

Grandstream Networks, Inc.

GWN780x Pro Managed Switches - User Manual



GWN780x Pro Managed Switches - User Manual

INTRODUCTION

The **GWN780x Pro Series** is a **Layer 2++ managed** network switch designed for small-to-medium enterprises that require scalable, secure, and high-performance networks with simplified management.

Each model delivers high-speed **Gigabit Ethernet** connectivity with **SFP or SFP+ uplink ports**, providing switching capacities up to **216 Gbps** to meet demanding business needs.

The series supports advanced features such as:

- **VLAN configuration** for flexible traffic segmentation
 - **QoS** for precise traffic prioritization
 - **IGMP/MLD Snooping** to optimize multicast performance
 - **Comprehensive security functions**, including ARP inspection, IP source guard, and DoS protection
- PoE-capable models offer **intelligent dynamic PoE/PoE+/PoE++ power allocation**, supplying power to IP phones, cameras, access points, and other network devices.

Management is versatile and free to use, with options including:

- **Embedded Web UI controller**
- **GDMS Networking** (cloud)
- **GWN Manager** (on-premise software)
- **GWN Series Routers**
- **Command-Line Interface (CLI)**

Combining enterprise-class performance, robust security, and flexible management, the **GWN780x Pro Series** delivers a complete switching solution ideal for modern business environments.

PRODUCT OVERVIEW

Technical Specifications

Feature	GWN7801P Pro	GWN7802P Pro	GWN7803 Pro	GWN7803PL Pro	GWN7803PH Pro	GWN7806PL Pro	GWN7806PH Pro
Interfaces							
Gigabit Ethernet Ports	8	16	24			48	
SFP/SFP+ Ports	2x 2.5G SFP	2x SFP+				6x SFP+	
Maximum Amount of Supported Modules	SM-10G: 2 MM-10G: 2 RJ45-10G: 2					SM-10G: 6 MM-10G: 6 RJ45-10G: 3 *Note: RJ45-10G modules must be interval inserted	
MGMT Ports	1x Console port						
Auxiliary Ports	1x Reset Pinhole						
LEDs							
System LEDs	1x tri-color LED for device tracking and status indication						

Power Supply LEDs	/		2x green-color LEDs for per power supply PWR&RPS	/	2x green-color LEDs for per power supply PWR&RPS		
Data Transferring LEDs	10x green-color LEDs	18x green-color LEDs	26x green-color LEDs			54x green-color LEDs	
PoE Supply LEDs	8x yellow-color LEDs	16x yellow-color LEDs	/	24x yellow-color LEDs		48x yellow-color LEDs	
System							
Flash	32MB Nor Flash					8MB Nor Flash, 128MB Nand Flash	
RAM	128MB RAM	256MB RAM				512MB RAM	
CPU	Single-core, MIPS interAptive 1GHz					Dual-core, MIPS interAptive™ 1GHz	
Forwarding Mode	Store-and-forward						
Total non-blocking throughput	13Gbps	36Gbps	44Gbps			108Gbps	
Switching Capability	26Gbps	72Gbps	88Gbps			216Gbps	
Forwarding Rate	19.344Mpps	53.568Mpps	65.472Mpps			160.704Mpps	
Packet Buffer	8.4Mb						
Network Latency	<4us						
Power Supply							
Power Supply	100-240V~ 50/60Hz						
Redundant Power Supply	/		1+1 External RPS, One by default	/	1+1 External RPS, One by default		
External Redundant Power Supply (RPS)	/		30W	/	460W		800W
Max Power Consumption	9.5W / 145.5W (PoE 130W)	21.8W / 294.4W (PoE 250W)	21.4W	27.5W / 299.2W (PoE 250W)	30.5W / 471.4W (PoE 400W)	65.4W / 509.3W (PoE 400W)	68.0W / 870.9W (PoE 800W)
Max Output Power	145.5W	294.4W	21.4W	299.2W	471.4W	509.3W	870.9W
PoE							
PoE Standards	IEEE 802.3af/at	IEEE 802.3af/at/bt	/	IEEE 802.3af/at	IEEE 802.3af/at/bt	IEEE 802.3af/at	IEEE 802.3af/at/bt
# of PoE Ports	8	16	/	24		48	
Max Output Power per PoE Port	30W	60W	/	30W	60W	30W	60W
Max Total PoE Output Power	130W	250W	/	250W	400W		800W
Physical							

Unit Dimension	330mm(L) x 175mm(W) x 44mm(H)	440mm(L) x 200mm(W) x 44mm(H)			440mm(L) x 300mm(W) x 44mm(H)		
Unit Weight	1.77Kg	2.9Kg	2.5Kg	3.06Kg	4.15Kg	5.05Kg	5.3Kg
Mounting	Desktop, Wall-Mount, or Rack-Mount (rack-mounting kits included)				Desktop, or Rack-Mount (rack-mounting kits included)		
Package Content	1x Switch 1x 25cm Ground Cable 4x Rubber Footpads 1x Power Cord Anti-Trip 8x Screws (KM3*6) 1x 1.2m(10A) AC Cable 1x Simplified Quick Installation Guide 1x Regulatory Paper						
	1x Extended Rack-Mounting Kits	2x Rack-Mounting Kits					
Environmental							
Temperature	Operation: 0°C to 45°C Storage: -10°C to 60°C						
Humidity	Operation: 10% to 90% RH (Non-condensing) Storage: 5% to 95% RH (Non-condensing)						
MTBF	7000H						
Fan	/	2	/	2	3	4	
CPU Monitoring	Monitoring CPU usage, over-CPU usage alarming						
Memory Usage	Monitoring memory usage, over-memory usage alarming						
Power Supply Monitoring	Monitoring of power supply model and status power supply failure alarming						
Fan Monitoring	Automatic speed adjustment fan failure alarming						
Temperature Monitoring	Temperature monitoring, over-temperature alarming						
Surge Protection	± 6KV CM for power ± 4KV CM for network ports						
ESD	± 12KV for contact discharge						
Compliance	FCC, CE, RCM, IC						
Software Specifications							
Network Protocol	IPv4, IPv6, IEEE 802.3, IEEE 802.3i, IEEE 802.3u, IEEE 802.3ab, IEEE 802.3z, IEEE 802.3ae, IEEE 802.3az, IEEE 802.3ad, IEEE 802.3x, IEEE 802.3af/at/bt, IEEE 802.1p, IEEE 802.1Q, IEEE 802.1d, IEEE 802.1w, IEEE 802.1s, IEEE 802.1x						
Stacking	/					Yes, up to 8 devices	
Switching	* Jumbo frame (maximum length: 12288) * 4K VLANs, port-based VLAN, IEEE 802.1Q VLAN tagging * QinQ * MAC-based VLAN * Protocol-based VLAN * Voice VLAN including auto voice VLAN, tagged OUI and untagged OUI * GVRP(pending) * ERPS						
	Spanning tree, support STP/RSTP/MSTP/PVST(+)/RPVST(+), 16 instances for MSTP/PVST(+)/RPVST(+)					Spanning tree, support STP/RSTP/MSTP/PVST(+)/RPVST(+), 64 instances for MSTP/PVST(+)/RPVST(+)	
	/					Private VLAN	
	16K MAC addresses including static, dynamic and filtering MAC address					32K MAC addresses including static, dynamic and filtering MAC address	
	Link aggregation, including static and LACP					Link aggregation, including static and LACP	
	Up to max 8 LAG groups and up to 8 members per LAG group					Up to max 32 LAG groups and up to 8 members per LAG group	
IP Service	* DHCP client, DHCP server, DHCP relay and DHCP snooping * DHCPv6 client and DHCPv6 snooping * ND snooping * DNS						

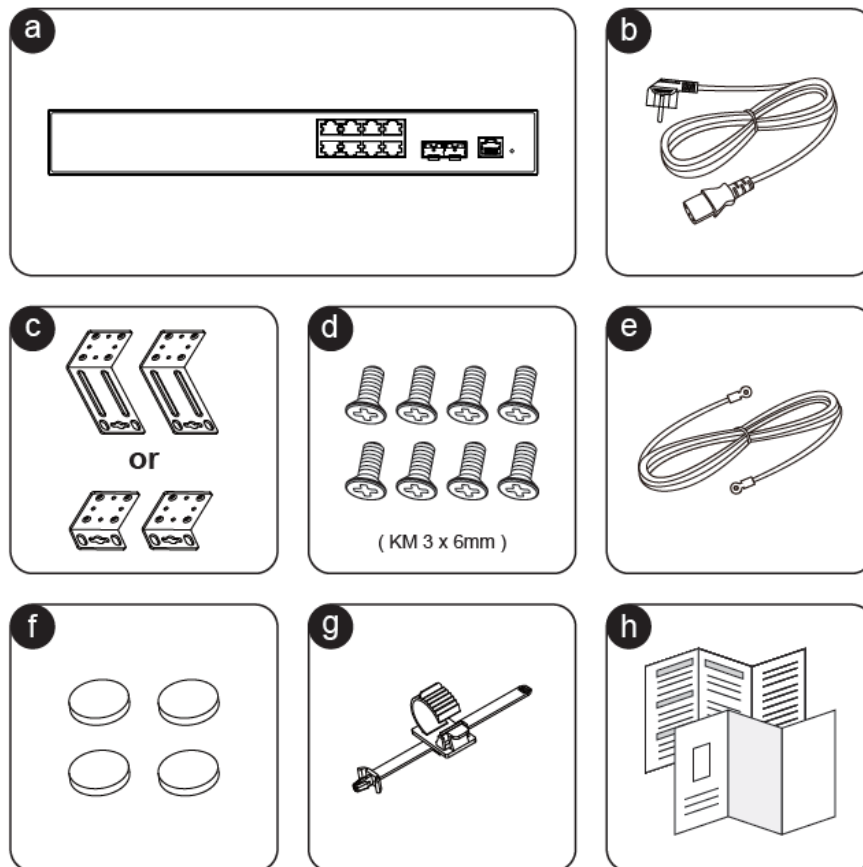
IP Service	64 ARP/NDP, including static and dynamic ARP/NDP		1K ARP/NDP, including static and dynamic ARP/NDP
	16 VLAN virtual interfaces with 9216 MTU		512 VLAN virtual interfaces with 9216 MTU
IP Routing	Policy routing (GWN7806PH Pro / GWN7806PL Pro)		
	32(IPv4)/32(IPv6) static routes		1K(IPv4)/1K(IPv6) static routes
Multicast	IGMP Snooping with IGMPv2 and IGMPv3, 256 IGMP Snooping groups	IGMP Snooping with IGMPv2 and IGMPv3, 384 IGMP Snooping groups	IGMP Snooping with IGMPv2 and IGMPv3, 640 IGMP Snooping groups
	MLD Snooping with MLDv1 and MLDv2, 256 MLD Snooping groups	MLD Snooping with MLDv1 and MLDv2, 384 MLD Snooping groups	MLD Snooping with MLDv1 and MLDv2, 640 MLD Snooping groups
QoS	* Port priority * Priority mapping, including 802.1p mapping, DSCP mapping and IP precedence mapping * Queue scheduling, including SP, WRR, WFQ, SP-WRR and SP-WFQ * Traffic shaping * Rate limit		
ACL	128 ACL for Ethernet, IPv4 and IPv6 with 1.5K ACE		256 ACL for Ethernet, IPv4 and IPv6 with 4K ACE
	* MAC ACLs (hardware ACLs based on source MAC address, destination MAC address, optional Ethernet type, and time range) * IPv4 ACLs (hardware ACLs based on source IP address, destination IP address, and optional protocol type, and time range) * IPv6 ACLs (hardware ACLs based on source IPv6 address, destination IPv6 address, and optional protocol type, and time range) * Expert ACLs (hardware ACLs based on flexible combinations of the VLAN ID, Ethernet type, MAC address, IP address, protocol type, and time range) (TBD) * Customized ACLs (ACL80) (TBD) * ACL redirection * ACL advanced settings, including statistics, mirror, priority mapping, and rate limit * ACL binding, including port and VLAN		
Security	* User hierarchical management and password protection, HTTPS, SSH, Telnet * Identity authentication, including 802.1X and MAC authentication * AAA authentication, including RADIUS, TACACS * Storm control * Port isolation * Port security, sticky MAC address, filtering invalid MAC addresses * IP/IPv6 source guard, DoS attack prevention, ARP inspection, CPU protection * Loop protection, including port loopback detection, BPDU protection, root protection, and loopback protection * Kensington Security Slot (Kensington Lock) support * Firmware signature		
Reliability	* Power supply modules in 1+1 redundancy mode * Stack intelligent upgrade		
Maintenance	* NTP * 1588v2 TC for precise time * CPU and memory monitoring * Fault detection and alarm for power supply and fan * SNMP including SNMPv1, SNMPv2c, SNMPv3 * RMON including history groups, event groups, alarm groups, and statistics groups * LLDP&LLDP-MED * Backup and restore * Syslog * Diagnostics including Ping, traceroute, Ping watchdog, mirror including SPAN and RSPAN, UDLD(TBD), copper test, fiber module, and one-click debugging * sFlow (GWN7806PH Pro / GWN7806PL Pro) * Upgrade via FTPS/ TFTP/ HTTP/ HTTPS or local upload, mass provisioning using DHCP Option/ TR-069 (pending)/ GDMS Networking/ GWN Manager/ GWN series routers		
Management Platform	* Local Web GUI: embedded controller * GDMS Networking: free cloud management platform for unlimited GWN78x0 Pro series switches * GWN Manager: premise-based software controller * GWN APP: integrated GDMS Networking and GWN Manager to manage GWN78x0 Pro series switches via the APP * Management Protocol: SNMP, RMON, TR-069 (pending)		

INSTALLATION

Before deploying and configuring the switches, the device needs to be properly powered up and connected to the network. This section describes detailed information on the installation, connection, and warranty policy of the GWN780x Pro switches.

Package Content

The package content that comes with the GWN780x Pro product contains the following elements.



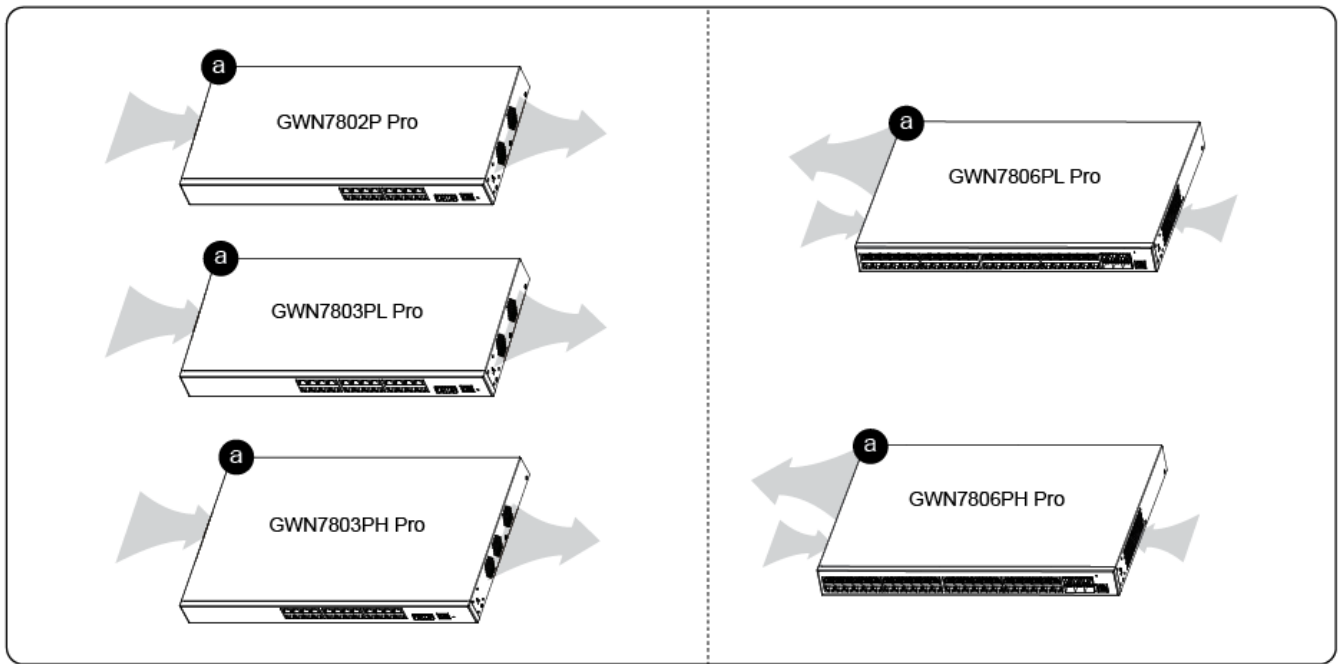
GWN780x Pro Package Content

a	GWN780x Pro Series
b	1x 1.2m (10A) AC Cable
c	Rack Mounting Kits or Extended Rack Mounting Kits
d	8x Screws (KM 3 x 6mm)
e	1x 25cm Ground Cable
f	4x Rubber Footpads
g	1x Power Cord Anti-Trip
h	Quick installation Guide and Regulatory Paper

GWN780x Pro Package Content

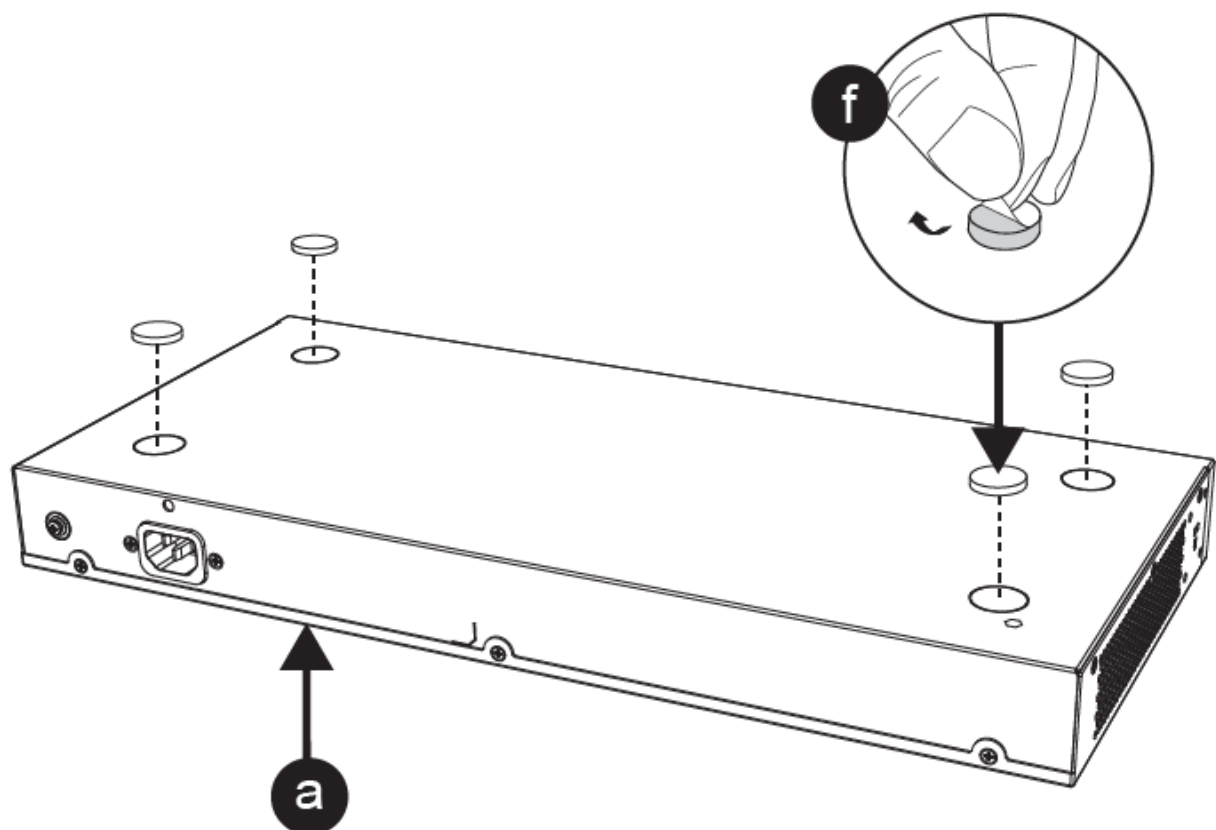
Fan Ventilation

The GWN780x Pro series features a dedicated ventilation system designed to keep the device cool in deployments where it delivers significant power to connected devices. This power delivery increases the device's workload and internal temperature. Depending on the model, the cooling mechanism and number of fans can vary. The illustration below highlights these differences:



GWN780x Pro Fan Ventilation

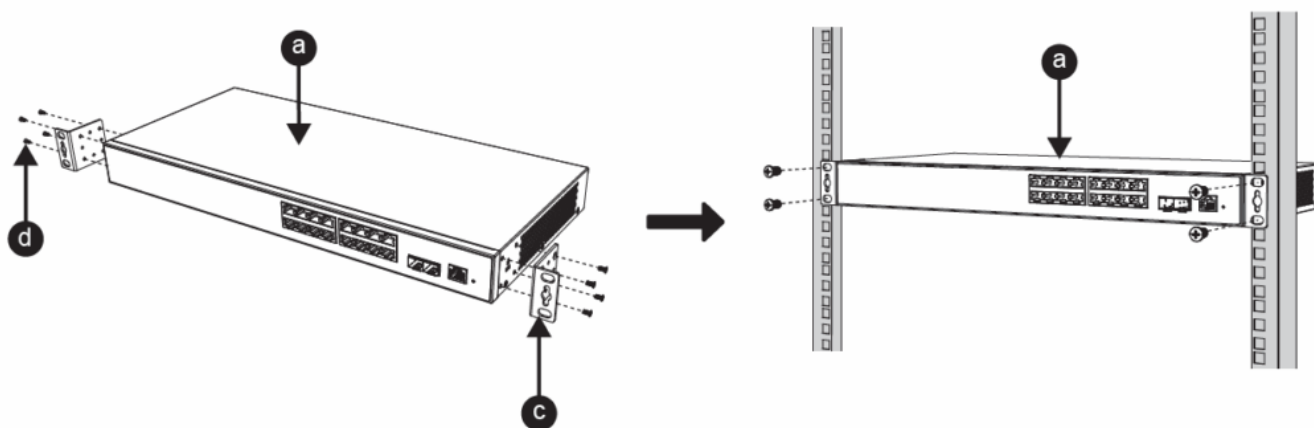
Install on the Desktop



Desktop Installation

1. Place the bottom of the 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 a 19" Standard Rack



Install on a 19 Standard Rack

1. Check the grounding and stability of the rack.
2. Install the two L-shaped rack-mounting accessories on both sides of the switch, and fix them with the screws provided (KM 3*6).
3. Place the switch in a proper position in the rack and support it with 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 GWN780x Pro

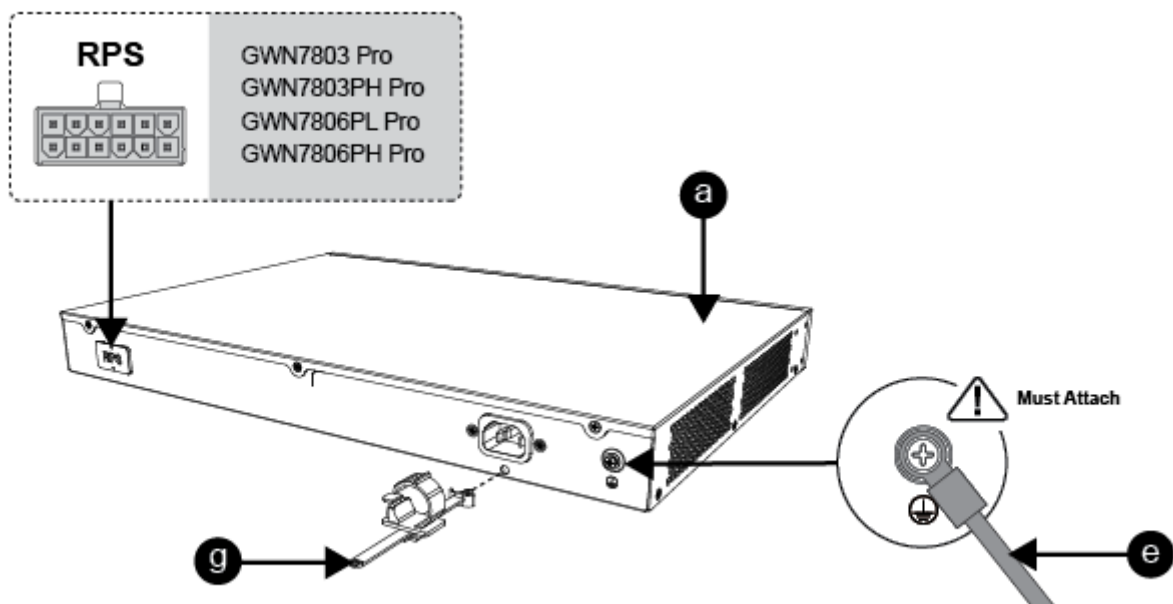
Connect the power cable and the switch first, then connect the power cable to the power supply system of the equipment room.

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

1. Place the smooth side of the fixing strap towards the power outlet and insert it into the hole on the side of it.
2. After plugging the power cord into the power outlet, slide the protector over the remaining strap until it slides over the end of the power cord.
3. Wrap the strap of the protective cord around the power cord and lock it tightly. Fasten the straps until the power cord is securely fastened.
4. Connect the RPS for the following models: GWN7803 Pro, GWN7803PH, GWN7806 Pro, GWN7806PL, GWN7806PH Pro

Connect the Grounding cable by following the steps below:

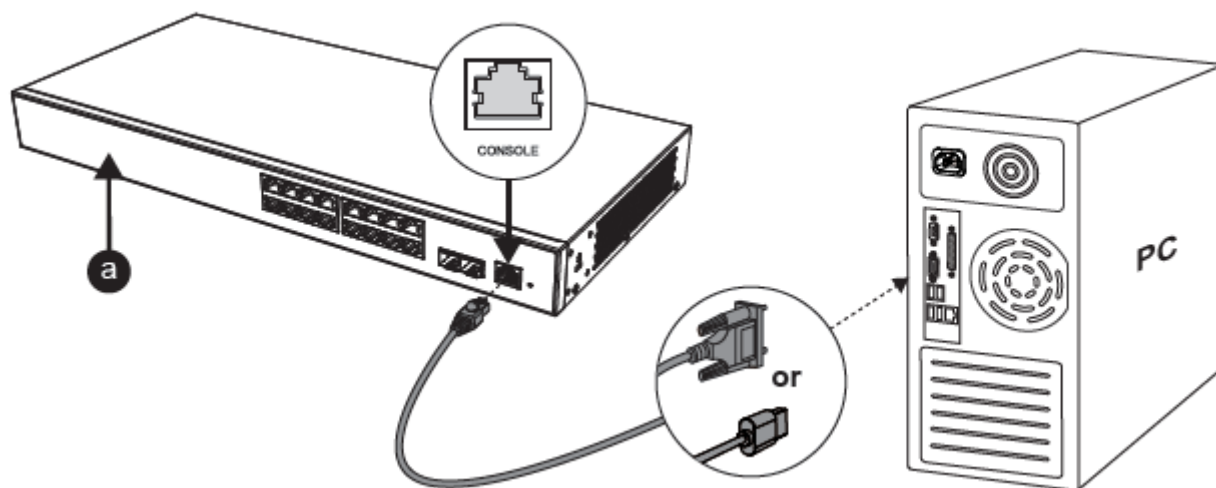
1. Remove the ground screw from the back of the switch, and connect one end of the ground cable to the wiring terminal of the switch.
2. Put the ground screw back into the screw hole, and tighten it with a screwdriver.
3. Connect the other end of the ground cable to another device that has been grounded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



Powering and Connecting GWN780x Pro

Connect to Console Port

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



Connect to Console Port

GETTING STARTED

LED Indicators

The front panel of the GWN780x Pro 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

System Indicator	Solid green	Booting
	Flashing green	Upgrade
	Solid blue	Normal use
	Flashing blue	Provisioning
	Solid red	Upgrade failed
	Flashing red	Factory reset
Port Indicator	Off	For all ports: port off For SFP/SFP+ ports: port failure
	Solid green	Port connected and there is no activity
	Flashing green	Port connected and data is transferring
	Solid yellow	Ethernet port connected, and there is no activity and PoE powered
	Flashing yellow	Ethernet port connected, data is transferring and PoE powered
	Alternately flashing yellow and green	Ethernet port failure
PWR/RPS Indicator	Off	Uninserted or failure
	Solid Green	In use/Inserted but not used (only for RPS)

LED Indicators

Access & Configure

Login Using the Console Port

1. Use the console cable to connect the console port of the switch and the serial port of the PC.
2. Open the terminal emulation program of PC (e.g., SecureCRT), enter the default username and password to log in. (The default administrator username is "admin" and the default random password can be found on the sticker on the GWN780x Pro switch).

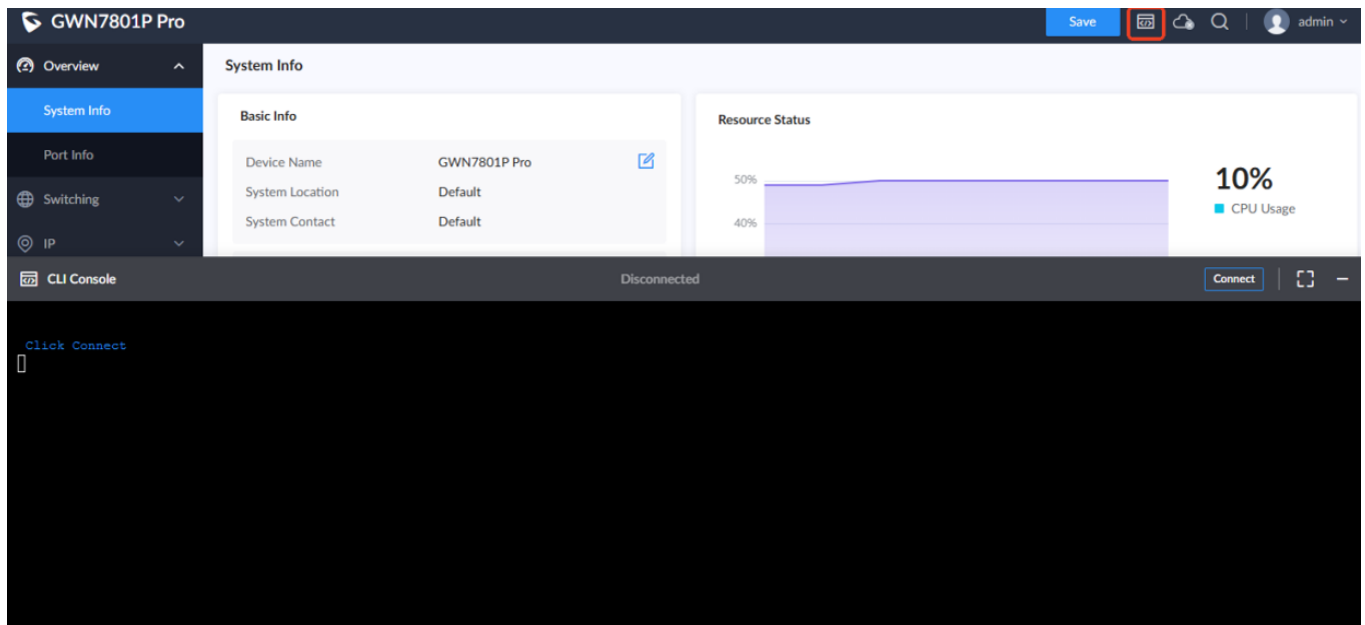
Login Remotely Using SSH

1. Enter **"cmd"** in PC/Start.
2. Enter **ssh <gwn780x Pro_IP>** in the cmd window.
3. Enter the default username and password to log in. (The default administrator username is "admin" and the default random password can be found on the sticker on the GWN780x Pro switch).

