



Grandstream Networks, Inc.

---

**GWN780x Pro Series Managed switches**

User Manual



# INTRODUCTION

The **GWN780x Pro Series** is are **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:

- o **VLAN configuration** for flexible traffic segmentation
- o **QoS** for precise traffic prioritization
- o **IGMP/MLD Snooping** to optimize multicast performance
- o **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:

- o **Embedded Web UI controller**
- o **GDMS Networking** (cloud)
- o **GWN Manager** (on-premise software)
- o **GWN Series Routers**
- o **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<br>Pro                       | GWN7802P<br>Pro | GWN7803<br>Pro | GWN7803PL<br>Pro | GWN7803P<br>H Pro | GWN7806P<br>L Pro                                                                                 | GWN7806P<br>H 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<br>MM-10G: 2<br>RJ45-10G: 2 |                 |                |                  |                   | SM-10G: 6<br>MM-10G: 6<br>RJ45-10G: 3<br><i>*Note: RJ45-10G modules must be interval inserted</i> |                   |
| 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 interAptiveTM 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                       | <4μs                                                       |                           |                                                  |                           |                                                  |                                    |                           |
| 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 120W)                                   | 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    | 120W                                                                                                                                                                                              | 250W                          | /     | 250W            | 400W                                                 |                 | 800W               |
| Physical                      |                                                                                                                                                                                                   |                               |       |                 |                                                      |                 |                    |
| Unit Dimension                | 330mm(L) × 175mm(W) × 44mm(H)                                                                                                                                                                     | 440mm(L) × 200mm(W) × 44mm(H) |       |                 | 440mm(L) × 300mm(W) × 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<br>1x 25cm Ground Cable<br>4x Rubber Footpads<br>1x Power Cord Anti-Trip<br>8x Screws (KM3*6)<br>1x 1.2m(10A) AC Cable<br>1x Simplified Quick Installation Guide<br>1x Regulatory Paper |                               |       |                 |                                                      |                 |                    |
|                               | 1x Extended Rack-Mounting Kits                                                                                                                                                                    | 2x Rack-Mounting Kits         |       |                 |                                                      |                 |                    |
| Environmental                 |                                                                                                                                                                                                   |                               |       |                 |                                                      |                 |                    |
| Temperature                   | Operation: 0°C to 45°C<br>Storage: -10°C to 60°C                                                                                                                                                  |                               |       |                 |                                                      |                 |                    |
| Humidity                      | Operation: 10% to 90% RH (Non-condensing)<br>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<br>power supply failure alarming                                                                                                                      |                               |       |                 |                                                      |                 |                    |
| Fan Monitoring                | Automatic speed adjustment<br>fan failure alarming                                                                                                                                                |                               |       |                 |                                                      |                 |                    |
| Temperature Monitoring        | Temperature monitoring, over-temperature alarming                                                                                                                                                 |                               |       |                 |                                                      |                 |                    |
| Surge Protection              | ± 6KV CM for power<br>± 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 802.3ac, 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               | <ul style="list-style-type: none"><li>○ Jumbo frame (maximum length: 12288)</li><li>○ 4K VLANs, port-based VLAN, IEEE 802.1Q VLAN tagging</li><li>○ QinQ</li><li>○ MAC-based VLAN</li><li>○ Protocol-based VLAN</li><li>○ Voice VLAN including auto voice VLAN, tagged OUI and untagged OUI</li><li>○ GVRP(pending)</li><li>○ ERPS(pending)</li></ul> |                                                                                               |
|                         | 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              | <ul style="list-style-type: none"><li>○ DHCP client, DHCP server, DHCP relay and DHCP snooping</li><li>○ DHCPv6 client and DHCPv6 snooping</li><li>○ ND snooping</li><li>○ DNS</li></ul>                                                                                                                                                              |                                                                                               |
|                         | 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                                                                                                                                                                                                                                                                                                              | 32 VLAN virtual interfaces with 9216 MTU                                                      |
| IP Routing              | Policy routing (pending)                                                                                                                                                                                                                                                                                                                              |                                                                                               |
|                         | 32(IPv4)/32(IPv6) static routes                                                                                                                                                                                                                                                                                                                       | 1K(IPv4)/1K(IPv6) static routes                                                               |

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |                                                                |                                                                |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------|----------------------------------------------------------------|
| <b>Multicast</b>   | 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     |
| <b>QoS</b>         | <ul style="list-style-type: none"> <li>Port priority</li> <li>Priority mapping, including 802.1p mapping, DSCP mapping and IP precedence mapping</li> <li>Queue scheduling, including SP, WRR, WFQ, SP-WRR and SP-WFQ</li> <li>Traffic shaping</li> <li>Rate limit</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                                                                |                                                                |
| <b>ACL</b>         | 128 ACL for Ethernet, IPv4 and IPv6 with 1.5K ACE                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                                                                | 256 ACL for Ethernet, IPv4 and IPv6 with 4K ACE                |
|                    | <ul style="list-style-type: none"> <li>MAC ACLs (hardware ACLs based on source MAC address, destination MAC address, optional Ethernet type, and time range)</li> <li>IPv4 ACLs (hardware ACLs based on source IP address, destination IP address, and optional protocol type, and time range)</li> <li>IPv6 ACLs (hardware ACLs based on source IPv6 address, destination Ipv6 address, and optional protocol type, and time range)</li> <li>Expert ACLs (hardware ACLs based on flexible combinations of the VLAN ID, Ethernet type, MAC address, IP address, protocol type, and time range) (TBD)</li> <li>Customized ACLs (ACL80) (TBD)</li> <li>ACL redirection</li> <li>ACL advanced settings, including statistics, mirror, priority mapping, and rate limit</li> <li>ACL binding, including port and VLAN</li> </ul> |                                                                |                                                                |
| <b>Security</b>    | <ul style="list-style-type: none"> <li>User hierarchical management and password protection, HTTPS, SSH, Telnet</li> <li>Identity authentication, including 802.1X and MAC authentication</li> <li>AAA authentication, including RADIUS, TACACS</li> <li>Strom control</li> <li>Port isolation</li> <li>Port security, sticky MAC address, filtering invalid MAC addresses</li> <li>IP/IPv6 source guard, DoS attack prevention, ARP inspection, CPU protection</li> <li>Loop protection, including port loopback detection, BPDU protection, root protection, and loopback protection</li> <li>Kensington Security Slot (Kensington Lock) support</li> <li>Firmware signature</li> </ul>                                                                                                                                    |                                                                |                                                                |
| <b>Reliability</b> | <ul style="list-style-type: none"> <li>Power supply modules in 1+1 redundancy mode</li> <li>Stack intelligent upgrade</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |                                                                |                                                                |
| <b>Maintenance</b> | <ul style="list-style-type: none"> <li>NTP</li> <li>1588v2 TC for precise time (Pending)</li> <li>CPU and memory monitoring</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                                                                |                                                                |

|                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                            | <ul style="list-style-type: none"> <li>○ Fault detection and alarm for power supply and fan</li> <li>○ SNMP including SNMPv1, SNMPv2c, SNMPv3</li> <li>○ RMON including history groups, event groups, alarm groups, and statistics groups</li> <li>○ LLDP&amp;LLDP-MED</li> <li>○ Backup and restore</li> <li>○ Syslog</li> <li>○ Diagnostics including Ping, traceroute, Ping watchdog, mirror including SPAN and RSPAN, UDLD(TBD), copper test, fiber module, and one-click debugging</li> <li>○ sFlow (pending)</li> <li>○ Upgrade via FTPS/ TFTP/ HTTP/ HTTPS or local upload, mass provisioning using DHCP Option/ TR-069 (pending)/ GDMS Networking/ GWN Manager/ GWN series routers</li> </ul> |
| <b>Management Platform</b> | <ul style="list-style-type: none"> <li>○ Local Web GUI: embedded controller</li> <li>○ GDMS Networking: free cloud management platform for unlimited GWN78x0 Pro series switches</li> <li>○ GWN Manager: premise-based software controller</li> <li>○ GWN APP: integrated GDMS Networking and GWN Manager to manage GWN78x0 Pro series switches via the APP</li> <li>○ Management Protocol: SNMP, RMON, TR-069 (pending)</li> </ul>                                                                                                                                                                                                                                                                   |

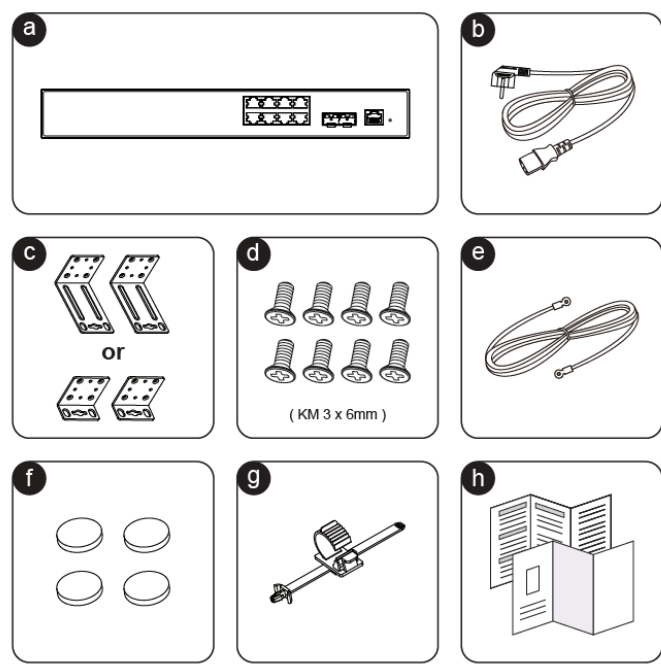
GWN780x Pro Technical Specifications

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

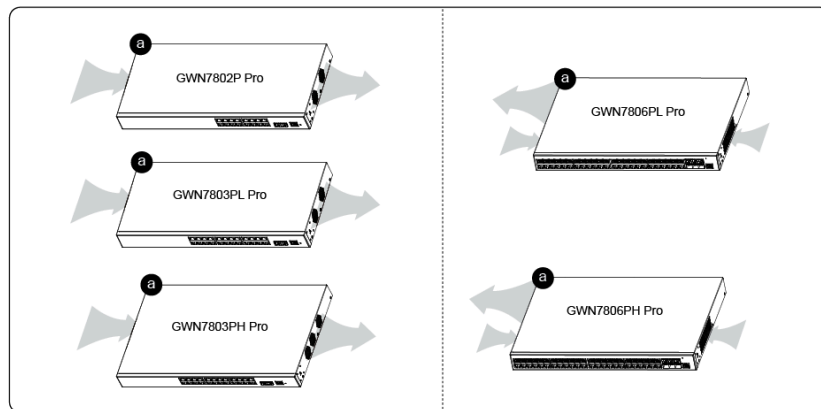
|   |                                                         |
|---|---------------------------------------------------------|
| a | GWN780x Pro Series                                      |
| b | 1x 1.2m (10A) AC Cable                                  |
| c | Rack Mounting Kits or<br>Extended Rack Mounting<br>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*

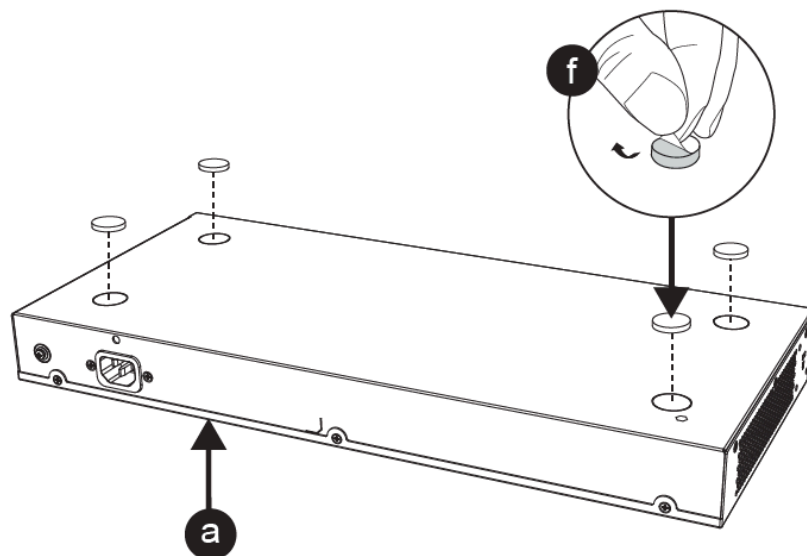
## Fan Ventilation

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*

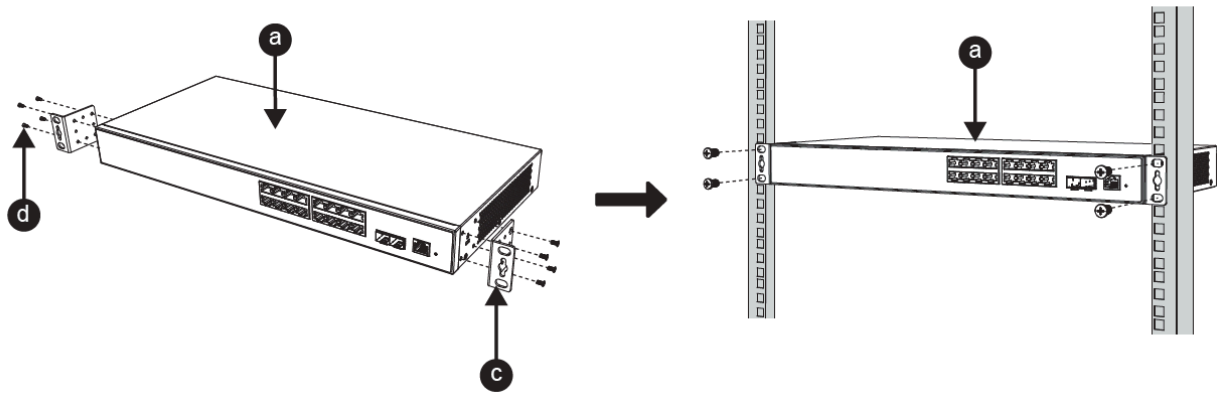
## Install on the Desktop



*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

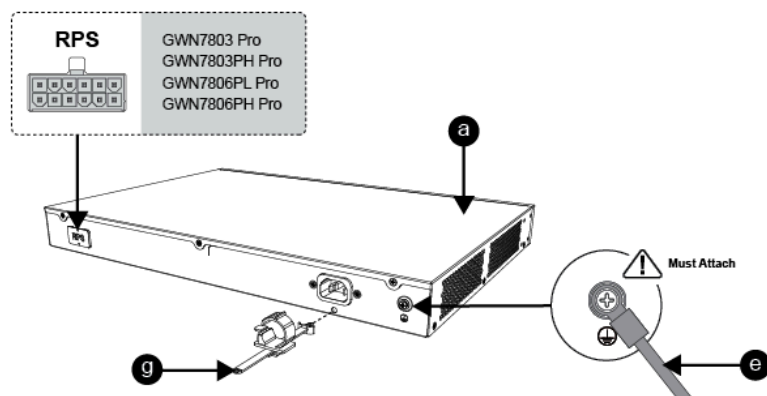
Connect the power cable and the switch first, then connect the power cable to the power supply system of the equipment room.

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 Pro, GWN7806 Pro, GWN7806PL Pro, GWN7806PH Pro

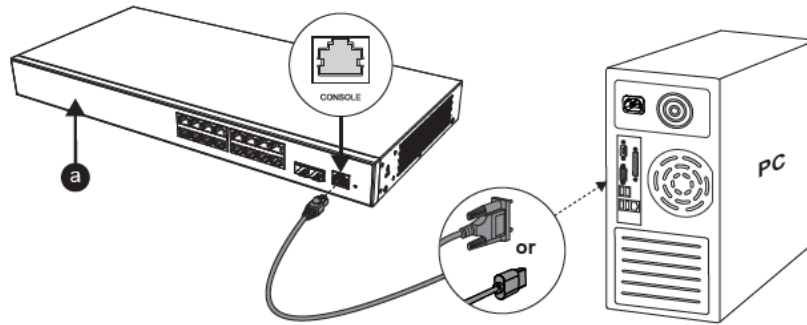
Connect the Grounding cable by following the steps below:

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.



## 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

### Safety Compliances

The GWN780x Pro Network Switch complies with FCC/CE and various safety standards. The GWN780x Pro power adapter is compliant with the UL standard. Use the universal power adapter provided with the GWN780x Pro package only. The manufacturer's warranty does not cover damage to the device caused by unsupported power adapters.

### Warranty

If the GWN780x Pro Network Switch was purchased from a reseller, please contact the company where the device was purchased for replacement, repair, or refund. If the device was purchased directly from Grandstream, contact our Technical Support Team for an RMA (Return Materials Authorization) number before the product is returned. Grandstream reserves the right to remedy the warranty policy without prior notification.

## GETTING STARTED

### LED Indicators

The front panel of the GWN780x 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                                                                                                               |
|                  | Solid green    | Booting                                                                                                                 |
|                  | Flashing green | Upgrade                                                                                                                 |
|                  | Solid blue     | Normal use                                                                                                              |
|                  | Flashing blue  | Provisioning                                                                                                            |
|                  | Solid red      | Upgrade failed                                                                                                          |
|                  | Flashing red   | Factory reset                                                                                                           |
| Port Indicator   | Off            | <ul style="list-style-type: none"> <li>• For all ports: port off</li> <li>• For SFP/SFP+ ports: port failure</li> </ul> |
|                  | 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                                                                                      |
| <b>PWR/RPS Indicator</b> | Off                                   | Uninserted or failure                                                                                      |
|                          | Solid Green                           | <ul style="list-style-type: none"> <li>○ In use</li> <li>○ Inserted but not used (only for RPS)</li> </ul> |

#### LED Indicators

#### Note

During the boot sequence, the LED indicator transitions through multiple color states.

## Access & Configure

#### Note

If no DHCP server is available, the GWN780x Pro default IP address is 192.168.0.254.

## 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).

#### Note

The baud rate needs to be set to 115200.

## 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).

#### Note:

Supports SSH and TELNET in #Mode (EXEC mode).

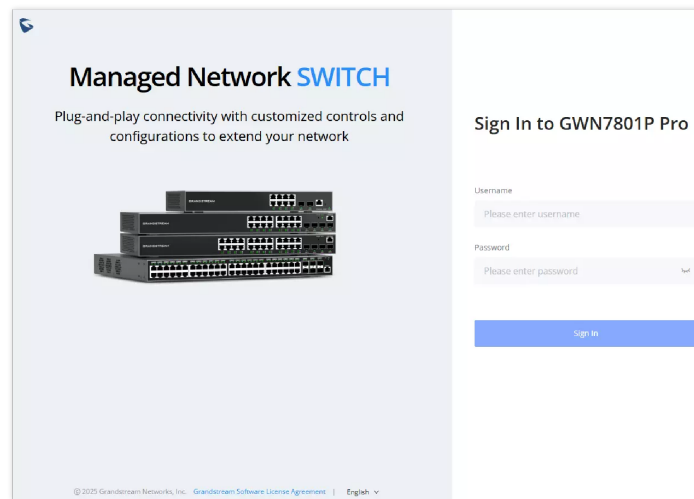
GWN Switches support [Web CLI](#).

## Configure Using GDMS Networking

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

## Login Using the Web UI

The GWN780x 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.



*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.)

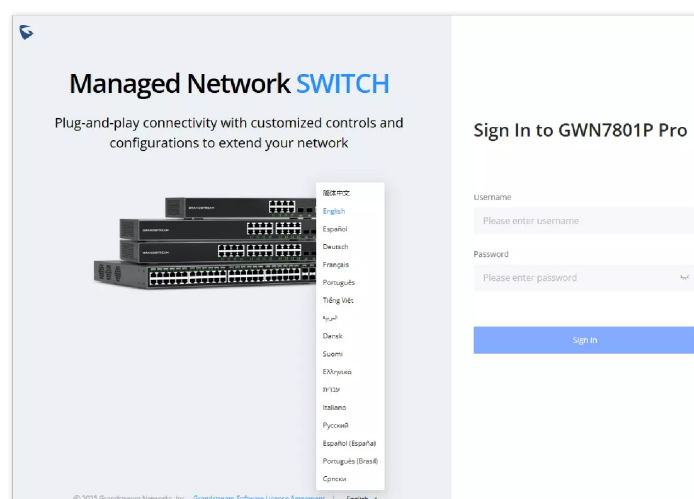
## CLI Access

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

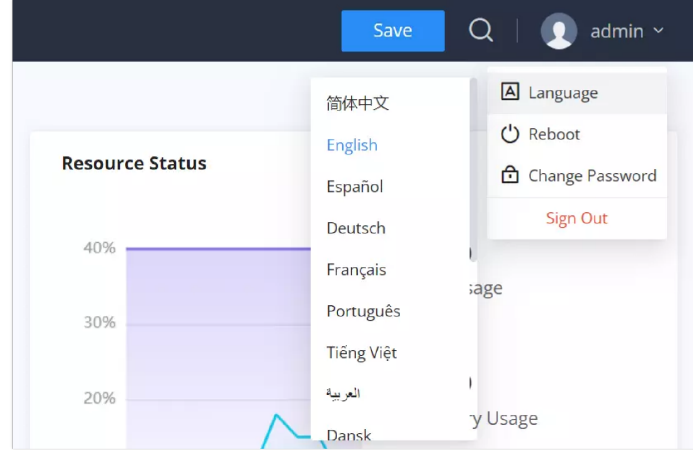
## Web GUI Languages

The 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

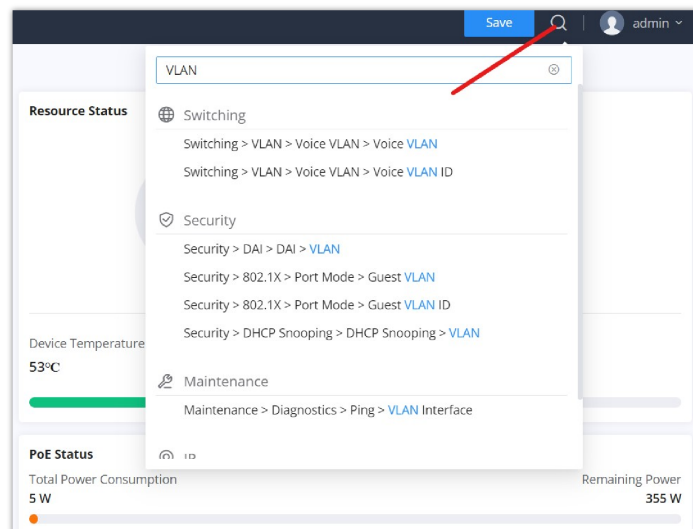
**Note:**

When the Web GUI language is manually changed from the login page or within the interface, the selected language will be saved in the device's configuration. This preference will persist across sessions, reboots, and browsers, regardless of the system's regional or browser settings.

