GWN780x Switch Firmware Release Notes

IMPORTANT UPGRADING NOTE

1. GWN780x 1.0.5.52 requires GWN Manager version to be at least 1.1.28.27 or newer.
2. Once GWN780x is upgraded to firmware 1.0.5.x, downgrading to 1.0.3.x or lower firmware version is not allowed.
3. Once GWN780x is upgraded to firmware 1.0.3.x, downgrading to 1.0.1.x or lower firmware version is not allowed.
4. [6/15/2023] Regarding Cloud management, any switch version below 1.0.3.x does not support GWN Cloud provision (1.0.1.x only supports GWN Cloud remote tunneling to local web UI). Therefore, upgrade from 1.0.1.x to 1.0.3.x or above cannot be performed through GWN Cloud. Administrators need to either login to device locally or remote tunneling from Cloud, and then upgrade to 1.0.3.x through local web UI. After upgrade 1.0.3.x device can be managed or perform further upgrade through GWN Cloud.

Table of Content

FIRMWARE FILE DOWNLOAD

Individual firmware files are available for downloading at URL below:

https://www.grandstream.com/support/firmware

FIRMWARE VERSION 1.0.9.15

PRODUCT NAME

GWN7801(P) / GWN7802(P) / GWN7803(P)

DATE

8/29/2024

FIRMWARE FILE INFORMATION

- GWN780x Firmware file name: gwn780xfw.bin

  MD5 checksum: a14d3146d0002f11425d3eb6ef28a6f0

CHANGES/ENHANCEMENT

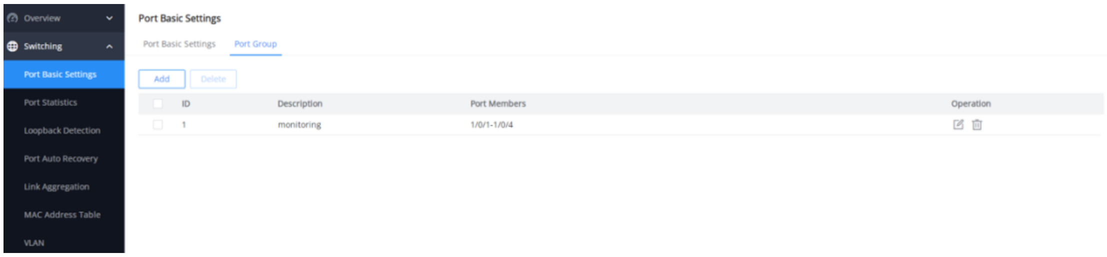
- Delete DAC cable configuration in Port Basic Settings.
- Delete 5s interval for port statistics.
- Added port groups.
- Added LLDP auto-config for Auto Voice VLAN mode in Voice VLAN.
- Added more features for STP, including ignore VLAN in BPDU, root protection and loopback protection.
- Added more OUI in Voice VLAN.
- Added IP configuration for MGMT VLAN.
- Added redirect to interface for ACE.
- Added VLAN binding to ACL function.
- Added mask for IPSG/IPv6SG.
- Added remote-ID configuration based on port for DHCP Snooping.
- Added entries fixed for DHCP/DHCPv6 Snooping.
- Added flow upgrade for upgrade via manual upgrade.
- Added more settings for logs, including minimum log level and log aggregation.
- Added Ping watchdog in diagnostics.

- Added connection diagnostics of GWN router.
- Added RSPAN, including port-based and ACL-based remotely mirroring.
- Added new SNMP Traps.
- Added 802.3bt info in LLDP.
- Added alert.
- Added management ACL, including hardware-based and software-based management ACL.
- Added Layer 3 discovery and management by GWN router.
- Added 1588v2 P2P TC.
- Added recovery function.
- Added NAS-Port-Type value 15 with alternate management VLAN.
- Added ability to shutdown port by profile group.
- Added support to ping from ports.
- Added ACL for VTY (SSH and telnet).
- Added additional Radius Access-Request Attributes.
- Optimized RIP/RIPng.
- Optimized CBS valid range in Queue Shaping.
- Optimized the rate limit groups from 32 to 128 in ACL.
- Fixed issue that high fan speed with a low load.
- Fixed issue that fans running non-stop at low temperature.
- Fixed DHCP's Option 82 is using wrong Circuit ID/Remote ID.
- Fixed internal bugs.

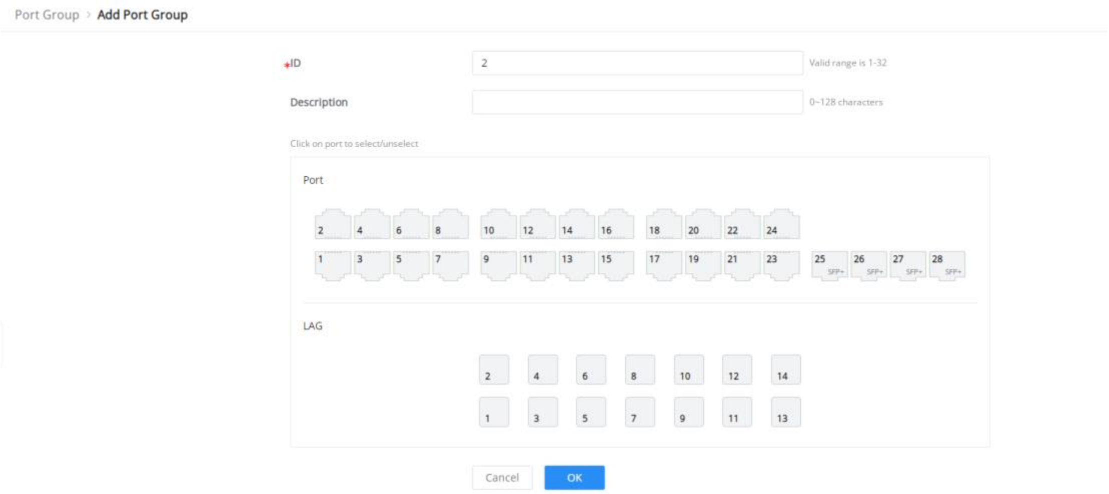
NEW FEATURE OVERVIEW

- **Add port groups**

Added port group settings to facilitate quick batch setting for port group ports.



□	ID	Description	Port Members	Operation
□	1	monitoring	1/0/1-1/0/4	

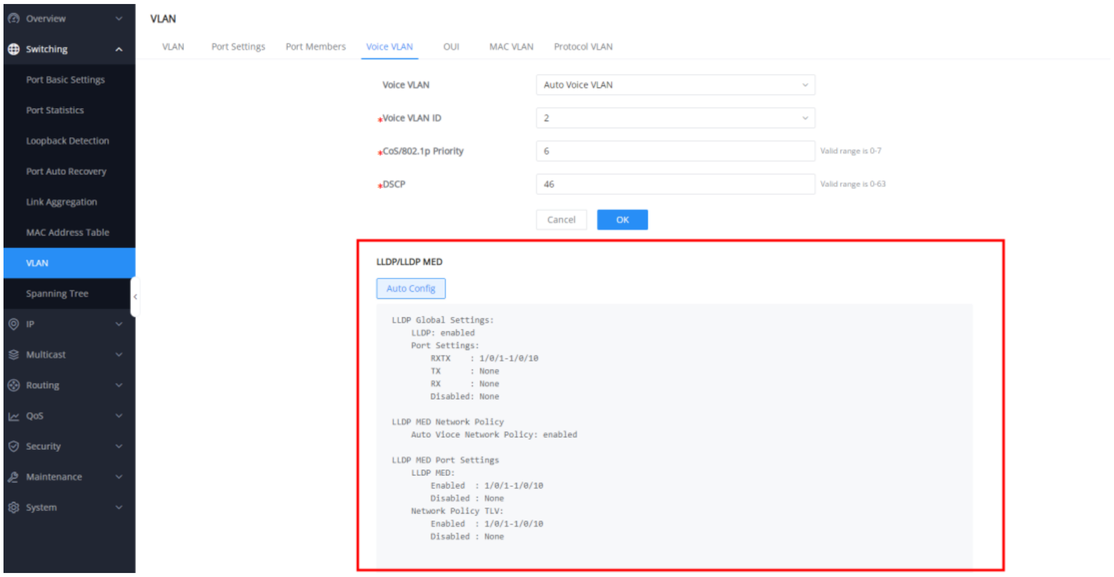

Port Group › Add Port Group
Click on port to select/unselect
Port
2 4 6 8 10 12 14 16 18 20 22 24
1 3 5 7 9 11 13 15 17 19 21 23 25 SFP+ 26 SFP+ 27 SFP+ 28 SFP+
LAG
2 4 6 8 10 12 14
1 3 5 7 9 11 13
Cancel
OK

*ID: 2 (Valid range is 1-32)

Description: (0~128 characters)

- **Added LLDP auto-config for Auto Voice VLAN mode in Voice VLAN**

  If you select Auto Voice VLAN for Voice VLAN mode, you need to go to LLDP to set network policies. LLDP automatic configuration is now added to voice VLANs, making it easier and faster for users to configure them with one click.



Voice VLAN: Auto Voice VLAN

*Voice VLAN ID: 2

*CoS/802.1p Priority: 6 (Valid range is 0-7)

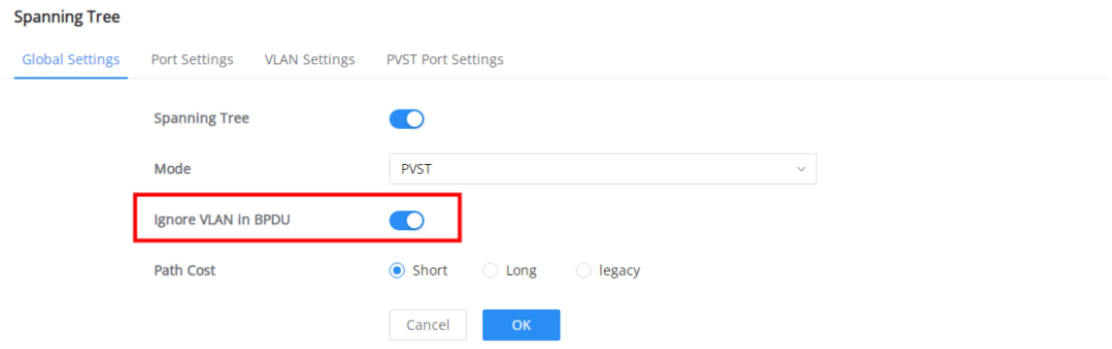
*DSCP: 46 (Valid range is 0-63)

```
LLDP Global Settings:
    LLDP: enabled
    Port Settings:
        RXTX    : 1/0/1-1/0/10
        TX      : None
        RX      : None
        Disabled: None

LLDP MED Network Policy
    Auto Vioce Network Policy: enabled

LLDP MED Port Settings
    LLDP MED:
        Enabled  : 1/0/1-1/0/10
        Disabled : None
    Network Policy TLV:
        Enabled  : 1/0/1-1/0/10
        Disabled : None
```

- **Added control over the processing of BPDU packets with VLANs.**



Spanning Tree

Global Settings | Port Settings | VLAN Settings | PVST Port Settings

Spanning Tree: On

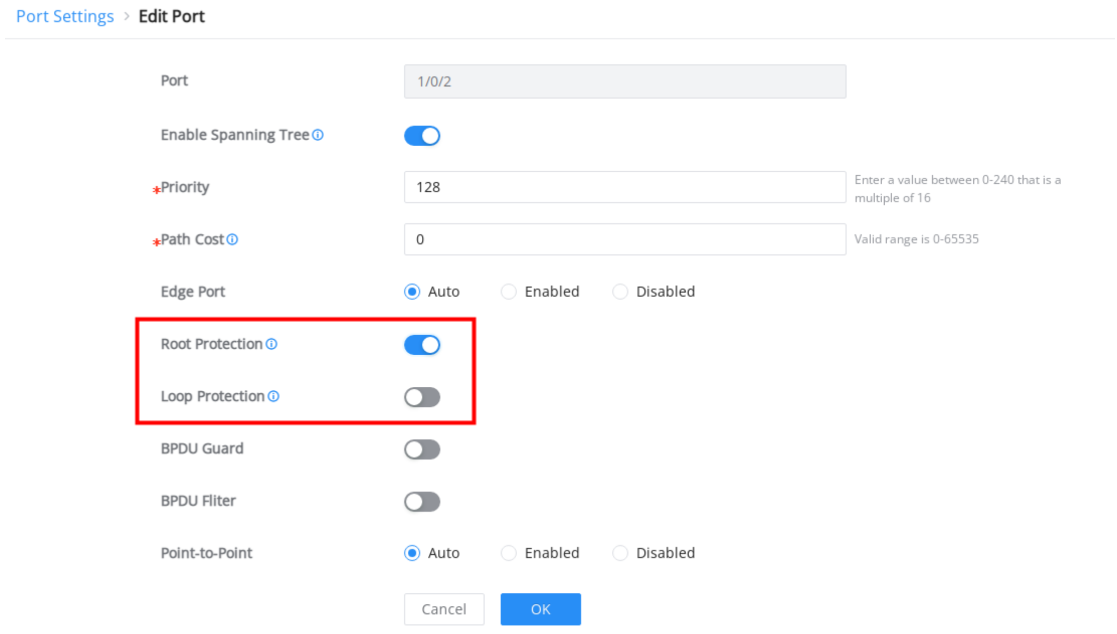
Mode: PVST

Ignore VLAN in BPDU: On

Path Cost: ● Short ○ Long ○ legacy

- **Added root protection and loopback protection for STP**

Root protection and loop protection are added to the port.
Note: Root protection and loop protection have one and only one can be enabled.



Port Settings > Edit Port

Port: 1/0/2

Enable Spanning Tree ⓘ: On

*Priority: 128 — Enter a value between 0-240 that is a multiple of 16

*Path Cost ⓘ: 0 — Valid range is 0-65535

Edge Port: ● Auto ○ Enabled ○ Disabled

Root Protection ⓘ: On

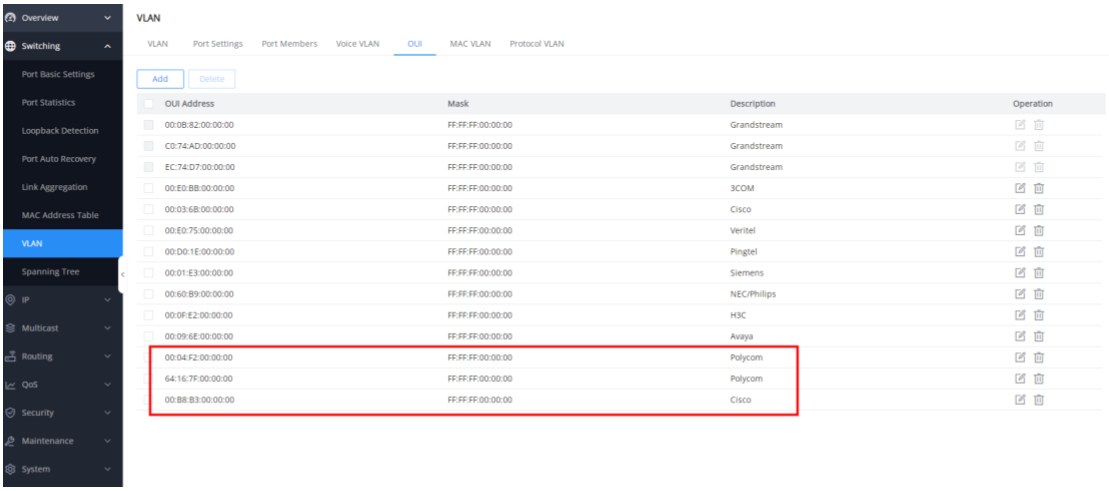
Loop Protection ⓘ: Off

BPDU Guard: Off

BPDU Fliter: Off

Point-to-Point: ● Auto ○ Enabled ○ Disabled

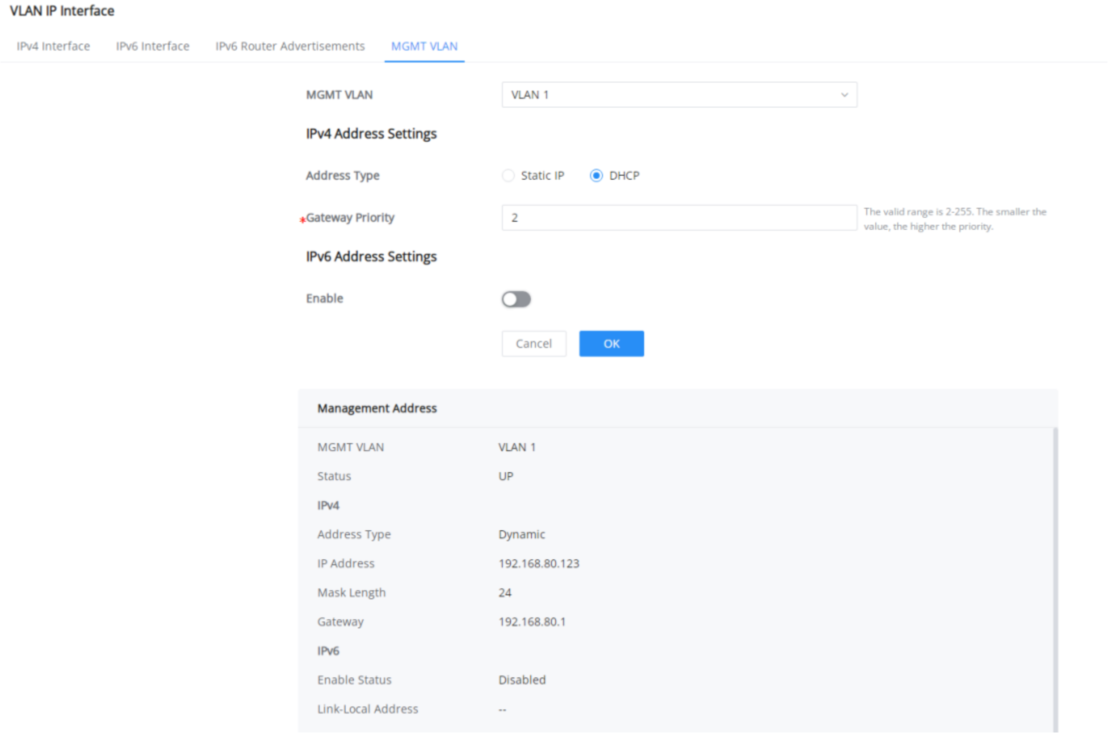
- **Added more OUI in Voice VLAN**



OUI Address	Mask	Description	Operation
00:0B:82:00:00:00	FF:FF:FF:00:00:00	Grandstream	
C0:74:AD:00:00:00	FF:FF:FF:00:00:00	Grandstream	
EC:74:D7:00:00:00	FF:FF:FF:00:00:00	Grandstream	
00:E0:BB:00:00:00	FF:FF:FF:00:00:00	3COM	
00:03:6B:00:00:00	FF:FF:FF:00:00:00	Cisco	
00:E0:75:00:00:00	FF:FF:FF:00:00:00	Veritel	
00:D0:1E:00:00:00	FF:FF:FF:00:00:00	Pingtel	
00:01:E3:00:00:00	FF:FF:FF:00:00:00	Siemens	
00:60:B9:00:00:00	FF:FF:FF:00:00:00	NEC/Philips	
00:0F:E2:00:00:00	FF:FF:FF:00:00:00	H3C	
00:09:6E:00:00:00	FF:FF:FF:00:00:00	Avaya	
00:04:F2:00:00:00	FF:FF:FF:00:00:00	Polycom	
64:16:7F:00:00:00	FF:FF:FF:00:00:00	Polycom	
00:B8:B3:00:00:00	FF:FF:FF:00:00:00	Cisco	

- **Added IP configuration for MGMT VLAN**

Adds the IP address configuration for the management VLAN interface and displays the result.
Note: The IP address configuration of the management VLAN interface is synchronized with the configuration of the corresponding VLAN interface in the IP interface.



MGMT VLAN: VLAN 1

IPv4 Address Settings

Address Type: ○ Static IP ● DHCP

*Gateway Priority: 2 — The valid range is 2-255. The smaller the value, the higher the priority.

IPv6 Address Settings

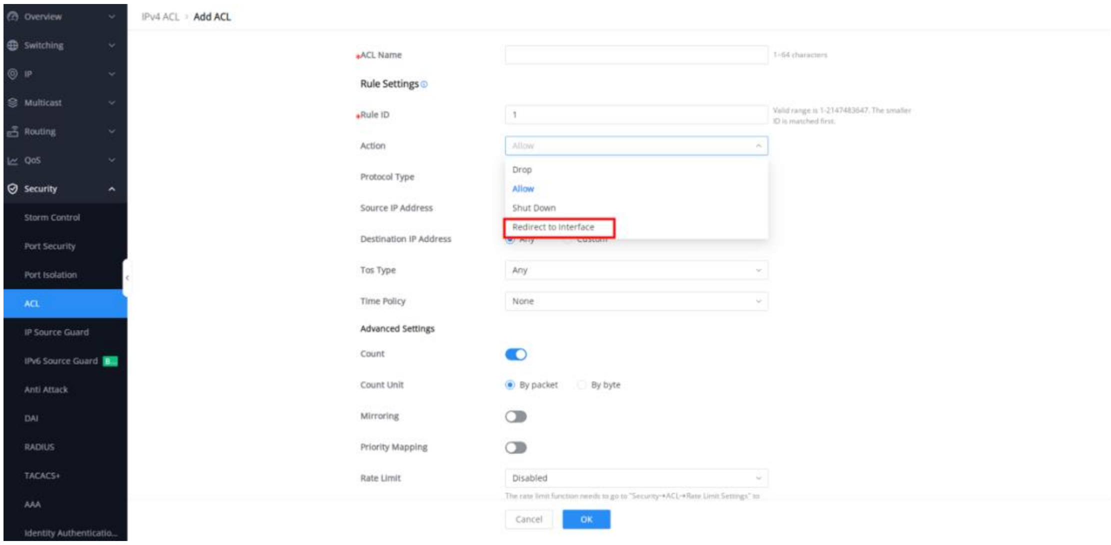
Enable: ○

Management Address

MGMT VLAN	VLAN 1
Status	UP
IPv4	
Address Type	Dynamic
IP Address	192.168.80.123
Mask Length	24
Gateway	192.168.80.1
IPv6	
Enable Status	Disabled
Link-Local Address	--

- **Added redirect to interface for ACE**

The function of redirecting ACL rules to interfaces is added.
Note: The selected interface does not contain the interface bound by the ACL.