Web CLI

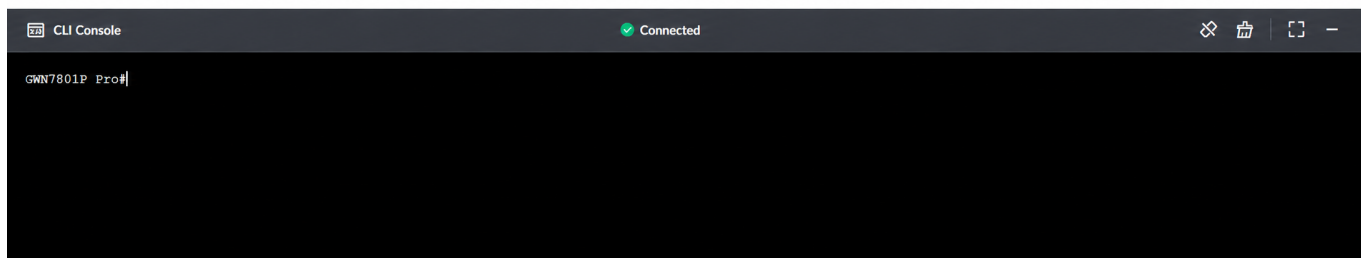
Web CLI provides access to the switch command-line interface directly from the Web UI, without opening a separate terminal application. Use it to run supported commands for configuration, status checks, and troubleshooting.

Click the **CLI Console** icon in the upper-right toolbar to open the console panel, then click **Connect** to start a CLI session.



Opening the Web CLI Console

When the status changes to **Connected**, enter a supported CLI command at the prompt and press **Enter**. Command output appears in the console. For command syntax and available operations, see the GWN78xx CLI User Guide.



Connected Web CLI Session Illustrative

Use the controls on the right side of the console header to **Disconnect** the session, **Clear the screen**, switch to **Full-screen Display**, or **Minimize** the panel. Disconnect when you have finished using the CLI.

Configure Using GDMS Networking

Sign in to GDMS Networking and add the switch to the trusted account. From the Devices page, the **Remote Access** operation opens the switch Web UI through GDMS. The same passwordless remote-access workflow is available through GWN Manager. Enable it on the switch under **System -> Access Control -> Passwordless Remote Access**; management-platform access remains restricted to authorized platform users.

Login Using the Web UI

The GWN780x Pro 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.



Managed Network SWITCH

Plug-and-play connectivity with customized controls and configurations to extend your network



Sign In to GWN7801P Pro

Username

Password

Sign In

© 2025 Grandstream Networks, Inc. [Grandstream Software License Agreement](#) | English ▾

Login Using the Web UI

1. A PC uses a network cable to correctly connect any RJ45 port of the switch.
2. Set the Ethernet (or local connection) IP address of the PC to 192.168.0.x ("x" is any value between 1-253), and the subnet mask to 255.255.255.0, so that it is in the same network segment as the switch IP address. If DHCP is used, this step could be skipped.
3. Type the switch's default management IP address **https://<GWN780x Pro_IP>** in the browser, and enter the username and password to log in. (The default administrator username is "admin" and the default random password can be found on the sticker on the GWN780x Pro switch.)

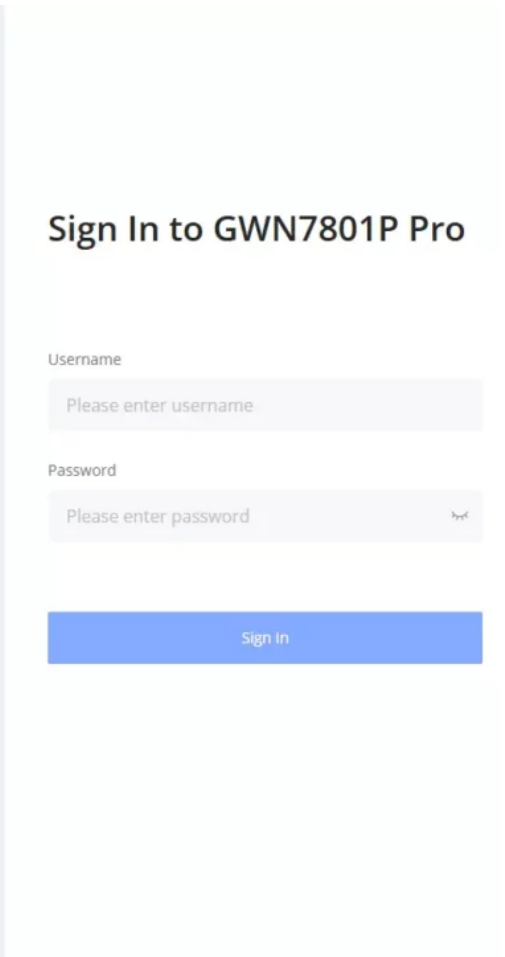
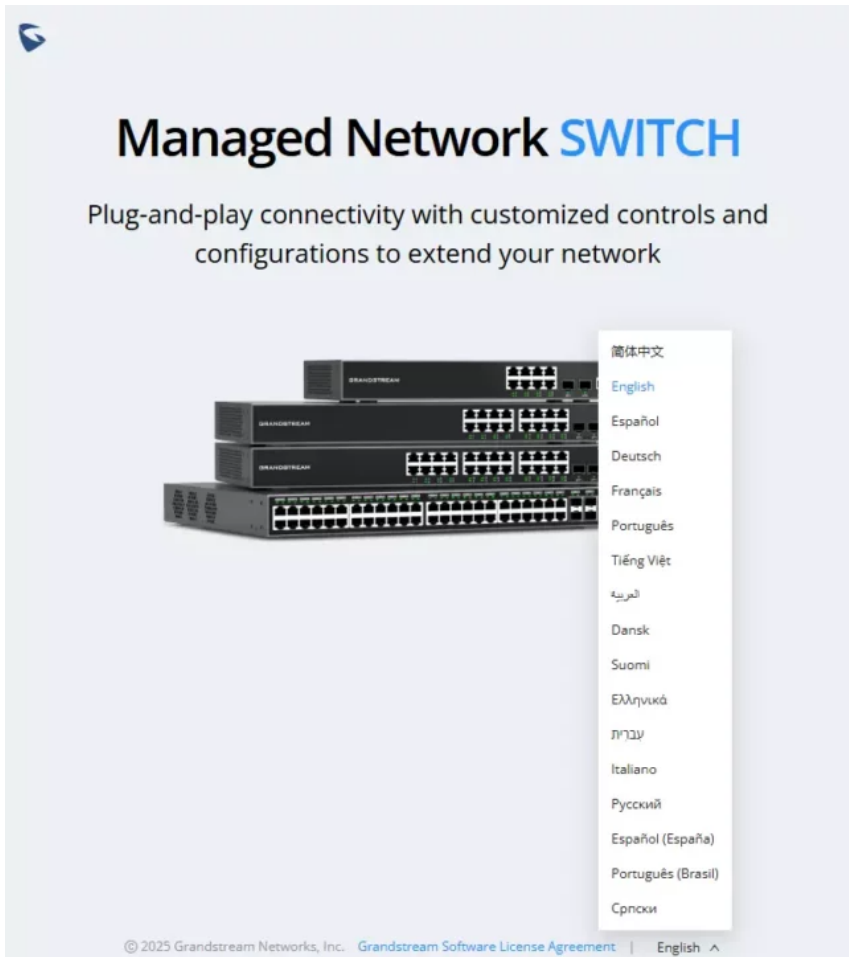
CLI Access

The GWN780x Pro series supports local, SSH, and Web CLI access. CLI output can be filtered with the pipe (|) operator. For the command reference, refer to the GWN78xx CLI User Guide.

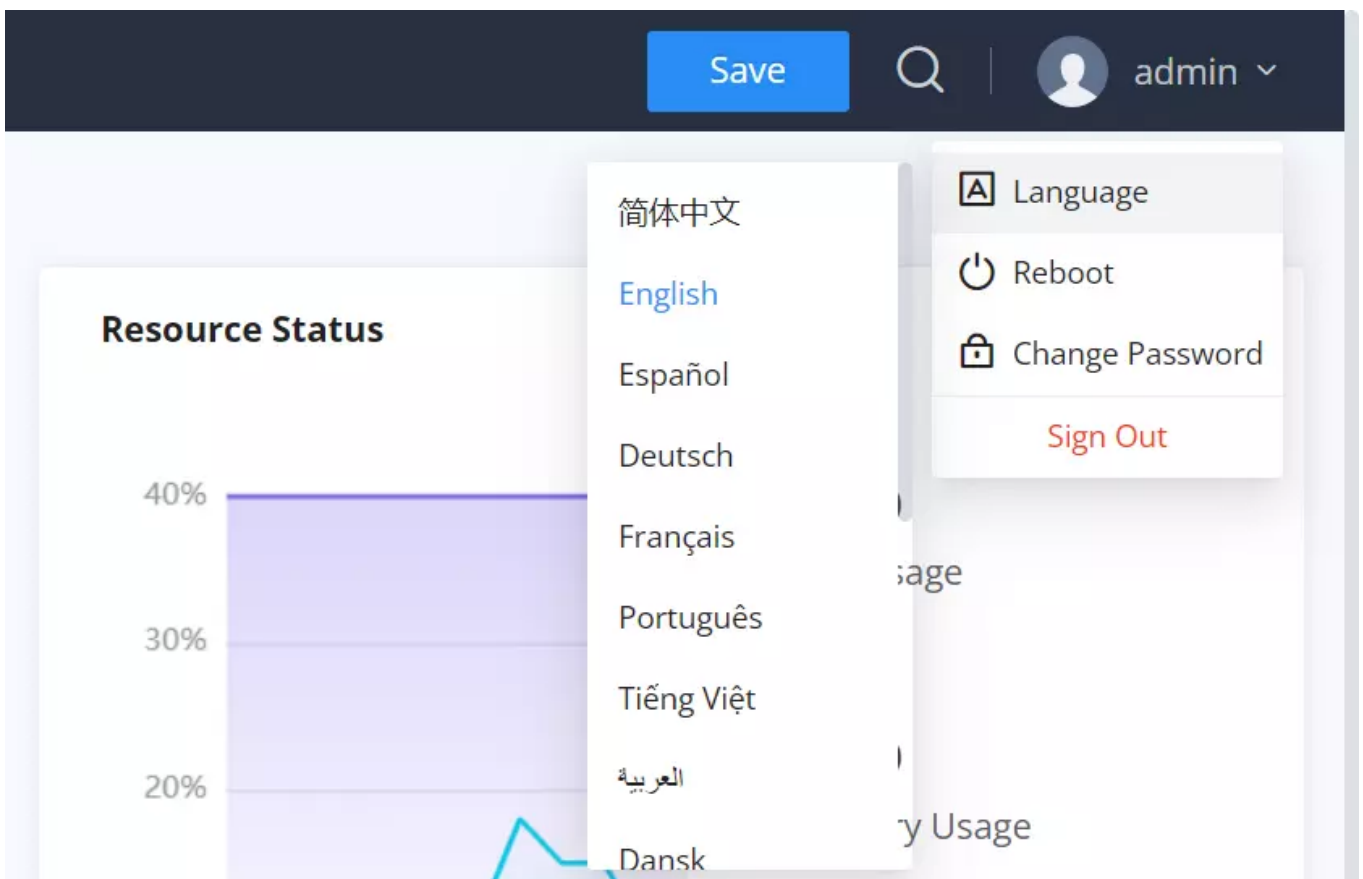
Web GUI Languages

The GWN780x Pro 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

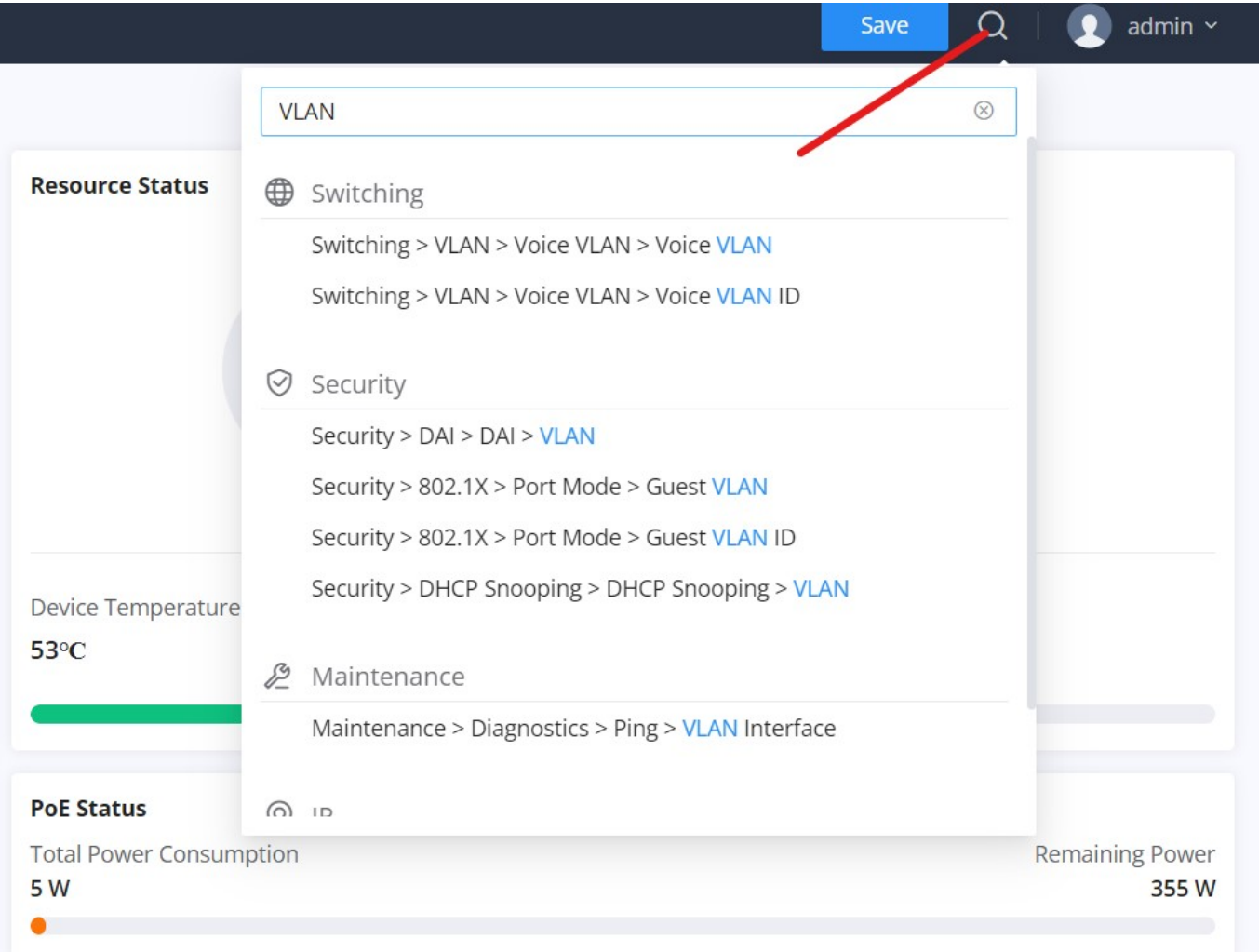


WEB GUI Start page

Search

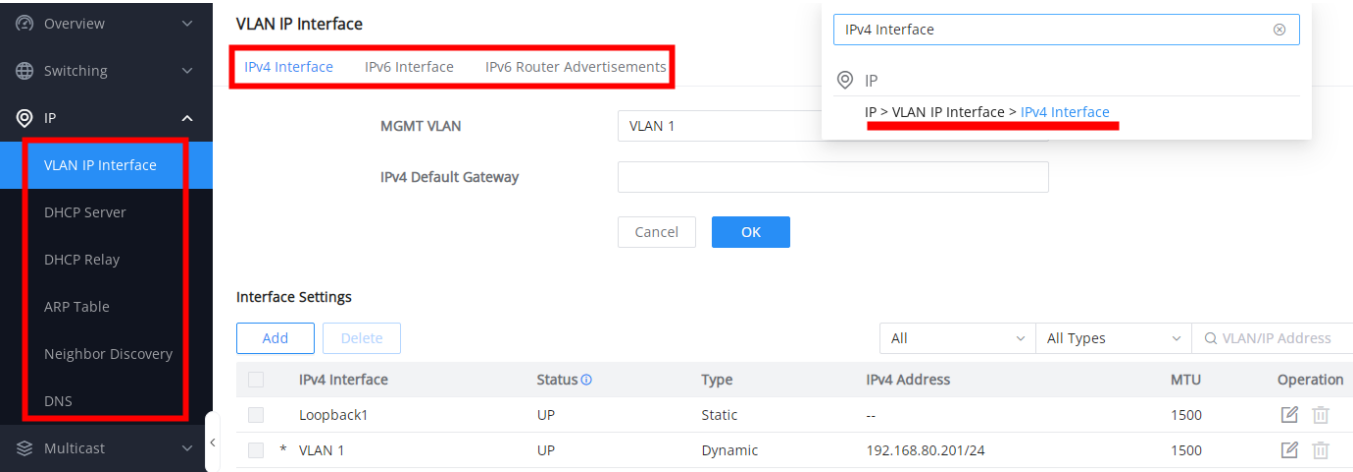
In case it's hard to go through every single section, GWN780x Pro Switches have search functionality to help the user find the right configuration, settings, or parameters, etc.

At the top of the page, there is a search icon. The user can click on it and then enter the keyword relevant to their search, and then they 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 of the GWN780x Pro system and port status for easy monitoring.

System Info

System Info is the first page after a successful login to the GWN780x Pro Web Interface. It provides an overall view of the GWN780x Pro Switch information presented in a Dashboard style for easy monitoring, including basic info, Resource Status, PoE Status, and System Events.

System Info

Basic Info

Device Name	GWN7801P Pro	✎
System Location	Default	
System Contact	Default	

MAC Address	EC:74:D7:8E:07:0E
System OID	1.3.6.1.4.1.40887
Part Number	96400
Serial Number	35800

MGMT VLAN	VLAN 1
IPv4 Address	172.16.142.28
IPv6 Global Unicast Address	::
IPv6 Link Local Address	::

IPv4 Default Gateway	172.16.142.1
IPv6 Default Gateway	::

System Time	2025-10-14 17:30:27 (UTC+08:00) Beiji
System Uptime	5 days, 8 hours, 21 minutes
System Version	1.0.0
Hardware Version	V1.0
Boot Version	1.0.0

Resource Status

Time	CPU Usage (%)	Memory Usage (%)
17:31:55	2	55
17:32:05	32	55
17:32:15	2	55
17:32:25	2	55
17:32:35	2	55
17:32:45	3	55

Total Power Consumption

0 W

Remaining Power

120 W

System Events

🔴 Emergency 0 >	🔴 Critical 2 >
🟡 Alert 0 >	🟡 Error 0 >
🟡 Warning 12 >	🟢 Information 0 >
🟢 Notification 5248 >	🔍 Debug 0 >

System Info

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

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

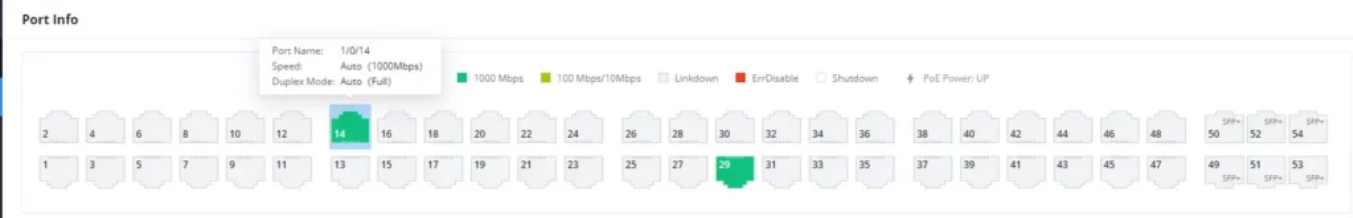
System Info page

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.

- 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

- 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.

Click on the port above to view port information

Basic Info	Neighbor Info
Port Name: 1/0/24 Port Description: -- Port Status: Up Speed: Auto (1000Mbps) Duplex Mode: Auto (Full) Flow Control: Disabled (Off) Jumbo Frame: 9216	Hostname: GWN7803P Device ID: C0:74:AD:BA:24:FC IPv4 Address: 192.168.80.37 IPv6 Address: -- Manufacturer: Grandstream Networks, Inc. Current Rate: 41.17Kbps 0bps Current Pkts/Bytes: 205168407 / 124.82MB 199820233 / 3.47GB Up Time: 5 hours, 24 minutes

Port Info page 2

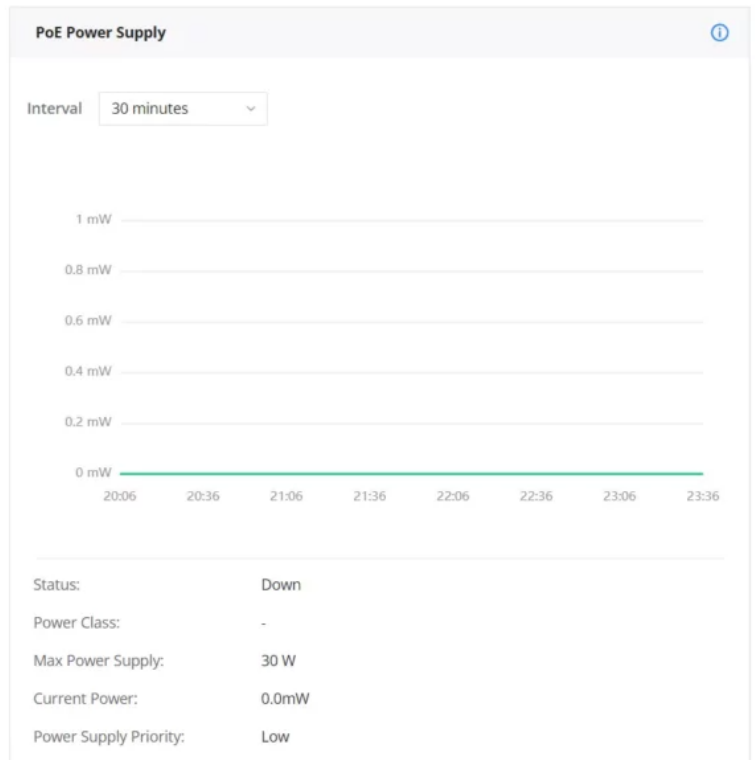
- Statistics

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.

- PoE Power Supply / Fiber Info

If the selected port is PoE-capable, the "PoE Power Supply" section shows power supply status and usage. If the port is SFP, the "Fiber Info" section displays details like signal loss, temperature, RX, and TX power.

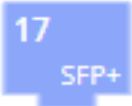
Statistics	
InOctets:	130986829
InUcastPkts:	65659
InNUcastPkts:	205103115
InDiscards:	0
OutOctets:	3727239001
OutUcastPkts:	47410
OutNUcastPkts:	199773098
OutDiscards:	0
InMulticastPkts:	100627720
InBroadcastPkts:	104475395
OutMulticastPkts:	84691835
OutBroadcastPkts:	115081263



Port Info page 3

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

	Grey: Linkdown
	White: shutdown
	Green: Ethernet RJ45 port with 1000 Mbps speed
	Light green: Ethernet RJ45 port with 100 Mbps/10 Mbps speed
	Red: ErrDisable
	Green: SFP/SFP+ Port set to 1000Mbps

	Purple: SFP/SFP+ Port set to 2.5Gbps Note: only for GWN7801P pro, GWN7802P Pro, GWN7803(PL/PH) Pro
	Blue: SFP+ port set to 10Gbps Note: only for GWN7802P Pro, GWN7803(PL/PH) Pro and GWN7806PL/PH Pro
	Symbol: PoE Power is enabled.

Port Info

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

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.
- **PoE Power Supply / Fiber Info:** The details icon forwards users to the respective detailed pages. For PoE, it forwards to the PoE Interface page, showing detailed information about PoE settings for each port. For 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

The switching section is used to configure port settings, link Aggregation, VLAN, Spanning Tree, etc.

Port Basic Settings

Use **Switching -> Port Basic Settings** to enable or disable a port, add a description, select its speed and duplex mode, configure jumbo frames and flow control, or apply an enable schedule. Copper and optical ports can be filtered and managed separately.

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

Port Basic Settings

Edit							All Ports
☒	Port	Port Type	Description	Status	Link Status	Speed	
☒	1/0/1	Copper	GWN76xx	Enabled	Down	Auto	
☒	1/0/2	Copper	Guests	Enabled	Down	Auto	
☒	1/0/3	Copper	--	Enabled	Down	Auto	Auto
☒	1/0/4	Copper	--	Enabled	Down	Auto	Auto
☒	1/0/5	Copper	--	Enabled	Down	Auto	Auto
☒	1/0/6	Copper	--	Enabled	Down	Auto	Auto
☒	1/0/7	Copper	--	Enabled	Down	Auto	Auto
☒	1/0/8	Copper	--	Enabled	Down	Auto	Auto
☒	1/0/9	Copper	--	Enabled	Down	Auto	Auto

Port Basic Settings

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

Port Basic Settings > Edit Port

Port	1/0/28
Port Type	SFP+
Description	0-128 characters
Port Enable	☒ Enable ☐ Disabled
Scheduled enabled	None
Auto Detect	☐
Speed	10Gbps
DAC Cable	Disabled
Duplex Mode	☒ Full
*Jumbo Frame	9216 Valid range is 1518-10000
Flow Control	☒ Disabled ☐ Enabled Flow Control setting will not take effect if Duplex Mode is set to "Half".
	Cancel OK

Port Basic Settings Edit port

Users can define schedules for specific ports, this is to enable precise control over when configurations are applied. These schedules dictate the exact times during which port settings will take effect.

Port	1/0/2
Port Type	Copper
Description	0-128 characters
Port Enable	☒ Enable ☐ Disabled
Scheduled enabled	None
Speed	None Working Hours Add
Duplex Mode	
Jumbo Frame	9216 Valid range is 1518-12288
Flow Control	☒ Disabled ☐ Enabled ☐ Auto Flow Control setting will not take effect if Duplex Mode is set to "Half".
	Cancel OK

Port Basic Settings scheduled enabled

For SFP+ ports that support a selectable operating mode, choose the **2.5 Gbps/10 Gbps** mode, save the configuration, and reboot the switch before selecting the corresponding speed on an individual optical port.

Port Basic Settings

Port Basic Settings Port Group SFP+ Speed Mode

 The speed mode will take effect after saving and rebooting the device.

Port	Speed Mode
1/0/49-1/0/50	☒ 100Mbps/1000Mbps/10Gbps ☐ 2.5Gbps/10Gbps
1/0/51-1/0/52	☒ 100Mbps/1000Mbps/10Gbps ☐ 2.5Gbps/10Gbps
1/0/53-1/0/54	☒ 100Mbps/1000Mbps/10Gbps ☐ 2.5Gbps/10Gbps

SFP+ Speed Mode

Port	The selected Gigabit Ethernet or SFP/SFP+ port.
Port Type	Displays the port type (Copper or SFP/SFP+).
Description	Describes the interface and its intended use. Up to 128 characters are supported.
Port Enable	Enables or disables the interface. The interface is enabled by default.
Scheduled Enabled	Selects the schedule during which the physical or LAG port is enabled.

Speed	Copper ports: Auto, 10 Mbps, 100 Mbps, or 1000 Mbps. The default is Auto. GWN7801P Pro optical ports: 100 Mbps, 1000 Mbps, or 2.5 Gbps. The default is 2.5 Gbps. GWN7802P Pro, GWN7803 Pro, GWN7803PL Pro, GWN7803PH Pro, GWN7806PL Pro, and GWN7806PH Pro optical ports: 100 Mbps, 1000 Mbps, 2.5 Gbps, or 10 Gbps. The default is 10 Gbps. To use 2.5 Gbps on an SFP+ port, first select the 2.5 Gbps/10 Gbps SFP+ speed mode, save the configuration, reboot the switch, and then set the port speed to 2.5 Gbps. When using a fixed speed, configure the peer port with the same value.
Duplex Mode	Gigabit Ethernet ports support Auto-negotiation, Full-duplex, and Half-duplex. Optical ports support Full-duplex only. Configure the peer port with the same fixed mode.
Jumbo Frame	Sets the jumbo-frame size from 1518 to 12288 bytes. The default is 9216 bytes.
Flow Control	Sets flow control to Disabled, Enabled, or Auto. The default is Disabled. Optical ports do not support Auto-negotiation mode.

Port Group

The port group feature allows administrators to logically bundle specific ports together under one group with a corresponding group ID. This can be useful when classifying the switch ports for identifying the usage of each set of ports, for example, ports 1 to 4 and LAG 1 and 2 can be set with ID 20, which will be the ports connecting Security devices.

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

Port Group > Add Port Group

ID

20

Valid range is 1-32

Description

Security Devices

0-128 characters, including digits, letters and special characters except ^?/,

Click on port to select/unselect

Port

2

4

6

8

1

3

5

7

9 SFP1

10 SFP2

LAG

2

4

6

8

1

3

5

7

Port Group

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

VLAN

20

Description

VLAN20

Member Type

All Ports

Port

Click port to change the member type

All Ports

20(Security Devices)

T Tagged

U Untagged

2

4

6

8

1

3

5

7

9 SFP1

10 SFP2

Port Group Selection

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

Port Basic Settings

Port Basic Settings

Port Group

Edit

Port Group2

All Ports

☐	Port	Port Type	Description	Status	Link Status	Speed	Duplex	Control	Operation
☐	1/0/1	Copper	--	Enable	Down	Auto	Auto	Disabled	
☐	1/0/2	Copper	--	Enable	Down	Auto	Auto	Disabled	
☐	1/0/3	Copper	--	Enable	Down	Auto	Auto	9216 Disabled	
☐	1/0/4	Copper	--	Enable	Down	Auto	Auto	9216 Disabled	
☐	1/0/5	Copper	--	Enable	Down	Auto	Auto	9216 Disabled	
☐	1/0/6	Copper	--	Enable	Down	Auto	Auto	9216 Disabled	

Delete Port Group

Port Statistics

Port Statistics displays Tx and Rx rate, utilization, bytes, packets, error packets, and queue-dropped packets in real time. Select a refresh interval, clear all counters, or open the operation control for a specific port.

Port Statistics

Clear All

Tx

Rx

Refresh Interval 10s

Port	Rate (bps)	Usage	Bytes	Packets	Error Packets	Queue Dropped Packets	Operation
1/0/1	--	--	--	--	--	--	① ↗
1/0/2	--	--	--	--	--	--	① ↗
1/0/3	--	--	--	--	--	--	① ↗
1/0/4	--	--	--	--	--	--	① ↗
1/0/5	--	--	--	--	--	--	① ↗
1/0/6	--	--	--	--	--	--	① ↗
1/0/7	--	--	--	--	--	--	① ↗
1/0/8	--	--	--	--	--	--	① ↗
1/0/9	--	--	--	--	--	--	① ↗
1/0/10	--	--	--	--	--	--	① ↗

Total 86

<

1

2

3

...

9

>

10 / page

Go to

Port Statistics with Queue Dropped Packets

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

Port Statistics

Statistics

Clear All

Port	R
1/0/1	4
1/0/2	--
1/0/3	--
1/0/4	--

Port:1/0/1

Refresh Clear

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

utOctets	OutPackets	Operation
748971	35826	① ↗
--	--	① ↗
--	--	① ↗
--	--	① ↗

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.