## Search

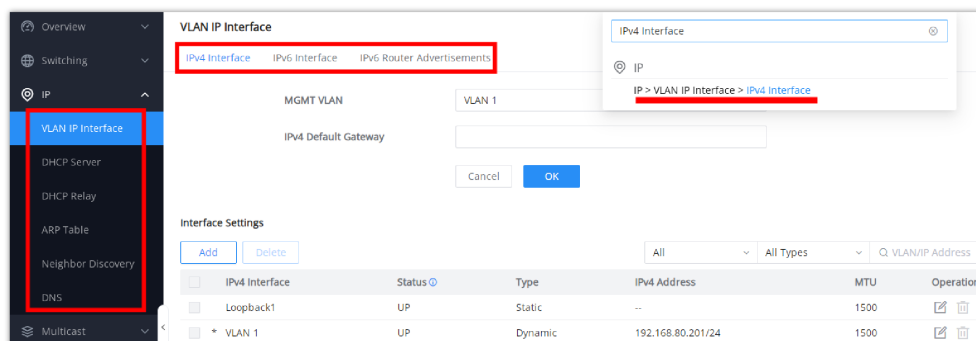
In case it's hard to go through every single section, GWN780x Pro Switches have search functionality to help the user find the right configuration, settings, or parameters, etc.

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:



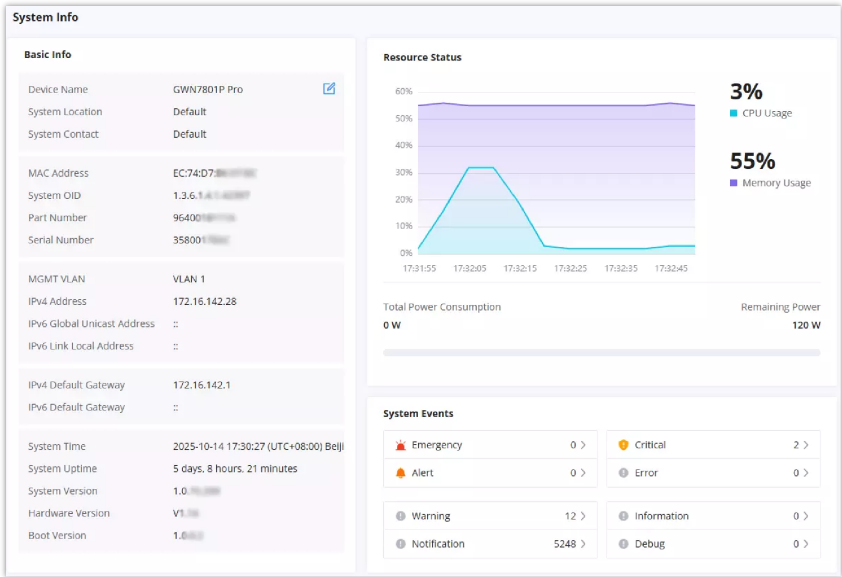
Search part 2

# 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

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).<br><i>Note: Clicking on any events category will redirect you to the Diagnostics page for further details.</i> |
| Fan             | Displays the fans operation status and speed.                                                                                                                                                         |
| Power Supply    | Shows the status of the built-in power supply as well as the RPS (Redundant Power Supply).                                                                                                            |

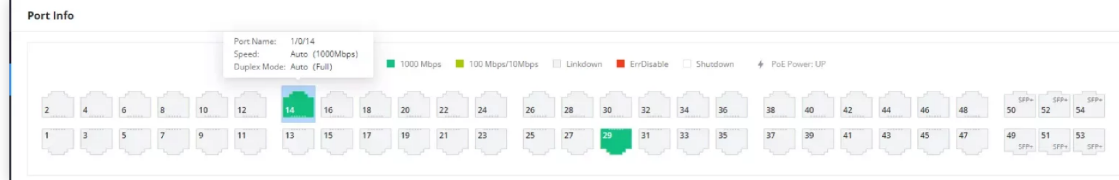
System Info page

## 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

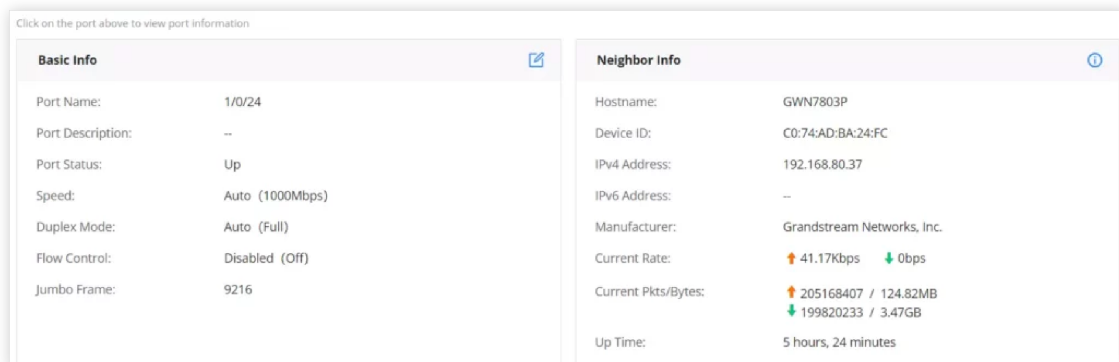
The “Port Info” section visually displays the status and speed of each port, using different colors for speeds and states. Users can quickly identify active, inactive, or problematic ports and their PoE power status.



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.



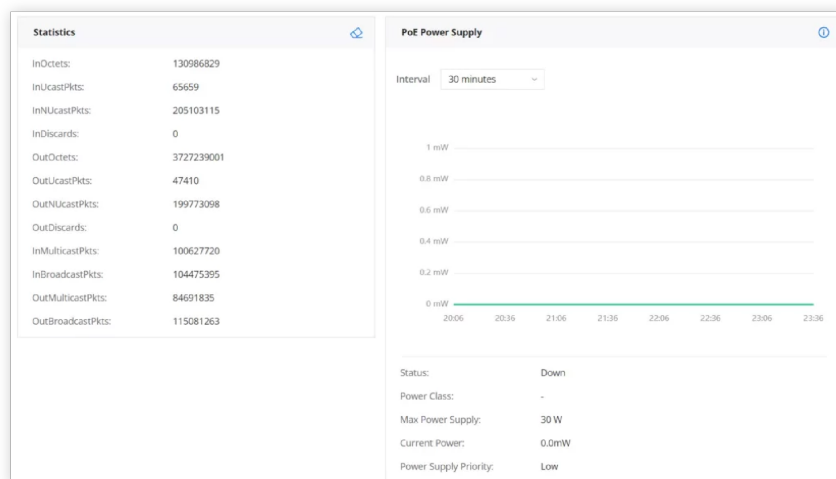
Port Info page 2

- 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.



Port Info page 3

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

|  |                                                                    |
|--|--------------------------------------------------------------------|
|  | <b>Grey:</b> Linkdown                                              |
|  | <b>White:</b> shutdown                                             |
|  | <b>Green:</b> Ethernet RJ45 port with 1000 Mbps speed              |
|  | <b>Light green:</b> Ethernet RJ45 port with 100 Mbps/10 Mbps speed |

|  |                                                                                                                     |
|--|---------------------------------------------------------------------------------------------------------------------|
|  | <b>Red:</b> ErrDisable                                                                                              |
|  | <b>Green:</b> SFP/SFP+ Port set to 1000Mbps                                                                         |
|  | <b>Purple:</b> SFP/SFP+ Port set to 2.5Gbps<br><b>Note:</b> only for GWN7801P pro, GWN7802P Pro, GWN7803(PL/PH) Pro |
|  | <b>Blue:</b> SFP+ port set to 10Gbps<br><b>Note:</b> only for GWN7802P Pro, GWN7803(PL/PH) Pro and GWN7806PL/PH Pro |
|  | <b>Symbol:</b> 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

On this page, you can configure the basic parameters for GWN780x Pro Switch ports, like disabling or enabling the port, adding a Description, specifying the speed by default as Auto, Duplex Mode, and Flow Control. There is also a filter on in case you want to edit only the Copper ports, which are the Gigabit Ethernet ports, or Fiber ports, which are the SFP+ ports.

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

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

Port Basic Settings

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

Port Basic Settings > **Edit Port**

|                   |                                                                                                                                                       |
|-------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|
| Port              | 1/0/28                                                                                                                                                |
| Port Type         | SFP+                                                                                                                                                  |
| Description       | <input type="text"/> 0~128 characters                                                                                                                 |
| Port Enable       | <input checked="" type="radio"/> Enable <input type="radio"/> Disabled                                                                                |
| Scheduled enabled | None                                                                                                                                                  |
| Auto Detect       | <input checked="" type="checkbox"/>                                                                                                                   |
| Speed             | 10Gbps                                                                                                                                                |
| DAC Cable         | Disabled                                                                                                                                              |
| Duplex Mode       | <input checked="" type="radio"/> Full                                                                                                                 |
| Jumbo Frame       | 9216 Valid range is 1518-10000                                                                                                                        |
| Flow Control      | <input checked="" type="radio"/> Disabled <input type="radio"/> Enabled<br>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 Basic Settings > **Edit Port**

|                   |                                                                                                                                                                                  |
|-------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Port              | 1/0/2                                                                                                                                                                            |
| Port Type         | Copper                                                                                                                                                                           |
| Description       | <input type="text"/> 0~128 characters                                                                                                                                            |
| Port Enable       | <input checked="" type="radio"/> Enable <input type="radio"/> Disabled                                                                                                           |
| Scheduled enabled | None                                                                                                                                                                             |
| Speed             | None                                                                                                                                                                             |
| Duplex Mode       | Working Hours                                                                                                                                                                    |
| Jumbo Frame       | 9216 Valid range is 1518-12288                                                                                                                                                   |
| Flow Control      | <input checked="" type="radio"/> Disabled <input type="radio"/> Enabled <input type="radio"/> Auto<br>Flow Control setting will not take effect if Duplex Mode is set to "Half". |

Cancel OK

Port Basic Settings scheduled enabled

|                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|--------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Port</b>              | The selected Port to be configured, it can be either Gigabit Ethernet port or SFP port.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Port Type</b>         | Displays the Port Type (Copper or SFP).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Description</b>       | It is used to configure the information description of this interface, which can be a description of usage, etc., with a maximum of 128 characters, and the characters limited to input are numbers 0-9, letters az / AZ and special characters.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Port Enable</b>       | Set whether to enable the interface.<br><i>it is enabled by default.</i>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Scheduled enabled</b> | From the drop-down list, select the schedule for when the port (including physical and LAG ports) will be enabled.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Speed</b>             | <p>Set the rate of the interface:</p> <ul style="list-style-type: none"> <li>• <b>Ethernet port (Copper):</b> the options are {Auto, 10Mbps, 100Mbps, 1000Mbps}, The default is auto-negotiation.</li> <li>• <b>SFP/SFP+ port:</b> the options are:</li> <li>• <b>GWN7801P Pro 2.5G SFP:</b> 100Mbps, 1000Mbps, 2.5Gbps. Default: 2.5Gbps</li> <li>• <b>GWN7802P Pro/GWN7803(PL/PH) Pro SFP+:</b> 100Mbps, 1000Mbps, 2.5Gbps, 10Gbps. Default: 10Gbps</li> <li>• <b>GWN7806PL/PH Pro SFP+:</b> 100Mbps, 1000Mbps, 10Gbps. Default: 10Gbps</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>• When set to Auto, the rate of the interface is automatically negotiated between the interface and the peer port.</li> <li>• When configuring a fixed speed, ensure the peer port is set to the same value. Otherwise, the port may not function properly.</li> </ul> |
| <b>Duplex Mode</b>       | Set the duplex mode of the interface. The GE ports options are { auto-negotiation, full-duplex, half-duplex}. The default is auto-negotiation.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

|                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|---------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                     | <ul style="list-style-type: none"> <li>● <b>Auto-negotiation:</b> The duplex state of an interface is determined by the auto-negotiation between the interface and the peer port.</li> <li>● <b>Duplex:</b> the interface send and receive data packets.</li> <li>● <b>Half-duplex:</b> interface can only send/ receive packets.</li> </ul> <p><i>Notes:</i></p> <ul style="list-style-type: none"> <li>● Optical ports only support full-duplex mode.</li> <li>● When setting Duplex Mode manually (Duplex or Half-duplex), ensure the same mode is configured on the peer port. Otherwise, the port may not work normally.</li> </ul> |
| <b>Jumbo Frame</b>  | Specify the Jumbo Frame, the valid range is 1518-12288. Default is 9216                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Flow Control</b> | <p>Set the flow control on the interface, the options are {Disabled, Enabled, Auto}. <i>The default is Disabled.</i></p> <p>After enabling it, if the local device is congested, it will send a message to the peer device to notify the peer device to temporarily stop sending packets, after receiving the message, the peer device will temporarily stop sending packets to the local and vice versa. Thus, the occurrence of packet loss is avoided.</p> <p><i>Note: The optical port does not support auto-negotiation mode.</i></p>                                                                                               |

#### Port Basic Settings – Edit port

## 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**

LAG

#### 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 VLAN

VLAN > **Edit**

VLAN: 20

Description: VLAN20

Member Type: All Ports

Port: Click port to change the member type

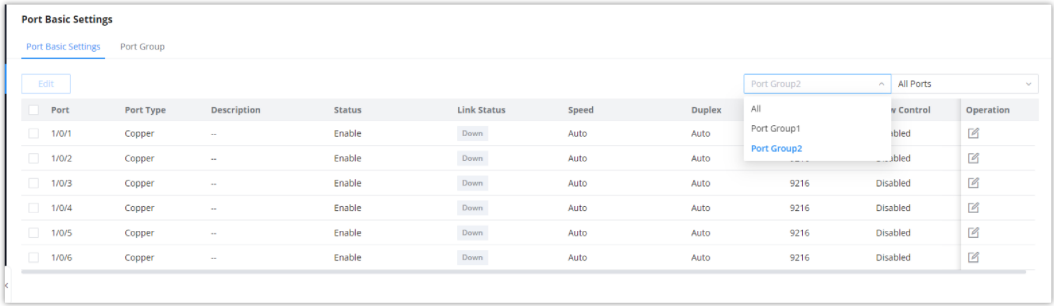
20(Security Devices)

Tagged (T) Untagged (U)

#### Port Group Selection



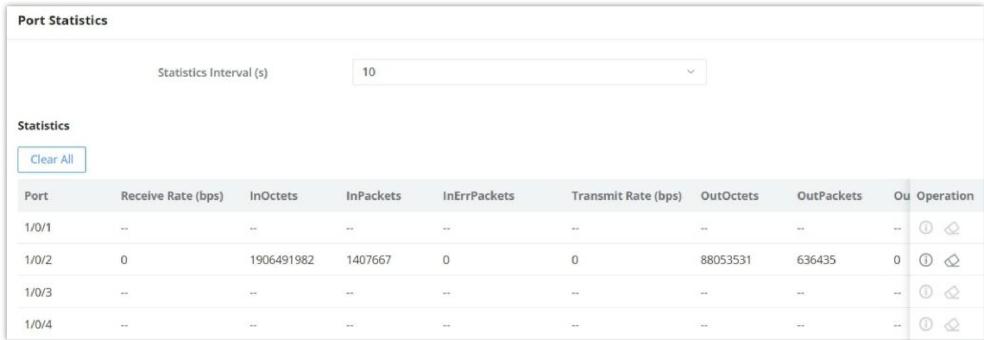
In addition, users can disable/enable specific ports based on the port group created, instead of going through each port selection separately:



Delete Port Group

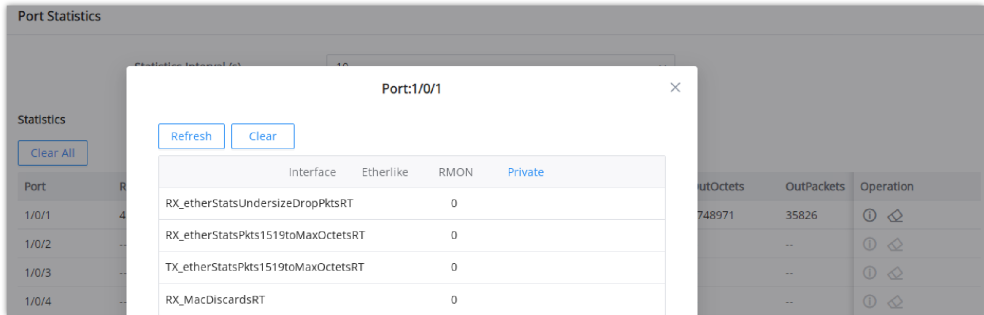
## Port Statistics

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



Port Statistics Part 1

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



Port Statistics part 2

## Loopback Detection

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

**Note:**

Interface Loopback Detection is not effective. If STP is enabled, because STP protection overrides interface Loopback Detection.

Loopback Detection ☐

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.

### Note

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

Port Auto Recovery

Recovery Items

☒ All

☒ ARP Packet Detection ☒ STP BPDU Guard

☒ DHCP Rate Limit ☒ DHCPv6 Rate Limit

☒ Broadcast Storm Control ☒ Unicast Storm Control

☒ Unknown Multicast Storm Control ☒ Port Selfloop

☒ BPDU Selfloop ☒ ACL

☒ Port Security

Delay Time (s)  Valid range is 30-85400

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

Link Aggregation 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                                                                             |
|------------------------------------------|-------------|--------|-------------|----------|-------------|--------------|---------------------------------------------------------------------------------------|
| <input checked="" type="checkbox"/> LAG1 | --          | Enable | Down        | 1000Mbps | 9216        | Disabled     |  |
| <input type="checkbox"/> LAG2            | --          | Enable | Down        | 1000Mbps | 9216        | Disabled     |  |
| <input type="checkbox"/> LAG3            | --          | Enable | Down        | 1000Mbps | 9216        | Disabled     |  |
| <input type="checkbox"/> LAG4            | --          | Enable | Down        | 1000Mbps | 9216        | Disabled     |  |
| <input type="checkbox"/> LAG5            | --          | Enable | Down        | 1000Mbps | 9216        | Disabled     |  |
| <input type="checkbox"/> 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.<br><i>it is enabled by default.</i>                                                                                                                                                                      |

|                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|---------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Speed</b>        | Set the rate of the interface, the options are {Auto, 10Mbps, 100Mbps, 1000Mbps}.<br><i>The default is auto-negotiation.</i><br><b>Note:</b> When set to Auto, the rate of the interface is automatically negotiated between the interface and the peer port.                                                                                                                                                                                      |
| <b>Jumbo Frame</b>  | Specify the jumbo frame, valid range is 1518-12288. Default value is 9216                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Flow Control</b> | Set the flow control on the interface, the options are { Disabled, Enabled, Auto}. <i>The default is Disabled</i><br>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**

Group LAG Settings **LACP**

System Priority: 32768 (Valid range is 1-65535)

Cancel OK

**LACP List**

Edit

| <input type="checkbox"/> | Port  | Port Priority | Timeout | Operation |
|--------------------------|-------|---------------|---------|-----------|
| <input type="checkbox"/> | 1/0/1 | 1             | Long    |           |
| <input type="checkbox"/> | 1/0/2 | 22            | Long    |           |
| <input type="checkbox"/> | 1/0/3 | 1             | Long    |           |
| <input type="checkbox"/> | 1/0/4 | 1             | Long    |           |
| <input type="checkbox"/> | 1/0/5 | 65            | Long    |           |
| <input type="checkbox"/> | 1/0/6 | 1             | Long    |           |
| <input type="checkbox"/> | 1/0/7 | 1             | Long    |           |

Link Aggregation LACP

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

### Link Aggregation – LACP

## MAC Address Table

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

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

## Dynamic Address

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

### Aging Time:

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

### Notes

- The value range is 0 or 60-1 000000, **the default is 300**. If it is set to 0, it means that dynamic MAC address entries will not be aged
- Dynamic table entries are lost after a system restart.

MAC Address Table

Dynamic Addresses

Static MAC Addresses

Blackhole Addresses

Port Secure Addresses

Aging Time (s)

300

Valid range is 0 and 60-1000000

Cancel

OK

Dynamic Addresses

Refresh

Add as Static MAC Address

Q VLAN/MAC Address/Port

| VLAN                                  | MAC Address       | Port  |
|---------------------------------------|-------------------|-------|
| <input checked="" type="checkbox"/> 1 | 00-0B-8C-17-4A-00 | 1/0/7 |
| <input checked="" type="checkbox"/> 1 | 00-0B-8C-1C-2F-00 | 1/0/7 |
| <input type="checkbox"/> 1            | 00-0B-8C-1C-2F-00 | 1/0/7 |
| <input type="checkbox"/> 1            | 00-0B-8C-2B-00-00 | 1/0/7 |
| <input type="checkbox"/> 1            | 00-0B-8C-2B-00-00 | 1/0/7 |

Dynamic MAC Address Table

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

## 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.

### Note

The static MAC address must be unicast.

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 AddressesStatic MAC AddressesBlackhole AddressesPort Secure Addresses

Add Blackhole Address

ⓘ Blackhole MAC address must be a unicast address.

\*MAC Address

:

:

:

:

:

:

\*VLAN

Valid range is 1-4094

CancelOK

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.