*ACL Name: (1~64 characters)

Rule Settings

*Rule ID: 1 (Valid range is 1-2147483647. The smaller ID is matched first.)

Action: Allow

Protocol Type

Source IP Address

Destination IP Address

Tos Type: Any

Time Policy: None

Advanced Settings

Count: on

Count Unit: ● By packet ○ By byte

Mirroring: off

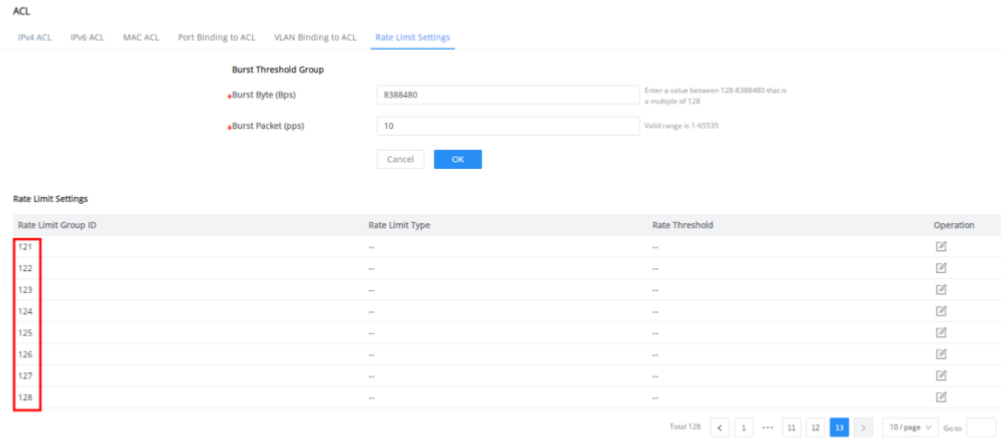
Priority Mapping: off

Rate Limit: Disabled

The rate limit function needs to go to "Security→ACL→Rate Limit Settings" to

- **Optimized the rate limit groups from 32 to128 in ACL**

The ACL rate limit group has been expanded from 32 groups to 128 groups.



Burst Threshold Group

*Burst Byte (Bps): 8388480 (Enter a value between 128-8388480 that is a multiple of 128)

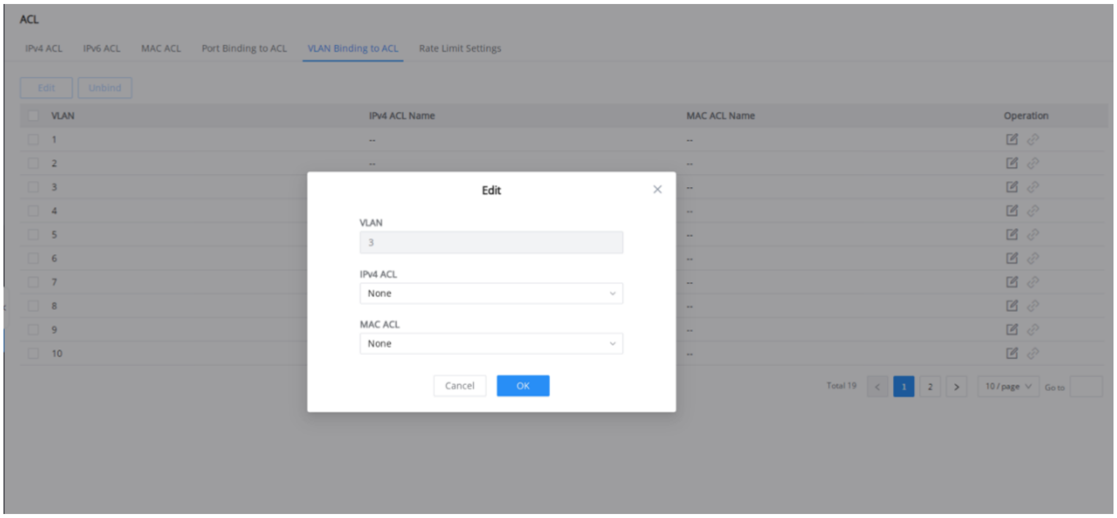
*Burst Packet (pps): 10 (Valid range is 1-65535)

Rate Limit Settings

Rate Limit Group ID	Rate Limit Type	Rate Threshold	Operation
121	--	--	
122	--	--	
123	--	--	
124	--	--	
125	--	--	
126	--	--	
127	--	--	
128	--	--	

- **Added VLAN binding to ACL function**

Added the binding of ACLs to VLANs.
Note: The binding of IPv6 ACLs to VLANs is not supported.



ACL

VLAN	IPv4 ACL Name	MAC ACL Name	Operation
1	--	--	
2	--	--	
3		--	
4		--	
5		--	
6		--	
7		--	
8		--	
9		--	
10		--	

Total 19

Edit

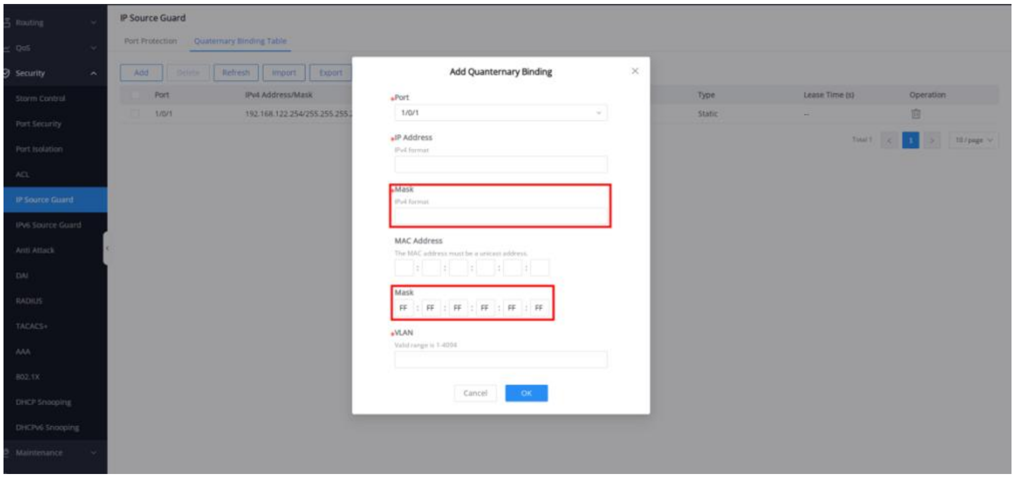
VLAN: 3

IPv4 ACL: None

MAC ACL: None

- **Added mask configuration for IPSG/IPv6SG**

In the quaternary binding table of IPSG and IPv6SG, the mask configuration is added for the IP address and MAC address to expand the coverage of the binding table.



IP Source Guard

Port	IPv4 Address/Mask	Type	Lease Time (s)	Operation
1/0/1	192.168.122.254/255.255.255.	Static	--	

Total 1

Add Quanternary Binding

*Port: 1/0/1

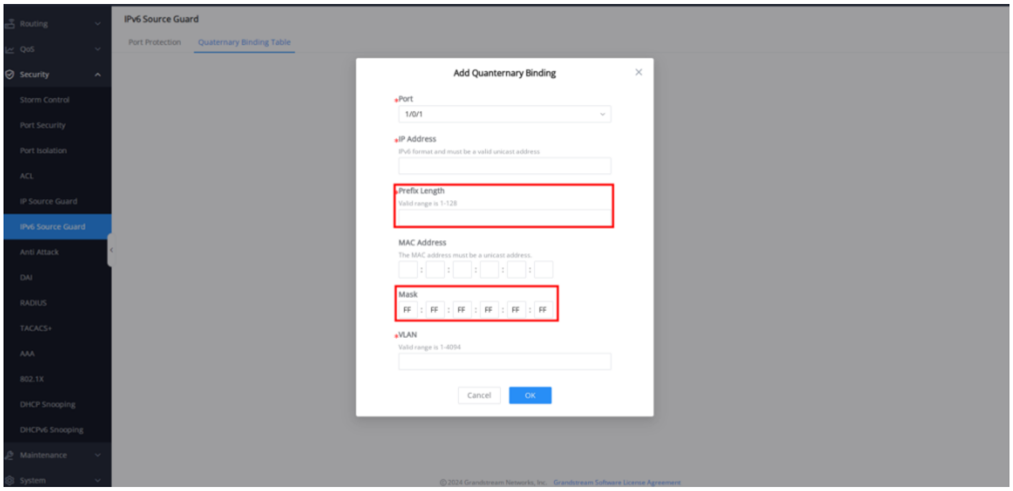
*IP Address: IPv4 format

*Mask: IPv4 format

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

Mask: FF : FF : FF : FF : FF : FF

*VLAN: Valid range is 1-4094



Add Quanternary Binding

*Port: 1/0/1

*IP Address: IPv6 format and must be a valid unicast address

*Prefix Length: Valid range is 1-128

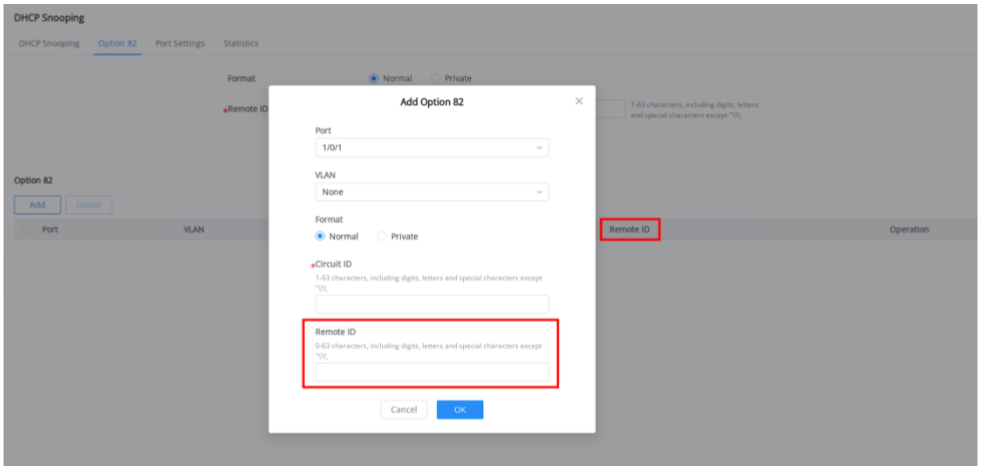
MAC Address: The MAC address must be a unicast address.

Mask: FF : FF : FF : FF : FF : FF

*VLAN: Valid range is 1-4094

- **Added remote-ID configuration based on port for DHCP Snooping**

Added use of port-based configuration for remote IDs.



Format: ● Normal ○ Private

*Remote ID: 1-63 characters, including digits, letters and special characters except "\?/,

Add Option 82

Port: 1/0/1

VLAN: None

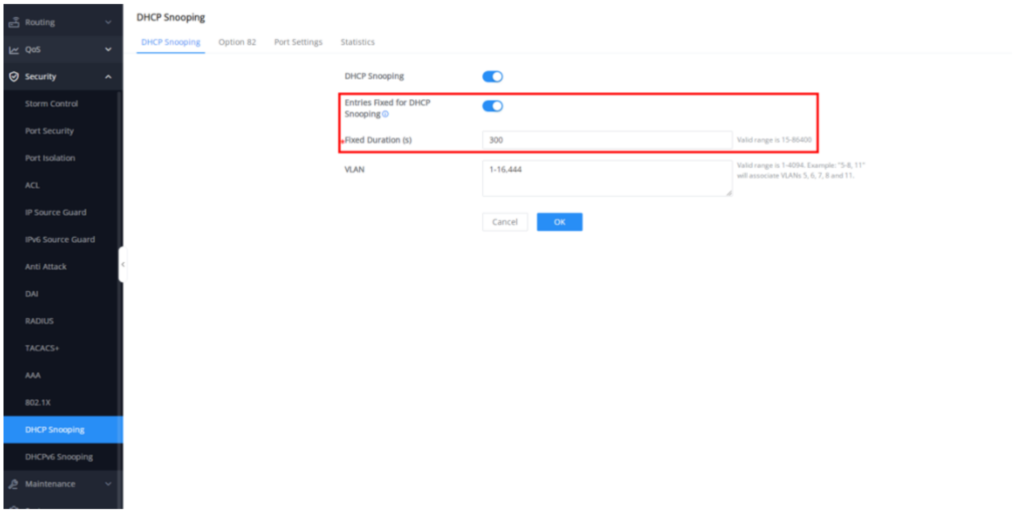
Format: ● Normal ○ Private

*Circuit ID: 1-63 characters, including digits, letters and special characters except "\?/,

Remote ID: 0-63 characters, including digits, letters and special characters except "\?/,

- **Added entries fixed for DHCP/DHCPv6 Snooping**

Added the entry fixing function for DHCP/DHCPv6 Snooping. Once enabled, the dynamic binding table of the IPSG/IPv6SG is automatically restored when the device restarts. Once turned on, the curing cycle needs to be set.



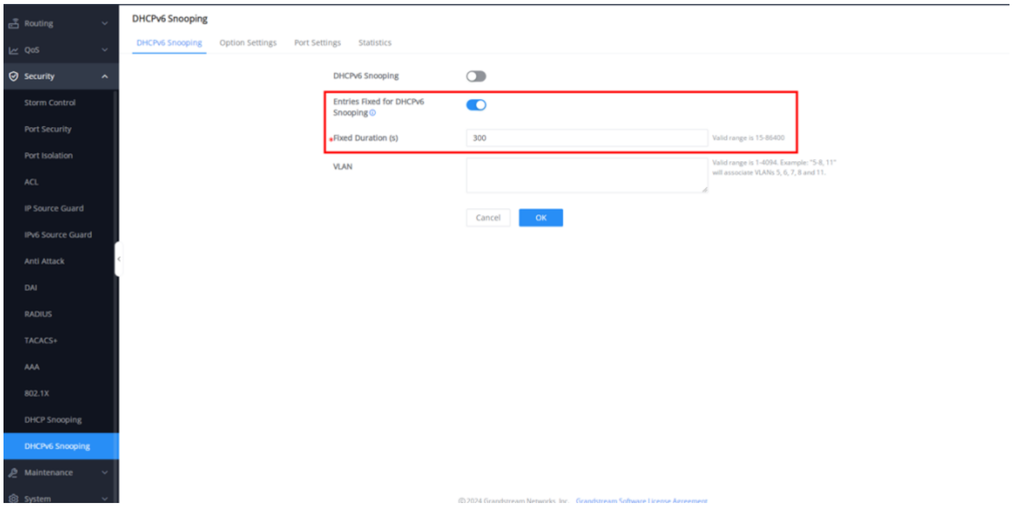
DHCP Snooping

DHCP Snooping ●

Entries Fixed for DHCP Snooping ●

*Fixed Duration (s) 300 Valid range is 15-86400

VLAN 1-16,444 Valid range is 1-4094. Example: "5-8, 11" will associate VLANs 5, 6, 7, 8 and 11.



DHCPv6 Snooping

DHCPv6 Snooping ○

Entries Fixed for DHCPv6 Snooping ●

*Fixed Duration (s) 300 Valid range is 15-86400

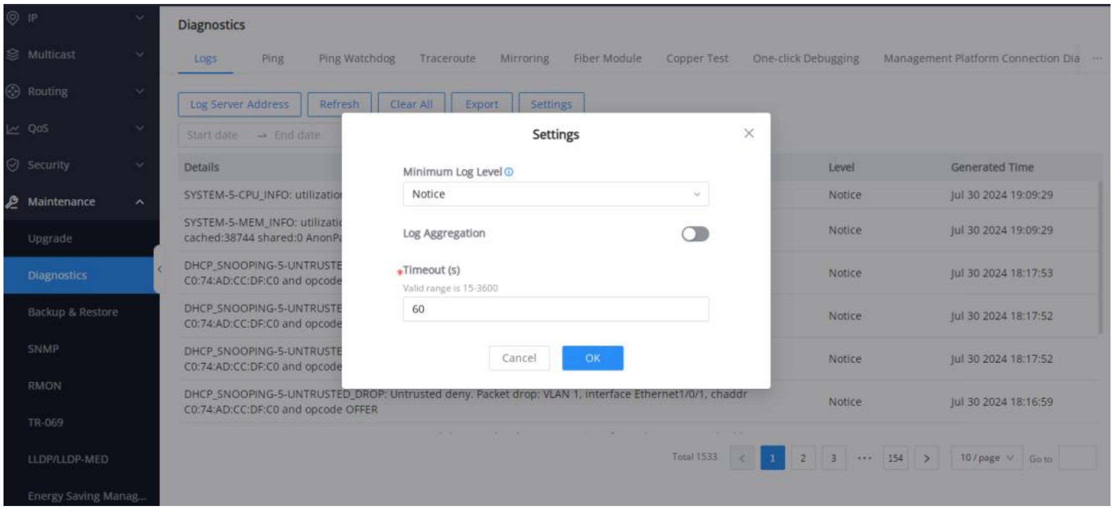
VLAN Valid range is 1-4094. Example: "5-8, 11" will associate VLANs 5, 6, 7, 8 and 11.

- **Added flow upgrade for upgrade via manual upload**

  Considering the memory problem of the device, the upload upgrade supports streaming upgrade, and the upgrade is carried out while uploading.

- **Added more settings for logs**

  Increase the minimum print level of web logs.
  The log aggregation function is added to merge and display the same logs within a certain period.



Settings

Minimum Log Level: Notice

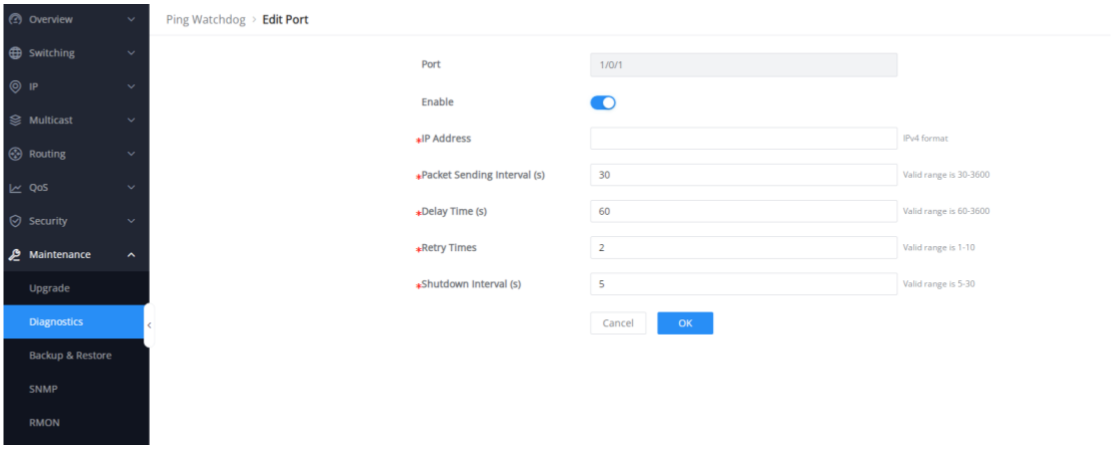
Log Aggregation: off

*Timeout (s): 60 (Valid range is 15-3600)

Details	Level	Generated Time
SYSTEM-5-CPU_INFO: utilizatio	Notice	Jul 30 2024 19:09:29
SYSTEM-5-MEM_INFO: utilizati cached:38744 shared:0 AnonP	Notice	Jul 30 2024 19:09:29
DHCP_SNOOPING-5-UNTRUSTE C0:74:AD:CC:DF:C0 and opcode	Notice	Jul 30 2024 18:17:53
DHCP_SNOOPING-5-UNTRUSTE C0:74:AD:CC:DF:C0 and opcode	Notice	Jul 30 2024 18:17:52
DHCP_SNOOPING-5-UNTRUSTE C0:74:AD:CC:DF:C0 and opcode	Notice	Jul 30 2024 18:17:52
DHCP_SNOOPING-5-UNTRUSTED_DROP: Untrusted deny. Packet drop: VLAN 1, interface Ethernet1/0/1, chaddr C0:74:AD:CC:DF:C0 and opcode OFFER	Notice	Jul 30 2024 18:16:59

- **Added Ping watchdog in diagnostics**

The port Ping watchdog function is added to automatically inflate the device by automatically detecting problems such as device crashes and faults to help solve the problem of unresponsive device failures in the environment



Port: 1/0/1

Enable: on

*IP Address: (IPv4 format)

*Packet Sending Interval (s): 30 (Valid range is 30-3600)

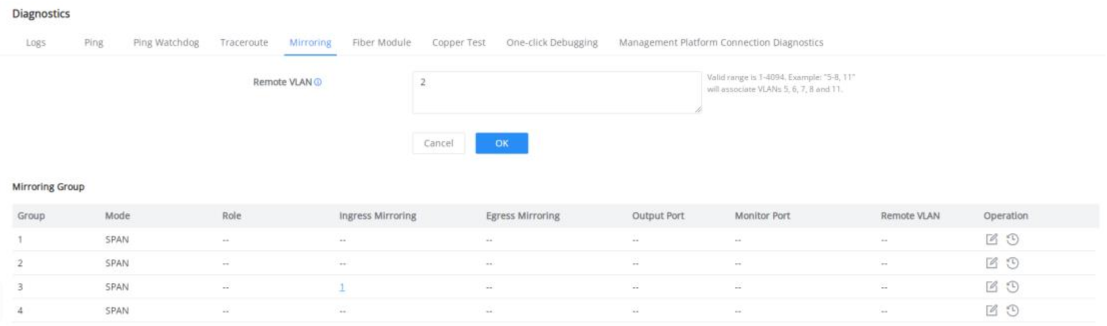
*Delay Time (s): 60 (Valid range is 60-3600)