Loopback Detection

Loopback Detection



Cancel

OK

Port

Edit

Refresh

☐	Port	Loopback Detection	Detection Status	Port Status	Time Left (s)	Operation
☐	1/0/1	Disabled	Disabled	normal	0	
☐	1/0/2	Disabled	Disabled	normal	0	
☐	1/0/3	Disabled	Disabled	normal	0	
☐	1/0/4	Disabled	Disabled	normal	0	
☐	1/0/5	Disabled	Disabled	normal	0	

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 the 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 the 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.

Port Auto Recovery

Recovery Items

- ☒ All
- ☒ ARP Packet Detection
- ☒ DHCP Rate Limit
- ☒ Broadcast Storm Control
- ☒ Unknown Multicast Storm Control
- ☒ BPDUs Selfloop
- ☒ Port Security
- ☒ STP BPDU Guard
- ☒ DHCPv6 Rate Limit
- ☒ Unicast Storm Control
- ☒ Port Selfloop
- ☒ ACL

Delay Time (s)

30

Valid range is 30-86400

Cancel

OK

Port

Refresh

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

Port Auto Recovery

Link Aggregation

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

Link Aggregation Group

There are two load balance modes on the GWN780x Pro 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 LACP7 or Link Aggregation Control Protocol, both are supported.

Link Aggregation

Group

LAG Settings

LACP

Load Balance Mode

MAC Address

Cancel

OK

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

Link Aggregation Group

Load Balancing Mode	Select your Load balance mode. MAC address - Aggregated group will balance the traffic based on different MAC addresses. Therefore, the packets from different MAC addresses will be sent to different links. IP/Mac Address - Aggregated group will balance the traffic based on MAC addresses and IP addresses. Therefore, the packets from same MAC addresses but different IP addresses will be sent to different links.
Edit Group	Name: Enter the name of the LA Group. Type: Use the drop down menu to specify the type for LAG. Static- The static aggregated port sends packets over active member without detecting or negotiating with remote aggregated port. LACP- The LACP aggregated ports place member into active only after negotiated with remote aggregated port for best reliability. GE: Click on port to check / uncheck which ones will be part of this LAG.

Link Aggregation Port

LAG Port Settings

On this page, the user can enable the Link Aggregation Group and add a Description as well as specify the speed and the flow control for LAG.

Link Aggregation

Group

LAG Settings

LACP

Edit

☐ Port	Description	Status	Link Status	Speed	Jumbo Frame	Flow Control	Operation
☒ LAG1	--	Enable	Down	1000Mbps	9216	Disabled	
☐ LAG2	--	Enable	Down	1000Mbps	9216	Disabled	
☐ LAG3	--	Enable	Down	1000Mbps	9216	Disabled	
☐ LAG4	--	Enable	Down	1000Mbps	9216	Disabled	
☐ LAG5	--	Enable	Down	1000Mbps	9216	Disabled	
☐ LAG6	--	Enable	Down	1000Mbps	9216	Disabled	

Link Aggregation Port Settings

Port	The selected LAG to be configured.
Description	It is used to configure the information description for this LAG , which can be a description of usage, etc., with a maximum of 128 characters, and the characters limited to input are numbers 0-9 , letters az / AZ and special characters.
Port Enable	Set whether to enable the interface. it is enabled by default.
Speed	Set the rate of the interface, the options are {Auto, 10Mbps, 100Mbps, 1000Mbps}. The default is auto-negotiation. Note: When set to Auto, the rate of the interface is automatically negotiated between the interface and the peer port .
Jumbo Frame	Specify the jumbo frame, valid range is 1518-12288. Default value is 9216
Flow Control	Set the flow control on the interface, the options are { Disabled, Enabled, Auto}. The default is Disabled After enabling it, if the local device is congested, it will send a message to the peer device to notify the peer device to temporarily stop sending packets, after receiving the message, the peer device will temporarily stop sending packets to the local and vice versa. Thus, the occurrence of packet loss is avoided.

Link Aggregation Settings

LACP

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

Link Aggregation

GroupLAG SettingsLACP

System Priority

32768

Valid range is 1-65535

CancelOK

LACP List

Edit

Port	Port Priority	Timeout	Operation
☐ 1/0/1	1	Long	
☐ 1/0/2	22	Long	
☐ 1/0/3	1	Long	
☐ 1/0/4	1	Long	
☐ 1/0/5	65	Long	
☐ 1/0/6	1	Long	
☐ 1/0/7	1	Long	

Link Aggregation LACP

System Priority	Set the system priority of LACP, the value range is an integer from 1-65535, the default is 32768.
Edit LACP	Port: Select the switch LAG interface to be configuredPort Priority:Set the LACP protocol priority of the port , the value range is an integer from 1 to 65535 , the default is 1.Note: The smaller the priority value of the port , the higher the LACP priority of the port.Timeout: Set the timeout time for receiving LACP packets, the options are { Short, Long} , the default is Short. Short mode: the default timeout period for receiving LACP protocol packets is 3 seconds. Long mode: the default timeout period for receiving LACP protocol packets is 90 seconds .

Link Aggregation - LACP

MAC Address Table

The MAC Address Table maps learned MAC addresses to VLANs and ports. Use its tabs to view dynamic, static, blackhole, and port-security entries.

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

Dynamic Address

When a frame arrives, the switch learns its source MAC address and associates it with the ingress port and VLAN. Receiving another frame from the same source refreshes the dynamic entry's aging timer.

MAC Address Hashing Algorithm: Determines how the switch combines the VLAN ID and MAC address to place a learned entry in its internal Layer 2 forwarding table. It changes only the internal table distribution; it does not modify the MAC address, select a forwarding port, or control link-aggregation load balancing. The modes are alternative hash profiles rather than increasing performance levels.

Mode	Internal hash-table pattern	Availability
------	-----------------------------	--------------

Mode 1	The upper half uses a sequential VID/MAC combination; the lower half uses a randomized VID/MAC combination.	All GWN780x Pro models
Mode 2	Both halves use a randomized VID/MAC combination.	All GWN780x Pro models
Mode 3	Both halves use a sequential VID/MAC combination.	GWN7806PH Pro and GWN7806PL Pro only
Mode 4	The upper half uses a randomized VID/MAC combination; the lower half uses a sequential VID/MAC combination.	GWN7806PH Pro and GWN7806PL Pro only

Sequential and randomized describe how the switch combines address bits to calculate an internal table location; neither method changes the displayed MAC address. Leave the current mode unchanged unless a different distribution is required while troubleshooting MAC-learning or table-collision behavior. After selecting a different mode, click **OK**, save the configuration, and reboot the switch for the new mode to take effect.

Aging Time: Sets how long an inactive dynamic MAC entry remains in the table. Enter **0** to disable aging, or a value from **60 to 1,000,000 seconds**. Traffic received from the learned source before the timer expires refreshes the entry.

MAC Address Table

Dynamic Addresses Static MAC Addresses Blockhole Addresses Port Secure Addresses MAC Address Migration Record

Aging Time (s) Valid range is 0 and 60-1000000

MAC Address Hashing Algorithm

Mode 1
Mode 2
Mode 3
Mode 4

Dynamic Addresses

☐	VLAN	MAC Address	Port	Operation
☐	1	00:0B:82:66:FF:D5	1/0/54	Lock Refresh Delete
☐	1	00:0B:82:6B:0F:F5	1/0/54	Lock Refresh Delete
☐	1	00:0B:82:73:8F:79	1/0/54	Lock Refresh Delete
☐	1	00:0B:82:A0:D4:B4	1/0/54	Lock Refresh Delete
☐	1	00:0B:82:F6:64:64	1/0/54	Lock Refresh Delete

MAC Address Hashing Modes

Click **Refresh** to update the list. Select one or more dynamic entries, then use **Solidify** to convert them to static entries, **Block** to add them to the blackhole list, or **Delete** to remove them. **Delete All** removes every dynamic entry.

Static MAC Address

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

MAC Address Table

Dynamic Addresses

Static MAC Addresses

Blackhole Addresses

Port Secure Addresses

Add Static Address

Static MAC address must be unicast

*MAC Address

:

:

:

:

:

*VLAN

Valid range is 1-4094

*Port

Cancel

OK

Static MAC Address

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

Static MAC Address

Black Hole Address

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

Click on the **"Add"** button, then enter the MAC Address and the VLAN.

MAC Address Table

Dynamic Addresses
Static MAC Addresses
Blackhole Addresses
Port Secure Addresses

Add Blackhole Address

Blackhole MAC address must be a unicast address.

*MAC Address

:

:

:

:

:

*VLAN

Valid range is 1-4094

Cancel

OK

to filter out illegal MAC addresses

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 the interface name, VLAN, and MAC address.

MAC Address Table

Dynamic Addresses	Static MAC Addresses	Blackhole Addresses	Port Secure Addresses
-------------------	----------------------	---------------------	-----------------------

Refresh

VLAN	MAC Address	Type	Port
 No Data			

Port Security Address

MAC Address Migration Record

The **MAC Address Migration Record** tracks instances in which the switch learns the same MAC address through a different port. A single migration can be expected after a device is reconnected or a wireless client roams between access points. Repeated migrations can help identify MAC flapping caused by a Layer 2 loop, unstable links, or an incorrect network topology.

This feature is supported only on **GWN7806PH Pro** and **GWN7806PL Pro**.

MAC Address Table

Dynamic Addresses Static MAC Addresses Blockhole Addresses Port Secure Addresses MAC Address Migration Record

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

MAC Address	VLAN	Start Time	End Time	Source Port	Migration Ports	Migration Count
 No Data						

MAC Address Migration Record

Each record identifies the **MAC Address** and **VLAN**, the **Start Time** and **End Time** of the observed migration period, the original **Source Port**, the **Migration Ports** where the address was subsequently learned, and the total **Migration Count**. Use these details to determine where the address was first learned and how frequently it moved.

Click **Refresh** to reload the records. Click **Clear All** to delete all MAC address migration records.

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 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 the "Add" button to add a new VLAN. It is possible to create many VLANs at the same time by specifying a range, for example, **(7-9)** will create VLANs 7,8, and 9, or create different separated VLANs, for example, **(11,89)** will create VLANs 11 and 89.

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

VLAN

VLAN Port Settings Port Members Voice VLAN OUI MAC VLAN Protocol VLAN

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

☐	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.

CancelOK

Add a VLAN

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

VLAN > **Edit**

VLAN

Description

Member Type

All Ports

Port

Click port to change the member type

T

 Tagged

U

 Untagged

2

4

6

8

1

3

5

7

9 SFP1

10 SFP2

LAG

Click port to change the member type

T

 Tagged

U

 Untagged

2

4

6

8

1

3

5

7

Edit VLAN

VLAN	The specified VLAN ID
------	-----------------------

Description	Enter a brief comment for the VLAN ID.
Member Type	Select from the drop-down list: Remove All: remove all ports GE/LAG from this VLAN Tagged All: Tag all ports GE/LAG to this VLAN Untagged All: Untag all ports GE/LAG from this VLAN
GE	Select individually which ports are tagged, untagged or unselected.Note: Unselected ports will not be part of the VLAN Tagged ports expects tagged frames (Trunk port) like connecting a switch with another switch. Untagged ports expects non-tagged frames (Access port) like connecting a switch with end device.
LAG	Select individually which LAGs are tagged, untagged or unselected.

Edit VLAN

Please refer to the table below for more details about Tagged and Untagged Ports.

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

VLAN Tagged and Untagged

VLAN Port Settings

The Port Settings tab configures VLAN behavior for each port or LAG, including the link type (Hybrid, Access, Trunk, or Dot1q-tunnel), PVID, ingress filtering, accepted frame type, VLAN translation, and protocol template.

Port Settings > Edit

Port	1/0/2
Link Type	Trunk Hybrid Access Trunk Dot1q-tunnel
PVID	
Accept Frame Type	
TPID	
VLAN Translation	☒
Type	☐ VLAN Mapping ☒ VLAN Stacking

VLAN Stacking

VLAN Stacking1

Cancel
OK

VLAN Port Settings Link Types

TPID

VLAN Translation ☒

Type ☐ VLAN Mapping ☒ VLAN Stacking

VLAN Stacking

VLAN Stacking1

Outer VLAN

Stacked Outer VLAN

Stacked Outer VLAN Priority Valid range is 0-7

Add

Cancel OK

VLAN Port Settings VLAN Translation

Port

Link Type

PVID Valid range is 1-4094

Accept Frame Type ☒ All ☐ Tag Only ☐ Untag Only

TPID

Ingress Filtering ☒

VLAN Translation ☐

MAC VLAN ☐

Protocol VLAN ☒

Protocol Template

Protocol Template VLAN 802.1p

Add

Cancel OK

VLAN Port Settings Protocol Template

Port	Shows the selected port or LAG.
Link Type	Select the port link type:Hybrid: connects switches or end devices and supports tagged and untagged traffic.Access: connects an end device to one VLAN.Trunk: carries traffic for multiple VLANs between network devices.Dot1q-tunnel: selects IEEE 802.1Q tunneling mode.
PVID	Enter the default VLAN ID assigned to untagged traffic received on the port.

Accept Frame Type	Specifies which Ethernet frames the port accepts. Available options depend on Link Type:Hybrid: All, Tag Only, or Untag Only.Access: All.Trunk: All or Tag Only.Dot1q-tunnel: All, Tag Only, or Untag Only.Note: Use Tag Only on a Trunk or Hybrid port when native-VLAN behavior must be disabled.
Ingress Filtering	Enables inbound filtering on a Hybrid port. It is enabled by default and discards traffic that is not permitted by the port's VLAN membership.
TPID	Selects the Tag Protocol Identifier used for VLAN-tagged frames.
VLAN Translation	Enable port-level VLAN translation, then select one or both supported types:VLAN Mapping: translates configured VLAN IDs on the port.VLAN Stacking: encapsulates customer VLAN traffic inside an outer carrier VLAN tag. Configure Outer VLAN, Stacked Outer VLAN, and Stacked Outer VLAN Priority (0-7), then click Add to create another entry.
MAC VLAN	Assigns traffic to a VLAN according to the source MAC address.
Protocol VLAN	Assigns traffic to a VLAN according to the frame protocol, such as IP or ARP.

VLAN Port Members

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

VLAN

Port Settings

Port Members

Voice VLAN

OUI

MAC VLAN

Protocol VLAN

Edit

☐	Port	Link Type	Tagged VLAN	Trunk Allowed VLANs	Untagged VLAN	PVID	
☐	1/0/1	Trunk	--	1	1	1	
☐	1/0/2	Trunk	--	1	1	1	
☐	1/0/3	Trunk	--	1	1	1	
☐	1/0/4	Trunk	--	1	1	1	
☐	1/0/5	Trunk	--	1	1	1	
☐	1/0/6	Trunk	--	1	1	1	
☐	1/0/7	Trunk	--	1	1	1	
☐	1/0/8	Trunk	--	1	1	1	
☐	1/0/9	Trunk	--	1	1	1	

All Link Types
All Link Types
Access
Trunk
Hybrid
Dot1q-tunnel

Total 86

<123...9>

10 / pageGo to

© 2026 Grandstream Networks, Inc. Grandstream Software License Agreement

VLAN Port Members Link Type Filter

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

VLAN
Port Settings
Port Members
Voice VLAN
OUI
MAC VLAN
Protocol VLAN

Port	Link Type	Tagged VLAN	Trunk Allowed VLANs	Untagged VLAN	PVID	Operation
1/0/1	Trunk				1	
1/0/2	Trunk				1	
1/0/3	Trunk				1	
1/0/4	QinQ				1	
1/0/5	Trunk				1	
1/0/6	Trunk				1	
1/0/7	Trunk				1	
1/0/8	Trunk				1	
1/0/9	Trunk				1	
1/0/10	Trunk				1	
LAG1	Trunk				1	
LAG2	Trunk				1	
LAG3	Trunk				1	
LAG4	Trunk				1	
LAG5	Trunk				1	
LAG6	Trunk				1	
LAG7	Trunk	--	--	1	1	

Edit Port Member

Port

1/0/5

Link Type

Trunk

Trunk Allowed VLANs

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

Untagged VLAN

1

PVID

Trunk port. Same as Untagged VLAN

1

Cancel

OK

VLAN Port Members Trunk

VLAN
Port Settings
Port Members
Voice VLAN
OUI
MAC VLAN
Protocol VLAN

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

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 GWN780x Pro 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.**

VLAN

VLAN

Port Settings

Port Members

Voice VLAN

OUI

MAC VLAN

Protocol VLAN

Voice VLAN

Tagged OUI

Disabled

Auto Voice VLAN

Tagged OUI

Untagged OUI

Valid range is 0-7

Voice VLAN ID

CoS/802.1p Priority

CoS Remarking

Aging Time (Min)

1440

Valid range is 30-65536

Cancel

OK

OUI Port Settings

Edit

Port	Status	Mode	Operation
☐ 1/0/1	Disabled	Manual	
☐ 1/0/2	Disabled	Manual	
☐ 1/0/3	Disabled	Manual	

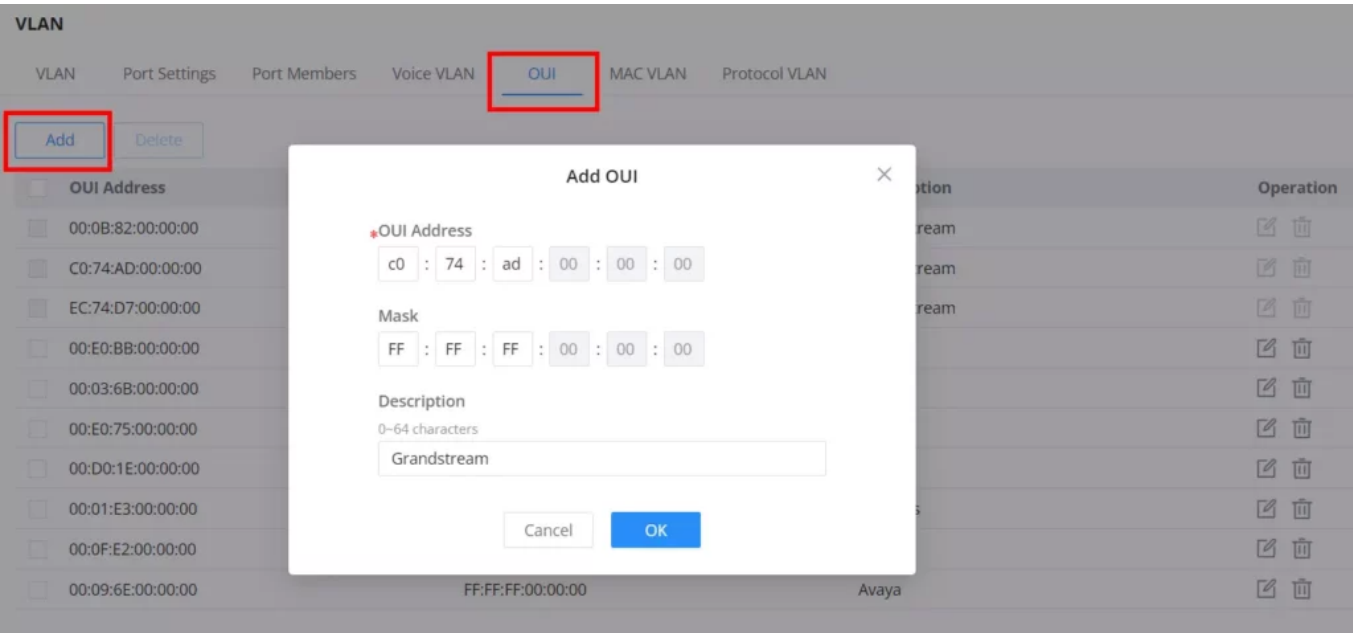
Voice VLAN

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

VLAN

VLAN Port Settings Port Members Voice VLAN OUI MAC VLAN Protocol VLAN

Add Delete Delete All

MAC Address	802.1p	Operation
-------------	--------	-----------

:

:

:

:

:

:

*MAC Address

Valid range is 9-48

48

*Mask Length

Please select

*VLAN

Valid range is 0-7

0

*802.1p

Cancel OK

VLAN MAC VLAN

Protocol VLAN

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

Only effective for Hybrid port.

VLAN

VLAN Port Settings Port Members Voice VLAN OUI MAC VLAN Protocol VLAN

Add Delete

Protocol Index	Frame Type	Protocol Type Value	Operation
----------------	------------	---------------------	-----------

Protocol Index

0

Frame Type

Ethernet II

*Protocol Type Value

Valid range: 0x600-0xFFFE

Cancel OK

VLAN Protocol VLAN

Spanning Tree

Spanning Tree Protocol (STP) prevents network loops by automatically detecting redundant links and blocking unnecessary ones. Without it, switches could forward packets in circles, causing broadcast storms and major outages.

This switch supports multiple versions of STP, each with different speed, complexity, and use cases:

- **STP** (Spanning Tree Protocol): The original standard. It prevents loops but takes 30+ seconds to recover from topology changes. Use only if required by old devices.
- **RSTP** (Rapid Spanning Tree Protocol): A faster, modern version of STP with sub-second failover. Ideal for most networks that don't require per-VLAN control.
- **MSTP** (Multiple Spanning Tree Protocol): Groups multiple VLANs into one spanning tree instance, reducing overhead. Best for large networks with many VLANs and structured VLAN planning.
- **PVST(+)** (Per-VLAN Spanning Tree Plus): Runs a separate spanning tree for each VLAN. Allows detailed control but increases CPU/memory usage. Good when VLAN isolation and per-VLAN optimization are required.
- **RPVST(+)** (Rapid PVST Plus): Adds fast convergence to PVST(+). Ideal for modern, VLAN-heavy networks needing both speed and per-VLAN flexibility.

Choosing a Mode:

- Use **RSTP** if you're not sure. It's fast and widely compatible.
- Choose **RPVST(+)** for VLAN-specific loop prevention with quick failover.
- Go with **MSTP** if you want scalable performance across many VLANs.
- **STP** is maintained for backward compatibility with legacy devices. It is not recommended for modern networks due to its slower convergence time.

Spanning Tree

Global Settings

Port SettingsMST InstanceMST Port Settings

Spanning Tree

Mode

Ignore VLAN in BPDU

Path Cost

*Bridge Priority

*Max Hops

*Hello Time (s)

*Max Aging Time (s)

*Forward Delay Time (s)

STP

RSTP

MSTP

PVST(+)

RPVST(+)

20

2

20

15

Enter a value between 0-61440 that is a multiple of 4096

Valid range is 1-40

Valid range is 1-10

Valid range is 6-40

Valid range is 4-30

Cancel

OK

Status

Bridge ID

Root Bridge ID

Root Port

32768-C0:74:AD:B9:3C:A7

0-00:00:00:00:00:00

--

Spanning Tree Global Settings

Spanning Tree	Set whether to enable Spanning Tree.
Mode	Set the operating mode of Spanning Tree (STP).STP: Standard Spanning Tree Protocol. Provides basic loop prevention but has slow convergence. Use only for compatibility with older or legacy network devices. RSTP: Rapid Spanning Tree Protocol. Faster convergence than STP, suitable for most modern networks. Recommended as the default for typical deployments.MSTP: Multiple Spanning Tree Protocol. Allows grouping of multiple VLANs into a single STP instance. Best suited for large networks with many VLANs that require efficient resource use.PVST+: Per-VLAN Spanning Tree Plus. Runs one STP instance per VLAN, offering detailed control of loop prevention per VLAN. Good for networks with high segmentation.RPVST(+): Rapid Per-VLAN Spanning Tree Plus. Combines the benefits of RSTP and PVST(+), offering fast convergence for each VLAN. Ideal for high-availability environments with VLAN-based traffic control.
Ignore VLAN in BPDU	This feature allows the switch to ignore VLAN-specific information in Bridge Protocol Data Units (BPDUs). This prevents VLAN configurations from influencing Spanning Tree Protocol (STP) decisions across multiple VLANs.
Path Cost	Specify the path cost method (Short, Long, or Legacy). Default is Short.
Bridge Priority	Select the Bridge Priority, In an STP network, the device with the smallest bridge ID is elected as the root bridge.Default is 32768.Note: The valid range is 0~61440, which must be a multiple of 4096
Max Hops	Select the Max Hops (the range is 1 - 40). Default is 20
Hello Time (s)	Specify the Hello Time in seconds (the range is 1 -10). Default is 2.Note: The time interval at which the device running the STP protocol sends the configuration message BPDU , which is used by the device to detect whether the link is faulty.
Max Aging Time (s)	Select The aging time of BPDU packets of the port (the range is 6 - 40). Default is 20.
Forward Delay Time (s)	Specify the Forward Delay Time in seconds (the range is 4 -30). Default is 15.

STP Global Settings

STP Port Settings

To configure STP on each port and LAG, then navigate to WEB UI -> Spanning Tree -> Port Settings, then click on the "**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
☒ 1/0/1	Enabled	128	4	Auto	Disabled	Disabled	Auto	Disabled	
☐ 1/0/2	Enabled	128	4	Auto	Disabled	Disabled	Auto	Disabled	
☐ 1/0/3	Enabled	128	4	Auto	Disabled	Disabled	Auto	Disabled	
☐ 1/0/4	Enabled	128	4	Auto	Disabled	Disabled	Auto	Disabled	
☐ 1/0/5	Enabled	128	4	Auto	Disabled	Disabled	Auto	Disabled	
☐ 1/0/6	Enabled	128	4	Auto	Disabled	Disabled	Auto	Disabled	
☐ 1/0/7	Enabled	128	4	Auto	Disabled	Disabled	Auto	Disabled	
☐ 1/0/8	Enabled	128	4	Auto	Disabled	Disabled	Auto	Disabled	
☐ 1/0/9	Enabled	128	4	Auto	Disabled	Disabled	Auto	Disabled	
☐ 1/0/10	Enabled	128	4	Auto	Disabled	Disabled	Auto	Disabled	
☐ 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

1/0/1

Enable Spanning Tree

☒

Priority

128

Enter a value between 0-240 that is a multiple of 16

Path Cost

0

Valid range is 0-65535

Edge Port

☒ Auto
 ☐ Enabled
 ☐ Disabled

Root Protection

☐

Loop Protection

☒

BPDU Guard

☐

BPDU Filter

☐

Point-to-Point

☒ Auto
 ☐ Enabled
 ☐ Disabled

Cancel

OK

Spanning Tree Edit Port Settings

Port	Displays the selected GE/LAG Port.
Enable STP	Set whether to enable STP on this port.
Priority	Priority is an important basis for determining whether the port will be selected as the root port. The port with higher priority under the same conditions will be selected as the root port . The smaller the value , the higher the priority . An integer in the range of 0-240, with a step size of 16, and a default of 128 .Note: The valid range is 0~240, which must be a multiple of 16
Path Cost	Set the path cost of the port on the specified spanning tree. The default value is 0, which means that path cost calculation is performed automatically.Note:The valid range of path cost depends on the path cost settings in Global Settings.If set to "Short" in Global Settings, the valid range is 0-65535; if set to "Long", the valid range is 0-200000000; if set to "legacy", the valid range is 0-200000.

Edge Port	Set whether to enable Edge Port or disable it, by default it's on auto. Notes: A port is considered as an edge port when it is directly connected to the user terminal or server, instead of any other switches or shared network segments. The edge port will not cause a loop upon network topology changes. In the edge mode, the interface would be put into the Forwarding state immediately upon link up. While in auto mode it will detect if the port is an edge or not.
Root Protection	Safeguards the root bridge by preventing designated ports from becoming the root port, thus protecting the current root bridge from being displaced by lower-priority BPDUs.
Loop Protection	Prevents Layer 2 loops by ensuring a blocking state on ports that stop receiving BPDUs, avoiding the formation of network loops.
BPDU Guard	Set whether to enable BPDU Guard. Note: BPDU Guard further protects your switch by turning this port into error state and shutdown if any BPDU received from this port.
BPDU Filter	Set whether to enable BPDU Filter. Note: Drop all BPDU packets and no BPDU will be sent.
Point-to-Point	Select Point-to-Point option (Auto, Enabled or Disabled). Default is Auto. Note: determines the STP of link type for this port automatically if set to Auto.

STP Port Settings

Multiple Spanning Tree Instances

MST or Multiple Spanning Tree Instance allows traffic of different VLANs to be mapped into different MST Instances. GWN780x Pro 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:

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 Hops	Operation
0	1-4094	61440	61440-C0:74:AD:DF:CC:94	32767-C0:74:AD:C9:72:E9	1/0/24	4	20	
1	--	32768	61440-C0:74:AD:DF:CC:94	61440-C0:74:AD:DF:CC:94	1/0/24	0	20	
2	--	32768	61440-C0:74:AD:DF:CC:94	61440-C0:74:AD:DF:CC:94	1/0/24	0	20	
3	--	32768	61440-C0:74:AD:DF:CC:94	61440-C0:74:AD:DF:CC:94	1/0/24	0	20	
4	--	32768	61440-C0:74:AD:DF:CC:94	61440-C0:74:AD:DF:CC:94	1/0/24	0	20	

Multiple Spanning Tree Instances

MSTI

0

VLAN

1-4094

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

*Priority

61440

Enter a value between 0-61440 that is a multiple of 4096

Cancel

OK

Bridge Identifier

61440-C0:74:AD:

Designated Root Bridge

32767-C0:74:AD:

Root Port

1/0/24

Root Path Cost

4

Remaining Hop

20

MST Edit Port

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

Spanning Tree

Global Settings

Port Settings

MST Instance

MST Port Settings

MSTI

0

Port Settings

Edit

Refresh

Port	Path Cost	Priority	Role	Status	Mode	Type	Designated Bridge ID	Operation
☒ 1/0/1	4	128	Disabled Port	Disabled	STP	Boundary	0-00:00:00:00:00:00	
☒ 1/0/2	4	128	Disabled Port	Forwarding	STP	Boundary	61440-C0:74:AD:	
☐ 1/0/3	4	128	Disabled Port	Disabled	STP	Boundary	0-00:00:00:00:00:00	
☐ 1/0/4	4	128	Disabled Port	Disabled	STP	Boundary	0-00:00:00:00:00:00	
☐ 1/0/5	4	128	Disabled Port	Disabled	STP	Boundary	0-00:00:00:00:00:00	
☐ 1/0/6	4	128	Disabled Port	Disabled	STP	Boundary	0-00:00:00:00:00:00	
☐ 1/0/7	4	128	Disabled Port	Disabled	STP	Boundary	0-00:00:00:00:00:00	

MST Port Settings

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

MSTI	0	
Port	1/0/2	
*Path Cost ⓘ	0	Valid range is 0-65535
*Priority	128	Enter a value between 0-240 that is a multiple of 16
Cancel OK		

Port Role	Disabled Port
Port Status	Forwarding
Mode	STP
Type	Boundary
Designated Bridge ID	61440-C0:74:AD
Designated Port ID	128-2
Designated Path Cost	4
Remaining Hop	20

MST Port Settings Edit port

PVST VLAN Settings

When the Per VLAN Spanning Tree protocol is selected as the STP protocol to be used, then the VLAN settings can be defined.

Spanning Tree						
Global Settings	Port Settings	VLAN Settings	PVST Port Settings			
VLAN	Enable PVST	Bridge Priority	Hello Time (s)	Max Aging Time (s)	Forward Delay Time (s)	Operation
1	Enabled	32768	2	20	15	
7	Disabled	32768	2	20	15	
Total 2 < 1 > 10 / page						

The following parameters are to be configured:

VLAN	Displays the VLAN on which the PVST rule will PVST protocol will be applied
Enable PVST	Enables/disables PVST per VLAN
Bridge Priority	Defines the bridge priority for the VLAN, valid range is 0-61440, default value is 32768. Note: All values should be a multiple of 4096
Hello Time (s)	Specify the Hello Time in seconds (the range is 1 -10). Default is 2. Note: The time interval at which the device running the STP protocol sends the configuration message BPDU , which is used by the device to detect whether the link is faulty.
Max Aging Time (s)	Select The aging time of BPDU packets of the port (the range is 6 - 40). Default is 20.
Forward Delay Time (s)	Specify the Forward Delay Time in seconds (the range is 4 -30). Default is 15.

