

# GWN7806(P)/7816(P)/7832 Switch Firmware Release Notes

## IMPORTANT UPGRADING NOTE

1. Once GWN7806(P)/7816(P)/7832 upgraded to 1.0.9.15, downgrading to 1.0.3.x or 1.0.1.x firmware version is not allowed.

## Table of Content

<b>IMPORTANT UPGRADING NOTE .....</b>	<b>1</b>
<b>FIRMWARE FILE DOWNLOAD .....</b>	<b>3</b>
<b>FIRMWARE VERSION 1.0.9.15 .....</b>	<b>4</b>
PRODUCT NAME .....	4
DATE .....	4
FIRMWARE FILE INFORMATION .....	4
CHANGES/ENHANCEMENT.....	4
NEW FEATURE OVERVIEW.....	7
<b>FIRMWARE VERSION 1.0.3.8 .....</b>	<b>43</b>
PRODUCT NAME .....	43
DATE .....	43
FIRMWARE FILE INFORMATION .....	43
CHANGES/ENHANCEMENT.....	43
<b>FIRMWARE VERSION 1.0.3.3 .....</b>	<b>44</b>
PRODUCT NAME .....	44
DATE .....	44
FIRMWARE FILE INFORMATION .....	44
CHANGES/ENHANCEMENT.....	44
<b>FIRMWARE VERSION 1.0.1.14 .....</b>	<b>45</b>
PRODUCT NAME .....	45
DATE .....	45
FIRMWARE FILE INFORMATION .....	45
CHANGES/ENHANCEMENT.....	45

## 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

GWN7806(P) / GWN7816(P) / GWN7832

### DATE

8/29/2024

### FIRMWARE FILE INFORMATION

- GWN7806(P) Firmware file name: gwn7806fw.bin  
MD5 checksum: caaedf38dbc458559f734a6fcbf354be
- GWN7816(P) Firmware file name: gwn7816fw.bin  
MD5 checksum: caaedf38dbc458559f734a6fcbf354be
- GWN7832 Firmware file name: gwn7832fw.bin  
MD5 checksum: caaedf38dbc458559f734a6fcbf354be

### 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.
- 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.

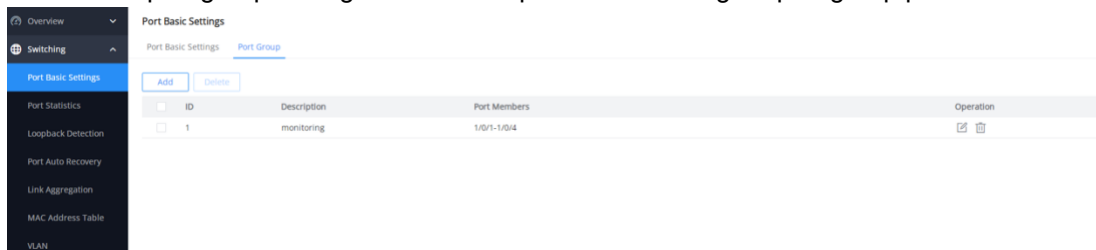
- Added untagged OUI mode for voice VLAN.
- Added gateway priority when using DHCP to get VLAN IP address.
- Added default gateway configuration under MGMT VLAN.
- Added ACL advanced settings, including mirroring, statistic and priority remapping for rule.
- Added rate limit by ACL binding to VLAN.
- 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.
- Optimized RIP/RIPng.
- Optimized CBS valid range in Queue Shaping.
- Optimized the rate limit groups from 32 to 128 in ACL.
- 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.
- 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 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

- **Add port groups**

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



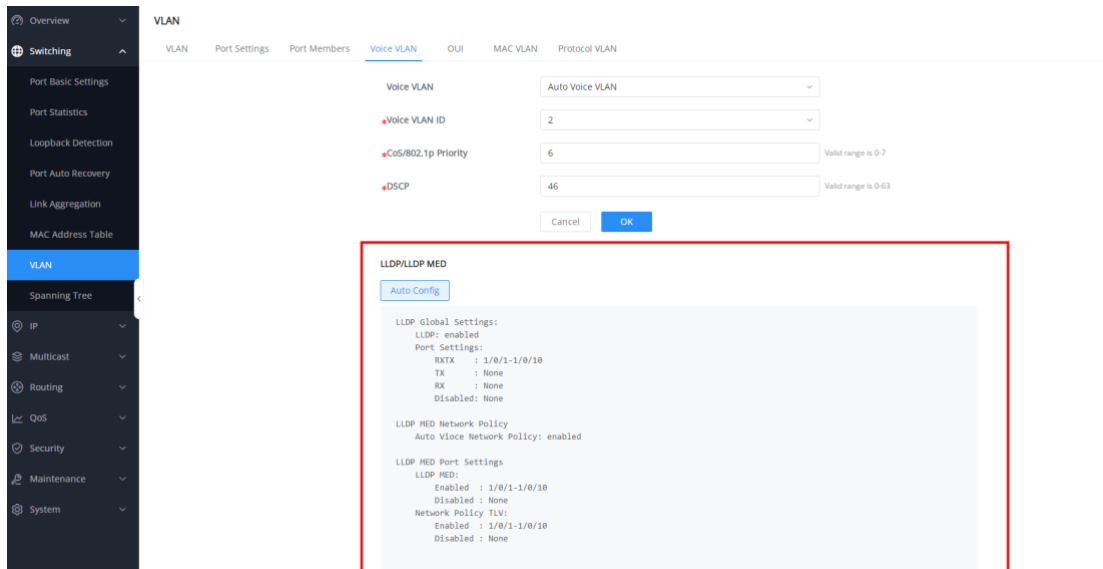
ID:  Valid range is 1-32  
 Description:  0-128 characters  
 Click on port to select/unselect

**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

- **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.



Overview  
 Switching  
 Port Basic Settings  
 Port Statistics  
 Loopback Detection  
 Port Auto Recovery  
 Link Aggregation  
 MAC Address Table  
**VLAN**  
 Spanning Tree  
 IP  
 Multicast  
 Routing  
 QoS  
 Security  
 Maintenance  
 System