*Retry Times: 2 (Valid range is 1-10)

*Shutdown Interval (s): 5 (Valid range is 5-30)

- **Added RSPAN, including port-based and ACL-based remotely mirroring**

Added support for remote mirroring.
Remote VLANs are used to transmit mirrored packets. In general, VLAN 1 is not recommended



Remote VLAN: 2

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

Mirroring Group

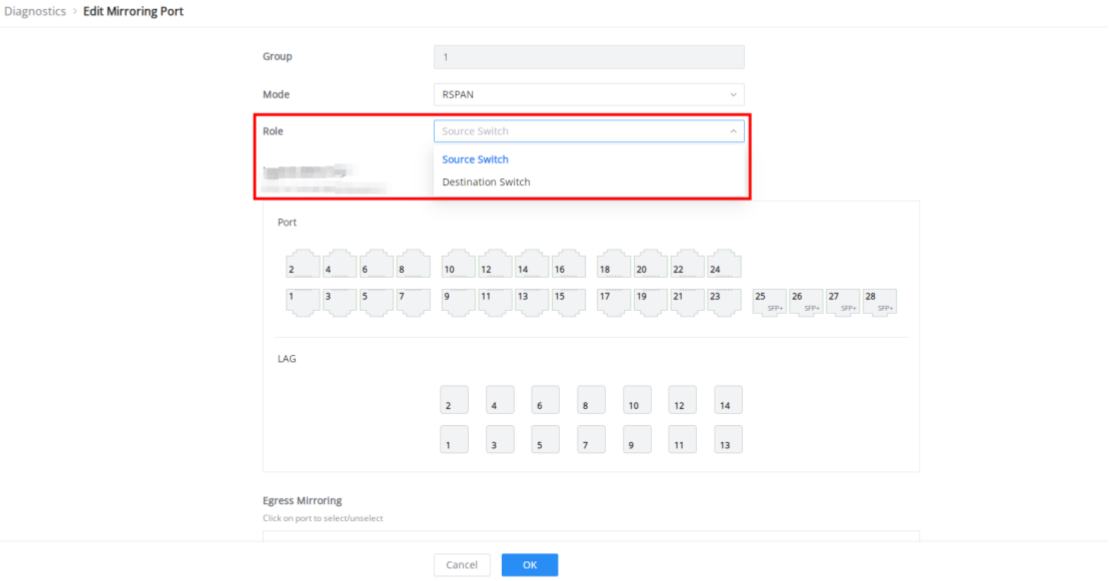
Group	Mode	Role	Ingress Mirroring	Egress Mirroring	Output Port	Monitor Port	Remote VLAN	Operation
1	SPAN	--	--	--	--	--	--	
2	SPAN	--	--	--	--	--	--	
3	SPAN	--	1	--	--	--	--	
4	SPAN	--	--	--	--	--	--	

Port-based RSPAN for remote mirroring:

Set up a mirror group. When you select RSPAN, you need to select the switch role.

If you use the source switch, you need to set the mirroring port, output port, and remote VLAN.

If you want to use the destination switch, you need to configure the source port, observation port, and remote VLAN


Diagnostics > Edit Mirroring Port
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
Click on port to select/unselect
Cancel
OK

Group: 1

Mode: RSPAN

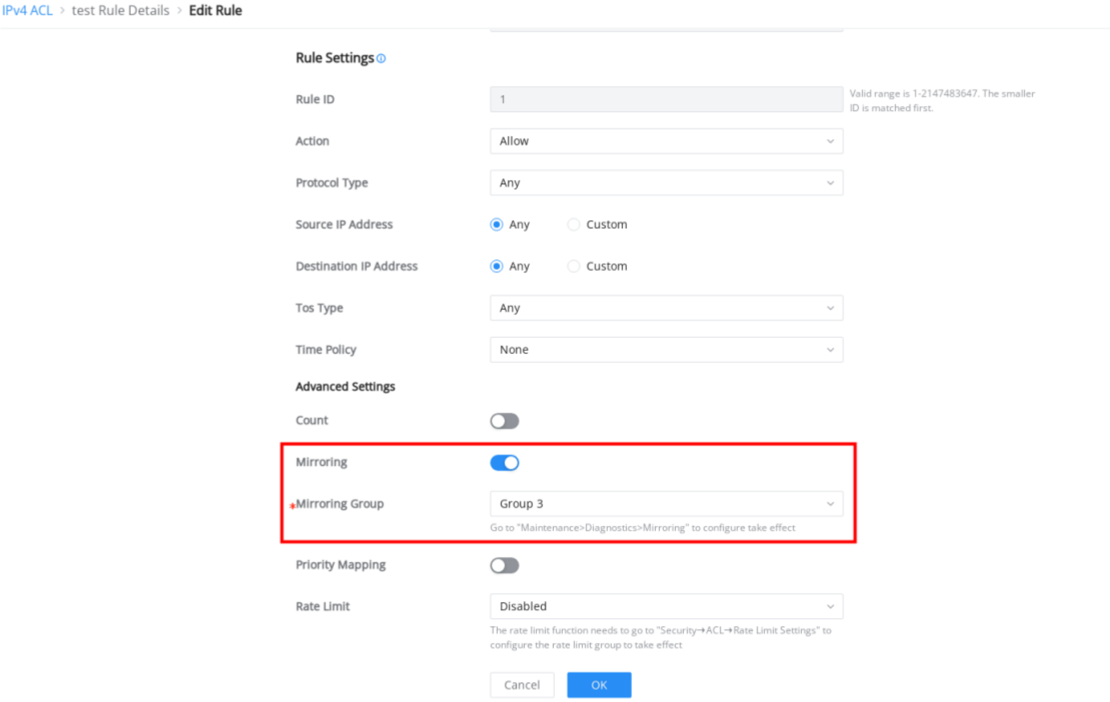
Role: Source Switch

- Source Switch
- Destination Switch

Egress Mirroring

Flow-based (ACL)-based RSPAN:

Select an image group in ACL Image



IPv4 ACL > test Rule Details > Edit Rule

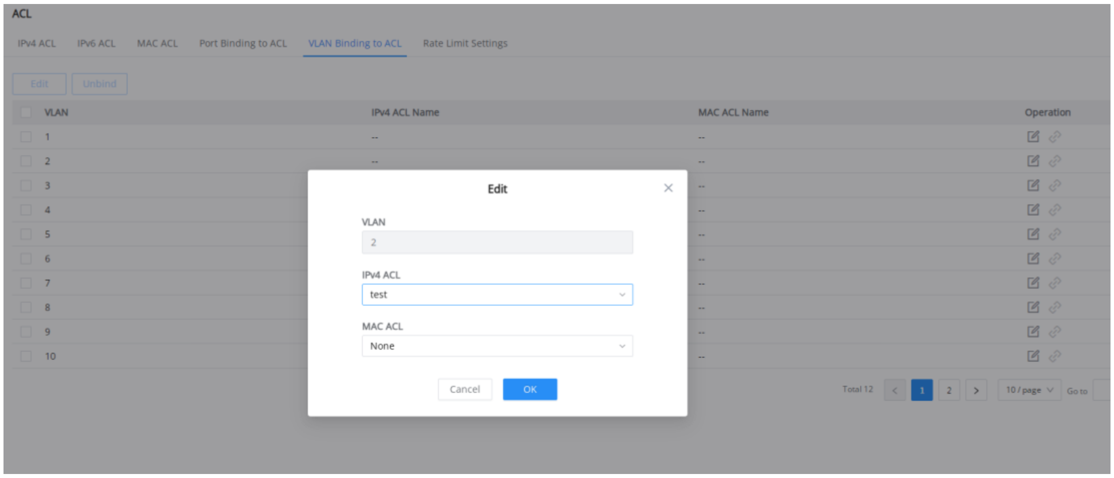
Rule Settings

Rule ID	1	Valid range is 1-2147483647. The smaller ID is matched first.
Action	Allow	
Protocol Type	Any	
Source IP Address	● Any ○ Custom	
Destination IP Address	● Any ○ Custom	
Tos Type	Any	
Time Policy	None	

Advanced Settings

Count	Off
Mirroring	On
*Mirroring Group	Group 3 Go to "Maintenance>Diagnostics>Mirroring" to configure take effect
Priority Mapping	Off
Rate Limit	Disabled The rate limit function needs to go to "Security→ACL→Rate Limit Settings" to configure the rate limit group to take effect

Then, select the corresponding port/VLAN binding ACL in the VLAN Binding ACL



ACL

VLAN	IPv4 ACL Name	MAC ACL Name	Operation
1	--	--	
2	--	--	
3		--	
4		--	
5		--	
6		--	
7		--	
8		--	
9		--	
10		--	

Total 12

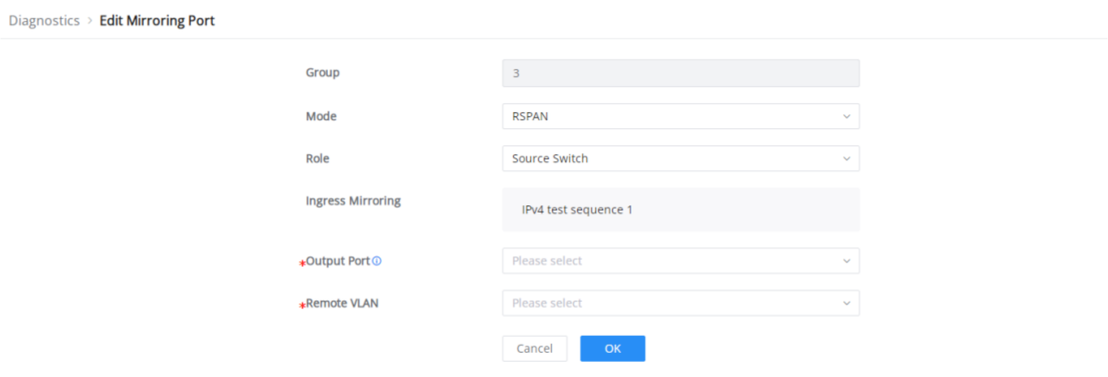
Edit

VLAN: 2

IPv4 ACL: test

MAC ACL: None

Then go to 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.



Group: 3

Mode: RSPAN

Role: Source Switch

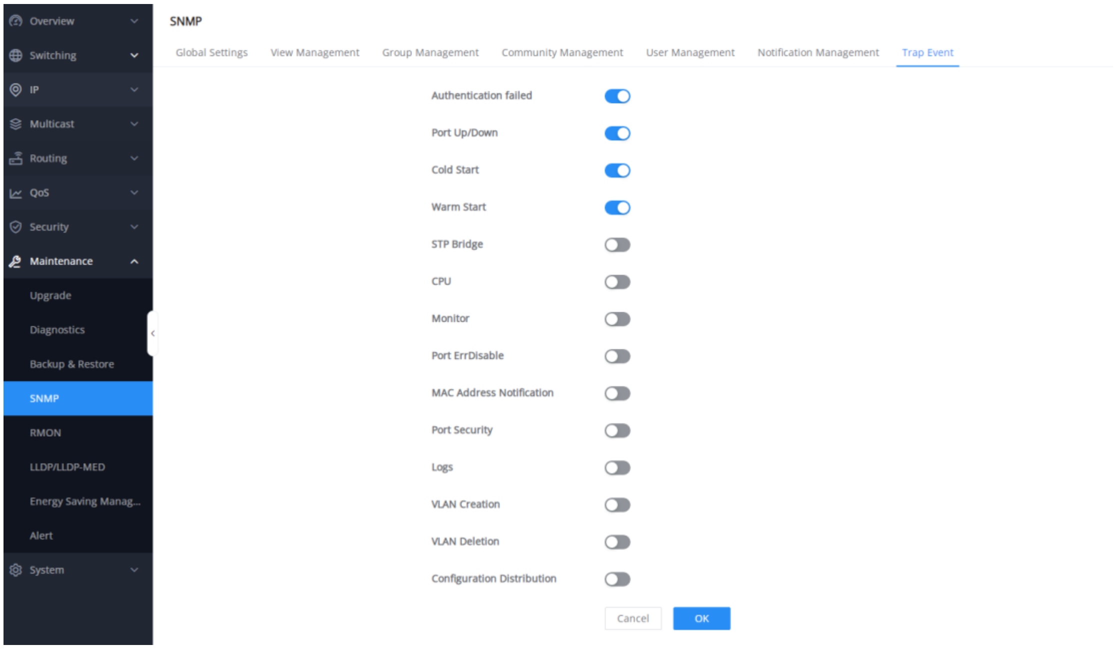
Ingress Mirroring: IPv4 test sequence 1

*Output Port: Please select

*Remote VLAN: Please select

- **Added new traps in SNMP**

Add more traps.



Authentication failed ☑

Port Up/Down ☑

Cold Start ☑

Warm Start ☑

STP Bridge ☐

CPU ☐

Monitor ☐

Port ErrDisable ☐

MAC Address Notification ☐

Port Security ☐

Logs ☐

VLAN Creation ☐

VLAN Deletion ☐

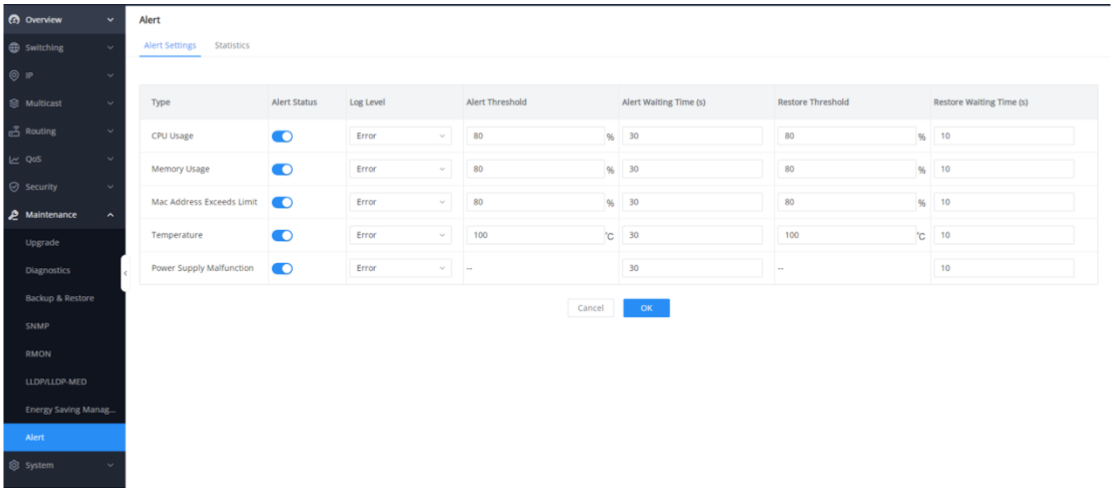
Configuration Distribution ☐

- **Added 802.3bt info in LLDP**

Port and neighbor information: Add 802.3 bt power supply information.

- **Added alert**

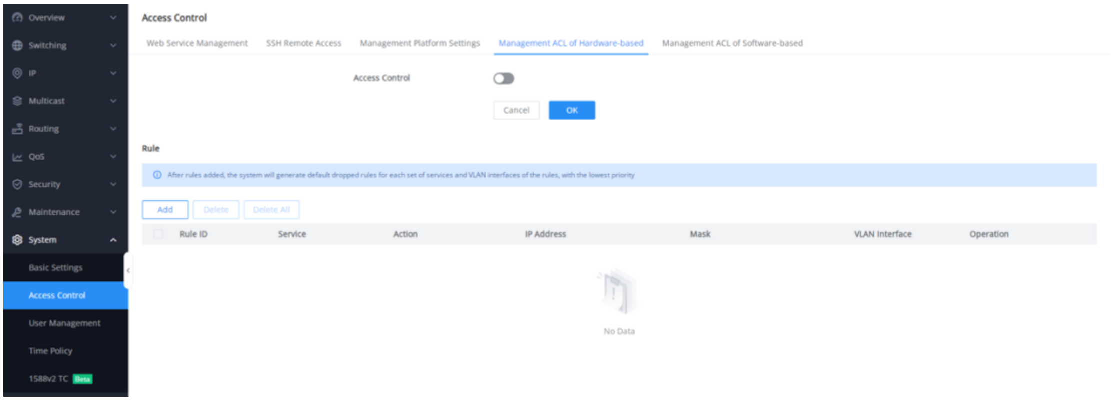
Local alarms are added, including CPU usage, memory usage, MAC address exceeding the limit, and temperature.



Type	Alert Status	Log Level	Alert Threshold	Alert Waiting Time (s)	Restore Threshold	Restore Waiting Time (s)
CPU Usage	●	Error	80 %	30	80 %	10
Memory Usage	●	Error	80 %	30	80 %	10
Mac Address Exceeds Limit	●	Error	80 %	30	80 %	10
Temperature	●	Error	100 ℃	30	100 ℃	10
Power Supply Malfunction	●	Error	--	30	--	10

- **Added management ACL, including hardware-based and software-based management ACL**

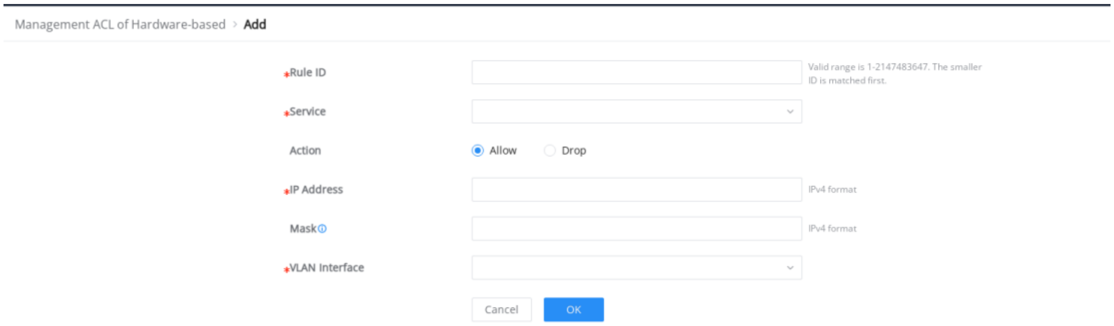
Hardware management ACLs and software management ACLs are added.
Hardware management ACL: The hardware-level management ACL is checked before the CPU is sent to reduce unnecessary resource consumption.



Access Control ○

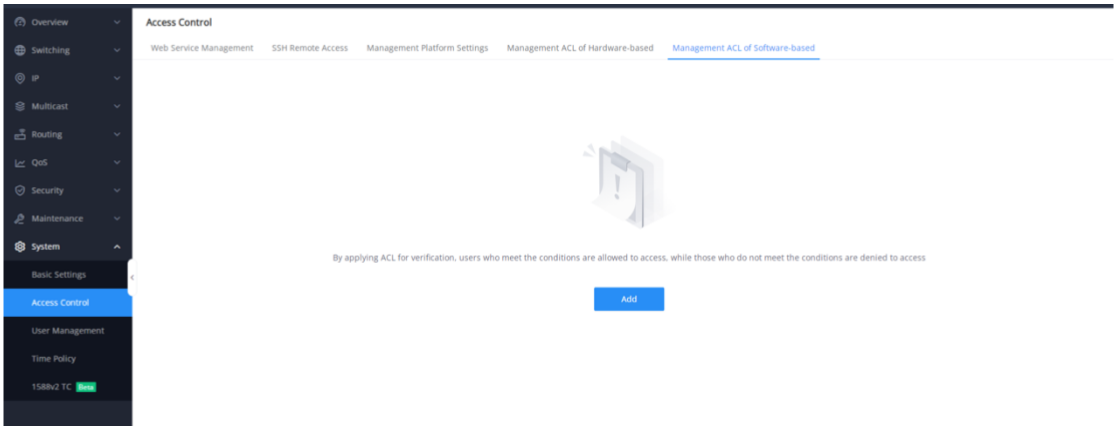
ⓘ After rules added, the system will generate default dropped rules for each set of services and VLAN interfaces of the rules, with the lowest priority

□	Rule ID	Service	Action	IP Address	Mask	VLAN Interface	Operation



*Rule ID		Valid range is 1-2147483647. The smaller ID is matched first.
*Service		
Action	● Allow ○ Drop	
*IP Address		IPv4 format
Mask ⓘ		IPv4 format
*VLAN Interface		

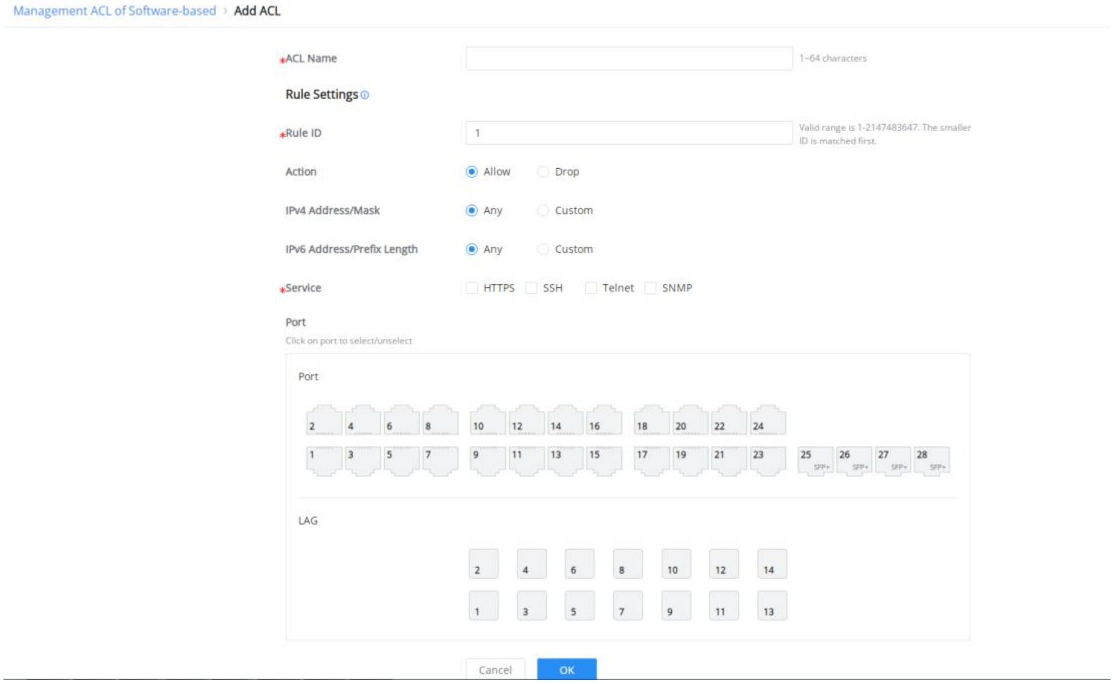
Software management ACL: Use firewall-like settings to control user access.



