port.
<b>Link Type</b>	<p>Select the Link Type:</p> <ul style="list-style-type: none"> <li>● <b>Hybrid:</b> Used for connection between switches, or switch and computer.</li> <li>● <b>Access:</b> used to connect the switch and the user terminal.</li> <li>● <b>Trunk:</b> used for interconnecting switches or connecting switches and routers, and can carry data frames of multiple different VLANs.</li> <li>● <b>QinQ:</b> encapsulates the user's private network VLAN tag within the public network (service provider) VLAN tag, allowing the double-layer VLAN tag packets to traverse the operator's backbone (public) network. In the public network, the packets are transmitted according to the outer VLAN tag (i.e., the</li> </ul>

	public network VLAN tag) and the user's private network VLAN tag is shielded, providing the user with a simple L2 VPN tunnel.
<b>PVID</b>	Enter the default VLAN ID.
<b>Accept Frame Type</b>	Select the Frame type (Tag Only, Untag Only or All).
<b>TPID</b>	Select TPID from the drop-down list. <b>Note:</b> TPID (Tag Protocol Identifier) is a 16-bit field in an Ethernet frame header, commonly set to "0x8100" to signal the presence of a VLAN tag, facilitating VLAN segmentation in network traffic.
<b>VLAN Translation</b>	Mutual mapping of different VLANs is achieved by modifying the VLAN Tag carried in packets. Toggle ON/OFF VLAN Translation, then configure the VLAN Mapping below. <b>Notes:</b> Only takes effect for Trunk and Hybrid ports. Configuration restrictions: <ul style="list-style-type: none"> <li>• GWN7800 series switches only support the 1 to 1 function of the outer VLAN (including 1:1 and N:1)</li> <li>• The outer VLAN allows the configuration of a single VLAN and the configuration of a VLAN range. Only one mapped outer VLAN can be configured, and it must be a VLAN that the port has joined.</li> <li>• The total number of VLAN mapping groups supported by the switch is 256, and the maximum number of VLAN mapping groups supported on a single port is 128.</li> <li>• The total number of VLAN ranges supported by the switch is 16, and the maximum VLAN range supported by the configuration on a single port is 16.</li> </ul>
<b>Ingress Filtering</b>	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. <b>Note:</b> Ingress filtering is a method used by enterprises and internet service providers (ISPs) to prevent suspicious traffic from entering a network.
<b>MAC VLAN</b>	Toggle ON/OFF MAC VLAN. <b>Notes:</b> MAC address to VLAN binding can be added in the MAC VLAN tab. Only effective for Hybrid port.
<b>Protocol Template</b>	Select the Protocol Template from the drop-down list and the VLAN associated to it, then the specify the priority (802.1p) the range 0-7. VLANs are divided according to the protocol type (family) and encapsulation format to which the data frame belongs. Based on 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. <b>Notes:</b> Protocol VLAN must be added first under Protocol VLAN tab. This only takes effect for Hybrid ports.

Edit VLAN

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

<b>Port</b>	Shows the selected Port.
-------------	--------------------------

<b>Link Type</b>	<p>Select the Link Type:</p> <ul style="list-style-type: none"> <li>● <b>Hybrid:</b> Used for connection between switches, or switch and computer.</li> <li>● <b>Access:</b> used to connect the switch and the user terminal.</li> <li>● <b>Trunk:</b> used for interconnecting switches or connecting switches and routers, and can carry data frames of multiple different VLANs.</li> <li>● <b>QinQ:</b> encapsulates the user's private network VLAN tag within the public network (service provider) VLAN tag, allowing the double-layer VLAN tag packets to traverse the operator's backbone (public) network. In the public network, the packets are transmitted according to the outer VLAN tag (i.e., the public network VLAN tag) and the user's private network VLAN tag is shielded, providing the user with a simple L2 VPN tunnel.</li> </ul>
<b>PVID</b>	Enter the default VLAN ID.
<b>Accept Frame Type</b>	Select the Frame type (Tag Only, Untag Only or All).
<b>TPID</b>	<p>Select TPID from the drop-down list.</p> <p><b>Note:</b> TPID (Tag Protocol Identifier) is a 16-bit field in an Ethernet frame header, commonly set to "0x8100" to signal the presence of a VLAN tag, facilitating VLAN segmentation in network traffic.</p>
<b>VLAN Translation</b>	<p>Mutual mapping of different VLANs is achieved by modifying the VLAN Tag carried in packets. Toggle ON/OFF VLAN Translation, then configure the VLAN Mapping below.</p> <p><b>Notes:</b> Only takes effect for Trunk and Hybrid ports.</p> <p>Configuration restrictions:</p> <ul style="list-style-type: none"> <li>● GWN7800 series switches only support the 1 to 1 function of the outer VLAN (including 1:1 and N:1)</li> <li>● The outer VLAN allows the configuration of a single VLAN and the configuration of a VLAN range. Only one mapped outer VLAN can be configured, and it must be a VLAN that the port has joined.</li> <li>● The total number of VLAN mapping groups supported by the switch is 256, and the maximum number of VLAN mapping groups supported on a single port is 128.</li> <li>● The total number of VLAN ranges supported by the switch is 16, and the maximum VLAN range supported by the configuration on a single port is 16.</li> </ul>
<b>Ingress Filtering</b>	<p>Set whether to enable the inbound filtering function of the interface.</p> <p>Ingress Filtering is only available for Hybrid port, and it's enabled by default.</p> <p><b>Note:</b> Ingress filtering is a method used by enterprises and internet service providers (ISPs) to prevent suspicious traffic from entering a network.</p>
<b>MAC VLAN</b>	<p>Toggle ON/OFF MAC VLAN.</p> <p><b>Notes:</b> MAC address to VLAN binding can be added in the MAC VLAN tab. Only effective for Hybrid port.</p>
<b>Protocol Template</b>	<p>Select the Protocol Template from the drop-down list and the VLAN associated to it, then the specify the priority (802.1p) the range 0-7.</p> <p>VLANs are divided according to the protocol type (family) and encapsulation format to which the data frame belongs. Based on 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.</p> <p><b>Notes:</b> Protocol VLAN must be added first under Protocol VLAN tab. This only takes effect for Hybrid ports.</p>

#### 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.

Port Settings > **Edit**

Port: 1/0/1

Link Type: Trunk

PVID:  Valid range is 1-4094

Accept Frame Type: Trunk

TPID: 0x8100

VLAN Translation:

Cancel OK

VLAN Port Settings – Link types

Port Settings > **Edit**

Port: 1/0/2

Link Type: Trunk

PVID: 1 Valid range is 1-4094

Accept Frame Type:  All  Tag Only  Untag Only

TPID: 0x8100

VLAN Translation:

Ingress:

**VLAN Mapping1**

Outer VLAN:

VLAN after Outer Mapping:

Add +

Cancel OK

VLAN Port Settings – VLAN Translation

Port Settings > **Edit**

Port: 1/0/2

Link Type: Hybrid

PVID: 1 Valid range is 1-4094

Accept Frame Type:  All  Tag Only  Untag Only

TPID: 0x8100

Ingress Filtering:

VLAN Translation:

MAC VLAN:

Protocol VLAN:

**Protocol Template**

Protocol Template:  VLAN:  802.1p:

Add +

Cancel OK

VLAN Port Settings – Protocol Template

<b>Port</b>	Shows the selected Port.
<b>Link Type</b>	<p>Select the Link Type:</p> <ul style="list-style-type: none"> <li>● <b>Hybrid</b>: Used for connection between switches, or switch and computer.</li> <li>● <b>Access</b>: used to connect the switch and the user terminal.</li> <li>● <b>Trunk</b>: used for interconnecting switches or connecting switches and routers, and can carry data frames of multiple different VLANs.</li> <li>● <b>QinQ</b>: encapsulates the user's private network VLAN tag within the public network (service provider) VLAN tag, allowing the double-layer VLAN tag packets to traverse the operator's backbone (public) network. In the public network, the packets are transmitted according to the outer VLAN tag (i.e., the</li> </ul>

	public network VLAN tag) and the user's private network VLAN tag is shielded, providing the user with a simple L2 VPN tunnel.
<b>PVID</b>	Enter the default VLAN ID.
<b>Accept Frame Type</b>	Select the Frame type (Tag Only, Untag Only or All).
<b>TPID</b>	Select TPID from the drop-down list. <b>Note:</b> <i>TPID (Tag Protocol Identifier) is a 16-bit field in an Ethernet frame header, commonly set to "0x8100" to signal the presence of a VLAN tag, facilitating VLAN segmentation in network traffic.</i>
<b>VLAN Translation</b>	Mutual mapping of different VLANs is achieved by modifying the VLAN Tag carried in packets. Toggle ON/OFF VLAN Translation, then configure the VLAN Mapping below. <b>Notes:</b> Only takes effect for Trunk and Hybrid ports. Configuration restrictions: <ul style="list-style-type: none"> <li>• GWN7800 series switches only support the 1 to 1 function of the outer VLAN (including 1:1 and N:1)</li> <li>• The outer VLAN allows the configuration of a single VLAN and the configuration of a VLAN range. Only one mapped outer VLAN can be configured, and it must be a VLAN that the port has joined.</li> <li>• The total number of VLAN mapping groups supported by the switch is 256, and the maximum number of VLAN mapping groups supported on a single port is 128.</li> <li>• The total number of VLAN ranges supported by the switch is 16, and the maximum VLAN range supported by the configuration on a single port is 16.</li> </ul>
<b>Ingress Filtering</b>	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. <b>Note:</b> <i>Ingress filtering is a method used by enterprises and internet service providers (ISPs) to prevent suspicious traffic from entering a network.</i>
<b>MAC VLAN</b>	Toggle ON/OFF MAC VLAN. <b>Notes:</b> <i>MAC address to VLAN binding can be added in the MAC VLAN tab. Only effective for Hybrid port.</i>
<b>Protocol Template</b>	Select the Protocol Template from the drop-down list and the VLAN associated to it, then the specify the priority (802.1p) the range 0-7. VLANs are divided according to the protocol type (family) and encapsulation format to which the data frame belongs. Based on 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. <b>Notes:</b> <i>Protocol VLAN must be added first under Protocol VLAN tab. This only takes effect for Hybrid ports.</i>

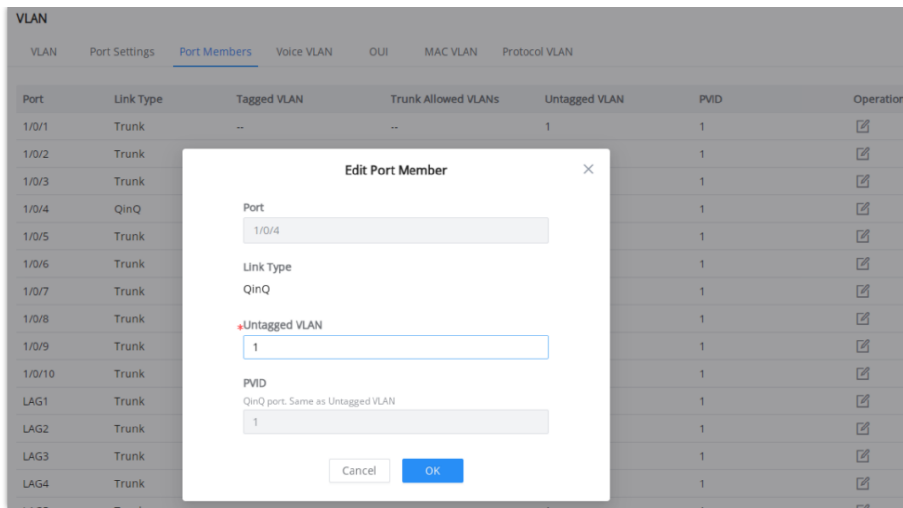
#### VLAN Port Settings

### VLAN Port Members

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

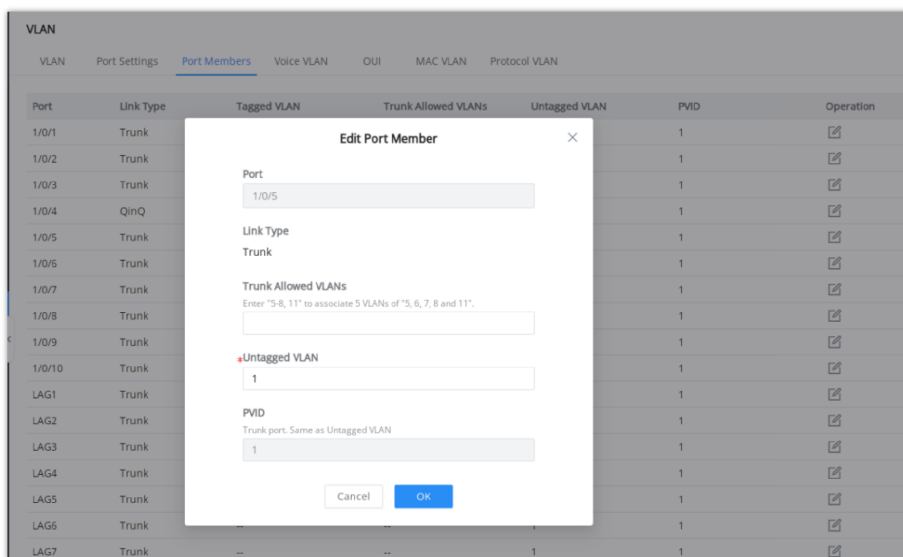
**Note**

**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

Port	Link Type	Tagged VLAN	Trunk Allowed VLANs	Untagged VLAN	PVID	Operation
1/0/1	Trunk	--	--	1	1	[Edit]
1/0/2	Trunk	2-16	2-298	1	1	[Edit]
1/0/3	Trunk	--	--	1	1	[Edit]
1/0/4	QinQ	--	--	1	1	[Edit]
1/0/5	Trunk	--	--	1	1	[Edit]

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.

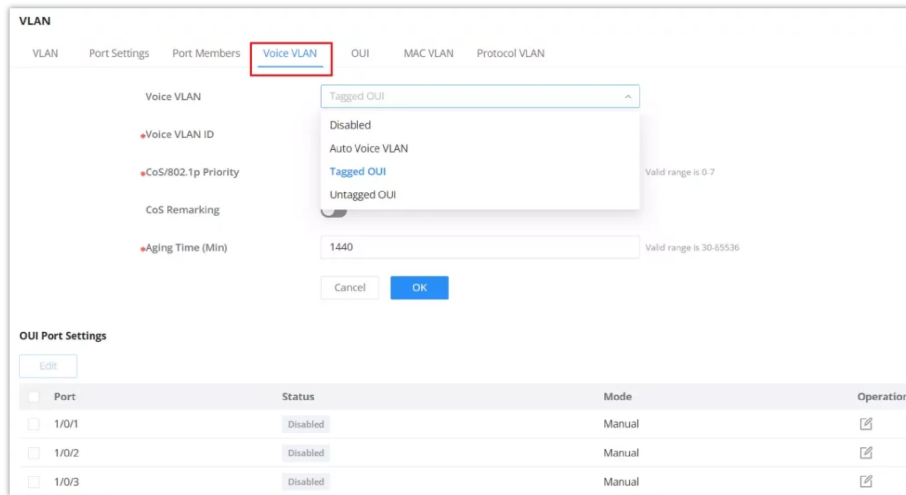
For example, when an IP phone is connected to a GWN78xx switch port, the switch prioritizes traffic in the voice VLAN, ensuring that voice packets are forwarded before other types of packets.

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

<b>Voice VLAN</b>	<p>Select from the drop-down list the Voice VLAN method:</p> <ul style="list-style-type: none"> <li>● Disabled</li> <li>● Auto Voice VLAN</li> <li>● Tagged OUI</li> <li>● Untagged OUI</li> </ul> <p><i>By default is disabled.</i></p>
<b>Voice VLAN ID</b>	<p>Select a VLAN as the voice VLAN from the VLAN list.  <b>Note:</b> <i>The default VLAN 1 cannot be used as a voice VLAN.</i></p>
<b>CoS/802.1p Priority</b>	<p>Specify the CoS/802.1p Priority, Valid range is 0-7.</p>
<b>If Auto Voice VLAN is selected</b>	
<b>DSCP</b>	<p>Specify the DSCP priority, an integer ranging from 0 to 63.</p>
<b>If Tagged or Untagged OUI is selected</b>	
<b>CoS</b>	<p>Set whether to enable CoS Remarking.</p>
<b>Aging Time</b>	<p>Set the aging time of the voice VLAN.  <i>The value range is an integer from 30 to 65536 , and the default is 1440 minutes .</i></p>
<b>Edit Port Settings</b>	<p><b>Port:</b> Displays the selected port.  <b>Status:</b> Set whether to enable the voice VLAN function of the port.  <i>it is disabled by default.</i>  <b>Mode:</b> Set the working mode of the voice VLAN on the port.</p>



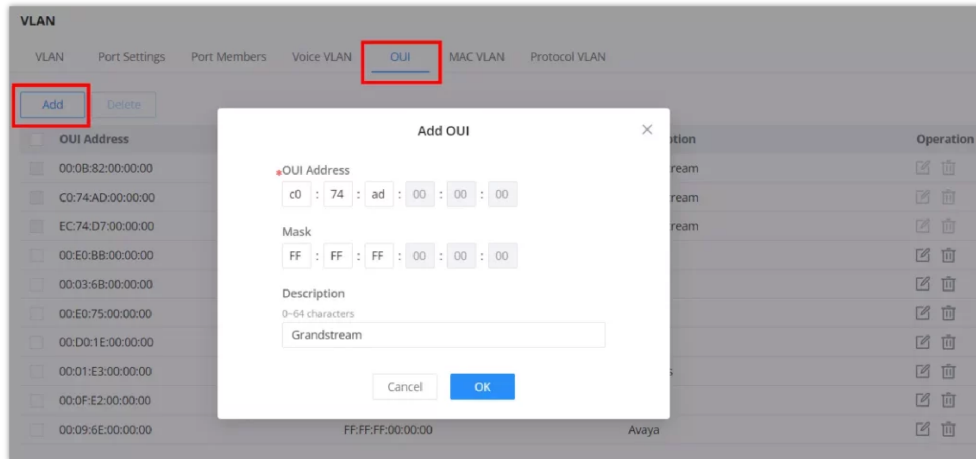
The default is manual.

**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

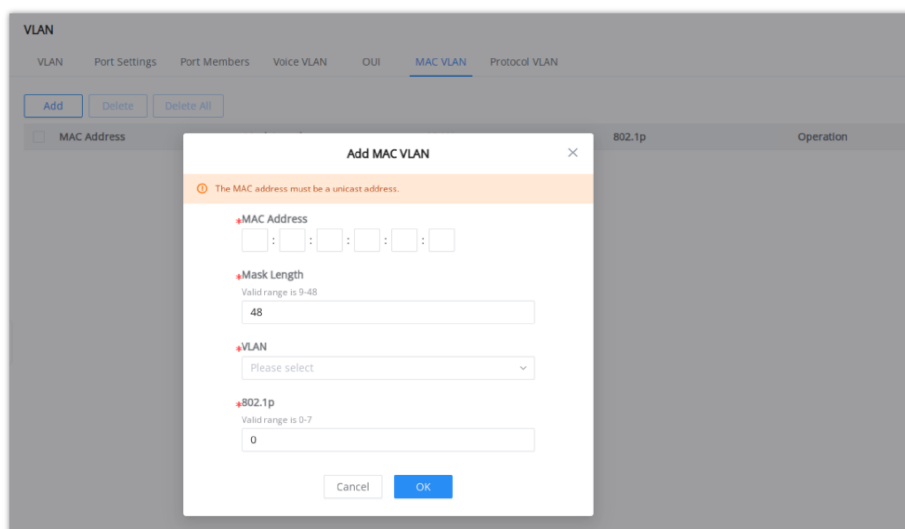
MAC VLAN is a networking technique where each VLAN is based on the source MAC address of incoming frames. Devices with the same MAC address share a VLAN. This segmentation enables isolated communication between devices within the same VLAN based on MAC addresses.

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.