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

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/LLDP MED**

Auto Config

```

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

LLDP MED Network Policy
Auto Voice 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

Mode

**Ignore VLAN in BPDU**

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

Enable Spanning Tree

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

\*Path Cost  Valid range is 0-65535

Edge Port  Auto  Enabled  Disabled

**Root Protection**

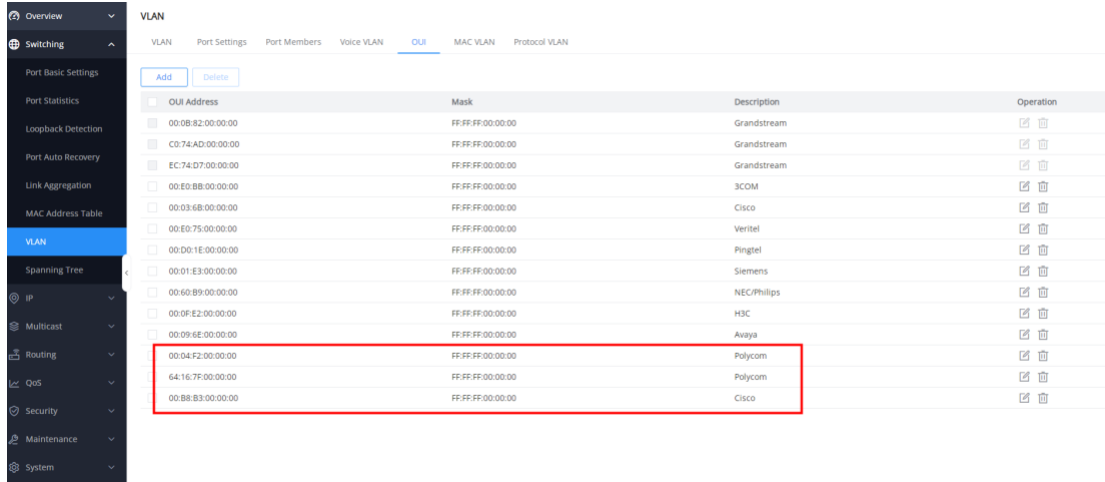
**Loop Protection**

BPDU Guard

BPDU Filter

Point-to-Point  Auto  Enabled  Disabled

- **Added more OUI in Voice VLAN**



OUI Address	Mask	Description	Operation
00:08:82:00:00:00	FF:FF:FF:00:00:00	Grandstream	[Edit] [Delete]
C0:74:AD:00:00:00	FF:FF:FF:00:00:00	Grandstream	[Edit] [Delete]
EC:74:D7:00:00:00	FF:FF:FF:00:00:00	Grandstream	[Edit] [Delete]
00:E0:BB:00:00:00	FF:FF:FF:00:00:00	3COM	[Edit] [Delete]
00:03:6B:00:00:00	FF:FF:FF:00:00:00	Cisco	[Edit] [Delete]
00:E0:75:00:00:00	FF:FF:FF:00:00:00	Veritel	[Edit] [Delete]
00:D0:1E:00:00:00	FF:FF:FF:00:00:00	Pingtel	[Edit] [Delete]
00:01:E3:00:00:00	FF:FF:FF:00:00:00	Siemens	[Edit] [Delete]
00:60:B9:00:00:00	FF:FF:FF:00:00:00	NEC/Philips	[Edit] [Delete]
00:0F:E2:00:00:00	FF:FF:FF:00:00:00	H3C	[Edit] [Delete]
00:09:6E:00:00:00	FF:FF:FF:00:00:00	Avaya	[Edit] [Delete]
00:04:F2:00:00:00	FF:FF:FF:00:00:00	Polycom	[Edit] [Delete]
64:16:7F:00:00:00	FF:FF:FF:00:00:00	Polycom	[Edit] [Delete]
00:88:B3:00:00:00	FF:FF:FF:00:00:00	Cisco	[Edit] [Delete]

- **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.

VLAN IP Interface

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

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:

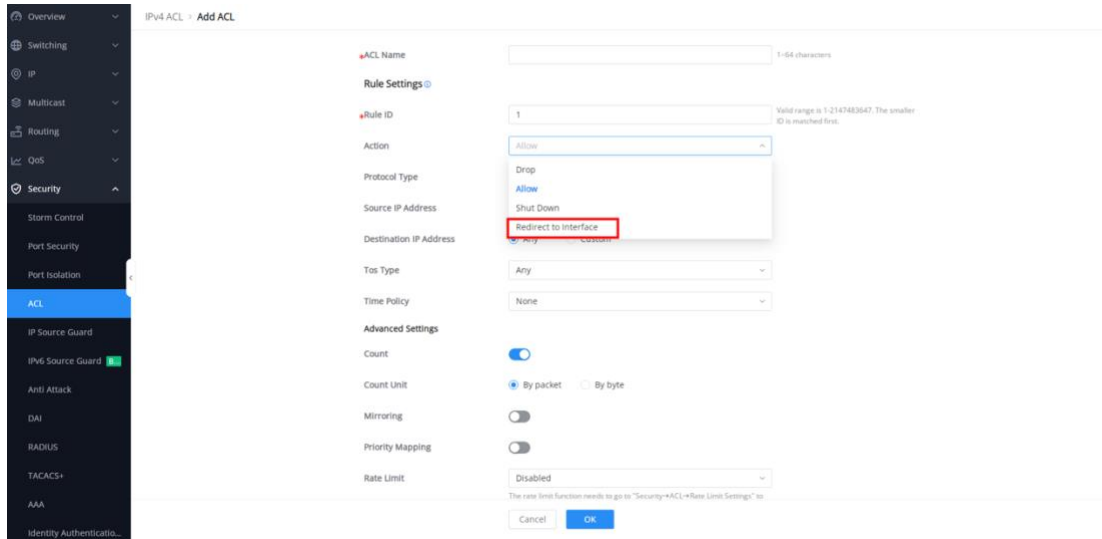
Cancel   OK

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**

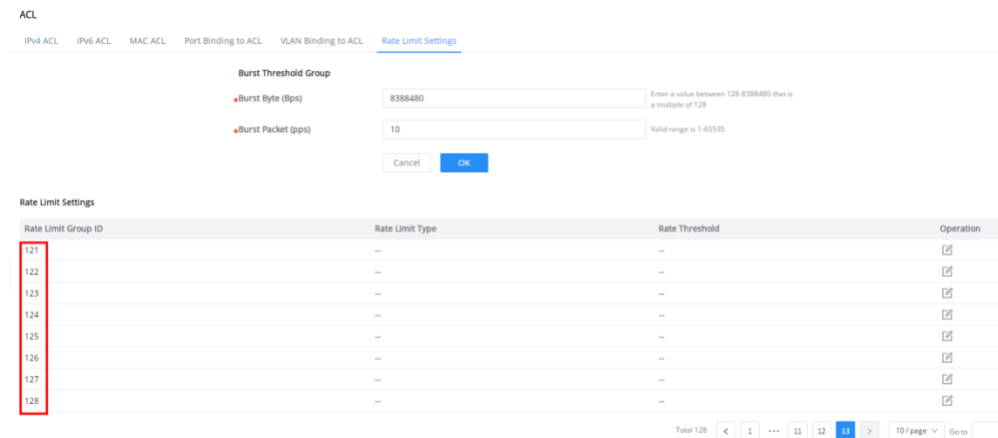
The function of redirecting ACL rules to interfaces is added.

Note: The selected interface does not contain the interface bound by the ACL.



- **Optimized the rate limit groups from 32 to 128 in ACL**

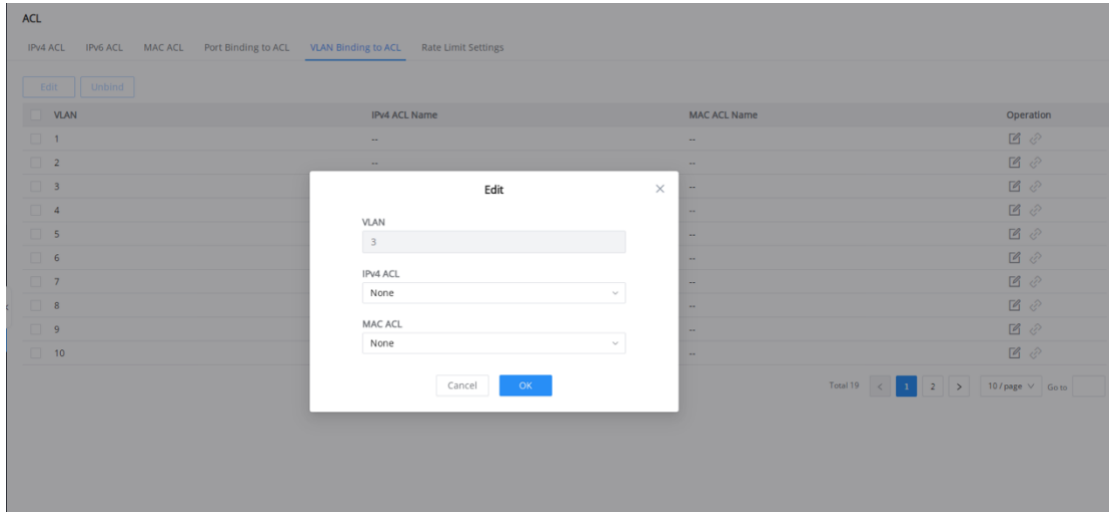
The ACL rate limit group has been expanded from 32 groups to 128 groups.



- **Added VLAN binding to ACL function**

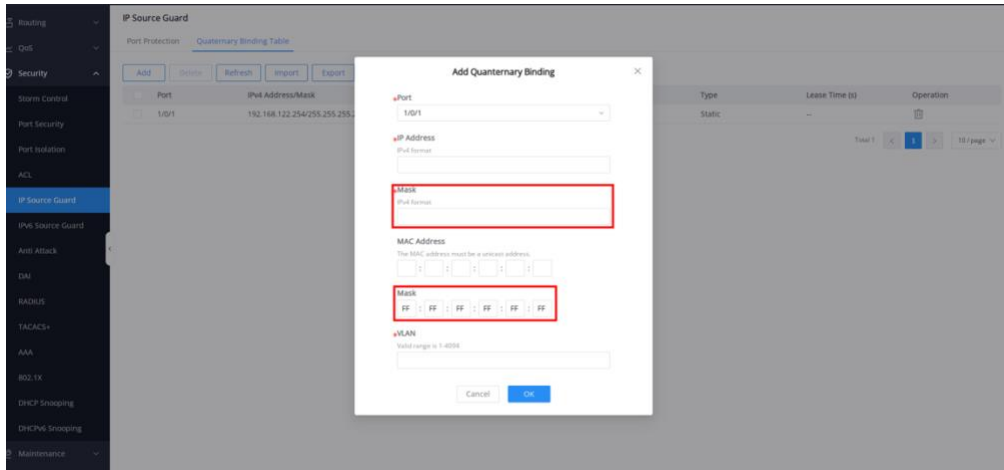
Added the binding of ACLs to VLANs.

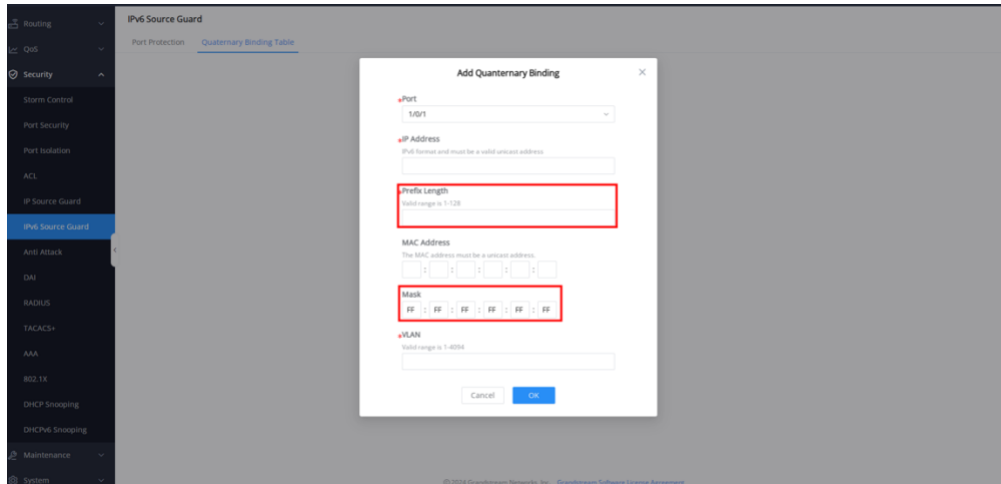