Note

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

| MAC Address Table                                                             |             |      |      |
|-------------------------------------------------------------------------------|-------------|------|------|
| Dynamic AddressesStatic MAC AddressesBlackhole AddressesPort Secure Addresses |             |      |      |
| Refresh                                                                       |             |      |      |
| VLAN                                                                          | MAC Address | Type | Port |
| <div>No Data</div>                                                            |             |      |      |

Port Security Address

# VLAN

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

**Note:**

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

| <input type="checkbox"/> VLAN | Description | Tagged Port | Untagged Port                            | Operation                         |
|-------------------------------|-------------|-------------|------------------------------------------|-----------------------------------|
| <input type="checkbox"/> 1    | Default     | --          | 1/0/1-1/0/6,1/0/8,1/0/18-1/0/28,LAG2-... | <div><div></div><div></div></div> |
| <input type="checkbox"/> 7    | Support     | 1/0/24      | 1/0/7                                    | <div><div></div><div></div></div> |
| <input type="checkbox"/> 9    | Sales       | 1/0/24      | 1/0/9-1/0/16                             | <div><div></div><div></div></div> |
| <input type="checkbox"/> 11   | Guests      | 1/0/24      | 1/0/17,LAG1,LAG5                         | <div><div></div><div></div></div> |

VLAN tab

Add VLAN

\*VLAN IDs

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

3-9,11

Cancel

OK

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

20

Description

VLAN20

Member Type

All Ports

Remove All

Tagged All

Untagged All

Port

Click port to change the member type

Tagged

Untagged

2

4

6

8

1

3

5

7

9 SFP1

10 SFP2

LAG

Click port to change the member type

Tagged

Untagged

2

4

6

8

1

3

5

7

Edit VLAN

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

#### VLAN Tagged and Untagged

### VLAN Port Settings

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

Port Settings > **Edit**

Port
1/0/1

Link Type
Trunk

PVID
Valid range is 1-4094

Accept Frame Type
Trunk

TPID
0x0100

VLAN Translation
☐

Cancel OK

VLAN Port Settings Link types



Port Settings > **Edit**

Port: 1/0/1

Link Type: Trunk

PVID: 1

Accept Frame Type: ☒ All ☐ Tag Only ☐ Untag Only

TPID: 0x8100

VLAN Translation: ☒

Ingress: ☐

VLAN Mapping1

Outer VLAN:

Inner VLAN:

VLAN after Outer Mapping:

VLAN after Inner Mapping:

Add 

Cancel OK

VLAN Port Settings VLAN Translation

Port Settings > **Edit**

Port: 1/0/2

Link Type: Hybrid

PVID: 1 Valid range is 1-4094

Accept Frame Type: ☒ All ☐ Tag Only ☐ Untag Only

TPID: 0x8100

Ingress Filtering: ☒

VLAN Translation: ☐

MAC VLAN: ☐

Protocol VLAN: ☒

Protocol Template

Protocol Template:  VLAN:  802.1p:  

Add 

Cancel OK

VLAN Port Settings Protocol Template

|                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Port</b>              | Shows the selected Port.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Link Type</b>         | <p>Select the Link Type:</p> <ul style="list-style-type: none"> <li>● <b>Hybrid:</b> Used for connection between switches, or switch and computer.</li> <li>● <b>Access:</b> used to connect the switch and the user terminal.</li> <li>● <b>Trunk:</b> used for interconnecting switches or connecting switches and routers, and can carry data frames of multiple different VLANs.</li> <li>● <b>QinQ:</b> This is an extended VLAN tagging technique where an additional VLAN tag is added, also known as “double tagging.” It allows Layer 2 tunneling and is often used by service providers to transport customer VLANs.</li> </ul>                                                                                                                                                                                                                                                                                                            |
| <b>PVID</b>              | Enter the default VLAN ID.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Accept Frame Type</b> | <p>Specifies which types of Ethernet frames are accepted by the port. Options vary depending on the selected <b>Link Type</b>:</p> <p><b>Hybrid:</b></p> <ul style="list-style-type: none"> <li>● <b>All:</b> Accept both tagged and untagged frames (default).</li> <li>● <b>Tag Only:</b> Accept only tagged VLAN frames; untagged packets will be dropped.</li> <li>● <b>Untag Only:</b> Accept only untagged frames; tagged frames will be dropped.</li> </ul> <p><b>Access:</b></p> <ul style="list-style-type: none"> <li>● <b>All:</b> Only this option is available. Untagged traffic is mapped to the configured PVID.</li> </ul> <p><b>Trunk:</b></p> <ul style="list-style-type: none"> <li>● <b>All:</b> Accept both tagged and untagged frames; untagged frames are assigned to the PVID (default behavior).</li> <li>● <b>Tag Only:</b> Accept only tagged frames; untagged traffic will be dropped (disables native VLAN).</li> </ul> |

|                          |                                                                                                                                                                                                                                                                                                                                                     |
|--------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                          | <p><b>QinQ:</b></p> <ul style="list-style-type: none"> <li>● <b>All:</b> Only this option is available due to double tagging structure.</li> </ul> <p><i><b>Note:</b> Setting Tag Only is the recommended method to <b>disable native VLAN</b> behavior on trunk and hybrid ports, providing better traffic control and increased security.</i></p> |
| <b>Ingress Filtering</b> | <p>Set whether to enable the inbound filtering function of the interface.</p> <p>Ingress Filtering is only available for Hybrid port, and it's enabled by default.</p> <p><i><b>Note:</b> Ingress filtering is a method used by enterprises and internet service providers (ISPs) to prevent suspicious traffic from entering a network.</i></p>    |
| <b>VLAN Translation</b>  | <p>Allows translating one VLAN ID to another at the port level. It's useful for scenarios where different parts of the network use different VLAN IDs but need to communicate with each other.</p>                                                                                                                                                  |
| <b>MAC VLAN</b>          | <p>Allows the switch to assign VLANs based on the MAC address of the incoming traffic. It can be used for more dynamic VLAN assignment, where devices can be automatically placed into specific VLANs based on their MAC addresses.</p>                                                                                                             |
| <b>Protocol VLAN</b>     | <p>Allows VLAN assignments based on the protocol type in the frame, such as IP or ARP. It enables grouping traffic from certain protocols into specific VLANs for easier network management.</p>                                                                                                                                                    |

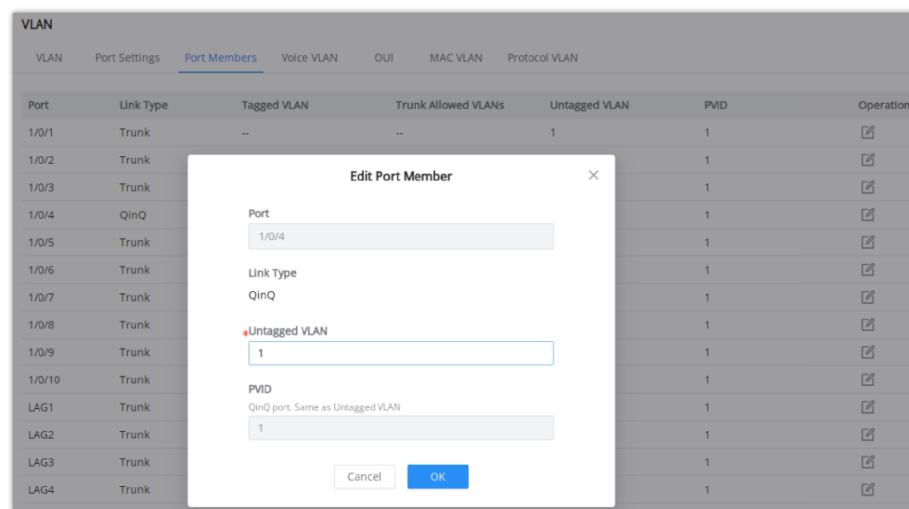
## VLAN Port Settings

### VLAN Port Members

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

#### Note

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



VLAN Port Members QinQ

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

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

VLAN Port Members Trunk

| VLAN  |               |              |                     |               |          |               |
|-------|---------------|--------------|---------------------|---------------|----------|---------------|
| 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 Port Settings Port Members **Voice VLAN** OUI MAC VLAN Protocol VLAN

Voice VLAN

•Voice VLAN ID

•CoS/802.1p Priority

CoS Remarking

•Aging Time (Min) 1440 Valid range is 30-65536

Tagged OUI

Disabled

Auto Voice VLAN

Tagged OUI

Untagged OUI

Valid range is 0-7

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 |           |

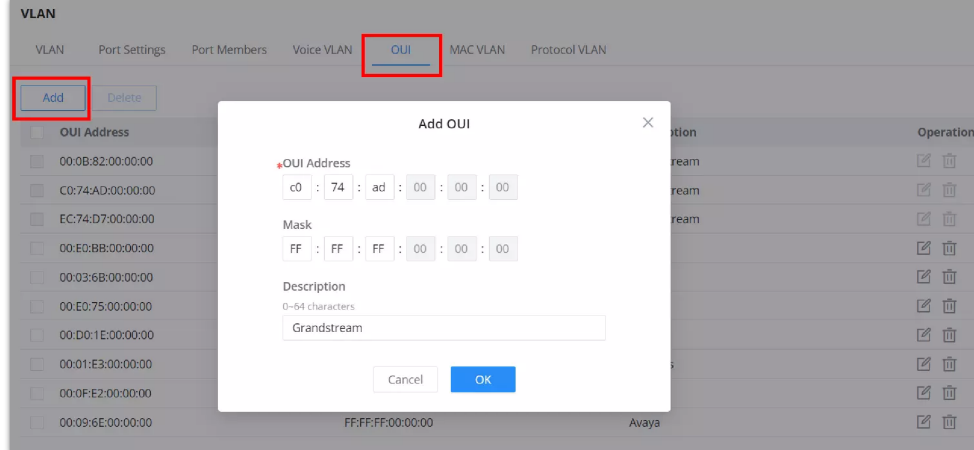
Voice VLAN

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

Voice VLAN

## OUI

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



VLAN OUI

## MAC VLAN

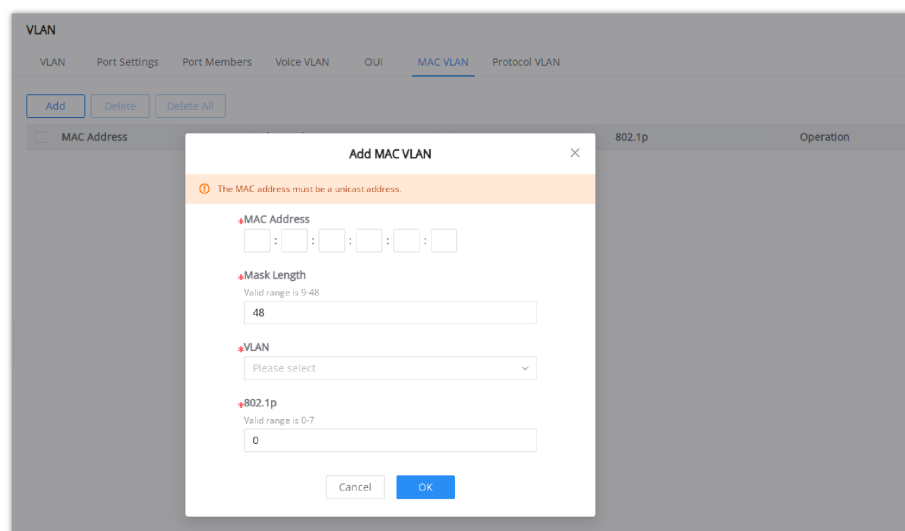
MAC VLAN is a networking technique where each VLAN is based on the source MAC address of incoming frames. Devices with the same MAC address share a VLAN. This segmentation enables isolated communication between devices within the same VLAN based on MAC addresses.

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).

### Note:

Only effective for Hybrid port.



VLAN MAC VLAN

## Protocol VLAN

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

### Note:

Only effective for Hybrid port.

**Add Protocol VLAN**

Protocol Index: 0

Frame Type: Ethernet II

Protocol Type Value:   
Valid range: 0x000-0xFFFF

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 Settings MST Instance MST Port Settings

Spanning Tree: ☒

Mode: RSTP

Ignore VLAN in BPDU: ☐

Path Cost:

Bridge Priority:

Max Hops: 20

Hello Time (s): 2

Max Aging Time (s): 20

Forward Delay Time (s): 15

Cancel OK

**Status**

|                |                         |
|----------------|-------------------------|
| Bridge ID      | 32768-C0:74:AD:B9:3C:A7 |
| Root Bridge ID | 0-00:00:00:00:00:00     |
| Root Port      | --                      |

Spanning Tree Global Settings

|                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Spanning Tree</b>          | Set whether to enable Spanning Tree.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Mode</b>                   | <p>Set the operating mode of Spanning Tree (STP).</p> <ul style="list-style-type: none"> <li>● <b>STP:</b> Standard Spanning Tree Protocol. Provides basic loop prevention but has slow convergence. Use only for compatibility with older or legacy network devices.</li> <li>● <b>RSTP:</b> Rapid Spanning Tree Protocol. Faster convergence than STP, suitable for most modern networks. Recommended as the default for typical deployments.</li> <li>● <b>MSTP:</b> 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.</li> <li>● <b>PVST+:</b> 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.</li> <li>● <b>RPVST(+):</b> 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.</li> </ul> |
| <b>Ignore VLAN in BPDU</b>    | 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.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Path Cost</b>              | Specify the path cost method (Short, Long, or Legacy). <i>Default is Short.</i>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Bridge Priority</b>        | <p>Select the Bridge Priority, In an STP network, the device with the smallest bridge ID is elected as the root bridge.</p> <p><i>Default is 32768.</i></p> <p><b>Note:</b> The valid range is 0~61440, which must be a multiple of 4096</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Max Hops</b>               | Select the Max Hops (the range is 1 – 40). <i>Default is 20</i>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Hello Time (s)</b>         | <p>Specify the Hello Time in seconds (the range is 1 -10). <i>Default is 2.</i></p> <p><b>Note:</b> 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.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Max Aging Time (s)</b>     | Select The aging time of BPDU packets of the port (the range is 6 – 40). <i>Default is 20.</i>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Forward Delay Time (s)</b> | Specify the Forward Delay Time in seconds (the range is 4 -30). <i>Default is 15.</i>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

## STP Global Settings

## STP Port Settings

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

Spanning Tree

Global SettingsPort SettingsMST InstanceMST Port Settings

Edit

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

### Spanning Tree Port Settings

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

The screenshot shows the 'Edit Port' configuration window for Spanning Tree. The settings are as follows:

- Port:** 1/0/1
- Enable Spanning Tree:** Enabled (toggle switch)
- Priority:** 128 (text input; note: Enter a value between 0-240 that is a multiple of 16)
- Path Cost:** 0 (text input; note: Valid range is 0-65535)
- Edge Port:** Auto (radio button selected; other options: Enabled, Disabled)
- Root Protection:** Disabled (toggle switch)
- Loop Protection:** Enabled (toggle switch)
- BPDU Guard:** Disabled (toggle switch)
- BPDU Filter:** Disabled (toggle switch)
- Point-to-Point:** Auto (radio button selected; other options: Enabled, Disabled)

Buttons at the bottom: Cancel, OK.

Spanning Tree Edit Port Settings

|                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Port</b>            | Displays the selected GE/LAG Port.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Enable STP</b>      | Set whether to enable STP on this port.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Priority</b>        | <p>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 .</p> <p><b>Note:</b> The valid range is 0~240, which must be a multiple of 16</p>                                                                                                                                                |
| <b>Path Cost</b>       | <p>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.</p> <p><b>Note:</b>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 0-2000000000; if set to “legacy”, the valid range is 0-200000.</p>                                                                                                                           |
| <b>Edge Port</b>       | <p>Set whether to enable Edge Port or disable it, by default it’s on auto.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>• A port is considered as an edge port when it is directly connected to the user terminal or server, instead of any other switches or shared network segments. The edge port will not cause a loop upon network topology changes.</li> <li>• In the edge mode, the interface would be put into the Forwarding state immediately upon link up. While in auto mode it will detect if the port is an edge or not.</li> </ul> |
| <b>Root Protection</b> | 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.                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Loop Protection</b> | Prevents Layer 2 loops by ensuring a blocking state on ports that stop receiving BPDUs, avoiding the formation of network loops.                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>BPDU Guard</b>      | <p>Set whether to enable BPDU Guard.</p> <p><b>Note:</b> BPDU Guard further protects your switch by turning this port into error state and shutdown if any BPDU received from this port.</p>                                                                                                                                                                                                                                                                                                                                                                         |
| <b>BPDU Filter</b>     | <p>Set whether to enable BPDU Filter.</p> <p><b>Note:</b> Drop all BPDU packets and no BPDU will be sent.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Point-to-Point</b>  | <p>Select Point-to-Point option (Auto, Enabled or Disabled). <i>Default is Auto.</i></p> <p><b>Note:</b> determines the STP of link type for this port automatically if set to Auto.</p>                                                                                                                                                                                                                                                                                                                                                                             |

## 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 SettingsPort SettingsMST InstanceMST Port Settings

Region Name

C0:74:AD:

1-32 alphanumeric characters and special characters ~,~

Revision Level

0

Valid range is 0-65535

CancelOK

| MSTI | VLAN   | Priority | Bridge Identifier       | Designated Root Bridge  | Root Port | Root Path Cost | Remaining Hop | 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

MST Instance > Edit MST Instance

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

CancelOK

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 SettingsPort SettingsMST InstanceMST Port Settings

MSTI

0

Port Settings

EditRefresh

| Port                                      | Path Cost | Priority | Role          | Status     | Mode | Type     | Designated Bridge ID | Operation |
|-------------------------------------------|-----------|----------|---------------|------------|------|----------|----------------------|-----------|
| <input checked="" type="checkbox"/> 1/0/1 | 4         | 128      | Disabled Port | Disabled   | STP  | Boundary | 0-00:00:00:00:00:00  |           |
| <input checked="" type="checkbox"/> 1/0/2 | 4         | 128      | Disabled Port | Forwarding | STP  | Boundary | 61440-C0:74:AD:      |           |
| <input type="checkbox"/> 1/0/3            | 4         | 128      | Disabled Port | Disabled   | STP  | Boundary | 0-00:00:00:00:00:00  |           |
| <input type="checkbox"/> 1/0/4            | 4         | 128      | Disabled Port | Disabled   | STP  | Boundary | 0-00:00:00:00:00:00  |           |
| <input type="checkbox"/> 1/0/5            | 4         | 128      | Disabled Port | Disabled   | STP  | Boundary | 0-00:00:00:00:00:00  |           |
| <input type="checkbox"/> 1/0/6            | 4         | 128      | Disabled Port | Disabled   | STP  | Boundary | 0-00:00:00:00:00:00  |           |
| <input type="checkbox"/> 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.

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

|           |       |                                                      |
|-----------|-------|------------------------------------------------------|
| 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 <b>VLAN Settings</b> 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:

|                               |                                                                                                                                                                                                                                                        |
|-------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>VLAN</b>                   | Displays the VLAN on which the PVST rule will PVST protocol will be applied                                                                                                                                                                            |
| <b>Enable PVST</b>            | Enables/disables PVST per VLAN                                                                                                                                                                                                                         |
| <b>Bridge Priority</b>        | Defines the bridge priority for the VLAN, valid range is 0-61440, default value is 32768.<br><b>Note:</b> All values should be a multiple of 4096                                                                                                      |
| <b>Hello Time (s)</b>         | Specify the Hello Time in seconds (the range is 1 -10). Default is 2.<br>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. |
| <b>Max Aging Time (s)</b>     | Select The aging time of BPDU packets of the port (the range is 6 – 40). Default is 20.                                                                                                                                                                |
| <b>Forward Delay Time (s)</b> | 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 Settings Port Settings VLAN Settings PVST Port Settings

VLAN 1

Port Settings

Edit Refresh

| <input type="checkbox"/> Port   | Path Cost | Priority | Role            | Status     | Designated Bridge ID    | Designated Port ID | Designated Path Cost | Operation |
|---------------------------------|-----------|----------|-----------------|------------|-------------------------|--------------------|----------------------|-----------|
| <input type="checkbox"/> 1/0/1  | 65535     | 128      | Disabled Port   | Disabled   | 0-00:00:00:00:00:00     | 0-0                | 65535                |           |
| <input type="checkbox"/> 1/0/2  | 65535     | 128      | Disabled Port   | Disabled   | 0-00:00:00:00:00:00     | 0-0                | 65535                |           |
| <input type="checkbox"/> 1/0/3  | 65535     | 128      | Disabled Port   | Disabled   | 0-00:00:00:00:00:00     | 0-0                | 65535                |           |
| <input type="checkbox"/> 1/0/4  | 65535     | 128      | Disabled Port   | Disabled   | 0-00:00:00:00:00:00     | 0-0                | 65535                |           |
| <input type="checkbox"/> 1/0/5  | 65535     | 128      | Disabled Port   | Disabled   | 0-00:00:00:00:00:00     | 0-0                | 65535                |           |
| <input type="checkbox"/> 1/0/6  | 65535     | 128      | Disabled Port   | Disabled   | 0-00:00:00:00:00:00     | 0-0                | 65535                |           |
| <input type="checkbox"/> 1/0/7  | 18        | 128      | Designated Port | Forwarding | 32769-EC:74:D7:3D:90:A4 | 128-7              | 18                   |           |
| <input type="checkbox"/> 1/0/8  | 65535     | 128      | Disabled Port   | Disabled   | 0-00:00:00:00:00:00     | 0-0                | 65535                |           |
| <input type="checkbox"/> 1/0/9  | 65535     | 128      | Disabled Port   | Disabled   | 0-00:00:00:00:00:00     | 0-0                | 65535                |           |
| <input type="checkbox"/> 1/0/10 | 65535     | 128      | Disabled Port   | Disabled   | 0-00:00:00:00:00:00     | 0-0                | 65535                |           |
| <input type="checkbox"/> 1/0/11 | 65535     | 128      | Disabled Port   | Disabled   | 0-00:00:00:00:00:00     | 0-0                | 65535                |           |
| <input type="checkbox"/> 1/0/12 | 65535     | 128      | Disabled Port   | Disabled   | 0-00:00:00:00:00:00     | 0-0                | 65535                |           |
| <input type="checkbox"/> 1/0/13 | 65535     | 128      | Disabled Port   | Disabled   | 0-00:00:00:00:00:00     | 0-0                | 65535                |           |
| <input type="checkbox"/> 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.<br><b>Note:</b> 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. |

# IP

## VLAN IP Interface

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

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

## IPv4/IPv6 Interface

To add an IP Interface, please click on 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

| <input type="checkbox"/> IPv4 Interface | Status | Type    | IPv4 Address      | MTU  | Operation |
|-----------------------------------------|--------|---------|-------------------|------|-----------|
| <input type="checkbox"/> Loopback1      | UP     | Static  | --                | 1500 |           |
| <input type="checkbox"/> * 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*

**Note:**

Gateway Usage Priority:

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

## IPv6 Router Advertisements

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

| VLAN IP Interface |                  |                   |             |                            |      |        |                                                                                       |
|-------------------|------------------|-------------------|-------------|----------------------------|------|--------|---------------------------------------------------------------------------------------|
| IPv4 Interface    |                  | IPv6 Interface    |             | IPv6 Router Advertisements |      |        |                                                                                       |
| IPv6 Interface    | Interface Enable | Route Information | Timeout (s) | Lifetime (s)               | Flag | Number | Operation                                                                             |
| * VLAN 1          | Disabled         | Disabled          | 600         | 1800                       | --   | 0      |  |
| VLAN 7            | Disabled         | Disabled          | 600         | 1800                       | --   | 0      |  |
| VLAN 9            | Disabled         | Disabled          | 600         | 1800                       | --   | 0      |  |

*IPv6 Router Advertisement*

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

IPv6 Router Advertisements > **Edit IPv6 Router Advertisements**

VLAN:

Interface Enable: ☐

Route Information: ☐

Timeout (s):  Valid range is 1-1800

Lifetime (s):  Valid range is 0-9000

Flag: ☐ M Flag ☐ O Flag

Default Route Priority:

---

**IPv6 Address/Prefix1**

IPv6 Address/Prefix:  /  Prefix range is 1-128

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

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

Flag: ☒ A Flag ☐ L Flag ☐ R Flag

[Add](#)

*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.