Access Control

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

By applying ACL for verification, users who meet the conditions are allowed to access, while those who do not meet the conditions are denied to access



Management ACL of Software-based › Add ACL

*ACL Name [ ] 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

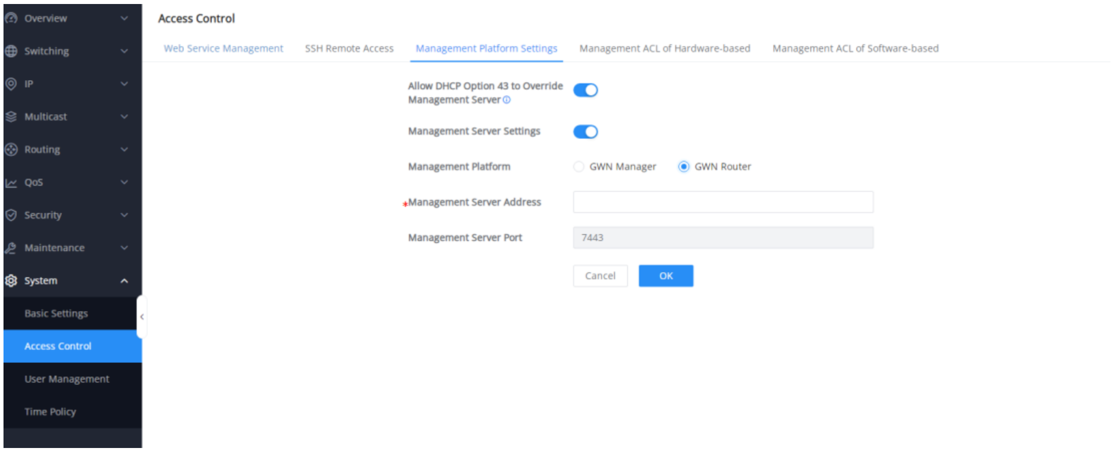
IPv6 Address/Prefix Length ● Any ○ Custom

*Service □ HTTPS □ SSH □ Telnet □ SNMP

Port
Click on port to select/unselect

- **Added Layer 3 discovery and management by GWN router**

  Layer 3 discovery of switches by cross-network segments and GWN routers is added. You need to set the Layer 3 server address and port on the switch.



Access Control

Allow DHCP Option 43 to Override Management Server: On

Management Server Settings: On

Management Platform: ○ GWN Manager ● GWN Router

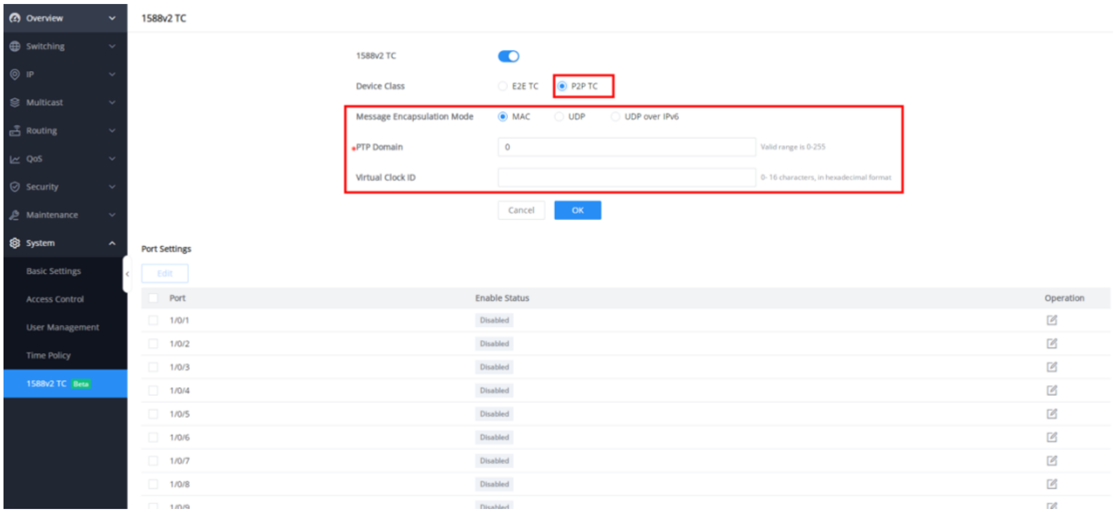
*Management Server Address:

Management Server Port: 7443

- **Added 1588v2 P2P TC**

Added 1588v2 P2P TC function.

Note: GWN7806(P)/1X takes effect for electrical ports, and GWN7830/31 takes effect for SFP ports (the Web UI should not be open yet).



1588v2 TC

1588v2 TC: On

Device Class: ○ E2E TC ● P2P TC

Message Encapsulation Mode: ● MAC ○ UDP ○ UDP over IPv6

*PTP Domain: 0 Valid range is 0-255

Virtual Clock ID: 0- 16 characters, in hexadecimal format

Port Settings

□	Port	Enable Status	Operation
□	1/0/1	Disabled	✎
□	1/0/2	Disabled	✎
□	1/0/3	Disabled	✎
□	1/0/4	Disabled	✎
□	1/0/5	Disabled	✎
□	1/0/6	Disabled	✎
□	1/0/7	Disabled	✎
□	1/0/8	Disabled	✎
□	1/0/9	Disabled	✎

- **Added recovery function**

When the device fails to boot, you can use the recovery function.

For details, see the Recovery User Guide.

FIRMWARE VERSION 1.0.5.61

PRODUCT NAME

GWN7801(P) / GWN7802(P) / GWN7803(P)

DATE

8/5/2024

FIRMWARE FILE INFORMATION

- GWN780x Firmware file name: gwn780xfw.bin

  MD5 checksum: 28cf361717a335c281ed3d8aacb6c163

CHANGES/ENHANCEMENT

- Optimized memory fragmentation caused by frequent configuration changes.
- Adjust the maximum length of the command line to 2000.
- Optimized searching for Web GUI.
- Optimized CPU and memory usage in Web GUI.
- Optimized device IP address display.
- Optimized trunk port settings.
- Optimized DHCP server and DHCP relay.
- Optimized DHCP option 43 settings for DHCP server.
- Optimized routing table.
- Optimized remote ID and Circuit ID for DHCP Snooping.
- Optimized EEE.
- Optimize GWN Manager settings.
- Added more port details such as neighbor and PoE power history info.
- Added port scheduled enabling feature.
- Added more port statistics info.

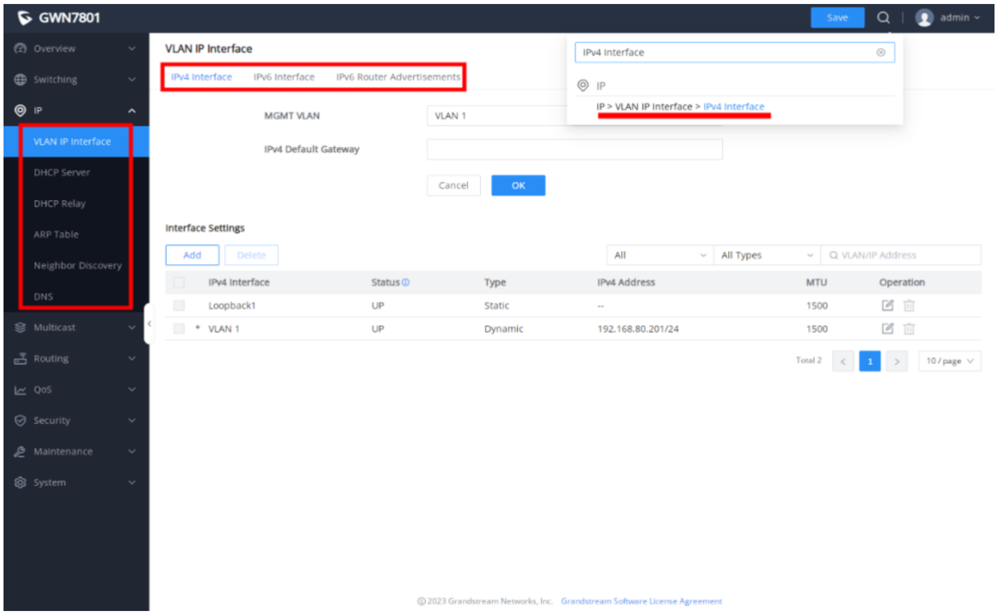
- Added loopback detection.
- Added support for QinQ.
- Added MAC-based VLAN.
- Added protocol-based VLAN.
- Added VLAN translation.
- Added untagged OUI mode for voice VLAN.
- Added gateway priority when using DHCP to get VLAN IP address.
- Added default gateway configuration under MGMT VLAN.
- Added ACL advanced settings, including mirroring, statistic and priority remapping for rule.
- Added rate limit by ACL binding to VLAN.
- Added import/export IPSG binding table for IP Source Guard.
- Added IPv6 Source Guard.
- Added mask for IPSG/IPv6SG.
- Added MAC bypass authentication.
- Added DHCPv6 Snooping.
- Added entries fixed for DHCP/DHCPv6 Snooping.
- Added upgrade by FTP and Explicit FTPS.
- Added connection diagnostics with GWN.Cloud/Manager.
- Add DST mode for time settings.
- Add HTTPS/SSH port customization.
- Add GWN Manager takeover function.
- Added support to see switch clients and other information.
- Fixed the issue when using STP, connected switch reboots might cause the entire system loses internet connectivity.
- Fixed the issue that the network packets show wrong Circuit ID/Remote ID of DHCP's Option 82.
- Fixed the issue that the device fails to pair with the GWN Manager.
- Fixed issue that Polycom devices failed to assume the Voice VLAN through LLDP-MED.

- Expanded DHCP leases range up to 11520 min
- Some internal bugs fixed.

NEW FEATURE OVERVIEW

- **Optimize searching for WEB GUI**

A secondary TAB on the left and a TAB at the top of a specific page have been added to support direct jump to a specified page.



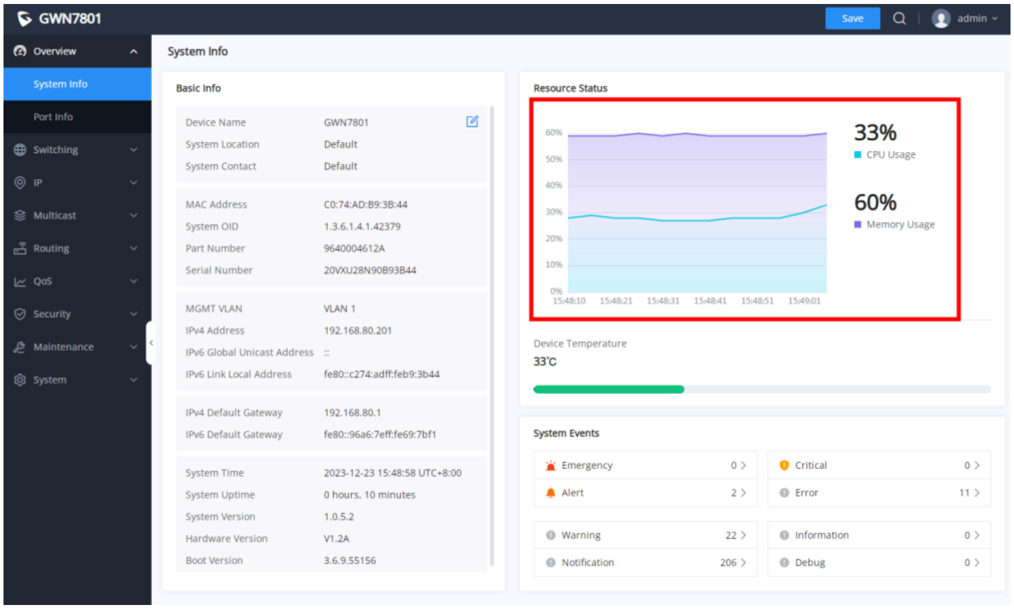
MGMT VLAN: VLAN 1

IPv4 Default Gateway:

	IPv4 Interface	Status	Type	IPv4 Address	MTU	Operation
□	Loopback1	UP	Static	--	1500	
□	* VLAN 1	UP	Dynamic	192.168.80.201/24	1500	

- **Optimize CPU and memory usage in Web GUI**

Supports viewing historical information of CPU and memory and assists in checking problems of high CPU and memory usage.



System Info

Basic Info

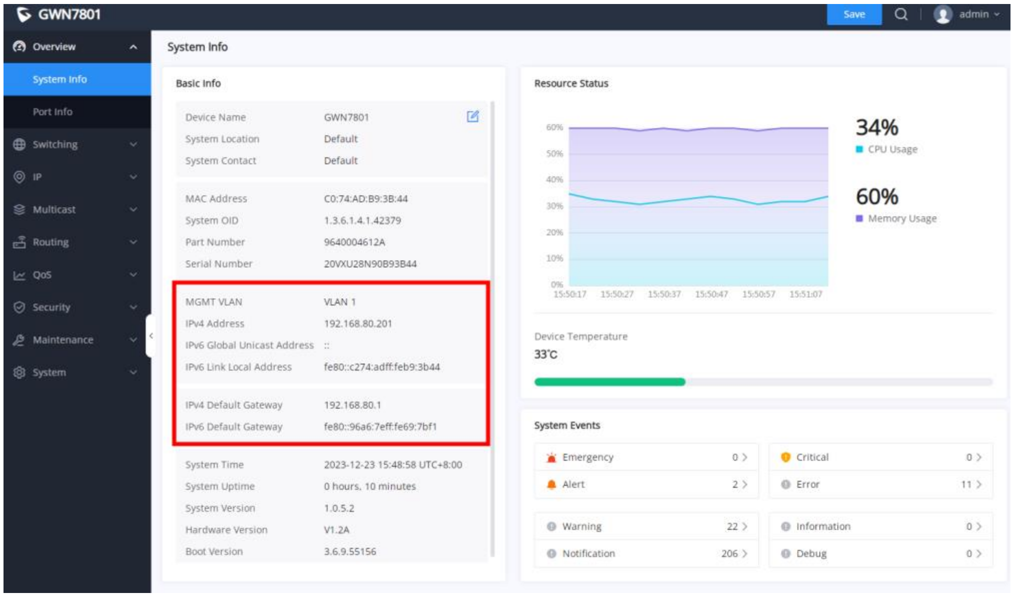
Device Name	GWN7801
System Location	Default
System Contact	Default
MAC Address	C0:74:AD:B9:3B:44
System OID	1.3.6.1.4.1.42379
Part Number	9640004612A
Serial Number	20VXU28N90B93B44
MGMT VLAN	VLAN 1
IPv4 Address	192.168.80.201
IPv6 Global Unicast Address	::
IPv6 Link Local Address	fe80::c274:adff:feb9:3b44
IPv4 Default Gateway	192.168.80.1
IPv6 Default Gateway	fe80::96a6:7eff:fe69:7bf1
System Time	2023-12-23 15:48:58 UTC+8:00
System Uptime	0 hours, 10 minutes
System Version	1.0.5.2
Hardware Version	V1.2A
Boot Version	3.6.9.55156

Device Temperature
33℃

Emergency	0 >	Critical	0 >
Alert	2 >	Error	11 >
Warning	22 >	Information	0 >
Notification	206 >	Debug	0 >

- **Optimize device IP address display**

Displays the IP address information of the management VLAN, including the IPv4 address, IPv6 link-local address, and global unicast address, and also displays the switch default gateway address.



System Info

Basic Info

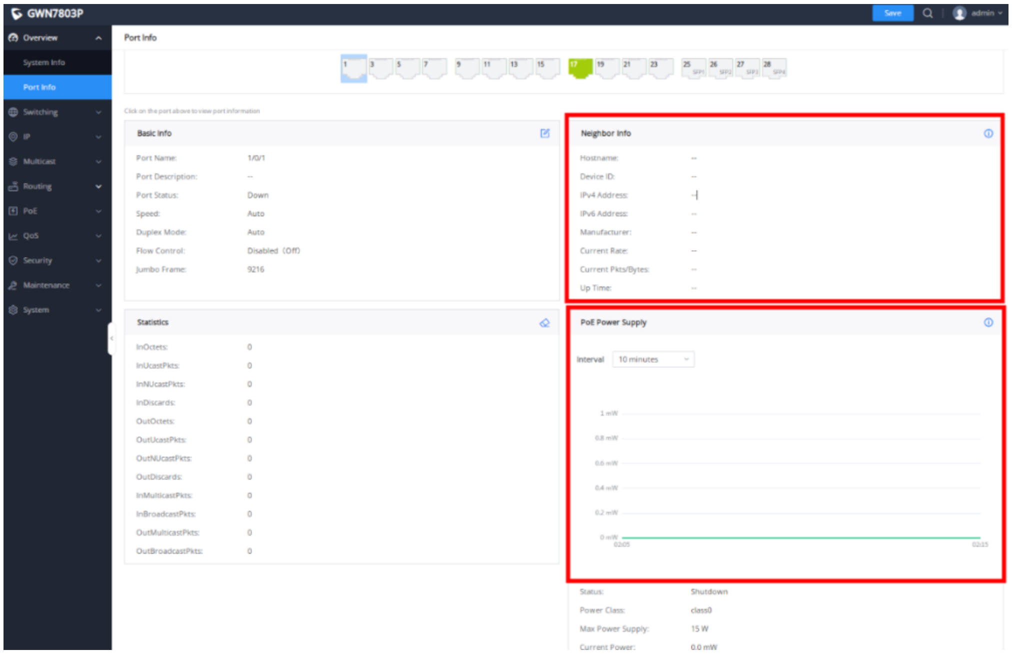
Device Name	GWN7801
System Location	Default
System Contact	Default
MAC Address	C0:74:AD:B9:3B:44
System OID	1.3.6.1.4.1.42379
Part Number	9640004612A
Serial Number	20VXU28N90B93B44
MGMT VLAN	VLAN 1
IPv4 Address	192.168.80.201
IPv6 Global Unicast Address	::
IPv6 Link Local Address	fe80::c274:adff:feb9:3b44
IPv4 Default Gateway	192.168.80.1
IPv6 Default Gateway	fe80::96a6:7eff:fe69:7bf1
System Time	2023-12-23 15:48:58 UTC+8:00
System Uptime	0 hours, 10 minutes
System Version	1.0.5.2
Hardware Version	V1.2A
Boot Version	3.6.9.55156

Device Temperature
33℃

Emergency	0 >	Critical	0 >
Alert	2 >	Error	11 >
Warning	22 >	Information	0 >
Notification	206 >	Debug	0 >

- **Add more port details such as neighbor, PoE power history info**

Supports viewing the port neighbor information, including device name, MAC address, IP address, speed, and connection duration.
Supports viewing the PoE power history to help troubleshoot PoE power supply.