PVST Port Settings

The PVST Port settings define the priority and path cost for each port of the switch, for each VLAN. It also displays, for each port, its role, designated Bridge ID, designated Port ID, and designated Path Cost.

Spanning Tree

Global SettingsPort SettingsVLAN SettingsPVST Port Settings

VLAN1

Port Settings

EditRefresh

☐	Port	Path Cost	Priority	Role	Status	Designated Bridge ID	Designated Port ID	Designated Path Cost	Operation
☐	1/0/1	65535	128	Disabled Port	Disabled	0-00:00:00:00:00:00	0-0	65535	
☐	1/0/2	65535	128	Disabled Port	Disabled	0-00:00:00:00:00:00	0-0	65535	
☐	1/0/3	65535	128	Disabled Port	Disabled	0-00:00:00:00:00:00	0-0	65535	
☐	1/0/4	65535	128	Disabled Port	Disabled	0-00:00:00:00:00:00	0-0	65535	
☐	1/0/5	65535	128	Disabled Port	Disabled	0-00:00:00:00:00:00	0-0	65535	
☐	1/0/6	65535	128	Disabled Port	Disabled	0-00:00:00:00:00:00	0-0	65535	
☐	1/0/7	18	128	Designated Port	Forwarding	32769-EC:74:D7:3D:90:A4	128-7	18	
☐	1/0/8	65535	128	Disabled Port	Disabled	0-00:00:00:00:00:00	0-0	65535	
☐	1/0/9	65535	128	Disabled Port	Disabled	0-00:00:00:00:00:00	0-0	65535	
☐	1/0/10	65535	128	Disabled Port	Disabled	0-00:00:00:00:00:00	0-0	65535	
☐	1/0/11	65535	128	Disabled Port	Disabled	0-00:00:00:00:00:00	0-0	65535	
☐	1/0/12	65535	128	Disabled Port	Disabled	0-00:00:00:00:00:00	0-0	65535	
☐	1/0/13	65535	128	Disabled Port	Disabled	0-00:00:00:00:00:00	0-0	65535	
☐	1/0/14	65535	128	Disabled Port	Disabled	0-00:00:00:00:00:00	0-0	65535	

The parameters to be defined are

Port	Displays the port, or ports that the settings will be applied on.
Priority	Displays the single port priority. valid range is 0-240 and the default value is 18. Note: The value must be a multiple of 16
Path Cost	Configures the port path cost for the port on the specified spanning tree. The value must be an integer between 0-65535. The default value is 0, which means the path cost calculation will be performed automatically.

ERPS

Ethernet Ring Protection Switching (ERPS) provides a backup path for switches connected in an Ethernet ring. It prevents loops during normal operation and switches traffic to the protection path when a ring link fails, helping keep services available.

Navigate to **Switching -> ERPS** and enable **ERPS**. Configure the ring settings, select the two ports connecting this switch to the ring, and assign each port its role according to the ring design.

ERPS

ERPS



Ring Settings

*Control VLAN		Valid range is 1-4094
*MEL	7	Valid range is 0-7
*WTR Timer (min)	5	Valid range is 5-12
*Guard Timer (ms)	1000	Valid range is 800-2000
*Holdoff Timer (ms)	0	Valid range is 0-10000

Port Settings

*Port 1	Please select
Role	☒ RPL Owner Port ☐ Normal Port
*Port 2	Please select
Role	☐ RPL Owner Port ☒ Normal Port
Cancel OK	

ERPS Settings

Control VLAN	VLAN used to carry ERPS control messages.
MEL	Maintenance entity group level used by the ring protection protocol.
WTR Timer (min)	Wait-to-Restore interval before reverting to the normal ring path after a failure clears.
Guard Timer (ms)	Interval that prevents outdated ring-protection messages from affecting a recovery transition.
Holdoff Timer (ms)	Delay before a detected link failure triggers ring protection switching.
Port 1 / Port 2	Select the two local interfaces that connect this switch to the Ethernet ring.
Role	Select RPL Owner Port for the port assigned to own the Ring Protection Link, or Normal Port for a normal ring port, according to the ring design.

IP

VLAN IP Interface

IPv4/IPv6 Interface

GWN7806PH Pro and GWN7806PL Pro support up to 512 VLAN IP interfaces. For the other Pro models, refer to the model-specific limits in [Technical Specifications](#).

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

VLAN IP Interface

IPv4 Interface

IPv6 Interface

IPv6 Router Advertisements

MGMT VLAN

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	192.168.50.168/24	1500	

Total 2

<

1

>

10 / page

VLAN IP Interface MGMT VLAN

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

Confirm to get IP address again?

Once successfully obtained, the IP address may be changed

Cancel

OK

Refresh IP address

Address Type:

- **If DHCP is selected:** hosts will obtain IP addresses automatically from the DHCP server pool is configured (a router, for example).

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

IPv6 Interface > Edit IPv6 Interface

VLAN

VLAN 1

IPv6 Enable



Link-Local Address

☒ Auto Generate ☐ Manually Configure

Global Unicast Address

SLAAC



*Gateway Priority

2

Valid range is 2-255

*MTU

1500

Valid range is 1280-9216

Cancel

OK

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 IPv4 Interface

***VLAN**

Valid range is 1-4094.

IPv4 Address Type

☒ Static IP ☐ DHCP

***IPv4 Address**

Mask

***Prefix Length**

Valid range is 8-30.

***MTU**

Valid range is 128-9216.

Add VLAN IP Interface

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	VLAN 1		
Interface Enable	☐		
Route Information	☐		
*Timeout (s)	600	Valid range is 1-1800	
*Lifetime (s)	1800	Valid range is 0-9000	
Flag	☐ M Flag ☐ O Flag		
Default Route Priority	中		

IPv6 Address/Prefix1

*IPv6 Address/Prefix		/	64	Prefix range 1-128
*Valid Lifetime (s)	2592000			Valid range is 0-4294967295
*Preferred Lifetime (s)	604800			Valid range is 0-4294967295
Flag	☒ A Flag ☐ L Flag ☐ R Flag			

Add 

Cancel

OK

Edit IPv6 Router Advertisement

MGMT VLAN

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

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

functions are aligned.

Management IP Interface

The management IP interface supports a configurable **Class of Service (CoS)** value so management traffic can receive the required Layer 2 priority.

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.

DHCP Server

A static VLAN IP interface can provide DHCP service to connected clients. Configure the service from **IP -> DHCP Server**. Address pools can be enabled or disabled individually, and the global pool settings include a gateway and DHCP options.

Please navigate to the **Web UI -> IP -> DHCP Server** page.

Step 1: Enable the DHCP Server.

DHCP Server

DHCP Server

Address Table

DHCP Service

Cancel

OK

Address Pool Settings

Add

Delete

All

Q Name

Address Pool Name	Enable	Type	IPv4 Interface	Address Pool	Used	Remained	Operation
No Data							

© 2026 Grandstream Networks, Inc.

Grandstream Software License Agreement

DHCP Server Address Pools

Step 2: In the Address Pool Settings section, click on the **"Add"** button to add a new address pool. Add a pool range for the DHCP Server, then select the interface (VLAN).

DHCP Server

Add Address Pool

Address Pool Name

1-64 characters allowed, including digits, letters and special characters except "\?/;

Enable

Type

Global

Interface

IP Pool Subnet

Mask Length

Valid range is 8-30

Gateway

+

Add

Duration (min)

120

Valid range is 1-11520

DNS Server

+

Add

Cancel

OK

Add DHCP Address Pool

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

*Duration (min) Valid range is 1-2880

DNS Server + Add +

WINS Server + Add +

Netbios Node Type

DHCP Option1

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

Type

Service

Option Content 0-255 characters

Add +

DHCP Server Add Pool DHCP Options

For each DHCP pool, select whether the pool is enabled, define its gateway and address range, and add the required DHCP options.

The address table will display the hosts (devices) MAC Addresses and the IP addresses when using the DHCP Server. Also, it's possible to make an entry a static one by clicking on the "**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
☒	C0:74:AD:93:0C:F8	70.0.0.32	Dynamic	6926	

Total 1

<

1

>

10 / page

DHCP DHCP Server

DHCP Relay

DHCP relay on the GWN780x Pro switch helps a network device pass DHCP messages between clients and servers that are on completely different networks. When you have a DHCP server that needs to serve clients on different subnets (or VLANs). A DHCP relay agent is a network device that can route between the client's subnet and the server's subnet. The relay agent gets the broadcast request from the client and sends it to the server, putting its own interface address as the gateway address (giaddr) field in the packet. This way, the server can tell which subnet the client is on and assign a suitable IP address. The server then sends the reply back to the relay agent, which passes it to the client.

DHCP Relay

DHCP Relay

Polling

*TTL

4

Valid range is 1-16.

Cancel

OK

DHCP Server

Add

Delete

☐	Interface	DHCP Server	Operation
☐	VLAN 7	192.168.7.1	

Total 1

<

1

>

10 / page

DHCP Relay

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

DHCP Relay

ARP Table

The ARP Table separates configured entries from effective learned entries, making it easier to manage static mappings and verify the mappings currently used for forwarding.

- **ARP Table:** Displays dynamically learned ARP entries. You can configure the **aging time** and enable **Strict ARP Learning**, which limits ARP entries to only those required for actual traffic forwarding.

Note: On models such as **GWN7801P Pro**, **GWN7802P Pro**, and **GWN7803PL/PH Pro**, ARP capacity is limited to **64 entries**. To prevent the table from filling with unnecessary data, enable **Strict ARP Learning** under **Web UI -> IP -> ARP Table**. When enabled, it is also recommended to go to **Web UI -> Routing -> Routing Table** and set the **Forwarding Mode** to **Manual** for consistent forwarding behavior.

- **Static ARP:** Allows administrators to define permanent IP-to-MAC address mappings that cannot be overwritten or aged out. This is typically used to ensure reliable communication with critical devices and to prevent spoofing.

To configure the ARP Table, please navigate to **Web UI -> IP -> ARP Table**.

ARP Table

ARP Table Static ARP

• Aging Time (s)

1200

Range 60-21600, associated with the aging time of Neighbor Table

ARP Learning Strict ⓘ



Cancel

OK

ARP Table

Refresh Solidify

All Types

Q. IP Interface/IP Address/MAC Addr...

	IP Address	MAC Address	IP Interface	Interface	Type	Expiration (s)	Operation
☐	172.16.142.1	7c:7a:3c:81:e5:72	VLAN 1	1/0/54	Dynamic	678	
☐	172.16.143.10	00:0b:82:5e:66:bd	VLAN 1	1/0/54	Dynamic	1058	
☐	172.16.143.9	00:0b:82:a0:d4:b4	VLAN 1	1/0/54	Dynamic	1013	
☐	172.16.143.7	ec:74:d7:62:e1:3c	VLAN 1	1/0/54	Dynamic	1113	
☐	172.16.142.251	c0:74:ad:13:adb3	VLAN 1	1/0/54	Dynamic	1058	
☐	172.16.142.235	00:0b:82:00:00:00	VLAN 1	1/0/54	Dynamic	1002	
☐	172.16.142.232	c0:74:ad:23:c3:f3	VLAN 1	--	Dynamic	231	

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 60 to 21600, and the default is 1200 seconds.

ARP Table

ARP Table Static ARP

• Aging Time (s)

1200

Range 60-21600, associated with the aging time of Neighbor Table

ARP Learning Strict ⓘ



Cancel

OK

ARP Table

Refresh Add as Static ARP

All Types

Q. VLAN/IP Address/MAC Addr...

	IP Address	MAC Address	VLAN Interface	Interface	Type	Expiration (s)	Operation
☐	169.254.100.1	c0:74:78:11:00:90	VLAN 100	1/0/10	Dynamic	1149	
☐	169.254.100.4	c0:74:ad:d8:f3:f8	VLAN 100	1/0/10	Dynamic	899	
☐	169.254.100.3	c0:74:ad:cc:de:8c	VLAN 100	1/0/10	Dynamic	353	
☐	169.254.100.2	c0:74:adb9:3bdc	VLAN 100	1/0/10	Dynamic	1155	
☐	192.168.180.176	c0:74:ad:cc:de:8c	VLAN 180	--	Dynamic	679	
☐	192.168.180.100	c0:74:adb9:3bdc	VLAN 180	1/0/10	Dynamic	1063	
☐	192.168.180.35	c0:74:ad:d8:f3:f8	VLAN 180	1/0/10	Dynamic	671	
☐	192.168.180.2	c0:74:78:11:00:90	VLAN 180	--	Dynamic	314	
☐	192.168.180.1	ec:74:d7:5d:a8:52	VLAN 180	1/0/10	Dynamic	1190	
☐	172.16.143.30	c0:74:adb9:3b:79	VLAN 1720	1/0/10	Dynamic	321	

ARP Table Operation

Click on the "Link" icon to make the dynamic entry a static entry.

Static ARP

The **Static ARP** tab allows administrators to manually configure fixed IP-to-MAC address mappings. These entries do not expire and cannot be overwritten by dynamic ARP learning, making them ideal for securing communication with critical network devices.

To improve network stability and security, especially in environments vulnerable to spoofing or with limited ARP table size, static entries ensure the device only uses predefined address pairs for specific peers.

Click **"Add Manually"** to create a new entry by specifying:

- **VLAN** - Select the VLAN interface the entry applies to
- **IP Address** - Must be in a valid IPv4 format
- **MAC Address** - Must be a unicast MAC address

Alternatively, click "**Add Quickly**" to select one or more existing dynamic ARP entries and convert them into static entries in bulk.

Access this tab via **Web UI -> IP -> ARP Table -> Static ARP**

ARP Table

ARP Table **Static ARP**



To improve security, static ARP can be added manually

[Add Manually](#) [Add Quickly](#)

Add Static ARP

Add Static ARP ×

 The MAC address must be an unicast one.

***VLAN**

***IP Address**

IPv4 format

***MAC Address**

: : : : :

Cancel

OK

Add Static ARP

Neighbor Discovery

Neighbor Discovery Protocol (NDP) provides IPv6 address resolution, neighbor reachability detection, duplicate-address detection, router discovery, redirects, and neighbor proxy functions. The interface separates configured entries from the effective neighbor table.

IPv6 address auto-configuration 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 Table

Neighbor Discovery

Neighbor Table

Static Neighbor

Aging Time (s)

1200

Range 60-21600, associated with the aging time of ARP Table

Cancel

OK

Neighbor Table

Refresh

Solidify

All Types

All (Router)

Q IP Interface/IPv6 Address/MAC A...

☐	IPv6 Address	MAC Address	IP Interface	Interface	Type	Expiration (s)	Router	Operation
No Data								

Neighbor Table

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 60 to 21600, and the default is 1200 seconds.

Click on the **"Refresh"** button to refresh the list for dynamic entries.

Static Neighbor

Click on the **"Add"** button to add a static entry, refer to the figure below:

Neighbor Discovery

Neighbor Table

Static Neighbor



To enhance security, you can manually add static neighbors

Add

Add Static Neighbor

Add Static Neighbor



ⓘ The MAC address must be an unicast one.

*VLAN

*IPv6 Address

*MAC Address

c0	:	74	:	ad	:	11	:	22	:	33
----	---	----	---	----	---	----	---	----	---	----

Cancel

OK

Add Static Neighbor

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

DNS

Domain Name System DNS provides translation services between domain names and IP addresses. GWN780x Pro 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.

DNS 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 GWN780x Pro switches, navigate to **Web UI -> IP -> DNS**, then click on the **Global Settings** tab.

DNS

Global Settings Domain Mapping Table

① DNS servers are sorted by the adding time from earliest to latest. The DNS server added the earliest has the highest priority.

DNS ☒

Domain Suffix 1-64 alphanumeric characters and special characters Add

DNS Server 1.1.1.1 Add

DNS Global Settings

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

Domain Mapping Table

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

DNS

Global Settings **Domain Mapping Table**

☐	Hostname	IP Address	Type	Expiration (s)	Operation
☐	grandstream.com	173.254.235.74	Static	--	
☐	pool.ntp.org	196.200.131.160	Dynamic	16	

Total 2 < 1 > 10 / page

DNS Domain Mapping Table

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

Add Static Domain

*Hostname

1-191 alphanumeric characters and special characters . _ -

grandstream.com

*IP Address

173.254.235.74

Cancel

OK

Add Static Domain

The user can also select the dynamic domains and then click on the "Add as a static domain" button or icon to make them 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 the 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 that do not need them, and thus control which ports receive specific multicast traffic.

IGMP Snooping Global Settings

This page allows the user to enable/disable the 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.

IGMP Snooping

Global Settings Router Port Multicast Address Multicast Policy Multicast Port

Unknown Multicast Packet	Flood	This option is associated with the same setting under MLD Snooping
IGMP Snooping	☒	
Multicast Forward Mode	MAC-Based	
IGMP Version	IGMPv2	
Report Suppression	☐	
Cancel OK		

VLAN Settings

Edit	All Q VLAN								
☒	VLAN	Status	Querier	Querier Version	Router Port Auto-Learning	Port Fast Leave	Query Robustness	Query Interval	Operation
☒	1	Disabled	Disabled	IGMPv2	Enabled	Disabled	2	125	
☒	7	Disabled	Disabled	IGMPv2	Enabled	Disabled	2	125	

IGMP Snooping Global Settings

Unknown Multicast Packet	Select an action for switch to handle with unknown multicast packet. Drop: Drop the unknown multicast data. Flood: Flood the unknown multicast data. Forward to Router port: Forward the unknown multicast data to router port.
IGMP Snooping	Enable or disable Global IGMP Snooping
Multicast Forward Mode	Set the Multicast Forward Mode. MAC-Based: Forward using MAC address. IP-Based: Forward using IP address
IGMP Version	Select the IGMP Version.
Report Suppression	Enable or disable the switch to handle IGMP reports between router and host, suppressing bandwidth used by IGMP.

IGMP Snooping Global Settings

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

VLAN	1	
IGMP Snooping	☒	
IGMP Snooping Querier	☐	
Router Port Auto-Learning	☒	
Port Fast Leave	☐	
*Query Robustness	2	Valid range is 1-7.
*Query Interval (s)	125	Valid range is 30-18000.
*Query Max Response Interval (s)	10	Valid range is 5-20.
*Last Member Query Count	2	Valid range is 1-7.
*Last Member Query Interval (s)	1	Valid range is 1-25.
Cancel <input checked="" type="button" value="OK"/>		

IGMP Snooping Edit VLAN

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

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 the "Edit" icon to modify an already created one.

IGMP Snooping

Global Settings Querier Router Port Multicast Address Multicast Policy Multicast Port

AddRefreshDelete

☐ VLAN	Static Router Port	Forbidden Port	Dynamic Port	Aging Time (s)	Operation
☐ 1	1/0/24	--	--	--	

Total 1<1>10 / page

IGMP Snooping Router Port

Router Port > Edit

*VLAN8

Static Router Port

Click on port to select/unselect

GE

2

4

6

8

1

3

5

7

1

2

LAG

2

4

6

8

1

3

5

7

Forbidden Port

Click on port to select/unselect

GE

2

4

6

8

1

3

5

7

1

2

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 clicking "Edit" icon to edit.

IGMP Snooping

[Global Settings](#) [Querier](#) [Router Port](#) [Multicast Address](#) [Multicast Policy](#) [Multicast Port](#)

AddRefreshDelete

Q VLAN/Multicast Address/Member Port

☐ VLAN	Multicast Address	Source IP Address	Member Port	Address Type	Aging Time (s)	Operation

IGMP Snooping Multicast Address page

Multicast Address > Edit

VLAN

Multicast Address

224.7.1.0

IPv4 format

Click on port to select/unselect

Port

2

4

6

8

10

12

14

16

18

20

22

24

1

3

5

7

9

11

13

15

17

19

21

23

25 SFP+

26 SFP+

27 SFP+

28 SFP+

LAG

2

4

6

8

10

12

14

1

3

5

7

9

11

13

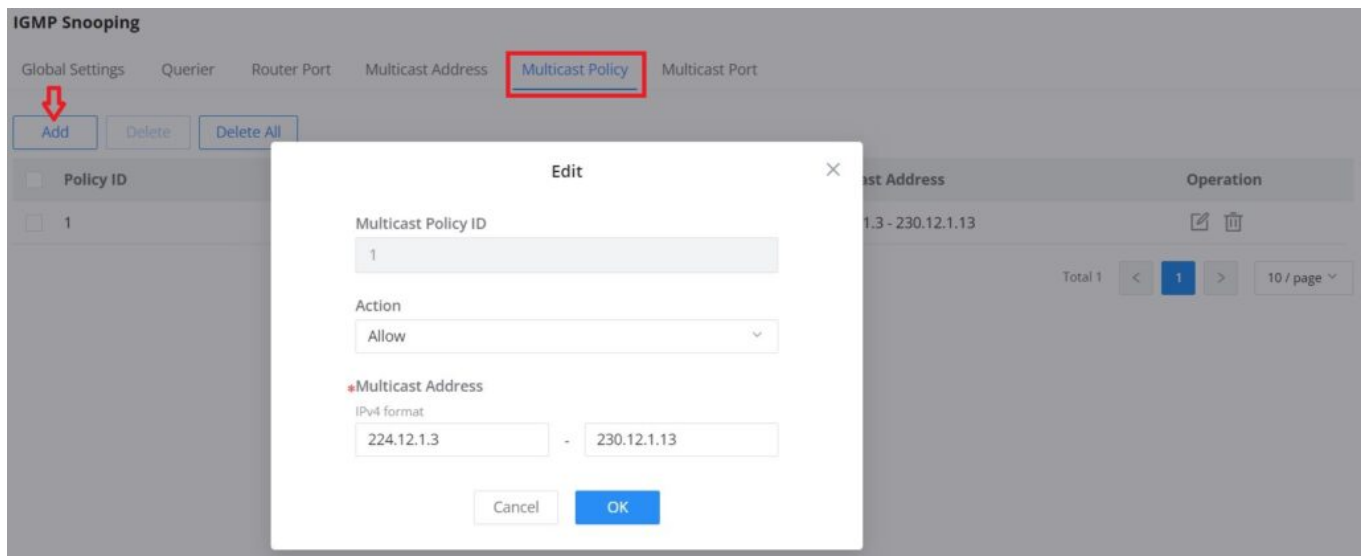
Cancel

OK

Add IGMP Snooping Multicast Address

IGMP Snooping Multicast Policy

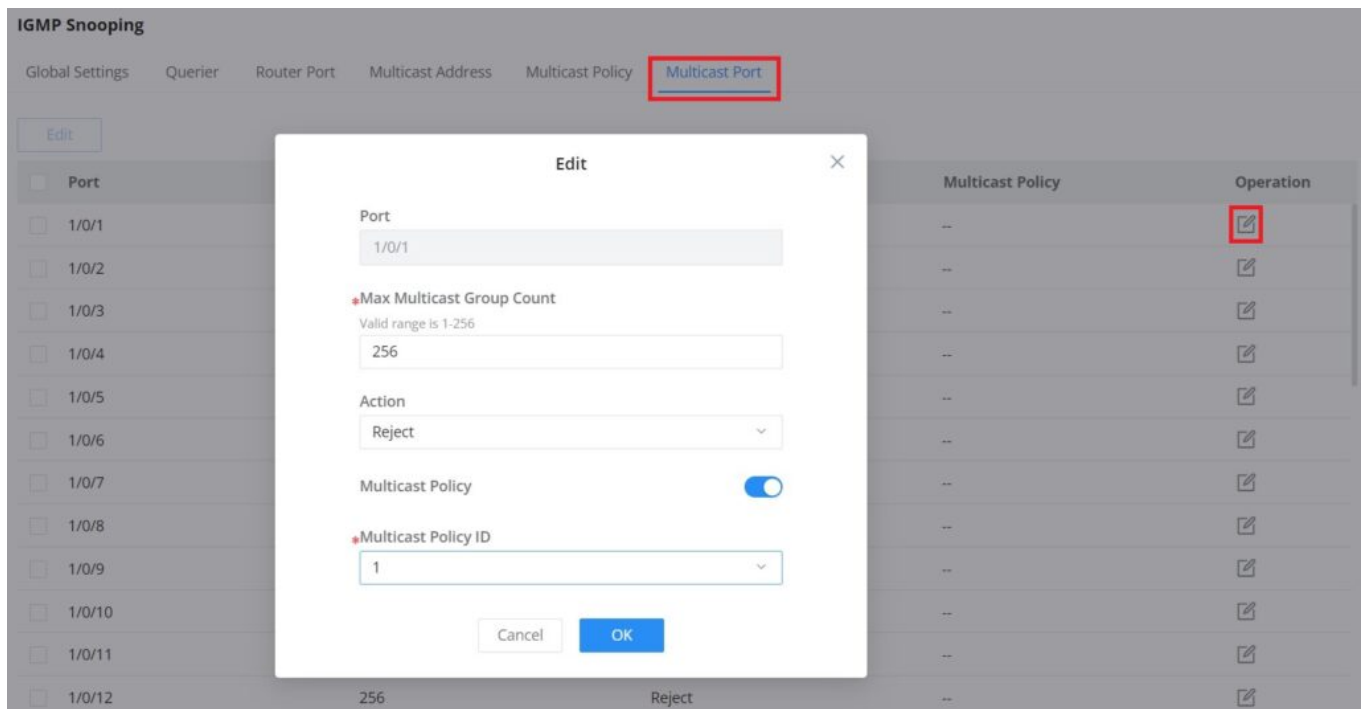
In this page, the user can add a Multicast Policy up to 128 Policy IDs to Allow or Reject a range of Multicast Addresses.



IGMP Snooping Multicast Policy

IGMP Snooping Multicast Port

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

Enable MLD Snooping globally, choose the multicast forwarding mode, and configure settings per VLAN.

Supported Models: Matching Domain is available on GWN7801P Pro, GWN7802P Pro, and GWN7803 Pro.

MLD Snooping

Global Settings

QuerierRouter PortMulticast AddressMulticast PolicyMulticast Port

MLD Snooping

Unknown Multicast Packet

Flood

This option is associated with the same setting under [IGMP Snooping](#)

Multicast Forward Mode

MAC-Based

IP-Based

MLD Version

MLDv1

MLDv2

Report Suppression

Cancel

OK

MLD Snooping Global Settings

Unknown Multicast Packet	Select an action for switch to handle with unknown multicast packet. Drop: Drop the unknown multicast data. Flood: Flood the unknown multicast data. Forward to Router port: Forward the unknown multicast data to router port. Note: This option is associated with the same one IGMP Snooping.
MLD Snooping	Enable or disable Global MLD Snooping
Multicast Forward Mode	Set the Multicast Forward Mode. MAC-Based: Forward using MAC address. IP-Based: Forward using IP address
MLD Version	Select the MLD Version.
Report Suppression	Enable or disable the switch to handle MLD reports between router and host, suppressing bandwidth used by MLD.

MLD Snooping Global Settings

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

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

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

MLD Snooping - Edit VLAN

MLD Snooping Router Port

If the router port is statically configured, the Layer 2 device will also forward the MLD report and leave

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

MLD Snooping

Global SettingsQuerierRouter PortMulticast AddressMulticast PolicyMulticast Port

AddRefreshDelete

☐ VLAN	Static Router Port	Forbidden Port	Dynamic Port	Aging Time (s)	Operation
☐ 1	1/0/1	--	--	--	

Total 1<1>10 / page

MLD Snooping Router Port page

Router Port > Edit

VLAN

1

Static Router Port

Click on port to select/unselect

Port

24

1016

1822

24

13

915

1721

23

2526

2728

LAG

24

1012

14

13

57

911

Forbidden Port

Click on port to select/unselect

Port

24

1016

1822

24

13

915

1721

23

2526

2728

Cancel

OK

Add MLD Snooping Router Port

MLD Snooping Multicast Address

GWN780x Pro Switches also support adding static multicast addresses by specifying the VLAN and member port.

MLD Snooping

Global Settings Querier Router Port **Multicast Address** Multicast Policy Multicast Port

↓

Add Refresh Delete

Q VLAN/Multicast Address/Member Port

☐ VLAN	Multicast Address	Source IP Address	Member Port	Address Type	Aging Time (s)	Operation
						

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

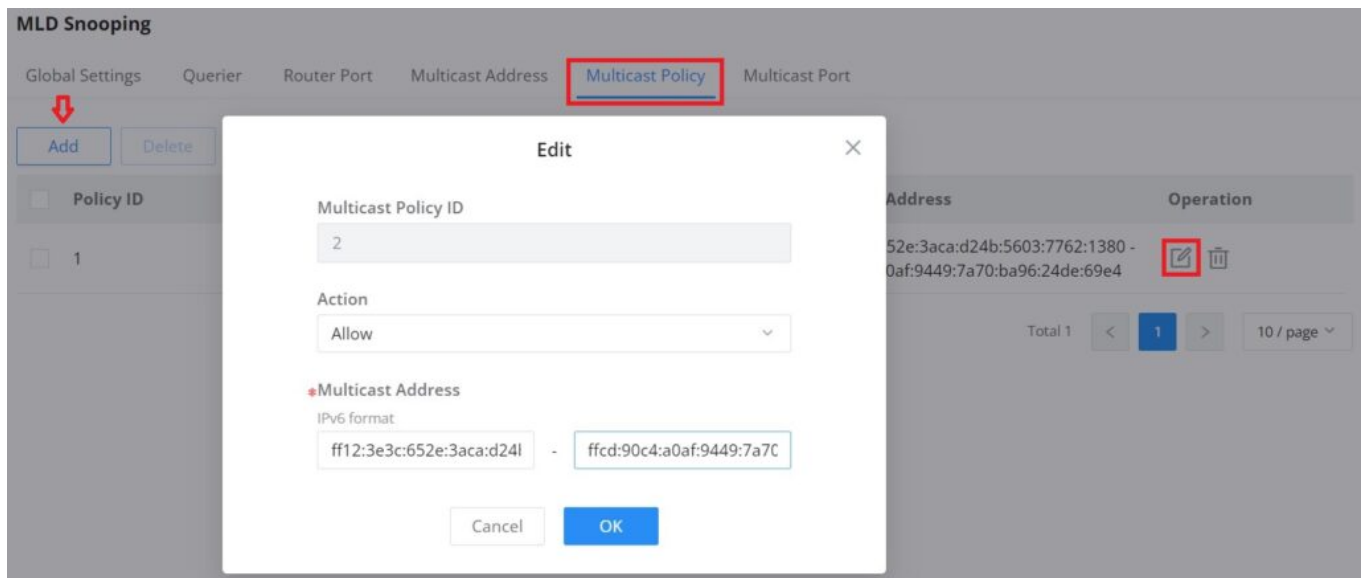
Cancel

OK

Add MLD Snooping Multicast Address

MLD Snooping Multicast Policy

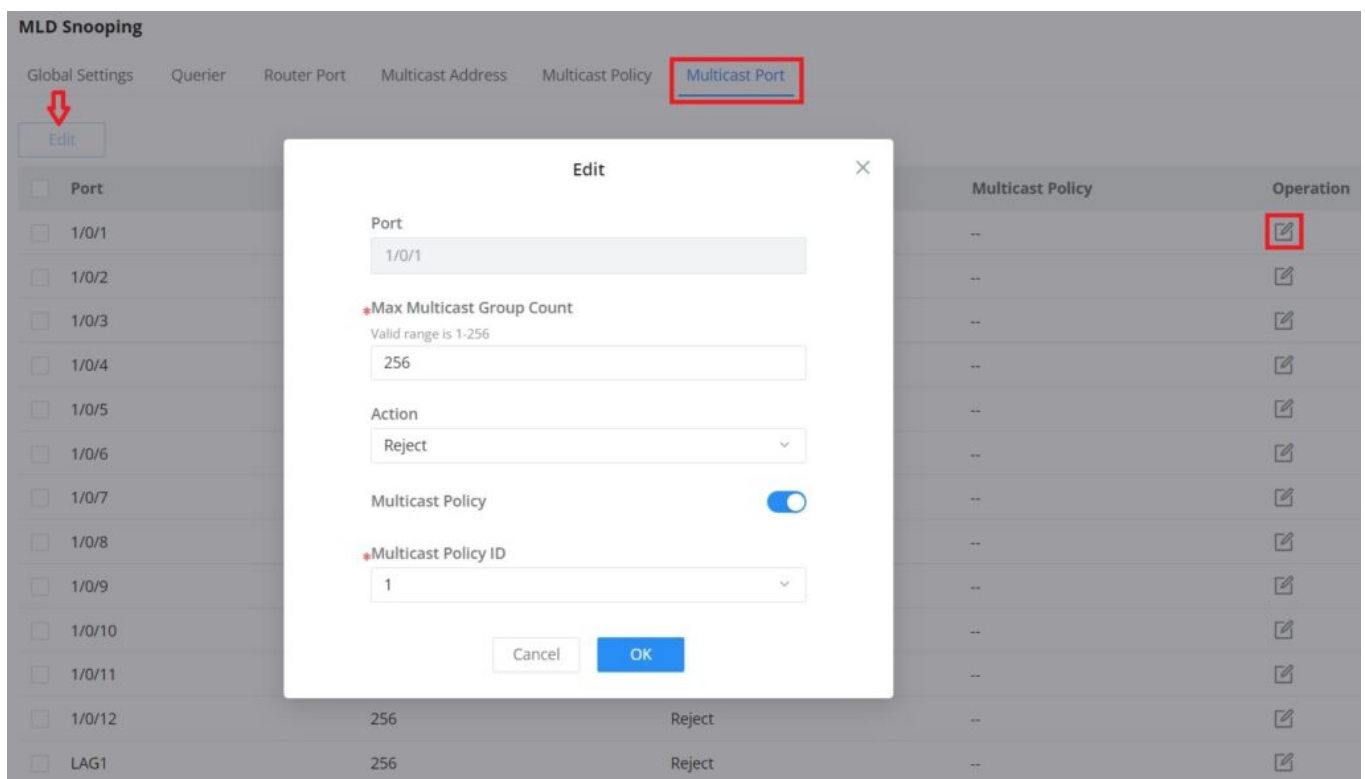
Multicast Policy can be created in this page to allow or reject a range of IPv6 Multicast Addresses. Up to 128 policies can be created.