## 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.

The screenshot shows the 'VLAN' configuration page with the 'Protocol VLAN' tab selected. The main interface has a table with columns for 'Protocol Index', 'Frame Type', 'Protocol Type Value', and 'Operation'. An 'Add Protocol VLAN' dialog box is open, containing the following fields:

- Protocol Index:** A text input field with the value '0'.
- Frame Type:** A dropdown menu with 'Ethernet II' selected.
- Protocol Type Value:** A text input field with a red error icon and the text 'Valid range: 0x000-0xFFFF'.

At the bottom of the dialog are 'Cancel' and 'OK' buttons.

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

<b>Spanning Tree</b>	Set whether to enable Spanning Tree.
<b>Mode</b>	Set the operating mode of Spanning Tree (STP). <ul style="list-style-type: none"> <li>● <b>STP</b>: Enable the Spanning Tree (STP) operation.</li> <li>● <b>RSTP</b>: Enable the Rapid Spanning Tree (RSTP) operation.</li> <li>● <b>MSTP</b>: Enable the Multiple Spanning Tree Protocol (MSTP) operation.</li> </ul>
<b>Path Cost</b>	Specify the path cost method (Short, Long). <i>Default is Short.</i>
<b>Bridge Priority</b>	Select the Bridge Priority, In an STP network, the device with the smallest bridge ID is elected as the root bridge. <i>Default is 32768.</i> <b>Note:</b> <i>The valid range is 0~61440, which must be a multiple of 4096</i>
<b>Max Hops</b>	Select the Max Hops (the range is 1 - 40). <i>Default is 20</i>
<b>Hello Time (s)</b>	Specify the Hello Time in seconds (the range is 1 -10). <i>Default is 2.</i> <b>Note:</b> <i>The time interval at which the device running the STP protocol sends the configuration message BPDU , which is used by the device to detect whether the link is faulty.</i>
<b>Max Aging Time (s)</b>	Select The aging time of BPDU packets of the port (the range is 6 - 40). <i>Default is 20.</i>
<b>Forward Delay Time (s)</b>	Specify the Forward Delay Time in seconds (the range is 4 -30). <i>Default is 15.</i>

### STP Global Settings

## STP Port Settings

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

**Spanning Tree**

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

[Edit](#)

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

Spanning Tree – Port Settings

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

Port Settings > **Edit Port**

Port: GE1

Enable STP:

\*Priority: 128

\*Path Cost: 0

Edge Port:  Auto  Enabled  Disabled

BPDU Guard:

BPDU Filter:

Point-to-Point:  Auto  Enabled  Disabled

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

Spanning Tree – Edit Port Settings

<b>Port</b>	Displays the selected GE/LAG Port.
<b>Enable STP</b>	Set whether to enable STP on this port.
<b>Priority</b>	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 . <b>Note:</b> The valid range is 0~240, which must be a multiple of 16
<b>Path Cost</b>	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. <b>Note:</b> The valid range is 0~200000000. 0 is equal to auto
<b>Edge Port</b>	Set whether to enable Edge Port or disable it, by default it's on auto. <b>Notes:</b>

	<ul style="list-style-type: none"> <li>• 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.</li> <li>• 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.</li> </ul>
<b>BPDU Guard</b>	Set whether to enable BPDU Guard. <b>Note:</b> BPDU Guard further protects your switch by turning this port into error state and shutdown if any BPDU received from this port.
<b>BPDU Filter</b>	Set whether to enable BPDU Filter. <b>Note:</b> Drop all BPDU packets and no BPDU will be sent.
<b>Point-to-Point</b>	Select Point-to-Point option (Auto, Enabled or Disabled). <i>Default is Auto.</i> <b>Note:</b> 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. GWN783x Switch supports up to 16 independent MST instances (0~15) where each instance can be associated with many VLANs.

**Spanning Tree**

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

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

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

Cancel OK

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

### Multiple Spanning Tree Instance

MST Instance > **Edit MST Instance**

MSTI: 0

VLAN: 1-4094

\*Priority: 32768

Cancel OK

Bridge Identifier	32768-C0:74:AD:C6:0D:DA
Designated Root Bridge	32767-C0:74:AD:B9:F1:9C
Root Port	GE8
Root Path Cost	4
Remaining Hop	20

### MST – Edit Port

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

**Spanning Tree**

Global Settings Port Settings MST Instance MST Port Settings

MSTI

**Port Settings**

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

MST Port Settings

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

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

MSTI

Port

\*Path Cost

\*Priority

Port Role	Disabled Port
Port Status	Disabled
Mode	MSTP
Type	Internal
Designated Bridge ID	0-00:00:00:00:00:00
Designated Port ID	0-0
Designated Path Cost	0
Remaining Hop	20

MST Port Settings – Edit port

## IP

### VLAN IP Interface

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

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

### IPv4/IPv6 Interface

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

**MGMT VLAN (Management VLAN):** as the name suggests it's the VLAN used to manage the switch, for example when using remote location with protocols like telnet, SSH, syslog etc. the default MGMT VLAN is VLAN 1 and the user have to choice to change it by selecting another VLAN from the drop-down list, and the Management VLAN is selected, IPv4 or IPv6 Default Gateway address can be specified (e.g. 192.168.80.1).

**VLAN IP Interface**

IPv4 Interface | IPv6 Interface | IPv6 Router Advertisements

MGMT VLAN: VLAN 1

IPv4 Default Gateway: 192.168.80.1

Cancel OK

VLAN IP Interface – MGMT VLAN

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

**VLAN IP Interface**

IPv4 Interface | IPv6 Interface | IPv6 Router Advertisements

MGMT VLAN: VLAN 1

IPv4 Default Gateway: 192.168.80.1

Cancel OK

**Interface Settings**

Add Delete

All All Types Q VLAN/IP Address

IPv4 Interface	Status	Type	IPv4 Address	MTU	Operation
Loopback1	UP	Static	--	1500	✍️ 🗑️ 🔄
* VLAN 1	UP	Dynamic	192.168.80.211/24	1500	✍️ 🗑️ 🔄
VLAN 7	UP	Static	70.0.0.1/24	1500	✍️ 🗑️ 🔄
VLAN 9	UP	Dynamic	90.0.0.25/24	1500	✍️ 🗑️ 🔄

VLAN IP Interface – add VLAN IP Interface

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.

**Confirm to get IP address again?**

Once successfully obtained, the IP address may be changed

Cancel OK

Refresh IP address

Address Type:

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

**Edit IPv4 Interface**

VLAN: VLAN 1

IPv4 Address Type:  Static IP  DHCP

\*Gateway Priority: Valid range is 2-255  
2

\*MTU: Valid range is 1280-9216  
1500

Cancel OK

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.



**VLAN IP Interface**

IPv4 Interface   IPv6 Interface   IPv6 Router Advertisements

IPv6 Interface	Interface Enable	Route Information	Timeout (s)	Lifetime (s)	Flag	Number	Operation
* VLAN 1	Disabled	Disabled	600	1800	--	0	
VLAN 7	Disabled	Disabled	600	1800	--	0	
VLAN 9	Disabled	Disabled	600	1800	--	0	

*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.

IPv6 Router Advertisements   **Edit IPv6 Router Advertisements**

VLAN:

Interface Enable:

Route Information:

Timeout (s):  Valid range is 1-1800

Lifetime (s):  Valid range is 0-9000

Flag:  M Flag  O Flag

Default Route Priority:

**IPv6 Address/Prefix1**

IPv6 Address/Prefix:  /  Prefix range 1-128

Valid Lifetime (s):  Valid range is 0-4294967295

Preferred Lifetime (s):  Valid range is 0-4294967295

Flag:  A Flag  L Flag  R Flag

*Edit IPv6 Router Advertisement*

## 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 Server**

DHCP Server   Address Table

DHCP Service:

**Address Pool Settings**

All

Address Pool Name	Type	VLAN IPv4 Interface	Address Pool	Used	Remained	Operation
Guest network	Interface	VLAN 9	90.0.0.2-90.0.0.254	0	253	 
7	Interface	VLAN 7	70.0.0.7-70.0.0.77	1	70	 

*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 Server > Add Address Pool

Address Pool Name: Network\_7\_pool (1-64 characters)

Type: Interface

Interface: VLAN 7

IPv4 Pool: 70.0.0.2 - 70.0.0.254

Duration (min): 120 (Valid range is 1-11520)

DNS Server: 1.1.1.1 (Add +)

WINS Server: (Add +)

Netbios Node Type: (dropdown)

**DHCP Option1**

DHCP Option: (empty) (The range is 2-254 (excluding 50-54, 56, 58, 59, 61 and 82))

Type: Hex

Option Content: (empty) (0-256 characters, and must be even)

(Add +)

(Cancel) (OK)

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:

Duration (min): 120 (Valid range is 1-2880)

DNS Server: (empty) (Add +)

WINS Server: (empty) (Add +)

Netbios Node Type: (dropdown)

**DHCP Option1**

DHCP Option: 43 (The range is 2-254 (excluding 50-54, 56, 58, 59, 61 and 82))

Type: ASCII

Service: Custom

Option Content: (empty) (0-255 characters)

(Add +)

(Cancel) (OK)

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 Server

DHCP Server [Address Table](#)

(Add) (Refresh) (Add as Static Binding IP) (Delete)

Q IPv4 Address/Client Name/C...

Client Name (MAC Address)	IPv4 Address	Type	Remaining Lease (s)	Operation
<input checked="" type="checkbox"/> C0:74:AD:93:0C:F8	70.0.0.32	Dynamic	6926	(refresh icon)

Total 1 < 1 > 10 / page

DHCP – DHCP Server

## DHCP Relay

DHCP relay on GWN783x 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

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

DHCP Relay

## ARP Table

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

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

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

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

**ARP Table**

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

**ARP Table**

All

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

ARP Table

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

**ARP Table**

All

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

ARP Table – Operation

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

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

**Add Static ARP**

The MAC address must be an unicast one.

\*VLAN

\*IP Address  
IPv4 format

\*MAC Address  :  :  :  :  :

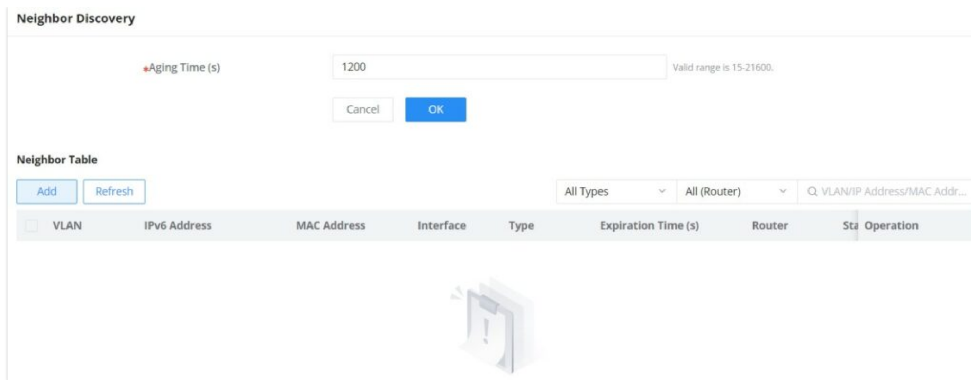
Add Static ARP

## Neighbor Discovery

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

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

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



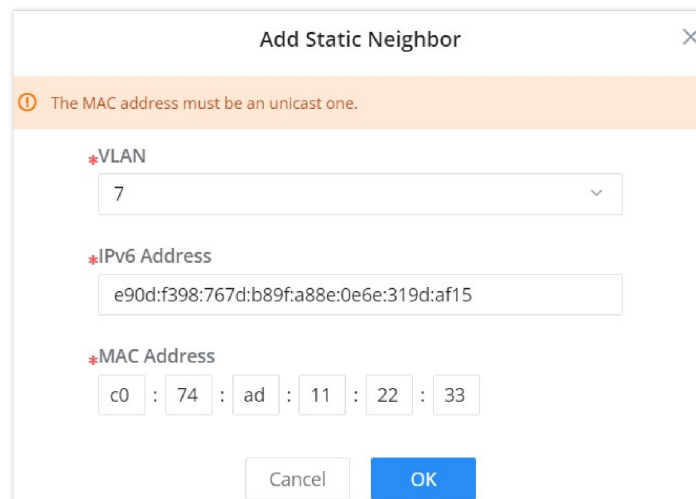
Neighbor Discovery

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

**Note:**

Aging time applies only to dynamic entries.

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



Add Static Neighbor

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

## DNS

Domain Name System DNS provides translation services between domain names and IP addresses. GWN783x 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 GWN783x 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 Suffix or DNS Server click on “+” icon and to delete click on “-” icon.

**Note:**

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

## Domain Mapping Table

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

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

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

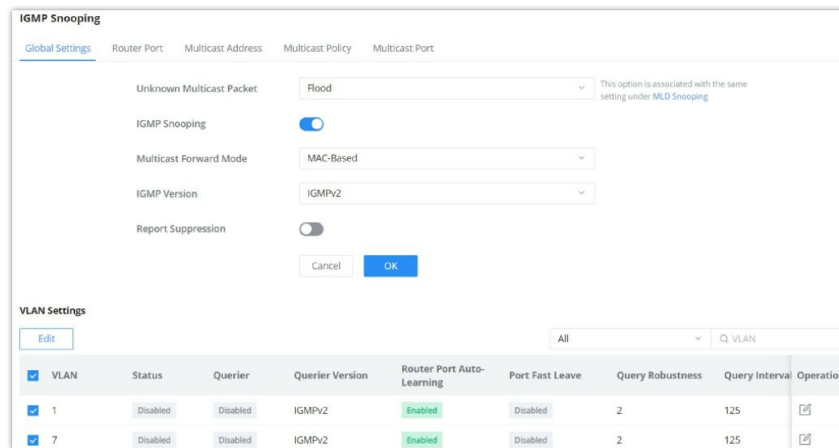
As an IPv4 Layer 2 multicast protocol, IGMP snooping is the process of listening to Internet Group Management Protocol (IGMP) network traffic. The feature allows a network switch to listen in on the IGMP conversation between hosts and routers. By listening to these conversations the switch maintains 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

<b>Unknown Multicast Packet</b>	<p>Select an action for switch to handle with unknown multicast packet.</p> <ul style="list-style-type: none"> <li>● <b>Drop:</b> Drop the unknown multicast data.</li> <li>● <b>Flood:</b> Flood the unknown multicast data.</li> <li>● <b>Forward to Router port:</b> Forward the unknown multicast data to router port.</li> </ul> <p><i>Note: This option is associated with the same one IGMP Snooping.</i></p>
<b>MLD Snooping</b>	Enable or disable Global MLD Snooping
<b>Multicast Forward Mode</b>	<p>Set the Multicast Forward Mode.</p> <ul style="list-style-type: none"> <li>● <b>MAC-Based:</b> Forward using MAC address.</li> <li>● <b>IP-Based:</b> Forward using IP address</li> </ul>
<b>MLD Version</b>	Select the MLD Version.

<b>Report Suppression</b>	Enable or disable the switch to handle MLD reports between router and host, suppressing bandwidth used by MLD.
---------------------------	--

*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*

<b>VLAN</b>	Displays the selected VLAN
<b>IGMP Snooping</b>	Click on the toggle button to enable IGMP Snooping for the selected VLAN.
<b>Router Port Auto-Learning</b>	Click on the toggle button to learn router port by IGMP query.
<b>Port Fast Leave</b>	Select Enable/Disable Fast Leave feature for the desired port. <b>Note:</b> If Fast Leave is enabled for a port, the switch will immediately remove this port from the multicast group upon receiving IGMP leave messages.
<b>Query Robustness</b>	Set a number which allows tuning for the expected packet loss on a subnet. <i>The valid range is 1-7</i>
<b>Query Interval (s)</b>	Set the interval of querier send general query.
<b>Query Max Response Interval (s)</b>	It specifies the maximum allowed time before sending a responding report. <b>Note:</b> The valid range is 5-20 in seconds.
<b>Last Member Query Count</b>	After querying 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). <b>Note:</b> The valid range is 1-7
<b>Last Member Query Interval (s)</b>	The maximum time interval between counting each member query message with no responses from any subscribed member. <b>Note:</b> 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.

VLAN	Static Router Port	Forbidden Port	Dynamic Port	Aging Time (s)	Operation
7	GE8	GE1		0	

IGMP Snooping Router Port

Router Port > Edit

VLAN: 8

Static Router Port  
Click on port to select/unselect

GE: 1, 2, 3, 4, 5, 6, 7, 8

LAG: 1, 2, 3, 4, 5, 6, 7, 8

Forbidden Port  
Click on port to select/unselect

GE: 1, 2, 3, 4, 5, 6, 7, 8

Buttons: Cancel, OK

IGMP Snooping Router Port – add or edit

### IGMP Snooping Multicast Address

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

VLAN	Multicast Address	Source IP Address	Member Port	Address Type	Aging Time (s)	Operation
No Data						

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.

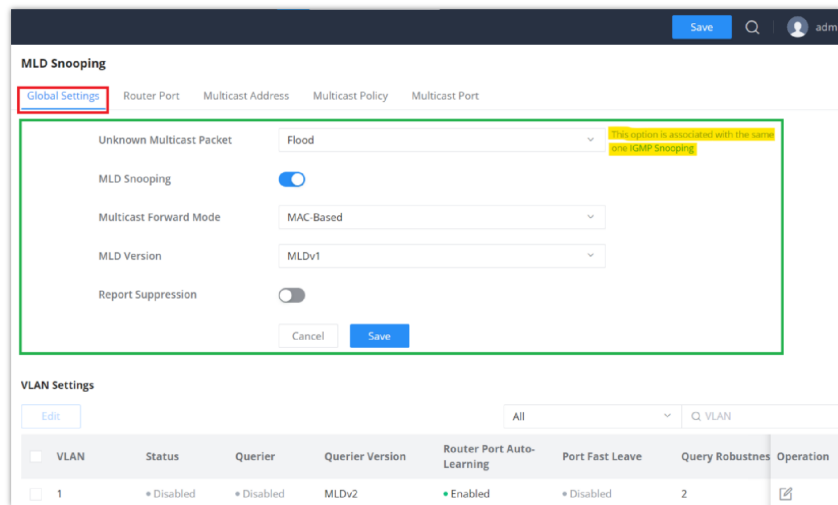
*IGMP Snooping Multicast Port*

### 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

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

MLD Snooping Global Settings

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

Global Settings > **Edit**

VLAN: 1

MLD Snooping:

MLD Snooping Querier:

MLD Snooping Querier Version: MLDv2

Router Port Auto-Learning:

Port Fast Leave:

Query Robustness: 2 (The range is 1-7)

Query Interval (s): 125 (The range is 30-18000)

Query Max Response Interval (s): 10 (The range is 5-20)

Last Member Query Count: 2 (The range is 1-7)

Last Member Query Interval (s): 1 (The range is 1-25)

Cancel Save

MLD Snooping – Edit VLAN

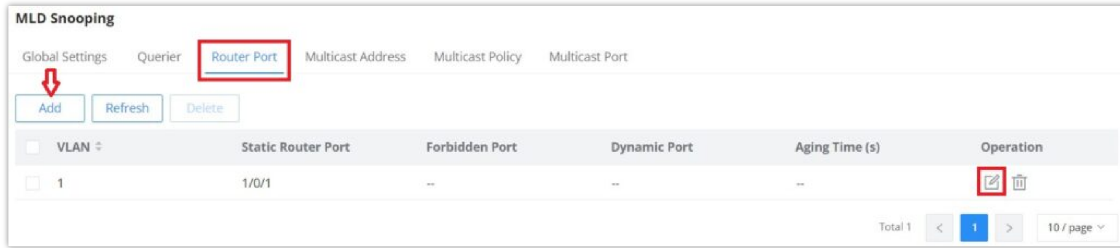
<b>VLAN</b>	Displays the selected VLAN
<b>MLD Snooping</b>	Click on the toggle button to enable MLD Snooping for the selected VLAN.
<b>MLD Snooping Querier</b>	Click the toggle button to enable the MLD Snooping Querier.
<b>MLD Snooping Querier Version</b>	Select from the drop-down list the MLD Snooping Querier Version.
<b>Router Port Auto-Learning</b>	Click on the toggle button to learn router port by MLD query.
<b>Port Fast Leave</b>	Select Enable/Disable Fast Leave feature for the desired port. <b>Note:</b> If Fast Leave is enabled for a port, the switch will immediately remove this port from the multicast group upon receiving MLD leave messages.
<b>Query Robustness</b>	Set a number which allows tuning for the expected packet loss on a subnet. <i>The valid range is 1-7</i>
<b>Query Interval (s)</b>	Set the interval of querier send general query.
<b>Query Max Response Interval (s)</b>	It specifies the maximum allowed time before sending a responding report. <b>Note:</b> The valid range is 5-20 in seconds.
<b>Last Member Query Count</b>	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). <b>Note:</b> The valid range is 1-7
<b>Last Member Query Interval (s)</b>	Set The maximum time interval between counting each member query message with no responses from any subscribed member. <b>Note:</b> The valid range is 1-25 in seconds

MLD Snooping – Edit VLAN

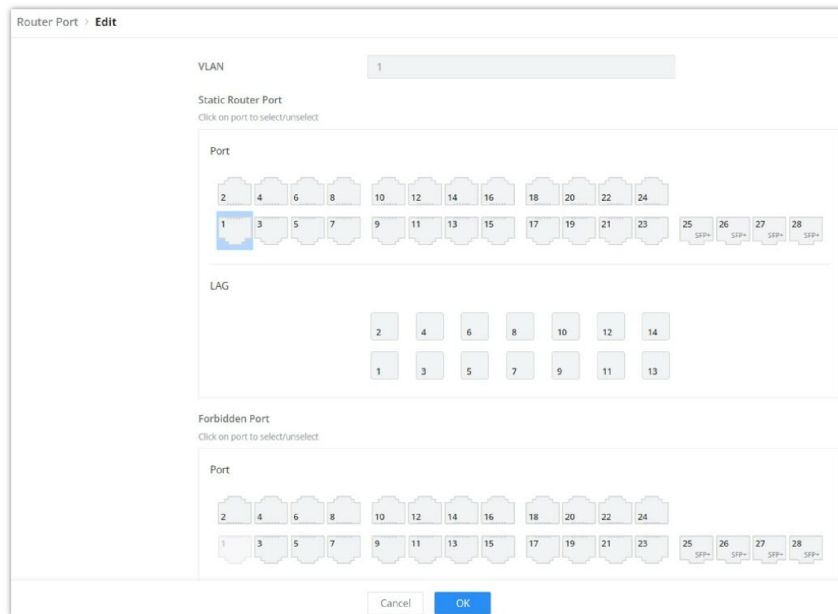
## MLD Snooping Router Port

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.