Port Info

Click on the port above to view port information

Basic Info

Port Name:	1/0/1
Port Description:	--
Port Status:	Down
Speed:	Auto
Duplex Mode:	Auto
Flow Control:	Disabled（Off)
Jumbo Frame:	9216

Statistics

InOctets:	0
InUcastPkts:	0
InNUcastPkts:	0
InDiscards:	0
OutOctets:	0
OutUcastPkts:	0
OutNUcastPkts:	0
OutDiscards:	0
InMulticastPkts:	0
InBroadcastPkts:	0
OutMulticastPkts:	0
OutBroadcastPkts:	0

Neighbor Info

Hostname:	--
Device ID:	--
IPv4 Address:	--
IPv6 Address:	--
Manufacturer:	--
Current Rate:	--
Current Pkts/Bytes:	--
Up Time:	--

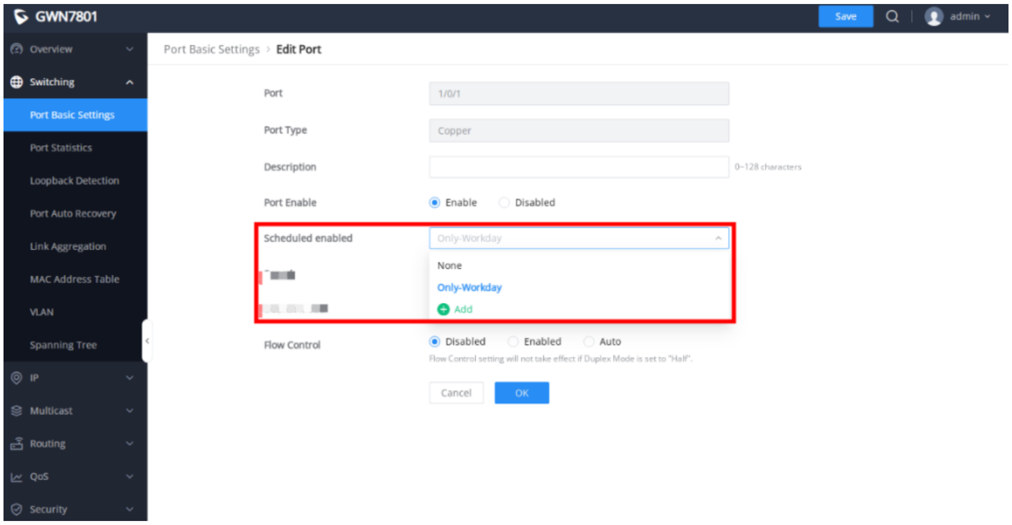
PoE Power Supply

Interval: 10 minutes

Status:	Shutdown
Power Class:	class0
Max Power Supply:	15 W
Current Power:	0.0 mW

- **Add port scheduled enabling feature**

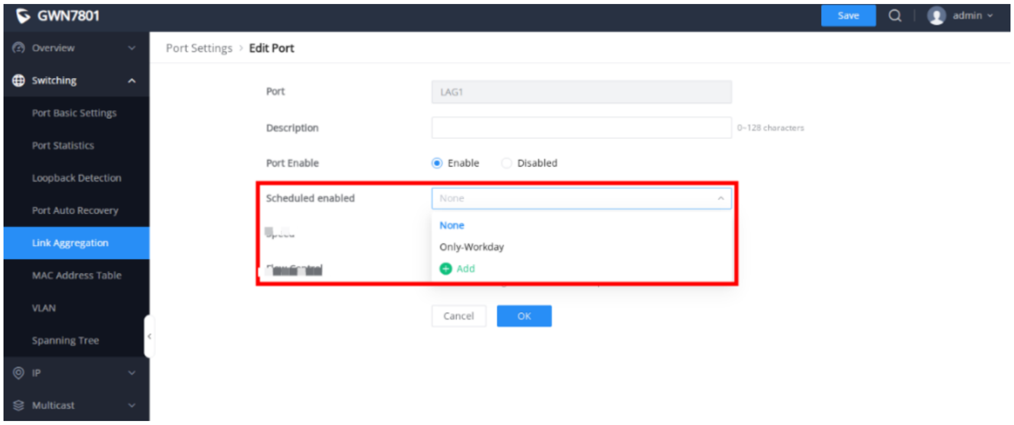
You can customize the Scheduled enable time for a port, including physical ports and LAGs.



Port Basic Settings > Edit Port

Port	1/0/1
Port Type	Copper
Description	0~128 characters
Port Enable	● Enable ○ Disabled
Scheduled enabled	Only-Workday
Flow Control	● Disabled ○ Enabled ○ Auto

Flow Control setting will not take effect if Duplex Mode is set to "Half".



Port: LAG1

Description: 0~128 characters

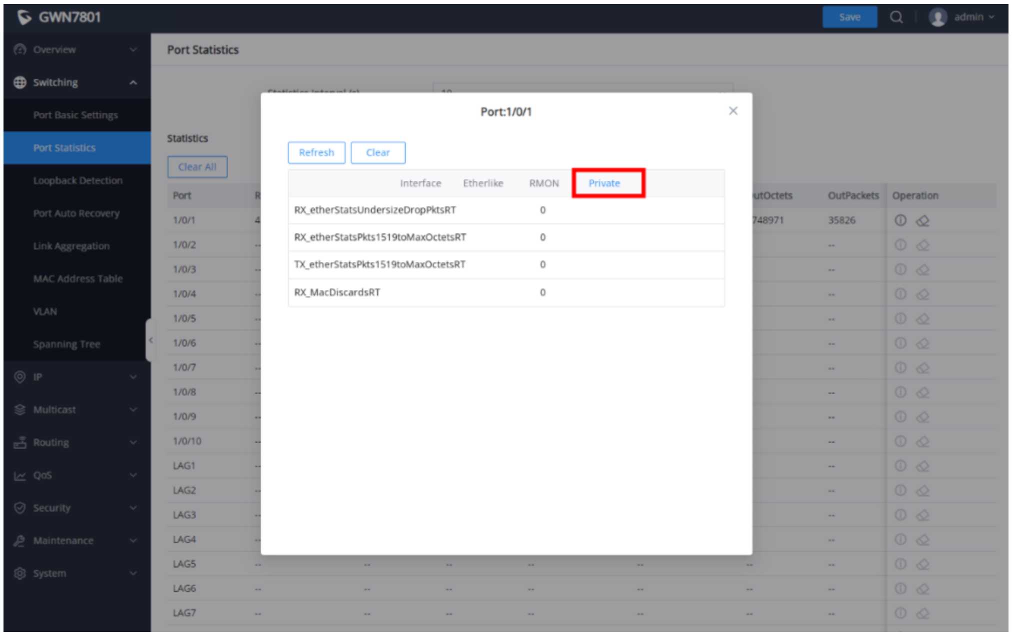
Port Enable: ● Enable ○ Disabled

Scheduled enabled: None

None
Only-Workday
Add

- **Add more port statistics info**

Support viewing port Private MIB information.



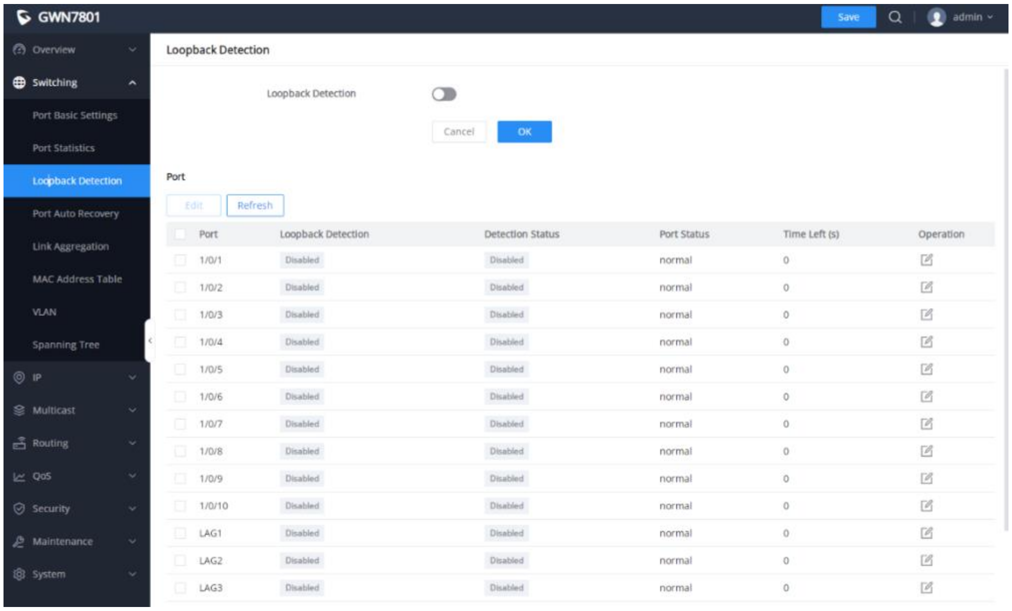
Port:1/0/1

RX_etherStatsUndersizeDropPktsRT	0
RX_etherStatsPkts1519toMaxOctetsRT	0
TX_etherStatsPkts1519toMaxOctetsRT	0
RX_MacDiscardsRT	0

- **Add loopback detection**

By enabling the interface loop detection function, detection messages are periodically sent from the interface to check whether the message is returned to the device, and then determine whether the device has a loop. After a loop is found, the port is automatically shut down to break the loop and ensure the normal operation of the network environment.

Note: If STP is enabled, STP loop protection takes precedence over interface loop protection, that is, interface loop protection will not take effect.



Loopback Detection

Loopback Detection ○

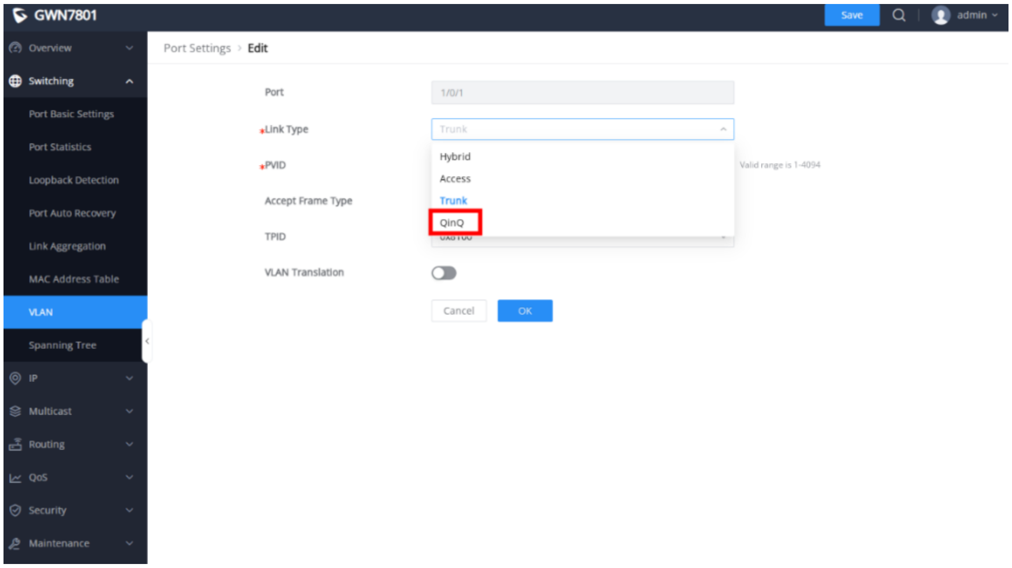
Port

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	✎
1/0/6	Disabled	Disabled	normal	0	✎
1/0/7	Disabled	Disabled	normal	0	✎
1/0/8	Disabled	Disabled	normal	0	✎
1/0/9	Disabled	Disabled	normal	0	✎
1/0/10	Disabled	Disabled	normal	0	✎
LAG1	Disabled	Disabled	normal	0	✎
LAG2	Disabled	Disabled	normal	0	✎
LAG3	Disabled	Disabled	normal	0	✎

- **Add QinQ**

An 802.1Q tag (VLAN tag) is added to the original 802.1Q packet header. Through the double-layer tag, the number of VLANs is increased to 802.1Q.

QinQ encapsulates the user's private network VLAN Tag in the public network (service provider) network VLAN Tag, allowing the double-layer VLAN Tag message to pass through the operator's backbone network (public network). In the public network, the message is transmitted according to the outer VLAN Tag (that is, the public network VLAN Tag), shielding the user's private network VLAN Tag, thereby providing a simple L2 VPN tunnel for the user.



Port Settings › Edit

Port: 1/0/1

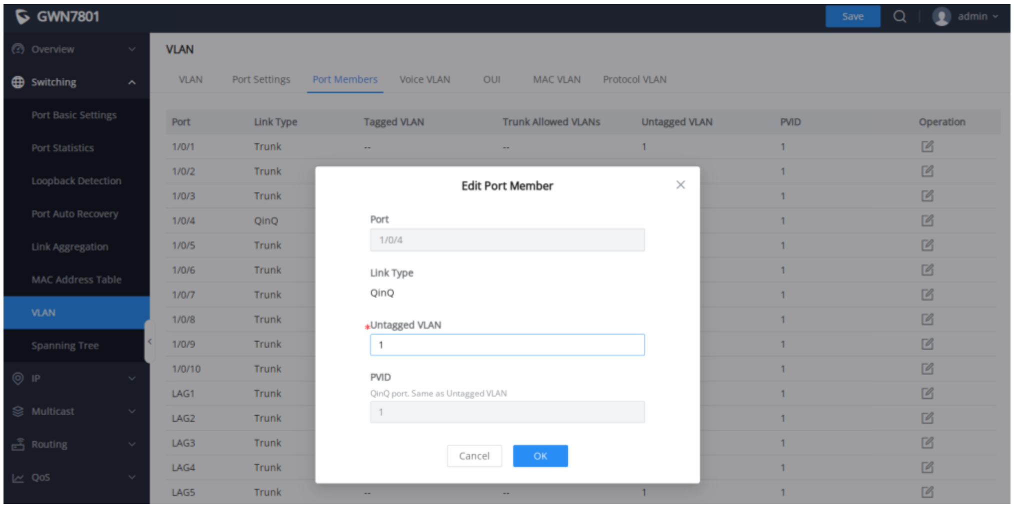
*Link Type: Trunk

*PVID — Valid range is 1-4094

Accept Frame Type

TPID: 0x8100

VLAN Translation ○



Edit Port Member

Port: 1/0/4

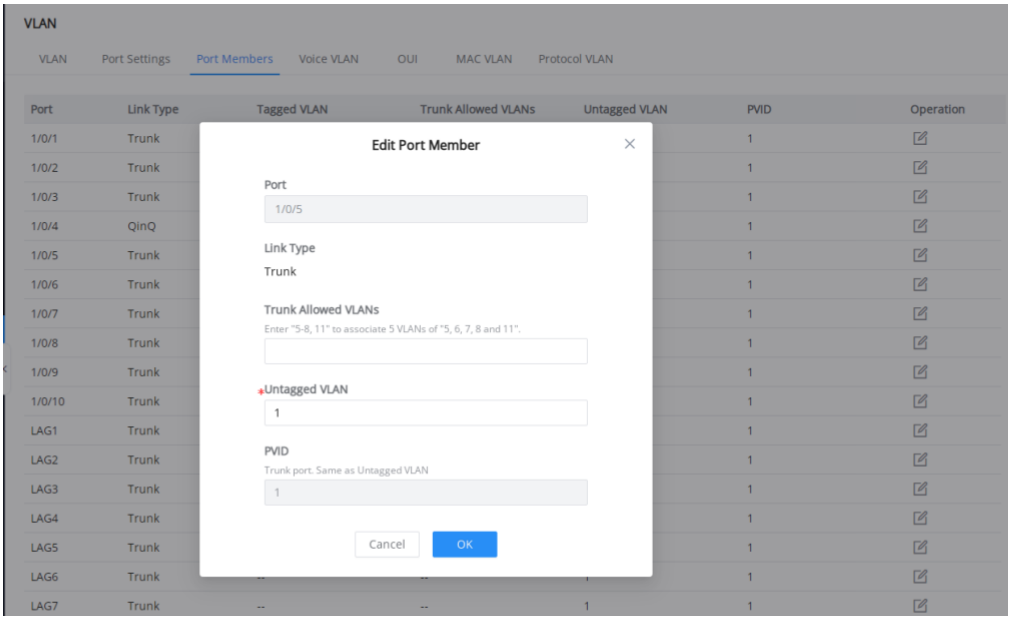
Link Type: QinQ

*Untagged VLAN: 1

PVID
QinQ port. Same as Untagged VLAN
1

- **Optimize trunk port settings**

Trunk Allowed VLANs allows configuration of VLANs that do not yet exist on the switch, and takes effect only for configured VLANs.



Edit Port Member

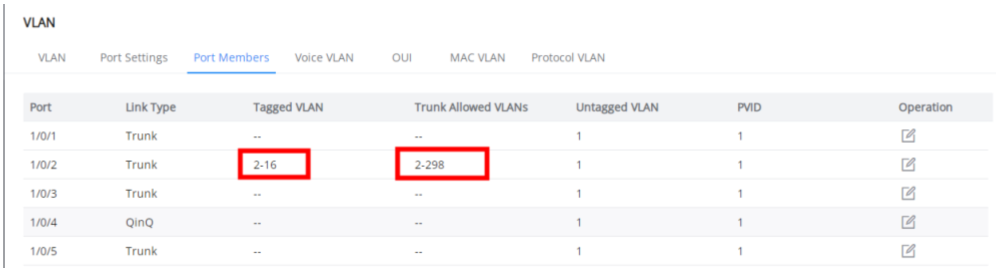
Port: 1/0/5

Link Type: Trunk

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

*Untagged VLAN: 1

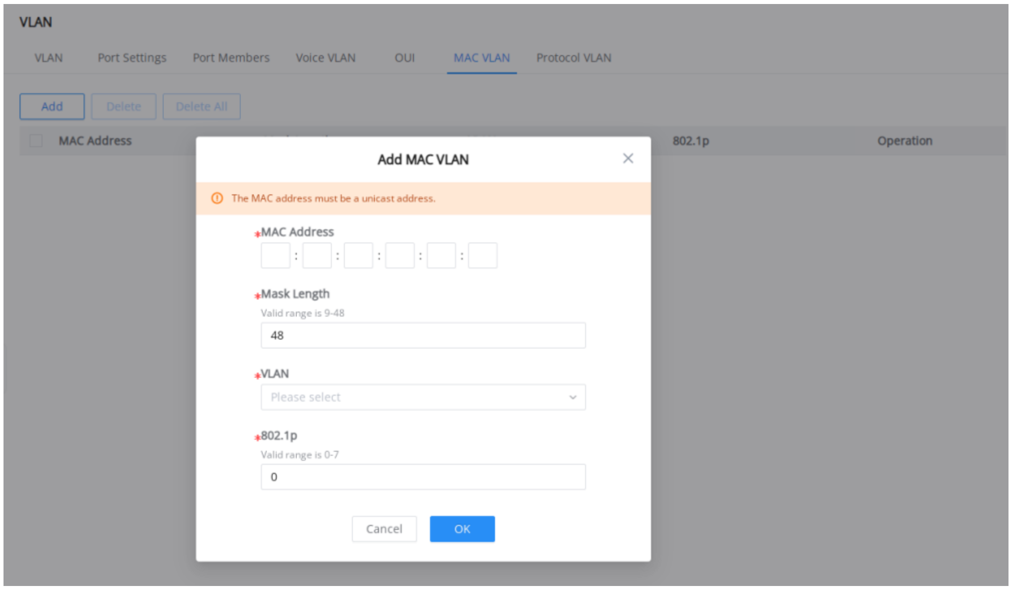
PVID
Trunk port. Same as Untagged VLAN
1



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	✎

- **Add MAC-based VLAN**

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 according to the mapping table.
Note: This is only effective for Hybrid ports.



Add MAC VLAN

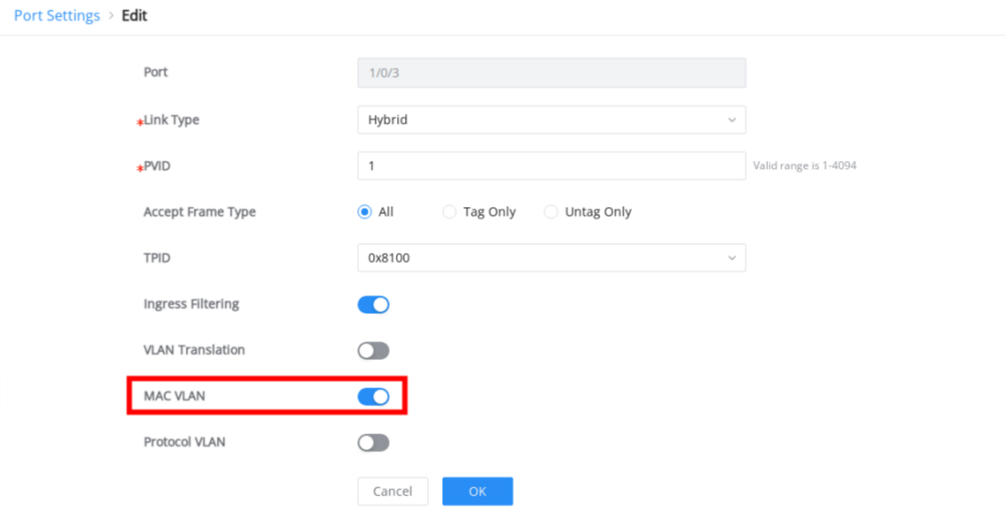
The MAC address must be a unicast address.

*MAC Address
: : : : :

*Mask Length
Valid range is 9-48
48

*VLAN
Please select

*802.1p
Valid range is 0-7
0

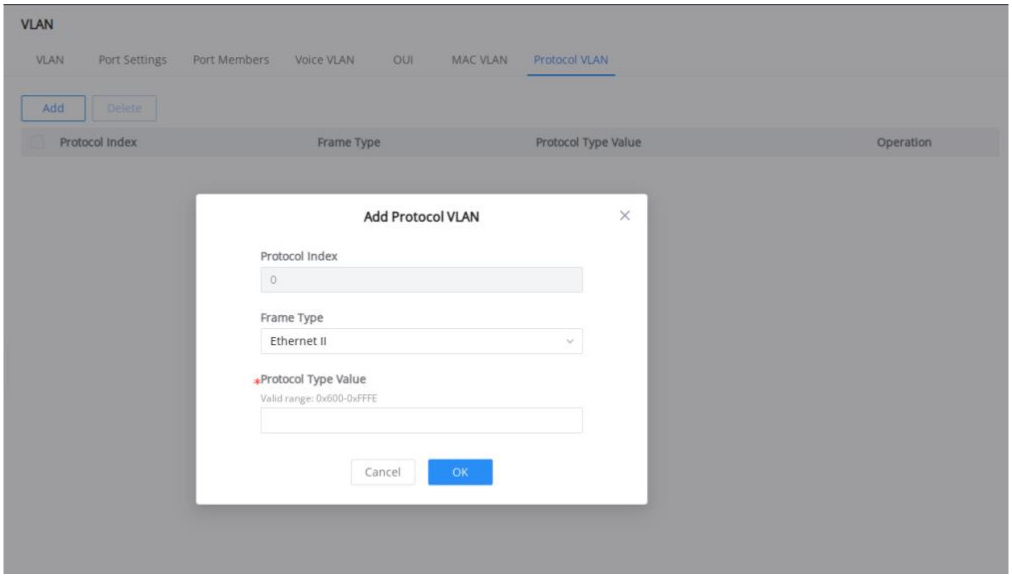


Port	1/0/3
*Link Type	Hybrid
*PVID	1 Valid range is 1-4094
Accept Frame Type	● All ○ Tag Only ○ Untag Only
TPID	0x8100
Ingress Filtering	On
VLAN Translation	Off
MAC VLAN	On
Protocol VLAN	Off

- **Add protocol-based VLAN**

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

Note: This is only effective for Hybrid ports.