**VLAN IP Interface**

IPv4 Interface IPv6 Interface IPv6 Router Advertisements **MGMT VLAN**

MGMT VLAN:

**IPv4 Address Settings**

Address Type: ☒ Static IP ☐ DHCP

IP Address:  IPv4 format

Mask: ☐ Subnet Mask ☒ Mask Length

Mask Length:  Valid range is 8-30

Static Gateway:  IPv4 format

**IPv6 Address Settings**

Enable: ☐

| Management Address |               |
|--------------------|---------------|
| MGMT VLAN          | VLAN 2        |
| Status             | DOWN          |
| IPv4               |               |
| Address Type       | Static        |
| IP Address         | 192.168.2.100 |
| Mask Length        | 24            |

*MGMT VLAN*

## DHCP Server

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

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

**Step 1:** Enable the DHCP Server.

**DHCP Server** | Address Table

DHCP Service ☒

**Address Pool Settings** ⓘ

All

| <input type="checkbox"/> | Address Pool Name | Type      | VLAN IPv4 Interface | Address Pool        | Used | Remained | Operation                                                                 |
|--------------------------|-------------------|-----------|---------------------|---------------------|------|----------|---------------------------------------------------------------------------|
| <input type="checkbox"/> | Guest network     | Interface | VLAN 9              | 90.0.0.2-90.0.0.254 | 0    | 253      | <input type="button" value="Edit"/> <input type="button" value="Delete"/> |
| <input type="checkbox"/> | 7                 | Interface | VLAN 7              | 70.0.0.7-70.0.0.77  | 1    | 70       | <input type="button" value="Edit"/> <input type="button" value="Delete"/> |

*DHCP Global Settings*

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

**Note:**

- The global address pool is only used for IP address allocation to the DHCP relay.
- When a VLAN is configured to use DHCP to automatically get an IP address, the system can now prioritize which **gateway** (the device routing traffic to other networks) to use.

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

DHCP Server > Add Address Pool

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

Type: Interface

Interface: VLAN 7

IPv4 Pool: 70.0.0.2 - 70.0.0.254

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

DNS Server: 1.1.1.1

WINS Server:

Netbios Node Type:

**DHCP Option1**

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

Type: Hex

Option Content:  (0-255 characters, and must be even)

*DHCP Add 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): 120 (Valid range is 1-2880)

DNS Server:

WINS Server:

Netbios Node Type:

**DHCP Option1**

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

Type: ASCII

Service: Custom

Option Content:  (0-255 characters)

*DHCP Server Add Pool 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...

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

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

Pollling

TTL

4

Valid range is 1-16.

Cancel

OK

DHCP Server

Add

Delete

| <input type="checkbox"/> | Interface | DHCP Server | Operation |
|--------------------------|-----------|-------------|-----------|
| <input type="checkbox"/> | VLAN 7    | 192.168.7.1 |           |

Total 1

<1>

10 / page

DHCP Relay

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

DHCP Relay

ARP Table

The ARP Table page provides tools to view and manage IP-to-MAC address mappings on the switch. It is divided into two tabs:

- **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**.

| IP Address                               | MAC Address       | VLAN Interface | Interface | Type    | Expiration (s) | Operation            |
|------------------------------------------|-------------------|----------------|-----------|---------|----------------|----------------------|
| <input type="checkbox"/> 169.254.100.1   | c0:74:78:11:00:90 | VLAN 100       | 1/0/10    | Dynamic | 1149           | <a href="#">Link</a> |
| <input type="checkbox"/> 169.254.100.4   | c0:74:ad:d8:f3:f8 | VLAN 100       | 1/0/10    | Dynamic | 899            | <a href="#">Link</a> |
| <input type="checkbox"/> 169.254.100.3   | c0:74:ad:cc:de:8c | VLAN 100       | 1/0/10    | Dynamic | 353            | <a href="#">Link</a> |
| <input type="checkbox"/> 169.254.100.2   | c0:74:ad:b9:3b:dc | VLAN 100       | 1/0/10    | Dynamic | 1155           | <a href="#">Link</a> |
| <input type="checkbox"/> 192.168.180.176 | c0:74:ad:cc:de:8c | VLAN 180       | --        | Dynamic | 679            | <a href="#">Link</a> |
| <input type="checkbox"/> 192.168.180.100 | c0:74:ad:b9:3b:dc | VLAN 180       | 1/0/10    | Dynamic | 1063           | <a href="#">Link</a> |
| <input type="checkbox"/> 192.168.180.35  | c0:74:ad:d8:f3:f8 | VLAN 180       | 1/0/10    | Dynamic | 671            | <a href="#">Link</a> |
| <input type="checkbox"/> 192.168.180.2   | c0:74:78:11:00:90 | VLAN 180       | --        | Dynamic | 314            | <a href="#">Link</a> |
| <input type="checkbox"/> 192.168.180.1   | ec:74:d7:5d:a8:52 | VLAN 180       | 1/0/10    | Dynamic | 1190           | <a href="#">Link</a> |
| <input type="checkbox"/> 172.16.143.30   | c0:74:ad:b9:3b:79 | VLAN 1720      | 1/0/10    | Dynamic | 321            | <a href="#">Link</a> |

ARP Table

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

| IP Address                               | MAC Address       | VLAN Interface | Interface | Type    | Expiration (s) | Operation            |
|------------------------------------------|-------------------|----------------|-----------|---------|----------------|----------------------|
| <input type="checkbox"/> 169.254.100.1   | c0:74:78:11:00:90 | VLAN 100       | 1/0/10    | Dynamic | 1149           | <a href="#">Link</a> |
| <input type="checkbox"/> 169.254.100.4   | c0:74:ad:d8:f3:f8 | VLAN 100       | 1/0/10    | Dynamic | 899            | <a href="#">Link</a> |
| <input type="checkbox"/> 169.254.100.3   | c0:74:ad:cc:de:8c | VLAN 100       | 1/0/10    | Dynamic | 353            | <a href="#">Link</a> |
| <input type="checkbox"/> 169.254.100.2   | c0:74:ad:b9:3b:dc | VLAN 100       | 1/0/10    | Dynamic | 1155           | <a href="#">Link</a> |
| <input type="checkbox"/> 192.168.180.176 | c0:74:ad:cc:de:8c | VLAN 180       | --        | Dynamic | 679            | <a href="#">Link</a> |
| <input type="checkbox"/> 192.168.180.100 | c0:74:ad:b9:3b:dc | VLAN 180       | 1/0/10    | Dynamic | 1063           | <a href="#">Link</a> |
| <input type="checkbox"/> 192.168.180.35  | c0:74:ad:d8:f3:f8 | VLAN 180       | 1/0/10    | Dynamic | 671            | <a href="#">Link</a> |
| <input type="checkbox"/> 192.168.180.2   | c0:74:78:11:00:90 | VLAN 180       | --        | Dynamic | 314            | <a href="#">Link</a> |
| <input type="checkbox"/> 192.168.180.1   | ec:74:d7:5d:a8:52 | VLAN 180       | 1/0/10    | Dynamic | 1190           | <a href="#">Link</a> |
| <input type="checkbox"/> 172.16.143.30   | c0:74:ad:b9:3b:79 | VLAN 1720      | 1/0/10    | Dynamic | 321            | <a href="#">Link</a> |

ARP Table Operation

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

## Static ARP

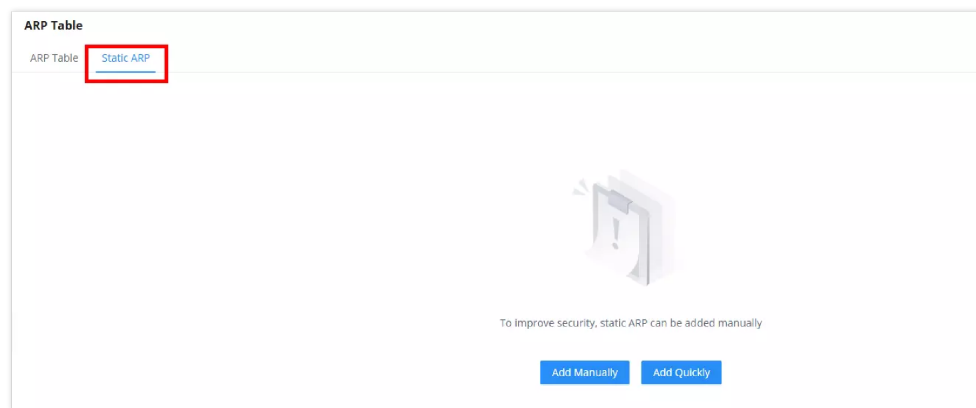
The **Static ARP** tab allows administrators to manually configure fixed IP-to-MAC address mappings. These entries do not expire and cannot be overwritten by dynamic ARP learning, making them ideal for securing communication with critical network devices.

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.



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

IPv6 address 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

Add as Static Neighbor

All Types

All (Router)

Q: VLAN/IPv6 Address/MAC Ad...

| IPv6 Address                                       | MAC Address       | VLAN Interface | Interface | Type    | Expiration (s) | Router | Status    | Operation |
|----------------------------------------------------|-------------------|----------------|-----------|---------|----------------|--------|-----------|-----------|
| <input type="checkbox"/> fe80::c274:adff:fed8:f3f8 | c0:74:ad:d8:f3:f8 | VLAN 1720      | 1/0/10    | Dynamic | 1104           | Yes    | Reachable |           |

Total 1

<

1

>

10 / page

Neighbor Discovery

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

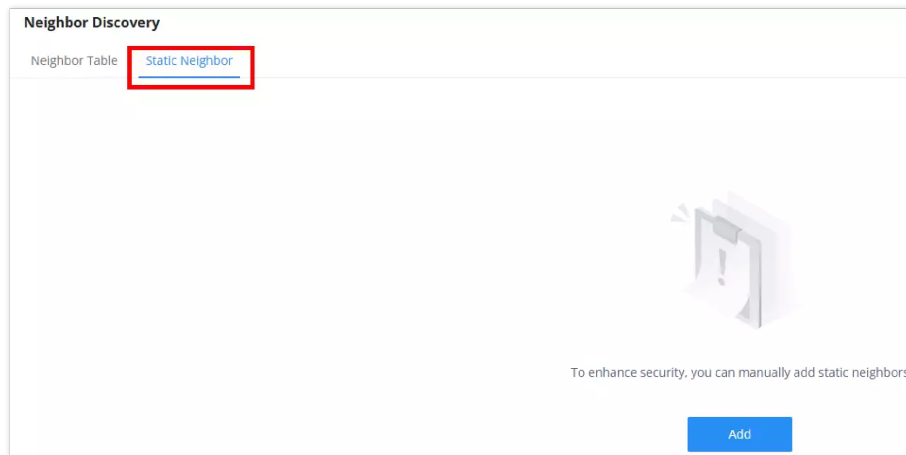
### Note:

Aging time applies only to dynamic entries.

Click on 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:



Add Static Neighbor

The screenshot shows the 'Add Static Neighbor' dialog box. It has a title bar with a close button. Below the title bar is an orange warning banner that says 'The MAC address must be an unicast one.' The form contains three fields: a dropdown menu for 'VLAN' with the value '7', a text input for 'IPv6 Address' with the value 'e90d:f398:767d:b89f:a88e:0e6e:319d:af15', and a text input for 'MAC Address' with the value 'c0 : 74 : ad : 11 : 22 : 33'. At the bottom, there are 'Cancel' and 'OK' buttons.

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.

## 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  -  - 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.

**Note:**

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

## Domain Mapping Table

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

**DNS**

Global Settings **Domain Mapping Table**

| <input type="checkbox"/> | Hostname        | IP Address      | Type    | Expiration (s) | Operation |
|--------------------------|-----------------|-----------------|---------|----------------|-----------|
| <input type="checkbox"/> | grandstream.com | 173.254.235.74  | Static  | --             |           |
| <input type="checkbox"/> | pool.ntp.org    | 196.200.131.160 | Dynamic | 16             |           |

Total 2  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 .\_-

\*IP Address

*Add Static Domain*

**Note:**

Up to 32 static domain names can be added.

The user can also select the dynamic domains and then click on 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.

**Note:**

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

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

| <input checked="" type="checkbox"/> | VLAN | Status   | Querier  | Querier Version | Router Port Auto-Learning | Port Fast Leave | Query Robustness | Query Interval | Operation |
|-------------------------------------|------|----------|----------|-----------------|---------------------------|-----------------|------------------|----------------|-----------|
| <input checked="" type="checkbox"/> | 1    | Disabled | Disabled | IGMPv2          | Enabled                   | Disabled        | 2                | 125            |           |
| <input checked="" type="checkbox"/> | 7    | Disabled | Disabled | IGMPv2          | Enabled                   | Disabled        | 2                | 125            |           |

IGMP Snooping Global Settings

|                          |                                                                                                                                                                                                                                                                                                                    |
|--------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Unknown Multicast Packet | <div>Select an action for switch to handle with unknown multicast packet.</div> <div><div><div>Drop:</div>Drop the unknown multicast data.</div><div><div>Flood:</div>Flood the unknown multicast data.</div><div><div>Forward to Router port:</div>Forward the unknown multicast data to router port.</div></div> |
|--------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

IGMP Snooping Global Settings

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

Global Settings > **Edit**

|                                                                         |                                     |                          |
|-------------------------------------------------------------------------|-------------------------------------|--------------------------|
| VLAN                                                                    | 1                                   |                          |
| IGMP Snooping                                                           | <input checked="" type="checkbox"/> |                          |
| IGMP Snooping Querier                                                   | <input type="checkbox"/>            |                          |
| Router Port Auto-Learning                                               | <input checked="" type="checkbox"/> |                          |
| Port Fast Leave                                                         | <input type="checkbox"/>            |                          |
| *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.     |
| <input type="button" value="Cancel"/> <input type="button" value="OK"/> |                                     |                          |

### IGMP Snooping Edit VLAN

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

### IGMP Snooping Edit VLAN

## IGMP Snooping Router Port

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

**IGMP Snooping**

Global Settings Querier Router Port Multicast Address Multicast Policy Multicast Port

Add Refresh Delete

| <input type="checkbox"/> VLAN | Static Router Port | Forbidden Port | Dynamic Port | Aging Time (s) | Operation |
|-------------------------------|--------------------|----------------|--------------|----------------|-----------|
| <input type="checkbox"/> 1    | 1/0/24             | --             | --           | --             |           |

Total 1 < 1 > 10 / page

IGMP Snooping Router Port

Router Port > Edit

VLAN 8

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

Add Refresh Delete

Q VLAN/Multicast Address/Member Port

| <input type="checkbox"/> 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.

The screenshot shows the 'IGMP Snooping' configuration page with the 'Multicast Policy' tab selected. An 'Add' button is highlighted with a red arrow. An 'Edit' dialog box is open, showing fields for Multicast Policy ID (1), Action (Allow), and Multicast Address (224.12.1.3 to 230.12.1.13).

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.

The screenshot shows the 'IGMP Snooping' configuration page with the 'Multicast Port' tab selected. An 'Edit' dialog box is open, showing fields for Port (1/0/1), Max Multicast Group Count (256), Action (Reject), Multicast Policy (checked), and Multicast Policy ID (1).

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.

The Global Settings page gives the user the ability to enable MLD Snooping as well as select Multicast Forward Mode, etc.

The screenshot shows the 'MLD Snooping' configuration page with the 'Global Settings' tab selected. The 'Unknown Multicast Packet' is set to Flood. MLD Snooping is enabled. Multicast Forward Mode is set to MAC-Based. MLD Version is set to MLDv1. Report Suppression is disabled. A green box highlights the MLD Snooping settings.



### MLD Snooping Global Settings

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

### MLD Snooping Global Settings

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

Global Settings > **Edit**

VLAN

1

MLD Snooping

☒

MLD Snooping Querier

☒

MLD Snooping Querier Version

MLDv2

Router Port Auto-Learning

☒

Port Fast Leave

☒

Query Robustness

2

The range is 1-7.

Query Interval (s)

125

The range is 30-18000.

Query Max Response Interval (s)

10

The range is 5-20.

Last Member Query Count

2

The range is 1-7.

Last Member Query Interval (s)

1

The range is 1-25.

Cancel

Save

### MLD Snooping Edit VLAN

|                                     |                                                                                                                                                                                                                                                |
|-------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>VLAN</b>                         | Displays the selected VLAN                                                                                                                                                                                                                     |
| <b>MLD Snooping</b>                 | Click on the toggle button to enable MLD Snooping for the selected VLAN.                                                                                                                                                                       |
| <b>MLD Snooping Querier</b>         | Click the toggle button to enable the MLD Snooping Querier.                                                                                                                                                                                    |
| <b>MLD Snooping Querier Version</b> | Select from the drop-down list the MLD Snooping Querier Version.                                                                                                                                                                               |
| <b>Router Port Auto-Learning</b>    | Click on the toggle button to learn router port by MLD query.                                                                                                                                                                                  |
| <b>Port Fast Leave</b>              | <p>Select Enable/Disable Fast Leave feature for the desired port.</p> <p><i><b>Note:</b> If Fast Leave is enabled for a port, the switch will immediately remove this port from the multicast group upon receiving MLD leave messages.</i></p> |
| <b>Query Robustness</b>             | Set a number which allows tuning for the expected packet loss on a subnet.                                                                                                                                                                     |

|                                        |                                                                                                                                                                                                             |
|----------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                        | <i>The valid range is 1-7</i>                                                                                                                                                                               |
| <b>Query Interval (s)</b>              | Set the interval of querier send general query.                                                                                                                                                             |
| <b>Query Max Response Interval (s)</b> | It specifies the maximum allowed time before sending a responding report.<br><i>Note: The valid range is 5-20 in seconds.</i>                                                                               |
| <b>Last Member Query Count</b>         | After quering 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).<br><i>Note: The valid range is 1-7</i> |
| <b>Last Member Query Interval (s)</b>  | Set The maximum time interval between counting each member query message with no responses from any subscribed member.<br><i>Note: The valid range is 1-25 in seconds</i>                                   |

#### MLD Snooping – Edit VLAN

## MLD Snooping Router Port

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

**MLD Snooping**

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

| <input type="checkbox"/> VLAN | Static Router Port | Forbidden Port | Dynamic Port | Aging Time (s) | Operation                                                                 |
|-------------------------------|--------------------|----------------|--------------|----------------|---------------------------------------------------------------------------|
| <input type="checkbox"/> 1    | 1/0/1              | --             | --           | --             | <input type="button" value="Edit"/> <input type="button" value="Delete"/> |

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: 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

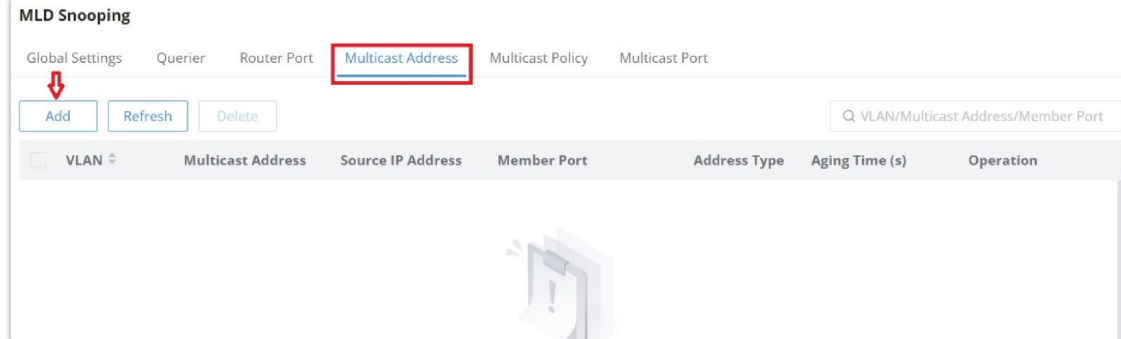
**Forbidden Port**  
Click on port to select/unselect

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 SFP+ 26 SFP+ 27 SFP+ 28 SFP+

#### 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 Multicast Address page

Add MLD Snooping Multicast Address

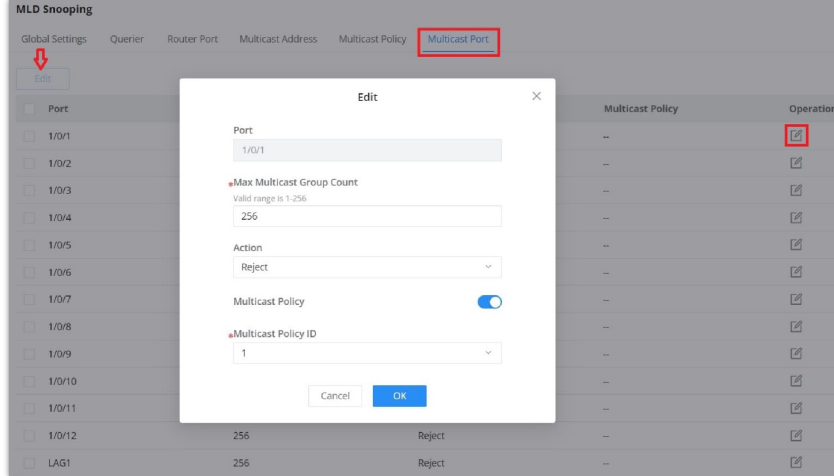
## MLD Snooping Multicast Policy

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

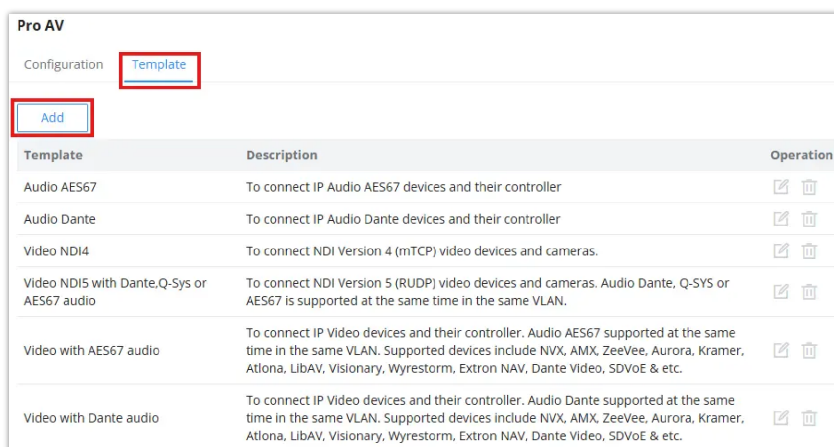
In the Web UI, navigate to **AV Control** → **Pro AV**. The Pro AV page includes two tabs: **Configuration** and **Template**.

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

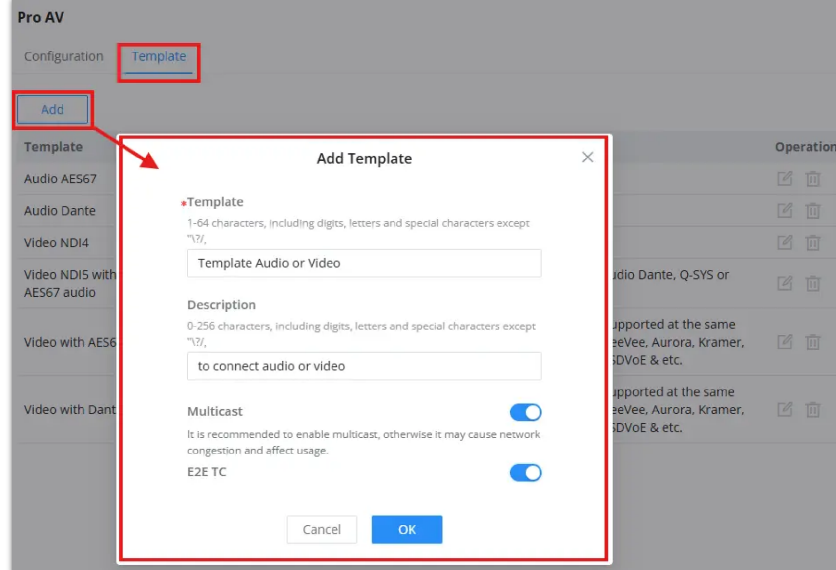
Open the **Template** tab to view the built-in AV templates and any custom templates you create.