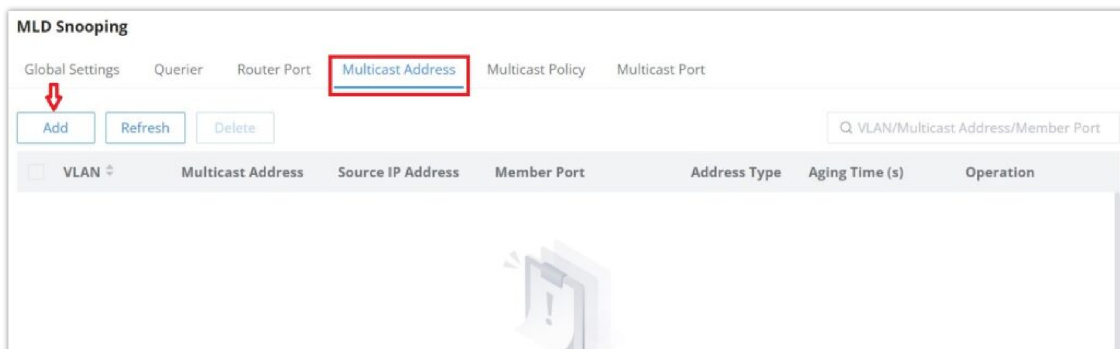
MLD Snooping Router Port page



Add MLD Snooping Router Port

## MLD Snooping Multicast Address

GWN783x Switches do also support adding static multicast addresses by specifying the VLAN and member port.



MLD Snooping Multicast Address page

Multicast Address > Edit

VLAN

Multicast Address  IPv6 format

Click on port to select/unselect

Port

1 SFP+ 2 SFP+ 3 SFP+ 4 SFP+ 5 SFP+ 6 SFP+ 7 SFP+ 8 SFP+ 9 SFP+ 10 SFP+ 11 SFP+ 12 SFP+

LAG

1 2 3 4 5 6

Cancel OK

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

Global Settings Querier Router Port Multicast Address Multicast Policy Multicast Port

Add Delete

Policy ID

1

Address Operation

52e:3aca:d24b:5603:7762:1380 - 0af:9449:7a70:ba96:24de:69e4

Total 1 < 1 > 10 / page

Edit

Multicast Policy ID

2

Action

Allow

Multicast Address

IPv6 format

ff12:3e3c:652e:3aca:d24l - ffdc:90c4:a0af:9449:7a7c

Cancel OK

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

Global Settings Querier Router Port Multicast Address Multicast Policy Multicast Port

Edit

Port

1/0/1 1/0/2 1/0/3 1/0/4 1/0/5 1/0/6 1/0/7 1/0/8 1/0/9 1/0/10 1/0/11 1/0/12 LAG1

Multicast Policy

Operation

256 Reject

256 Reject

Edit

Port

1/0/1

Max Multicast Group Count

Valid range is 1-256

256

Action

Reject

Multicast Policy

1

Multicast Policy ID

1

Cancel OK

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).

GWN783x support IPv4 and IPv6 static routing.

## Routing Table

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

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

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

Routing Table

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

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

## Static Routes

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

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

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

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

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 IPv4 Static Route**

\*Destination IP Address  
192.168.7.0

\*Mask Length  
Valid range is 0-32.  
24

Gateway  
 Next Hop  Outgoing Interface

\*Outgoing Interface  
VLAN 7

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

Cancel OK

*Add static route*

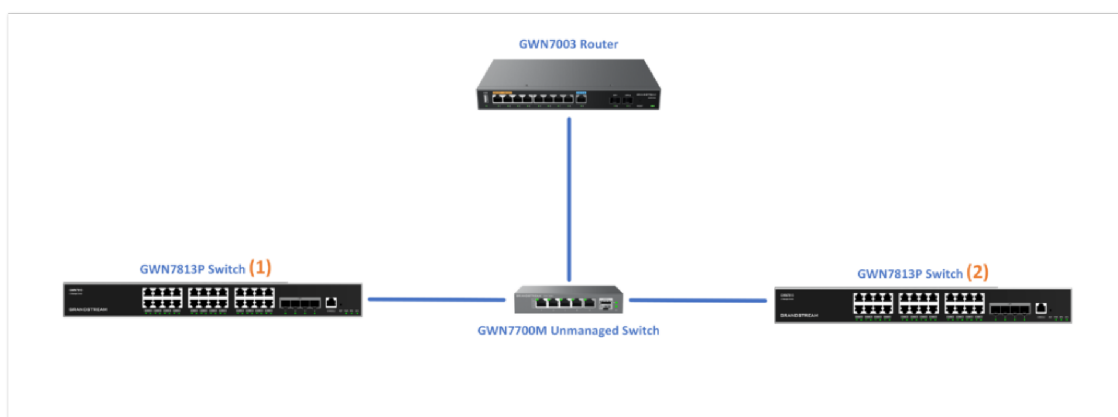
## OSPF (Open Shortest Path First)

OSPF stands for Open Shortest Path First, it's a routing protocol and uses a link state routing algorithm, in other words it collects information about the state of each link in the network to build an overall map about the whole network topology. OSPF is an interior gateway protocol (IGP) same as RIP (Routing Information Protocol), it's a protocol based on distance vector algorithms. OSPF has many advantages over other routing protocols, such as RIP.

Some Advantages of OSPF protocol:

- OSPF can perform route summarization, which reduces the size of the routing table and improves scalability.
- OSPF supports IPv4 and IPv6.
- OSPF can split the network into areas, which are logical groups of routers that share the same link state information. This reduces the amount of routing information that needs to be exchanged and processed by each router.
- OSPF can use authentication to secure the exchange of routing information between routers.
- OSPF can deal with variable length subnet masks (VLSM), which allows for more efficient use of IP addresses and network design.

In this example we will be using two GWN781x(P) switches directly connected (neighbors) and a router serving as a DHCP server. Please refer to the figure below:





## OSPF Global

To start using OSPF, please navigate to **Web UI** → **Routing** → **OSPF page** → **Global tab**:

Toggle ON OSPF and enter the Router ID (it can be any IPv4 address) then scroll down to the bottom of the page and click the **“OK”** button, please refer to the figure below:

### Note:

If adjacency relationship has been established, OSPF process needs to be rebooted for the router ID to take effect. Caution: this action will invalidate OSPF routing and result in recalculation. Please use with caution.

OSPF – Global

## OSPF Area Settings

The Area Settings tab allows you to configure different OSPF areas. An OSPF area is a logical grouping of routers that exchange OSPF information.

Area ID	Area Type	No Summary	Conversion Type	Operation
0.0.0.0	None	Disabled	--	
2.2.2.2	Stub	Disabled	--	

OSPF – Area Settings

To edit an Area Settings, click on **“Edit”** button.

- **Area ID:** The unique identifier for the OSPF area. Area 0.0.0.0 is the backbone area and must be configured in every OSPF network.
- **Area Type:** Defines the type of the area. OSPF supports different area types, including:
  - **None:** A normal OSPF area that supports all OSPF features.
  - **Stub Area:** Does not allow external routes to be advertised into the area, reducing the size of the routing table.
  - **Not-So-Stubby Area (NSSA):** Allows limited external routes, typically from an ASBR (Autonomous System Boundary Router) within the area.

- **No Summary:** (only for Stub and NSSA) disables the summarization of routes, forcing the router to advertise specific routes rather than aggregated routes. This may be useful in certain network designs where precise routing information is required.

OSPF – Edit Area Settings

## OSPF Interface Settings

On the Interface Settings tab, click on “**Edit**” icon to enable the [VLAN IP Interface](#).

OSPF									
Global Area Settings <u>Interface Settings</u> NBMA Neighbor Neighbor Info Database Info									
Interface	Status	Interface Address	Area ID	Network Type	Interface Suppression	Ignore MTU Validation	LS In	Operation	
VLAN 1	Enabled	192.168.80.211/24	0.0.0.0	Broadcast	Disabled	Disabled	5		
VLAN 7	Enabled	70.0.0.1/24	0.0.0.0	Broadcast	Disabled	Disabled	5		
VLAN 10	Enabled	10.0.0.1/8	0.0.0.0	Broadcast	Disabled	Disabled	5		
VLAN 20	Enabled	20.0.0.1/24	0.0.0.0	Broadcast	Disabled	Disabled	5		
VLAN 90	Enabled	90.0.0.1/24	0.0.0.0	Broadcast	Disabled	Disabled	5		

OSPF – Interface Settings

Toggle ON the OSPF on the selected interface then scroll down and click on “**OK**” button.

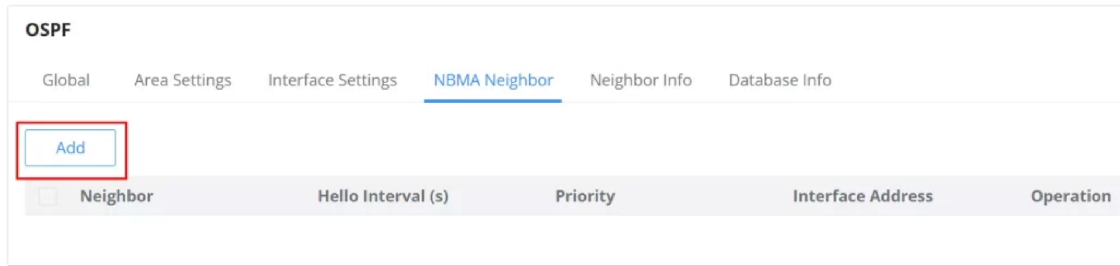
OSPF – Interface Settings – Edit Interface

## OSPF NBMA Neighbor

In Non-Broadcast Multi-Access (NBMA) networks, OSPF cannot automatically discover neighbors as it does in broadcast networks. Therefore, you must manually configure the neighbors.

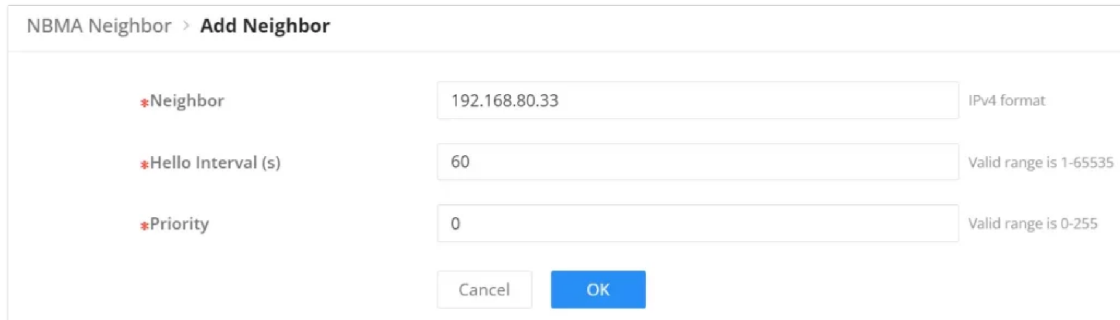
- **Neighbor:** The IP address of the neighbor OSPF router that you want to manually add.
- **Hello Interval (s):** The time interval between sending hello packets to this neighbor.
- **Priority:** The priority assigned to the neighbor. This value influences the selection of the Designated Router (DR) and Backup Designated Router (BDR).
- **Interface Address:** The local IP address of the interface that will communicate with the neighbor.

Click on “**Add**” button to add a neighbor.



OSPF – Neighbor Info

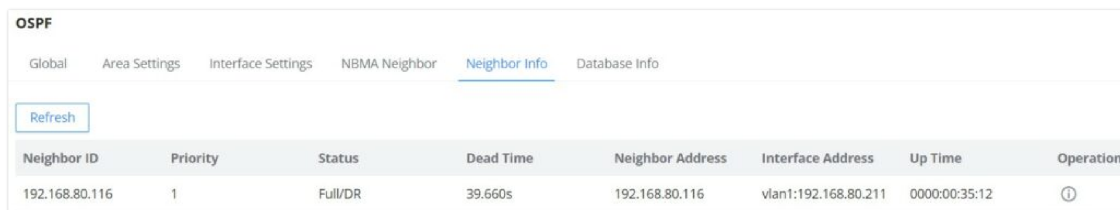
Then specify the Neighbor IP address (IPv4 format).



OSPF – Neighbor Info – Add neighbor

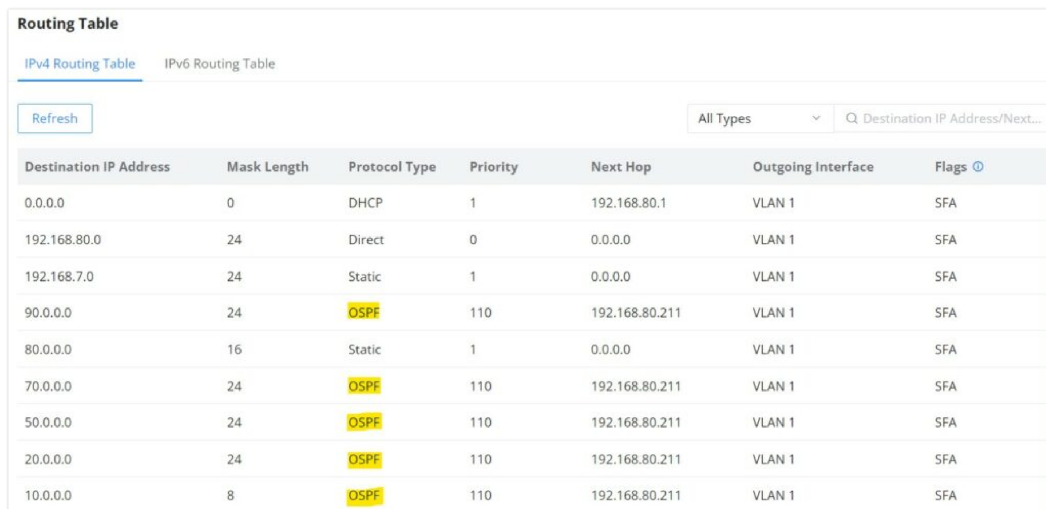
## OSPF Neighbor Info

Please do the same steps on the second switch, then on the **Neighbor Info tab**, click on “**refresh**” button for the adjacent (directly connected) switches to appear.



OSPF – Neighbor Info

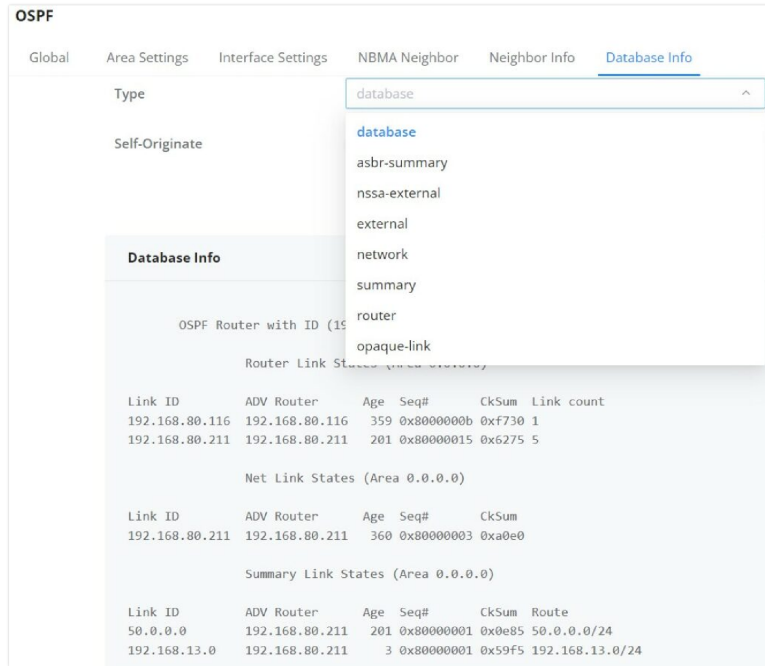
Navigate to the Routing table **Web UI → Routing → Routing table** to confirm that the routing table contains routes to the previously created VLAN IP Interfaces on the other switch. Please refer to the figure below:



IPv4 Routing Table

## OSPF Database Info

To check the **LSDB** (Link State DataBase), click on the **Database Info tab**, select the type (database) then click on “**Query**” Button to see the Database info which is a list of all **LSA** (Link State Advertisements) that the OSPF routers use to get information about other routers running OSPF protocol and that is what helps to populate the routing table for the best route to each destination.



OSPF – Database Info

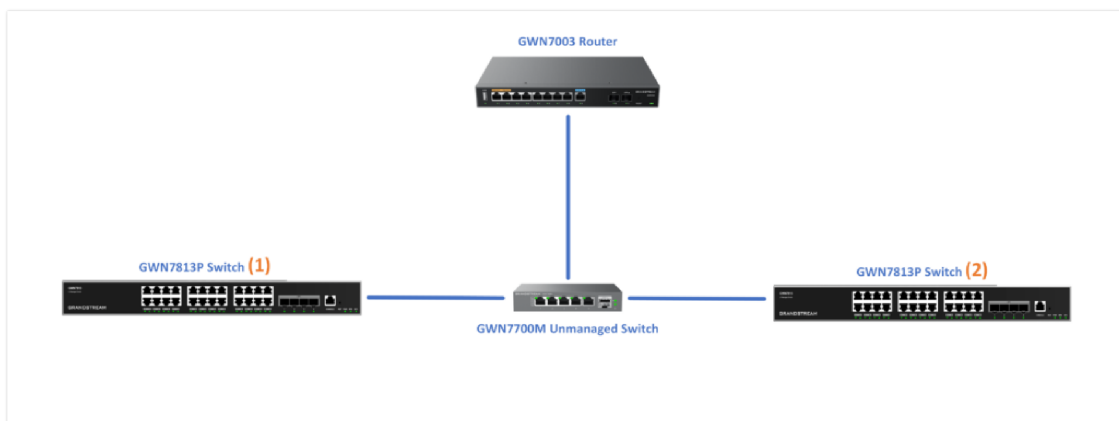
### OSPFv3

Building upon [OSPF](#), OSPFv3 (Open Shortest Path First Version 3) is specifically designed for IPv6 networks. While it shares many principles with OSPFv2, OSPFv3 introduces enhancements to accommodate IPv6 addressing and security features.