MLD Snooping Multicast Policy

MLD Snooping Multicast Port

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



MLD Snooping Multicast Port

AV Control

Pro AV

Pro AV (Professional Audio/Video) is a feature set designed to simplify the deployment of networks that carry professional AV traffic. It provides a template-based workflow to create an AV-focused configuration, assign it

to specific ports or link aggregation groups (LAGs), and apply a dedicated VLAN for the AV deployment. Depending on the network design, a configured profile can also enable VLAN routing and provide DHCP service for the AV VLAN.

In the Web UI, navigate to **AV Control -> Pro AV**. The Pro AV page includes two tabs: **Configuration** and **Template**.

Pro AV is built around two pieces:

1. A **Template** represents an AV scenario (for example AES67, Dante, or NDI). Templates also include optional feature flags such as **Multicast** and **E2E TC** (IEEE 1588v2 End-to-End Transparent Clock support). Templates are intended to be reusable.
2. A **Configured Profile** is where the template is actually deployed. A profile selects a template, assigns a **VLAN ID**, and applies the profile to specific **ports and/or LAGs** using **Tagged** or **Untagged** membership. Profiles can additionally enable **VLAN Routing** (create a routed interface for the VLAN) and, if needed, enable the switch's **DHCP Server** for that VLAN.

Template

Open the **Template** tab to view the built-in AV templates and any custom templates you create.

Pro AV

Configuration **Template**

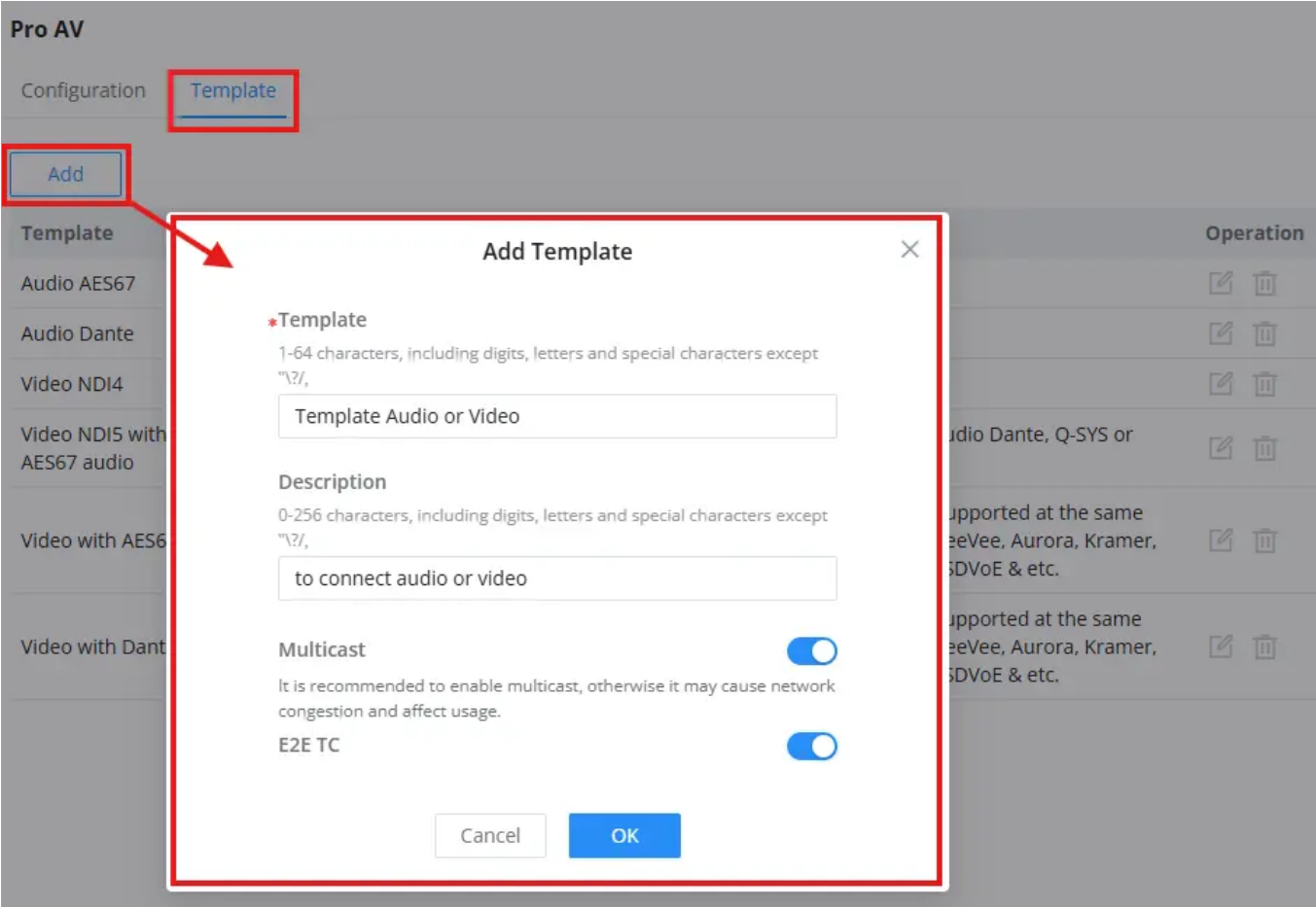
Add

Template	Description	Operation
Audio AES67	To connect IP Audio AES67 devices and their controller	 
Audio Dante	To connect IP Audio Dante devices and their controller	 
Video NDI4	To connect NDI Version 4 (mTCP) video devices and cameras.	 
Video NDI5 with Dante, Q-Sys or AES67 audio	To connect NDI Version 5 (RUDP) video devices and cameras. Audio Dante, Q-SYS or AES67 is supported at the same time in the same VLAN.	 
Video with AES67 audio	To connect IP Video devices and their controller. Audio AES67 supported at the same time in the same VLAN. Supported devices include NVX, AMX, ZeeVee, Aurora, Kramer, Atlona, LibAV, Visionary, Wyrestorm, Extron NAV, Dante Video, SDVoE & etc.	 
Video with Dante audio	To connect IP Video devices and their controller. Audio Dante supported at the same time in the same VLAN. Supported devices include NVX, AMX, ZeeVee, Aurora, Kramer, Atlona, LibAV, Visionary, Wyrestorm, Extron NAV, Dante Video, SDVoE & etc.	 

Pro AV Template Tab

Built-in templates provide ready-to-use scenarios (for example Audio AES67, Audio Dante, Video NDI4, and mixed video/audio templates).

To add a custom template, click **Add** on the Template page. Enter a template name and a description that clearly identifies the intended AV use case. If the deployment relies on multicast traffic, enable **Multicast**. If the AV environment requires timing synchronization support, enable **E2E TC** (IEEE 1588v2 End-to-End Transparent Clock). Click **OK** to save the template.



Add a Template

Field	Description
Template	Enter a name for the template. This name will appear in the template list and in the Template selection list when creating configured profiles.
Description	Enter a brief description to identify the intended AV use case.
Multicast	Enables multicast support for the template. Enable this option when multicast discovery or multicast streams are expected in the AV deployment.
E2E TC	Enables IEEE 1588v2 End-to-End Transparent Clock (PTP) support for the template. Enable this option when the AV deployment requires precise time synchronization.

Add a Template

Configuration

Open the **Configuration** tab to create, apply, and manage configured profiles. This page provides a visual map of **ports** and **LAGs** and a table listing existing profiles.

Pro AV

Configuration

Template

Port

LAG

Configured Profiles

Add

Configured Profiles	Template	VLAN ID	IP Address	Num. of Ports	Operation
 No Data					

Pro AV Configuration tab

Configured profiles are displayed with key details such as the selected template, VLAN ID, and (when VLAN routing is enabled) the VLAN interface IP address. The color indicator helps you visually identify which ports belong to a profile in the port map.

To create a new profile, click **Add** under **Configured Profiles** on the Configuration tab. The profile creation process includes two parts: selecting members (ports/LAGs) and defining profile settings.

Configuration > Add Configured Profile

Member Type

Please select

Remove All

Tagged All

Untagged All

Port

Click port to change the member type

Port selection interface showing 10 ports (1-10) and 2.5G ports (9, 10). Port 6 is selected with a blue 'U' icon (Untagged). Port 5 is selected with a blue 'T' icon (Tagged). A legend indicates 'T' for Tagged and 'U' for Untagged.

LAG

Click port to change the member type

LAG selection interface showing 8 LAG members (1-8). Port 6 is selected with a blue 'U' icon (Untagged). Port 3 is selected with a blue 'T' icon (Tagged). A legend indicates 'T' for Tagged and 'U' for Untagged.

Pro AV Profile Selecting members

First, assign member interfaces. You can click ports (and LAG members) to set their membership type. Membership type determines how the VLAN is presented on that interface:

- Tagged membership is typically used for uplinks or trunks where VLAN tags must be carried.
- Untagged membership is typically used for endpoint devices that do not tag VLANs (common for many AV endpoints).

If you are adding many ports at once, use the **Member Type** drop-down to apply bulk changes (for example set all selected ports to Tagged or Untagged, or remove all assignments).

Next, configure the profile settings in the **Add Configured Profile** page. Complete the required fields, then enable optional features such as **VLAN Routing** and **DHCP Server** if they are needed for the AV VLAN. The purpose of each field is described in Table below. Click **OK** to save the profile and apply the configuration to the selected ports/LAGs.

★Configured Profiles

Audio & Video

1-64 characters, including digits, letters and special characters except "\?/,

★Template

Template Audio or Video

★VLAN ID

10

Valid range is 1-4094

Color

#6699FF

VLAN Routing

☒

Address Type

☒ Static IP
 ☐ DHCP

★IP Address

10.0.0.5

IPv4 format

★Subnet Mask

255.0.0.0

IPv4 format

DHCP Server

☒

★Address Pool

10.0.0.1

-

10.255.255.254

Preferred DNS Server ⓘ

10.0.0.1

Alternative DNS Server

★Duration (min)

120

Valid range is 1-11520

Cancel

OK

Pro AV configure the profile settings

Field	Description
Configured Profiles	Enter a name for the configured profile. This name appears in the Configured Profiles list.
Template	Select the Pro AV template to apply with this profile.
VLAN ID	Enter the VLAN ID used for this AV deployment.
Color	Select a color used to visually identify member ports for this profile in the port map.
VLAN Routing	Enables routing for the AV VLAN. When enabled, the switch creates a VLAN interface for this VLAN and allows Layer 3 configuration.
Address Type	Select how the VLAN interface obtains an IPv4 address: Static IP or DHCP.
IP Address	Enter the IPv4 address for the VLAN interface (required when Address Type is set to Static IP).
Subnet Mask	Enter the subnet mask for the VLAN interface (required when Address Type is set to Static IP).
DHCP Server	Enables the DHCP server for the AV VLAN so the switch can assign IP addresses to devices in this VLAN.
Address Pool	Specifies the DHCP address range assigned to clients in this VLAN.
Preferred DNS Server	Specifies the primary DNS server provided to DHCP clients.
Alternative DNS Server	Specifies the secondary DNS server provided to DHCP clients.
Duration (min)	Specifies the DHCP lease duration, in minutes.

Click **OK** to save the profile. After creating the profile, the selected ports/LAGs are associated with the profile and the profile appears in the configured profile list.

Pro AV

Configuration Template

Port



LAG



Configured Profiles

Add

Configured Profiles	Template	VLAN ID	IP Address	Num. of Ports	Operation
 Audio & Video	Template Audio or Video	10	10.0.0.5	2	  

Pro AV after the Profile is applied

Once applied, the configured profile provides a consistent deployment method: ports are placed into the specified VLAN (tagged/untagged as configured), and optional services (VLAN routing and DHCP) are applied if enabled. This lets you build an AV segment quickly and keep the configuration consistent across all ports used for AV devices.

ROUTING

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

GWN780x Pro supports IPv4 and IPv6 static routing.

Routing Table

The Routing Table page displays the routes used by the switch to forward packets between networks or VLANs. Routing enables the switch to function as a Layer 3 device, allowing it to make packet forwarding decisions based on destination IP addresses.

GWN780x Pro switches support both **IPv4** and **IPv6** static routing. This section includes options for viewing

current routes and configuring the **Forwarding Mode**.

Forwarding Mode

Choose between **Traditional** and **Manual**.

- **Traditional** -> automatic ARP/neighbor learning for routing between VLANs.
- **Manual** -> disables that automation; forwarding depends only on static routes and static ARP entries.

Notes:

- If the number of hosts on VLAN interfaces exceeds **64** (as with models like GWN7801P Pro, GWN7802P Pro, or GWN7803PL/PH Pro), it is recommended to use **Manual mode** to ensure proper routing behavior and compatibility with **Strict ARP Learning**.
- When **Strict ARP Learning** is enabled under **Web UI -> IP -> ARP Table**, the **Forwarding Mode** should be manually set here to ensure stable communication and avoid exceeding ARP limits.

To view and manage routes:

Go to **Web UI -> Routing -> Routing Table**.

Routing Table

IPv4 Routing Table IPv6 Routing Table

Forwarding Mode ⓘ Traditional

When the number of hosts on the VLAN interfaces of the device exceeds 64, it is recommended to use "Manual" mode.

Cancel OK

Refresh

All Types Q Destination IP Address/Next...

Destination IP Address	Protocol Type	Priority	Cost	Next Hop	Outgoing Interface	Flags ⓘ
0.0.0.0/0	DHCP	1	0	172.16.142.1	VLAN 1720	SFA
192.168.180.0/24	Direct	0	0	0.0.0.0	VLAN 180	SFA
172.16.142.0/23	Direct	0	0	0.0.0.0	VLAN 1720	SFA
169.254.100.0/24	Direct	0	0	0.0.0.0	VLAN 100	SFA

Total 4 < 1 > 10 / page

Routing Table

IPv4 Routing Table

In the **IPv4 Routing Table** tab, users can view and manage all IPv4 routing entries. Each entry defines how packets should be forwarded based on their destination IP address and subnet mask.

The table displays the following details for each entry:

- **Destination IP Address**
- **Protocol Type** (Static, DHCP, or Direct)
- **Priority**
- **Cost**
- **Next Hop**
- **Outgoing Interface**
- **Flags**

Forwarding Mode

The **Forwarding Mode** option defines how the switch handles routing and neighbor table behavior.

- **Traditional:** Direct routes and neighbor tables take effect normally.
- **Manual:** Direct routes become invalid, and only static entries in the neighbor table are used.

Tip: When the number of hosts on VLAN interfaces exceeds 64, it is recommended to use Manual mode for improved stability and performance.

IPv6 Routing Table

The **IPv6 Routing Table** tab allows configuration and monitoring of IPv6 routes. It provides the same functional options as the IPv4 table but applies to IPv6 addressing and neighbor discovery mechanisms.

Static Routes

Static routes are manually configured forwarding entries. They remain in effect until they are edited or deleted and do not automatically adapt when the network topology changes.

Navigate to **Routing -> Static Routes**. Use the **IPv4 Static Routes** and **IPv6 Static Routes** tabs to manage each address family.

Static Routes

IPv4 Static Routes

IPv6 Static Routes

Number of IPv4 Static Routes

1024

Valid range is 0-3010

Cancel

OK

Routing Resources

Add

Delete

Q Destination IP Address/Next ...

☐	Destination IP Address	Mask Length	Priority	Next Hop	Outgoing Interface	Operation
☐	0.0.0.0	0	1	172.16.142.1	--	

Total 1

< 1 >

10 / page

© 2026 Grandstream Networks, Inc.

Grandstream Software License Agreement

Static Routes

Configure Static Route Capacity

Use **Number of IPv4 Static Routes** or **Number of IPv6 Static Routes** to set the static-route capacity for that address family within the range displayed by the switch. **Routing Resources** shows the current allocation and available capacity.

Unicast routing statistics information distribution:

Routing-Name	Attribute	IPv4	IPv6	Multiple
Hardware	Read-Only	2562	2563	0
Default	Read-Only	1	1	0
Direct	Read-Only	32/0	33/0	0/0
Static	Read-Write	0	0	0

Summary:

IPv4 Current Direct Routing 1, IPv6 Current Direct Routing 1.

IPv4 left Static Routing 1024, IPv6 left Static Routing 1024, Multiple 0.

Dynamically adjust the maximum value : IPv4 Unicast Routing 3010, IPv6 Unicast Routing 3010, Multiple 0.

Codes: Attribute

Read-Only: This type of route cannot be modified.

Read-Write: This type of routing can modify the specification size.

Add a Static Route

1. Select **IPv4 Static Routes** or **IPv6 Static Routes**, then click **Add**.
2. Enter the destination address and its **Mask Length** or **Prefix Length**.
3. For IPv4, select **Next Hop** or **Outgoing Interface** under **Gateway**. For IPv6, enter the next hop, select the outgoing interface, or configure both as required.
4. Set the **Priority**. Lower values have higher priority.
5. Click **OK**, then click **Save** to apply the pending configuration.

Add IPv4 Static Route



*Destination IP Address

*Mask Length

Valid range is 0-32

Gateway

☒ Next Hop

☐ Outgoing Interface

*Next Hop

*Priority

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

Cancel

OK

Add IPv4 Static Route

Add IPv6 Static Route



❗ If the next hop is the link-local address, the outgoing interface and next hop must be configured at the same time. Otherwise, only the next hop or outgoing interface needs to be configured.

*Destination IPv6 Address

*Prefix Length

Valid range is 0-128

Next Hop

Outgoing Interface

Cancel

OK

Add IPv6 Static Route

Field	Description
IPv4 Static Routes / IPv6 Static Routes	Select the tab for the route's address family.
Number of IPv4/IPv6 Static Routes	Sets the static-route capacity for the selected address family. Enter a value within the valid range displayed by the switch, click OK, and save the pending configuration.
Routing Resources	Shows the IPv4 and IPv6 hardware, default, direct, and static-route allocations and the remaining capacity. Hardware, default, and direct routes are read-only; the static-route allocation is read-write.
Destination IP Address	Enter the destination IPv4 network address.
Mask Length	Enter the IPv4 mask length from 0 to 32.
Destination IPv6 Address	Enter the destination IPv6 network address.
Prefix Length	Enter the IPv6 prefix length from 0 to 128.
Gateway	For an IPv4 route, select Next Hop or Outgoing Interface.
Next Hop	Enter the next-hop IPv4 or IPv6 address.
Outgoing Interface	Select the interface used to forward matching traffic. For an IPv6 link-local next hop, both the next hop and outgoing interface are required; otherwise, the IPv6 form accepts either one.
Priority	Enter a value from 1 to 255. A smaller value has a higher priority.

Policy Route

Policy Route forwards IPv4 or IPv6 traffic that matches a selected ACL rule to a specified next hop. Use the separate IPv4 and IPv6 tabs to manage policies for each address family.

Navigate to **Routing -> Policy Route**.

Policy Route

[IPv4 Policy Route](#)

IPv6 Policy Route



Routes are forwarded based on the specified policies

Add

Policy Route

Add a Policy Route

A policy route references an existing ACL rule to identify the traffic that the switch forwards to the configured next hop.

1. Select **IPv4 Policy Route** or **IPv6 Policy Route**, then click **Add**.
2. Enter a policy **Name**.
3. Select the **ACL Name** and the matching **Rule ID**. Click **View rules** when you need to review the selected

ACL.

- 4. Enter the **Next Hop**. For an IPv6 link-local next hop, also select the **Outgoing Interface**.
- 5. Click **OK**, then click **Save** to apply the pending configuration.

IPv4 Policy Route > Add IPv4 Policy Route

✖Name

1-64 characters allowed, including digits, letters and special characters except “/”;

✖ACL Name

✖Rule ID

📄View rules

✖Next Hop

Cancel

OK

© 2026 Grandstream Networks, Inc. Grandstream Software License Agreement

Add IPv4 Policy Route

IPv6 Policy Route > Add IPv6 Policy Route

ⓘ If the next hop is a link-local address, both the next hop and the outgoing interface must be configured. Otherwise, only the next hop is required.

✖Name

1-64 characters allowed, including digits, letters and special characters except “/”;

✖ACL Name

✖Rule ID

📄View rules

✖Next Hop

Outgoing Interface

Cancel

OK

© 2026 Grandstream Networks, Inc. Grandstream Software License Agreement

Add IPv6 Policy Route

Field	Description
IPv4 Policy Route / IPv6 Policy Route	Select the tab that matches the address family of the traffic and next hop.
Name	Enter a name from 1 to 64 characters. The interface accepts letters, digits, and supported special characters.
ACL Name	Select the ACL that contains the rule used to match traffic. Use Add in the selector if a suitable ACL is not available.
Rule ID	Select the rule within the chosen ACL. Use View rules to review the ACL rule definitions.

Next Hop	Enter the IPv4 or IPv6 address of the next-hop router for matching traffic.
Outgoing Interface	For an IPv6 link-local next hop, select the outgoing interface. For other IPv6 next-hop addresses, only the next hop is required. This field is not displayed for IPv4 policy routes.

POE

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

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

Global

This page displays PoE power-supply information, including the number of PoE ports, total and remaining PoE power, and supply voltage. The GWN7801P Pro provides a total PoE budget of **130 W**.

Global

Power Supply Info

Settings

PoE Reboot

Global	
Number of PoE Interfaces	8
Total PoE Power	120W
PoE Reserved Power	20W
Configured Power	0W
PoE Power Consumption	0.0mW
PoE Power Supply Support Type	802.3 af/at

Chip1	
Operation Status	On
Supply Voltage	54.0V

PoE Global -> Power Supply Info

Click on the "PoE Reboot" button to soft-restart the PoE module function.

PoE Reserved power

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

Global

Power Supply Info Settings

*PoE Reserved Power (W)

20

Valid range is 0-119

Cancel

OK

PoE Global Settings

Application scenarios:

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

Interface PoE configuration

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

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

Interface

Edit

☐	Interface	Power Status	Power Supply Standard	Power Mode	Power Supply Priority	Operation
☒	1/0/1	Unpowered	802.3at	Auto	Low	
☐	1/0/2	Unpowered	802.3at	Auto	Low	
☐	1/0/3	Unpowered	802.3at	Auto	Low	
☐	1/0/4	Unpowered	802.3at	Auto	Low	
☐	1/0/5	Unpowered	802.3at	Auto	Low	
☐	1/0/6	Unpowered	802.3at	Auto	Low	
☐	1/0/7	Unpowered	802.3at	Auto	Low	
☐	1/0/8	Unpowered	802.3at	Auto	Low	

Total 8

<

1

>

10 / page ▾

PoE Interface page

Interface	1/0/1
Power Supply Standard	802.3bt
Power Mode	Auto
Power Limit Mode	Class
Power Supply Priority	Low
Power-Off Schedule	None
Cancel OK	

PoE Interface edit port

QoS

The 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, 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" policy that governs 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

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

Please navigate to **Web UI -> QoS -> Port Priority** page.

Port Priority

Edit

☐	Port	Trust Mode	CoS	Remarking CoS	Remarking DSCP	Remarking IP Precedence	Operation
☐	1/0/1	802.1p	6	Enabled	Disabled	Disabled	
☒	1/0/2	None	0	Disabled	Disabled	Disabled	
☒	1/0/3	None	0	Disabled	Disabled	Disabled	
☒	1/0/4	None	0	Disabled	Disabled	Disabled	
☐	1/0/5	None	0	Disabled	Disabled	Disabled	

QoS Port Priority

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

Edit Port Priority

Port

1/0/1

Trust Mode

802.1p

*CoS

Valid range is 0-7.

6

Remarking CoS



Remarking DSCP



Remarking IP Precedence



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

Cancel

OK

Edit Port Priority

Port	Displays the selected port GE/LAG.
Trust Mode	Select the QoS operation mode: None: no packet priority is trusted, and the interface default priority is used. CoS: Traffic is mapped to queues based on the CoS Queue Mapping, it can configured in QoS -> Priority Mapping -> CoS Mapping page. DSCP: All IP traffic is mapped to queues based on the DSCP field in the IP header. If the traffic is not IP traffic, it is mapped to the lowest priority queue. CoS-DSCP: All IP traffic is mapped to queues based on the DSCP field in the IP header. If the traffic is not IP traffic but has VLAN tag, mapped to queues based on the CoS value in the VLAN tag. it can configured in QoS -> Priority Mapping -> DSCP Mapping page. IP-Precedence: The IP precedence is a 3-bit field in TOS that threats high priority packets as more important than other packets. it can configured in QoS -> Priority Mapping -> IP Mapping page.
CoS	Set the CoS value of the interface, the value range is an integer from 0 to 7 (7 is the highest priority), the default is 0.
Remarking CoS	Set whether to enable Remarking CoS function of outgoing packets, which is disabled by default.
Remarking DSCP	Set whether to enable Remarking DSCP function of outgoing packets, and it is disabled by default.
Re-marking IP Precedence	Set whether to enable Remarking IP Precedence function of outgoing packets, and it is disabled by default.Note : Only one of DSCP and IP Precedence re-marking can be enabled.

Priority Mapping

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

- CoS Mapping

Shows the mapping relationship between queues and CoS remarking priorities.

Priority Mapping

CoS Mapping

DSCP Mapping

IP Mapping

802.1p (CoS) - Queue Mapping

Reset

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

Queue-CoS Remarking Mapping

Reset

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

Cancel

OK

CoS Mapping

- DSCP Mapping

Shows the mapping relationship between DSCP values and queue priorities.

Priority Mapping

CoS Mapping [DSCP Mapping](#) IP Mapping

DSCP-Queue Mapping

[Reset](#)

DSCP	Queue	DSCP	Queue	DSCP	Queue	DSCP	Queue	DSCP	Queue	DSCP	Queue	DSCP	Queue	DSCP	Queue
0[CS0]	0	8[CS1]	1	16[CS2]	2	24[CS3]	3	32[CS4]	4	40[CS5]	5	48[CS6]	6	56[CS7]	7
1	0	9	1	17	2	25	3	33	4	41	5	49	6	57	7
2	0	10[AF11]	1	18[AF21]	2	26[AF31]	3	34[AF41]	4	42	5	50	6	58	7
3	0	11	1	19	2	27	3	35	4	43	5	51	6	59	7
4	0	12[AF12]	1	20[AF22]	2	28[AF32]	3	36[AF42]	4	44	5	52	6	60	7
5	0	13	1	21	2	29	3	37	4	45	5	53	6	61	7
6	0	14[AF13]	1	22[AF23]	2	30[AF33]	3	38[AF43]	4	46[EF]	5	54	6	62	7

[Cancel](#)

[OK](#)

DSCP Mapping

- IP Mapping

Shows the mapping relationship between IP priority and queue.

Priority Mapping

CoS Mapping [DSCP Mapping](#) [IP Mapping](#)

IP-Queue Mapping

[Reset](#)

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

Queue-IP Remarking Mapping

[Reset](#)

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

[Cancel](#)

[OK](#)

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):** Based on 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

Edit

☐	Port	Queuing Algorithm	Weight								Operation
			0	1	2	3	4	5	6	7	
☒	1/0/1	Weighted Fair Queuing(WFQ)	90	95	100	105	110	115	120	127	
☐	1/0/2	Weighted Round Robin (WRR)	1	20	30	50	70	90	100	127	
☐	1/0/3	SP-WFQ	0	30	40	55	77	99	111	127	
☐	1/0/4	SP-WRR	0	30	44	50	77	99	111	127	
☐	1/0/5	Strict Priority (SP)	--	--	--	--	--	--	--	--	

Queue Scheduling

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

Queue Shaping									
CIR Maximum Rate/CIR (Kbps)									
Port	Queue								Operation
	0	1	2	3	4	5	6	7	
1/0/1	100000	--	--	--	--	--	--	--	
1/0/2	--	--	--	--	--	--	--	--	
1/0/3	--	--	--	--	--	--	--	--	
1/0/4	--	--	--	--	--	--	--	--	
1/0/5	--	--	--	--	--	--	--	--	
1/0/6	--	--	--	--	--	--	--	--	
1/0/7	--	--	--	--	--	--	--	--	
1/0/8	--	--	--	--	--	--	--	--	

Queue Shaping

To configure a port, click on the "Edit" icon under the 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 multiple of 16. By default, it's the port rate.

Queue Shaping > Edit

Port1/0/2

Queue ID	Enable	Maximum Rate/CIR (Kbps) ⓘ
0	☒	1000000
1	☐	
2	☐	
3	☐	
4	☐	
5	☐	
6	☐	
7	☐	

Cancel

OK

Configuration of Maximum Rate

Rate Limit

The interface rate limit controls the total traffic sent or received on a port through a token bucket. When the configured rate is non-zero, excess packets can be dropped and the dropped-packet counter can be reviewed in Statistics. When the rate is set to zero, select whether matching traffic is dropped or the port enters an err-disabled state.

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 the **"Edit"** icon under the 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		

Rate Limit Edit a port

SECURITY

GWN780x Pro Switches series supports 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 dropping packets or shutting down interfaces.