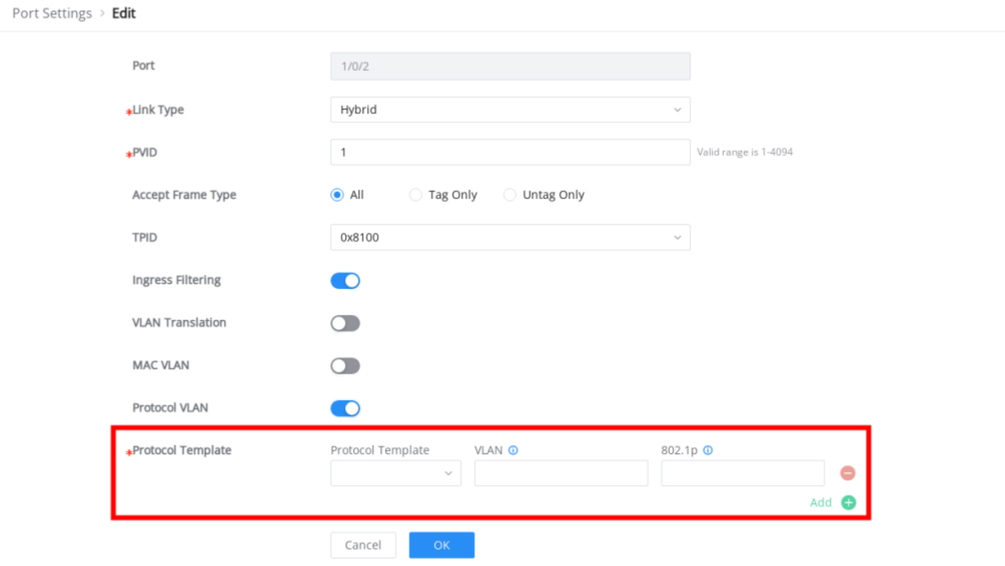
Protocol Index	Frame Type	Protocol Type Value	Operation

Add Protocol VLAN

Protocol Index: 0

Frame Type: Ethernet II

*Protocol Type Value
Valid range: 0x600-0xFFFE



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: on

VLAN Translation: off

MAC VLAN: off

Protocol VLAN: on

*Protocol Template: Protocol Template | VLAN | 802.1p

- **Add VLAN translation**

By modifying the VLAN Tag carried in the message, different VLANs can be mapped to each other.

Note: a. This feature is only effective for Trunk and Hybrid ports.

b. Configuration restrictions:

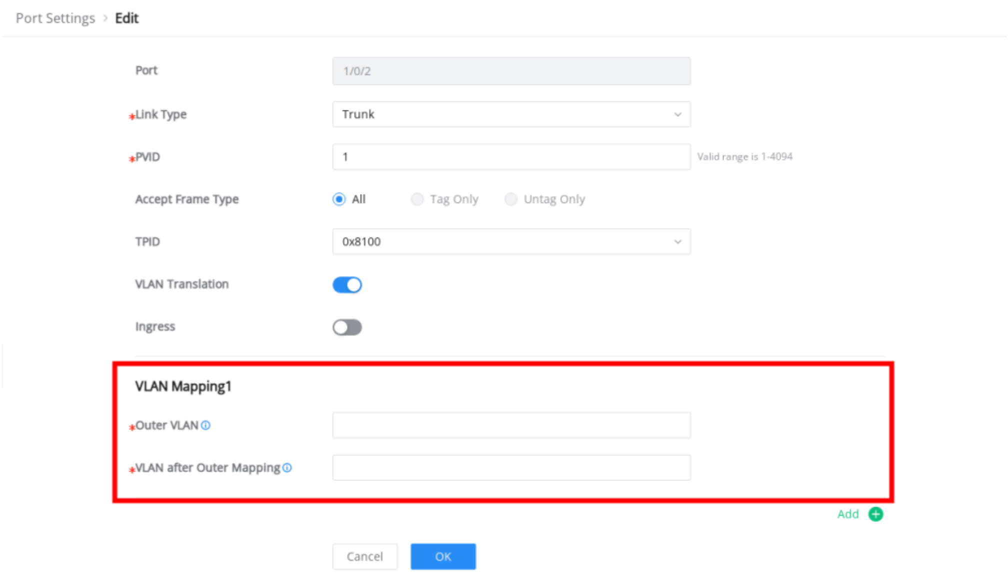
(1) The GWN7800 series switches only support the 1 to 1 function of the outer VLAN (including 1:1 and N:1).

(2) The outer VLAN allows the configuration of a single VLAN or a VLAN range. Only one outer VLAN

can be configured after mapping, and it must be a VLAN to which the port has been added.

(3) The total number of VLAN mapping groups supported by the switch is 256, and the maximum number of VLAN mapping groups supported on a single port is 128.

(4) The total number of VLAN ranges supported by the switch is 16, and the maximum number of VLAN ranges supported on a single port is 16.



Port Settings > Edit

Port: 1/0/2

*Link Type: Trunk

*PVID: 1 — Valid range is 1-4094

Accept Frame Type: ● All ○ Tag Only ○ Untag Only

TPID: 0x8100

VLAN Translation: on

Ingress: off

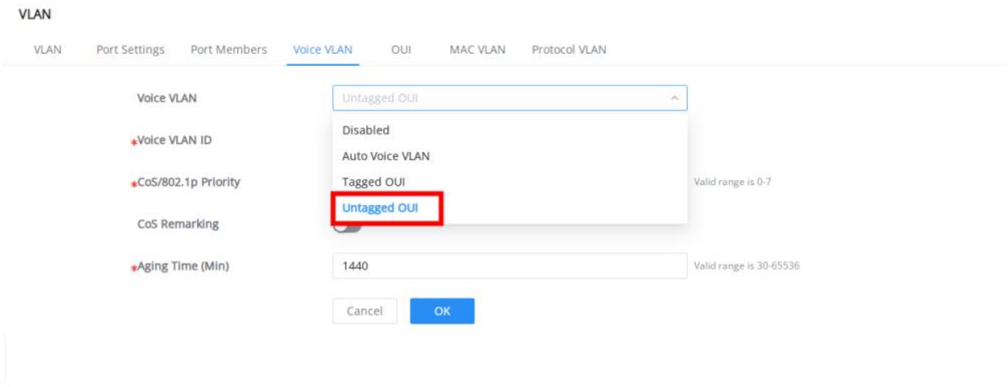
VLAN Mapping1

*Outer VLAN

*VLAN after Outer Mapping

- **Add untagged OUI mode for voice VLAN**

Compared with the Tagged OUI mode, the Untagged OUI mode is added. The only difference is that the Untagged label is added, and the rest is the same as the Tagged OUI mode.



Voice VLAN: Untagged OUI

*Voice VLAN ID

*CoS/802.1p Priority — Valid range is 0-7

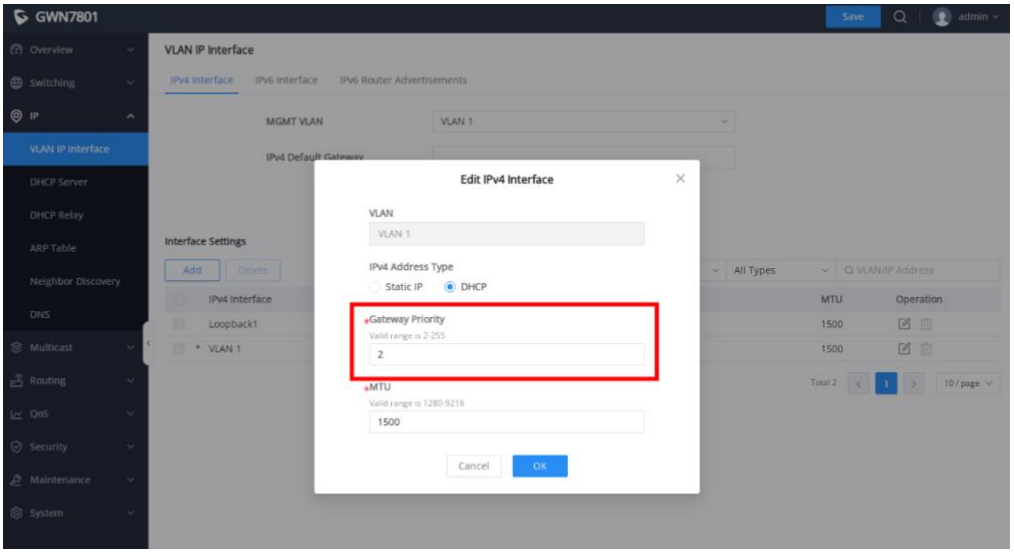
CoS Remarking

*Aging Time (Min): 1440 — Valid range is 30-65536

- **Add gateway priority when using DHCP to get VLAN IP address**

The IPv4 interface supports specifying a priority when obtaining a gateway from DHCP; the IPv6 interface supports specifying a priority when obtaining an IPv6 global unicast address gateway from SLAAC, Stateless DHCPv6, and Stateful DHCPv6.

Note: The gateway priority is: statically configured gateway > gateway with a set priority (the smaller the priority value, the greater the priority) > gateway obtained from DHCP on the VLAN interface (VLAN ID from small to large, first come first served). If the statically configured gateway network segment is the same as any interface network segment, the statically configured gateway takes effect. Otherwise, the effective gateway is selected according to the gateway priority configuration. If the priorities are the same, the gateway with the smaller VLAN ID takes effect first.



MGMT VLAN: VLAN 1

IPv4 Default Gateway

	IPv4 Interface	MTU	Operation
□	Loopback1	1500	
□	VLAN 1	1500	

Edit IPv4 Interface

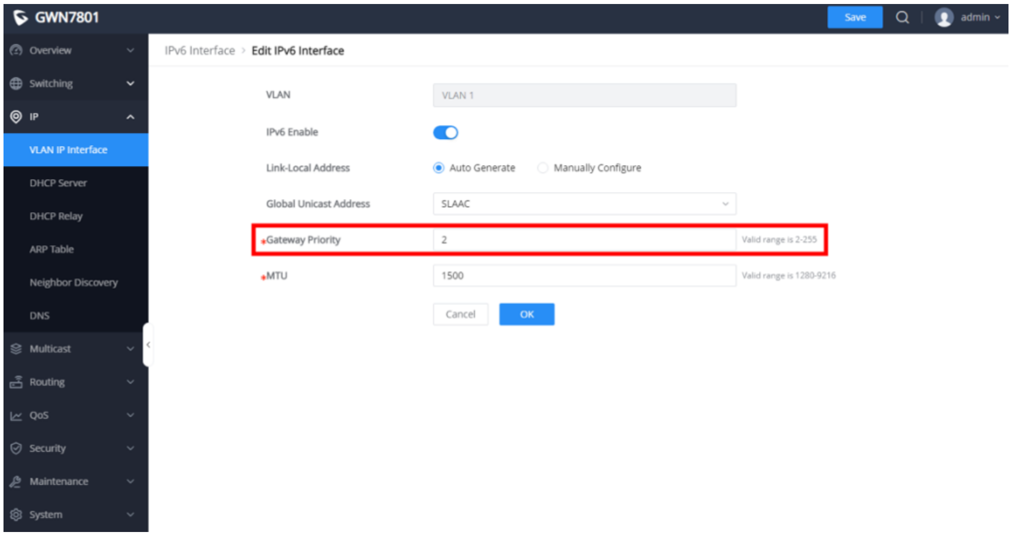
VLAN: VLAN 1

IPv4 Address Type: ○ Static IP ● DHCP

*Gateway Priority (Valid range is 2-255): 2

*MTU (Valid range is 1280-9216): 1500

Cancel OK



IPv6 Interface > Edit IPv6 Interface

VLAN: VLAN 1

IPv6 Enable

Link-Local Address: ● Auto Generate ○ Manually Configure

Global Unicast Address: SLAAC

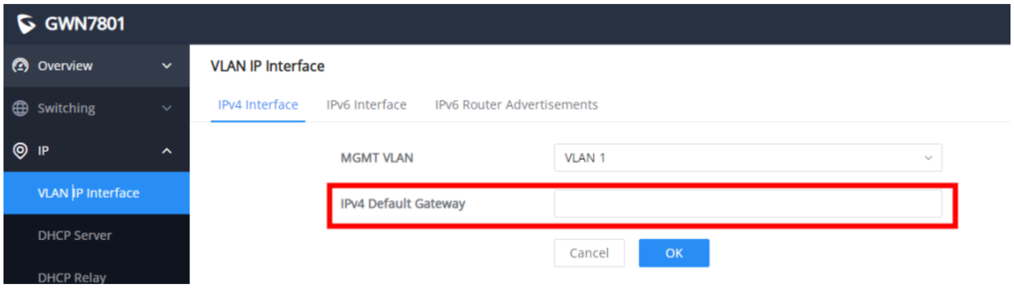
*Gateway Priority: 2 Valid range is 2-255

*MTU: 1500 Valid range is 1280-9216

Cancel OK

- **Add default gateway configuration under MGMT VLAN**

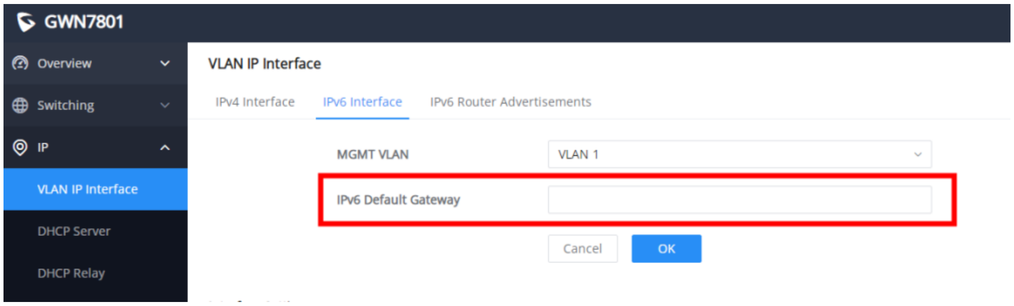
Configure a default static gateway in the MGMT VLAN and keep the configuration synchronized with the default route next hop address added to the static route.



VLAN IP Interface

MGMT VLAN: VLAN 1

IPv4 Default Gateway



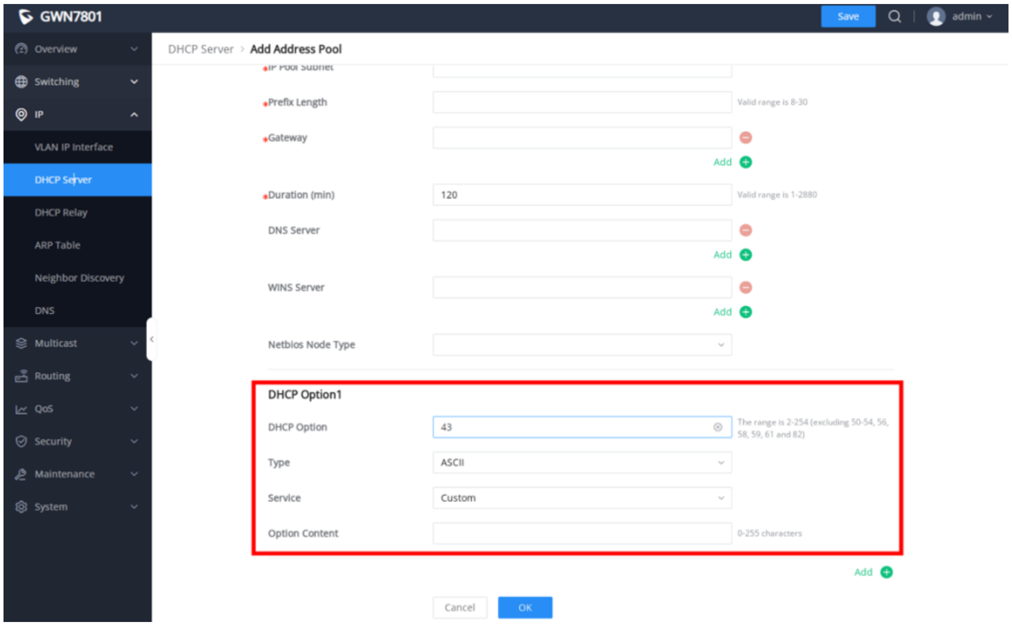
VLAN IP Interface

MGMT VLAN: VLAN 1

IPv6 Default Gateway

- **Optimize DHCP option 43 configurations for DHCP server**

Supports configuring specified services for DHCP Option 43.



*IP Pool Subnet

*Prefix Length — Valid range is 8-30

*Gateway

*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)

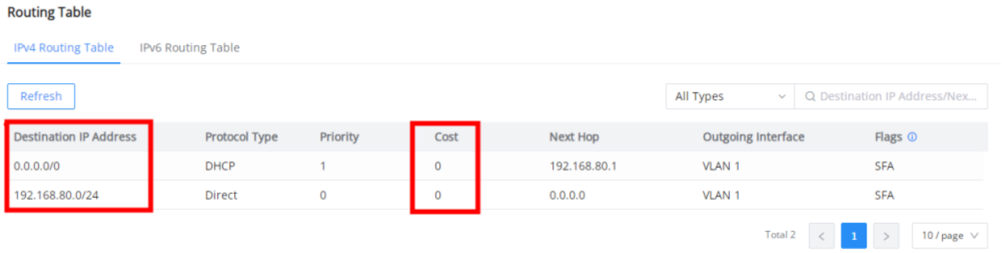
Type: ASCII

Service: Custom

Option Content — 0-255 characters

- **Optimize routing table**

Optimize the destination IP address display and increase the Path Cost value

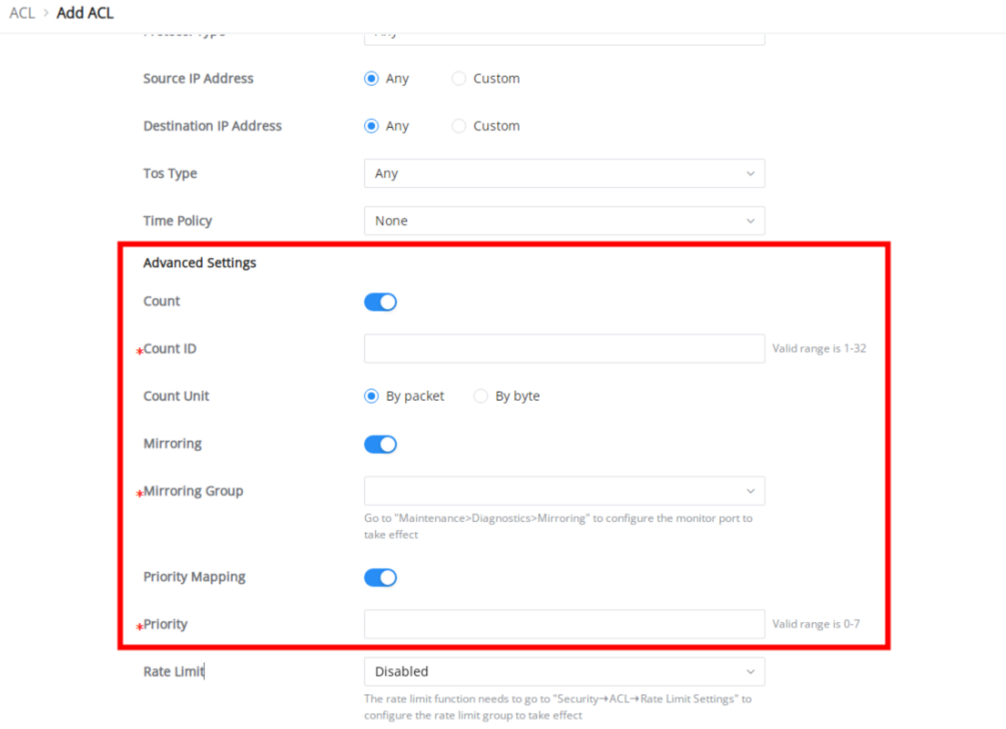


Routing Table

Destination IP Address	Protocol Type	Priority	Cost	Next Hop	Outgoing Interface	Flags ⓘ
0.0.0.0/0	DHCP	1	0	192.168.80.1	VLAN 1	SFA
192.168.80.0/24	Direct	0	0	0.0.0.0	VLAN 1	SFA

- **Add ACL advanced settings, including mirroring, statistic and priority remapping for rule**

Statistics: Once the ACL rule is hit, the counting starts. Supports statistics by packet or by byte.
Mirror: After selecting the mirror group, you need to go to Maintenance → Diagnosis → Mirror Configuration Observation Port to take effect.
Priority Mapping: After it is turned on, once the ACL rule is hit, the priority of the message will be remapped inside the switch.