Key differences and advantages of OSPFv3 over OSPFv2:

- **IPv6 Support:** OSPFv3 is designed to support IPv6 natively, allowing for seamless integration into modern IPv6 networks.
- **Authentication:** OSPFv3 uses IPsec for authentication, providing enhanced security over OSPFv2, which uses built-in authentication methods like MD5.
- **Address Family Separation:** OSPFv3 separates the routing logic from the addressing, allowing for easier extension and support for multiple address families.
- **Link-State Advertisements (LSAs):** Introduces new LSAs to support IPv6 prefixes efficiently.

In this example, we will be using two GWN781x(P) switches directly connected (neighbors) and a router serving as a DHCP server. Please refer to the figure below:



Example – two GWN781x(P)

To start using OSPFv3, please navigate to **Web UI → Routing → OSPFv3:**

## OSPFv3 Global

Toggle ON OSPFv3 and enter the Router ID (it can be any IPv4 address). Configure the SPF calculation intervals and LSA parameters as needed. Click the **"OK"** button to save the settings. Refer to the figure below:

### Note:

If an adjacency relationship has been established, the OSPFv3 process needs to be rebooted for the Router ID to take effect. Caution: this action will invalidate OSPFv3 routing and result in recalculation. Please use with caution.

OSPFv3

Router ID  IPv4 format

Route Administrative Distance

**SPF Calculation**

Waiting Interval (ms)  Valid range is 0-600000

Minimum Interval (ms)  Valid range is 0-600000

Maximum Interval (ms)  Valid range is 0-600000

**LSA Parameters**

Receive Time (ms)  Valid range is 0-600000

**External Route Import**

Route Type  Direct  Static  RIPng

**Status**

OSPFv3 Routing Process (0) with Router-ID 1.1.1.1  
Running 01:30:26  
LSA minimum arrival 1900 msec

OSPFv3 – Global Configuration

## OSPFv3 Area Settings

On the Area Settings tab, click on the **"Edit"** icon to add and configure areas by specifying the Area ID and Area Type.

Area ID	Area Type	No Summary	Operation
0.0.0.0	None	<input type="checkbox"/> Disabled	<input type="button" value="Edit"/>
1.1.1.1	None	<input type="checkbox"/> Disabled	<input type="button" value="Edit"/>

Total 2    10 / page

OSPFv3 – Area Settings

## OSPFv3 Interface Settings

In the Interface Settings tab, click on the **"Edit"** icon to enable the [VLAN IP Interface](#).

Interface	Status	Interface Address	Area ID	Network Type	Interface Suppression	MTU	Ignore MTU Validity	Operation
VLAN 1	<input checked="" type="checkbox"/> Enabled	fe80::c274:adff:fedfcc94	1.1.1.1	Broadcast	<input type="checkbox"/> Disabled	1500	<input type="checkbox"/> Disabled	<input type="button" value="Edit"/> ⓘ
VLAN 7	<input checked="" type="checkbox"/> Enabled	fe80::c274:adff:fedfcc94	0.0.0.0	Broadcast	<input type="checkbox"/> Disabled	1500	<input type="checkbox"/> Disabled	<input type="button" value="Edit"/> ⓘ

Total 2    10 / page

OSPFv3 – Interface Settings – Edit Interface

Toggle ON OSPFv3 on the selected interface, then scroll down and click on the **"OK"** button.

Do the same steps on the second switch, then on the **Neighbor Info** tab, click on the **"Refresh"** button for the adjacent (directly connected) switches to appear.

Neighbor ID	Priority	Status	Dead Time	Neighbor Address	Interface Address	Up Time	Operation
No Data							

OSPFv3 – Neighbor Info

## OSPFv3 Database Info

To check the **LSDB** (Link State DataBase), click on the **Database Info** tab, select the type (database), then click on the **“Query”** Button to see the Database info, which is a list of all **LSAs** (Link State Advertisements) that the OSPFv3 routers use to get information about other routers running OSPFv3 protocol. This helps to populate the routing table for the best route to each destination.

Type	LSID	AdvRouter	Age	SeqNum	Payload
Area Scoped Link State Database (Area 1.1.1.1)					
Type	LSID	AdvRouter	Age	SeqNum	Payload
I/F Scoped Link State Database (I/F vln7 in Area 0.0.0.0)					
Type	LSID	AdvRouter	Age	SeqNum	Payload
I/F Scoped Link State Database (I/F vln1 in Area 1.1.1.1)					
Type	LSID	AdvRouter	Age	SeqNum	Payload
Lnk	0.0.0.3	1.1.1.1	1214	80000003	fe80::c274:adff:fedf:cc94
AS Scoped Link State Database					
Type	LSID	AdvRouter	Age	SeqNum	Payload

OSPFv3 – Database Info

## QoS

Popularity of the network and the diversification of services have led to a surge in Internet traffic, resulting in network congestion, increased forwarding delay, and even packet loss in severe cases, resulting in reduced service quality or even unavailability. Therefore, in order to carry out these real-time services on the network, it is necessary to solve the problem of network congestion. The best way is to increase the bandwidth of the network, but considering the cost of operation and maintenance, this is not realistic. The most effective solution is to apply a “Guaranteed” policies govern network traffic. QoS technology is developed under this background. QoS is quality of service, and its purpose is to provide end-to-end service quality assurance for various business needs. QoS is a tool for effectively utilizing network resources. It allows different traffic flows to compete for network resources unequally. Voice, video and important data applications can be prioritized in network equipment.

## Port Priority

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

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

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

QoS – Port Priority

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

### Edit Port Priority

Port

Trust Mode

\*CoS  
 Valid range is 0-7.

Remarking CoS

Remarking DSCP

Remarking IP Precedence

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

Edit Port Priority

<b>Port</b>	Displays the selected port GE/LAG.
<b>Trust Mode</b>	Select the QoS operation mode: <ul style="list-style-type: none"> <li>● <b>None</b>: no packet priority is trusted, and the interface default priority is used.</li> <li>● <b>CoS</b>: Traffic is mapped to queues based on the CoS Queue Mapping, it can configured in QoS → Priority Mapping → CoS Mapping page.</li> <li>● <b>DSCP</b>: 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.</li> <li>● <b>CoS-DSCP</b>: 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.</li> <li>● <b>IP-Precedence</b>: The IP precedence is a 3-bit field in TOS that treats high priority packets as more important than other packets. it can configured in QoS → Priority Mapping → IP Mapping page.</li> </ul>
<b>CoS</b>	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.
<b>Remarking CoS</b>	Set whether to enable Remarking CoS function of outgoing packets, which is disabled by default.

<b>Remarking DSCP</b>	Set whether to enable Remarking DSCP function of outgoing packets, <i>and it is disabled by default.</i>
<b>Re-marking IP Precedence</b>	Set whether to enable Remarking IP Precedence function of outgoing packets, <i>and it is disabled by default.</i> <b>Note :</b> <i>Only one of DSCP and IP Precedence re-marking can be enabled.</i>

### QoS Port Priority

## Priority Mapping

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

### o CoS Mapping

Shows the mapping relationship between queues and CoS remarking priorities.

The screenshot shows the 'Priority Mapping' configuration interface. It has three tabs: 'CoS Mapping', 'DSCP Mapping', and 'IP Mapping'. The 'CoS Mapping' tab is active. Underneath, there are two main sections: '802.1p (CoS) - Queue Mapping' and 'Queue-CoS Remarking Mapping'. Each section contains a table with 'CoS' or 'Queue' values in the first column and a dropdown menu for the corresponding 'Queue' or 'CoS' value in the second column. The values range from 0 to 6. At the bottom of each section is a 'Reset' button. At the bottom of the entire configuration area are 'Cancel' and 'OK' buttons.

CoS Mapping

### o DSCP Mapping

Shows the mapping relationship between DSCP values and queue priorities.

The screenshot shows the 'Priority Mapping' configuration interface with the 'DSCP Mapping' tab active. It displays a 'DSCP-Queue Mapping' table. The table has 13 columns: 'DSCP' and 'Queue' pairs for each of the 7 DSCP values (0-6). Each 'Queue' cell contains a dropdown menu. For example, for DSCP 0, the queue options are 0, 1, 2, 3, 4, 5, 6, 7. At the bottom of the table are 'Cancel' and 'OK' buttons.

DSCP Mapping

### o IP Mapping

Shows the mapping relationship between IP priority and queue.



**Priority Mapping**

CoS Mapping   DSCP Mapping   IP Mapping

**IP-Queue Mapping**      **Queue-IP Remarking Mapping**

IP	Queue	Queue	IP
0	0	0	0
1	1	1	1
2	2	2	2
3	3	3	3
4	4	4	4
5	5	5	5
6	6	6	6

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

Queue Scheduling

Queue Scheduling > **Edit**

Port: 1/0/1

Queuing Algorithm: Weighted Fair Queuing(WFQ)

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

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

Cancel OK

Queue Scheduling – Edit port

## Queue Shaping

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

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

**Queue Shaping**

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

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

Queue Shaping

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

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

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

Queue Shaping > **Edit**

Port: 1/0/1

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

Cancel OK

Queue Shaping – Edit port

## Rate Limit

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

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

Rate Limit

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

Rate Limit

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

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

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

Rate Limit > **Edit**

Port: 1/0/1

Ingress:

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

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

Egress:

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

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

Cancel OK

## SECURITY

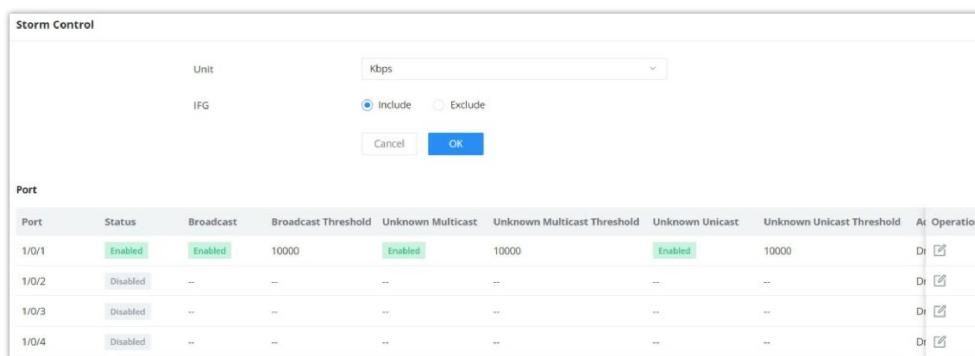
GWN783x Switches series support many tools and features to enhance the security of the device against misconfiguration or attacks.

### 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.

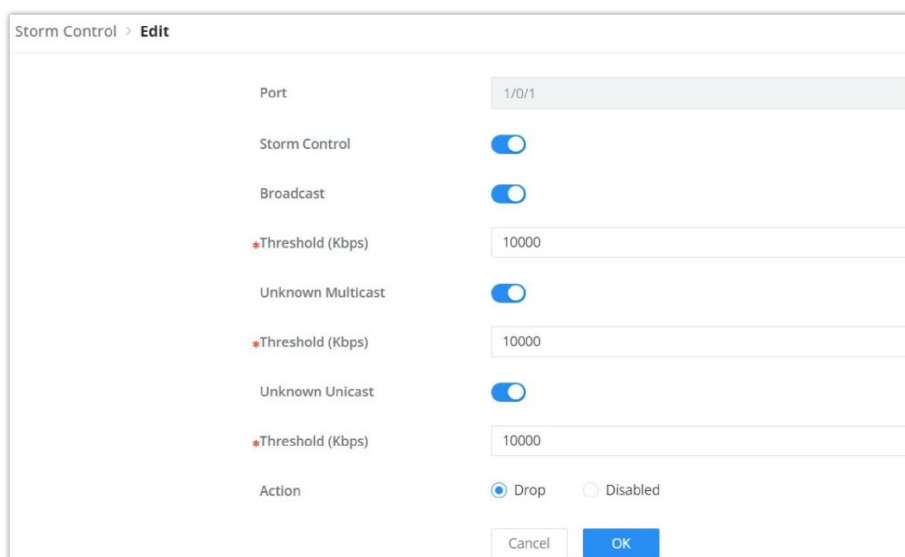
Storm control can block the traffic of broadcast, unknown multicast and unknown unicast packets by blocking packets or shutting down ports. The device supports storm control for the above three types of packets on the interface according to the packet rate, byte rate, and percentage. During a detection 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.



Port	Status	Broadcast	Broadcast Threshold	Unknown Multicast	Unknown Multicast Threshold	Unknown Unicast	Unknown Unicast Threshold	Ar	Operation
1/0/1	Enabled	Enabled	10000	Enabled	10000	Enabled	10000	Di	
1/0/2	Disabled	--	--	--	--	--	--	Di	
1/0/3	Disabled	--	--	--	--	--	--	Di	
1/0/4	Disabled	--	--	--	--	--	--	Di	

Storm Control page



Storm Control > Edit

Port: 1/0/1

Storm Control:

Broadcast:

Threshold (Kbps): 10000

Unknown Multicast:

Threshold (Kbps): 10000

Unknown Unicast:

Threshold (Kbps): 10000

Action:  Drop  Disabled

Cancel OK

Storm Control edit port

<b>Unit</b>	Select Unit: <ul style="list-style-type: none"> <li>● kbps: Storm control rate will be calculated by octet-based.</li> </ul>
-------------	--

	<ul style="list-style-type: none"> <li>● <b>pps</b>: Storm control rate will be calculated by packet-based.</li> </ul>
<b>IFG</b>	Select IFG ( Inter Frame Gap ): <ul style="list-style-type: none"> <li>● <b>Excluded</b>: Exclude IFG when count ingress storm control rate.</li> <li>● <b>Included</b>: Include IFG when count ingress storm control rate.</li> </ul>
<b>Storm Control → Edit</b>	
<b>Port</b>	Displays the selected port.
<b>Storm Control</b>	Select whether to enable Storm Control on the selected port or not.
<b>Broadcast</b>	Set whether to enable the storm threshold setting for broadcast packets. If Enabled Please enter a Treshhold (Kbps). <i>Note: The valid range is 16~1000000, which must be a multiple of 16. Default is 10000.</i>
<b>Unknown Multicast</b>	Set whether to enable the storm threshold setting for the Unknown Multicast packets If Enabled Please enter a Treshhold (Kbps). <i>Note: The valid range is 16~1000000, which must be a multiple of 16. Default is 10000.</i>
<b>Unknown Unicast</b>	Set whether to enable the storm threshold setting for the Unknown Unicast packets. If Enabled Please enter a Treshhold (Kbps). <i>Note: The valid range is 16~1000000, which must be a multiple of 16. Default is 10000.</i>
<b>Action</b>	Select the state of setting <ul style="list-style-type: none"> <li>● <b>Drop</b>: Packets exceed storm control rate will be dropped.</li> <li>● <b>Shutdown</b>: Port exceeds storm control rate will be shutdown.</li> </ul>

Storm Control

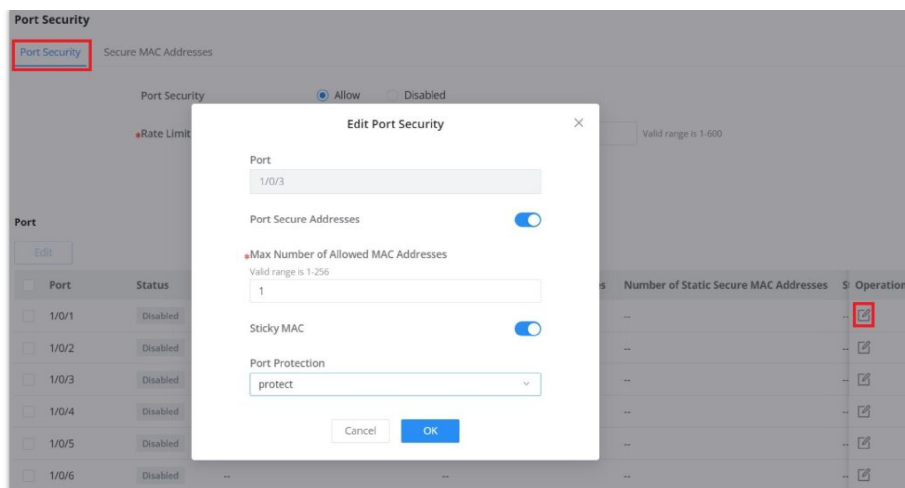
## Port Security

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.

<b>Secure Dynamic MAC Address</b>	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.
<b>Secure Static MAC Address</b>	Static MAC address manually configured when port security is enabled.	The entries will not be aged, and will not be lost after a reboot.
<b>Sticky MAC Address</b>	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

<b>Port Security</b>	Click Allow to set the port security function to be enabled globally , by default is disabled.
<b>Rate Limit (packet/s)</b>	Set the rate at which the port MAC address is learned. The value is an integer from 1 to 600, the default is 100.
<b>Edit Port Security</b>	
<b>Port</b>	Displays the selected ports.
<b>Port Security Address</b>	Click to enable Port Security Address, by default is disabled.
<b>Maximum MAC Number</b>	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).
<b>Sticky MAC</b>	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.
<b>Port Protection</b>	<p>Set the protection action when the number of MAC addresses learned by the interface reaches the maximum number or static MAC address flapping occurs .</p> <p>There are three modes (<b>Protect, Restrict or Shutdown</b>), the default is Protect.</p> <ul style="list-style-type: none"> <li>● <b>Protect:</b> Only discard the packets whose source MAC address does not exist, and does not report an alarm.</li> <li>● <b>Restrict:</b> Discard packets with nonexistent source MAC addresses and report an alarm.</li> <li>● <b>Shutdown:</b> The interface state is set to error-down and an alarm is reported.</li> </ul> <p><i><b>Note:</b> By default, an interface will not automatically recover after being shut down, and the interface can only be enabled by the network administrator under the interface. If you want the shut down interface to be restored automatically , you can enable Port Auto Recovery function to automatically restore the interface status to Up.</i></p>

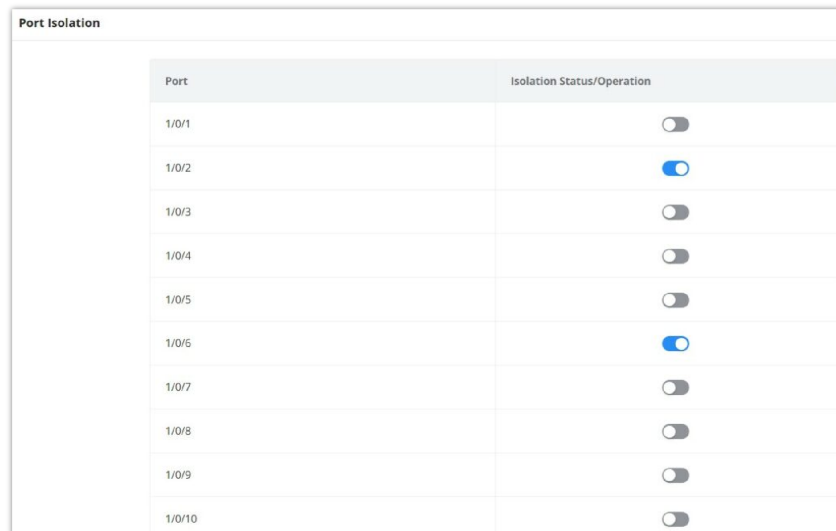
Port Security

## Port Isolation

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

### Note:

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



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

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 > Add ACL

\*ACL Name

**Rule Settings**

\*Rule ID

Action

Protocol Type

Source IP Address  Any  Custom

\*Source IP Address

\*Source IP Mask

Destination IP Address  Any  Custom

Tos Type

Time Policy

ACL – IPv4/IPv6

Tos Type

Time Policy

**Advanced Settings**

Count

\*Count ID  Valid range is 1-32

Count Unit  By packet  By byte

Mirroring

\*Mirroring Group

Go to "Maintenance>Diagnostics>Mirroring" to configure the monitor port to take effect

Priority Mapping

\*Priority  Valid range is 0-7

Rate Limit

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

ACL IPv4/IPv6 – Advanced Settings

Tos Type

Time Policy

**Advanced Settings**

Count

Mirroring

Priority Mapping

**Rate Limit**

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

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.