Pro AV 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.



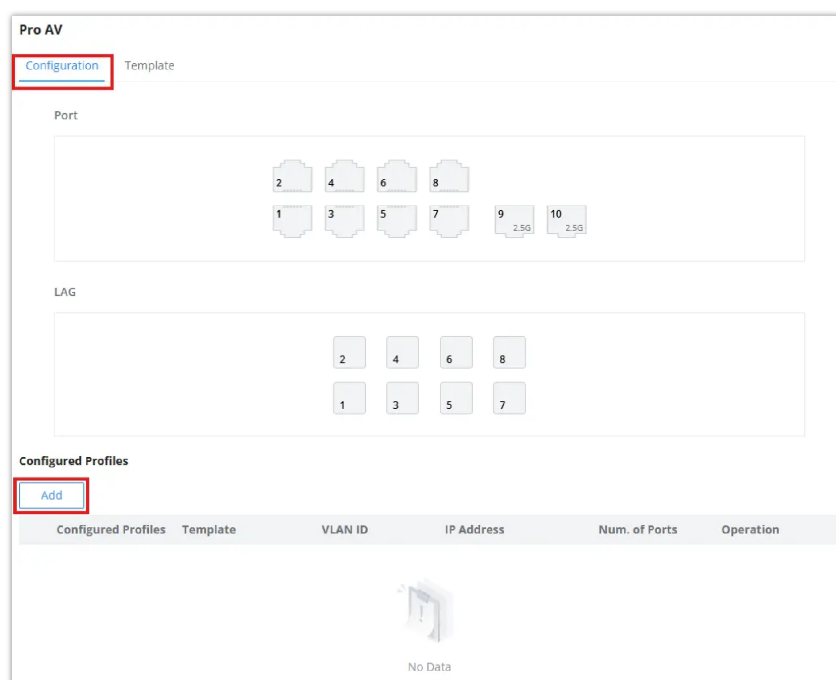
Add a Template

| Field              | Description                                                                                                                                                       |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Template</b>    | Enter a name for the template. This name will appear in the template list and in the Template selection list when creating configured profiles.                   |
| <b>Description</b> | Enter a brief description to identify the intended AV use case.                                                                                                   |
| <b>Multicast</b>   | Enables multicast support for the template. Enable this option when multicast discovery or multicast streams are expected in the AV deployment.                   |
| <b>E2E TC</b>      | 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

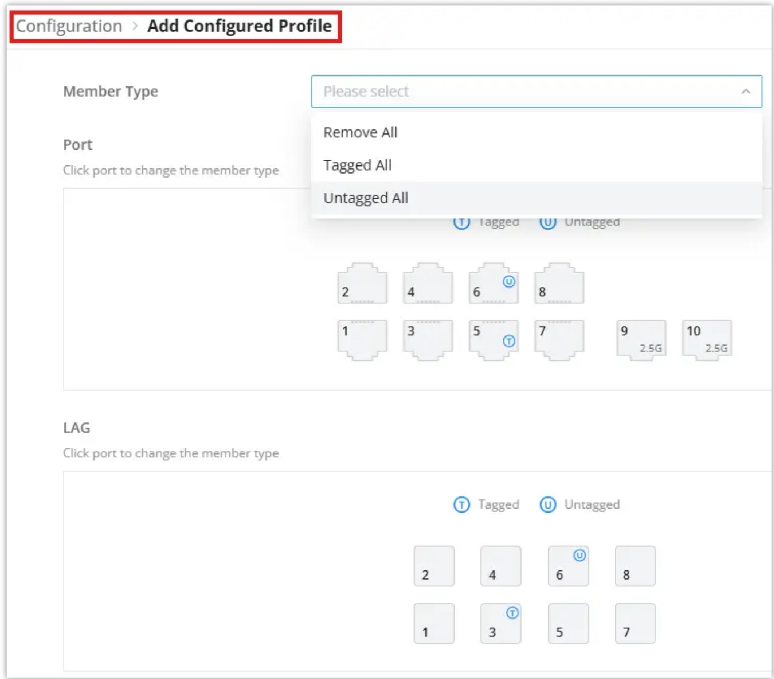
Open the **Configuration** tab to create, apply, and manage configured profiles. This page provides a visual map of **ports** and **LAGs** and a table listing existing profiles.



Pro AV Configuration 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.



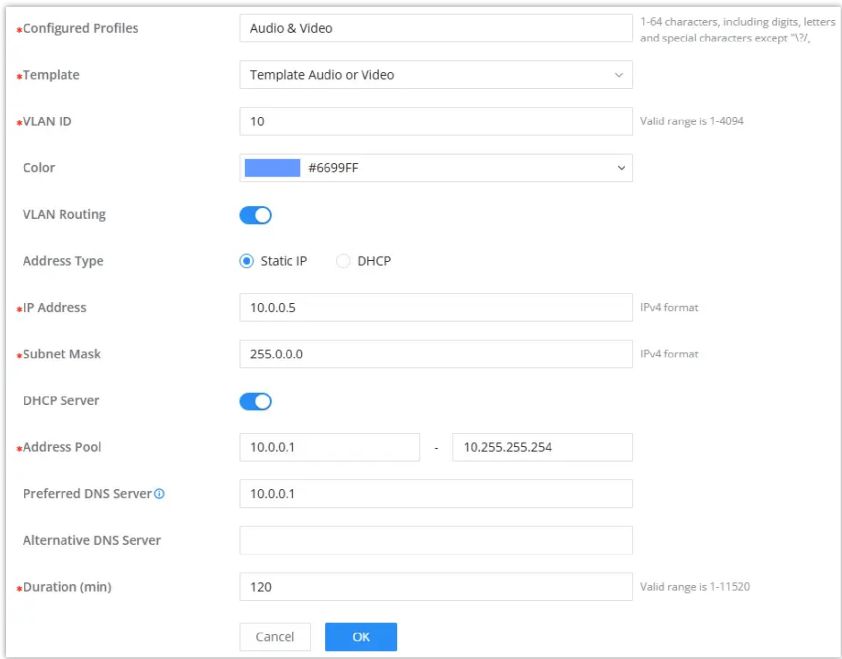
Pro AV Profile Selecting members

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.



Pro AV configure the profile settings

| Field | Description |
|-------|-------------|
|-------|-------------|

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

*Pro AV – configure the profile settings*

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

2 4 6 8  
1 3 5 7 9 10

LAG

2 4 6 8  
1 3 5 7

**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**.

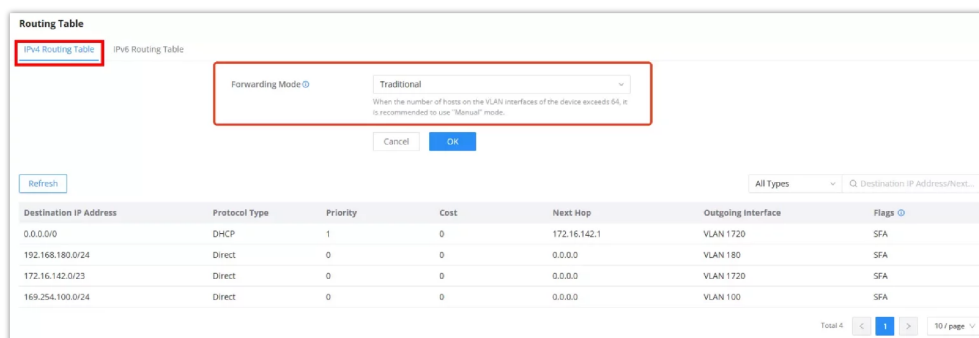
- **Traditional** → automatic ARP/neighbor learning for routing between VLANs.
- **Manual** → disables that automation; forwarding depends only on static routes and static ARP entries.

### 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

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

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

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

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

| Static Routes                       |                        |                                  |          |             |                    |                                                                                                                                                                             |
|-------------------------------------|------------------------|----------------------------------|----------|-------------|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| IPv4 Static Routes                  |                        | IPv6 Static Routes               |          |             |                    |                                                                                                                                                                             |
| Add Delete                          |                        | Q Destination IP Address/Next... |          |             |                    |                                                                                                                                                                             |
| <input checked="" type="checkbox"/> | Destination IP Address | Mask Length                      | Priority | Next Hop    | Outgoing Interface | Operation                                                                                                                                                                   |
| <input checked="" type="checkbox"/> | 192.168.7.0            | 24                               | 2        | --          | VLAN 1             |   |
| <input type="checkbox"/>            | 192.168.7.0            | 24                               | 1        | 192.168.8.0 | --                 |   |
| <input type="checkbox"/>            | 192.168.80.0           | 24                               | 1        | 192.168.7.0 | --                 |   |

Static Routes

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

Please refer to the figure below:

### Add IPv4 Static Route

\*Destination IP Address

\*Mask Length

Valid range is 0-32.

Gateway

☐ Next Hop
 ☒ Outgoing Interface

\*Outgoing Interface

\*Priority

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

Cancel

OK

Add a static route

# POE

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

Usually, the terminal devices of the access point need to use 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 the Power Supply Info like the number of PoE, Total and Remaining PoE Power, etc, and even the Supply Voltage.

| 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)      Valid range is 0-119

*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

| <input checked="" type="checkbox"/> | Interface | Power Status | Power Supply Standard | Power Mode | Power Supply Priority | Operation                                                                           |
|-------------------------------------|-----------|--------------|-----------------------|------------|-----------------------|-------------------------------------------------------------------------------------|
| <input checked="" type="checkbox"/> | 1/0/1     | Unpowered    | 802.3at               | Auto       | Low                   |  |
| <input type="checkbox"/>            | 1/0/2     | Unpowered    | 802.3at               | Auto       | Low                   |  |
| <input type="checkbox"/>            | 1/0/3     | Unpowered    | 802.3at               | Auto       | Low                   |  |
| <input type="checkbox"/>            | 1/0/4     | Unpowered    | 802.3at               | Auto       | Low                   |  |
| <input type="checkbox"/>            | 1/0/5     | Unpowered    | 802.3at               | Auto       | Low                   |  |
| <input type="checkbox"/>            | 1/0/6     | Unpowered    | 802.3at               | Auto       | Low                   |  |
| <input type="checkbox"/>            | 1/0/7     | Unpowered    | 802.3at               | Auto       | Low                   |  |
| <input type="checkbox"/>            | 1/0/8     | Unpowered    | 802.3at               | Auto       | Low                   |  |

Total 8 < 1 > 10 / page

PoE Interface page

Interface > Edit

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

QoS Port Priority

Then the user can click on 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               | <p>Select the QoS operation mode:</p> <ul style="list-style-type: none"> <li>● <b>None:</b> no packet priority is trusted, and the interface default priority is used.</li> <li>● <b>CoS:</b> Traffic is mapped to queues based on the CoS Queue Mapping, it can configured in QoS → Priority Mapping → CoS Mapping page.</li> <li>● <b>DSCP:</b> All IP traffic is mapped to queues based on the DSCP field in the IP header. If the traffic is not IP traffic, it is mapped to the lowest priority queue.</li> <li>● <b>CoS-DSCP:</b> All IP traffic is mapped to queues based on the DSCP field in the IP header. If the traffic is not IP traffic but has VLAN tag, mapped to queues based on the CoS value in the VLAN tag. it can configured in QoS → Priority Mapping → DSCP Mapping page.</li> <li>● <b>IP-Precedence:</b> The IP precedence is a 3-bit field in TOS that threats high priority packets as more important than other packets. it can configured in QoS → Priority Mapping → IP Mapping page.</li> </ul> |
| 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 | <p>Set whether to enable Remarking IP Precedence function of outgoing packets, and it is disabled by default.</p> <p><b>Note :</b> Only one of DSCP and IP Precedence re-marking can be enabled.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

## 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

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

Queue Scheduling

Queue Scheduling > **Edit**

Port

1/0/1

Queuing Algorithm

Weighted Fair Queuing(WFQ)

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

| Queue ID | Weight                           |
|----------|----------------------------------|
| 0        | <input type="text" value="90"/>  |
| 1        | <input type="text" value="95"/>  |
| 2        | <input type="text" value="100"/> |
| 3        | <input type="text" value="105"/> |
| 4        | <input type="text" value="110"/> |
| 5        | <input type="text" value="115"/> |
| 6        | <input type="text" value="120"/> |
| 7        | <input type="text" value="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                        | 0      | 1  | 2  | 3  | 4  | 5  | 6  | 7  | Operation |
| 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**

Port 1/0/2

| Queue ID | Enable                              | Maximum Rate/CIR (Kbps) ⓘ            |
|----------|-------------------------------------|--------------------------------------|
| 0        | <input checked="" type="checkbox"/> | <input type="text" value="1000000"/> |
| 1        | <input type="checkbox"/>            | <input type="text"/>                 |
| 2        | <input type="checkbox"/>            | <input type="text"/>                 |
| 3        | <input type="checkbox"/>            | <input type="text"/>                 |
| 4        | <input type="checkbox"/>            | <input type="text"/>                 |
| 5        | <input type="checkbox"/>            | <input type="text"/>                 |
| 6        | <input type="checkbox"/>            | <input type="text"/>                 |
| 7        | <input type="checkbox"/>            | <input type="text"/>                 |

Cancel OK

Configuration of Maximum Rate

## Rate Limit

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

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

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

Rate Limit

To configure a port, click on 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 | Al | Operation |
|-------|----------|-----------|---------------------|-------------------|-----------------------------|-----------------|---------------------------|----|-----------|
| 1/0/1 | Enabled  | Enabled   | 10000               | Enabled           | 10000                       | Enabled         | 10000                     | Dr |           |
| 1/0/2 | Disabled | --        | --                  | --                | --                          | --              | --                        | Dr |           |
| 1/0/3 | Disabled | --        | --                  | --                | --                          | --              | --                        | Dr |           |
| 1/0/4 | Disabled | --        | --                  | --                | --                          | --              | --                        | Dr |           |

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

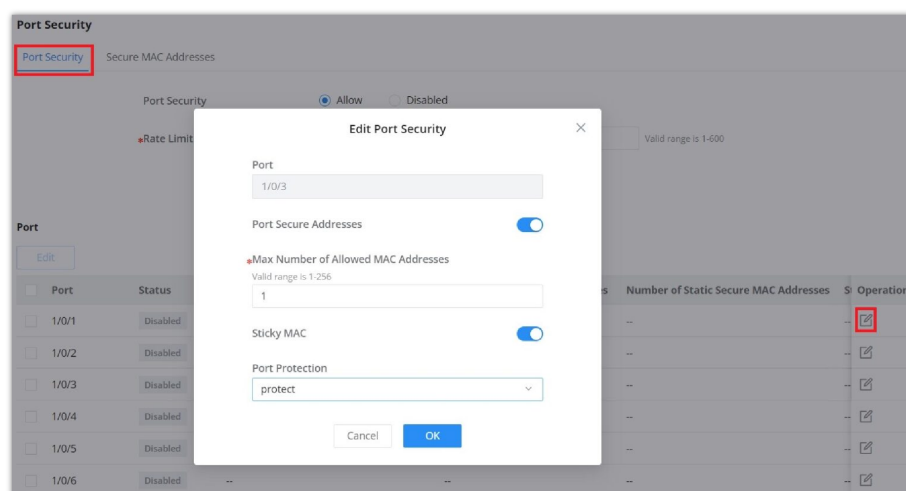
## Port Security

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.

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

### Secure MAC Address Types



### Port Security

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

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

#### Port Security

## Port Isolation

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

#### Note:

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

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

#### Port Isolation

## ACL

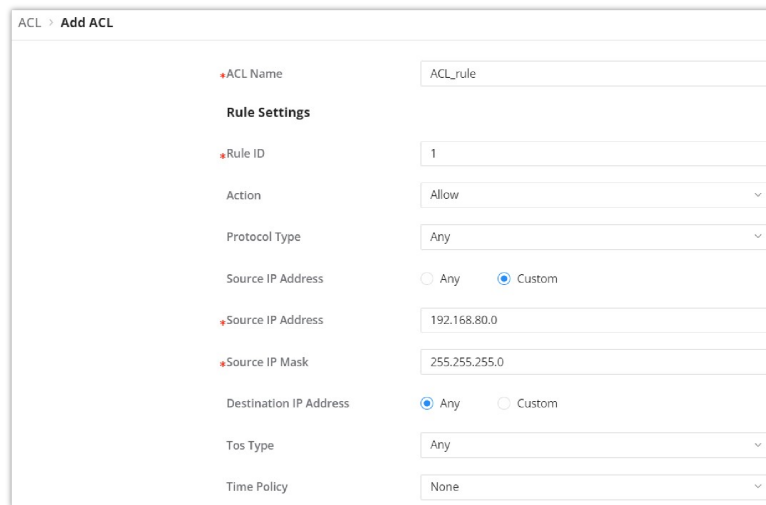
Access control list (ACL) is a collection of one or more rules. A rule is a judgment statement that describes the matching conditions of a packet. These conditions can be the source address, destination address, port number, etc., of the packet. ACL is essentially a packet filter, and the rule is the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

#### Notes:

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

## IPv4/IPv6 ACL

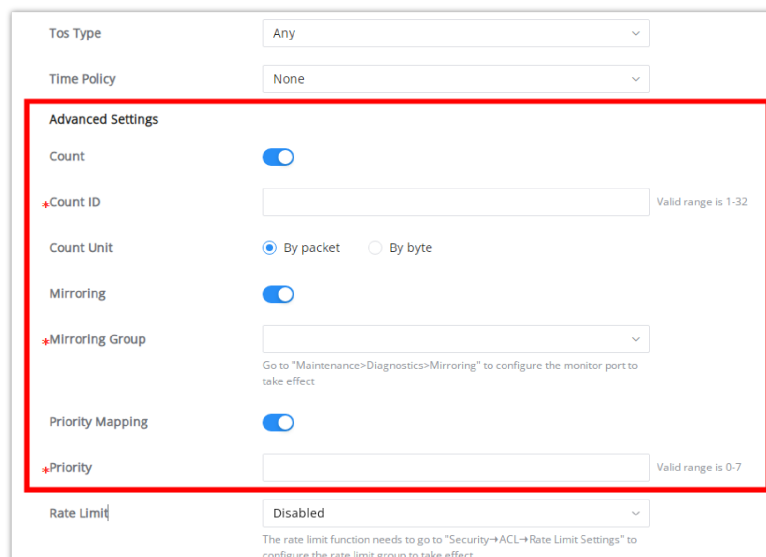
To add an IPv4 or IPv6 ACL rule, navigate to **Security → ACL → IPv4 tab or IPv6 tab**, then click on the **"Add"** button to add an IPv4/IPv6-based ACL rule.



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.



ACL IPv4IPv6 Advanced Settings

ACL IPv4IPv6 Rate Limit

#### Note

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

## Configuring an ACL-based RSPAN

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

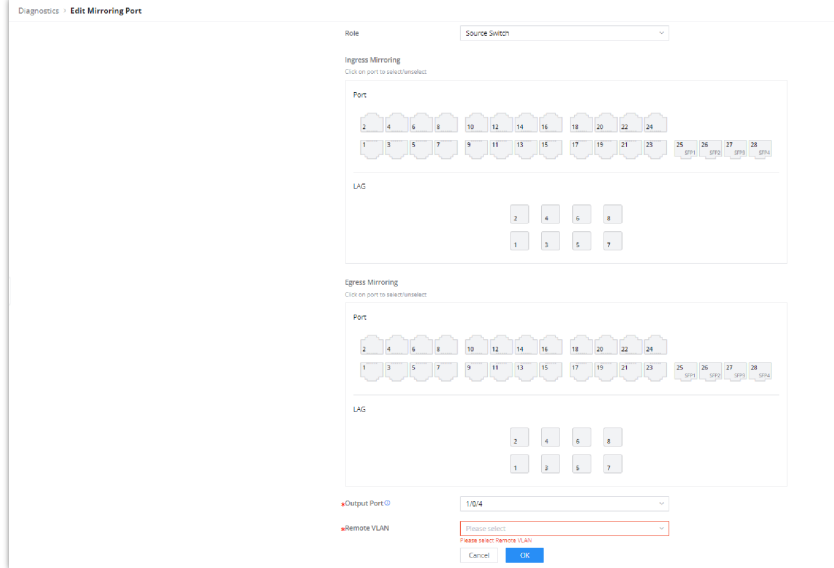
- Select an image group in ACL Image

ACL Based RSPAN

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

IPv4 ACL VLAN

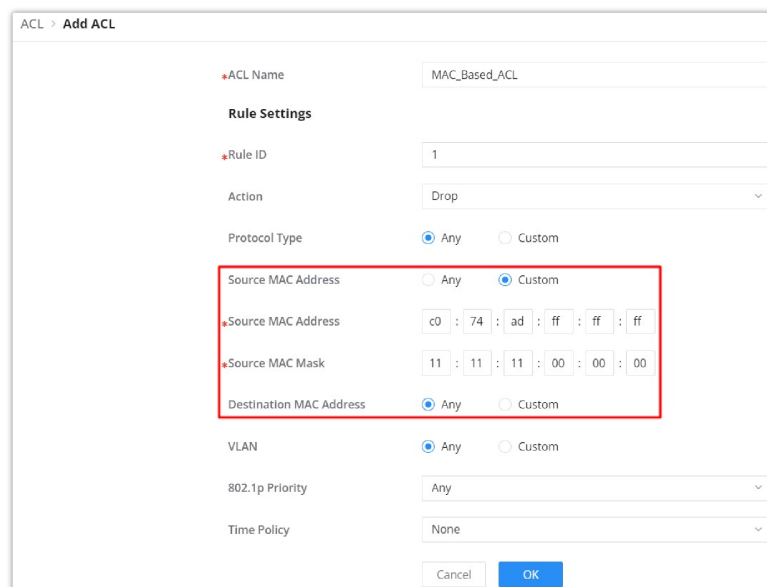
- Then go to **Diagnostics → Mirroring → Setup Mirroring Group**. If you select RSPAN, you can only use it as a source switch, and you need to set the output port and remote VLAN.