ACL > Add ACL

Source IP Address ● Any ○ Custom

Destination IP Address ● Any ○ Custom

Tos Type: Any

Time Policy: None

Advanced Settings

Count: on

*Count ID: Valid range is 1-32

Count Unit ● By packet ○ By byte

Mirroring: on

*Mirroring Group:

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

Priority Mapping: on

*Priority: Valid range is 0-7

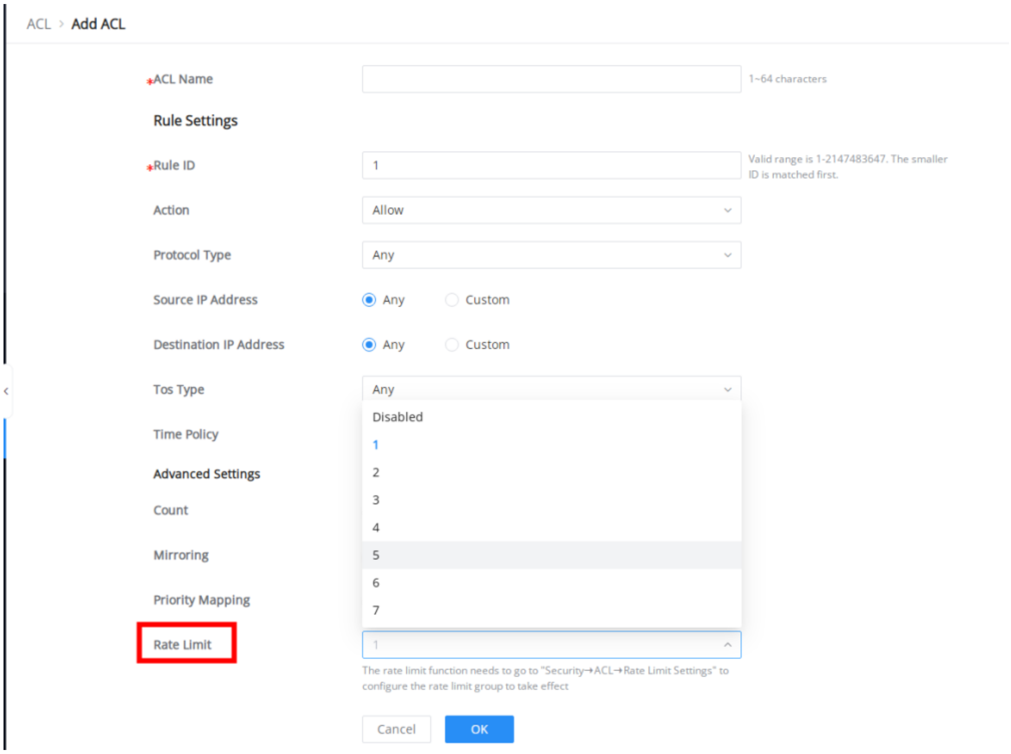
Rate Limit: Disabled

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

- **Add rate limit by ACL binding to VLAN**

Speed limit for VLAN. By binding VLAN to ACL, speed limit is achieved by selecting speed limit group for rules. Once the rule is hit, it will take effect according to the settings of the specified speed limit group.

ACL rule setting speed limit function: select speed limit group.



ACL > Add ACL

*ACL Name: (empty) — 1~64 characters

Rule Settings

*Rule ID: 1 — Valid range is 1-2147483647. The smaller ID is matched first.

Action: Allow

Protocol Type: Any

Source IP Address: ● Any ○ Custom

Destination IP Address: ● Any ○ Custom

Tos Type: Any

Time Policy

Advanced Settings

Count

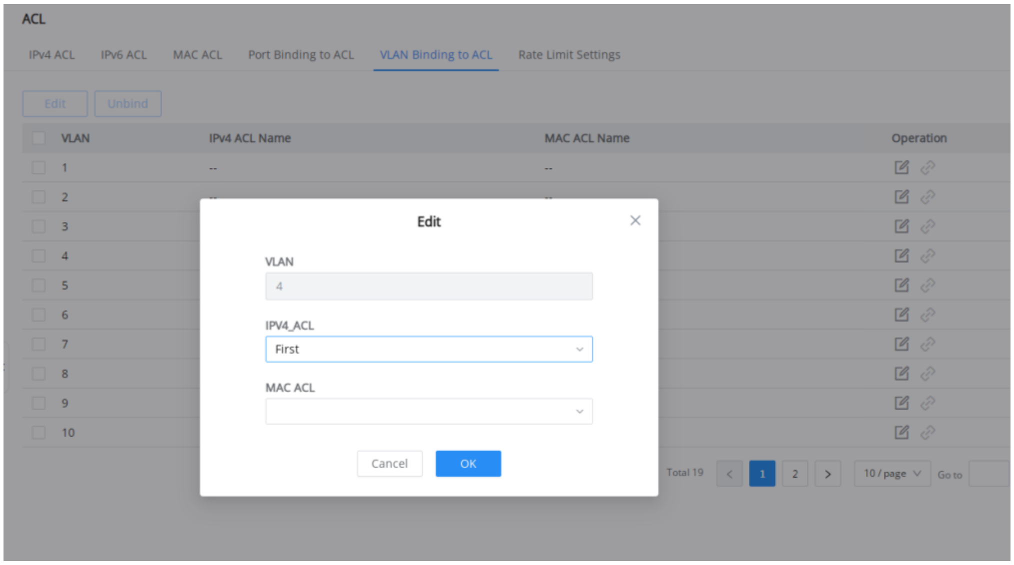
Mirroring

Priority Mapping

Rate Limit: 1

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

VLAN bind ACL：



ACL

VLAN	IPv4 ACL Name	MAC ACL Name	Operation
1	--	--	
2	--	--	
3			
4			
5			
6			
7			
8			
9			
10			

Total 19

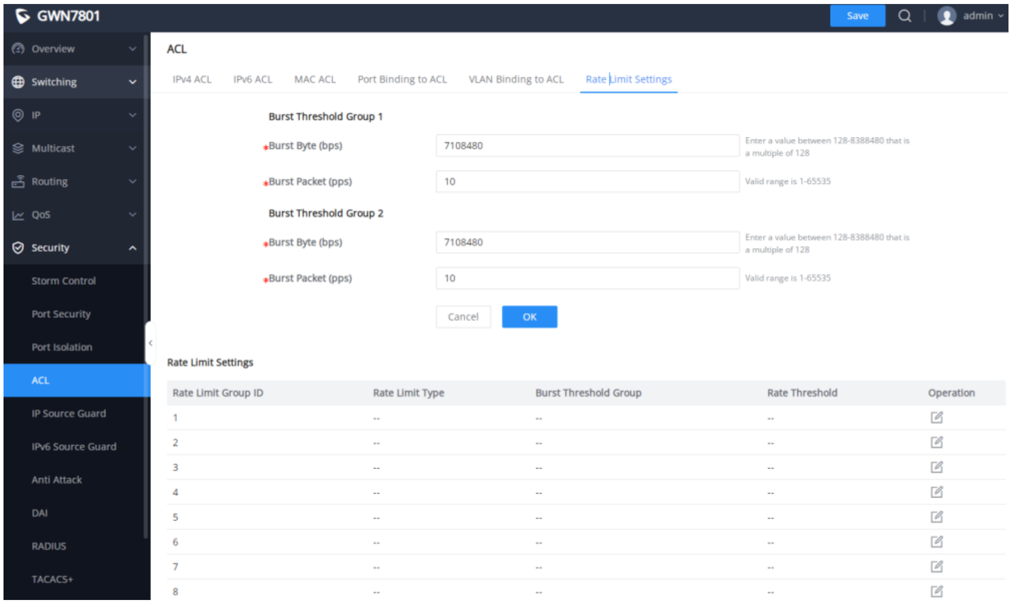
Edit

VLAN: 4

IPV4_ACL: First

MAC ACL: (empty)

Speed limit group settings:



ACL

Burst Threshold Group 1

*Burst Byte (bps): 7108480 — Enter a value between 128-8388480 that is a multiple of 128

*Burst Packet (pps): 10 — Valid range is 1-65535

Burst Threshold Group 2

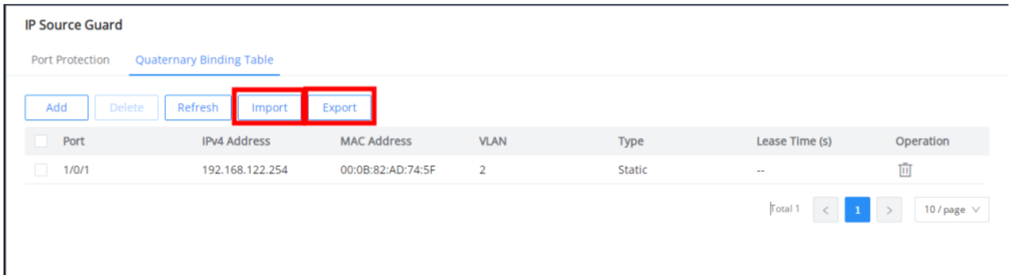
*Burst Byte (bps): 7108480 — Enter a value between 128-8388480 that is a multiple of 128

*Burst Packet (pps): 10 — Valid range is 1-65535

Rate Limit Settings

Rate Limit Group ID	Rate Limit Type	Burst Threshold Group	Rate Threshold	Operation
1	--	--	--	✎
2	--	--	--	✎
3	--	--	--	✎
4	--	--	--	✎
5	--	--	--	✎
6	--	--	--	✎
7	--	--	--	✎
8	--	--	--	✎

- **Add import/export IPSG binding table for IP Source Guard**



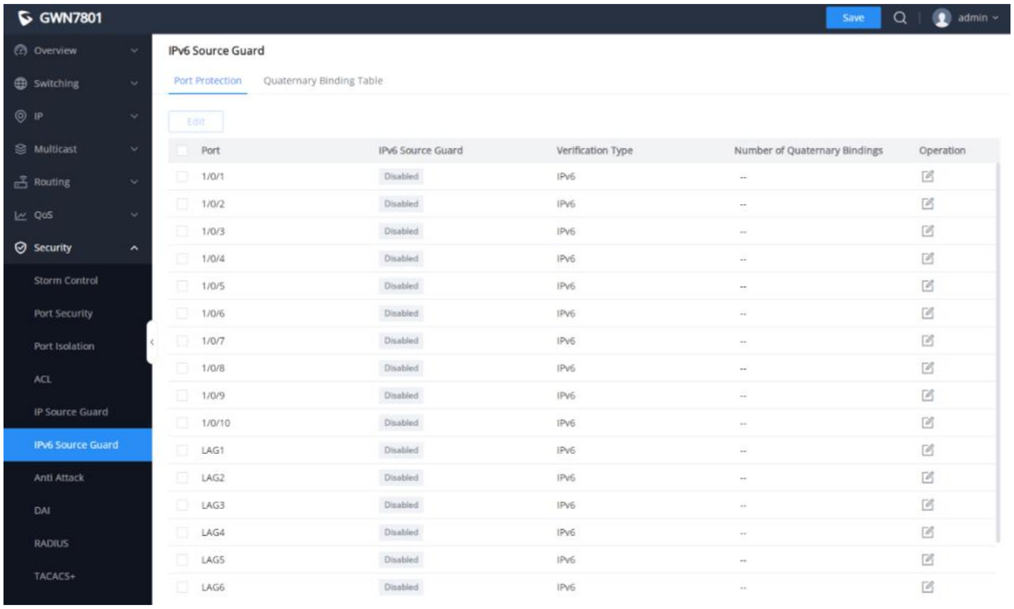
IP Source Guard

□	Port	IPv4 Address	MAC Address	VLAN	Type	Lease Time (s)	Operation
□	1/0/1	192.168.122.254	00:0B:82:AD:74:5F	2	Static	--	🗑

- **Add IPv6 Source Guard**

IPv6 source attack protection is a source IPv6 address filtering technology based on the Layer 2 interface. It can prevent malicious hosts from forging the IPv6 addresses of legitimate hosts to impersonate legitimate hosts and ensure that unauthorized hosts cannot access or attack the network by setting their own IPv6 addresses.

IPv6SG uses the binding table (source IPv6 address, source MAC address, VLAN, and inbound interface binding) to match and check the IPv6 packets received on the Layer 2 interface. Only packets that match the binding table are allowed to pass, and other packets will be discarded.

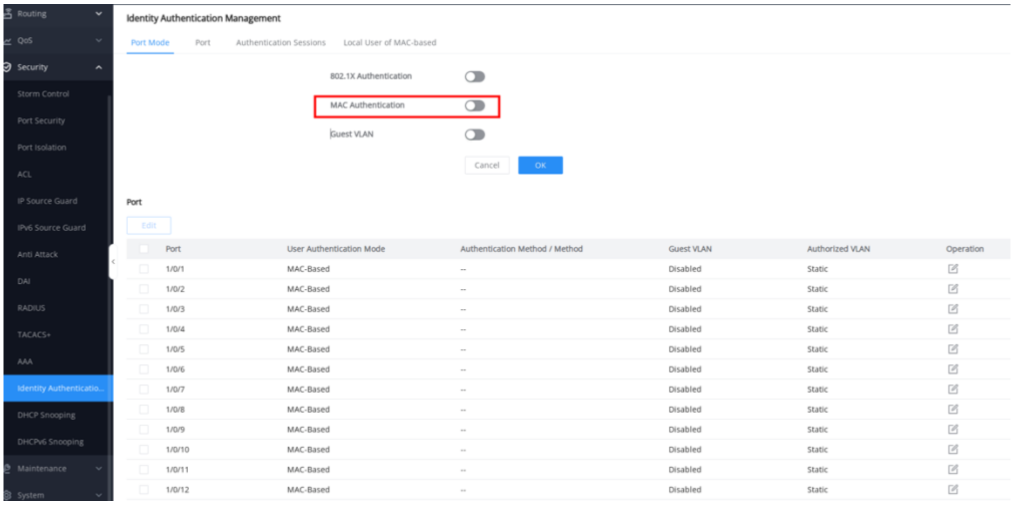


IPv6 Source Guard

Port	IPv6 Source Guard	Verification Type	Number of Quaternary Bindings	Operation
1/0/1	Disabled	IPv6	--	✎
1/0/2	Disabled	IPv6	--	✎
1/0/3	Disabled	IPv6	--	✎
1/0/4	Disabled	IPv6	--	✎
1/0/5	Disabled	IPv6	--	✎
1/0/6	Disabled	IPv6	--	✎
1/0/7	Disabled	IPv6	--	✎
1/0/8	Disabled	IPv6	--	✎
1/0/9	Disabled	IPv6	--	✎
1/0/10	Disabled	IPv6	--	✎
LAG1	Disabled	IPv6	--	✎
LAG2	Disabled	IPv6	--	✎
LAG3	Disabled	IPv6	--	✎
LAG4	Disabled	IPv6	--	✎
LAG5	Disabled	IPv6	--	✎
LAG6	Disabled	IPv6	--	✎

- **Add MAC bypass authentication**

In addition to the previously supported 802.1X authentication, identity authentication management now supports MAC authentication.



Identity Authentication Management

802.1X Authentication ○

MAC Authentication ○

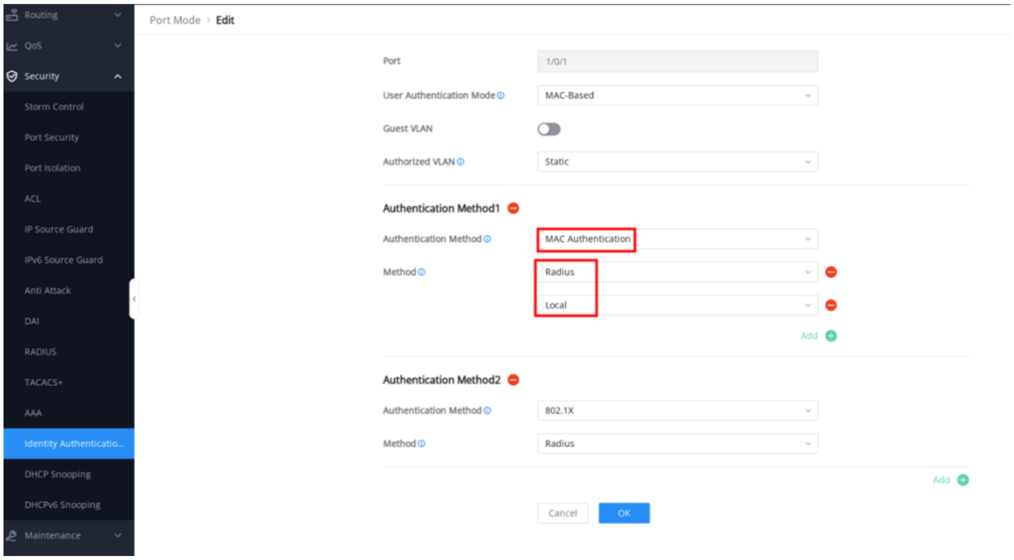
Guest VLAN ○

Port

Port	User Authentication Mode	Authentication Method / Method	Guest VLAN	Authorized VLAN	Operation
1/0/1	MAC-Based	--	Disabled	Static	✎
1/0/2	MAC-Based	--	Disabled	Static	✎
1/0/3	MAC-Based	--	Disabled	Static	✎
1/0/4	MAC-Based	--	Disabled	Static	✎
1/0/5	MAC-Based	--	Disabled	Static	✎
1/0/6	MAC-Based	--	Disabled	Static	✎
1/0/7	MAC-Based	--	Disabled	Static	✎
1/0/8	MAC-Based	--	Disabled	Static	✎
1/0/9	MAC-Based	--	Disabled	Static	✎
1/0/10	MAC-Based	--	Disabled	Static	✎
1/0/11	MAC-Based	--	Disabled	Static	✎
1/0/12	MAC-Based	--	Disabled	Static	✎

MAC authentication has been added to the port authentication method, and the authentication methods support RADIUS and Local.

By default, the order of port authentication methods is 802.1X, MAC, and the order of authentication methods is RADIUS, Local.



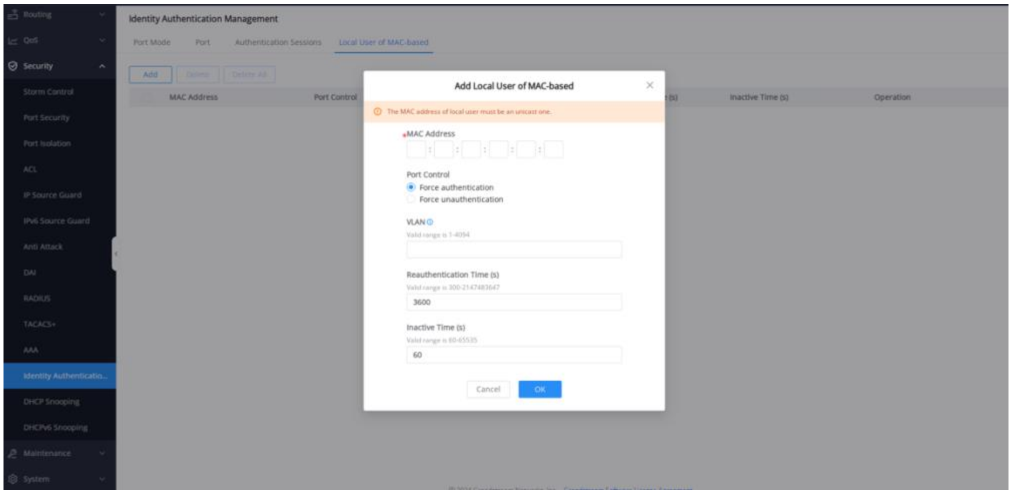
Port Mode › Edit

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

Authentication Method1
Authentication Method: MAC Authentication
Method: Radius
Local

Authentication Method2
Authentication Method: 802.1X
Method: Radius

To add a MAC-based local user, you need to add the MAC address, port control mode, VLAN authorized for use after authentication, re-authentication time, and inactive time.



Identity Authentication Management

Add Local User of MAC-based

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

*MAC Address: __:__:__:__:__:__

Port Control
● Force authentication
○ Force unauthentication

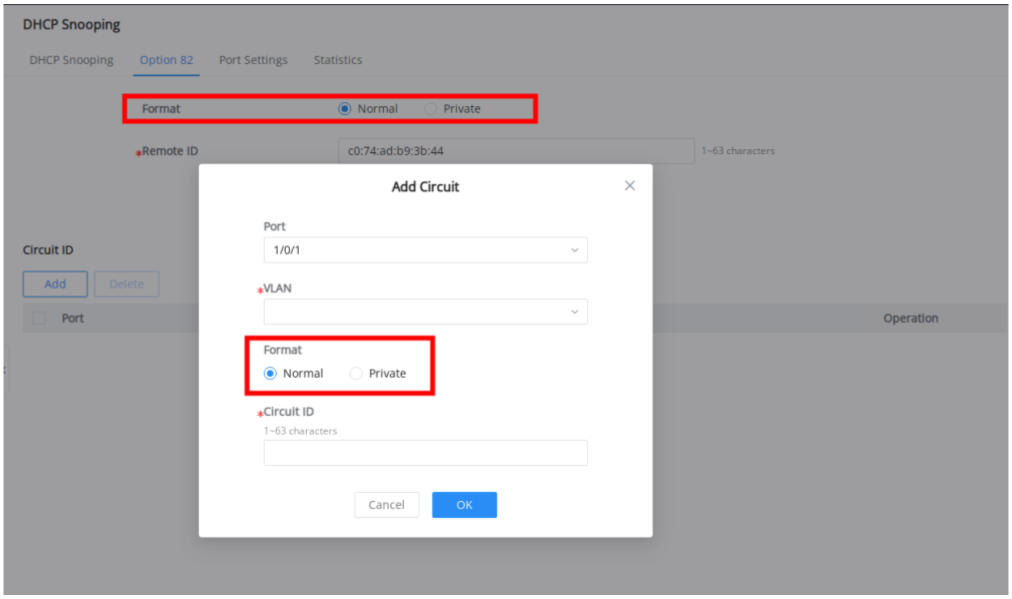
VLAN
Valid range is 1-4094

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

Inactive Time (s)
Valid range is 60-65535
60

- **Optimize remote ID and Circuit ID for DHCP Snooping**

The Remote ID and Circuit ID of Option 82 can be configured in standard format and private format.
Standard format: The default format is set according to TLV (type-length-value).
Private format: Only Value is used for setting.