Note: The binding of IPv6 ACLs to VLANs is not supported.



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

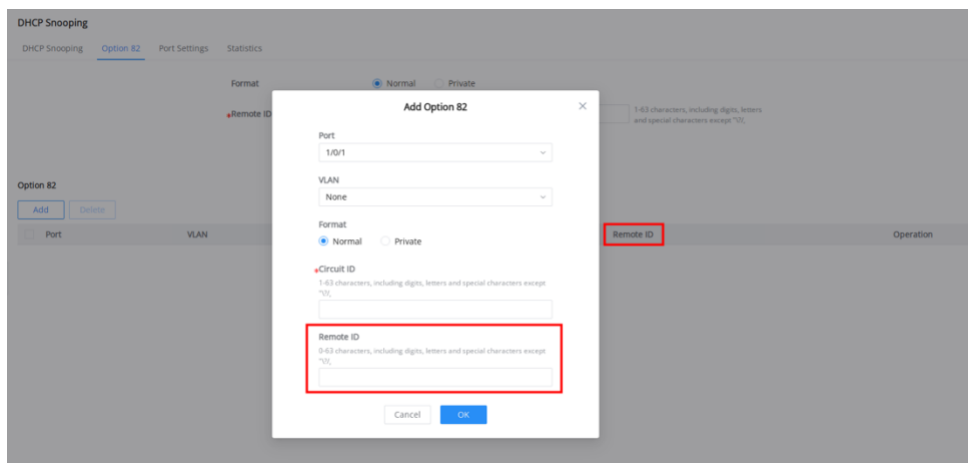
In the quaternary binding table of IPSG and IPv6SG, the mask configuration is added for the IP address and MAC address to expand the coverage of the binding table.





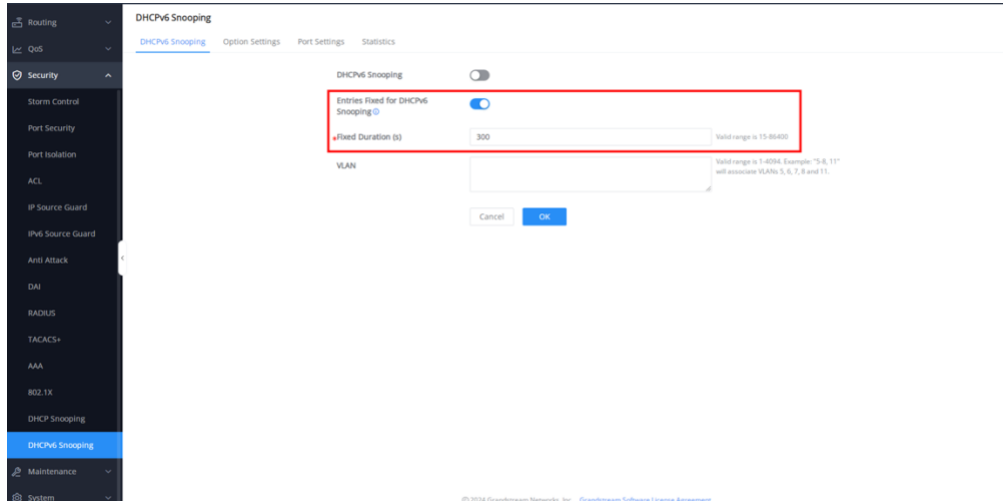
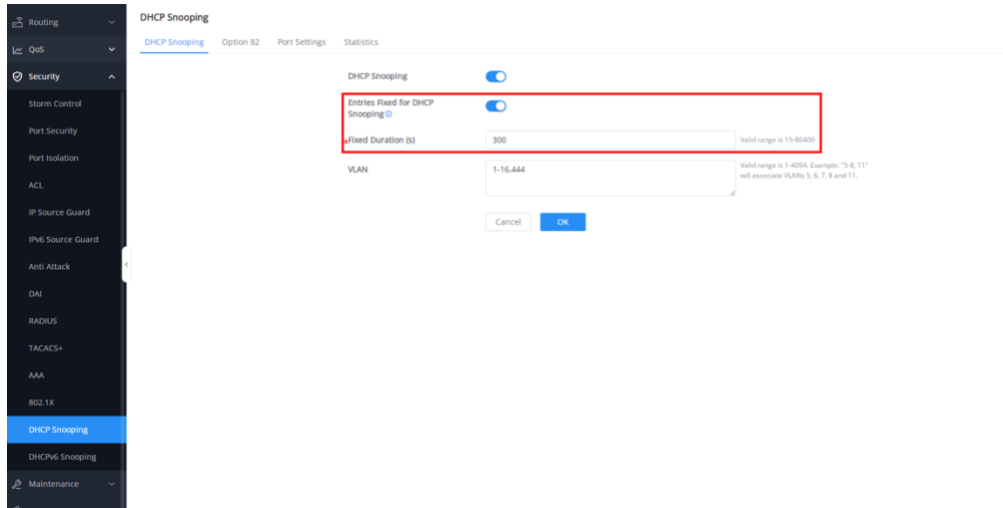
- **Added remote-ID configuration based on port for DHCP Snooping**

Added use of port-based configuration for remote IDs.



- **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.



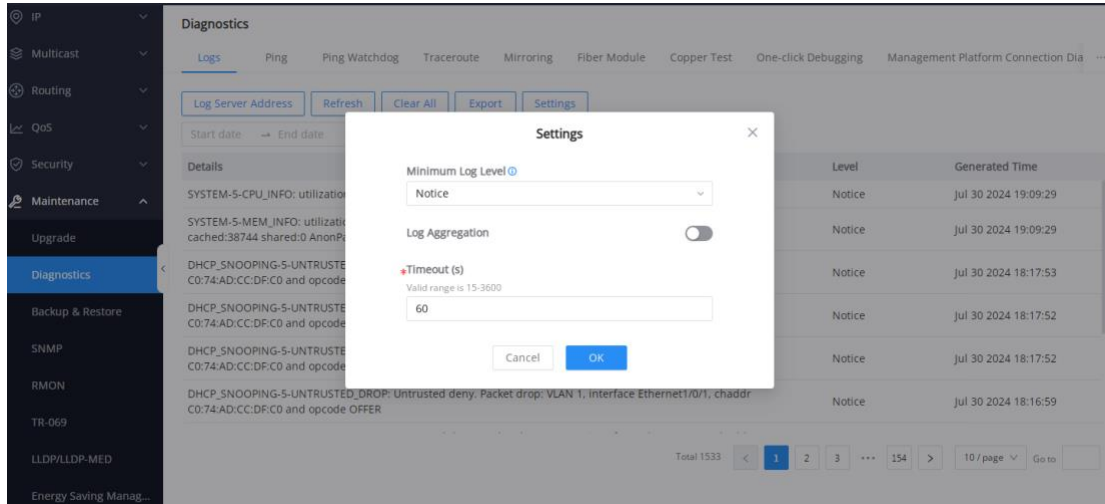
- **Added flow upgrade for upgrade via manual upload**

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**

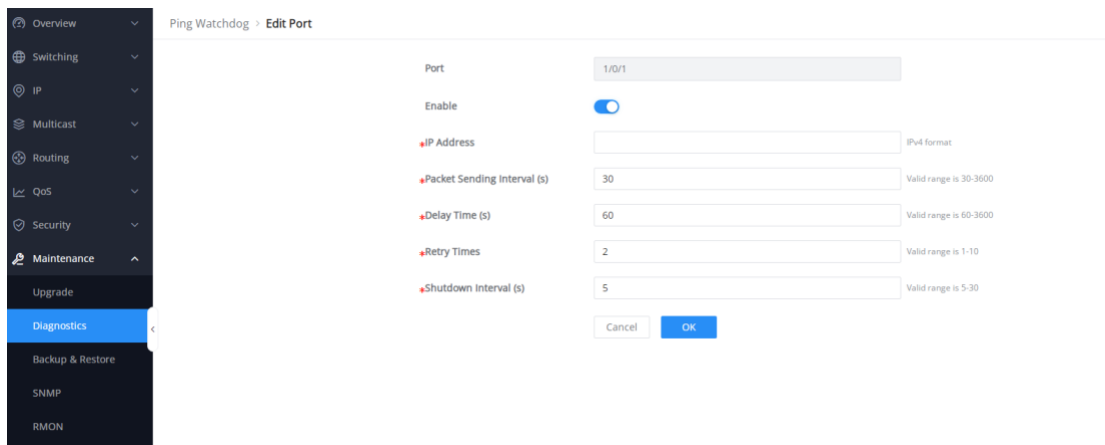
Increase the minimum print level of web logs.

The log aggregation function is added to merge and display the same logs within a certain period.



- **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



- **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

**Diagnostics**

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

Remote VLAN  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	--	--	--	--	--	--	<input type="checkbox"/> ↻
2	SPAN	--	--	--	--	--	--	<input type="checkbox"/> ↻
3	SPAN	--	<u>1</u>	--	--	--	--	<input type="checkbox"/> ↻
4	SPAN	--	--	--	--	--	--	<input type="checkbox"/> ↻

### 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

Group:

Mode:

Role:  (highlighted in red box)

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

Egress Mirroring

Click on port to select/unselect

### Flow-based (ACL)-based RSPAN:

Select an image group in ACL Image



IPv4 ACL > test Rule Details > Edit Rule

**Rule Settings**

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

Action:

Protocol Type:

Source IP Address:  Any  Custom

Destination IP Address:  Any  Custom

Tos Type:

Time Policy:

**Advanced Settings**

Count:

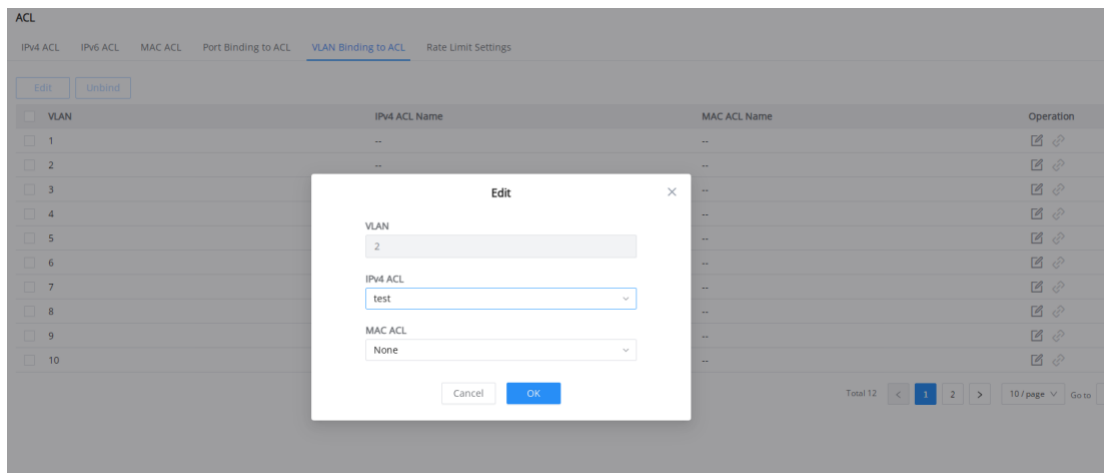
Mirroring:

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

Priority Mapping:

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

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



ACL

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

Table:

VLAN	IPv4 ACL Name	MAC ACL Name	Operation
<input type="checkbox"/> 1	--	--	<input type="checkbox"/> <input type="checkbox"/>