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:



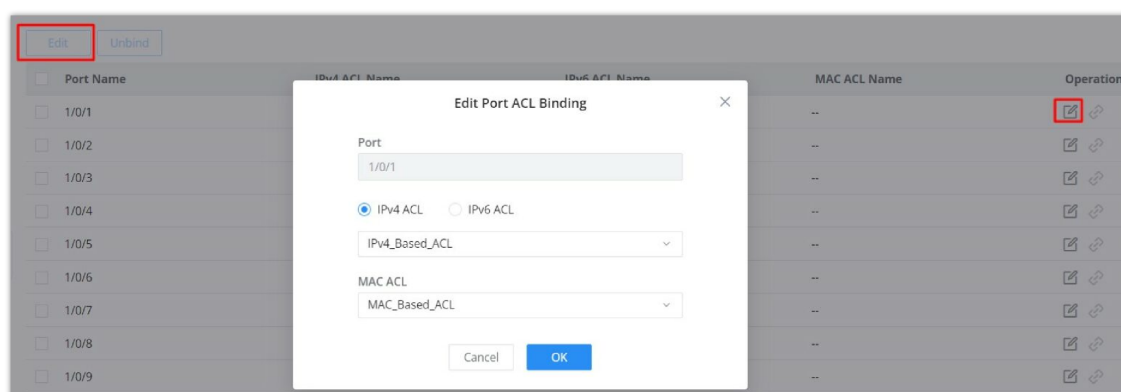
MAC address based ACL

## 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:



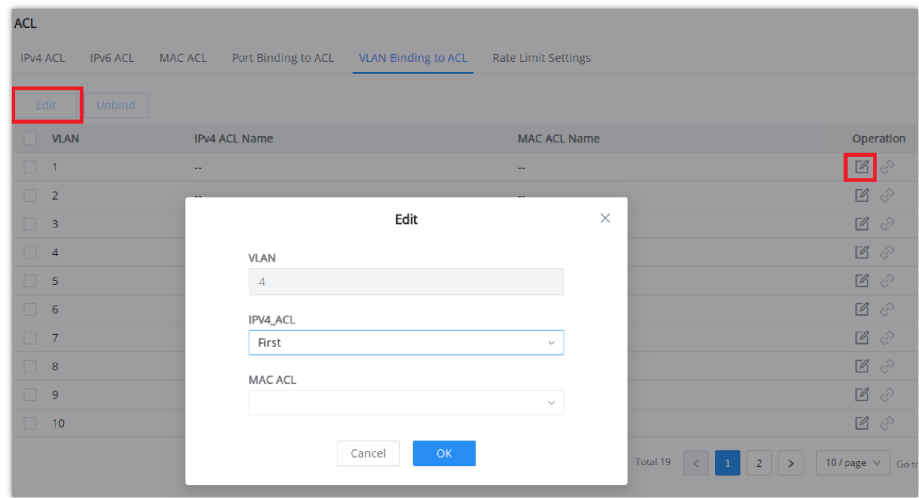
ACL Binding

## 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

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

| ACL                                                                                                  |                 |                 |                |           |
|------------------------------------------------------------------------------------------------------|-----------------|-----------------|----------------|-----------|
| IPv4 ACL   IPv6 ACL   MAC ACL   Port Binding to ACL   VLAN Binding to ACL <u>Rate Limit Settings</u> |                 |                 |                |           |
| Rate Limit Group ID                                                                                  | Rate Limit Type | Burst Threshold | Rate Threshold | Operation |
| 1                                                                                                    | By packet       | 20000 pps       | 150000 pps     |           |
| 2                                                                                                    | By byte         | 8388480 Bps     | 125000 KBps    |           |
| 3                                                                                                    | --              | --              | --             |           |
| 4                                                                                                    | --              | --              | --             |           |
| 5                                                                                                    | --              | --              | --             |           |
| 6                                                                                                    | --              | --              | --             |           |
| 7                                                                                                    | --              | --              | --             |           |
| 8                                                                                                    | --              | --              | --             |           |
| 9                                                                                                    | --              | --              | --             |           |
| 10                                                                                                   | --              | --              | --             |           |

ACL Rate Limit Settings

The users can configure up to 128 groups 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

1

Rate Limit Type

☒ By packet
 ☐ By byte

\*Burst Packet (pps)

Valid range is 1-65535

20000

\*Rate Threshold (pps)

Valid range is 1-262143

150000

Cancel

OK

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.

### Note:

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

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 |
|-------------------------------------------|-----------------|-------------------|-------------------------------|-----------|
| <input type="checkbox"/> 1/0/1            | Disabled        | IP                | 1                             |           |
| <input checked="" type="checkbox"/> 1/0/2 | Enabled         | IP                | --                            |           |
| <input type="checkbox"/> 1/0/3            | Disabled        | IP                | --                            |           |

IP Source Guard

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

Edit Port Security

Port

1/0/1

IPSG

☒

Verification Type

☒ IP
 ☐ IP-MAC

\*Max Entries

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

0

Cancel

OK

IP Source Guard Edit port

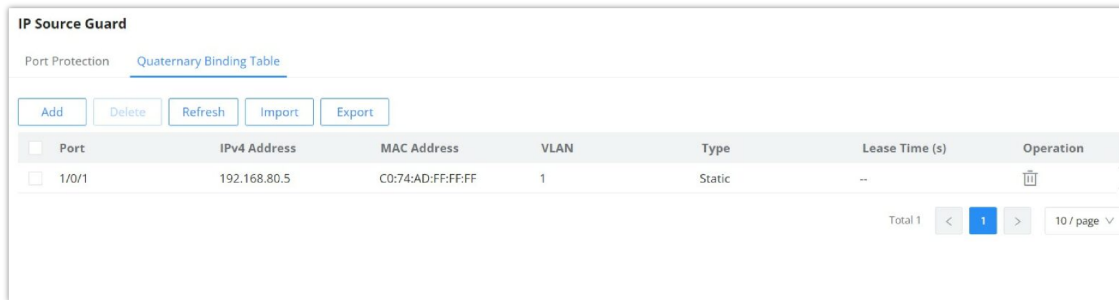


This page displays the dynamic binding (port, IP, MAC, VLAN) generated when DHCP Snooping is enabled on the GWN780x Pro switches. Also, the user can add static binding by clicking on the “Add” button, as shown below:

**Note:**

Dynamic entries require enabling **DHCP Snooping**.

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

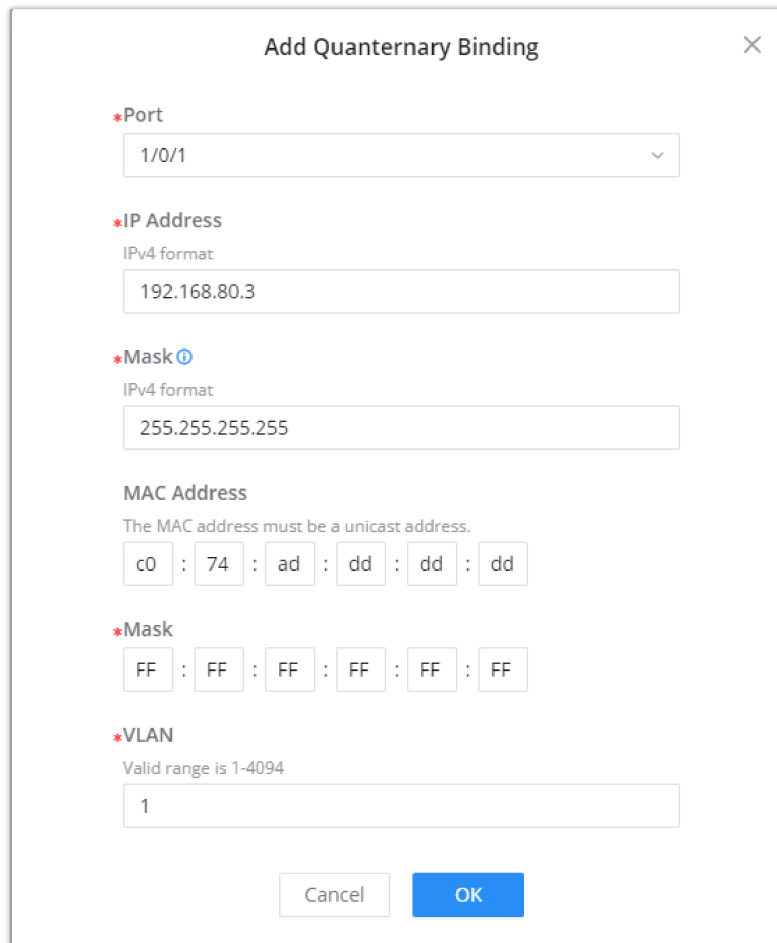


The screenshot shows the 'IP Source Guard' configuration page with the 'Quaternary Binding Table' tab selected. At the top, there are buttons for 'Add', 'Delete', 'Refresh', 'Import', and 'Export'. Below these is a table with the following columns: Port, IPv4 Address, MAC Address, VLAN, Type, Lease Time (s), and Operation. A single entry is visible in the table: Port 1/0/1, IPv4 Address 192.168.80.5, MAC Address C0:74:AD:FF:FF:FF, VLAN 1, Type Static, and Lease Time --. The Operation column contains a trash icon. At the bottom right of the table, it says 'Total 1' and shows pagination controls for page 1 of 10.

| 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 | --             |           |

*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.



The 'Add Quaternary Binding' dialog box contains the following fields and controls:

- \*Port**: A dropdown menu showing '1/0/1'.
- \*IP Address**: A text field with '192.168.80.3'. Below it, the text 'IPv4 format' is displayed.
- \*Mask**: A text field with '255.255.255.255'. Below it, the text 'IPv4 format' is displayed.
- MAC Address**: A section with the instruction 'The MAC address must be a unicast address.' and a row of six input boxes containing 'c0', '74', 'ad', 'dd', 'dd', and 'dd'.
- \*Mask**: A row of six input boxes containing 'FF', 'FF', 'FF', 'FF', 'FF', and 'FF'.
- \*VLAN**: A text field with '1'. Below it, the text 'Valid range is 1-4094' is displayed.
- At the bottom, there are 'Cancel' and 'OK' buttons.

*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

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

IPv6 Source Guard

To enable IPv6 Source Guard on a port, select the port 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

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

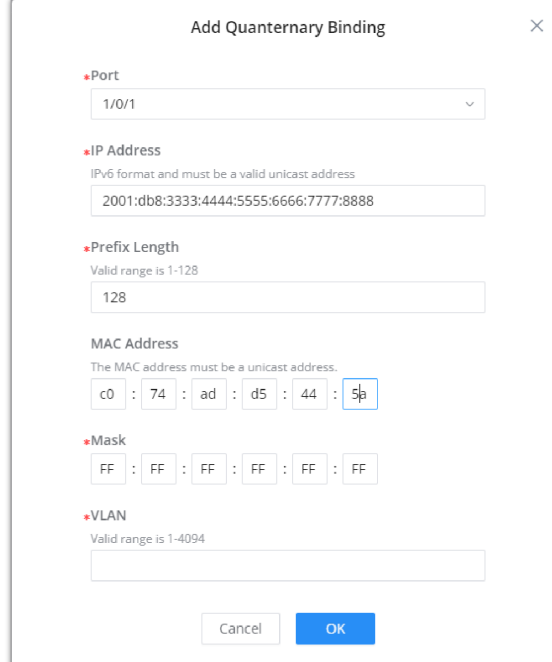
Total 1

<1>

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

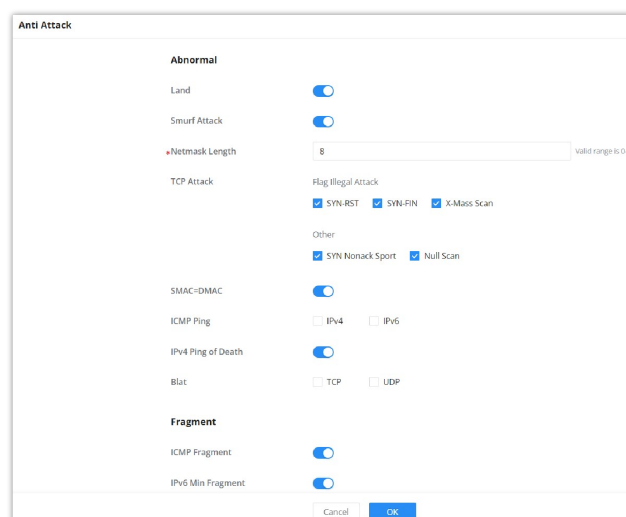
IPv6 Quaternary Binding edit port

## 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 8 valid range is 0-32

TCP Attack

Flag Illegal Attack

☒ SYN-RST ☒ SYN-FIN ☒ X-Mass Scan

Other

☒ SYN Nonack Sport ☒ Null Scan

SMAC=DMAC ☒

ICMP Ping ☐ IPv4 ☐ IPv6

IPv4 Ping of Death ☒

Blat ☐ TCP ☐ UDP

**Fragment**

ICMP Fragment ☒

IPv6 Min Fragment ☒

Cancel OK

Anti Attack

## Dynamic ARP Inspection (DAI)

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

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

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

DAI

DAIStatistics

DAI

VLAN

1

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

Cancel

OK

Port

Edit

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

DAI page

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)

0

Valid range is 0-50

Cancel

OK

DAI Edit port

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

DAI

DAIStatistics

Clear

Refresh

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

DAI Statistics

## RADIUS

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

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

**RADIUS**

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

| Server Address                                  | UDP Port                                                     | Priority    | Max Retransmission Count | Timeout (s) | Operation |
|-------------------------------------------------|--------------------------------------------------------------|-------------|--------------------------|-------------|-----------|
| <input checked="" type="checkbox"/> 192.168.5.5 | <input checked="" type="checkbox"/> RADIUS Server Address    | 192.168.5.5 |                          |             |           |
|                                                 | <input checked="" type="checkbox"/> UDP Port                 | 1812        |                          |             |           |
|                                                 | <input checked="" type="checkbox"/> Priority                 | 16          |                          |             |           |
|                                                 | <input checked="" type="checkbox"/> Shared Key               | password    |                          |             |           |
|                                                 | <input checked="" type="checkbox"/> Max Retransmission Count | 1           |                          |             |           |
|                                                 | <input checked="" type="checkbox"/> Timeout (s)              | 10          |                          |             |           |

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

RADIUS

**Note:**

While RADIUS shared keys can be configured via the Web UI, only the CLI supports input of pre-encrypted password strings (e.g., \$6\$...) for secure deployment and automation. For CLI usage and formatting guidelines, refer to the GWN78xx CLI User Guide.

## TACACS+

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

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

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

**TACACS+**

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

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

☒ TACACS+ Server Address

☒ TCP Port

☒ Priority

☒ Shared Key

☒ Timeout (s)

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

TACACS+

**Note:**

While TACACS+ shared keys can be configured via the Web UI, only the CLI supports input of pre-encrypted password strings (e.g., \$6\$...) for secure deployment and automation. For CLI usage and formatting guidelines, refer to the GWN78xx CLI User Guide.

## AAA

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

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

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

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

The screenshot shows the AAA configuration interface. Under 'Login Authentication', there are dropdown menus for Console (default), Telnet (User1), and SSH (SSH). The 'Method' section has an 'Add' button highlighted with a red box. Below it is a table with columns: AAA Name, Method 1, Method 2, Method 3, Method 4, and Operation. The table lists three methods: default, User1, and SSH. The 'Operation' column for each method contains a 'Modify' icon (pencil) and a 'Delete' icon (trash). The 'Modify' icon for the 'default' method is highlighted with a red box.

| AAA Name | Method 1 | Method 2 | Method 3 | Method 4 | Operation |
|----------|----------|----------|----------|----------|-----------|
| default  | None     | Empty    | Empty    | Empty    |           |
| User1    | Local    | Empty    | Empty    | Empty    |           |
| SSH      | Enable   | Empty    | Empty    | Empty    |           |

AAA

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

The 'Edit Method' dialog box is shown. It has a title bar with a close button. Inside, there is a text field for 'AAA Name' containing 'User1'. Below it is a dropdown menu for 'Method 1' with 'Local' selected. A list of options is shown below the dropdown: None, Local (highlighted in blue), Enable, Radius, and Tacacs+. There is also a dropdown for 'Method 4' with 'Local' selected. At the bottom are 'Cancel' and 'OK' buttons.

AddEdit a method

| Method | Description                                                                                                                                      | Applicability                |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------|
| None   | No authentication is performed. Users can log in without a username or password. This setting should generally be avoided due to security risks. | Console, Telnet, SSH, Web UI |

|                |                                                                                                                                                                                                                                                                                   |                              |
|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------|
| <b>Local</b>   | Uses the local user database on the switch for authentication. User credentials are stored directly on the switch.                                                                                                                                                                | Console, Telnet, SSH, Web UI |
| <b>Enable</b>  | Requires users to enter an enable password to gain elevated privileges (admin access). This provides an additional layer of security after initial authentication. <b>Note:</b> <i>The password for user mode to enter privileged mode must be set using <a href="#">CLI</a>.</i> | Console, Telnet, SSH         |
| <b>RADIUS</b>  | Utilizes a RADIUS server for authentication. RADIUS (Remote Authentication Dial-In User Service) is used for centralized Authentication, Authorization, and Accounting management.                                                                                                | Console, Telnet, SSH, Web UI |
| <b>TACACS+</b> | Utilizes a TACACS+ server for authentication. TACACS+ (Terminal Access Controller Access-Control System Plus) offers more granular control over authorization and is used for centralized AAA management.                                                                         | Console, Telnet, SSH, Web UI |

### AAA Methods

## Identity Authentication Management

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

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

### Port Mode

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

Guest VLAN

Guest VLAN ID

Cancel

OK

Port

Edit

| Port                           | User Authentication Mode | Authentication Method / Method | Guest VLAN | Authorized VLAN | Operation |
|--------------------------------|--------------------------|--------------------------------|------------|-----------------|-----------|
| <input type="checkbox"/> 1/0/1 | Port-Based               | 802.1X / Radius                | Disabled   | Static          |           |
| <input type="checkbox"/> 1/0/2 | MAC-Based                | MAC Authentication / Local     | Disabled   | Static          |           |
| <input type="checkbox"/> 1/0/3 | Single User              | 802.1X / Radius                | Enabled    | Static          |           |
| <input type="checkbox"/> 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 Mode > **Edit**

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

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

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

| <input type="checkbox"/> | Port  | Port Control           | Reauthentication | Max User Count | Reauthentication Timer | Inactive Timer | Quiet Timer | Operation                                                                           |
|--------------------------|-------|------------------------|------------------|----------------|------------------------|----------------|-------------|-------------------------------------------------------------------------------------|
| <input type="checkbox"/> | 1/0/1 | Force authentication   | Enabled          | 256            | 3600                   | 60             | 60          |  |
| <input type="checkbox"/> | 1/0/2 | Auto                   | Enabled          | 256            | 3600                   | 60             | 60          |  |
| <input type="checkbox"/> | 1/0/3 | Force unauthentication | Enabled          | 256            | 3600                   | 60             | 60          |  |
| <input type="checkbox"/> | 1/0/4 | Disable                | Disabled         | 256            | 3600                   | 60             | 60          |  |

Identity Authentication Management port page

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

Identity Authentication Management > Edit

Port

1/0/1

Port Control

Force authentication

Disable

Force authentication

Force unauthentication

Auto

Valid range is 1-256

Reauthentication

Max User Count

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

#### Note:

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

Example of 802.1X configuration on GXV3480 IP Video phone.

802.1X Mode

802.1X Mode

802.1X Identity

802.1X Secret

EAP-MD5

hope

....

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 ModePortAuthentication SessionsLocal User of MAC-based

RefreshClear All

Q Session ID/Port/M

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

Authentication Sessions

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

| Refresh              | Clear All |                   |            |
|----------------------|-----------|-------------------|------------|
| Session ID           | Port      | MAC Address       | Status     |
| 000000091184<br>7958 | 1/0/6     | C0:74:AD:03:CA:80 | Authorized |

Authentication Sessions Status Authorized

|                      |       |                   |        |
|----------------------|-------|-------------------|--------|
| 000000091184<br>7958 | 1/0/6 | C0:74:AD:03:CA:80 | Locked |
|----------------------|-------|-------------------|--------|

Authentication Sessions Status Locked

|                      |       |                   |       |
|----------------------|-------|-------------------|-------|
| 000000091184<br>7958 | 1/0/6 | C0:74:AD:03:CA:80 | Guest |
|----------------------|-------|-------------------|-------|

Authentication Sessions Status Guest

## Local User of a MAC-based

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

| Identity Authentication Management |                   |                         |                         |                           |                   |                                                                                                                                                                             |
|------------------------------------|-------------------|-------------------------|-------------------------|---------------------------|-------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Port Mode                          | Port              | Authentication Sessions | Local User of MAC-based |                           |                   |                                                                                                                                                                             |
| Add                                | Delete            | Delete All              |                         |                           |                   |                                                                                                                                                                             |
| <input type="checkbox"/>           | MAC Address       | Port Control            | VLAN                    | Reauthentication Time (s) | Inactive Time (s) | Operation                                                                                                                                                                   |
| <input type="checkbox"/>           | C0:74:AD:01:92:94 | Force Unauthorized      | --                      | --                        | --                |   |
| <input type="checkbox"/>           | C0:74:AD:03:CA:80 | Force Authorized        | 1                       | 3600                      | 60                |   |

Local User of MAC based

Add Local User of MAC-based

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

\*MAC Address

C0 : 74 : AD : 01 : 92 : 94

Port Control

☒ Force Authorized
☐ Force Unauthorized

VLAN ⓘ

Valid range is 1-4094

1

Reauthentication Time (s)

Valid range is 300-2147483647

3600

Inactive Time (s)

Valid range is 60-65535

60

Cancel

OK

Add local User of MAC based

|                           |                                                                                                                                                                                                                                                                                                                      |
|---------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| MAC Address               | The MAC address of the local user must be a unicast one.                                                                                                                                                                                                                                                             |
| Port Control              | <ul style="list-style-type: none"> <li>• <b>Force Authorized:</b> Forces the port to authorize the device with the specified MAC address, allowing it access to the network.</li> <li>• <b>Force Unauthorized:</b> Forces the port to not authorize the device, preventing it from accessing the network.</li> </ul> |
| VLAN                      | Valid range is 1-4094.                                                                                                                                                                                                                                                                                               |
| Reauthentication Time (s) | Valid range is 300-2147483647.                                                                                                                                                                                                                                                                                       |
| Inactive Time (s)         | Valid range is 60-65535.                                                                                                                                                                                                                                                                                             |

Add local User of MAC-based

## DHCP Snooping

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

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

When the device reboots, the dynamic binding table for 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 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 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  
SwichPort1

Remote ID  
0~63 characters  
Main Router

Cancel

OK

DHCP Snooping Option 82 Add Circuit

### Note

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

## DHCP Snooping Port Settings

On this page, the 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                                                                             |
|-------------------------------------------|------------|---------------------|------------|-----------|----------------|---------------------------------------------------------------------------------------|
| <input checked="" type="checkbox"/> 1/0/1 | Enabled    | Disabled            | 0          | Enabled   | Keep           |  |
| <input type="checkbox"/> 1/0/2            | Disabled   | Disabled            | 0          | Disabled  | Drop           |  |
| <input type="checkbox"/> 1/0/3            | Disabled   | Disabled            | 0          | Disabled  | Drop           |  |
| <input type="checkbox"/> 1/0/4            | Disabled   | Disabled            | 0          | Disabled  | Drop           |  |
| <input type="checkbox"/> 1/0/5            | Disabled   | Disabled            | 0          | Disabled  | Drop           |  |

DHCP Snooping Port Settings

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

Port Settings > Edit

Port  
1/0/1

Trust Mode  
☒

Chaddr Verification  
☐

\*Rate (pps)  
0

Valid range is 0-300

Option 82  
☒

Option 82 Mode  
Keep

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 Snooping

Option 82

Port Settings

Statistics

Clear

Refresh

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

DHCP Snooping Statistics

## DHCPv6 Snooping

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

To enable 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

1,5-8,20

⊗

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

Cancel

OK

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

c0:74:ad:ba:24:fc

⊗

1~63 characters

Cancel

OK

Option 18

Add

Delete

| <input checked="" type="checkbox"/> | Port  | Interface ID | Operation |
|-------------------------------------|-------|--------------|-----------|
| <input checked="" type="checkbox"/> | 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

Format

\*Interface ID

*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                                                                                                          |            |       |           |           |                                     |  |
|--------------------------------------------------------------------------------------------------------------------------|------------|-------|-----------|-----------|-------------------------------------|--|
| <a href="#">DHCPv6 Snooping</a> <a href="#">Option Settings</a> <a href="#">Port Settings</a> <a href="#">Statistics</a> |            |       |           |           |                                     |  |
| <input type="button" value="Edit"/>                                                                                      |            |       |           |           |                                     |  |
| <input checked="" type="checkbox"/> Port                                                                                 | Trust Mode | Speed | Option 18 | Option 37 | Operation                           |  |
| <input checked="" type="checkbox"/> 1/0/1                                                                                | Enabled    | 300   | Drop      | Keep      | <input type="button" value="Edit"/> |  |
| <input type="checkbox"/> 1/0/2                                                                                           | Disabled   | 0     | Disabled  | Disabled  | <input type="button" value="Edit"/> |  |
| <input type="checkbox"/> 1/0/3                                                                                           | Disabled   | 0     | Disabled  | Disabled  | <input type="button" value="Edit"/> |  |
| <input type="checkbox"/> 1/0/4                                                                                           | Disabled   | 0     | Disabled  | Disabled  | <input type="button" value="Edit"/> |  |

*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 Settings > **Edit**

Port

Trust Mode ☒

\*Rate (pps)  Valid range is 0-300

Option 18 ☒

Option 18 Mode

Option 37 ☒

Option 37 Mode

*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.