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

Storm Control

Unit

IFG ☒ Include ☐ Exclude

Port

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

Storm Control page

Storm Control > Edit

Port

Storm Control ☒

Broadcast ☒

*Threshold (Kbps)

Unknown Multicast ☒

*Threshold (Kbps)

Unknown Unicast ☒

*Threshold (Kbps)

Action ☒ Drop ☐ Disabled

Storm Control edit port

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

Unknown Multicast	Set whether to enable the storm threshold setting for the Unknown Multicast packets. If Enabled Please enter a Treshold (Kbps).Note: The valid range is 16~1000000, which must be a multiple of 16. Default is 10000.
Unknown Unicast	Set whether to enable the storm threshold setting for the Unknown Unicast packets. If Enabled Please enter a Treshold (Kbps).Note: The valid range is 16~1000000, which must be a multiple of 16. Default is 10000.
Action	Select the state of setting Drop: Packets exceed storm control rate will be dropped. Shutdown: Port exceeds storm control rate will be shutdown.

Storm Control

Port Security

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

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

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

Secure MAC Address Types

The screenshot displays the 'Port Security' configuration page. A modal window for 'Edit Port Security' is active for port 1/0/3. In this modal, the 'Port Secure Addresses' and 'Sticky MAC' options are enabled (toggled on). The 'Max Number of Allowed MAC Addresses' is set to 1. The 'Port Protection' is set to 'protect'. The background interface shows a list of ports (1/0/1 to 1/0/6) all with a 'Disabled' status. To the right, there is a table for 'Secure MAC Addresses' with columns for 'Number of Static Secure MAC Addresses' and 'Operation'. The 'Operation' column contains edit icons for each entry.

Port Security

Global Settings	
Port Security	Enables or disables Port Security globally. The default is disabled.
Rate Limit (packet/s)	Sets the port MAC-address learning rate from 1 to 600 packets per second. The default is 100.

Edit Port Security	
Port	Displays the selected port.
Port Security Address	Enables secure MAC-address learning on the selected port. The default is disabled.
Maximum MAC Number	Sets the maximum number of MAC addresses learned by the interface. The valid range is 0-2048. After the maximum is reached, a packet with an unknown source MAC address triggers the configured Port Protection action.
Sticky MAC	Converts learned secure dynamic MAC addresses into Sticky MAC entries. When the maximum is reached, additional non-sticky entries are discarded and a trap can be reported according to the protection mode.
Port Protection	Selects the action used when the learned-MAC limit is reached or static MAC flapping occurs: Protect: discards packets whose source MAC address does not exist, without reporting an alarm. Restrict: discards the packets and reports an alarm. Shutdown: places the interface in error-down and reports an alarm. Recovery is manual unless Port Auto Recovery is enabled.

Port Isolation

Port Isolation separates interfaces within the same VLAN. Select **Layer 2 isolated, Layer 3 communication** to block Layer 2 forwarding while retaining Layer 3 communication, or select **Both Layer 2 and Layer 3 are isolated**. For each interface, **Unidirectional Isolation** prevents it from sending to the selected isolated interface, while **Bidirectional Isolation** prevents either interface from sending to the other.

Port Isolation

Isolation Mode

☒ Layer 2 isolated, Layer 3 communication

☐ Both Layer 2 and Layer 3 are isolated

Cancel

OK

Isolation Group

Unidirectional Isolation: The isolation group interface stops sending data to the unidirectionally isolated interface. Bidirectional isolation: Neither interface sends data to the other.

Clear Configuration

☐	Interface	Bidirectional Isolation	Unidirectional Isolation	Operation
☐	1/0/1	--	--	
☐	1/0/2	--	--	
☐	1/0/3	--	--	
☐	1/0/4	--	--	
☐	1/0/5	--	--	
☐	1/0/6	--	--	
☐	1/0/7	--	--	

Port Isolation Modes and Directional Isolation

ACL

An Access Control List (ACL) contains packet-matching rules and the actions applied when those rules match. ACL advanced statistics include the current statistics rate and manual refresh, while CLI output also reports ACL resource utilization.

IPv4/IPv6 ACL

To add an IPv4 or IPv6 ACL rule, navigate to **Security -> ACL -> IPv4 tab or IPv6 tab**, then click on the "

Add" button to add an IPv4/IPv6-based ACL rule.

ACL > **Add ACL**

*ACL Name	ACL_rule
Rule Settings	
*Rule ID	1
Action	Allow
Protocol Type	Any
Source IP Address	☐ Any ☒ Custom
*Source IP Address	192.168.80.0
*Source IP Mask	255.255.255.0
Destination IP Address	☒ Any ☐ Custom
Tos Type	Any
Time Policy	None

ACL IPv4IPv6

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

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

Tos Type Any

Time Policy None

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 Disabled

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

ACL IPv4IPv6 Advanced Settings

Tos Type

Time Policy

Advanced Settings

Count

Mirroring

Priority Mapping

Rate Limit

Any

Disabled

1

2

3

4

5

6

7

1

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

Cancel

OK

ACL IPv4IPv6 Rate Limit

Configuring an ACL-based RSPAN

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

- Select an image group in ACL Image

IPv4 ACL > Add ACL

Rule Settings

Rule ID

1

Valid range is 1-2147483647. The smaller ID is matched first.

Action

Allow

Protocol Type

Any

Source IP Address

☒ Any ☐ Custom

Destination IP Address

☒ Any ☐ Custom

Tos Type

Any

Time Policy

None

Advanced Settings

Count

☐

Mirroring

☒

Mirroring Group

Group 1

Go to "Maintenance>Diagnostics>Mirroring" to configure take effect

Priority Mapping

☐

Rate Limit

Disabled

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

Cancel

OK

ACL Based RSPAN

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

ACL

IPv4 ACL IPv6 ACL MAC ACL Port Binding to ACL **VLAN Binding to ACL** Rate Limit Settings

Edit Unbind

VLAN	IPv4 ACL Name	MAC ACL Name	Operation
1	--	--	 

Total 1 < 1 > 10 / page

Edit

VLAN

1

IPv4 ACL

TEST

MAC ACL

None

Cancel

OK

© 2024 Grandstream Networks, Inc. Grandstream Software License Agreement

IPv4 ACL VLAN

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

Role

Source Switch

Ingress Mirroring

Click on port to select/unselect

Port

2 4 6 8 10 12 14 16 18 20 22 24

1 3 5 7 9 11 13 15 17 19 21 23 25 SFP1 26 SFP2 27 SFP3 28 SFP4

LAG

2 4 6 8

1 3 5 7

Egress Mirroring

Click on port to select/unselect

Port

2 4 6 8 10 12 14 16 18 20 22 24

1 3 5 7 9 11 13 15 17 19 21 23 25 SFP1 26 SFP2 27 SFP3 28 SFP4

LAG

2 4 6 8

1 3 5 7

Output Port

1/0/4

Remote VLAN

Please select

Please select Remote VLAN

Cancel OK

Set up Mirroring Group

MAC ACL

To add an ACL based on the MAC address, on the MAC ACL tab, click on the **"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 Name

Rule Settings

*Rule ID

Action

Protocol Type ☒ Any ☐ Custom

Source MAC Address ☐ Any ☒ Custom

*Source MAC Address : : : : :

*Source MAC Mask : : : : :

Destination MAC Address ☒ Any ☐ Custom

VLAN ☒ Any ☐ Custom

802.1p Priority

Time Policy

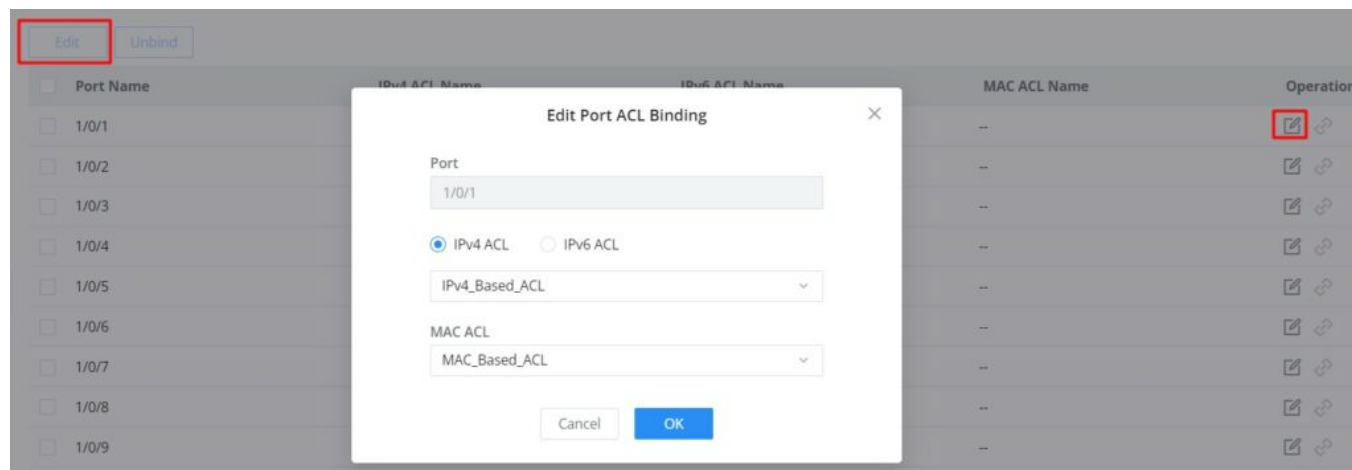
MAC address based ACL

Port Binding to ACL

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

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

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



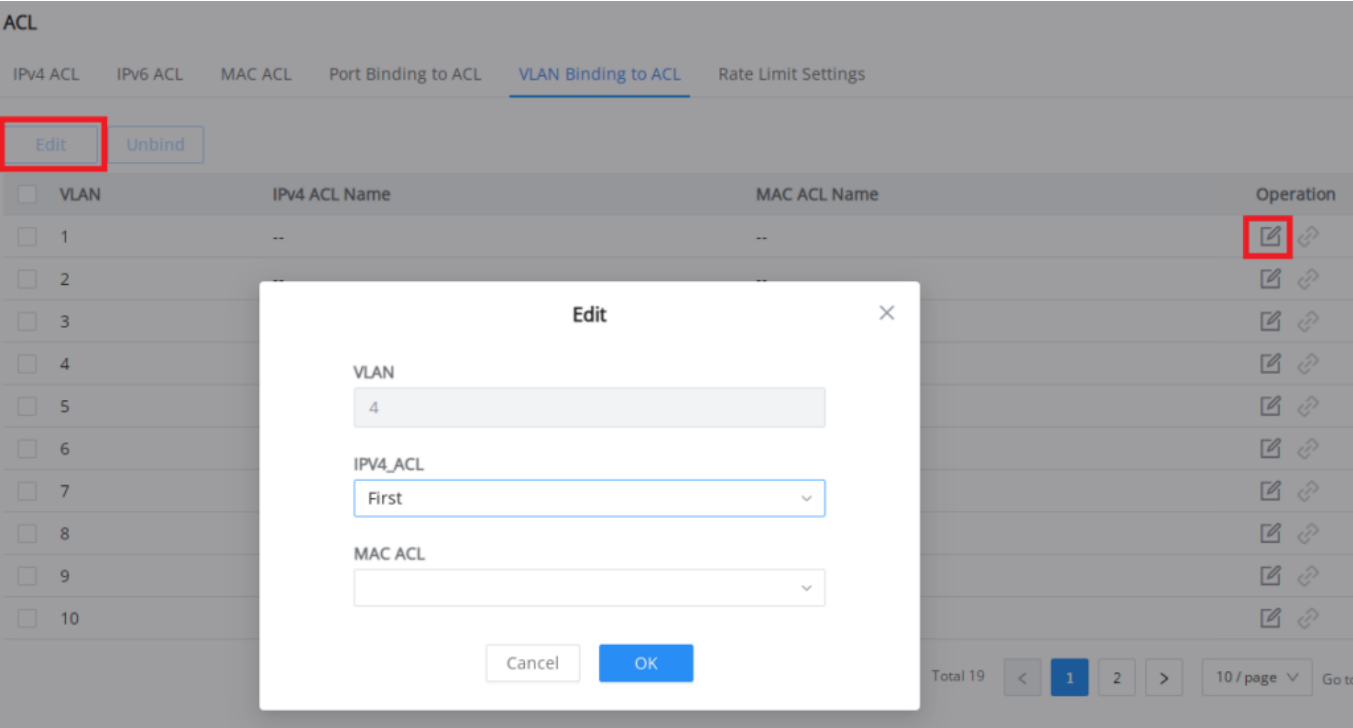
ACL Binding

VLAN Binding to ACL

On this page, the users can bind the IP/MAC ACL rule to a VLAN(s), to apply the ACL rules to multiple VLANs. First, check the VLANs from the list, then click on the "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 a 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

ACL Rate Limit Settings provides 128 reusable rate-limit groups. For each group, select a packet- or byte-based **Rate Limit Type**, then configure the **Burst Threshold** and **Rate Threshold**. The group is referenced by the applicable ACL rule; this page defines the thresholds rather than a separate drop or error-disable action.

ACL

IPv4 ACL

IPv6 ACL

MAC ACL

Port Binding to ACL

VLAN Binding to ACL

Rate Limit Settings

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	--	--	--	

The users can configure up to 128 groups by clicking on the "**Edit icon**" under the 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.

Edit



Rate Limit Group ID

Rate Limit Type

☒ By packet ☐ By byte

*Burst Packet (pps)

Valid range is 1-65535

*Rate Threshold (pps)

Valid range is 1-262143

ACL Edit Rate Limit Group

IP Source Guard

IP source guard is a source IP address filtering technology based on the 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 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.

To enable IP Source Guard, first navigate to the **Security -> IP Source Guard** page, then select the port and

click on "Edit" to configure the port.

IP Source Guard

Port Protection Quaternary Binding Table

Edit

Port	IP Source Guard	Verification Type	Number of Quaternary Bindings	Operation
☐ 1/0/1	Disabled	IP	1	
☒ 1/0/2	Enabled	IP	--	
☐ 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

Valid range is 0-50. 0 indicates no limit.

0

Cancel

OK

IP Source Guard Edit port

This page displays the dynamic binding (port, IP, MAC, VLAN) generated when DHCP Snooping is enabled on the GWN780x Pro switches. Also, the user can add static binding by clicking on the "Add" button, as shown below:

To import or export the list, click on the 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
☐	1/0/1	192.168.80.5	C0:74:AD:FF:FF:FF	1	Static	--	

Total 1

<1>

10 / page

Quaternary Binding Table

The binding requires specifying the port, IP Address and its mask, MAC address and its mask, and the VLAN ID. This information will be used to verify the traffic and ensure that all the traffic is generated by legitimate users.

Add Quaternary Binding

*Port

1/0/1

*IP Address

IPv4 format

192.168.80.3

*Mask ⓘ

IPv4 format

255.255.255.255

MAC Address

The MAC address must be a unicast address.

c0 : 74 : ad : dd : dd : dd

*Mask

FF : FF : FF : FF : FF : FF

*VLAN

Valid range is 1-4094

1

Cancel

OK

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
☐ 1/0/1	Disabled	IPv6	--	
☒ 1/0/2	Enabled	IPv6	--	
☐ 1/0/3	Disabled	IPv6	--	

IPv6 Source Guard

To enable IPv6 Source Guard on a port, select the port and click on the "Edit" button under the 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**

Valid range is 0-50. 0 indicates no limit.

0

Cancel

OK

IPv6 Source Guard Edit port

On this tab, the user can see the list of bindings, both static and dynamic (DHCP Snooping must be enabled). To add a static entry, click on the "**Add**" button. It's also possible to import or export the list as shown below:

IPv6 Source Guard

Port Protection Quaternary Binding Table

Add		Delete	Refresh	Import	Export		
☐	Port	IPv6 Address	MAC Address	VLAN	Type	Lease Time (s)	Operation
☐	1/0/1	2001:db8:85a3::8a2e: 370:7334	C0:74:AD:FF:FF:FF	1	Static	--	

Total 1 < 1 > 10 / page

IPv6 Quaternary Binding Table

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

Add Quaternary Binding

*Port

1/0/1

*IP Address

IPv6 format and must be a valid unicast address

2001:db8:3333:4444:5555:6666:7777:8888

*Prefix Length

Valid range is 1-128

128

MAC Address

The MAC address must be a unicast address.

c0 : 74 : ad : d5 : 44 : 5a

*Mask

FF : FF : FF : FF : FF : FF

*VLAN

Valid range is 1-4094

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 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

Abnormal

Land

Smurf Attack

*Netmask Length

TCP Attack

SMAC=DMAC

ICMP Ping

IPv4 Ping of Death

Blat

8

Valid range is 0-32

Flag Illegal Attack

☒ SYN-RST

☒ SYN-FIN

☒ X-Mass Scan

Other

☒ SYN Nonack Sport

☒ Null Scan

Fragment

ICMP Fragment

IPv6 Min Fragment

Cancel

OK

Anti Attack

Dynamic ARP Inspection (DAI)

Dynamic ARP Inspection (DAI) helps protect a Layer 2 network from forged ARP messages. For ARP traffic on VLANs where DAI is enabled, the switch compares the packet's IP address, MAC address, receiving interface, and VLAN information with the binding table. Packets that pass the configured checks are forwarded; packets that fail are discarded and counted in DAI Statistics.

DAI Settings

Navigate to **Security -> DAI**. On the **DAI** tab, enable the feature and enter the VLANs that require inspection. The example below demonstrates individual VLAN 100 and VLAN range 200-202 and shows the current per-port inspection status.

DAI

Statistics

DAI

☒

VLAN

100, 200-202

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

Cancel

OK

Port

Edit

☐	Port	Trust Port	Source MAC Address Verification	Destination MAC Address Verification	IP Address Verification	Speed (pps)	Operation
☐	1/0/1	Disabled	Disabled	Disabled	Disabled	0	
☐	1/0/2	Disabled	Disabled	Disabled	Disabled	0	
☐	1/0/3	Disabled	Disabled	Disabled	Disabled	0	
☐	1/0/4	Disabled	Disabled	Disabled	Disabled	0	
☐	1/0/5	Disabled	Disabled	Disabled	Disabled	0	

DAI VLAN Scope and Port Overview

DAI Port Settings

Select one or more interfaces and click **Edit**, or use the edit icon under **Operation** for a single interface. Configure trust mode, the required MAC and IP checks, and an optional inspection rate. Enabling **IP Address Verification** also displays the **All-Zero Address** policy. The example below shows all three verification checks enabled, all-zero addresses forbidden, and a 10 pps rate with the Drop action.

DAI > Edit

Port

1/0/1

Trust Port

☐

Source MAC Address Verification

☒

Destination MAC Address Verification

☒

IP Address Verification

☒

All-Zero Address

☒ Forbid
 ☐ Allow

Rate (pps)

10

Range: 0-50, 0 indicates no rate limit

Action

☒ Drop
 ☐ ErrDisable

When the rate is set to "0", the action does not take effect

Cancel

OK

DAI Port Inspection Settings

Setting	Description
Trust Port	Enables or disables DAI trust mode on the selected interface.
Source MAC Address Verification	Checks that the Ethernet source MAC address matches the sender MAC address carried in the ARP message.
Destination MAC Address Verification	Checks that the Ethernet destination MAC address matches the destination MAC address carried in the ARP message.
IP Address Verification	Checks ARP packets for invalid IP addresses. Enabling this option also displays the All-Zero Address setting.

All-Zero Address	Select Forbid or Allow to control whether an all-zero IP address is accepted.
Rate (pps)	Sets the per-port inspection rate from 0 to 50 packets per second. A value of 0 disables rate limiting.
Action	When the rate is nonzero, select Drop to discard packets above the limit or ErrDisable to place the interface in an error-disabled state. The action does not take effect when the rate is 0.

DAI Statistics

The **Statistics** tab reports forwarded packets, each verification-failure category, IP-to-MAC binding failures, and packets dropped by the configured rate limit for every physical or LAG interface. Click **Refresh** to retrieve the current counters. Select one or more interfaces and click **Clear**, or use the per-row operation, to reset the applicable counters.

DAI		<u>Statistics</u>				
		Clear Refresh				
☐	Port	Forwarding Packets	Source MAC Address Verification Failures	Destination MAC Address Verification Failures	Source IP Address	Operation
☐	1/0/1	0	0	0	0	
☐	1/0/2	0	0	0	0	
☐	1/0/3	0	0	0	0	
☐	1/0/4	0	0	0	0	
☐	1/0/5	0	0	0	0	

DAI Statistics

RADIUS

RADIUS centralizes authentication, authorization, and accounting. A named server group can contain multiple authentication servers and multiple accounting servers, allowing the group to be reused by AAA or Identity Authentication Management.

Under **Security -> RADIUS**, click **Add** and name the group. Add the required entries on the **Authentication Server** and **Accounting Server** tabs. Use **Add** within either tab for additional servers, then select the group in the service that will use it.

RADIUS > Add

Name

Office-AAA

1-64 characters allowed, including digits letters and special characters except "\?"

Authentication Server

Accounting Server

Authentication Server1

RADIUS Authentication Server

192.0.2.10

Port

1812

The port range is 1-65535

Priority

10

Valid range is 0-65535

Shared Key

1-64 characters allowed, including digits letters and special characters except "\?"

Maximum Transmission Count

3

Valid range is 1-5

Timeout (s)

5

Valid range is 1-120

RADIUS Server Group Authentication Server

Field	Description
Name	Identifies the server group. Use a descriptive name so it can be recognized when selected in AAA or Identity Authentication Management.
RADIUS Authentication Server / RADIUS Accounting Server	Specifies the server address for the selected tab. Configure authentication and accounting destinations separately.
Port	Sets the destination UDP port. The initial values are 1812 for authentication and 1813 for accounting.
Priority	Sets the server's configured priority within its group. Use the intended priority consistently across the servers.
Shared Key	Enter the secret configured for this switch on the RADIUS server. The values must match; keep the secret confidential.
Maximum Transmission Count	Sets the transmission limit for a request. Range: 1-5; initial value: 3.
Timeout (s)	Sets the wait for a server response. Range: 1-120 seconds; initial value: 5.

TACACS+

TACACS+ centralizes management authentication, authorization, and accounting. Configure named server groups under **Security -> TACACS+**, then reference the required groups in AAA methods.

Click **Add**, name the group, and enter its server settings. Use **Add** inside the group to define additional servers before confirming the group.

★Name	Office-Admin	1-64 characters allowed, including digits letters and special characters except "\"?
Server1		
★TACACS+ Server Address	192.0.2.20	
★Port	49	The port range is 1-65535
★Priority	10	Valid range is 0-65535
★Shared Key		1-64 characters allowed, including digits letters and special characters except "\"?
★Timeout (s)	5	Valid range is 1-30

[Add](#)

TACACS+ Server Group

Field	Description
Name	Identifies the server group when selecting it in AAA.
TACACS+ Server Address	Specifies the server that processes the TACACS+ requests.
Port	Sets the destination TCP port. The initial value is 49.
Priority	Sets the server's configured priority within the group.
Shared Key	Enter the secret configured for this switch on the TACACS+ server. Keep the secret confidential.
Timeout (s)	Sets the wait for a server response. Range: 1-30 seconds; initial value: 5.

For command syntax and CLI-only credential formats, refer to the GWN78xx CLI User Guide.

AAA

Authentication, Authorization, and Accounting (AAA) controls who can sign in, which actions they may perform, and how their activity is recorded. Configure RADIUS or TACACS+ server groups first when using external servers, then create the corresponding AAA methods under **Security -> AAA**.

Use the **Login Authentication**, **Session Authorization**, and **Session Accounting** tabs for the respective service. Add a named method, configure its ordered Method 1 through Method 4 entries, and assign the method to the required management access type.

Warning: An unreachable server or an incorrect authorization method can prevent management access. Verify the server settings and preserve a working recovery access method before applying AAA changes. The UI specifically warns that methods other than Local and None may make the device inaccessible.

AAA

Login Authentication

Session Authorization

Session Accounting

Console

default

Telnet

default

SSH

default

HTTPS

default

Cancel

OK

Method

Add

Delete

☐	Name	Method 1	Method 2	Method 3	Method 4	Operation
--------------------------	------	----------	----------	----------	----------	-----------

AAA Session Authorization

Field	Description
Name	Identifies the method list used for a management access type.
Method 1-4	Defines the ordered methods. Choose the supported local option or a configured RADIUS/TACACS+ group. Empty leaves a subsequent position unused. None means the corresponding check or accounting service is not performed; it is not equivalent to local authentication.
Console / Telnet / SSH / HTTPS	Assigns the method for each access type. HTTPS appears for login authentication and session authorization, not session accounting.
Accounting Mode	For session accounting, select Start&End, End Only, or None according to the records required by the accounting server.
Real-time Accounting Interval (s)	Controls periodic session-accounting updates. A value of 0 disables periodic updates; it does not select the session start/end accounting mode.

Access type	Login authentication	Session authorization	Command authorization	Session accounting	Command accounting
Console / Telnet / SSH	Yes	Yes	Yes	Yes	Yes
HTTPS	Yes	Yes	No	No	No

Command authorization and command accounting apply to command-line management sessions. Refer to the GWN78xx CLI User Guide for the general command reference. Command authorization and accounting configuration should follow the commands supported by the installed firmware.

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", and click on the "OK" button to save.

On this page, 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

Port

Authentication Sessions

Local User of MAC-based

802.1X Authentication

☒

MAC Authentication

☒

User ID format of MAC-based

XXXXXXXXXXXX

Guest VLAN

☒

*Guest VLAN ID

7

Cancel

OK

Port

Edit

☐	Port	User Authentication Mode	Authentication Method / Method	Guest VLAN	Authorized VLAN	Operation
☐	1/0/1	Port-Based	802.1X / Radius	Disabled	Static	
☐	1/0/2	MAC-Based	MAC Authentication / Local	Disabled	Static	
☐	1/0/3	Single User	802.1X / Radius	Enabled	Static	
☐	1/0/4	MAC-Based	--	Disabled	Static	

Identity Authentication Management Port Mode

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

Note: a RADIUS server must first be added under [Security -> RADIUS](#).

Port	1/0/1
User Authentication Mode ⓘ	MAC-Based
Guest VLAN	
Authorized VLAN ⓘ	

Authentication Method1

Authentication Method ⓘ	MAC Authentication
Method ⓘ	Local
	Radius
	Add 

Authentication Method2

Authentication Method ⓘ	802.1X
Method ⓘ	Radius

Add 

Cancel

OK

Port Mode Edit port

Port	The specific port being configured. This field shows the port number (e.g.
User Authentication Mode	The mode of user authentication to be used on this port. Options include: MAC-Based
Guest VLAN	Enables or disables the Guest VLAN for this port. If enabled
Authorized VLAN	Specifies the VLAN ID that authenticated users will be assigned to. This ensures that authorized devices are placed in the correct network segment.
Authentication Methods(x)Note: click on "Add+" to add another method.	
Authentication Method1	Select the authentication method, two options:802.1X: it will use 802.1x authentication, RADIUS must be first added.MAC Authentication: it will use local MAC Addresses under Security -> Identity Authentication Management page -> Local User of MAC-based or RADIUS depending on the seleted method.
Method	* If MAC Authentication is selected, the user can add two methods: Radius and Local.* If 802.1x is selected, the user can only select radius.Note: When Radius is selected, the switch includes the Calling-Station-Id attribute in the Access-Request message, containing the MAC address of the connected device. This allows RADIUS servers to apply identity-based policies and track client devices using their hardware address.

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 the **"Edit"** button or icon to configure the port(s) as shown below:

Identity Authentication Management

Port Mode **Port** Authentication Sessions Local User of MAC-based

Edit								
☐	Port	Port Control	Reauthentication	Max User Count	Reauthentication Timer	Inactive Timer	Quiet Timer	Operation
☐	1/0/1	Force authentication	Enabled	256	3600	60	60	
☐	1/0/2	Auto	Enabled	256	3600	60	60	
☐	1/0/3	Force unauthentication	Enabled	256	3600	60	60	
☐	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	Disable
*Max User Count	Force authentication
	Force unauthentication
	Auto
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
Cancel OK	

Identity Authentication Management port edit port

Example of 802.1X configuration on GXV3480 IP Video phone.

802.1X Mode

<

802.1X Mode

>

802.1X Mode

EAP-MD5

>

802.1X Identity

hope

802.1X Secret

....

8021X 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

Q Session ID/Port/M.

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
0000000911847958	1/0/6	C0:74:AD:03:CA:80	Authorized

Authentication Sessions Status Authorized

0000000911847958	1/0/6	C0:74:AD:03:CA:80	Locked
------------------	-------	-------------------	--------

Authentication Sessions Status Locked

0000000911847958	1/0/6	C0:74:AD:03:CA:80	Guest
------------------	-------	-------------------	-------

Authentication Sessions Status Guest

Local User of a MAC-based

Local User of MAC-based manages devices by MAC address for local MAC authentication. Click **Add** to enter a unicast MAC address, an optional **Name**, the required port-control mode, VLAN, reauthentication time, and inactive time. Click **Import** to add entries in bulk.

Identity Authentication Management

Port Mode

Port

Authentication Sessions

Local User of MAC-based



No Data

Add

Import

Local User of MAC Based Authentication

X

Add Local User of MAC-based

! The MAC address of local user must be a unicast one.

***MAC Address**

:

:

:

:

:

Name

0-32 characters allowed, including digits, letters and special characters except "\?/";

Port Control

☒ Force authentication
☐ Force unauthentication

VLAN ?

Valid range is 1-4094

Cancel

OK

Add a Local MAC User

MAC Address	Enter the local user's unicast MAC address.
Name	Enter an optional descriptive name of up to 32 characters.
Port Control	Force authentication permits the specified device; Force unauthentication prevents it from authenticating.
VLAN	Enter a VLAN ID from 1 to 4094.
Reauthentication Time (s)	Enter a value from 300 to 2,147,483,647 seconds.
Inactive Time (s)	Enter a value from 60 to 65,535 seconds.

DHCP Snooping

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

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

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

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

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

To enable the DHCP Snooping feature on GWN780x Pro switches, navigate to Security -> DHCP Snooping, then enable DHCP Snooping. To enable DHCP snooping on a VLAN, specify the VLANs or a VLAN range,

for example, 5-8 means VLANs from 5 to 8, and click the "OK" button to save. Please refer to the figure below:

DHCP Snooping

DHCP Snooping

Option 82

Port Settings

Statistics

DHCP Snooping

Entries Fixed for DHCP Snooping

Fixed Duration (s)

VLAN

300

1-2

Valid range is 15-86400

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

Cancel

OK

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 **Private**:

- **Normal Format:** is generally used when interoperability between different vendors' equipment is required. For GWN780x Pro switches, by default, the MAC Address of the switch will be used, but any other characters in the range of 1-63 can be used.
- **Private Format:** is specific to the vendor's ecosystem and may not be compatible with other vendors' equipment (check the vendor-specific format).

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

DHCP Snooping

DHCP Snooping

Option 82

Port Settings

Statistics

Format

Remote ID

Normal

Private

c0:74:ad:ba:24:fc

1-63 characters

Cancel

OK

Option 82

Add

Delete

Port

VLAN

Circuit ID

Remote ID

No Data

DHCP Snooping Option 82

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

✕

Add Option 82

Port

1/0/1

VLAN

VLAN1

Format

☒ Normal
 ☐ Private

*Circuit ID

1~63 characters

SwicthPort1

Remote ID

0~63 characters

Main Router

Cancel

OK

DHCP Snooping Option 82 Add Circuit

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

DHCP Snooping Port Settings

On this page, the 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, GWN780x Pro will protect users from rogue DHCP servers that are plugged into untrusted ports.