<input type="checkbox"/> 2	--	--	<input type="checkbox"/> <input type="checkbox"/>
<input type="checkbox"/> 3	--	--	<input type="checkbox"/> <input type="checkbox"/>
<input type="checkbox"/> 4	--	--	<input type="checkbox"/> <input type="checkbox"/>
<input type="checkbox"/> 5	--	--	<input type="checkbox"/> <input type="checkbox"/>
<input type="checkbox"/> 6	--	--	<input type="checkbox"/> <input type="checkbox"/>
<input type="checkbox"/> 7	--	--	<input type="checkbox"/> <input type="checkbox"/>
<input type="checkbox"/> 8	--	--	<input type="checkbox"/> <input type="checkbox"/>
<input type="checkbox"/> 9	--	--	<input type="checkbox"/> <input type="checkbox"/>
<input type="checkbox"/> 10	--	--	<input type="checkbox"/> <input type="checkbox"/>

Dialog Box: Edit

VLAN:

IPv4 ACL:

MAC ACL:

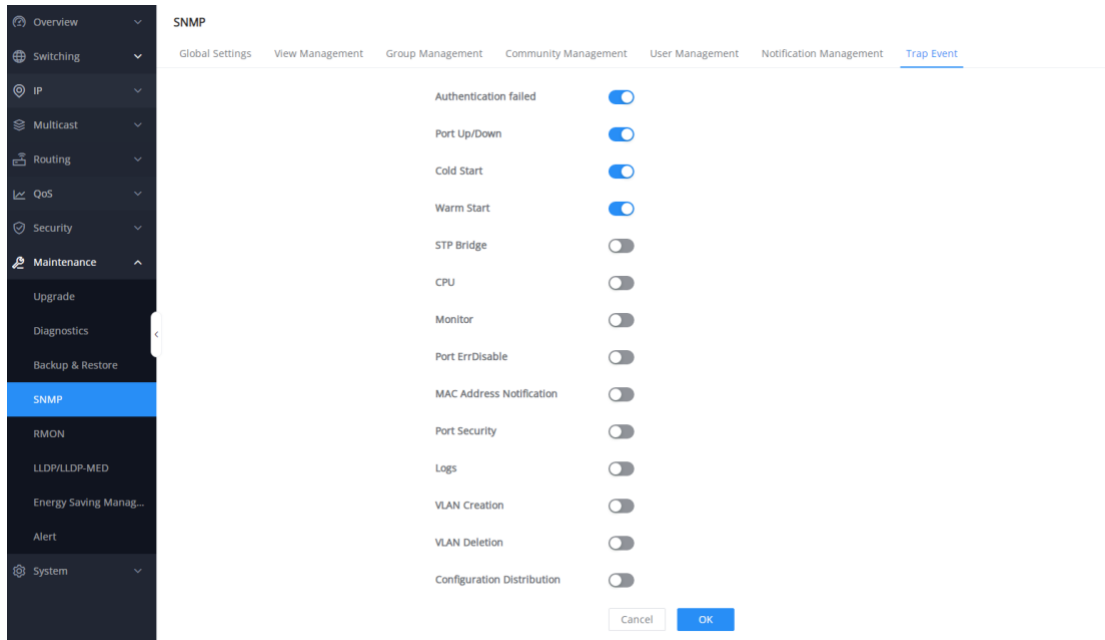
Total 12 < 1 2 > 10 / page Go to

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
<input type="button" value="Cancel"/> <input type="button" value="OK"/>	

- **Added new traps in SNMP**

Add more traps.



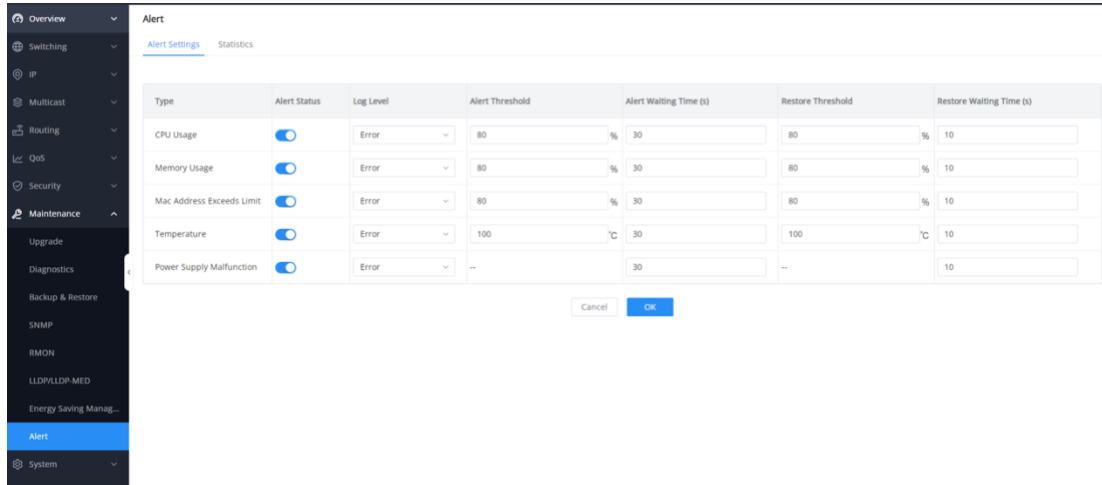
SNMP	
Global Settings View Management Group Management Community Management User Management Notification Management <u>Trap Event</u>	
Authentication failed	<input checked="" type="checkbox"/>
Port Up/Down	<input checked="" type="checkbox"/>
Cold Start	<input checked="" type="checkbox"/>
Warm Start	<input checked="" type="checkbox"/>
STP Bridge	<input type="checkbox"/>
CPU	<input type="checkbox"/>
Monitor	<input type="checkbox"/>
Port ErrDisable	<input type="checkbox"/>
MAC Address Notification	<input type="checkbox"/>
Port Security	<input type="checkbox"/>
Logs	<input type="checkbox"/>
VLAN Creation	<input type="checkbox"/>
VLAN Deletion	<input type="checkbox"/>
Configuration Distribution	<input type="checkbox"/>
<input type="button" value="Cancel"/> <input type="button" value="OK"/>	

- **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.

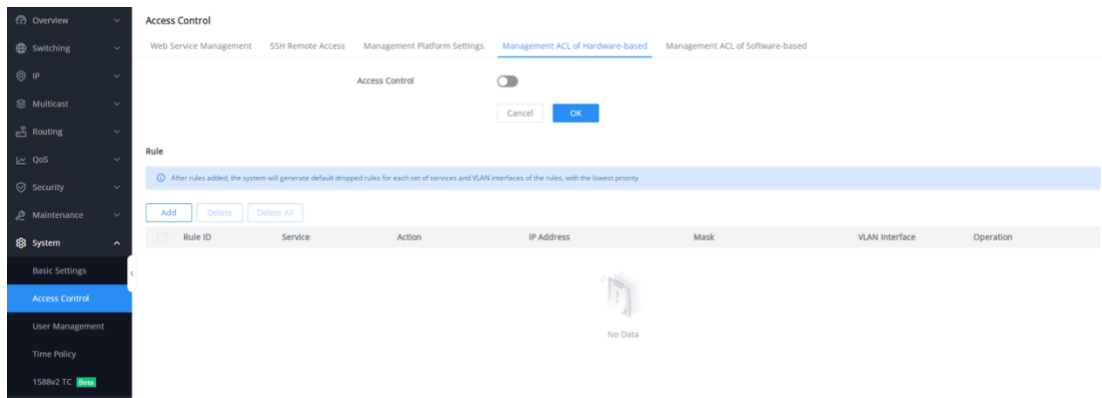


Type	Alert Status	Log Level	Alert Threshold	Alert Waiting Time (s)	Restore Threshold	Restore Waiting Time (s)
CPU Usage	<input checked="" type="checkbox"/>	Error	80 %	30	80 %	10
Memory Usage	<input checked="" type="checkbox"/>	Error	80 %	30	80 %	10
Mac Address Exceeds Limit	<input checked="" type="checkbox"/>	Error	80 %	30	80 %	10
Temperature	<input checked="" type="checkbox"/>	Error	100 °C	30	100 °C	10