**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:



ACL > Add ACL

ACL Name: MAC\_Based\_ACL

**Rule Settings**

Rule ID: 1

Action: Drop

Protocol Type:  Any  Custom

Source MAC Address:  Any  Custom

Source MAC Address: c0 : 74 : ad : ff : ff : ff

Source MAC Mask: 11 : 11 : 11 : 00 : 00 : 00

Destination MAC Address:  Any  Custom

VLAN:  Any  Custom

802.1p Priority: Any

Time Policy: None

Cancel OK

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:

Edit Unbind

Port Name	IPv4 ACL Name	IPv6 ACL Name	MAC ACL Name	Operation
<input type="checkbox"/> 1/0/1			--	
<input type="checkbox"/> 1/0/2			--	
<input type="checkbox"/> 1/0/3			--	
<input type="checkbox"/> 1/0/4			--	
<input type="checkbox"/> 1/0/5			--	
<input type="checkbox"/> 1/0/6			--	
<input type="checkbox"/> 1/0/7			--	
<input type="checkbox"/> 1/0/8			--	
<input type="checkbox"/> 1/0/9			--	

**Edit Port ACL Binding**

Port: 1/0/1

IPv4 ACL  IPv6 ACL

IPv4 ACL: IPv4\_Based\_ACL

MAC ACL: MAC\_Based\_ACL

Cancel OK

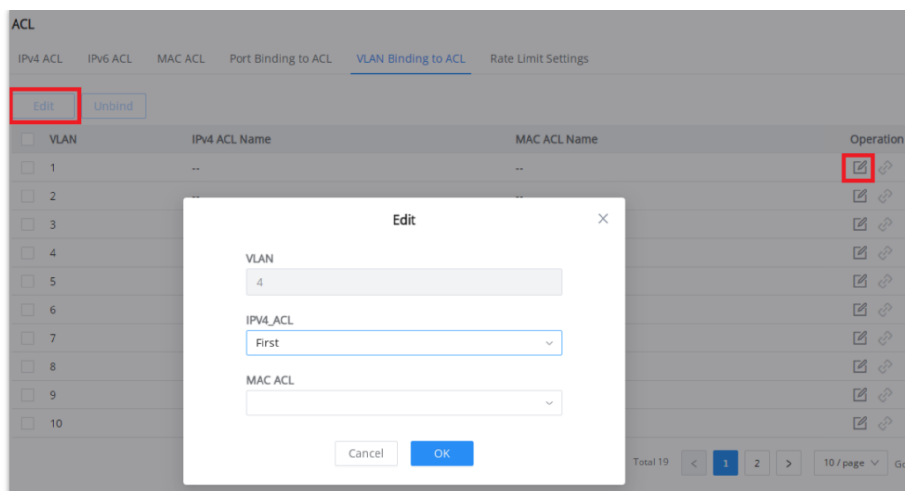
ACL Binding

## 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

The Rate Limit Settings section in ACL (Access Control List) allows users to configure rate limiting for up to 128 groups. Rate limiting helps manage and control the amount of traffic sent or received on the network, preventing congestion and ensuring fair usage. This feature is crucial for maintaining optimal network performance and avoiding overloads.

Rate Limit Group ID	Rate Limit Type	Burst Threshold	Rate Threshold	Operation
1	By packet	20000 pps	150000 pps	
2	By byte	8388480 Bps	125000 KBps	
3	--	--	--	
4	--	--	--	
5	--	--	--	
6	--	--	--	
7	--	--	--	
8	--	--	--	
9	--	--	--	
10	--	--	--	

ACL – Rate Limit Settings

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

- Click on the **"Edit icon"** under the Operation column to configure a group.
- Select the **Rate Limit Type** to determine if the limit will be by **packet or byte**.
- Specify the **Burst Packet/Byte**, which sets the maximum number of packets or bytes allowed to be sent in a burst.
- Set the **Rate Threshold**, which defines the maximum rate of packets or bytes per second.

ACL – Edit Rate Limit Group

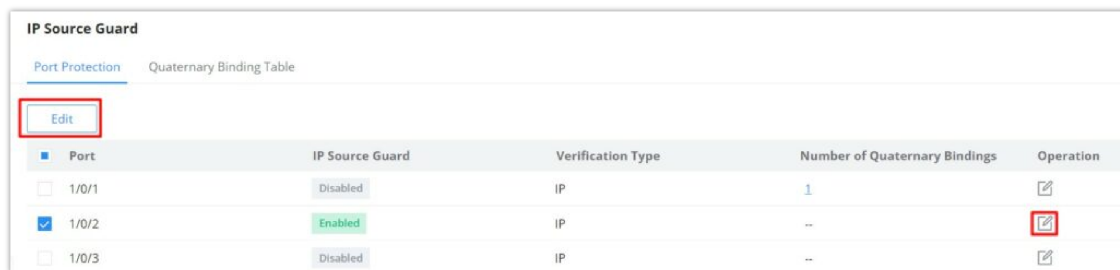
## IP Source Guard

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**.

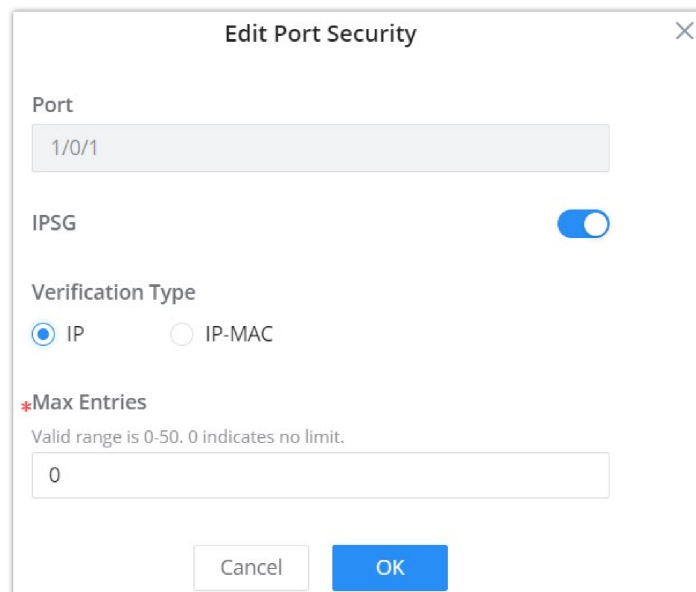
To enable IP Source Guard, first navigate to **Security** → **IP Source Guard** page, then select the port and click on "**Edit**" to configure the port.



Port	IP Source Guard	Verification Type	Number of Quaternary Bindings	Operation
<input type="checkbox"/> 1/0/1	Disabled	IP	1	
<input checked="" type="checkbox"/> 1/0/2	Enabled	IP	--	
<input type="checkbox"/> 1/0/3	Disabled	IP	--	

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.



### Edit Port Security

Port: 1/0/1

IPSG:

Verification Type:  IP  IP-MAC

\*Max Entries: 0  
Valid range is 0-50. 0 indicates no limit.

Cancel OK

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.

**IP Source Guard**

Port Protection [Quaternary Binding Table](#)

[Add](#) [Delete](#) [Refresh](#) [Import](#) [Export](#)

Port	IPv4 Address	MAC Address	VLAN	Type	Lease Time (s)	Operation
<input type="checkbox"/> 1/0/1	192.168.80.5	C0:74:AD:FF:FF:FF	1	Static	--	

Total 1 < 1 > 10 / page v

*Quaternary Binding Table*

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

**Add Quaternary Binding** ✕

**\*Port**

**\*IP Address**  
 IPv4 format

**\*MAC Address**  
 The MAC address must be a unicast address.  
 :  :  :  :  :

**\*VLAN**  
 Valid range is 1-4094

*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**

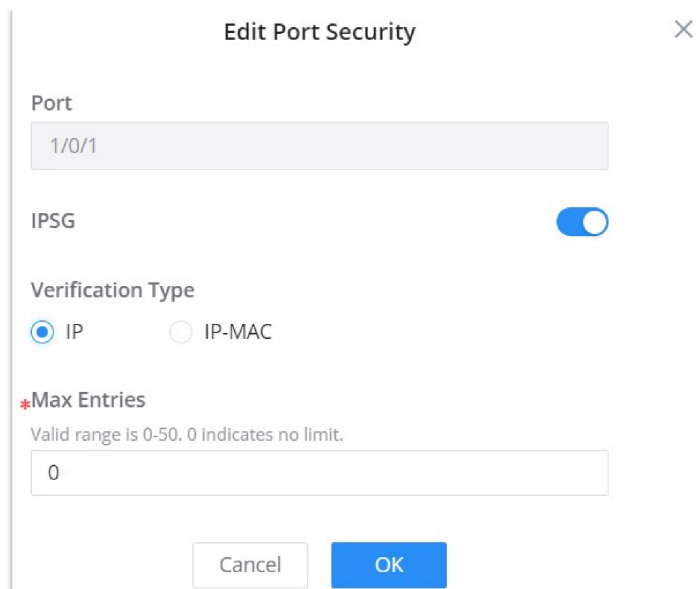
[Port Protection](#) [Quaternary Binding Table](#)

[Edit](#)

Port	IPv6 Source Guard	Verification Type	Number of Quaternary Bindings	Operation
<input type="checkbox"/> 1/0/1	Disabled	IPv6	--	
<input checked="" type="checkbox"/> 1/0/2	Enabled	IPv6	--	
<input type="checkbox"/> 1/0/3	Disabled	IPv6	--	

*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**.



**Edit Port Security**

Port: 1/0/1

IPSG:

Verification Type:  IP  IP-MAC

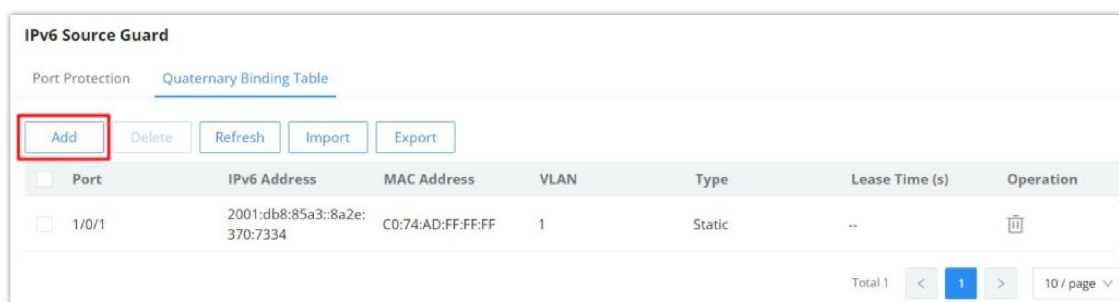
\*Max Entries: 0 (Valid range is 0-50. 0 indicates no limit.)

Buttons: Cancel, OK

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 Source Guard**

Port Protection | Quaternary Binding Table

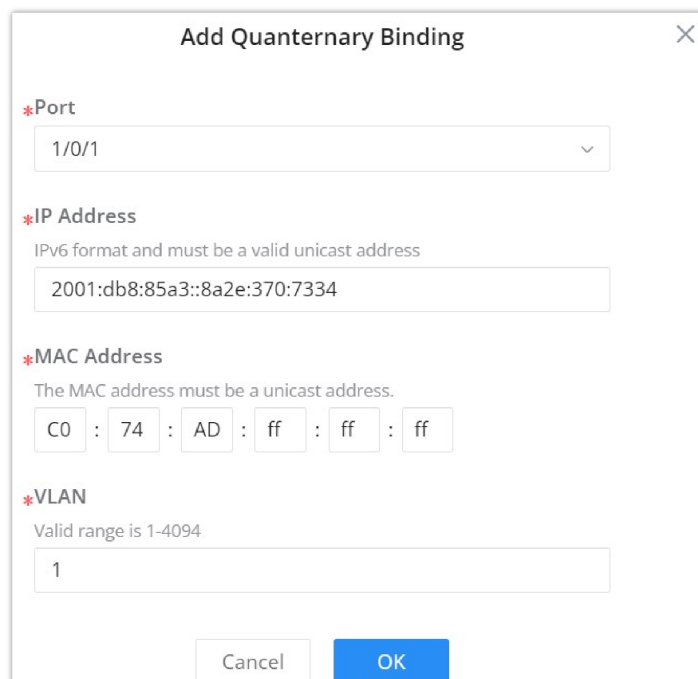
Buttons: Add, Delete, Refresh, Import, Export

Port	IPv6 Address	MAC Address	VLAN	Type	Lease Time (s)	Operation
<input type="checkbox"/> 1/0/1	2001:db8:85a3::8a2e:370:7334	C0:74:AD:FF:FF:FF	1	Static	--	

Total 1 | 1 / page

IPv6 Quaternary Binding Table

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



**Add Quaternary Binding**

\*Port: 1/0/1

\*IP Address: 2001:db8:85a3::8a2e:370:7334 (IPv6 format and must be a valid unicast address)

\*MAC Address: C0 : 74 : AD : ff : ff : ff (The MAC address must be a unicast address.)

\*VLAN: 1 (Valid range is 1-4094)

Buttons: Cancel, OK

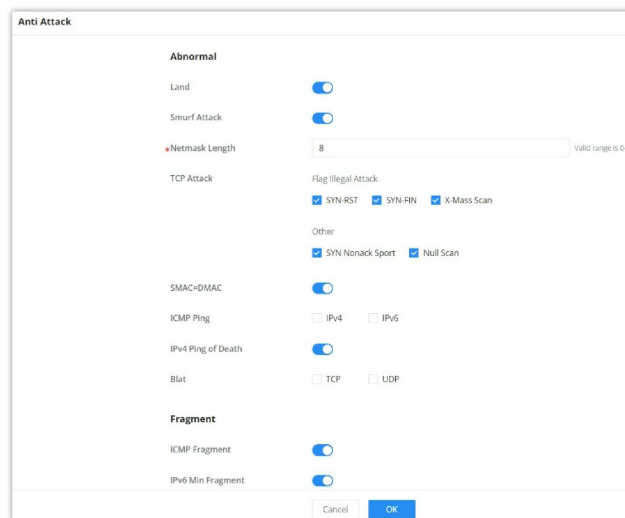
IPv6 Quaternary Binding – edit port

## 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, 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**

DAI Statistics

DAI

VLAN  Valid range is 1-4094. Example: "5-8, 11" will associate VLANs 5, 6, 7, 8 and 11.

**Port**

<input type="checkbox"/>	Port	Trust Port	Source MAC Address Verification	Destination MAC Address Verification	IP Address Verification	Speed (pps)	Operation
<input type="checkbox"/>	1/0/1	Disabled	Enabled	Enabled	Enabled	0	<input type="button" value="⌵"/>
<input type="checkbox"/>	1/0/2	Disabled	Disabled	Disabled	Disabled	0	<input type="button" value="⌵"/>
<input type="checkbox"/>	1/0/3	Disabled	Disabled	Disabled	Disabled	0	<input type="button" value="⌵"/>

DAI page

DAI > **Edit**

Port

Trust Port

Source MAC Address Verification

Destination MAC Address Verification

IP Address Verification

All-Zero Address  Forbid  Allow

Rate (pps)  Valid range is 0-50

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.

**DAI**

DAI Statistics

<input checked="" type="checkbox"/>	Port	Forwarding Packets	Source MAC Address Verification Failures	Destination MAC Address Verification Failures	Source IP Address Verification Failures	Des	Operation
<input checked="" type="checkbox"/>	1/0/1	0	0	0	0	0	<input type="button" value="⌵"/>
<input checked="" type="checkbox"/>	1/0/2	0	0	0	0	0	<input type="button" value="⌵"/>
<input checked="" type="checkbox"/>	1/0/3	0	0	0	0	0	<input type="button" value="⌵"/>
<input checked="" type="checkbox"/>	1/0/4	0	0	0	0	0	<input type="button" value="⌵"/>
<input checked="" type="checkbox"/>	1/0/5	0	0	0	0	0	<input type="button" value="⌵"/>
<input checked="" type="checkbox"/>	1/0/6	0	0	0	0	0	<input type="button" value="⌵"/>
<input checked="" type="checkbox"/>	1/0/7	0	0	0	0	0	<input type="button" value="⌵"/>
<input checked="" type="checkbox"/>	1/0/8	0	0	0	0	0	<input type="button" value="⌵"/>
<input checked="" type="checkbox"/>	1/0/9	0	0	0	0	0	<input type="button" value="⌵"/>
<input checked="" type="checkbox"/>	1/0/10	0	0	0	0	0	<input type="button" value="⌵"/>
<input checked="" type="checkbox"/>	1/0/11	0	0	0	0	0	<input type="button" value="⌵"/>

DAI Statistics

## RADIUS

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

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

**RADIUS**

Server Address	UDP Port	Priority	Max Retransmission Count	Timeout (s)	Operation
<input checked="" type="checkbox"/> 192.168.5.5					<input type="checkbox"/> <input type="checkbox"/>

\*RADIUS Server Address: 192.168.5.5

\*UDP Port: 1812

\*Priority: 16

\*Shared Key: password

\*Max Retransmission Count: 1

\*Timeout (s): 10

Cancel Save

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+**

Server Address	TCP Port	Priority	Timeout (s)	Operation
<input checked="" type="checkbox"/> 192.168.5.11	49	3	5	<input type="checkbox"/> <input type="checkbox"/>

\*TACACS+ Server Address: 192.168.5.11

\*TCP Port: 49

\*Priority: 3

\*Shared Key: password

\*Timeout (s): 5

Cancel Save

TACACS+

## AAA

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

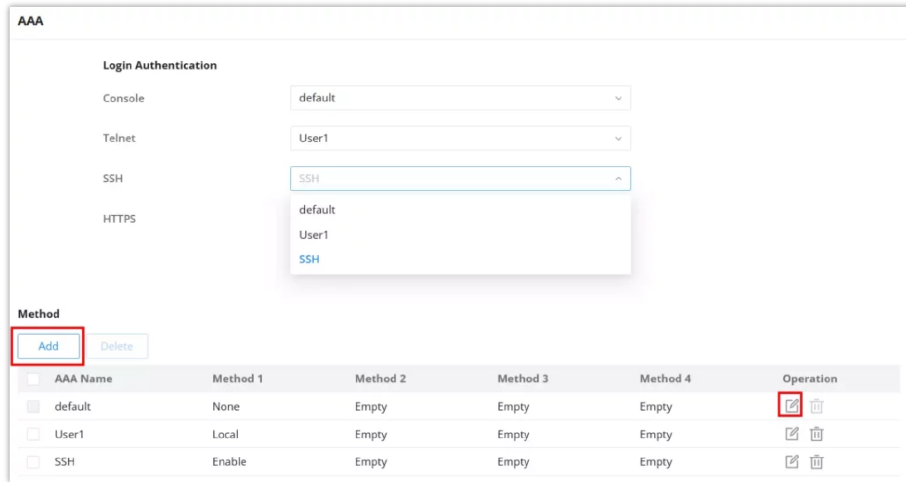
As a management mechanism of network security , AAA provides services in a modular manner:

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



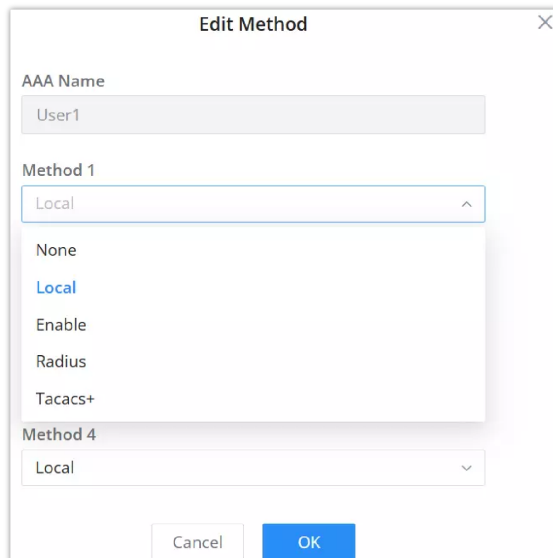
events and traffic, and also monitor the network.