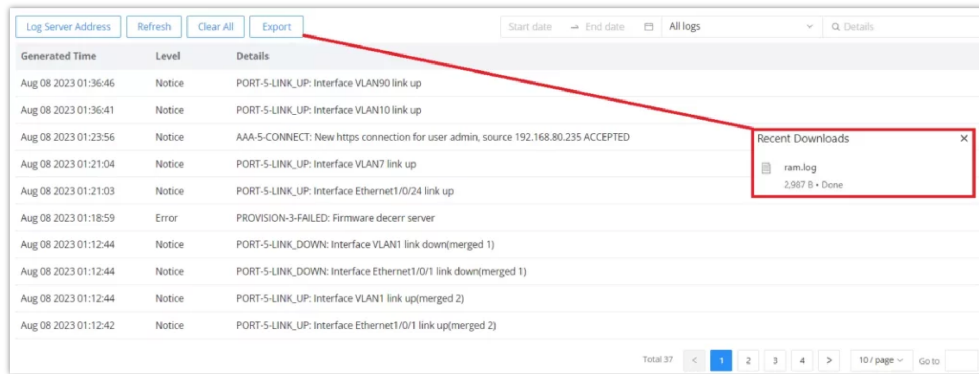
To clear the statistics, select the ports and click on the **"Clear"** button as shown below:





## 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.



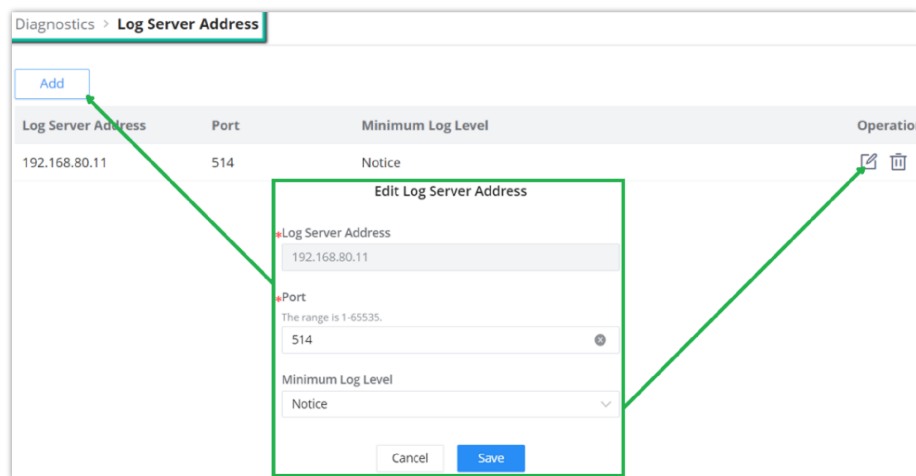
| Generated Time       | Level  | Details                                                                            |
|----------------------|--------|------------------------------------------------------------------------------------|
| Aug 08 2023 01:36:46 | Notice | PORT-5-LINK_UP: Interface VLAN90 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-S-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  
2,967 B • Done

Diagnostics Logs

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



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

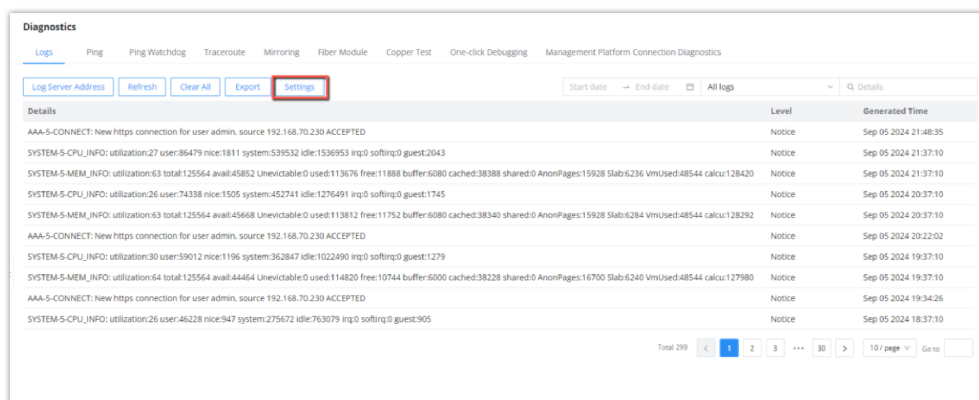
Minimum Log Level  
Notice

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 Unavailable: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 Unavailable: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 Unavailable: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\*retryes a 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**

traceroute 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.

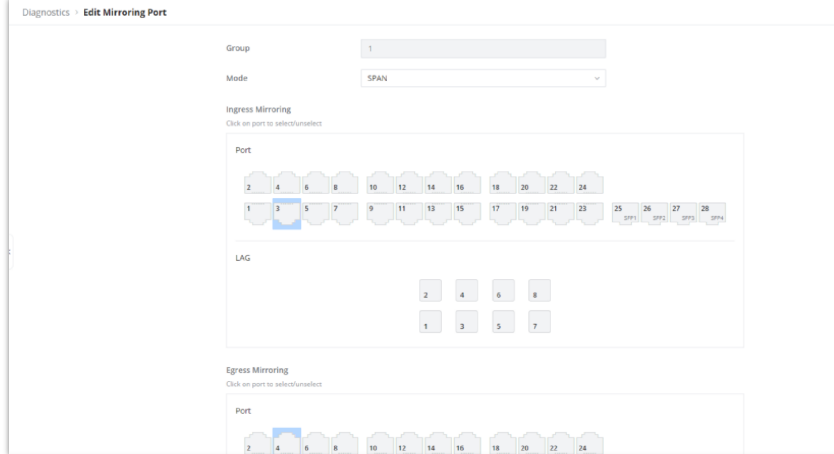
The GWN780x Pro switches support two modes of Port Mirroring: SPAN and RSPAN:

- **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.



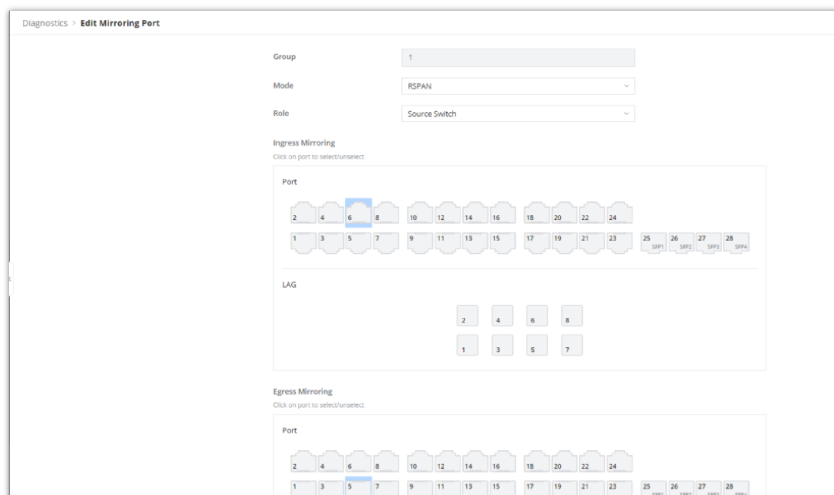
Port Mirroring

## RSPAN

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

### Source Switch Role (RSPAN)

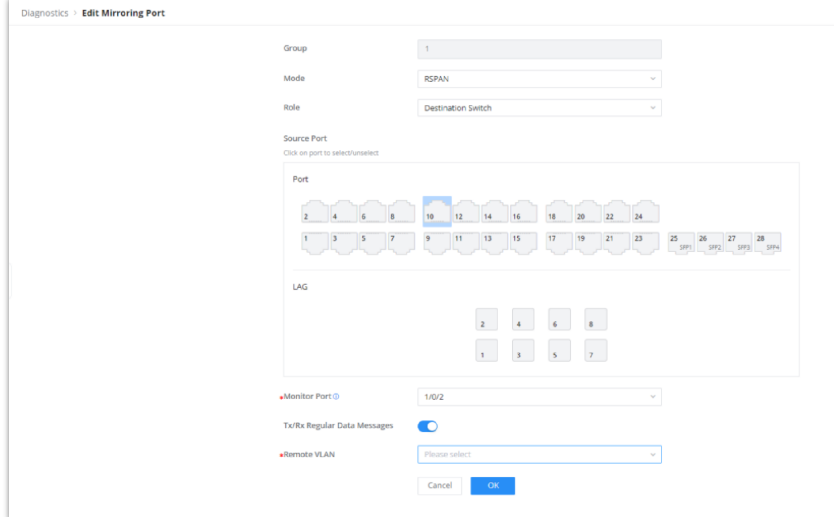
- **Ingress Mirroring:** This captures incoming traffic on the specified source port(s). It mirrors the packets received by the port before they are processed by the switch, forwarding them to the designated destination for monitoring or analysis.
- **Egress Mirroring:** This captures outgoing traffic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



Source Switch Role

### Destination Switch Role (RSPAN)

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

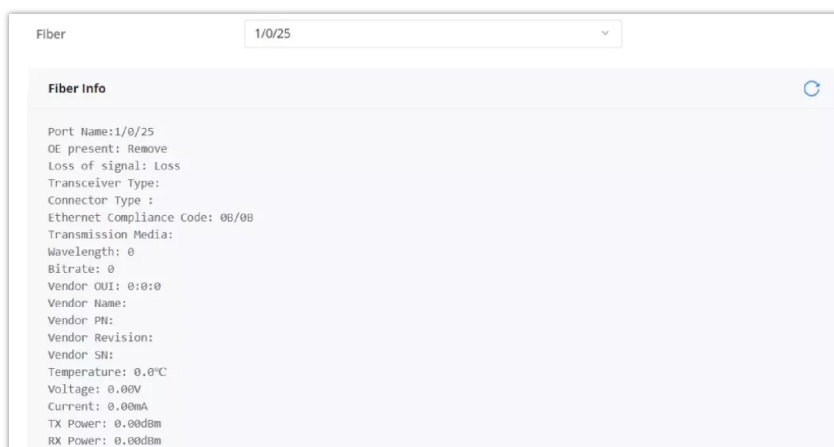


Destination Switch Role RSPAN

## Fiber Module

This 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 Module

## Copper Test

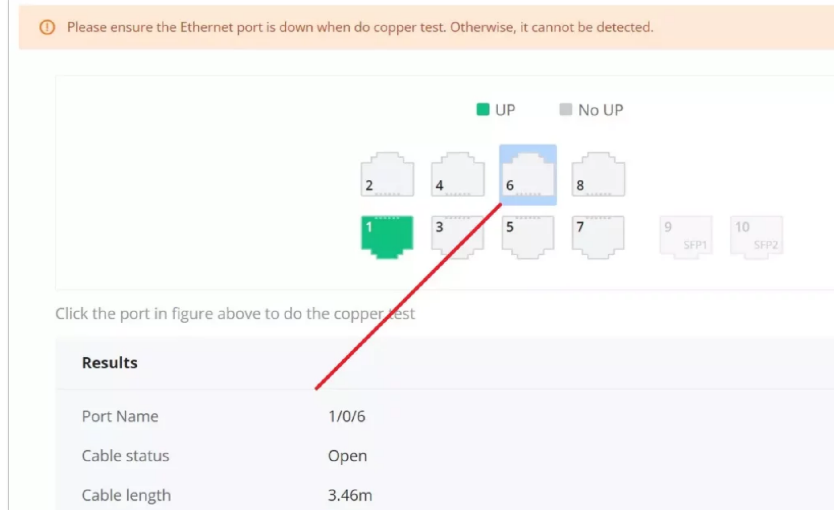
Copper test can detect whether the cable connected to the switch is faulty and the location of the fault. Using this function can assist in the daily engineering installation diagnosis .

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

### Note:

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

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



*Copper Test*

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

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

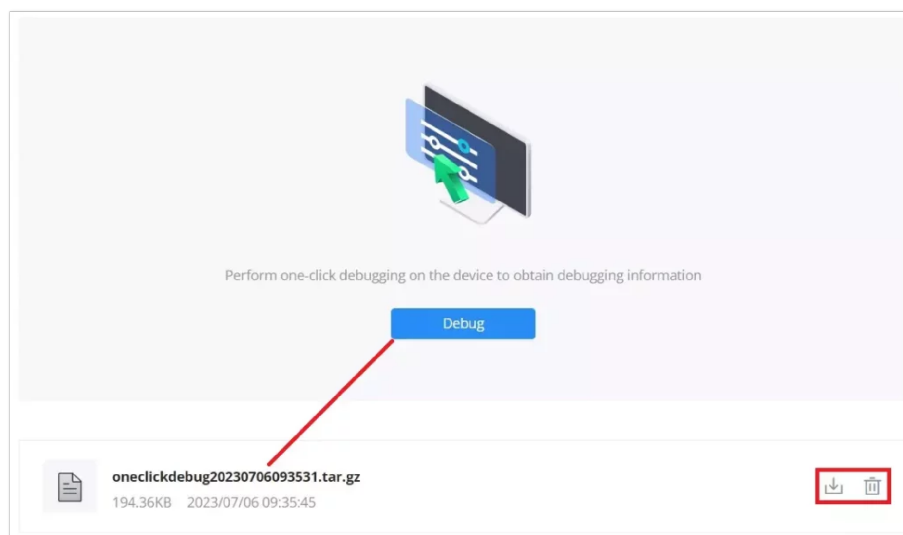
#### Cable Length:

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

### One-click Debugging

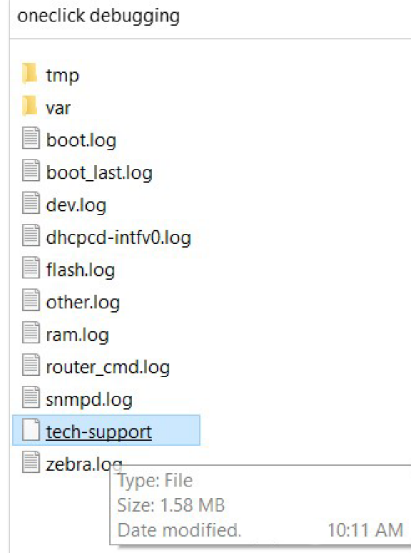
On GWN780x Pro switches, the One-click debugging feature can help administrators or tech support to quickly and easily get debugging information about the GWN switch in a matter of a few minutes.

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



*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.

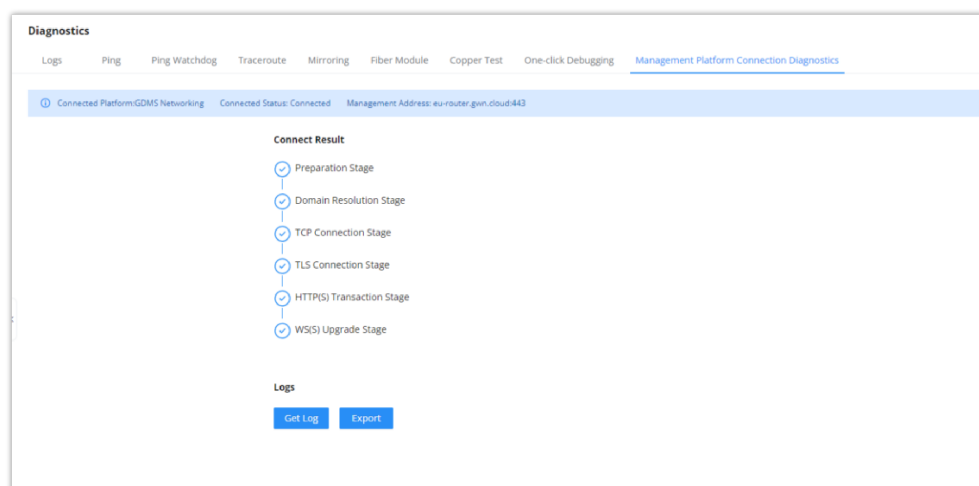


One click Debugging Folder

## Management Platform Connection Diagnostics

If the GWN780x Pro switch is added to the GDMS networking, GWN Manager, or a GWN Router, it will display a Cloud icon with a green check mark (as shown in the figure below) indicating it's added to a GDMS Networking account, GWN Manager, or to a GWN Router.

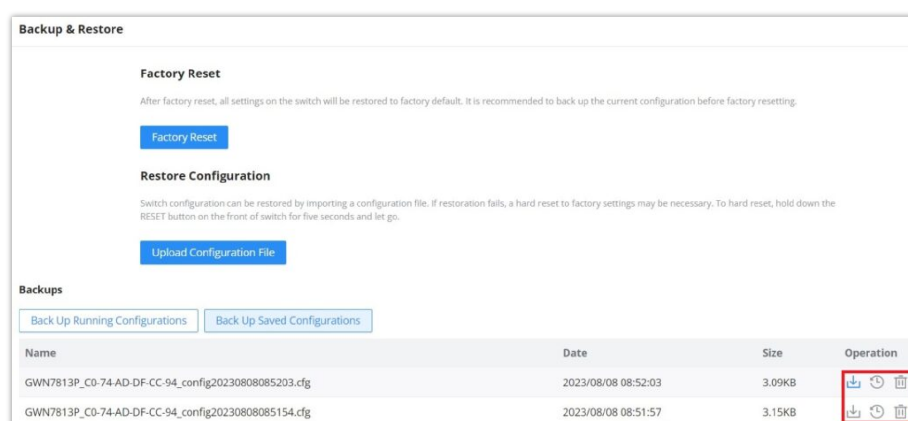
In case there is an issue with the connection, then the user can navigate to **Maintenance → System Diagnosis → Cloud/Manager Connection Diagnostics** and then click on the “**Detection**” or “**Redetection**” button to see in what stage/step the connection has failed. Refer to the figure below:



CloudManager Connection Diagnostics

## Backup and Restore

Click on the “Factory Reset” button to reset the GWN780x Pro Switch back to default settings, or restore to previously saved backup by uploading a configuration file. These configuration files can be used as a way to back up the device running configuration or saved configuration.