Power Supply Malfunction	<input checked="" type="checkbox"/>	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

Rule

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

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

Management ACL of Hardware-based > Add

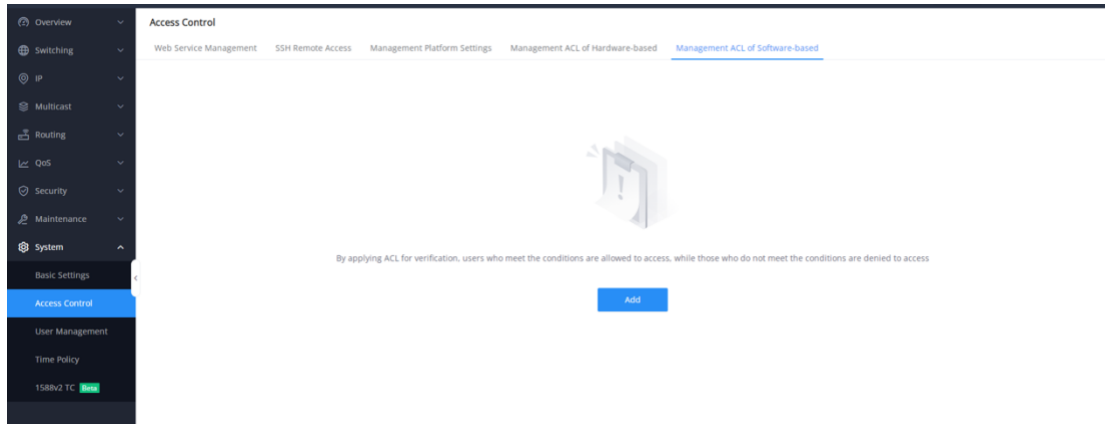
Valid range is 1-2147483647. The smaller ID is matched first.

Action  Allow  Drop

IPv4 format

IPv4 format

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



### Management ACL of Software-based > Add ACL

1-64 characters

**Rule Settings**

Rule ID 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

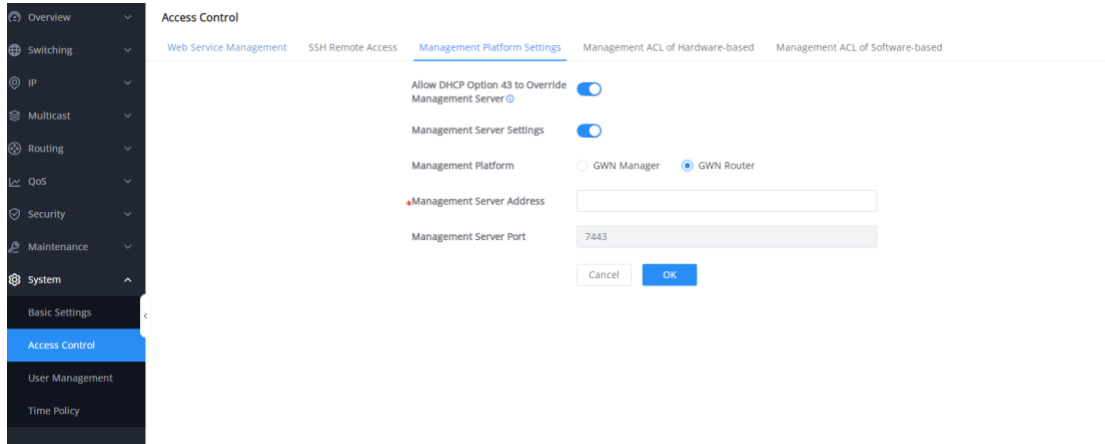
2	4	6	8	10	12	14	16	18	20	22	24				
1	3	5	7	9	11	13	15	17	19	21	23	25 SFP+	26 SFP+	27 SFP+	28 SFP+

LAG

2	4	6	8	10	12	14
1	3	5	7	9	11	13

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

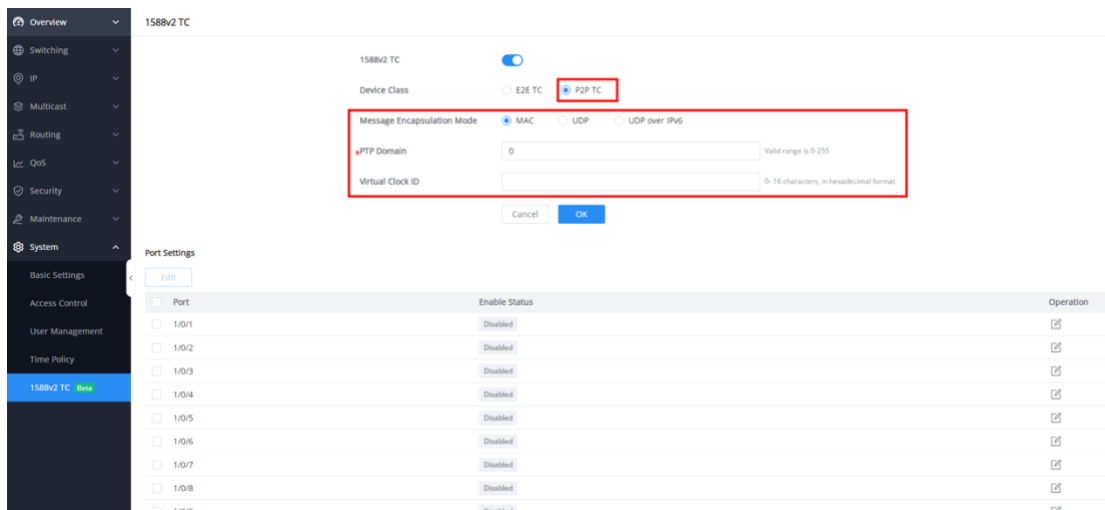
Layer 3 discovery of switches by cross-network segments and GWN routers is added. You need to set the Layer 3 server address and port on the switch.



- **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).



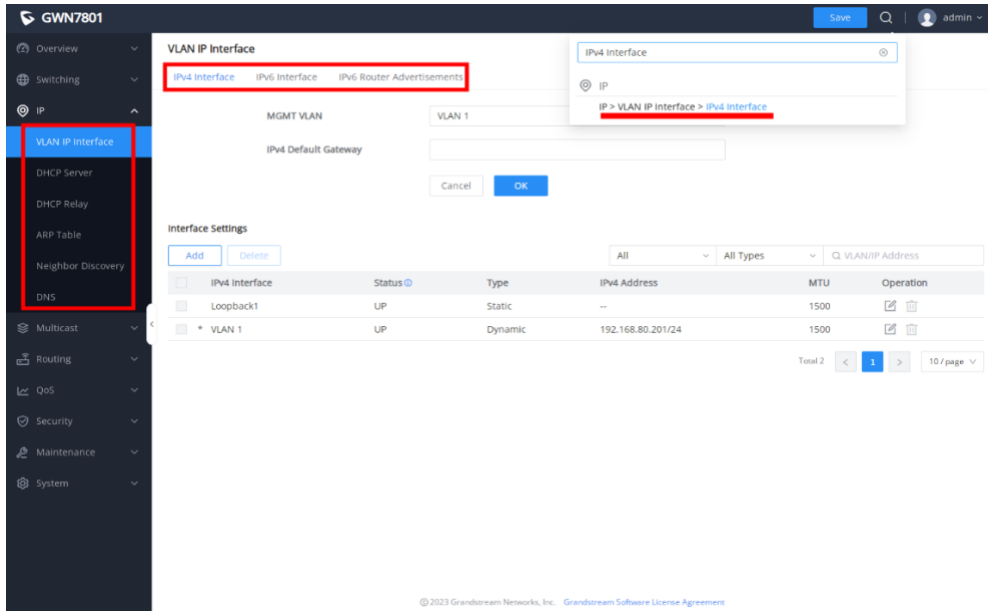
- **Added recovery function**

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

For details, see the Recovery User Guide.

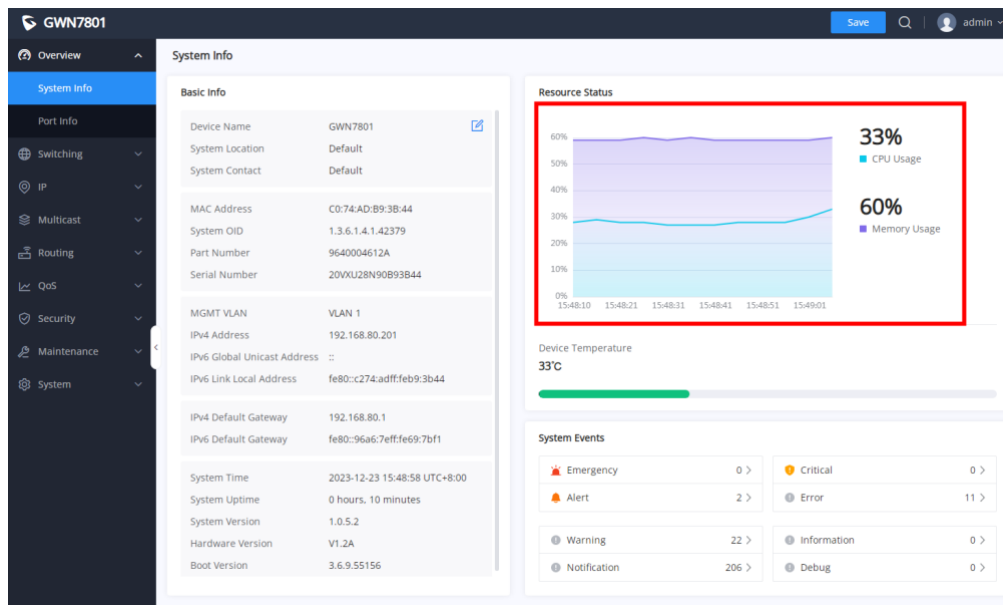
- **Optimize searching for WEB GUI**

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.



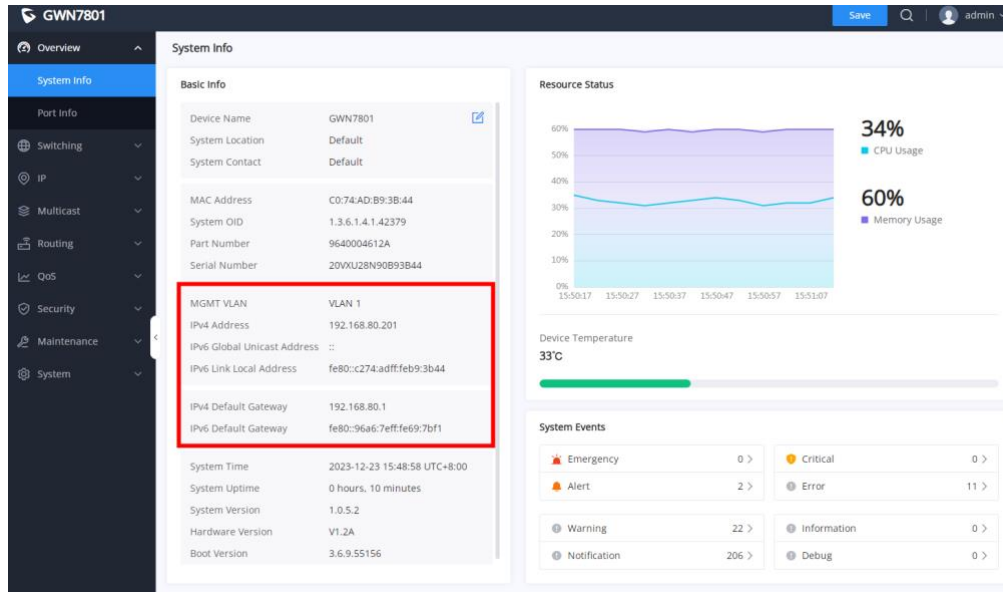
- **Optimize CPU and memory usage in Web GUI**

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



- **Optimize device IP address display**

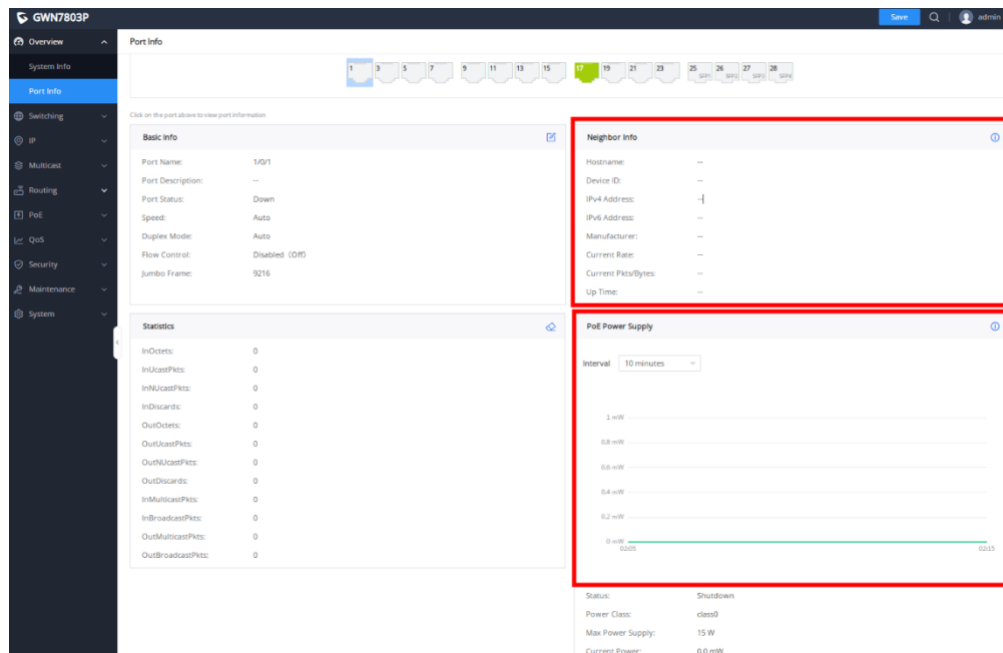
Displays the IP address information of the management VLAN, including the IPv4 address, IPv6 link-local address, and global unicast address, and also displays the switch default gateway address.



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

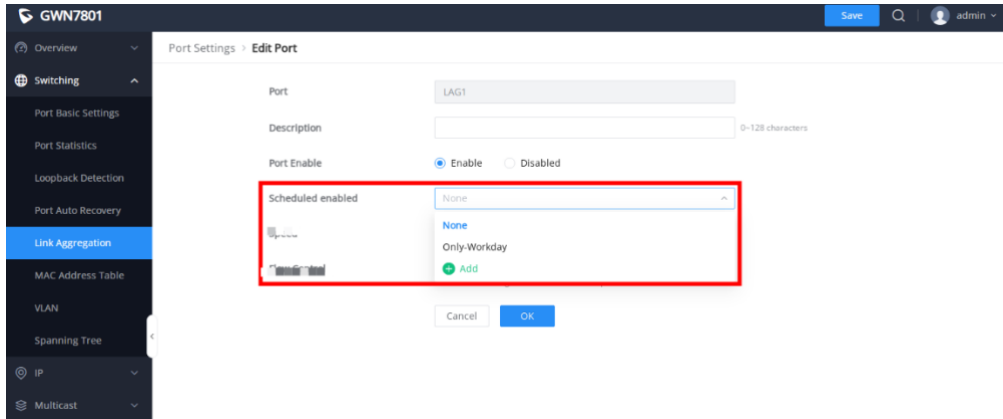
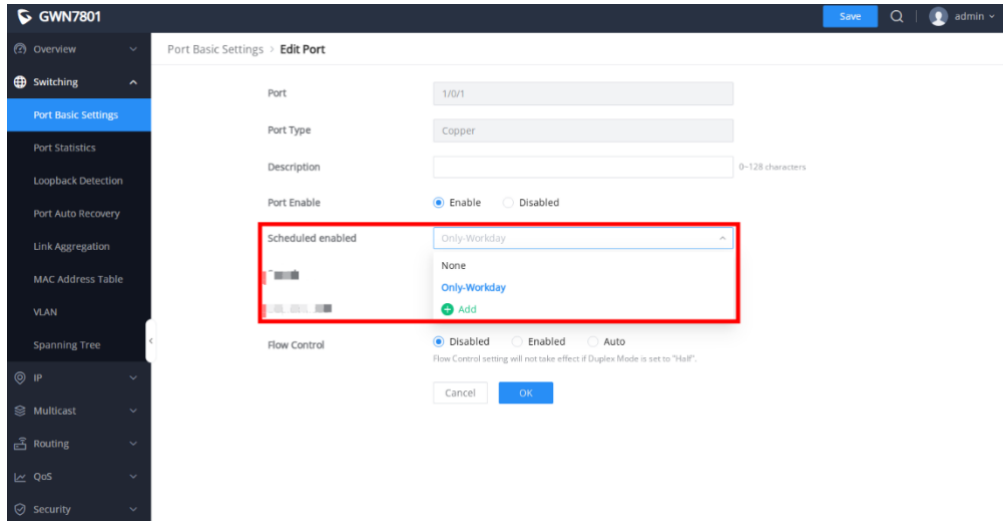
Supports viewing the port neighbor information, including device name, MAC address, IP address, speed, and connection duration.

Supports viewing the PoE power history to help troubleshoot PoE power supply.



- **Add port scheduled enabling feature**

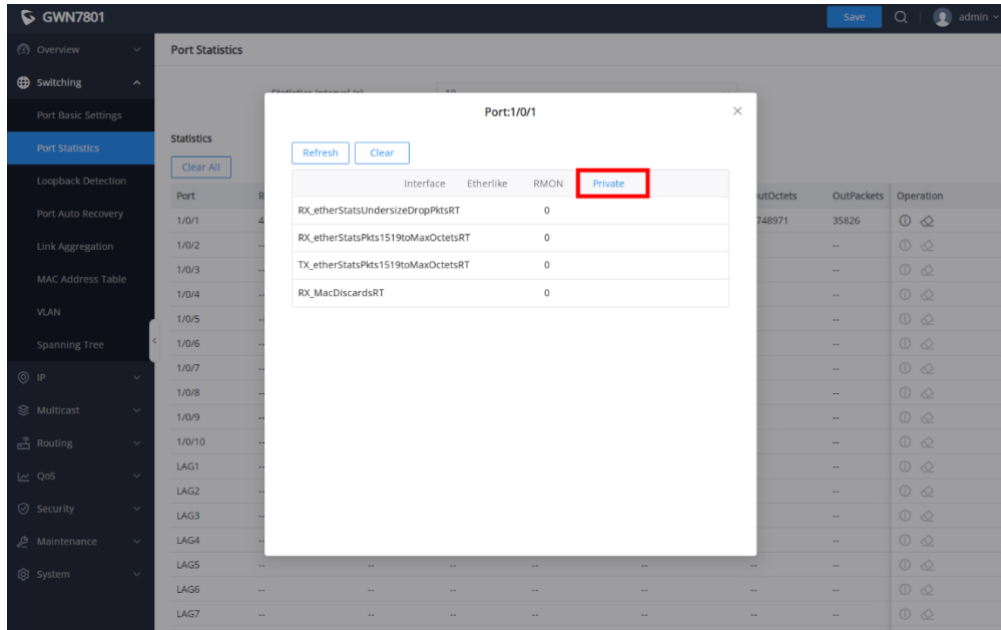
You can customize the Scheduled enable time for a port, including physical ports and LAGs.



- **Add more port statistics info**

Support viewing port Private MIB information.