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



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. <b>Note:</b> <i>The password for user mode to enter privileged mode must be set using <a href="#">CLI</a>.</i>	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

<b>TACACS+</b>	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

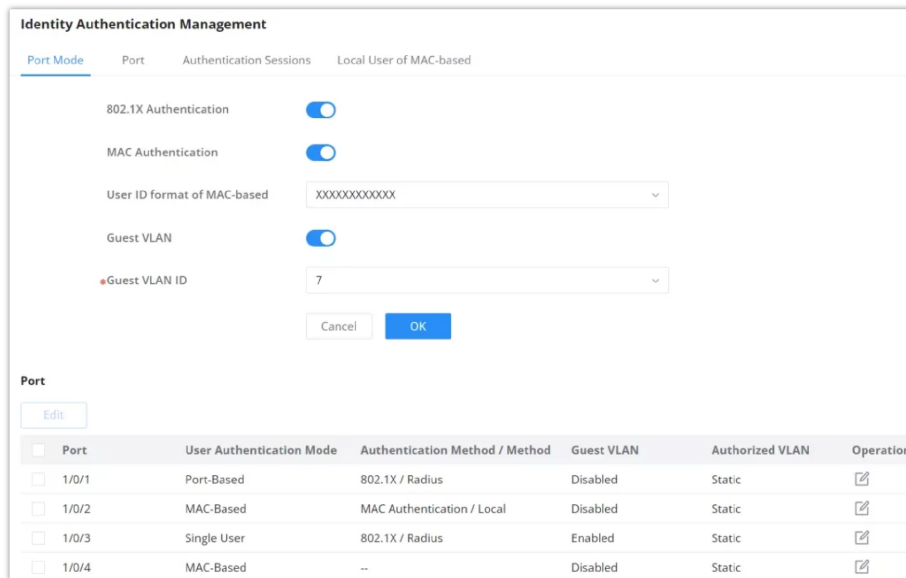
The Identity Authentication Management feature on Grandstream GWN switches provides a robust method for securing network access through 802.1X and MAC-based authentication. It allows administrators to configure and manage user authentication settings, ensuring only authorized devices can connect to the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

<b>Port</b>	The specific port being configured. This field shows the port number (e.g.
<b>User Authentication Mode</b>	The mode of user authentication to be used on this port. Options include: MAC-Based
<b>Guest VLAN</b>	Enables or disables the Guest VLAN for this port. If enabled
<b>Authorized VLAN</b>	Specifies the VLAN ID that authenticated users will be assigned to. This ensures that authorized devices are placed in the correct network segment.
<b>Authentication Methods(x)</b> <i>Note: click on "Add+" to add another method.</i>	
<b>Authentication Method1</b>	<p>Select the authentication method, two options:</p> <ul style="list-style-type: none"> <li>• <b>802.1X</b>: it will use 802.1x authentication, RADIUS must be first added.</li> <li>• <b>MAC Authentication</b>: it will use local MAC Addresses under Security → Identity Authentication Management page → Local User of MAC-based or RADIUS depending on the selected method.</li> </ul>
<b>Method</b>	<ul style="list-style-type: none"> <li>• If <b>MAC Authentication</b> is selected, the user can add two methods: Radius and Local.</li> <li>• If <b>802.1x</b> is selected, the user can only select radius.</li> </ul>

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 Mode	<b>Port</b>	Authentication Sessions	Local User of MAC-based					
<input type="button" value="Edit"/>								
<input type="checkbox"/>	Port	Port Control	Reauthentication	Max User Count	Reauthentication Timer	Inactive Timer	Quiet Timer	Operation
<input type="checkbox"/>	1/0/1	Force authentication	Enabled	256	3600	60	60	
<input type="checkbox"/>	1/0/2	Auto	Enabled	256	3600	60	60	
<input type="checkbox"/>	1/0/3	Force unauthentication	Enabled	256	3600	60	60	
<input type="checkbox"/>	1/0/4	Disable	Disabled	256	3600	60	60	

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 > **Edit**

Port: 1/0/1

**Port Control**: Force authentication

Reauthentication: Enabled

Max User Count: 256 (Valid range is 1-256)

**Common Timer**

Reauthentication Time (s): 3600 (Valid range is 300-2147483647)

Inactive Interval (s): 60 (Valid range is 60-65535)

Quiet Time (s): 60 (Valid range is 0-65535)

**802.1X Parameters Settings**

Resend EAP Request (s): 30 (Valid range is 1-65535)

Supplicant Timeout (s): 30 (Valid range is 1-65535)

Identity Authentication Management – port – edit port

**Note:**

The 802.1X must be also configured on the device connected to the GWN783x 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:

**Identity Authentication Management**

Port Mode   Port   Authentication Sessions   Local User of MAC-based

[Refresh](#)   [Clear All](#)  

Session ID	Port	MAC Address	Status	Configuration		
				VLAN	Session Time (s)	Inactive Time (s)
						

Authentication Sessions

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

[Refresh](#)   [Clear All](#)

Session ID	Port	MAC Address	Status
000000091184 7958	1/0/6	C0:74:AD:03:CA:80	Authorized

Authentication Sessions – Status Authorized

000000091184 7958	1/0/6	C0:74:AD:03:CA:80	Locked
----------------------	-------	-------------------	--------

Authentication Sessions – Status Locked

000000091184 7958	1/0/6	C0:74:AD:03:CA:80	Guest
----------------------	-------	-------------------	-------

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.

**Identity Authentication Management**

Port Mode   Port   Authentication Sessions   Local User of MAC-based

[Add](#)   [Delete](#)   [Delete All](#)

<input type="checkbox"/>	MAC Address	Port Control	VLAN	Reauthentication Time (s)	Inactive Time (s)	Operation
<input type="checkbox"/>	C0:74:AD:01:92:94	Force Unauthorized	--	--	--	 
<input type="checkbox"/>	C0:74:AD:03:CA:80	Force Authorized	1	3600	60	 

Local User of MAC-based

Add local User of MAC-based

<b>MAC Address</b>	The MAC address of the local user must be a unicast one.
<b>Port Control</b>	<ul style="list-style-type: none"> <li>• <b>Force Authorized:</b> Forces the port to authorize the device with the specified MAC address, allowing it access to the network.</li> <li>• <b>Force Unauthorized:</b> Forces the port to not authorize the device, preventing it from accessing the network.</li> </ul>
<b>VLAN</b>	Valid range is 1-4094.
<b>Reauthentication Time (s)</b>	Valid range is 300-2147483647.
<b>Inactive Time (s)</b>	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.

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 specifies 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).

**Circuit ID** is used to identify the VLAN, interface and other information where the client is located. To add a Circuit ID click on **"Add"** button as shown below:

Port	VLAN	Circuit ID	Operation
<input type="checkbox"/> 1/0/24	VLAN1	port24	

*DHCP Snooping – Option 82*

Then, select a port, VLAN and Format, and specify the Circuit ID based on what Format is selected.

Port: 1/0/24

\*VLAN: VLAN1

Format:  Normal  Private

\*Circuit ID: 1-63 characters  
SwitchPort24

*DHCP Snooping – Option 82 – Add Circuit*

## DHCP Snooping Port Settings

On this page, the user 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**

DHCP Snooping   Option 82   Port Settings   Statistics

**Edit**

Port	Trust Mode	Chaddr Verification	Speed(pps)	Option 82	Option 82 Mode	Operation
<input checked="" type="checkbox"/> 1/0/1	Enabled	Disabled	0	Enabled	Keep	
<input type="checkbox"/> 1/0/2	Disabled	Disabled	0	Disabled	Drop	
<input type="checkbox"/> 1/0/3	Disabled	Disabled	0	Disabled	Drop	
<input type="checkbox"/> 1/0/4	Disabled	Disabled	0	Disabled	Drop	
<input type="checkbox"/> 1/0/5	Disabled	Disabled	0	Disabled	Drop	

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:

Port Settings > **Edit**

Port: 1/0/1

Trust Mode:

Chaddr Verification:

Rate (pps): 0 Valid range is 0-300

Option 82:

Option 82 Mode: Keep

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**

DHCP Snooping   Option 82   Port Settings   Statistics

**Clear**   Refresh

Port	Forwarding Packets	Chaddr Verification Drops	Untrusted Port Drops	Untrusted Ports with Option 82 Drops	Operation
<input type="checkbox"/> 1/0/21	0	0	0	0	
<input type="checkbox"/> 1/0/22	0	0	0	0	
<input type="checkbox"/> 1/0/23	0	0	0	0	
<input checked="" type="checkbox"/> 1/0/24	31	0	31	0	
<input type="checkbox"/> 1/0/25	0	0	0	0	
<input type="checkbox"/> 1/0/26	0	0	0	0	
<input type="checkbox"/> 1/0/27	0	0	0	0	

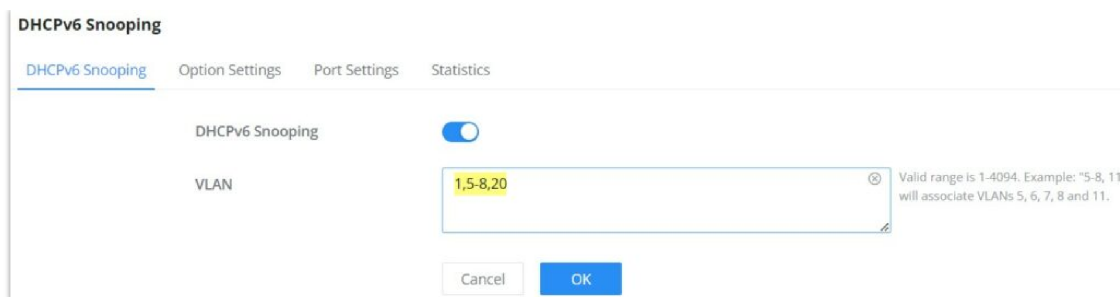
DHCP Snooping – Statistics

## 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:





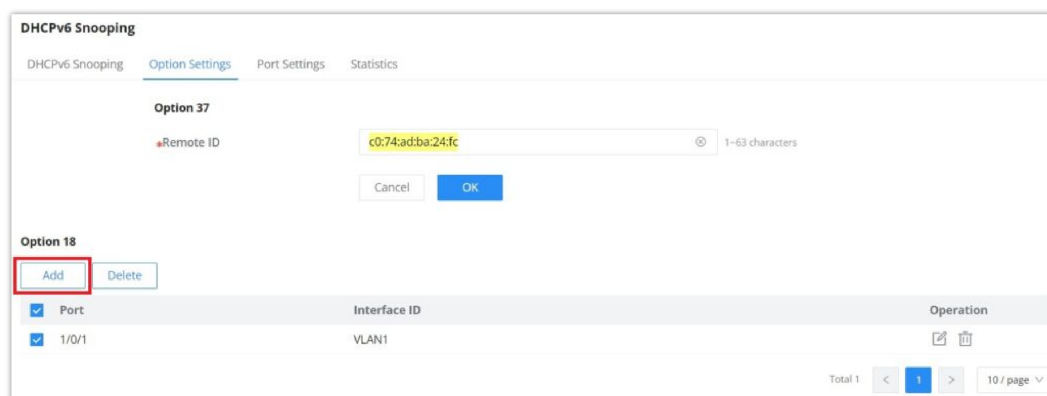
DHCPv6 Snooping

## DHCPv6 Snooping Option 82

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

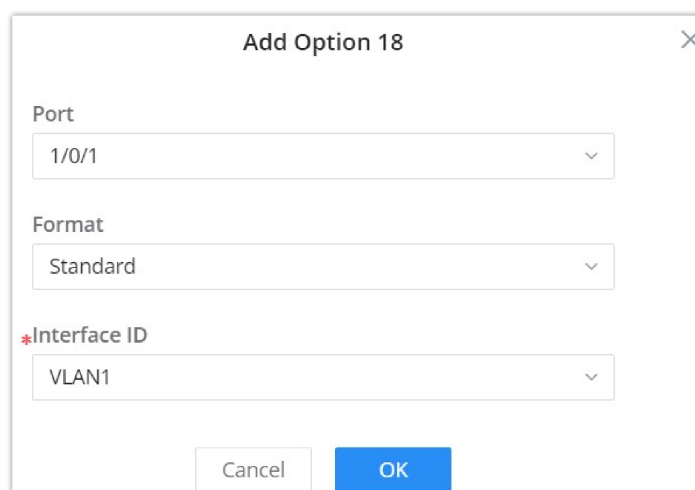
The DHCPv6 Relay-Option, encompassing Option 18 and Option 37, enables a DHCPv6 relay agent to embed circuit-specific and remote information as a TLV (type-length-value) within the relay message sent to the DHCPv6 server. In this scenario, the managed device functions as a DHCPv6 relay agent.

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:

Port	Trust Mode	Speed	Option 18	Option 37	Operation
<input checked="" type="checkbox"/> 1/0/1	Enabled	300	Drop	Keep	
<input type="checkbox"/> 1/0/2	Disabled	0	Disabled	Disabled	
<input type="checkbox"/> 1/0/3	Disabled	0	Disabled	Disabled	
<input type="checkbox"/> 1/0/4	Disabled	0	Disabled	Disabled	

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:

Port Settings > Edit

Port: 1/0/1

Trust Mode:

Rate (pps): 300 (Valid range is 0-300)

Option 18:

Option 18 Mode: Drop

Option 37:

Option 37 Mode: Keep

Buttons: Cancel, OK

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:

Port	Forwarding Packets	Untrusted Port Drops	Untrusted Ports with Option 37 Drops	Untrusted Ports with Option 18 Drops	Invalid Drop	Operation
<input checked="" type="checkbox"/> 1/0/1	0	0	0	0	0	
<input type="checkbox"/> 1/0/2	0	0	0	0	0	
<input type="checkbox"/> 1/0/3	0	0	0	0	0	
<input type="checkbox"/> 1/0/4	0	0	0	0	0	

DHCPv6 Snooping – Statistics

# MAINTENANCE

## Upgrade

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

Upgrading via network is also possible using 5 these protocols:

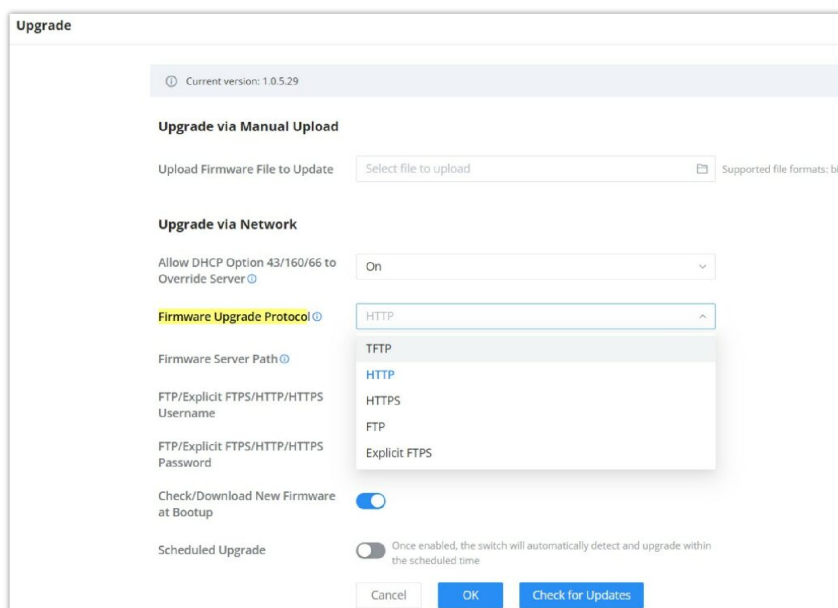
- o TFTP

- o HTTP
- o HTTPS
- o FTP
- o Explicit FTPS

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

**Note:**

- o Username and Password must be specified if the Server requires it.
- o For FTP protocol use the header "ftp://" and for FTPS use "ftps://"



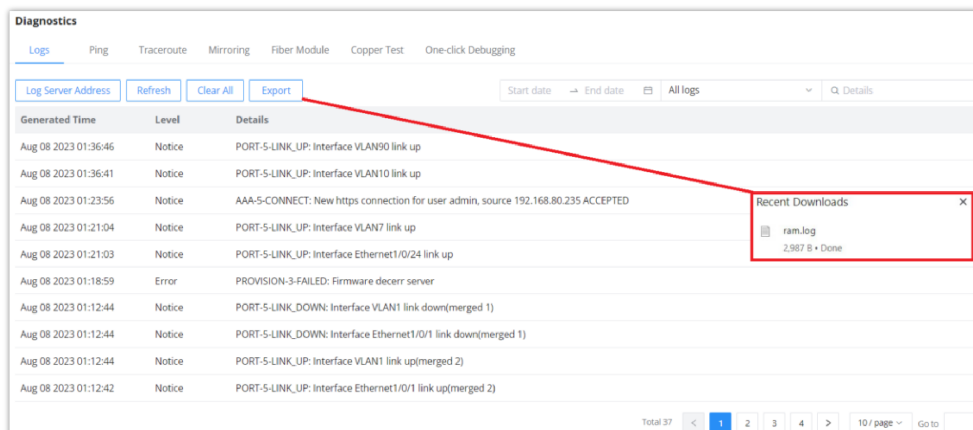
Upgrade

## Diagnostics

GWN783x Switches support many diagnostics tools that can help the user troubleshoot the issue and resolve it. These tools include Logs, Ping, Traceroute, Mirroring and Fiber Module.

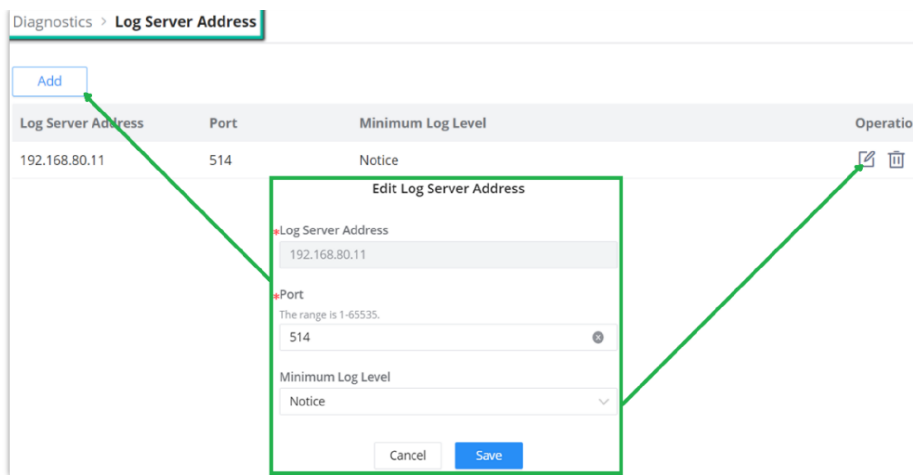
## Logs

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



Diagnostics – Logs

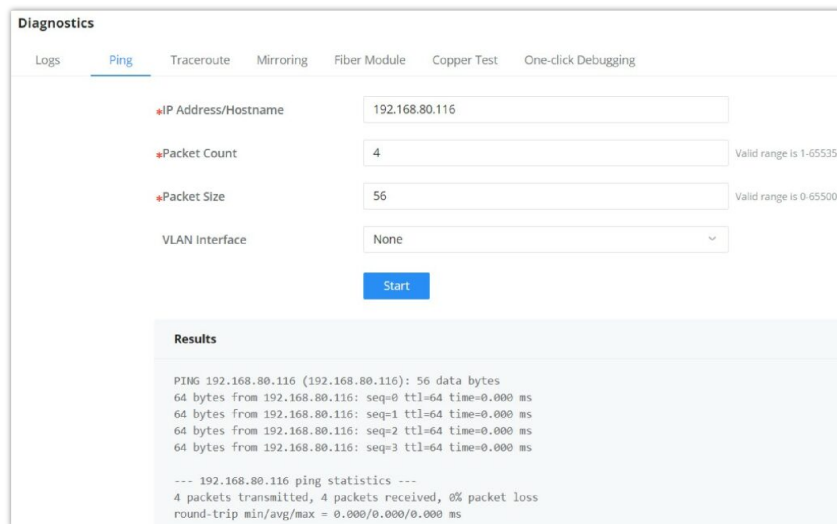
Adding a Log Server Address to the logs to be sent to is also supported on the GWN783x Switches.