Backup and Restore

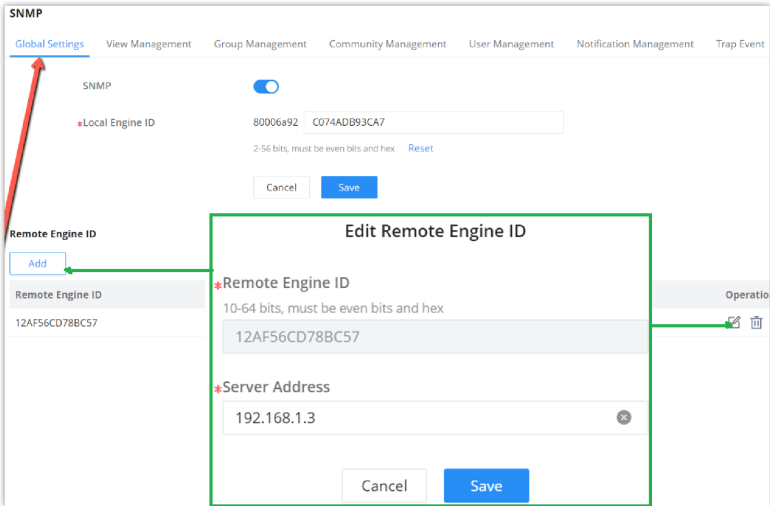
SNMP

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

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

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

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



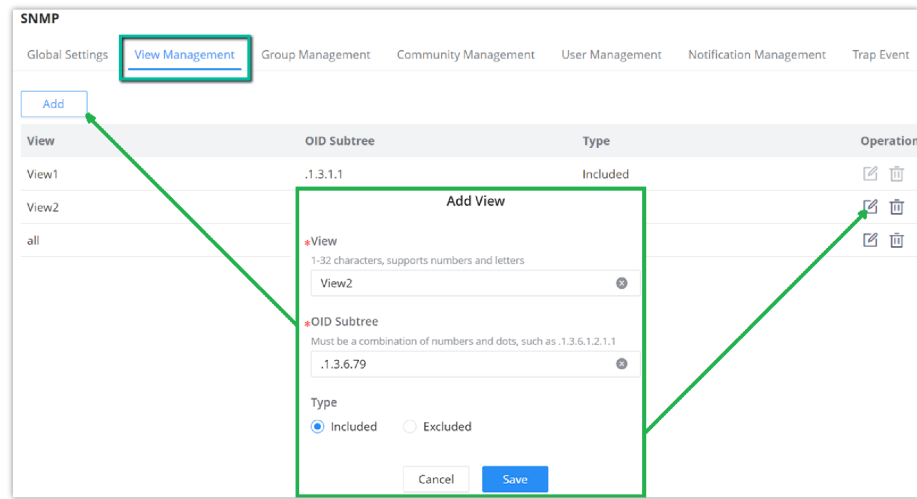
SNMP Global Settings

|                       |                                                                                                                                                                                                                                                                                                                                                                                  |
|-----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SNMP                  | Select whether to enable SNMP.                                                                                                                                                                                                                                                                                                                                                   |
| Local Engine ID       | Set the engine ID of the local SNMP entity or click “Reset” to restore to the initial value.<br><i>Note: The default is 8000 A59Dxxxxxxx, where xxxxxxxx is the device MAC address by default, which can be modified by the user . It is expressed in hexadecimal , and the length is limited between 2 and 56 characters. The number of characters must be an even number .</i> |
| Edit Remote Engine ID |                                                                                                                                                                                                                                                                                                                                                                                  |
| Remote Engine ID      | Set the engine ID of the SNMP management side , and the remote user is established under the remote engine. The input length is limited to 10-64 characters, expressed in hexadecimal , and the number of characters must be an even number.                                                                                                                                     |
| Server Address        | Set the address of the network management station server, support input of Hostname and IP address (including IPv4 and IPv6), and need to meet the requirements of various types of address formats, otherwise an error message is required.                                                                                                                                     |

SNMP Global Settings



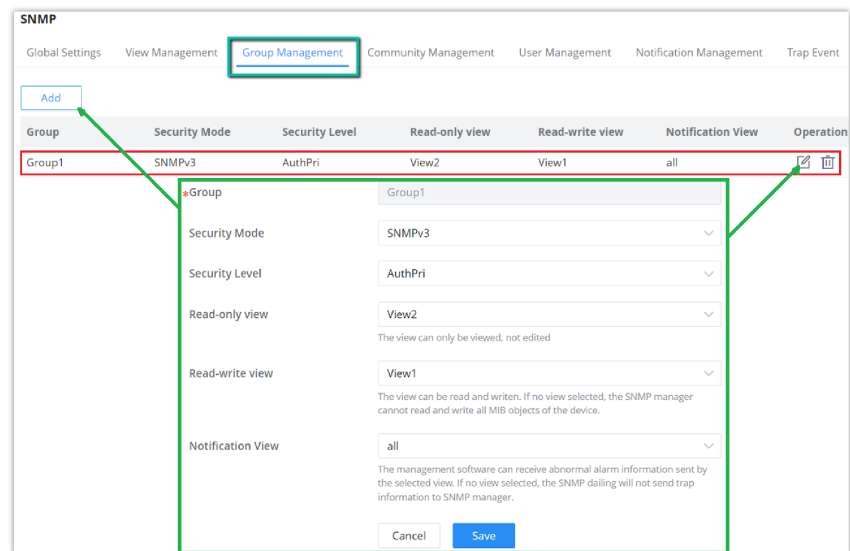
This page allows the network administrator to create MIB views (Management Information Base) and then include or exclude OID (Object Identifier) in a view.



SNMP View Management

## Group Management

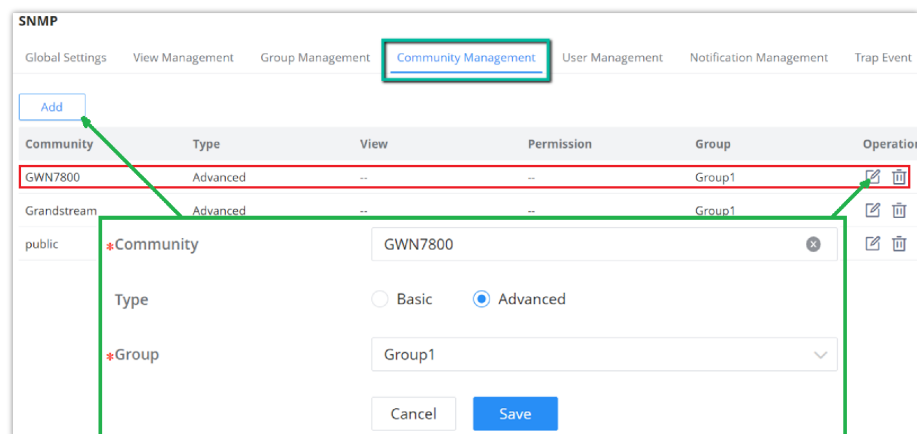
This page allows the network administrator to group SNMP users and assign different authorization and access privileges.



SNMP Group Management

## Community Management

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



SNMP Community Management

## SNMP User Management

This page allows a user to configure the SNMPv3 user profile.

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

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

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

SNMP

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: ☐

Port Security: ☐

PoE Power Supply: ☐

Logs: ☐

Configuration Distribution: ☐

Cancel OK

SNMP Trap Event

## 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.

### Note:

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

## RMON Statistics

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

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

RMON Statistics

## RMON History

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

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

**RMON History**

Statistics **History** Event Alarm

[Add](#)

| History ID | Port | Sampling Interval | Operation |
|------------|------|-------------------|-----------|
| 1          | GE1  | 1800              |           |

**Edit History**

History ID: 1

\*Port: GE1

\*Maximum Samples: 50 (The range is 1-50.)

\*Sampling Interval (s): 1800 (The range is 1-3600.)

Owner: Admin (0-32 characters, supports numbers and letters)

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

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.

The screenshot shows the RMON configuration interface with the 'Event' tab active. A table displays event configurations, and a modal form is open for editing the first event (ID 1). The modal form includes fields for Event ID, Detail, Type, Community, and Owner, each with a description of its constraints. The 'Add' button in the table is highlighted with a green arrow, and the modal form is outlined in green. The table row for the event is also highlighted with a red border.

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

Modal Form Fields:

- Event ID: 1
- Detail: 0-32 characters, supports numbers and letters. Value: Admin
- Type: Log&Trap
- Community: 1-32 characters, supports numbers and letters. Value: Grandstream
- Owner: 0-32 characters, supports numbers and letters. Value: Admin

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.

The screenshot shows the RMON configuration interface with the 'Alarm' tab active. A table displays alarm configurations, and a modal form is open for editing the first alarm (ID 1). The modal form includes fields for Alarm ID, Port, Counter, Sampling Type, Sampling Interval, Owner, Trigger Mode, Rising Threshold, and Rising Event, each with a description of its constraints. The 'Add' button in the table is highlighted with a green arrow, and the modal form is outlined in green. The table row for the alarm is also highlighted with a red border.

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

Modal Form Fields:

- Alarm ID: 1
- Port: GE1
- Counter: Drop Events
- Sampling Type: Absolute (selected), Delta
- Sampling Interval (s): 100
- Owner: Admin
- Trigger Mode: Rising
- Rising Threshold: 100
- Rising Event: 1

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

LLDP ☒

TLV Advertise Interval (s)  Valid range is 5-32767

TTL Multiplier  Valid range is 2-10

Port Reinitializing Delay Time (s)  Valid range is 1-10

LLDPDU Transmit Delay Time (s)  Valid range is 1-8191

Cancel OK

Port Settings

Edit

| Port                                      | Mode  | TLV                                                                                                   | Operation |
|-------------------------------------------|-------|-------------------------------------------------------------------------------------------------------|-----------|
| <input checked="" type="checkbox"/> 1/0/1 | Tx/Rx | PortDescription, SysName, SysDescription, SysCapabilities, ManagementAddrSel, PVID, MacPhySel, Lin... |           |
| <input checked="" type="checkbox"/> 1/0/2 | Tx/Rx | PortDescription, SysName, SysDescription, SysCapabilities, ManagementAddrSel, PVID, MacPhySel, Lin... |           |
| <input checked="" type="checkbox"/> 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

Mode

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  Valid range is 1-10

Auto Voice Network Policy ☒

Cancel OK

Network Policy

Add Delete

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

LLDP MED Network Policy

To add a Network Policy, click on 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 <small>Valid range is 0-4095</small> |
| 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 |
|-----------------------------------------|----------|--------------------|---------------|-----------------------------|-------------|-----------|
| <input checked="" type="checkbox"/> GE1 | Enabled  | Enabled            | Enabled       | Disabled                    | Disabled    |           |
| <input type="checkbox"/> GE2            |          |                    |               |                             |             |           |
| <input type="checkbox"/> GE3            |          |                    |               |                             |             |           |
| <input type="checkbox"/> GE4            |          |                    |               |                             |             |           |
| <input type="checkbox"/> GE5            |          |                    |               |                             |             |           |
| <input type="checkbox"/> GE6            |          |                    |               |                             |             |           |
| <input type="checkbox"/> GE7            |          |                    |               |                             |             |           |
| <input type="checkbox"/> GE8            |          |                    |               |                             |             |           |
| <input type="checkbox"/> GE9            |          |                    |               |                             |             |           |
| <input type="checkbox"/> GE10           |          |                    |               |                             |             |           |

Port GE1

LLDP MED ☒

Network Policy TLV ☒

\*Network Policy Voice 1

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**

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

**Local Device Info**

|                               |                |
|-------------------------------|----------------|
| Chassis ID Subtype            | MacAddr        |
| Chassis ID                    | C0:74:AD:...   |
| 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:...   |
| 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

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

Refresh Delete

Search

| <input type="checkbox"/>                                                                         | Local Port | Chassis ID Subtype | Chassis ID | Neighbor ID Subtype | Neighbor Port ID | Device Name | System Description | Survival | Operation |
|--------------------------------------------------------------------------------------------------|------------|--------------------|------------|---------------------|------------------|-------------|--------------------|----------|-----------|
|  <p>No Data</p> |            |                    |            |                     |                  |             |                    |          |           |

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

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

LLDP Statistics

## Energy Efficient Ethernet

EEE or **Energy Efficient Ethernet** helps 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

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

Energy Efficient Ethernet

To enable EEE on a port, select a port, then click on the “Edit” button, then toggle ON 802.3 EEE as shown below:

Edit Port

Port

1/0/1

802.3 EEE

Cancel

OK

## Alert

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

Alert

[Alert Settings](#)
[Statistics](#)

| Type                      | Alert Status                        | Log Level | Alert Threshold | Alert Waiting Time (s) | Restore Threshold | Restore Waiting Time (s) |
|---------------------------|-------------------------------------|-----------|-----------------|------------------------|-------------------|--------------------------|
| CPU Usage                 | <input checked="" type="checkbox"/> | Error     | 80%             | 30                     | 80%               | 10                       |
| Memory Usage              | <input checked="" type="checkbox"/> | Error     | 80%             | 30                     | 80%               | 10                       |
| PoE Power                 | <input checked="" type="checkbox"/> | Error     | 80%             | 30                     | 80%               | 10                       |
| Mac Address Exceeds Limit | <input checked="" type="checkbox"/> | Error     | 80%             | 30                     | 80%               | 10                       |
| Temperature               | <input checked="" type="checkbox"/> | Error     | 77℃             | 30                     | 77℃               | 10                       |
| Fan Malfunction           | <input checked="" type="checkbox"/> | Error     | --              | 30                     | --                | 10                       |
| PoE Chip Malfunction      | <input checked="" type="checkbox"/> | Error     | --              | 30                     | --                | 10                       |

Cancel

OK

## Alert Statistics

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

| Alert                     |                |                     |                         |                     |                           |             |
|---------------------------|----------------|---------------------|-------------------------|---------------------|---------------------------|-------------|
| Alert Settings            |                | Statistics          |                         |                     |                           |             |
| <div>Refresh</div>        |                |                     |                         |                     |                           |             |
| 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           |

## SYSTEM

## Basic Settings

The basic settings page is split into three categories:

- o **Basic Info:** first section, the user can specify a name for the GWN780x Pro switch with a system location and contact.
- o **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.
- o **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                | <div>Select time synchronization method: Manual or Automatic (NTP Server).</div> <div><div><div>● Manual:</div>specify the time manually.</div><div><div>● Automatic (NTP Server):</div>time will be synced automatically with NTP Server.</div></div> <div><i>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.</i></div> |
| System Time                | <div><div>● If Manual is selected,</div>the user can specify the date and time.</div> <div><div>● If Automatic (NTP Server) is selected,</div>the current time and time will be displayed,</div>                                                                                                                                                                                                                                                                                                                            |
| 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 | <div><div>● Disabled:</div>DayLight Saving mode will be disabled.</div> <div><div>● Recurring:</div>if the Daylight saving is recurring (repetitive).</div> <div><div>● Non Recurring:</div>if selected the user can specify the offset (min) and daylight saving time start date and end date.</div> <div><div>● Recurring USA:</div>for USA region.</div> <div><div>● Recurring EU:</div>for EU region</div>                                                                                                              |
| 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 (min):** (the range is from 15 seconds to 1440), which is how much time before the GWN780x Pro switch will log out automatically.
- **HTTPS:** the HTTPS port, by default, is 443. It can be changed if necessary. (It's recommended to keep it 443).
- **Telnet:** can be enabled, but by default is disabled (it's recommended to keep it disabled, it's not secure, and use SSH instead).
- **SSH:** SSH is enabled by default, and it's a better alternative to Telnet. The default port is 22. It can be changed if necessary. (It's recommended to keep it to 22)

Access Control Web Service Management

### Note:

VTY (Virtual Teletype) sessions allow remote management of network devices through a command-line interface. GWN780x Pro switches now support up to 12 simultaneous VTY sessions, enabling concurrent SSH or Telnet access for administrators.

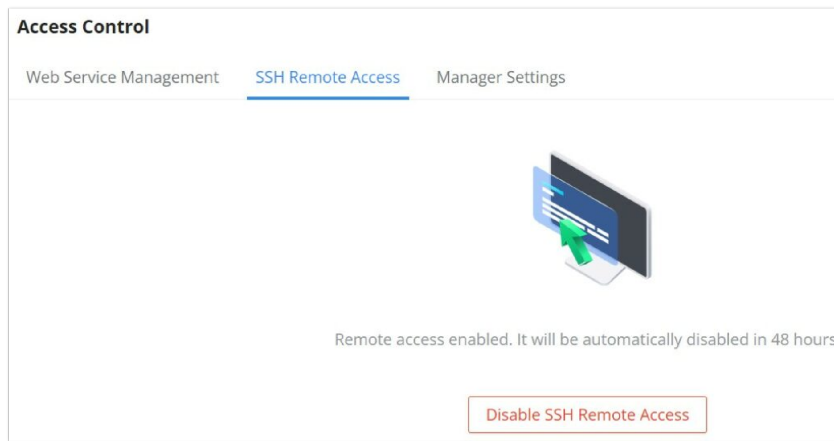
## SSH Remote Access

### Note:

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

Access Control SSH Remote Access disabled

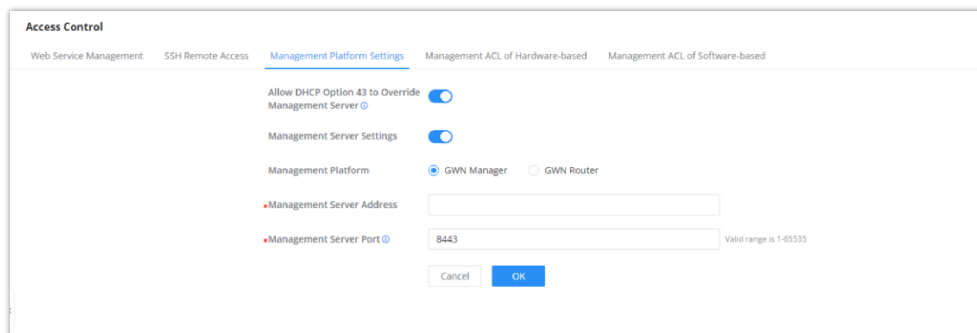
Enter the password, then click on the “SSH Remote Access” button. It will be automatically disabled in 48 hours.



*Access Control SSH Remote Access enabled*

## 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.



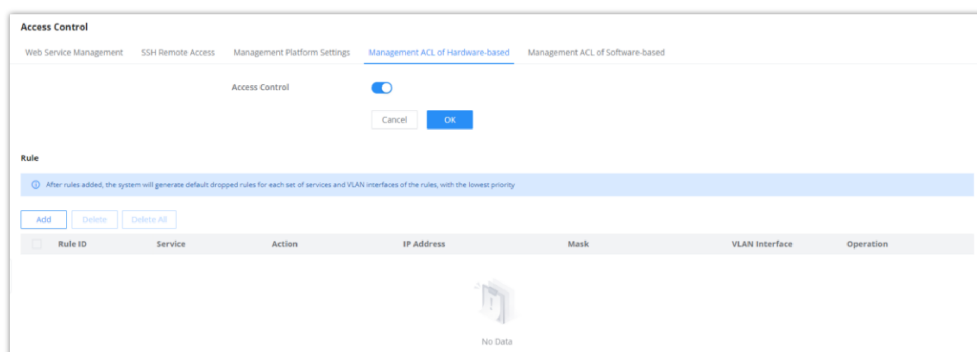
*Access Control Manager Settings*

### Note:

When the GWN Manager wants to take over a managed switch, it can force the takeover by entering the switch's current password.

## 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.



*Management ACL of Hardware based*

Management ACL of Hardware-based > Add

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

Buttons: 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.

Management ACL of Software-based > Add ACL

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 Grid: 28 ports (1-28) in a 2x14 grid. Ports 1-24 are standard, 25-28 are SFPs.

LAG Grid: 7 LAGs (1-7) in a 2x4 grid.

*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.

### Note:

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

### 3. Monitor

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

#### Note:

Can only view information.

Click on the "Add" button to add a new user, then specify the password and the user level (Operator or Monitor).

The screenshot shows the 'User Management' interface. On the left, there is a table with columns 'Username' and 'Level'. The table contains four rows: 'admin' (Administrator), 'User1' (Monitor), 'Devs' (Operator), and 'Technician' (Monitor). The 'Add' button is highlighted with a red arrow, and the 'Delete' button is highlighted with a green arrow. On the right, the 'Add User' dialog box is open. It has three input fields: 'Username' (with a hint '1-64 characters, supports numbers, letters and special characters which contains \_@#&'), 'Password' (with a hint '8-64 characters, must contain two of digits, letters and special characters'), and 'Confirm Password'. Below these fields are radio buttons for 'User Level': 'Operator' (All features except setting management IP address and factory reset of admin are allowed) and 'Monitor' (Can only view information). The 'Monitor' option is selected. At the bottom of the dialog are 'Cancel' and 'OK' buttons.

User Management

## 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.

The screenshot shows the 'Time Policy' interface. On the left, there is a sidebar with a 'Create Policy' button and an 'Upgrade Schedule' button. The main area is titled 'Create Policy' and contains a warning message: 'If both weekly and absolute schedules are configured on the same day, only the absolute schedule will take effect.' Below this, there is a 'Policy Name' input field with the value 'Reboot Schedule'. Under the 'Weekly' section, there is a table with columns for days of the week and time slots. The 'Saturday' column is highlighted in blue. At the bottom, there is an 'Absolute Date / Time' section with two input fields: 'Please select date (multiple choices are allowed)' and 'Please select time (multiple choices are allowed)'. There are 'Cancel' and 'OK' buttons at the bottom right.

Time Policy

#### Note:

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

## 1588v2 TC

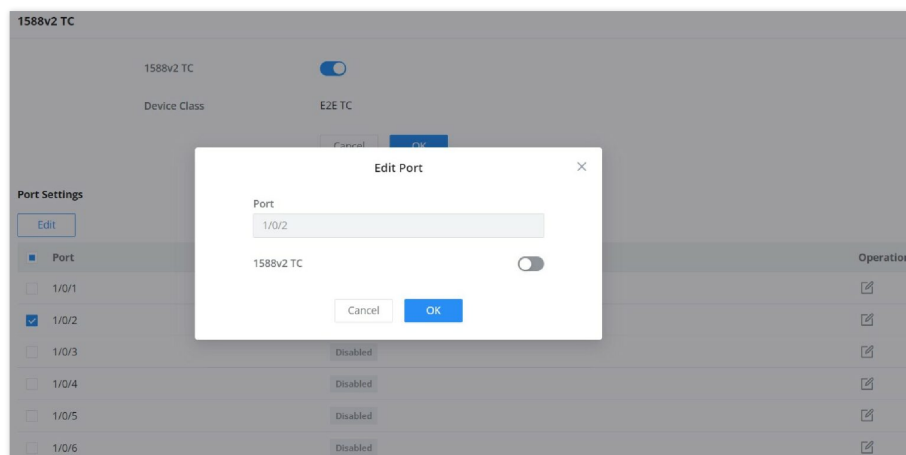
IEEE 1588v2, also known as Precision Time Protocol (PTP), is used to synchronize time across devices in a network.

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 multiple supported GWN780x Pro switch models to operate as a single logical unit, simplifying network management, increasing redundancy, and expanding port density. This feature is available only on the following models:

### Note:

**Supported Models:** GWN7806PL/PH 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

In this section, you can enable stack mode, assign a device ID and priority, and define the physical ports used for stacking.

**Stack Settings**

Stack ☒

Device ID  Valid range is 1-4

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

Stack Port 1

Stack Port 2

Cancel OK

### Stack Settings

#### Stack

Enable or disable stacking functionality.

- When enabled, this device becomes part of a stack group.
- Make sure the ports used are in shutdown status before configuration.
- Only 10G fiber modules are supported.

#### Note:

After setting and saving, reboot the switch to take effect. Cross connect the switches and power them on (it is recommended to power on the preset primary switch first) to form a stacking system.

#### Device ID

Unique identifier for the device in the stack.

- Range: **1–4**
- Must be **unique** across all devices in the same stack.

#### Note:

Device ID must be unique; otherwise switch cannot join the stack.

#### Priority

Sets the priority level for master election during stack formation.

- Range: **1–255**
- Higher value = higher priority

#### Stack Port 1 & Stack Port 2

Select the two physical ports to use for stacking interconnection.

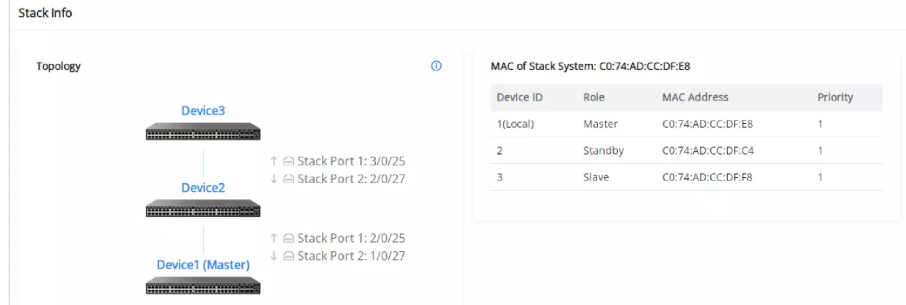
- Must be 10G ports
- Ensure that these ports are correctly cross-connected between switches

#### Note:

After configuring Stack settings, you must click Save and reboot the switch for changes to take effect.

## Stack Info

This page displays the current stack topology and status, including member switches and their roles (Master/Member), device IDs, priorities, and port mappings.



#### 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 1.0.15.219

*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.
-