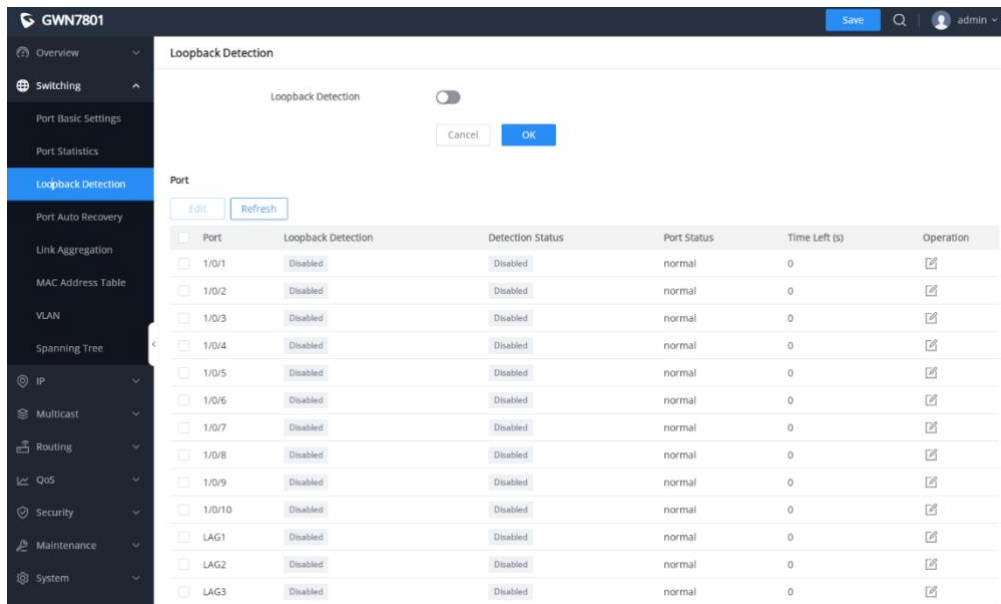




- **Add loopback detection**

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.

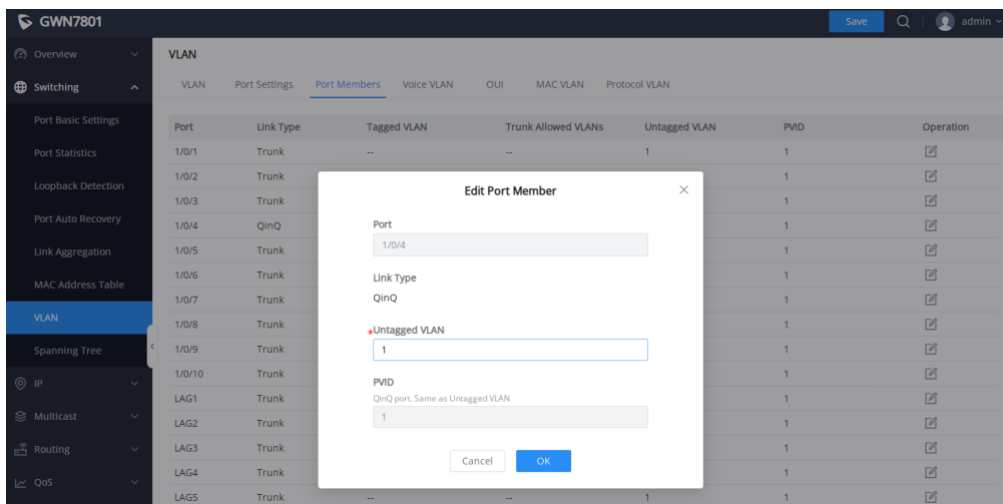
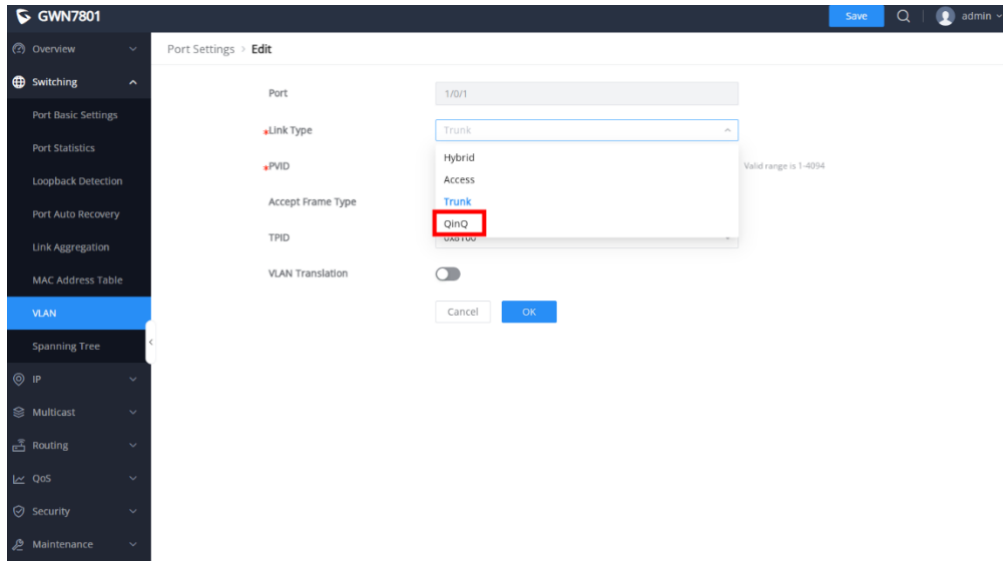
Note: If STP is enabled, STP loop protection takes precedence over interface loop protection, that is, interface loop protection will not take effect.



- **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.



- **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.

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	--	--	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	

**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

PVID  
Trunk port. Same as Untagged VLAN

VLAN

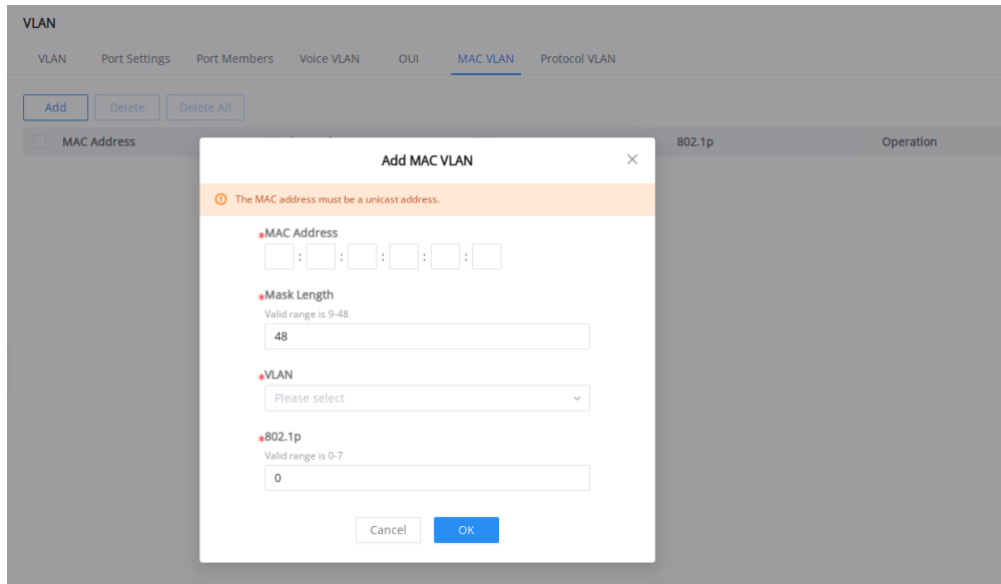
VLAN Port Settings **Port Members** Voice VLAN OUI MAC VLAN Protocol VLAN

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	

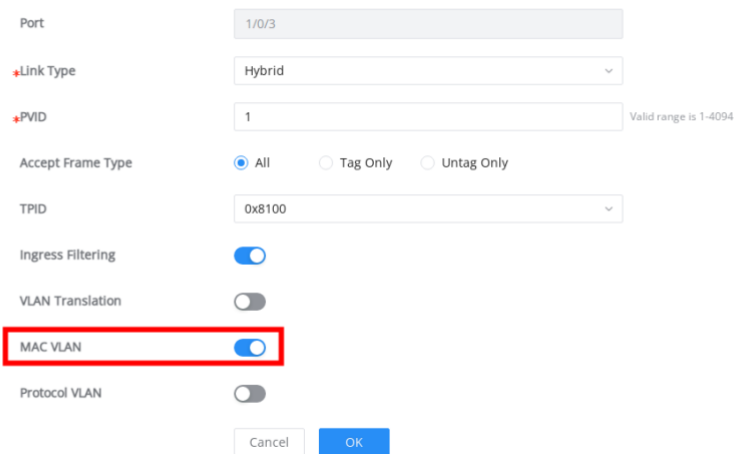
- **Add MAC-based VLAN**

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.



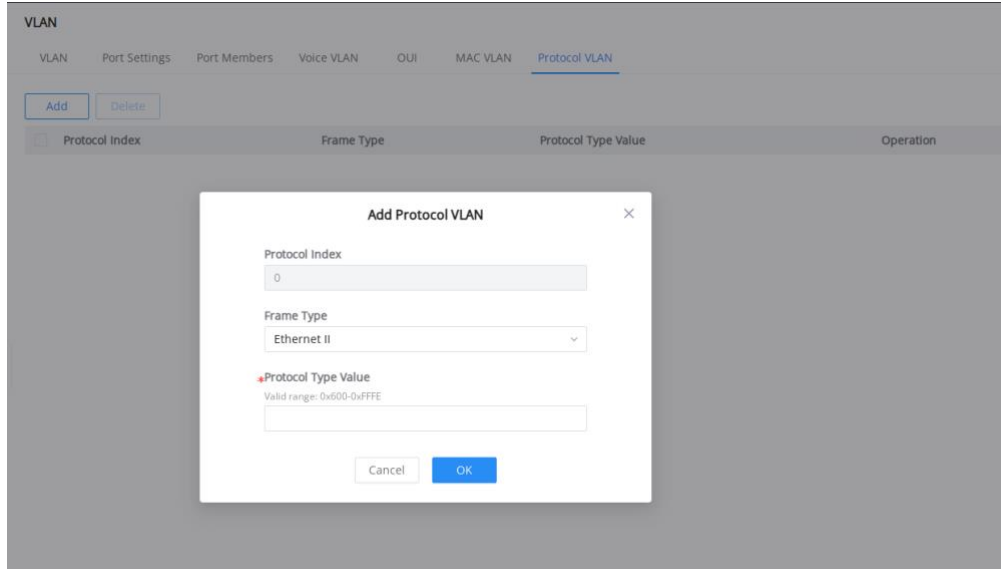
Port Settings > Edit



- **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.



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:  VLAN:  802.1p:

Add

Cancel OK

- **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:

Ingress:

**VLAN Mapping1**

Outer VLAN:

VLAN after Outer Mapping:

Add 

- **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.

VLAN

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

Voice VLAN: Untagged OUI

Voice VLAN ID:  Valid range is 0-7

CoS/802.1p Priority:

CoS Remarking:

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

Untagged OUI

Disabled

Auto Voice VLAN

Tagged OUI

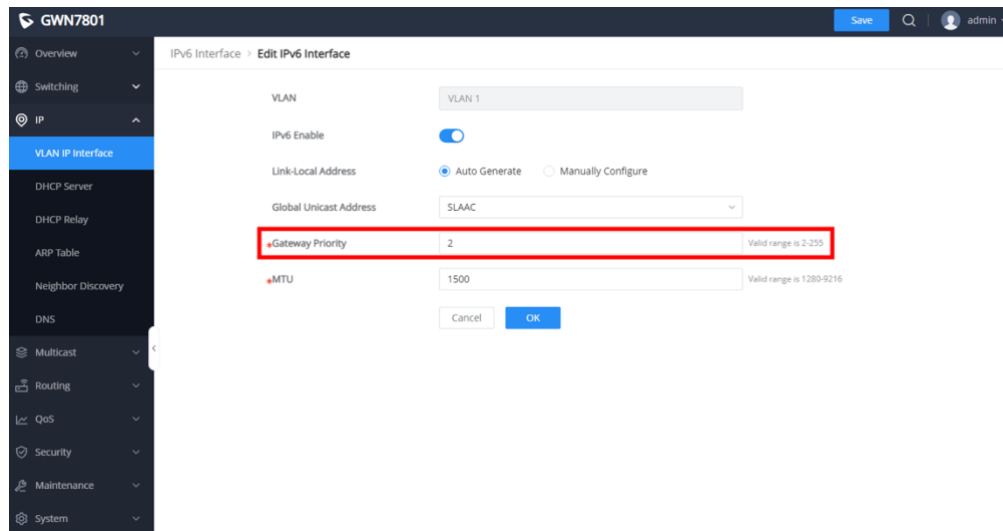
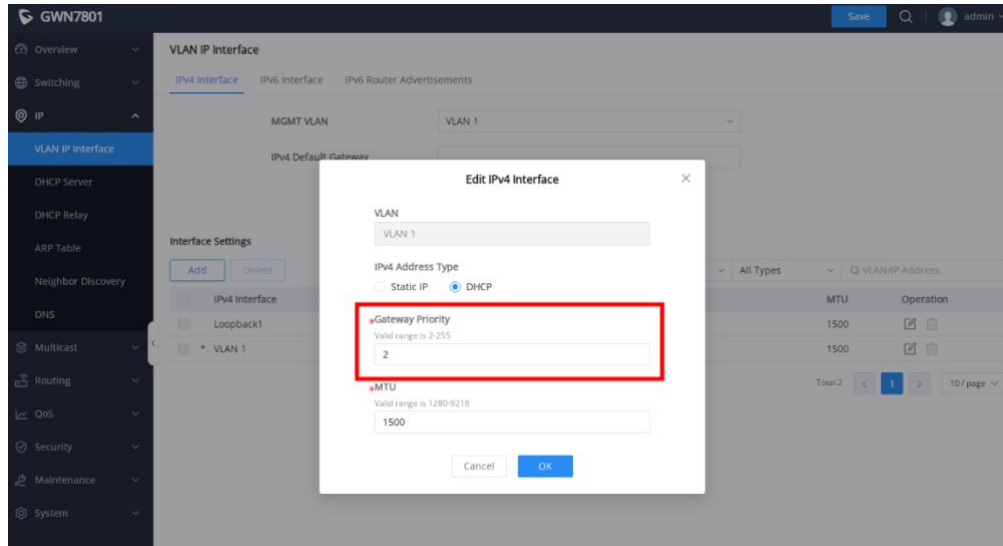
**Untagged OUI**

- **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.

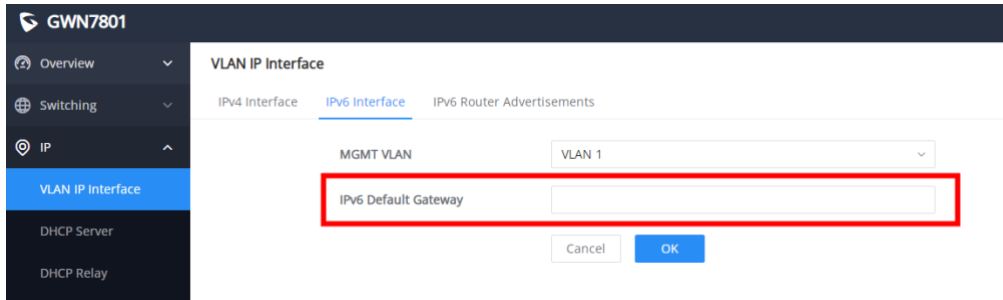
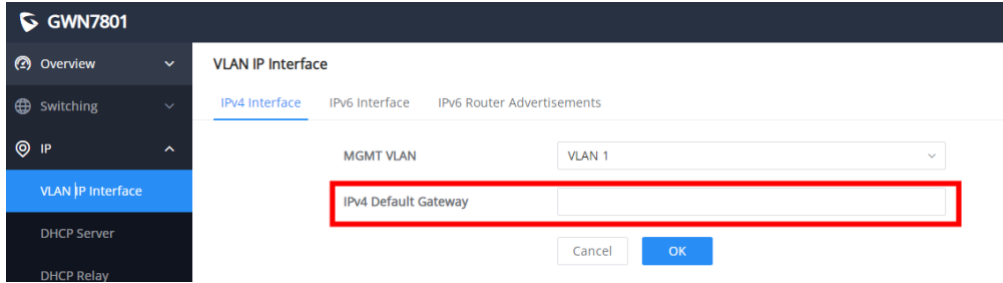
Note: The gateway priority is: statically configured gateway > gateway with a set priority (the smaller the priority value, the greater the priority) > gateway obtained from DHCP on the VLAN interface (VLAN

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.



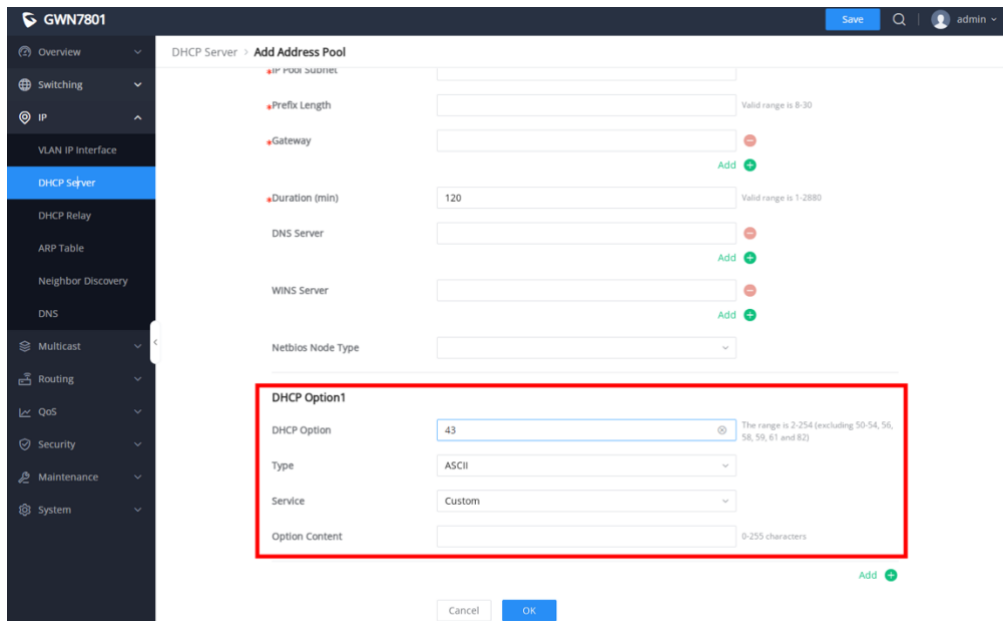
- **Add default gateway configuration under MGMT VLAN**

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.



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