Log Server Address

## Ping

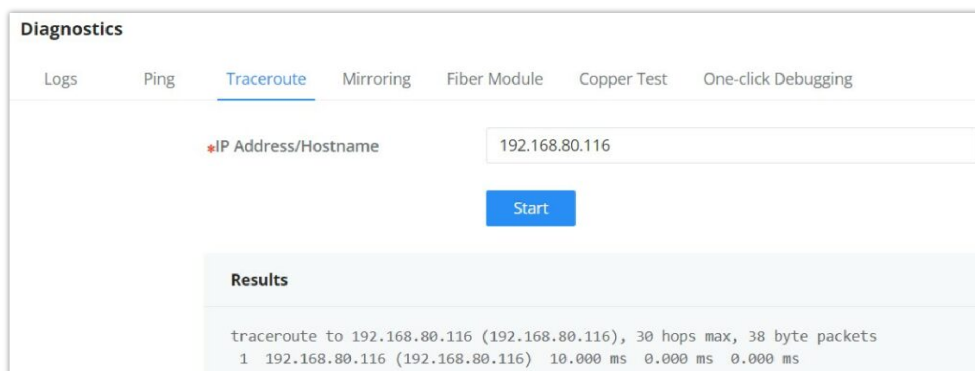
The user in this page can enter the IP Address or Hostname then click "Start", the results of the ping command will be shown below.



Ping

## Traceroute

Another tool is Traceroute that shows the number of hops, and GWN783x Switches enables the user to run Traceroute commands right from the Switches WEB UI.

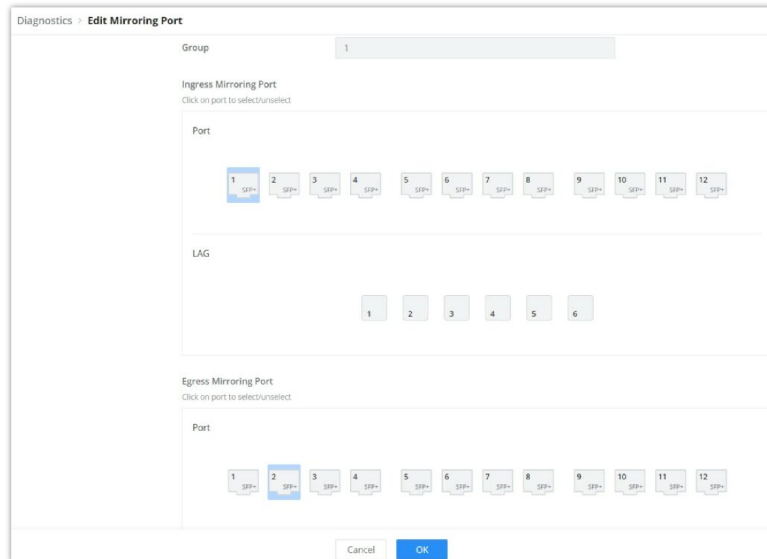


Traceroute

## Port Mirroring

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

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

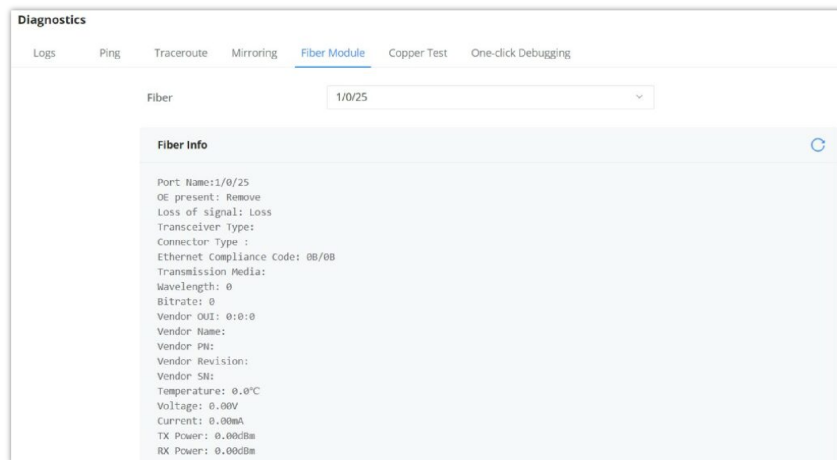


Port Mirroring

## Fiber Module

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

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



Fiber Module

## Copper Test

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

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

**Note:**

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

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

**Diagnostics**

Logs Ping Traceroute Mirroring Fiber Module **Copper Test** One-click Debugging

ⓘ Please ensure the Ethernet port is down when do copper test. Otherwise, it cannot be detected.

Click the port in figure above to do the copper test

Results	
Port Name	1/0/6
Cable status	Open
Cable length	3.46m

*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.

**Diagnostics**

Logs Ping Traceroute Mirroring Fiber Module Copper Test **One-click Debugging**

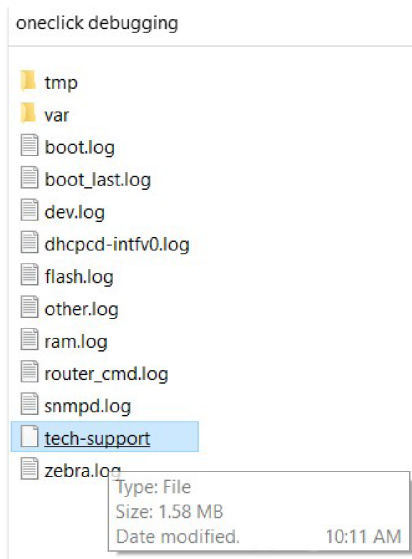
Perform one-click debugging on the device to obtain debugging information

**Debug**

oneclickdebug20230706093531.tar.gz  
194.36KB 2023/07/06 09:35:45

*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.

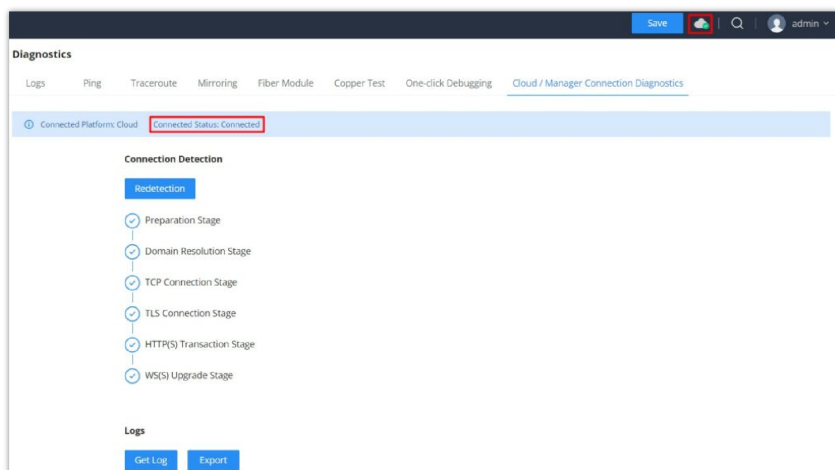


One-click Debugging Folder

## Cloud/Manager Connection Diagnostics

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

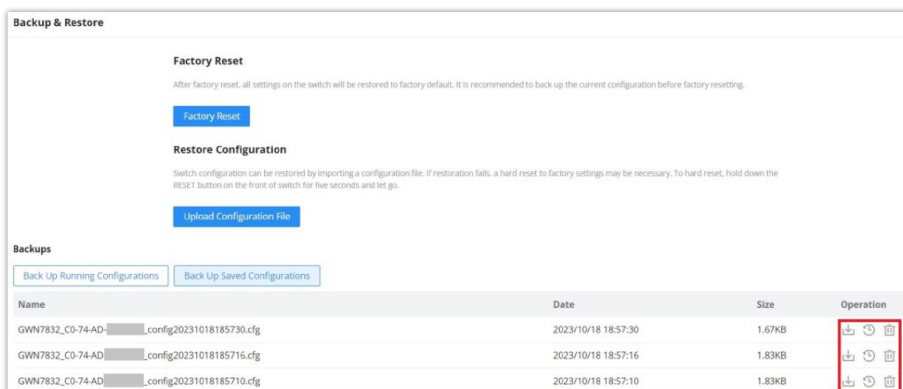
In case there is an issue with the connection, then the user can navigate to **Maintenance** → **System Diagnosis** → **Cloud/Manager Connection Diagnostics** and then click on **"Detection"** or **"Redetection"** button to see in what stage/step the connection has failed. Refer to the figure below:



Cloud/Manager Connection Diagnostics

## Backup and Restore

Click on "Factory Reset" button to reset the GWN783x 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.

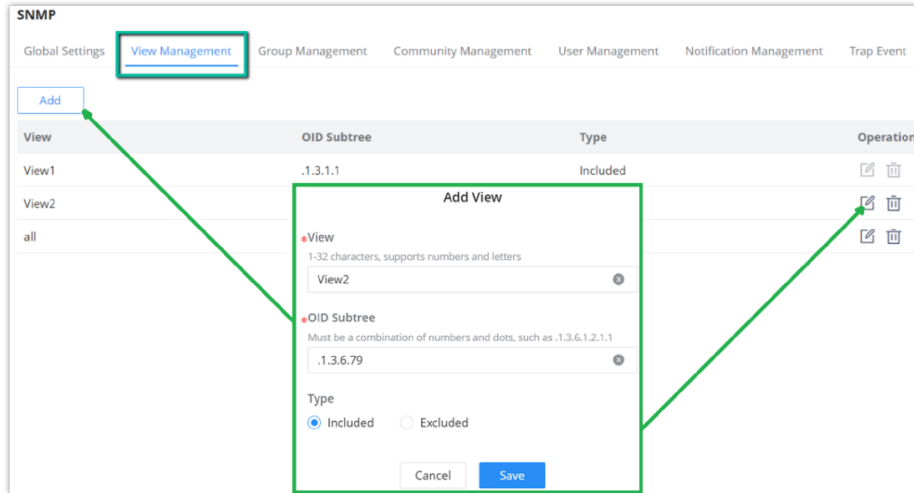
SNMP -Global Settings

<b>SNMP</b>	Select whether to enable SNMP.
<b>Local Engine ID</b>	Set the engine ID of the local SNMP entity or click "Reset" to restore to the initial value. <b>Note:</b> The default is 8000 A59Dxxxxxxx, where xxxxxxx 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 .
<b>Edit Remote Engine ID</b>	
<b>Remote Engine ID</b>	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.
<b>Server Address</b>	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.



## View Management

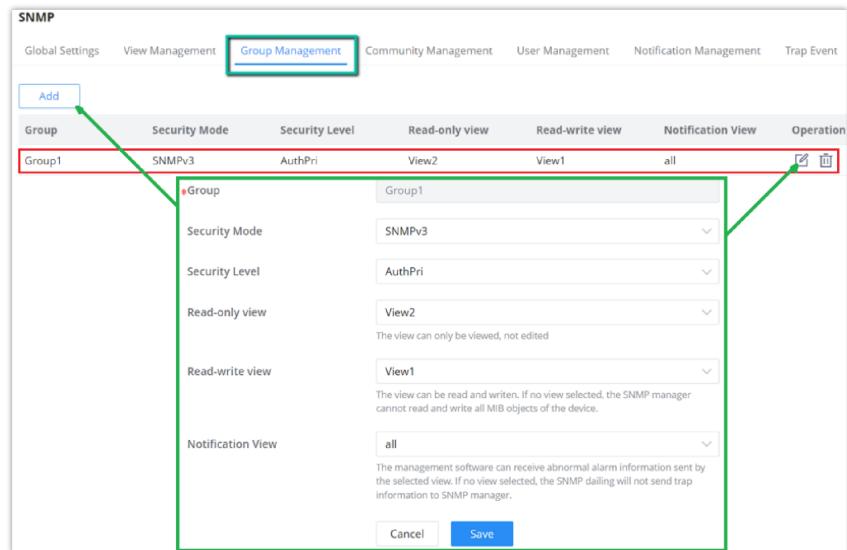
This page allows the network administrator to create MIB views (Management information base) and then include or exclude OID (Object Identifier) in a view.



SNMP – View Management

## Group Management

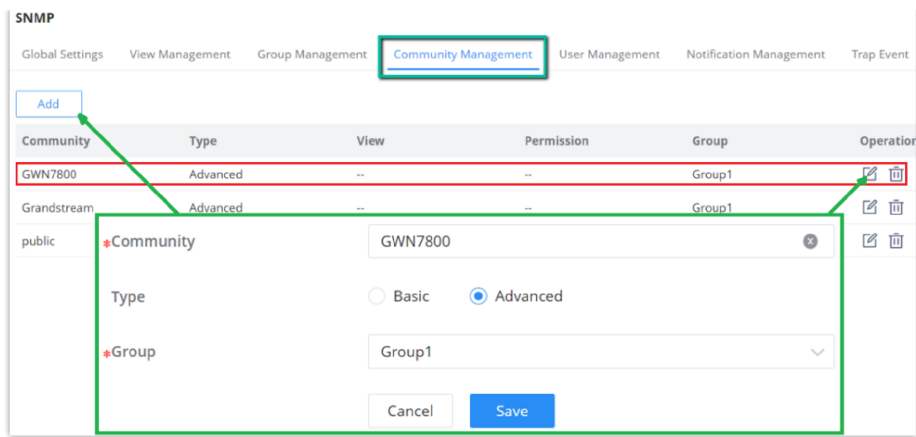
This page allows the network administrator to group SNMP users and assign different authorization and access privileges.



SNMP – Group Management

## Community Management

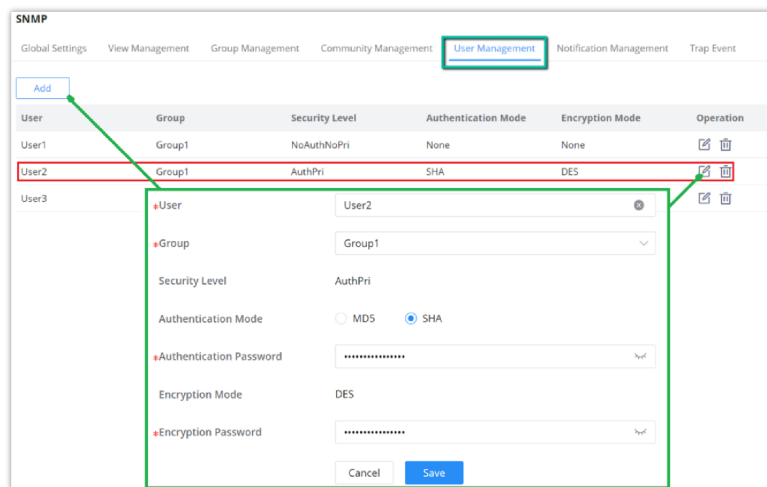
This page allows a user to add/remove multiple communities of SNMP.



SNMP – Community Management

## SNMP User Management

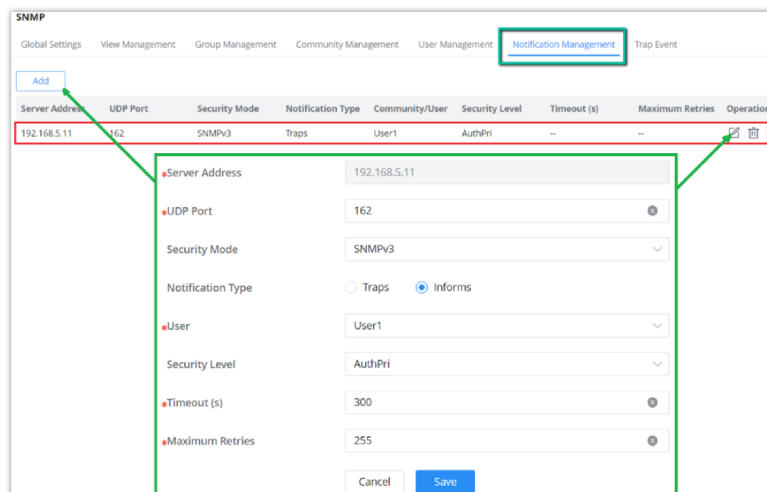
This page allows a user to configure SNMPv3 user profile.



SNMP – User Management

## Notification Management

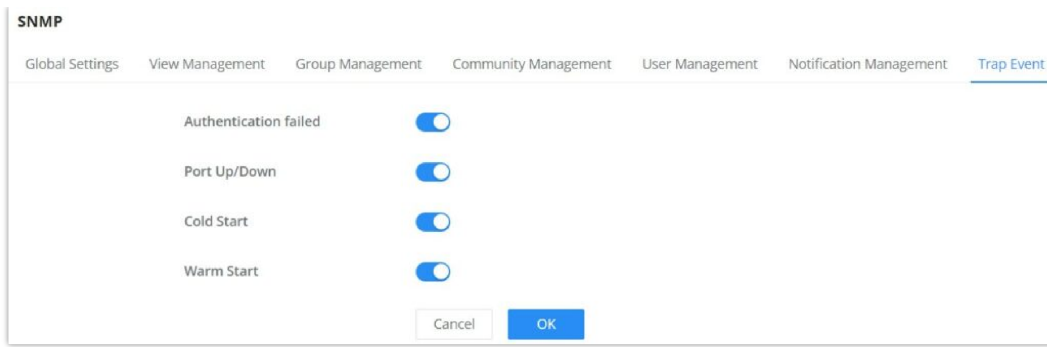
This page allows a user to configure a host to receive SNMPv1/v2/v3 notification.