Format ● Normal ○ Private

*Remote ID c0:74:ad:b9:3b:44 1~63 characters

Port 1/0/1

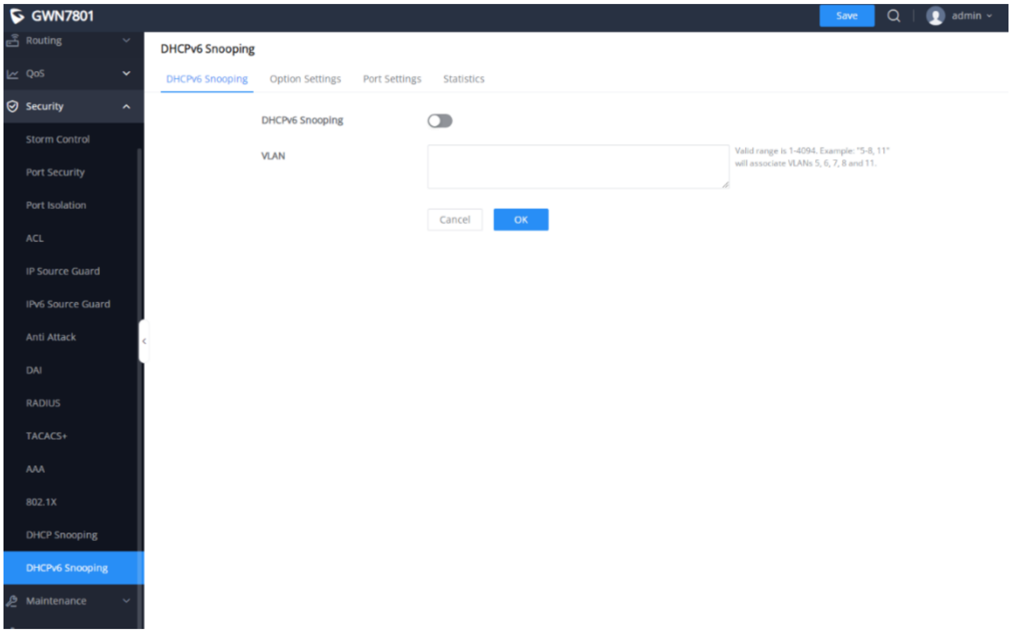
*VLAN

Format ● Normal ○ Private

*Circuit ID 1~63 characters

- **Add DHCPv6 Snooping**

It is used to ensure that the client obtains an IPv6 address or IPv6 prefix from a valid server and can record the correspondence between the DHCPv6 client IPv6 address or IPv6 prefix and the MAC address.

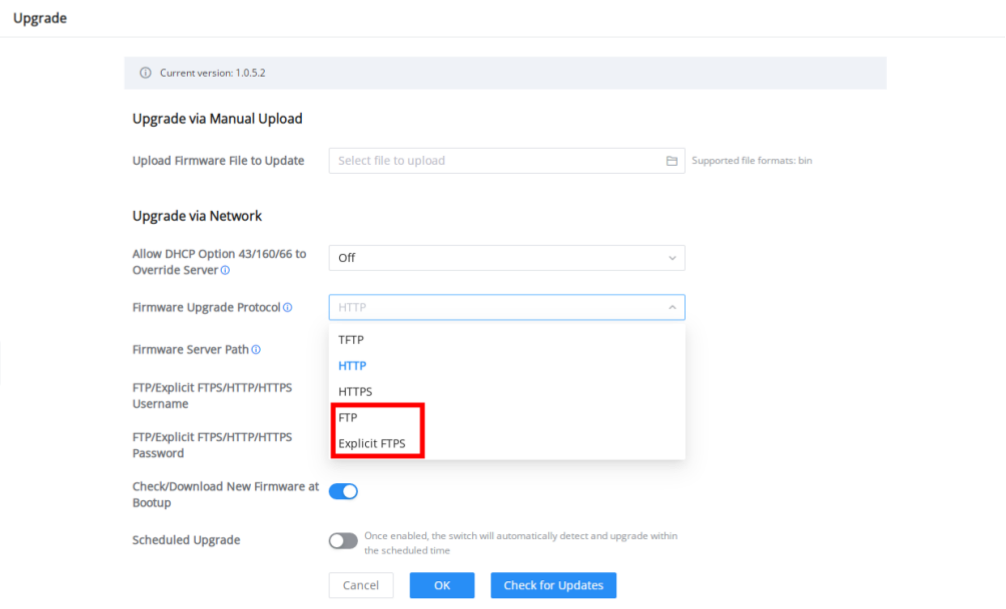


DHCPv6 Snooping ○

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

- **Add upgrade by FTP and Explicit FTPS**

Network upgrade supports FTP and explicit FTPS. Firmware detection and upgrade are performed by filling in the FTP or explicit FTPS firmware server address.
It also supports DHCP Option to carry FTP or explicit FTPS server address. The device reads and parses it and uses this address for upgrade.
Note: ftp:// protocol header refers to FTP upgrade method, and ftps:// protocol header refers to FTPS upgrade method.



Upgrade

ⓘ Current version: 1.0.5.2

Upgrade via Manual Upload

Upload Firmware File to Update: Select file to upload — Supported file formats: bin

Upgrade via Network

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

Firmware Upgrade Protocol ⓘ: HTTP

Firmware Server Path ⓘ

FTP/Explicit FTPS/HTTP/HTTPS Username

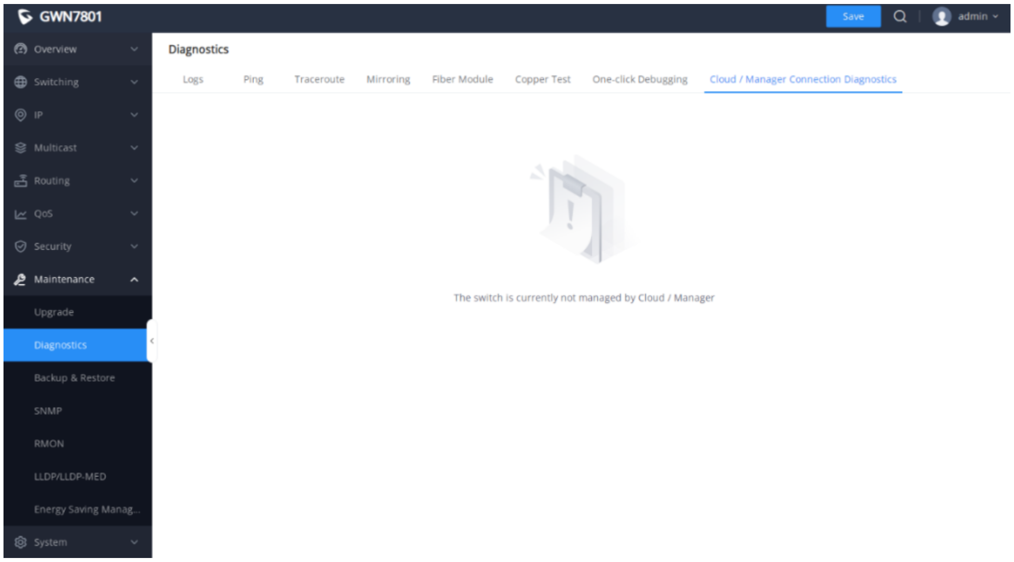
FTP/Explicit FTPS/HTTP/HTTPS Password

Check/Download New Firmware at Bootup: ●

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

- **Add connection diagnostics with GWN.Cloud/Manager**

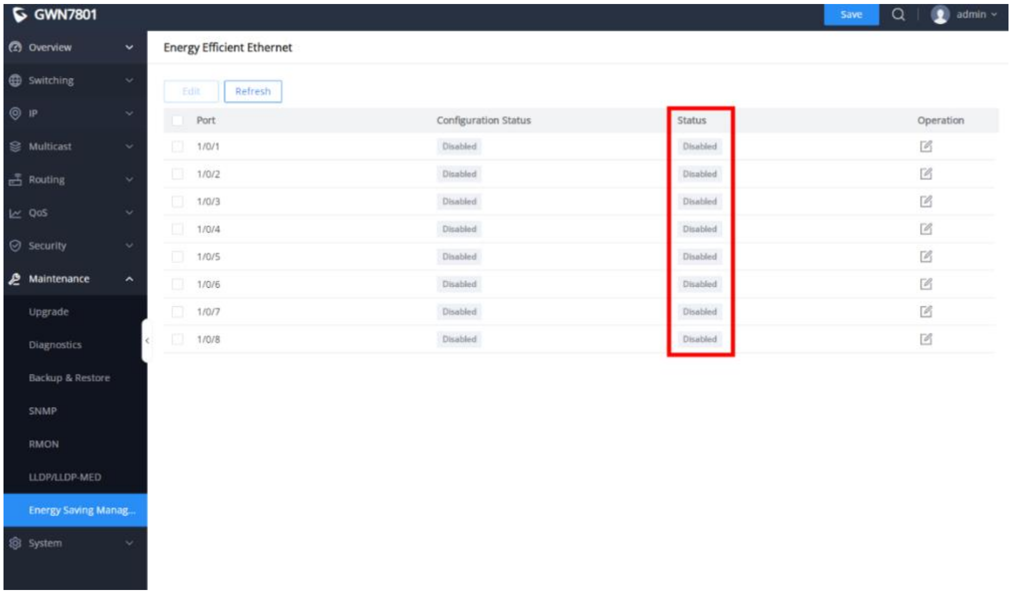
When the switch and GWN.Cloud/GWN Manager connection is unstable, the user can log in to the local Web GUI diagnostic page to check the cloud connection status and view related logs.



The switch is currently not managed by Cloud / Manager

- **Optimize EEE**

Added actual port status display.

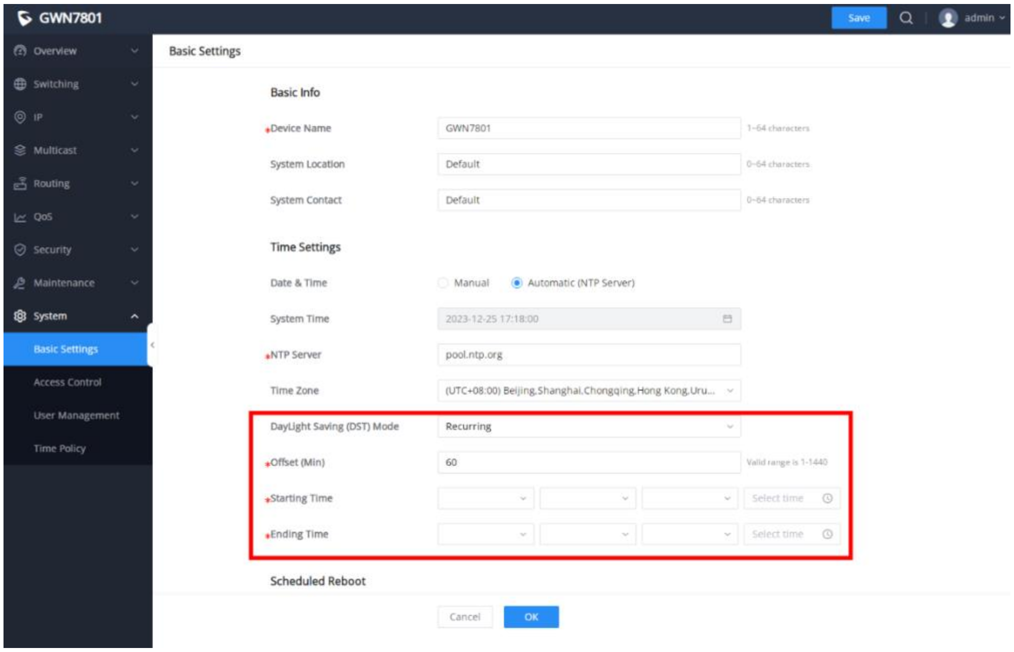


Energy Efficient Ethernet

□	Port	Configuration Status	Status	Operation
□	1/0/1	Disabled	Disabled	✎
□	1/0/2	Disabled	Disabled	✎
□	1/0/3	Disabled	Disabled	✎
□	1/0/4	Disabled	Disabled	✎
□	1/0/5	Disabled	Disabled	✎
□	1/0/6	Disabled	Disabled	✎
□	1/0/7	Disabled	Disabled	✎
□	1/0/8	Disabled	Disabled	✎

- **Add DST mode for time settings**

Added daylight saving time offset setting and automated time configuration.



Basic Settings

Basic Info

*Device Name: GWN7801 (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: 2023-12-25 17:18:00

*NTP Server: pool.ntp.org

Time Zone: (UTC+08:00) Beijing,Shanghai,Chongqing,Hong Kong,Uru...

DayLight Saving (DST) Mode: Recurring

*Offset (Min): 60 (Valid range is 1-1440)

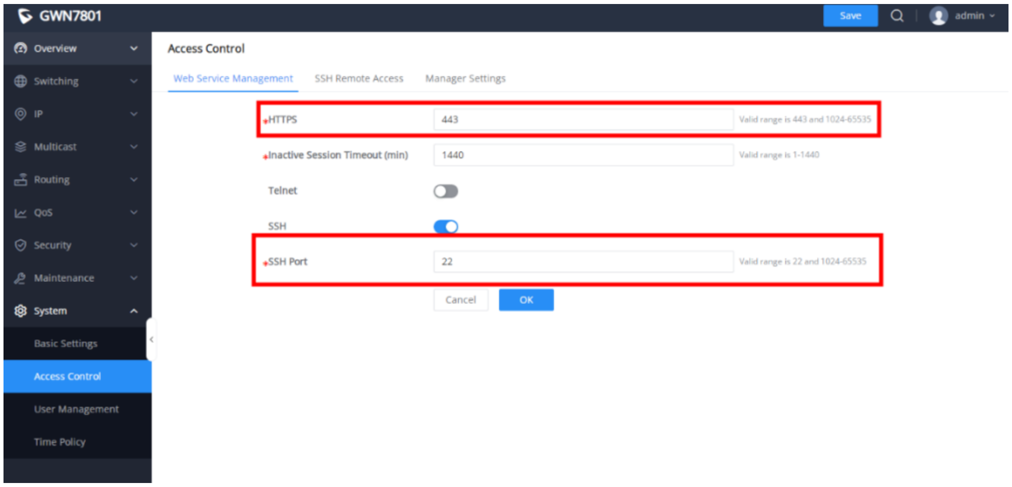
*Starting Time: Select time

*Ending Time: Select time

Scheduled Reboot

- **Add HTTPS/SSH port customization**

Users use customized HTTPS and SSH ports to access and configure device.



Access Control

*HTTPS: 443 (Valid range is 443 and 1024-65535)

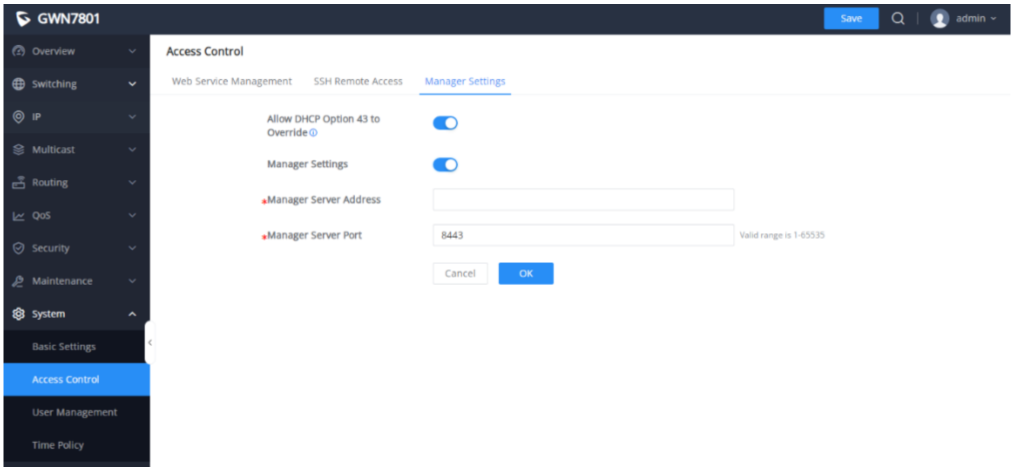
*Inactive Session Timeout (min): 1440 (Valid range is 1-1440)

Telnet: ○

SSH: ●

*SSH Port: 22 (Valid range is 22 and 1024-65535)

- **Optimize Manager settings**



Access Control

Allow DHCP Option 43 to Override ⓘ: on

Manager Settings: on

*Manager Server Address:

*Manager Server Port: 8443 Valid range is 1-65535

Cancel OK

- **Add GWN Manager takeover function**

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

FIRMWARE VERSION 1.0.3.37

PRODUCT NAME

GWN7801(P) / GWN7802(P) / GWN7803(P)

DATE

10/30/2023

FIRMWARE FILE INFORMATION

- GWN780x Firmware file name: gwn780xfw.bin

  MD5 checksum: f32b7e5265d345f4fd357fdb33b434ab

CHANGES/ENHANCEMENT

- Added support for GWN Cloud 1.1.25.23.
- Optimized CPU usage.
- Added support of SSH and TELNET in # mode.
- Added support of Dynamic Voice VLAN.
- Added support of voice VLAN OUI untagged mode.
- Added support of EXEC CLI config commands by GWN Cloud.
- Added support of backspace when using CLI.
- Fixed an issue that GWN7803P randomly get stuck.
- Fixed an issue that when configure two radius servers, after entering a wrong account, it will repeatedly ask to enter the account password, and the authentication status will not enter the lock state.
- Fixed an issue that after restarting, the path cost in the PVST port settings will become to the default value.
- Fixed an SSH issue that it lost the management IP address after changing the management IP address from DHCP to static.
- Fixed an LLDP/LLDP-MED issue that after restarting the device, the automatic voice network policy will be turned off.

- Fixed some issues related to Spanning Tree feature.
- Fixed some GWN Cloud related issues.
- Fixed some GWN Manager related issues.
- Improved some strings and translations.
- Internal bug fixes.

FIRMWARE VERSION 1.0.3.19

PRODUCT NAME

GWN7801(P) / GWN7802(P) / GWN7803(P)

DATE

6/15/2023

FIRMWARE FILE INFORMATION

- GWN780x Firmware file name: gwn780xfw.bin

  MD5 checksum: 9d77cf78b454a26c22216e20c78afbde

CHANGES/ENHANCEMENT

- Added feature of IPv6 RA, RS.
- Added feature of DHCP server.
- Added feature of DHCP relay.
- Added feature of ARP table.
- Added feature of routing table.
- Added feature of static routing.
- Added feature of time scheduling.
- Added feature of one key debugging.
- Added feature of copper test.
- Added support of port based enable/disable in QoS port priority.
- Added support of SP-WRR and SP-WFQ to queue policy of QoS.
- Added support of neighbor discovery.
- Added support of VPN IP interface configuration.
- Added support of switch IP interface DNS configuration.
- Added support of mDNS discovery.

- Added support of fan status to system information.
- Added support of ErrDisable status to port information.
- Added support of EEE.
- Added support of SSH/Telnet client.
- Added support of SSH remote access.
- Added support of Layer 2 and Layer 3 GWN Manager discovery.
- Optimized port information display.
- Optimized port power limitation for PoE models.
- Fixed an issue causing high CPU load.
- Internal bug fixes.

FIRMWARE VERSION 1.0.1.36

PRODUCT NAME

GWN7801(P) / GWN7802(P) / GWN7803(P)

DATE

4/18/2023

FIRMWARE FILE INFORMATION

- GWN780x Firmware file name: gwn780xfw.bin

  MD5 checksum: 44a95a0d0610cce7e2aa8ebdc7057c29

CHANGES/ENHANCEMENT

- Added DNS configurations for switch IP service.
- Fixed some webUI display issues.
- Fixed an issue which causes core file when creating a user with username longer than 32 characters.
- Fixed an issue that after VLAN is removed from a port, the PVID will not be automatically restored.
- Fixed an issue that causes monitor user lost.
- Fixed an issue of CLI command “show tech-support” causing long loading.
- Fixed an issue that port status display incorrectly when shutdown by loop detection.
- Fixed an issue that illegal NTP server settings cause boot abnormal.
- Internal bug fixes.

FIRMWARE VERSION 1.0.1.30

PRODUCT NAME

GWN7801(P) / GWN7802(P) / GWN7803(P)

DATE

2/7/2023

FIRMWARE FILE INFORMATION

- GWN780x Firmware file name: gwn780xfw.bin

  MD5 checksum: 6c24de94be8f8b1ecb1884aae02aabed

CHANGES/ENHANCEMENT

- Added
- Fixed the issue that GWN781x OSPF sometimes configuration loss after modifying the area, also added error prompt when the key character range is exceeded.
- Fixed the issue that after deleted a static NDP, it cannot re-create it.
- Fixed the issue that after unplugging ethernet cable on static IP interface, the IP address would change to 0.0.0.0.
- Fixed the issue that in very rare conditions that the device might automatically restart.
- Fixed the issue that when IPSG is enabled, sender with IP 0.0.0.0 still has ARP probe packets dropped.
- Fixed the issue that Time Policy allow create new policy with exist names.
- Fixed the issue that the switch obtains an ipv6 address stateless, but after the interface is down, the ipv6 address is still present.
- Fixed the issue that Neighbor Discovery query results for the web and CLI are incorrect.
- Fixed the issue that if OSPF key mode is set to md5, the key cannot be saved n plain text, and an error message is displayed.
- Fixed some issues when work with GWN Cloud.

- Internal bug fixes.

FIRMWARE VERSION 1.0.1.20

PRODUCT NAME

GWN7801(P) / GWN7802(P) / GWN7803(P)

DATE

12/7/2022

FIRMWARE FILE INFORMATION

- GWN780x Firmware file name: gwn780xfw.bin

  MD5 checksum: 4744afc107d6ca02b8e085a13c394eb3

CHANGES/ENHANCEMENT

- This is the first release of GWN780x.