Supports configuring specified services for DHCP Option 43.





- **Optimize routing table**

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

Routing Table

IPv4 Routing Table IPv6 Routing Table

Refresh

All Types

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

Total 2 < 1 > 10 / page

- **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

Time Policy

**Advanced Settings**

Count

\*Count ID  Valid range is 1-32

Count Unit  By packet  By byte

Mirroring

\*Mirroring Group

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

Priority Mapping

\*Priority  Valid range is 0-7

Rate Limit

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

- **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**  1-64 characters

**Rule Settings**

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

**Action**

**Protocol Type**

**Source IP Address**  Any  Custom

**Destination IP Address**  Any  Custom

**Tos Type**

**Time Policy**

**Advanced Settings**

**Count**

**Mirroring**

**Priority Mapping**

**Rate Limit**

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

VLAN bind ACL:

ACL

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

VLAN	IPv4 ACL Name	MAC ACL Name	Operation
<input type="checkbox"/> 1	--	--	<input type="checkbox"/> <input type="checkbox"/>
<input type="checkbox"/> 2			<input type="checkbox"/> <input type="checkbox"/>
<input type="checkbox"/> 3			<input type="checkbox"/> <input type="checkbox"/>
<input type="checkbox"/> 4			<input type="checkbox"/> <input type="checkbox"/>
<input type="checkbox"/> 5			<input type="checkbox"/> <input type="checkbox"/>
<input type="checkbox"/> 6			<input type="checkbox"/> <input type="checkbox"/>
<input type="checkbox"/> 7			<input type="checkbox"/> <input type="checkbox"/>
<input type="checkbox"/> 8			<input type="checkbox"/> <input type="checkbox"/>
<input type="checkbox"/> 9			<input type="checkbox"/> <input type="checkbox"/>
<input type="checkbox"/> 10			<input type="checkbox"/> <input type="checkbox"/>

**Edit** ✕

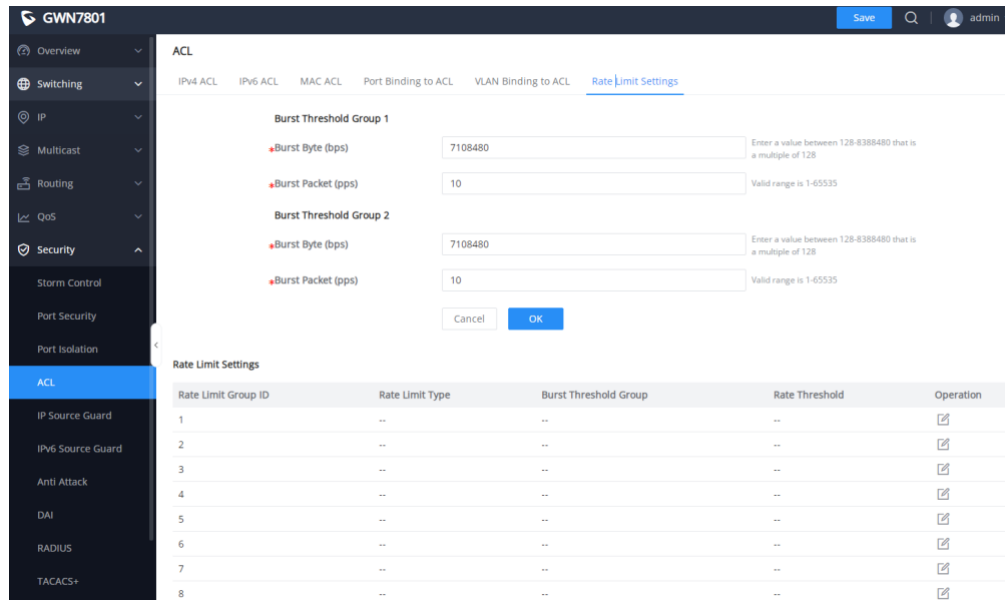
**VLAN**

**IPv4\_ACL**

**MAC\_ACL**

Total 19 < 1 2 > 10/page Go to

Speed limit group settings:



**ACL**

IPV4 ACL   IPV6 ACL   MAC ACL   Port Binding to ACL   VLAN Binding to ACL   Rate Limit Settings

**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**

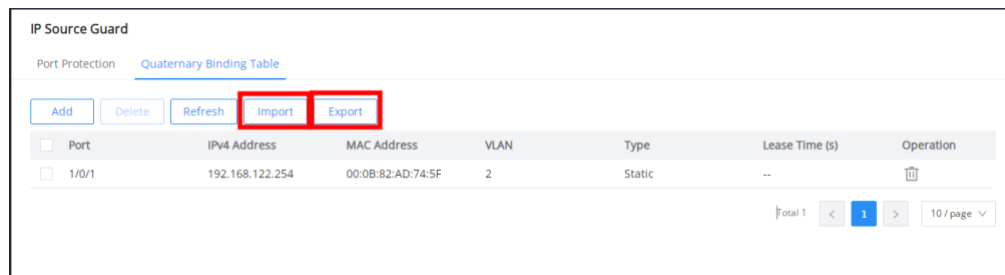
- Burst Byte (bps): 7108480 (Enter a value between 128-8388480 that is a multiple of 128)