To configure a port(s), either select the port(s) and click on the "Edit" button or click on the "Edit icon" under the 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
☒	1/0/1	Enabled	Disabled	0	Enabled	Keep	
☐	1/0/2	Disabled	Disabled	0	Disabled	Drop	
☐	1/0/3	Disabled	Disabled	0	Disabled	Drop	
☐	1/0/4	Disabled	Disabled	0	Disabled	Drop	
☐	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

Cancel

OK

DHCP Snooping Port Settings Edit

DHCP Snooping Statistics

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

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

DHCP Snooping

DHCP SnoopingOption 82Port SettingsStatistics

Clear

Refresh

☒	Port	Forwarding Packets	Chaddr Verification Drops	Untrusted Port Drops	Untrusted Ports with Option 82 Drops	Operation
☐	1/0/21	0	0	0	0	
☐	1/0/22	0	0	0	0	
☐	1/0/23	0	0	0	0	
☒	1/0/24	31	0	31	0	
☐	1/0/25	0	0	0	0	
☐	1/0/26	0	0	0	0	
☐	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 the DHCPv6 Snooping feature on GWN780x Pro 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, which means VLANs from 5 to 8, and click the "OK" button to save. Please refer to the figure below:

DHCPv6 Snooping

[DHCPv6 Snooping](#) [Option Settings](#) [Port Settings](#) [Statistics](#)

DHCPv6 Snooping ☒

VLAN

Cancel

OK

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

DHCPv6 Snooping

DHCPv6 Snooping Option 18

On this page, the user can configure the Remote ID (Option 37). By default, GWN780x Pro switches use the GWN780x Pro 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 option 18 for a port, click on the **"Add"** button as shown below:

DHCPv6 Snooping

[DHCPv6 Snooping](#) [Option Settings](#) [Port Settings](#) [Statistics](#)

Option 37

Remote ID

Cancel

OK

1-63 characters

Option 18

Add

Delete

☒	Port	Interface ID	Operation
☒	1/0/1	VLAN1	

Total 1

< 1 >

 10 / page

DHCPv6 Snooping Option Settings

Then, select the port, Format (Standard, Extended). When the Standard format is selected, 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.

Add Option 18



Port

1/0/1

Format

Standard

*Interface ID

VLAN1

Cancel

OK

DHCPv6 Snooping Add option 18

DHCPv6 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, GWN780x Pro will protect users from rogue DHCP servers that are plugged into untrusted ports.

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

DHCPv6 Snooping

DHCPv6 Snooping

Option Settings

Port Settings

Statistics

Edit

Port	Trust Mode	Speed	Option 18	Option 37	Operation
☒ 1/0/1	Enabled	300	Drop	Keep	
☐ 1/0/2	Disabled	0	Disabled	Disabled	
☐ 1/0/3	Disabled	0	Disabled	Disabled	
☐ 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 = packets per second) 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	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
Cancel OK	

DHCPv6 Snooping Port Settings Edit

DHCPv6 Snooping Statistics

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

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

DHCPv6 Snooping

DHCPv6 Snooping Option Settings Port Settings Statistics

Clear Refresh						
Port	Forwarding Packets	Untrusted Port Drops	Untrusted Ports with Option 37 Drops	Untrusted Ports with Option 18 Drops	Invalid Drop	Operation
1/0/1	0	0	0	0	0	
1/0/2	0	0	0	0	0	
1/0/3	0	0	0	0	0	
1/0/4	0	0	0	0	0	

DHCPv6 Snooping Statistics

ND Snooping

ND Snooping validates IPv6 Neighbor Discovery traffic and builds legitimate IPv6 address-to-port bindings. These bindings can be used by IPv6 Source Guard and related inspection functions to reduce address spoofing and gateway impersonation. Navigate to **Security -> ND Snooping**.

ND Snooping Global Settings

Enable ND Snooping, select the **Global Unicast Address** and/or **Link-Local Address** type, and specify the VLANs to inspect. Scheduled Detection adds configurable detection-count and detection-interval controls; the waiting interval and lifetime are configured independently.

ND Snooping

ND Snooping

Port Settings

Prefix Management Table

Statistics

ND Snooping

Address Type

☐ Global Unicast Address
☐ Link-Local Address

VLAN

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

Scheduled Detection

Waiting Interval (ms)

250

Valid range is 1-5000

Lifetime (ms)

500

Valid range is 1-10000

Cancel

OK

© 2026 Grandstream Networks, Inc.

Grandstream Software License Agreement

ND Snooping Global Settings

Setting	Description
ND Snooping	Enables or disables ND Snooping globally.
Address Type	Select Global Unicast Address, Link-Local Address, or both address types for inspection.
VLAN	Specifies the VLANs on which ND Snooping operates. Valid VLAN IDs are 1-4094; separate individual IDs with commas and enter ranges with a hyphen.
Scheduled Detection	Enables active detection. When enabled, the page also displays Detection Count and Detection Interval.
Detection Count	Sets the number of detection attempts from 1 to 10. This field appears only when Scheduled Detection is enabled.
Detection Interval (ms)	Sets the interval between scheduled detection attempts from 1 to 10000 milliseconds. This field appears only when Scheduled Detection is enabled.
Waiting Interval (ms)	Sets the ND Snooping waiting interval from 1 to 5000 milliseconds.
Lifetime (ms)	Sets the ND Snooping lifetime from 1 to 10000 milliseconds.

ND Snooping Port Settings

To configure a physical or LAG interface, select the port and click **Edit**, or use its edit icon under **Operation**. Enable **Trust Mode** only on controlled upstream links that legitimately carry trusted Neighbor Discovery traffic. When validation is required, enable **Validation Check** and select the applicable **NA** (Neighbor Advertisement), **NS** (Neighbor Solicitation), and/or **RS** (Router Solicitation) packet types.

ND Snooping

ND Snooping

Port Settings

Prefix Management Table

Statistics

Edit

☐	Port	Trust Mode	Validation Check	Operation
☐	1/0/1	Disabled	Disabled	
☐	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	

Total 86

<123...9>

10 / page

Go to

© 2026 Grandstream Networks, Inc.

Grandstream Software License Agreement

ND Snooping Port Settings

Prefix Management

Click **Add** to create a static prefix entry, then enter its IPv6 address, prefix length from 1 to 128, and VLAN ID from 1 to 4094. Learned entries appear as **Dynamic**; select a dynamic entry and click **Solidify** to convert it to **Static**. Static entries can be edited, while dynamic entries must be solidified first.

ND Snooping

ND Snooping

Port Settings

Prefix Management Table

Statistics

Refresh

Add

Solidify

Delete

☐	IPv6 Address/Prefix Length	VLAN	Type	Lease Time (s)	Operation
No Data					

© 2026 Grandstream Networks, Inc.

Grandstream Software License Agreement

ND Snooping Prefix Management

ND Snooping Statistics

Statistics show each port's total received Neighbor Discovery packets; received **NS**, **NA**, **RS**, **RA**, and other packets; transmitted NS packets; and discarded packets. Click **Refresh** to update the counters, or select the required ports and click **Clear** to reset their statistics.

ND Snooping

ND Snooping

Port Settings

Prefix Management Table

Statistics

Clear

Refresh

☐	Port	Total Rx Packets	NS Packets	NA Packets	RS Packets	RA Packets	Other Packets	Operation
☐	1/0/1	0	0	0	0	0	0	
☐	1/0/2	0	0	0	0	0	0	
☐	1/0/3	0	0	0	0	0	0	
☐	1/0/4	0	0	0	0	0	0	
☐	1/0/5	0	0	0	0	0	0	
☐	1/0/6	0	0	0	0	0	0	
☐	1/0/7	0	0	0	0	0	0	
☐	1/0/8	0	0	0	0	0	0	
☐	1/0/9	0	0	0	0	0	0	

Total 86

<

1

2

3

...

9

>

10 / page

Go to

© 2026 Grandstream Networks, Inc.

Grandstream Software License Agreement

ND Snooping Statistics

MAINTENANCE

Upgrade

GWN780x Pro Switches support manual upload firmware upgrade via a BIN file that can be downloaded from the Grandstream Firmware page: <https://www.grandstream.com/support/firmware>.

Upgrading via network is also possible using 5 of these protocols:

- TFTP
- HTTP
- HTTPS
- FTP
- Explicit FTPS

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

Upgrade

Current version: 1.0.5.29

Upgrade via Manual Upload

Upload Firmware File to Update

Select file to upload



Supported file formats: bin

Upgrade via Network

Allow DHCP Option 43/160/66 to Override Server

On

Firmware Upgrade Protocol

HTTP

TFTP

HTTP

HTTPS

FTP

Explicit FTPS

Firmware Server Path

FTP/Explicit FTPS/HTTP/HTTPS Username

FTP/Explicit FTPS/HTTP/HTTPS Password

Check/Download New Firmware at Bootup



Scheduled Upgrade



Once enabled, the switch will automatically detect and upgrade within the scheduled time

Cancel

OK

Check for Updates

Upgrade

Diagnostics

Diagnostics includes Logs, Ping, Ping Watchdog, Traceroute, Mirroring, Fiber Module, Copper Test, One-click Debugging, Capture, Remote Support, and management-platform connection diagnostics.

Logs

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

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

Recent Downloads



ram.log

2,987 B • Done

Total 37



1

2

3

4



10 / page

Go to

Diagnostics Logs

Adding a Log Server Address to the logs to be sent to is also supported on the GWN780x Pro Switches.

Diagnostics > Log Server Address

Add

Log Server Address	Port	Minimum Log Level	Operation
192.168.80.11	514	Notice	 

Edit Log Server Address

Log Server Address

192.168.80.11

Port

The range is 1-65535.

514

Minimum Log Level

Notice

Cancel

Save

Log Server Address

Users can configure the following elements in the logs settings:

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

Diagnostics

Logs

Ping

Ping Watchdog

Traceroute

Mirroring

Fiber Module

Copper Test

One-click Debugging

Management Platform Connection Diagnostics

Log Server Address

Refresh

Clear All

Export

Settings

Start date

→

End date

All logs

Q Details

Details	Level	Generated Time
AAA-S-CONNECT: New https connection for user admin, source 192.168.70.230 ACCEPTED	Notice	Sep 05 2024 21:48:35
SYSTEM-S-CPU_INFO: utilization:27 user:86479 nice:1811 system:539532 idle:1536953 irq:0 softirq:0 guest:2043	Notice	Sep 05 2024 21:37:10
SYSTEM-S-MEM_INFO: utilization:63 total:125564 avail:45852 Unevictable:0 used:113676 free:11888 buffer:6080 cached:38388 shared:0 AnonPages:15928 Slab:6236 VmUsed:48544 calcu:128420	Notice	Sep 05 2024 21:37:10
SYSTEM-S-CPU_INFO: utilization:26 user:74338 nice:1505 system:452741 idle:1276491 irq:0 softirq:0 guest:1745	Notice	Sep 05 2024 20:37:10
SYSTEM-S-MEM_INFO: utilization:63 total:125564 avail:45668 Unevictable:0 used:113812 free:11752 buffer:6080 cached:38340 shared:0 AnonPages:15928 Slab:6284 VmUsed:48544 calcu:128292	Notice	Sep 05 2024 20:37:10
AAA-S-CONNECT: New https connection for user admin, source 192.168.70.230 ACCEPTED	Notice	Sep 05 2024 20:22:02
SYSTEM-S-CPU_INFO: utilization:30 user:59012 nice:1196 system:362847 idle:1022490 irq:0 softirq:0 guest:1279	Notice	Sep 05 2024 19:37:10
SYSTEM-S-MEM_INFO: utilization:64 total:125564 avail:44464 Unevictable:0 used:114820 free:10744 buffer:6000 cached:38228 shared:0 AnonPages:16700 Slab:6240 VmUsed:48544 calcu:127980	Notice	Sep 05 2024 19:37:10
AAA-S-CONNECT: New https connection for user admin, source 192.168.70.230 ACCEPTED	Notice	Sep 05 2024 19:34:26
SYSTEM-S-CPU_INFO: utilization:26 user:46228 nice:947 system:275672 idle:763079 irq:0 softirq:0 guest:905	Notice	Sep 05 2024 18:37:10

Total 299

<

1

2

3

...

30

>

10 / page

Go to

Log Diagnostics

Settings



Minimum Log Level

Debug



Log Aggregation



*Timeout (s)

Valid range is 15-3600

60

Cancel

OK

Log Diagnostics

Ping

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

*IP Address/Hostname

192.168.80.116

*Packet Count

4

Valid range is 1-65535

*Packet Size

56

Valid range is 0-65500

VLAN Interface

None



Start

Results

```
PING 192.168.80.116 (192.168.80.116): 56 data bytes
64 bytes from 192.168.80.116: seq=0 ttl=64 time=0.000 ms
64 bytes from 192.168.80.116: seq=1 ttl=64 time=0.000 ms
64 bytes from 192.168.80.116: seq=2 ttl=64 time=0.000 ms
64 bytes from 192.168.80.116: seq=3 ttl=64 time=0.000 ms

--- 192.168.80.116 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 0.000/0.000/0.000 ms
```

Ping

Ping Watchdog

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

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

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

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

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

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

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

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

Ping Watchdog > **Edit Port**

PoE port needs to consider the PD device boot time to ensure that the device has been booted and can work normally. Namely: enable delay time + send packet interval * retries ≥ PD boot time

Port

1/0/2

Enable

☒

• IP Address

192.168.70.25

IPv4 format

• Packet Sending Interval (s)

30

Valid range is 30-3600

• Delay Time (s)

60

Valid range is 60-3600

• Retry Times

2

Valid range is 1-10

• Shutdown Interval (s)

5

Valid range is 5-30

Cancel

OK

Ping watchdog

Traceroute

Another tool is Traceroute, which shows the number of hops, and GWN780x Pro Switches enable the user to run Traceroute commands right from the Switches' WEB UI.

*IP Address/Hostname

192.168.80.116

Start

Results

```
tracert to 192.168.80.116 (192.168.80.116), 30 hops max, 38 byte packets
 1  192.168.80.116 (192.168.80.116)  10.000 ms  0.000 ms  0.000 ms
```

Traceroute

Mirroring

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

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

The GWN780x Pro switches support two modes of Port Mirroring: SPAN and RSPAN:

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

SPAN

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

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

Group
1

Mode
SPAN

Ingress Mirroring
Click on port to select/unselect

Port

2 4 6 8 10 12 14 16 18 20 22 24

1 3 5 7 9 11 13 15 17 19 21 23 25 SFP1 26 SFP2 27 SFP3 28 SFP4

LAG

2 4 6 8

1 3 5 7

Egress Mirroring
Click on port to select/unselect

Port

2 4 6 8 10 12 14 16 18 20 22 24

Port Mirroring

RSPAN

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

Source Switch Role (RSPAN)

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

Group

1

Mode

RSPAN

Role

Source Switch

Ingress Mirroring

Click on port to select/unselect

Port

2

4

6

8

10

12

14

16

18

20

22

24

1

3

5

7

9

11

13

15

17

19

21

23

25 SFP1

26 SFP2

27 SFP3

28 SFP4

LAG

2

4

6

8

1

3

5

7

Egress Mirroring

Click on port to select/unselect

Port

2

4

6

8

10

12

14

16

18

20

22

24

1

3

5

7

9

11

13

15

17

19

21

23

25 SFP1

26 SFP2

27 SFP3

28 SFP4

Source Switch Role

Destination Switch Role (RSPAN)

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

Group

1

Mode

RSPAN

Role

Destination Switch

Source Port

Click on port to select/unselect

Port

2

4

6

8

10

12

14

16

18

20

22

24

1

3

5

7

9

11

13

15

17

19

21

23

25 SFP1

26 SFP2

27 SFP3

28 SFP4

LAG

2

4

6

8

1

3

5

7

Monitor Port

1/0/2

Tx/Rx Regular Data Messages

☒

Remote VLAN

Please select

Cancel

OK

Destination Switch Role RSPAN

Fiber Module

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

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

Fiber

1/0/25

Fiber Info



Port Name:1/0/25
OE present: Remove
Loss of signal: Loss
Transceiver Type:
Connector Type :
Ethernet Compliance Code: 0B/0B
Transmission Media:
Wavelength: 0
Bitrate: 0
Vendor OUI: 0:0:0
Vendor Name:
Vendor PN:
Vendor Revision:
Vendor SN:
Temperature: 0.0°C
Voltage: 0.00V
Current: 0.00mA
TX Power: 0.00dBm
RX Power: 0.00dBm

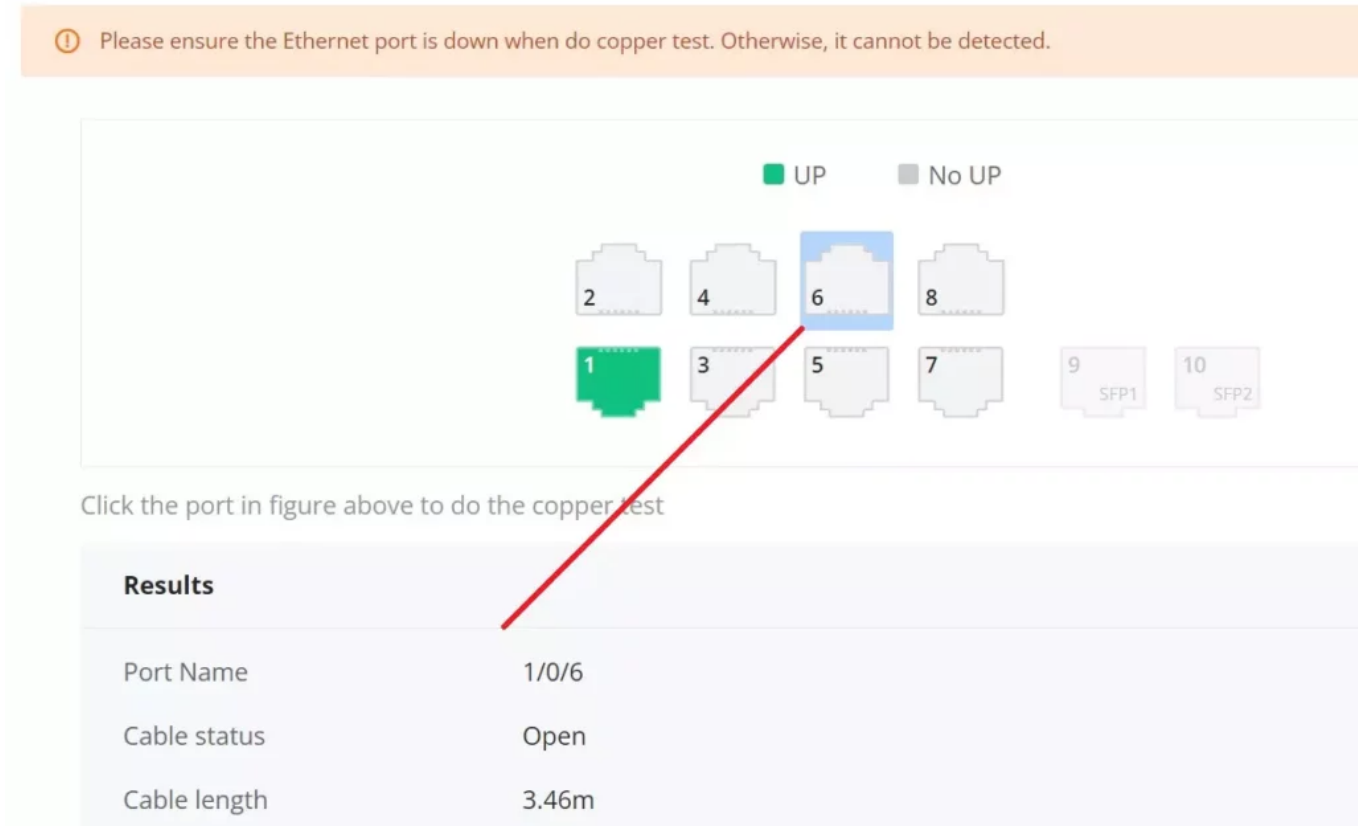
Fiber Module

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.**

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



Copper Test

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

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

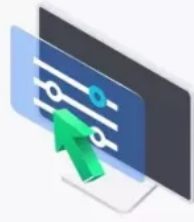
Cable Length:

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

One-click Debugging

On GWN780x Pro switches, the 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 a few minutes.

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



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 log files and even a tech-support file that contains valuable information like the switch configuration, etc.

oneclick debugging

- tmp
- var
- boot.log
- boot_last.log
- dev.log
- dhcpcd-intfv0.log
- flash.log
- other.log
- ram.log
- router_cmd.log
- snmpd.log
- tech-support**
- zebra.log

Type: File
Size: 1.58 MB
Date modified. 10:11 AM

One click Debugging Folder

Capture

Capture records packets that match the selected criteria. Choose **Local PC** or a **TFTP server** as the destination, set the capture duration, select the PCAP or TAR output, and optionally filter by VLAN, source or destination MAC address, and the selected switch port.

Diagnostics

LogsPingPing WatchdogTracerouteMirroringsFlowFiber ModuleCopper TestOne-click DebuggingCaptureRemote SupportManagem...

Basic Settings

Storage Location ⓘ

Local PC

TFTP Server

Capture Duration (Min)

30

Format

pcap

tar

If capturing packets for an extended period, it is recommended to choose the tar format for segmented packet capture file generation.

Packet Matching

VLAN

Valid range is 1-4094

Source MAC Address

:

:

:

:

Destination MAC Address

:

:

:

:

Port

Packet Capture

Remote Support

Remote Support temporarily authorizes Grandstream to access diagnostic data, logs, and configuration information for troubleshooting. Open **Maintenance -> Diagnostics -> Remote Support**, enter the administrator password, and use **Remote Support** only when working with an authorized support engineer.

Diagnostics

LogsPingPing WatchdogTracerouteMirroringFiber ModuleCopper TestOne-click DebuggingRemote SupportManagement Platform Conn...

① Once enabled, you will authorize Grandstream to temporarily access device diagnostic data, logs, and configuration information. This service is used only for troubleshooting and device maintenance, and no personal privacy information will be collected. All remote access sessions are fully encrypted, and this feature will be automatically disabled 48 hours after enablement.

*Password

Enter admin password to access

Remote Support

Remote Support Before Activation

Diagnostics

Logs Ping Ping Watchdog Traceroute Mirroring Fiber Module Copper Test One-click Debugging **Remote Support** Management Platform Connection Diagnostics

Once enabled, you will authorize Grandstream to temporarily access device diagnostic data, logs, and configuration information. This service is used only for troubleshooting and device maintenance, and no personal privacy information will be collected. All remote access sessions are fully encrypted, and this feature will be automatically disabled 48 hours after enablement.



Remote support is in process...

Disable Remote Support

Remote Support Active Session

Security: Remote sessions are encrypted. The feature automatically disables 48 hours after enablement. Enable it only for a support session that you have authorized.

Management Platform Connection Diagnostics

This page shows the current connection state for the selected configured management platform.

Navigate to **Maintenance -> Diagnostics -> Management Platform Connection Diagnostics**. Select the available **Management Platform**, check its **Connected Status**, and click **View Log** to inspect the connection log.

Diagnostics

chdog Traceroute Mirroring sFlow Fiber Module Copper Test One-click Debugging Capture Remote Support **Management Platform Connection Diagnostics**

Management Platform

GDMS Networking

Connected Status

• Connected

View Log

Management Platform Connection Diagnostics

sFlow

sFlow samples traffic and exports flow and counter records to a collector for real-time visibility and performance analysis.

sFlow Global Settings

Use Global Settings to connect the switch to an sFlow collector. The switch acts as the sFlow agent: it identifies itself with an agent address and exports sampled traffic and counter data to the collector, where monitoring software stores and analyzes the information. Configure which ports provide samples separately under Interface Settings.

Diagnostics
Logs
Ping
Ping Watchdog
Traceroute
Mirroring
sFlow
Fiber Module
Copper Test
One-click Debugging
Capture
Remote Support
...

Global
Interface Settings

Agent
IPv4/IPv6 Format

Collector Settings

IP Address
IPv4/IPv6 Format

Maximum Packet Size (Bytes)
Valid range is 200-8192

UDP Port
Valid range is 1024-65535

Description
0-64 characters allowed, including digits, letters and special characters except '\?/';

Cancel
OK

sFlow Global Settings

Setting	Description
Agent	Enter a stable IPv4 or IPv6 address that identifies this switch in sFlow datagrams. Normally, use an address assigned to the switch that the monitoring system can associate with this device.
Collector IP Address	Enter the IPv4 or IPv6 address of the server or monitoring platform running the sFlow collector. The switch sends its exported samples and counters to this destination.
Maximum Packet Size (Bytes)	Sets the maximum size of each exported sFlow datagram. The displayed default is 1400 bytes; the permitted range is 200-8192 bytes.
UDP Port	Enter the UDP port on which the collector listens for sFlow datagrams. It must match the collector configuration. The standard and displayed default is 6343; the permitted range is 1024-65535.
Description	Enter an optional label that helps identify the collector configuration. Up to 64 characters are supported.

Interface Settings

Use Interface Settings to choose which ports contribute monitoring data. Flow Sampling exports samples of packet headers from ingress traffic, egress traffic, or both directions. Counter Sampling periodically exports interface counters. Enable either sampling method independently according to the information required by the collector.

Diagnostics

Ping

Ping Watchdog

Traceroute

Mirroring

sFlow

Fiber Module

Copper Test

One-click Debugging

Capture

Remote Support

Management Pla

...

Global

Interface Settings

Edit

☐	Port	Flow Sampling				Counter Sampling		Operation
		Status	Sampling Direction	Maximum Packet Size (Bytes)	Sampling Rate	Status	Sampling Interval (s)	
☐	1/0/1	Disabled	--	--	--	Disabled	--	
☐	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	--	

Total 54

<123...6>

10 / pageGo to

© 2026 Grandstream Networks, Inc. Grandstream Software License Agreement

sFlow Interface Settings

Backup and Restore

Backup & Restore supports manual backup and restore, factory reset, and automatic backup of the running configuration. Enable **Scheduled Backup** and set the **Backup Time** for recurring backups. In the backup list, enable **Restore Configuration on Reboot** for the configuration file that the switch should load during the next reboot.

Backup & Restore

Factory Reset

After factory reset, all settings on the switch will be restored to factory default. It is recommended to back up the current configuration before factory resetting.

Factory Reset

Restore Configuration

Switch configuration can be restored by importing a configuration file. If restoration fails, a hard reset to factory settings may be necessary. To hard reset, hold down the RESET button on the front of switch for five seconds and let go.

Upload Configuration File

Backups

Back Up Running Configurations

Back Up Saved Configurations

Import

Scheduled Backup (Off)

Name	Date	Size	Restore Configuration on Reboot	Operation
GWN7806PH_Pro_EC74D7A8C094_1-0-17-7_20260818191956_Upgrade.cfg	2026/08/18_19:56	2.39KB	☐	

Backup and Restore

SNMP

Simple Network Management Protocol (SNMP) lets a network management system monitor the switch, retrieve operational data, and receive event notifications. The switch is the managed device, its SNMP agent exposes management information, and the network management station (NMS) queries that information and receives traps.

Navigate to **Maintenance -> SNMP**, enable the service, and select the SNMP versions required by the NMS.

Configure the engine IDs, then define the views, access groups, communities or SNMPv3 users, notification destinations, and trap events required by the monitoring design.

SNMP

Global Settings

View Management

Group Management

Community Management

User Management

Notification Management

Trap Event

SNMP

SNMP Version

SNMPv1/SNMPv2c

SNMPv3

Local Engine ID

8000a59d

ec74d7a8c094

2-56 characters. Value must be an even number and in hexadecimal format.

Reset

Cancel

OK

Remote Engine ID

Add

Remote Engine ID	Server Address	Operation
------------------	----------------	-----------



SNMP Global Settings

Field	Description
SNMP	Enables or disables the switch's SNMP agent.
SNMP Version	Selects SNMPv1/SNMPv2c, SNMPv3, or both according to the versions supported by the NMS.
Local Engine ID	Identifies the switch's local SNMP engine. The displayed fixed prefix is followed by an editable suffix of 2-56 hexadecimal characters; the suffix must contain an even number of characters. Use Reset to restore the initial value.
Remote Engine ID	Identifies the remote SNMP engine associated with the server. Enter 10-64 hexadecimal characters with an even number of characters.
Server Address	Specifies the server associated with the remote engine ID.

SNMP Global Settings Fields

View Management

A view defines which parts of the Management Information Base (MIB) a manager can access. Click **Add**, name the view, and configure a Type and OID Subtree pair. Use **Add** within Type & OID Subtree to include multiple pairs in the same view; each pair includes or excludes the specified subtree. Assign the view to the appropriate access group or community.

View Management > Add View

View

Type & OID Subtree

Type
Included

OID Subtree

1-32 characters allowed, including digits, letters and special characters except \"?/;

Add

Cancel

OK

© 2026 Grandstream Networks, Inc. Grandstream Software License Agreement

Add an SNMP View

Group Management

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

SNMP

Global Settings

View Management

Group Management

Community Management

User Management

Notification Management

Trap Event

Add

Group	Security Mode	Security Level	Read-only view	Read-write view	Notification View	Operation
Group1	SNMPv3	AuthPri	View2	View1	all	

*Group

Group1

Security Mode

SNMPv3

Security Level

AuthPri

Read-only view

View2

The view can only be viewed, not edited

Read-write view

View1

The view can be read and written. If no view selected, the SNMP manager cannot read and write all MIB objects of the device.

Notification View

all

The management software can receive abnormal alarm information sent by the selected view. If no view selected, the SNMP dailling will not send trap information to SNMP manager.

Cancel

Save

SNMP Group Management

Community Management

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

SNMP

Global Settings View Management Group Management **Community Management** User Management Notification Management Trap Event

Add

Community	Type	View	Permission	Group	Operation
GWN7800	Advanced	--	--	Group1	 
Grandstream	Advanced	--	--	Group1	 
public					 

*Community: GWN7800

Type: ☐ Basic ☒ Advanced

*Group: Group1

Cancel Save

SNMP Community Management

SNMP User Management

SNMP User Management configures SNMPv3 identities. Select the user's group and configure authentication and privacy to match the network management system. For a group using authentication and privacy (AuthPri), choose the authentication mode and password, then select DES or AES under **Encryption Mode** and enter the encryption password. SNMPv3 must be enabled in Global Settings.

SNMP

Global Settings View Management Group Management Community Management **User Management** Notification Management Trap Event

Add

User	Group	Security Level	Authentication Mode	Encryption Mode	Operation
User1	Group1	NoAuthNoPri	None	None	 
User2	Group1	AuthPri	SHA	DES	 
User3					 

*User: User2

*Group: Group1

Security Level: AuthPri

Authentication Mode: ☐ MD5 ☒ SHA

*Authentication Password:

Encryption Mode: DES

*Encryption Password:

Cancel Save

SNMP User Management

Notification Management

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

SNMP

Global Settings View Management Group Management Community Management User Management **Notification Management** Trap Event

[Add](#)

Server Address	UDP Port	Security Mode	Notification Type	Community/User	Security Level	Timeout (s)	Maximum Retries	Operation
192.168.5.11	162	SNMPv3	Traps	User1	AuthPri	--	--	 

*Server Address 192.168.5.11

*UDP Port 162

Security Mode SNMPv3

Notification Type ☐ Traps ☒ Informs

*User User1

Security Level AuthPri

*Timeout (s) 300

*Maximum Retries 255

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

SNMP Notification Management

Trap Event

Trap Event selects the conditions reported to an SNMP manager. Enable only the events required by the monitoring system.