SNMP – Notification Management

## Trap Event

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



SNMP – Trap Event

## RMON

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

### Note:

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

## RMON Statistics

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

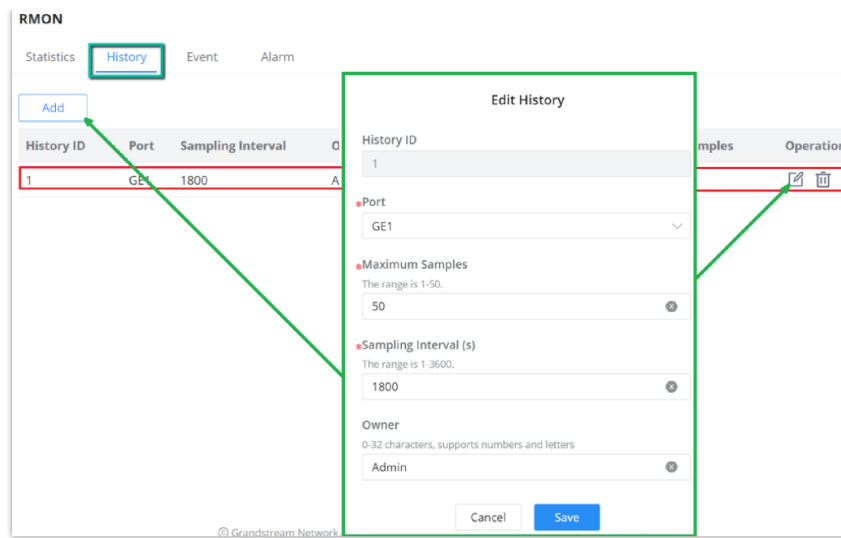
Port	Received Bytes	Drop Events	Received Packets	Broadcast Packets	Multicast Packets	CRC & Align Errors	Undersize Packets	Operation
1/0/1	14294925	0	99520	5450	9731	0	0	
1/0/2	0	0	0	0	0	0	0	
1/0/3	0	0	0	0	0	0	0	
1/0/4	0	0	0	0	0	0	0	
1/0/5	0	0	0	0	0	0	0	
1/0/6	0	0	0	0	0	0	0	
1/0/7	0	0	0	0	0	0	0	
1/0/8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

RMON – Statistics

## RMON History

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

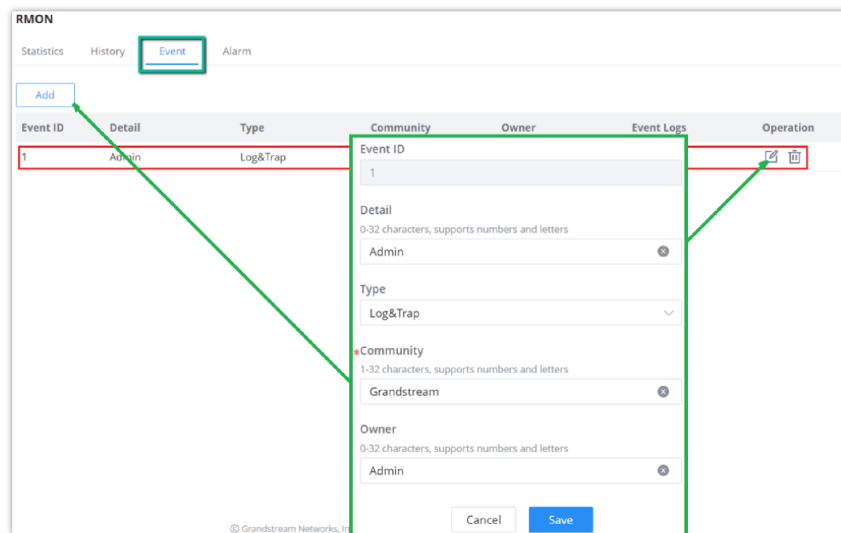
Click on “Add” button to create a History ID specifying the Port as well.



RMON – History

## RMON Event

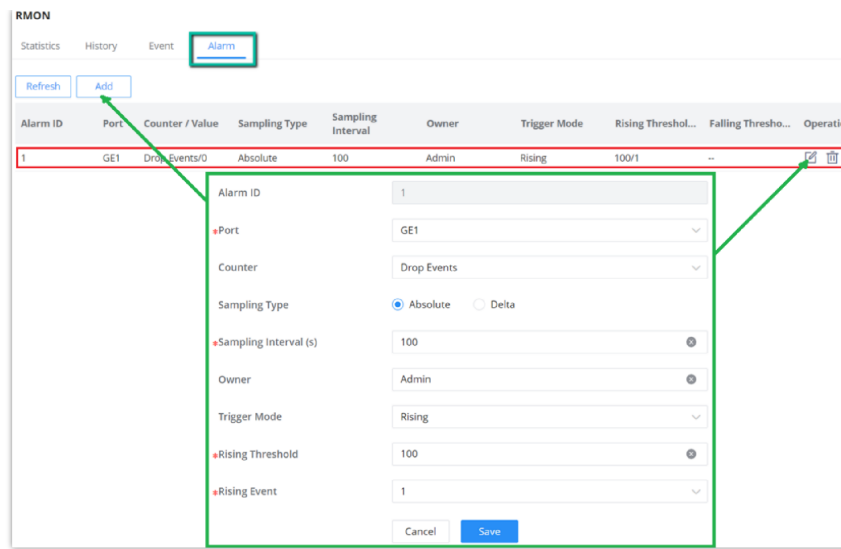
The event group controls the events and prompts from the device, and provides all events generated by the RMON Agent. When an event occurs, it can record logs or send Trap to the network management station.



RMON Event

## RMON Alarm

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



*RMON – Alarm*

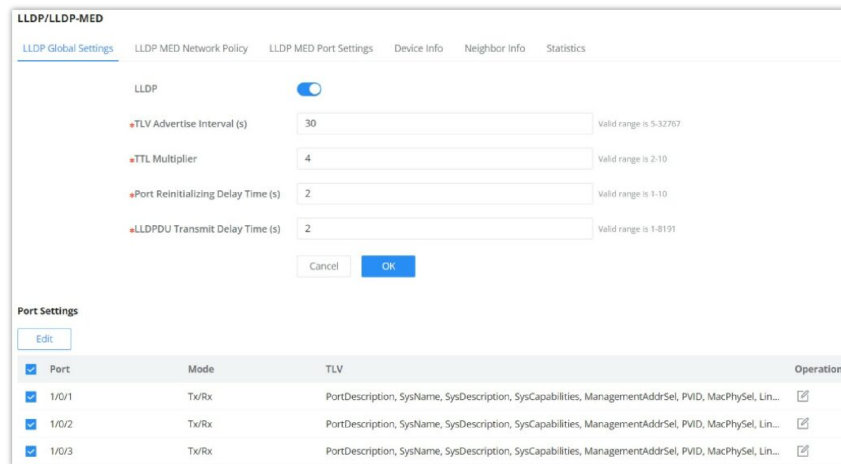
## LLDP/LLDP MED

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

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

## LLDP Global Settings

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



*LLDP Global Settings*

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

LLDP Global Settings > **Edit Port Settings**

Port: 1/0/1

Mode: Tx/Rx

TLV

Basic TLV

Port Description TLV     System Name TLV

System Description TLV     System Capabilities TLV

Management Address TLV

IEEE 802.1TLV

Port VLAN ID TLV     VLAN Name TLV

IEEE 802.3TLV

MAC/PHY Configuration/Status TLV     Link Aggregation TLV

Maximum Frame Size TLV     Power via MDI TLV

Cancel    **OK**

LLDP Port Settings

## LLDP MED Network Policy

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

**LLDP/LLDP-MED**

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



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

Auto Voice Network Policy:

Cancel    **OK**

**Network Policy**

Add    Delete

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

LLDP MED Network Policy

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

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

Policy ID: 1

Application: Voice

\*VLAN: 7    Valid range is 0-4095

VLAN Tag: Tagged

CoS: 6

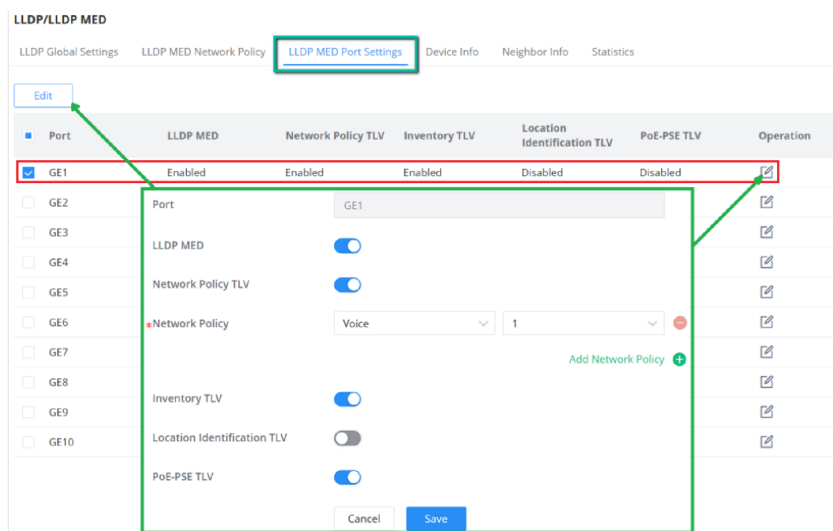
DSCP: 43

Cancel    **OK**

Add/Edit Network Policy

## LLDP MED Port Settings

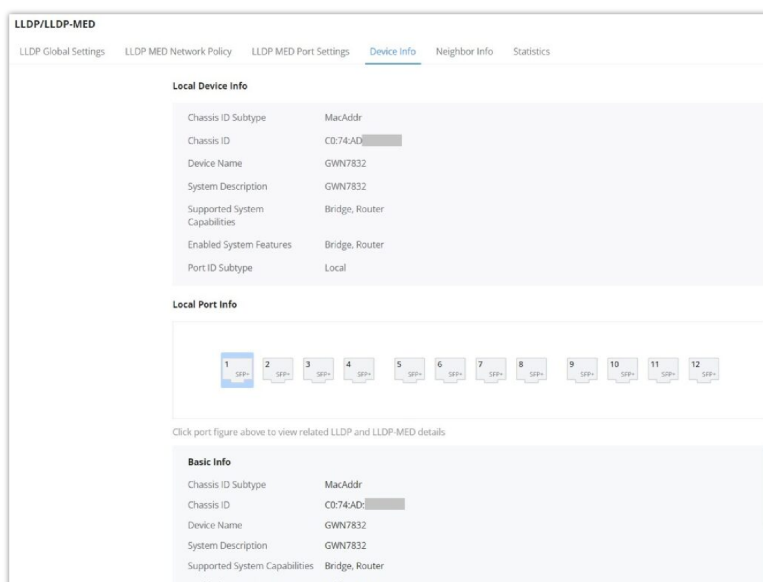
The user can configure LLDP MED Settings for each port in this page.



LLDP MED Port Settings

## LLDP Device Info

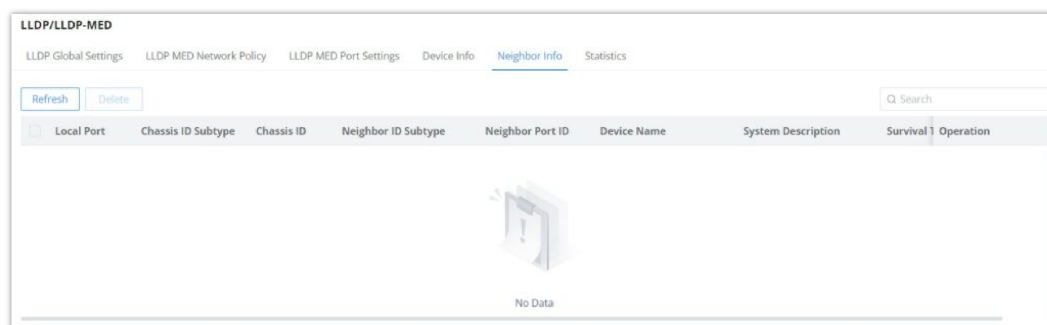
This page displays information for LLDP Local Device connected to each port. Click on the port to view related LLDP information about that port.



LLDP Device Info

## Neighbor Info

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



LLDP Neighbor Info

## LLDP Statistics

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

LLDP/LLDP-MED

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

**Global Statistics**

Insertions	1
Delete	1
Drops	0
Age-Outs	0

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

**Port Statistics**

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

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

LLDP Statistics

## Energy Efficient Ethernet

EEE 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**

[Edit](#) [Refresh](#)

Port	Configuration Status	Status	Operation
<input checked="" type="checkbox"/> 1/0/1	Enabled	Enabled	
<input type="checkbox"/> 1/0/2	Enabled	Disabled	
<input type="checkbox"/> 1/0/3	Disabled	Disabled	
<input type="checkbox"/> 1/0/4	Disabled	Disabled	
<input type="checkbox"/> 1/0/5	Disabled	Disabled	

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:

**Edit Port** ✕

Port  
1/0/1

802.3 EEE

[Cancel](#) [OK](#)

Energy Efficient Ethernet

## 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 Info**

• Device Name  1-64 characters

System Location  0-64 characters

System Contact  0-64 characters

**Time Settings**

Date & Time  Manual  Automatic (NTP Server)

System Time  🗓️

• NTP Server

Time Zone

DayLight Saving (DST) Mode

• Offset (Min)  Valid range is 1-1440

• Starting Time     🕒

• Ending Time     🕒

**Scheduled Reboot**

Reboot Time

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	<p>Select time synchronization method: Manual or Automatic (NTP Server).</p> <ul style="list-style-type: none"> <li>• <b>Manual:</b> specify the time manually.</li> <li>• <b>Automatic (NTP Server):</b> time will be synced automatically with NTP Server.</li> </ul> <p><i>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.</i></p>
System Time	<ul style="list-style-type: none"> <li>• <b>If Manual is selected,</b> the user can specify the date and time.</li> <li>• <b>If Automatic (NTP Server) is selected,</b> the current time and time will be displayed,</li> </ul>
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	<ul style="list-style-type: none"> <li>• <b>Disabled:</b> DayLight Saving mode will be disabled.</li> <li>• <b>Recurring:</b> if the Daylight saving is recurring (repetitive).</li> </ul>

	<ul style="list-style-type: none"> <li>● <b>Non Recurring:</b> if selected the user can specify the offset (min) and daylight saving time start date and end date.</li> <li>● <b>Recurring USA:</b> for USA region.</li> <li>● <b>Recurring EU:</b> for EU region</li> </ul>
<b>Offset (Min)</b>	Specify the Offset by minutes, range from 1 to 1440.
<b>Starting Time</b>	Specify the starting date and time.
<b>Ending Time</b>	Specify the ending date and time.
<b>Scheduled Reboot</b>	
<b>Reboot Time</b>	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*

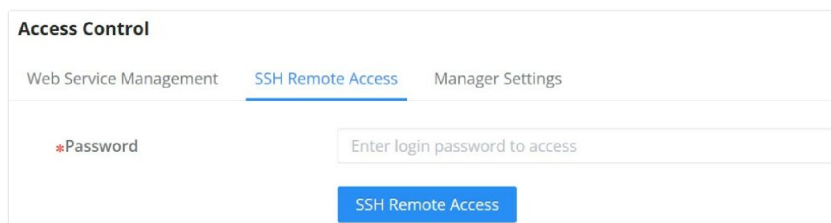
**Note:**

VTY (Virtual Teletype) sessions allow remote management of network devices through a command-line interface. GWN783x switches now support up to 12 simultaneous VTY sessions, enabling concurrent SSH or Telnet access for administrators.

## SSH Remote Access

**Note:**

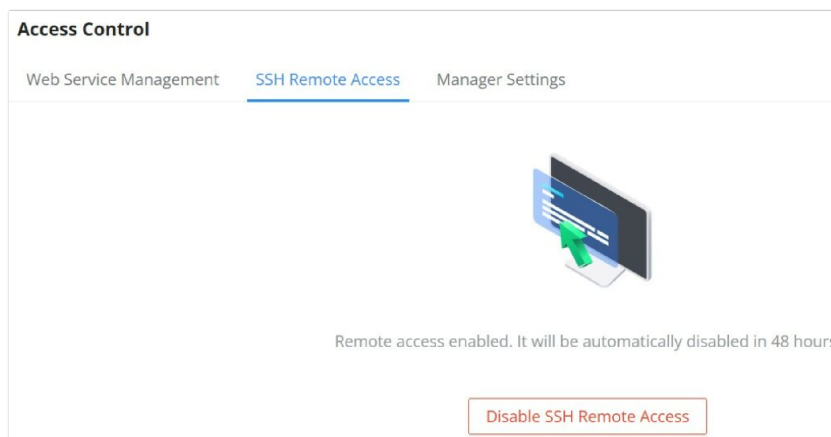
This feature is exclusively used for troubleshooting purposes by our developers and support engineers. When remote access is requested by either party, please enter the current user's password to grant permission to access to the device.



The screenshot shows the 'Access Control' interface with three tabs: 'Web Service Management', 'SSH Remote Access', and 'Manager Settings'. The 'SSH Remote Access' tab is active. Below the tabs, there is a label '\*Password' followed by a text input field containing the placeholder text 'Enter login password to access'. Below the input field is a blue button labeled 'SSH Remote Access'.

*Access Control – SSH Remote Access disabled*

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

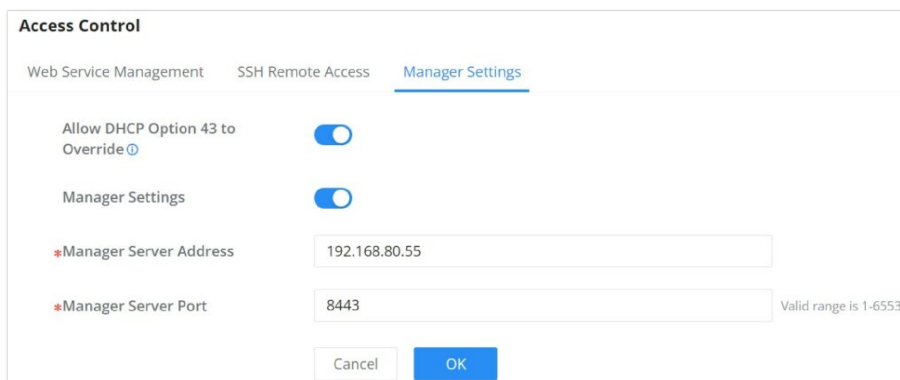


The screenshot shows the 'Access Control' interface with the 'SSH Remote Access' tab active. In the center, there is an illustration of a computer monitor with a green checkmark. Below the illustration, the text reads 'Remote access enabled. It will be automatically disabled in 48 hours.' At the bottom right, there is a red-bordered button labeled 'Disable SSH Remote Access'.

*Access Control – SSH Remote Access enabled*

## Manager Settings

Manager Settings tab allows the users to configure GWN Manager 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.



The screenshot shows the 'Access Control' interface with the 'Manager Settings' tab active. It contains several configuration options: 'Allow DHCP Option 43 to Override' with a blue toggle switch; 'Manager Settings' with a blue toggle switch; '\*Manager Server Address' with a text input field containing '192.168.80.55'; and '\*Manager Server Port' with a text input field containing '8443' and a note 'Valid range is 1-65535'. At the bottom, there are 'Cancel' and 'OK' buttons.

*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.

## User Management

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

### 1. Administrator

- Each device has one and only one administrator.

- The highest privileges, can execute any command.
- The username admin cannot be changed, only the password can be changed.
- Support adding, deleting operator and monitor.

## 2. Operator

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

### Note:

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

## 3. Monitor

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

### Note:

Can only view information.

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

The screenshot shows the 'User Management' interface. On the left, there is a table with columns 'Username' and 'Level'. The table contains the following entries:

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

Below the table are 'Add' and 'Delete' buttons. A red arrow points to the 'Add' button, and a green arrow points to the 'Delete' button. To the right of the table is the 'Add User' form, which is highlighted with a green border. The form contains the following fields:

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

At the bottom of the form are 'Cancel' and 'OK' buttons.

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.

The screenshot shows the 'Time Policy' configuration page. On the left, there are buttons for '+ Create Policy', 'Upgrade Schedule', and a trash icon. The main area is titled 'Create Policy' and contains a warning message: 'If both weekly and absolute schedules are configured on the same day, only the absolute schedule will take effect.' Below this, the 'Policy Name' is set to 'Reboot Schedule'. A 'Weekly' schedule table is shown with columns for days of the week and rows for time intervals. The Saturday column is highlighted in blue. Below the table, there is an 'Absolute Date / Time' section with input fields for date and time, and an 'Add' button.

Select All	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday
00:00-00:30							
00:30-01:00							
01:00-01:30							
01:30-02:00							
02:00-02:30							
02:30-03:00							
03:00-03:30							
03:30-04:00							
04:00-04:30							
04:30-05:00							
05:00-05:30							

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 GWN783x switches user manuals. Only major new features or major document updates are listed here. Minor updates for corrections or editing are not documented here.

### Version 1.0.7.71

Product Name: GWN7830/GWN7831

- 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](#)]
- Added refresh IP address when using DHCP to get VLAN IP address. [[VLAN IP Interface](#)]
- Added support for OSPFv3. [[OSPFv3](#)]
- Added support for 12 VTY (SSH or telnet) sessions. [[Access Control](#)]
- Added support to see switch clients and other information. [[Port Info](#)]

### **Version 1.0.3.1**

- This is the initial release.

### **Need Support?**

Can't find the answer you're looking for? Don't worry we're here to help!

[CONTACT SUPPORT](#)