- **Authentication Failed:** reports an unauthorized login attempt.
- **Port Up/Down:** reports a port link-state change.
- **Cold Start/Warm Start:** reports a restart.
- **STP Bridge and CPU:** report the corresponding spanning-tree and CPU events.
- **Monitor:** reports configured monitor events.
- **Port ErrDisable:** reports a port entering an error-disabled state.
- **MAC Address Notification:** reports configured MAC-address events.
- **Port Security:** reports Port Security events.
- **PoE Power Supply:** reports PoE power events.
- **Logs:** reports configured log events.
- **VLAN Creation/Deletion:** reports VLAN configuration changes.
- **Configuration Distribution:** reports configuration-distribution events.
- **ARP Notification:** reports configured ARP events.
- **Fiber Module Alert:** reports optical-module threshold events.

SNMP

Global Settings View Management Group Management Community Management User Management Notification Management Trap Event

Authentication failed	☒
Port Up/Down	☒
Cold Start	☒
Warm Start	☒
STP Bridge	☐
CPU	☐
Monitor ⓘ	☐
Port ErrDisable	☐
MAC Address Notification	☐
Port Security	☐

SNMP Trap Events

RMON

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

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, the number of error frames of various types, the number of collisions, etc. The number of data packets, the number of broadcast and multicast packets, the number of received bytes, the number of received packets, etc.

RMON

To use RMON, please enable SNMP>Global Settings>SNMP.

Statistics History Event Alarm

Refresh

Clear

☒	Port	Received Bytes	Drop Events	Received Packets	Broadcast Packets	Multiast Packets	CRC & Align Errors	Undersize Pack	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 the "Add" button to create a History ID specifying the Port as well.

RMON

Statistics History Event Alarm

History

Add

History ID	Port	Sampling Interval	Operation
1	GE1	1800	

Edit History

History ID

1

*Port

GE1

*Maximum Samples

The range is 1-50.

50

*Sampling Interval (s)

The range is 1-3600.

1800

Owner

0-32 characters, supports numbers and letters

Admin

Cancel

Save

© Grandstream Network

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 a Trap to the network management station.

RMON

StatisticsHistoryEventAlarm

Add

Event ID	Detail	Type	Community	Owner	Event Logs	Operation
1	Admin	Log&Trap				

Event ID

1

Detail

0-32 characters, supports numbers and letters

Admin

Type

Log&Trap

Community

1-32 characters, supports numbers and letters

Grandstream

Owner

0-32 characters, supports numbers and letters

Admin

CancelSave

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

Statistics History Event **Alarm**

Refresh Add

Alarm ID	Port	Counter / Value	Sampling Type	Sampling Interval	Owner	Trigger Mode	Rising Threshol...	Falling Thresho...	Operatio
1	GE1	Drop Events/0	Absolute	100	Admin	Rising	100/1	--	 

Alarm ID: 1

*Port: GE1

Counter: Drop Events

Sampling Type: ☒ Absolute ☐ Delta

*Sampling Interval (s): 100

Owner: Admin

Trigger Mode: Rising

*Rising Threshold: 100

*Rising Event: 1

Cancel Save

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/LLDP-MED

LLDP Global SettingsLLDP MED Network PolicyLLDP MED Port SettingsDevice InfoNeighbor InfoStatistics

LLDP

TLV Advertise Interval (s)

30

Valid range is 5-32767

TTLMultiplier

4

Valid range is 2-10

Port Reinitializing Delay Time (s)

2

Valid range is 1-10

LLDPDU Transmit Delay Time (s)

2

Valid range is 1-8191

Cancel

OK

Port Settings

Edit

☒	Port	Mode	TLV	Operation
☒	1/0/1	Tx/Rx	PortDescription, SysName, SysDescription, SysCapabilities, ManagementAddrSel, PVID, MacPhySel, Lin...	
☒	1/0/2	Tx/Rx	PortDescription, SysName, SysDescription, SysCapabilities, ManagementAddrSel, PVID, MacPhySel, Lin...	
☒	1/0/3	Tx/Rx	PortDescription, SysName, SysDescription, SysCapabilities, ManagementAddrSel, PVID, MacPhySel, Lin...	

LLDP Global Settings

More configurations can be 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 the MED (Media Endpoint Discovery) network policy. Click on the "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

☒	Policy ID	Application	VLAN	VLAN Tag	CoS	DSCP	Operation
☒	1	Voice	7	Tagged	6	43	

LLDP MED Network Policy

To add a Network Policy, click on the "Add" button or click on the "Edit" icon under the 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

AddEdit Network Policy

LLDP MED Port Settings

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

LLDP/LLDP MED

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

Edit

Port	LLDP MED	Network Policy TLV	Inventory TLV	Location Identification TLV	PoE-PSE TLV	Operation
☒ GE1	Enabled	Enabled	Enabled	Disabled	Disabled	
☐ GE2						
☐ GE3						
☐ GE4						
☐ GE5						
☐ GE6						
☐ GE7						
☐ GE8						
☐ GE9						
☐ GE10						

Port

GE1

LLDP MED

Network Policy TLV

*Network Policy

Voice

1

Add Network Policy

Inventory TLV

Location Identification TLV

PoE-PSE TLV

Cancel

Save

LLDP MED Port Settings

LLDP Device Info

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

LLDP/LLDP-MED

Local Device Info

Chassis ID Subtype	MacAddr
Chassis ID	C0:74:AD: [redacted]
Device Name	GWN7813P
System Description	GWN7813P
Supported System Capabilities	Bridge, Router
Enabled System Features	Bridge, Router
Port ID Subtype	Local

Local Port Info



Click port figure above to view related LLDP and LLDP-MED details

Basic Info	
Chassis ID Subtype	MacAddr
Chassis ID	C0:74:AD: [redacted]
Device Name	GWN7813P
System Description	GWN7813P
Supported System Capabilities	Bridge, Router
Enabled System Features	Bridge, Router

LLDP Device Info

Neighbor Info

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

LLDP/LLDP-MED

RefreshDelete

Q Search

☐ Local Port	Chassis ID Subtype	Chassis ID	Neighbor ID Subtype	Neighbor Port ID	Device Name	System Description	Survival	Operation
 No Data								

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		
☒	1/0/1	862	0	0	0	0	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	

LLDP Statistics

Energy Efficient Ethernet

EEE or **Energy Efficient Ethernet** helps in reducing the power consumption on interfaces like GWN780x Pro 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 GWN780x Pro switch, it will show if it's enabled or not.

Energy Efficient Ethernet

Edit

Refresh

☒	Port	Configuration Status	Status	Operation
☒	1/0/1	Enabled	Enabled	
☐	1/0/2	Enabled	Disabled	
☐	1/0/3	Disabled	Disabled	
☐	1/0/4	Disabled	Disabled	
☐	1/0/5	Disabled	Disabled	

Energy Efficient Ethernet

To enable EEE on a port, select a port, then click on the "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

Alert

Alert settings monitor hardware and service conditions such as CPU and memory usage, PoE power, MAC-address limits, temperature, fan and PoE-chip faults, ARP-limit conditions, and fiber-module events.

Alert Settings

For each supported condition, enable or disable monitoring, select the log level, and configure the alert and recovery thresholds and their waiting times where available.

Alert

Alert SettingsFiber Module AlertStatisticsScheduled Notification

Type	Alert Status	Log Level	Alert Threshold	Alert Waiting Time (s)	Restore Threshold	Restore Waiting Time (s)
CPU Usage	☒	Error	80 %	30	80 %	10
Memory Usage	☒	Error	80 %	30	80 %	10
PoE Power	☒	Error	80 %	30	80 %	10
Mac Address Exceeds Limit	☒	Error	80 %	30	80 %	10
Temperature	☒	Error	75 °C	30	75 °C	10
Fan Malfunction	☒	Error	--	30	--	10

CancelOK

Alert Settings

Use **ARP Limit Exceeded** to monitor ARP-table usage. Configure its alert threshold and waiting time, along with the restore threshold and waiting time, to control when an alert is raised and when recovery is reported.

Fiber Module Alert

Fiber Module Alert monitors each optical port for high or low temperature, voltage, transmit power, receive power, and laser bias current. Select the port and click **Edit** to enable the required alert types and configure their reporting and recovery settings.

Alert

Alert Settings

Fiber Module Alert

Statistics

Scheduled Notification

Edit

☐	Port	High Temperature Alert	Low Temperature Alert	Overvoltage Alert	Undervoltage Alert	High Tx Power Alert	Low Tx Power Alert	Operation
☐	1/0/49	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled	
☐	1/0/50	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled	
☐	1/0/51	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled	
☐	1/0/52	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled	
☐	1/0/53	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled	
☐	1/0/54	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled	

© 2026 Grandstream Networks, Inc.

Grandstream Software License Agreement

Fiber Module Alert

Field	Description
Alert Status / Log Level	Enables each alert type and selects the severity used when reporting it.
Alert Difference / Recovery Difference	Configures the alert and recovery differences for the selected measurement. The displayed unit follows the measurement: °C, V, dBm, or mA.
Alert Waiting Time (s)	Sets how long the alert condition must persist before it is reported.
Restore Waiting Time (s)	Sets how long the recovery condition must persist before restoration is reported.

Alert Statistics

Alert Statistics shows the current status of monitored hardware and services together with the most recent alert and restore times.

Alert

Alert Settings

Statistics

Refresh

Type	Current Status	Last Alert Time	Last Alert Actual Value	Last Restore Time	Last restore Actual Value	Alert Times
CPU Usage	normal	1970-01-01 08:00:00	0%	1970-01-01 08:00:00	0%	0
Memory Usage	normal	1970-01-01 08:00:00	0%	1970-01-01 08:00:00	0%	0
PoE Power	normal	1970-01-01 08:00:00	0%	1970-01-01 08:00:00	0%	0
Mac Address Exceeds Limit	normal	1970-01-01 08:00:00	0%	1970-01-01 08:00:00	0%	0
Temperature	normal	1970-01-01 08:00:00	0°C	1970-01-01 08:00:00	0°C	0
Fan Malfunction	normal	1970-01-01 08:00:00	--	1970-01-01 08:00:00	--	0
PoE Chip Malfunction	normal	1970-01-01 08:00:00	--	1970-01-01 08:00:00	--	0

Alert Statistics

SYSTEM

Basic Settings

The basic settings page is split into three categories:

- **Basic Info:** first section, the user can specify a name for the GWN780x Pro switch with a system location and contact.
- **Time Settings:** In this section, the users can configure the time either manually or using an NTP Server. It's also possible to configure Daylight Saving (DST) Mode according to the location or recurrence.
- **Scheduled Reboot:** The users can enable scheduled reboot by adding a schedule under the [Time Policy](#).

Please navigate to the **System -> Basic Settings** page.

Basic Info

Device Name

GWN7822P

1~64 characters

System Location

Default

0~64 characters

System Contact

Default

0~64 characters

Time Settings

Date & Time

Manual

Automatic (NTP Server)

System Time

2024-10-17 23:08:30

NTP Server

pool.ntp.org

Time Zone

(UTC+08:00) Beijing,Shanghai,Chongqing,Hong Kong,Urum...

DayLight Saving (DST) Mode

Recurring

Offset (Min)

60

Valid range is 1-1440

Starting Time

July

Week 1

Sunday

00:00

Ending Time

December

Week 1

Sunday

00:00

Scheduled Reboot

Reboot Time

Disabled

Cancel

OK

Basic Settings

Basic Info	
Device Name	Specify a name for the device.
System Location	Enter system location.
System Contact	Specify the system contact.
Time Settings	
Date & Time	Select time synchronization method: Manual or Automatic (NTP Server). Manual: specify the time manually. Automatic (NTP Server): time will be synced automatically with NTP Server. Note: if the device is added to the GDMS Networking 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 GDMS Networking.

System Time	If Manual is selected, the user can specify the date and time. If Automatic (NTP Server) is selected, the current time and time will be displayed,
NTP Server	If Date & Time is set to Automatic (NTP Server), please specify the NTP Server address, by default is set to "pool.ntp.org" .
Time Zone	Select the time zone from the drop-down list.
DayLight Saving (DST) Mode	Disabled: DayLight Saving mode will be disabled. Recurring: if the Daylight saving is recurring (repetitive). Non Recurring: if selected the user can specify the offset (min) and daylight saving time start date and end date. Recurring USA: for USA region. Recurring EU: for EU region
Offset (Min)	Specify the Offset by minutes, range from 1 to 1440.
Starting Time	Specify the starting date and time.
Ending Time	Specify the ending date and time.
Scheduled Reboot	
Reboot Time	Select a reboot time from the drop-down list or click on "+" button to add a schedule. By default is disabled.

Basic Settings

Access Control

In this section, the user can configure access to GWN780x Pro switches.

Please navigate to **System -> Access Control**.

Web Service Management

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

- **Inactive Session Timeout:** sets how long an inactive Web UI session remains signed in.
- **HTTPS Port:** sets the Web UI service port. **Minimum TLS Version** and **Maximum TLS Version** define the permitted TLS range. Select compatible limits for the browsers and management clients that must connect.
- **Telnet:** enables or disables Telnet and selects its service port. Telnet is disabled by default; SSH is recommended.
- **SSH:** enables or disables SSH and selects its service port (22 by default).

Access Control

Web Service Management
Passwordless Remote Access
Management Platform Settings
Management ACL of Hardware-based
Management ACL of Software-based

Inactive Session Timeout (min)

1440

Valid range is 1-1440

HTTPS Port

443

Valid range is 443 and 1024-65535

Minimum TLS Version ⓘ

TLS 1.2

Maximum TLS Version ⓘ

TLS 1.2

Telnet

☐

SSH

☒

SSH Port

22

Valid range is 22 and 1024-65535

Cancel
OK

Passwordless Remote Access

Passwordless Remote Access allows GDMS Networking or GWN Manager to open the managed switch's Web UI without requesting a separate switch username and password. Configure the switch's management platform first, then enable **Passwordless Remote Access** under **System -> Access Control** when this workflow is required.

Security: Enable this only for a trusted management platform and restrict the platform accounts permitted to manage the switch.

Management Platform Settings

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

Access Control

Web Service Management SSH Remote Access Management Platform Settings Management ACL of Hardware-based Management ACL of Software-based

Allow DHCP Option 43 to Override Management Server ☒

Management Server Settings ☒

Management Platform ☒ GWN Manager ☐ GWN Router

• Management Server Address

• Management Server Port Valid range is 1-65535

Access Control Manager Settings

Management ACL of Hardware-based

On a GWN780x Pro switch, the hardware management Access Control List (ACL) is designed to optimize resource efficiency by filtering traffic directly at the hardware level before it reaches the CPU. This pre-processing step ensures that only traffic matching the defined security rules is forwarded for further handling, effectively reducing unnecessary CPU load and enhancing overall performance. By offloading the initial traffic validation to the switch hardware, the GWN780x Pro improves both network efficiency and security.

Access Control

Web Service Management SSH Remote Access Management Platform Settings Management ACL of Hardware-based Management ACL of Software-based

Access Control ☒

Rule

① After rules added, the system will generate default dropped rules for each set of services and VLAN interfaces of the rules, with the lowest priority

Rule ID	Service	Action	IP Address	Mask	VLAN Interface	Operation
 No Data						

Management ACL of Hardware based

•Rule ID

1

Valid range is 1-2147483647. The smaller ID is matched first.

•Service

HTTPS

Action

☐ Allow ☒ Drop

•IP Address

192.168.40.1

IPv4 format

Mask ⓘ

255.255.255.0

IPv4 format

•VLAN Interface

1

Cancel

OK

Add a Hardware based ACL Rule

Management ACL of Software-based

On the GWN780x Pro switch, the software-based Management ACL uses firewall-like rules to control who can access the network and its management features. This means it sets up restrictions to make sure that only authorized users and devices can access important parts of the switch, helping to keep the network secure and well-managed.

•ACL Name

Test_Rule ⓘ

1~64 characters

Rule Settings ⓘ

•Rule ID

1

Valid range is 1-2147483647. The smaller ID is matched first.

Action

☒ Allow ☐ Drop

IPv4 Address/Mask

☒ Any ☐ Custom

IPv6 Address/Prefix Length

☒ Any ☐ Custom

•Service

☐ HTTPS ☐ SSH ☐ Telnet ☐ SNMP

Port

Click on port to select/unselect

Port

2 4 6 8 10 12 14 16 18 20 22 24

1 3 5 7 9 11 13 15 17 19 21 23 25 SFP1 26 SFP2 27 SFP3 28 SFP4

LAG

2 4 6 8

1 3 5 7

Management ACL of Software based

User Management

There are three levels of users, namely administrator, operator, and monitor. The administrator authenticates and authorizes users who log in to the switch according to management needs, 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 and deleting operators and monitors.

2. Operator

- Added by an 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 the password.
- Support adding and deleting Monitor users.

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 or configuration authority.
- Can't change the username, only the password.

Click **Add** to create an Operator or Monitor account. To configure key-based SSH access, use the SSH public-key operation for the required account in the user list, paste its public key, and confirm the change. Sign in using the corresponding private key, which must remain on the SSH client. SSH must also be enabled under **System -> Access Control -> Web Service Management**.

User Management

AddDelete

☐	Username	Level	SSH Public Key	Creator	Creation Time	Operation
☐	admin	Administrator	--	--	--	 

© 2026 Grandstream Networks, Inc. Grandstream Software License Agreement

User Management and SSH Public Key

Time Policy

The time policy page helps to create schedules, for example, Office working hours, Upgrade schedules, or reboot schedules.

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

Time Policy

+ Create Policy

Upgrade Schedule

Create Policy

If both weekly and absolute schedules are configured on the same day, only the absolute schedule will take effect.

Policy Name

Reboot Schedule

1-64 characters

Weekly

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							

Absolute Date / Time (If no time period is selected on the scheduled date, no service on the corresponding date will be excuted.)

Please select date (multiple choices are allowed)

Please select time (multiple choices are allowed)

Add

Cancel

OK

Time Policy

1588v2 TC

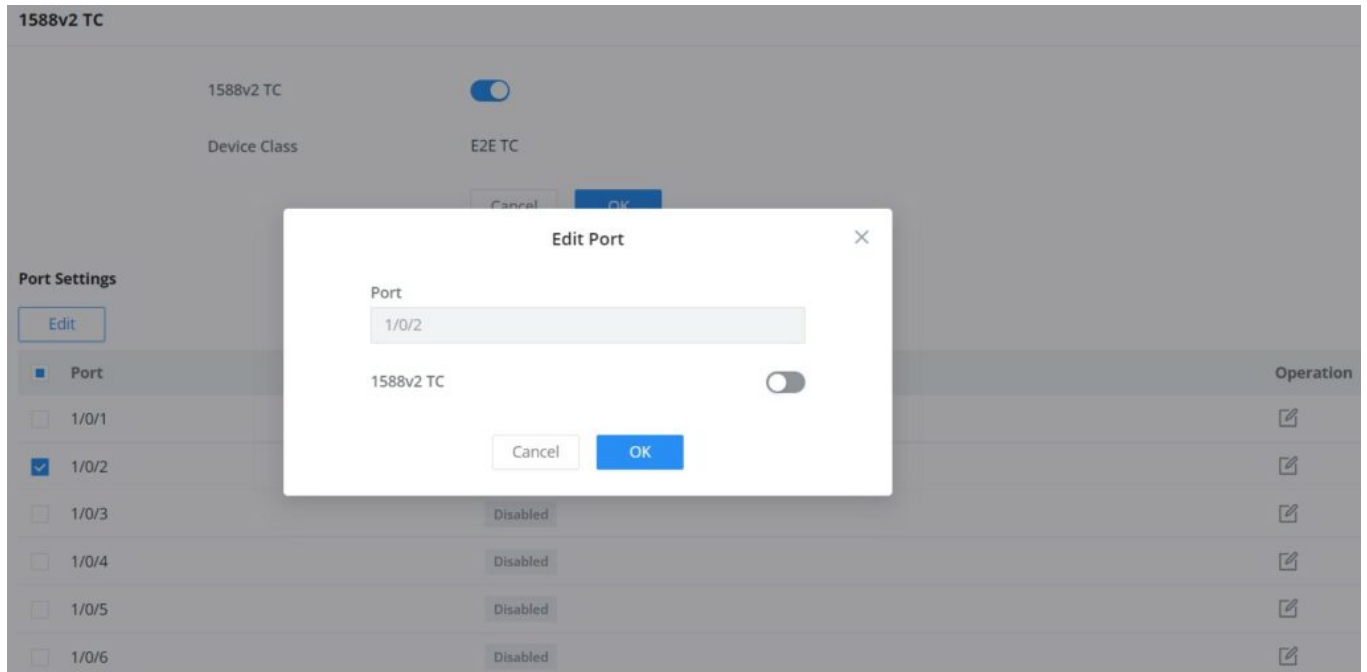
IEEE 1588v2, also known as Precision Time Protocol (PTP), is used to synchronize time across devices in a network.

Transparent Clock (TC) is a PTP switch operation mode where the switch measures the time a PTP message spends transiting the switch and updates the correction information accordingly. This helps endpoint devices (PTP master and slave clocks) maintain accurate time synchronization.

In End-to-End Transparent Clock (E2E TC) mode, delay is measured across the path between the master and slave clocks, while the switch contributes its measured residence time to the PTP correction field.

How to configure IEEE 1588v2 TC

1. Go to Settings -> 1588v2 TC.
2. Enable 1588v2 TC globally.
3. Set Device Class to E2E TC.
4. Under Port Settings, enable 1588v2 TC on the required ports (per-port configuration).



1588v2 TC

Note: This feature is currently in Beta. The Web UI supports E2E TC only.

STACK

Stacking allows supported switches to operate as one logical unit.

Supported Models: GWN7806PL Pro and GWN7806PH Pro.

To access this feature, navigate to: **Web UI -> Stack -> Stack Settings**

For full configuration examples, topology use cases, and best practices, please refer to the GWN78xx Stacking Feature Guide.

Stack Settings

Use Stack Settings to assign the device ID and election priority that will apply after the next reboot, and select the two physical stack ports. Once the stack is formed, its controller can manage multicast, SNMP, RMON, Identity Authentication Management, and ACL functions across the stack.

Stack Settings

ⓘ Please ensure that the device ID is unique; otherwise, the device will be unable to join the stack. After configuration, reboot the switch for the settings to take effect. Use optical modules to cross-connect the stack ports. Once connected, power on the switches (it is recommended to power on the pre-configured primary switch first) to form the stack. Switches in a stack must run the same software version. Please upgrade them to the same version in advance.

Device ID	Device ID for Next Boot	Priority	Priority for Next Boot	Stack Port 1	Stack Port 2	Operation
1	1	1	1	--	--	

Stack Settings

Stack Settings > Edit

Device ID

1

•Device ID for Next Boot

1

Valid range is 1-8

Priority

1

•Priority for Next Boot

1

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

Stack Port 1

Please select

Stack Port 2

Please select

Cancel

OK

Stack Member Settings

Field	Description
Device ID for Next Boot	Assigns the member's unique stack ID after reboot. Valid range: 1-8.
Priority for Next Boot	Sets the member's election priority after reboot. Valid range: 1-255; a higher value gives the member a higher priority.
Stack Port 1 / Stack Port 2	Selects the two 10 Gbps optical ports used to cross-connect the stack members.

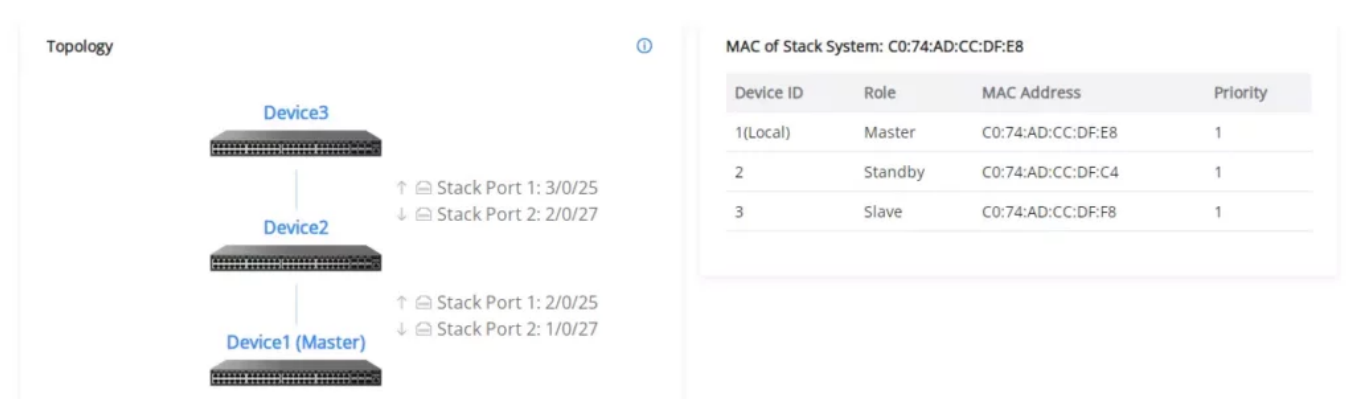
Stack Member Settings Fields

Warning: Save the settings and reboot the switch for the next-boot values to take effect. Use switches of the same model and firmware version. Set eligible SFP+ stacking ports to 10 Gbps and shut down the physical ports before assigning them to a stack. Cross-connect Stack Port 1 to Stack Port 2 on the neighboring member. Power on the preconfigured primary switch first when possible.

Stack Info

Stack Info displays the stack topology, roles, device IDs, priorities, and port mappings. To configure an individual member, open **Stack -> Stack Settings** and edit that member's row.

Stack Info



Stack Info

- If no data appears, ensure stack settings are properly configured and devices are connected.
- All stacked switches must be running the same firmware version.

CHANGE LOG

This section documents significant changes from previous versions of the GWN780x Pro 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 1.0.17.11

Product Name: GWN7801P Pro / GWN7802P Pro / GWN7803 Pro / GWN7803PL Pro / GWN7803PH Pro / GWN7806PH Pro / GWN7806PL Pro

- Added [[ERPS](#)].
- Added multiple RADIUS server groups and RADIUS authorization/accounting in [[RADIUS](#)] and [[AAA](#)].
- Added multiple TACACS+ server groups and TACACS+ authorization/accounting in [[TACACS+](#)] and [[AAA](#)].
- Replaced SSH Remote Access with [[Remote Support](#)] under Diagnostics.
- Added [[Web CLI](#)].
- Added HTTPS TLS-version settings under [[Web Service Management](#)].
- Updated the GWN7801P Pro total PoE power to 130 W in [[Technical Specifications](#)].

Version 1.0.17.6

Product Name: GWN7801P Pro / GWN7802P Pro / GWN7803 Pro / GWN7803PL Pro / GWN7803PH Pro / GWN7806PH Pro / GWN7806PL Pro

- Added 2.5 Gbps SFP+ support in [[Port Basic Settings](#)].
- Added queue-dropped packet counters in [[Port Statistics](#)].
- Expanded Grandstream OUI support for [[Voice VLAN](#)].
- Added two selectable MAC-table hashing profiles for GWN7801P Pro, GWN7802P Pro, GWN7803 Pro, GWN7803PL Pro, and GWN7803PH Pro in [[MAC Address Table](#)].
- Added MAC address migration records for GWN7806PH Pro and GWN7806PL Pro in [[MAC Address Migration Record](#)].

- Extended VLAN Stacking support to all GWN780x Pro models in [[VLAN Port Settings](#)].
- Added Class of Service to the [[management IP interface](#)].
- Optimized [[DHCP Server](#)] address pools and [[ARP/NDP](#)].
- Added [[Policy Route](#)] for GWN7806PH/PL Pro and custom route specifications for [[Static Routes](#)].
- Added MLD Matching Domain for GWN7801P Pro, GWN7802P Pro, and GWN7803 Pro under [[MLD Snooping](#)].
- Optimized [[Port Security](#)], [[Port Isolation](#)], ACL statistics, and ACL utilization reporting.
- Updated nonzero rate-limit actions and dropped-packet counters under [[Dynamic ARP Inspection \(DAI\)](#)].
- Optimized [[Identity Authentication Management](#)] and added [[ND Snooping](#)].
- Added automatic backup and boot-configuration selection under [[Backup & Restore](#)].
- Expanded [[Capture](#)] to all Pro models and optimized [[management-platform diagnostics](#)].
- Added [[sFlow](#)] support.
- Optimized [[SNMP](#)].
- Added more [[alerts](#)].
- Added Telnet port configuration under [[Web Service Management](#)].
- Added SSH public-key support for users under [[User Management](#)].
- Added [[Passwordless Remote Access](#)] through GDMS Networking and GWN Manager.
- Expanded [[Stack](#)] management.
- Increased the maximum allowed MAC-address limit to 2000 under [[Port Security](#)].
- Added pipe filtering under [[CLI Access](#)].

Version 1.0.17.5

Product Name: GWN7806PH Pro / GWN7806PL Pro

- Added selectable 2.5 Gbps/10 Gbps SFP+ speed modes under [[Port Basic Settings](#)].
- Added the Queue Dropped Packets column in [[Port Statistics](#)].
- Expanded the built-in Grandstream entries under [[Voice VLAN OUI](#)].
- Added four selectable MAC-table hashing profiles in [[MAC Address Table](#)].
- Added the [[MAC Address Migration Record](#)].
- Added VLAN Stacking in [[VLAN Port Settings](#)].
- Added Class of Service to the [[management IP interface](#)].
- Expanded [[DHCP Server](#)] address-pool controls with per-pool enable/disable, a global-pool gateway, and DHCP options.
- Reorganized [[ARP Table](#)] and [[Neighbor Discovery](#)] into learned/dynamic and static-entry views.
- Added [[Policy Route](#)].
- Added user-configurable route specifications in [[Static Routes](#)].
- Expanded [[Port Isolation](#)] with Layer 2/Layer 3 isolation modes and unidirectional or bidirectional interface isolation.
- Expanded advanced statistics and utilization reporting under [[ACL](#)].
- Added a Drop action for nonzero DAI rate limits and corresponding dropped-packet statistics under [[Dynamic ARP Inspection \(DAI\)](#)].
- Expanded local MAC authentication with Import and Name under [[Identity Authentication Management](#)].
- Added [[ND Snooping](#)].
- Added Scheduled Backup under [[Backup and Restore](#)].
- Added per-file Restore Configuration on Reboot under [[Backup and Restore](#)].
- Added [[Capture](#)].

- Expanded [[Management Platform Connection Diagnostics](#)] with platform selection, connected status, and connection-log access.
- Added [[sFlow](#)].
- Expanded [[SNMP](#)] with version selection, view/group/OID management, AES privacy, and additional trap information.
- Added ARP and fiber-module events under [[Alert](#)].
- Added Telnet port configuration under [[Web Service Management](#)].
- Added SSH public-key management under [[User Management](#)].
- Added passwordless remote access through [[GDMS Networking and GWN Manager](#)].
- Expanded [[Stack](#)] management for multicast, SNMP, RMON, Identity Authentication Management, and ACL.
- Added member-specific controls under [[Stack Settings](#)].
- Increased the Maximum MAC Number to 2000 under [[Port Security](#)].
- Added pipe filtering under [[CLI Access](#)].
- Increased the supported VLAN IP interfaces to 512 under [[IPv4/IPv6 Interface](#)].

Version 1.0.15.219

Product Name: GWN7801P Pro / GWN7802P Pro / GWN7803 Pro / GWN7803PL Pro / GWN7803PH Pro / GWN7806PL Pro / GWN7806PH Pro

- Added support for [[Pro AV](#)].
- Added support for [[IEEE 1588 PTP](#)].

Version 1.0.15.211

Product Name: GWN7801P Pro / GWN7802P Pro / GWN7803 Pro / GWN7803PL Pro / GWN7803PH Pro / GWN7806PL Pro / GWN7806PH Pro

- This is the initial version.
-