- Burst Packet (pps): 10 (Valid range is 1-65535)

Cancel   **OK**

**Rate Limit Settings**

Rate Limit Group ID	Rate Limit Type	Burst Threshold Group	Rate Threshold	Operation
1	--	--	--	<input checked="" type="checkbox"/>
2	--	--	--	<input checked="" type="checkbox"/>
3	--	--	--	<input checked="" type="checkbox"/>
4	--	--	--	<input checked="" type="checkbox"/>
5	--	--	--	<input checked="" type="checkbox"/>
6	--	--	--	<input checked="" type="checkbox"/>
7	--	--	--	<input checked="" type="checkbox"/>
8	--	--	--	<input checked="" type="checkbox"/>

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



**IP Source Guard**

Port Protection   Quaternary Binding Table

Add   Delete   Refresh   **Import**   **Export**

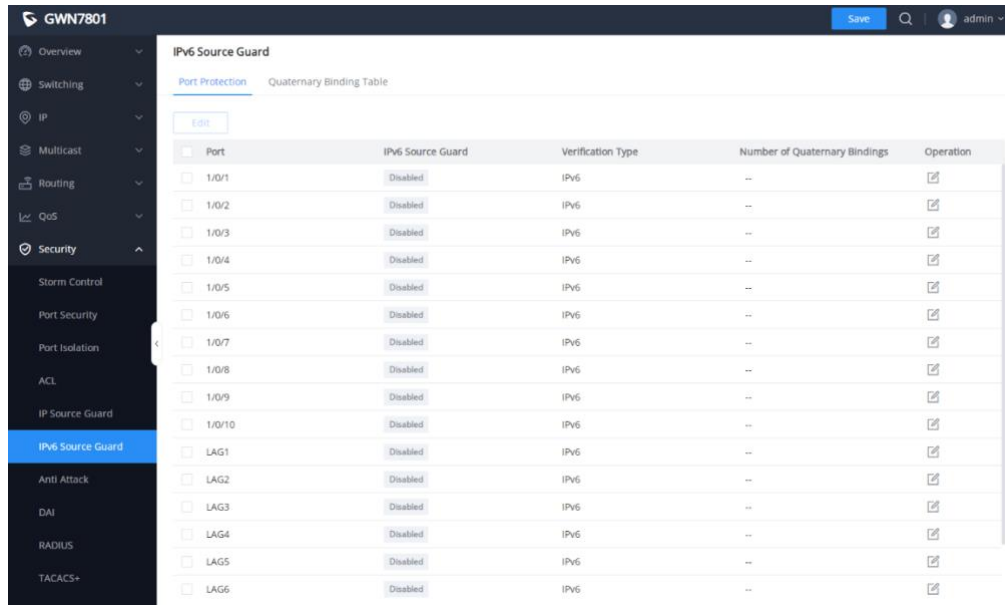
Port	IPv4 Address	MAC Address	VLAN	Type	Lease Time (s)	Operation
<input type="checkbox"/> 1/0/1	192.168.122.254	00:08:82:AD:74:5F	2	Static	--	<input type="checkbox"/> <input checked="" type="checkbox"/>

Total 1   < 1 >   10 / page

- **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.

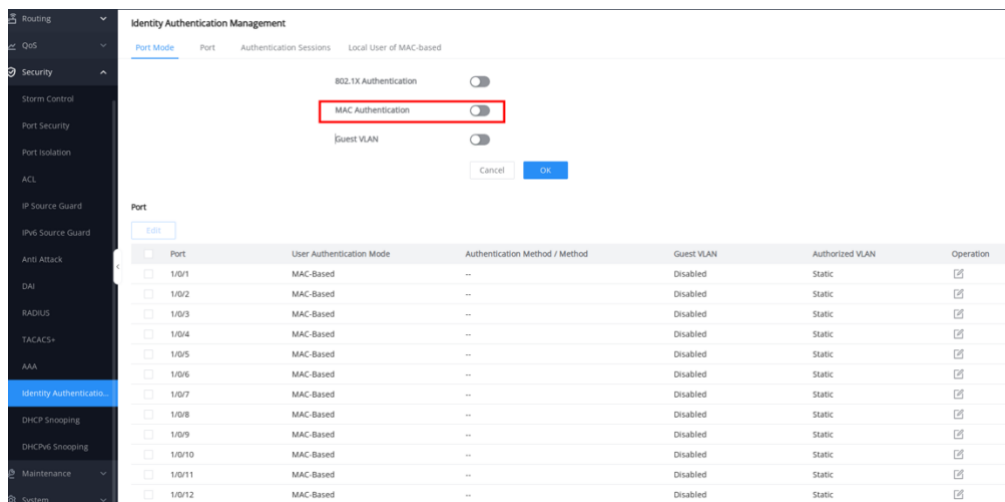


The screenshot shows the IPv6 Source Guard configuration page in the GWN7801 web interface. The left sidebar is expanded to 'Security' > 'IPv6 Source Guard'. The main content area has two tabs: 'Port Protection' (selected) and 'Quaternary Binding Table'. Below the tabs is an 'Edit' button and a table with the following data:

Port	IPv6 Source Guard	Verification Type	Number of Quaternary Bindings	Operation
<input type="checkbox"/> 1/0/1	Disabled	IPv6	--	
<input type="checkbox"/> 1/0/2	Disabled	IPv6	--	
<input type="checkbox"/> 1/0/3	Disabled	IPv6	--	
<input type="checkbox"/> 1/0/4	Disabled	IPv6	--	
<input type="checkbox"/> 1/0/5	Disabled	IPv6	--	
<input type="checkbox"/> 1/0/6	Disabled	IPv6	--	
<input type="checkbox"/> 1/0/7	Disabled	IPv6	--	
<input type="checkbox"/> 1/0/8	Disabled	IPv6	--	
<input type="checkbox"/> 1/0/9	Disabled	IPv6	--	
<input type="checkbox"/> 1/0/10	Disabled	IPv6	--	
<input type="checkbox"/> LAG1	Disabled	IPv6	--	
<input type="checkbox"/> LAG2	Disabled	IPv6	--	
<input type="checkbox"/> LAG3	Disabled	IPv6	--	
<input type="checkbox"/> LAG4	Disabled	IPv6	--	
<input type="checkbox"/> LAG5	Disabled	IPv6	--	
<input type="checkbox"/> LAG6	Disabled	IPv6	--	

- **Add MAC bypass authentication**

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

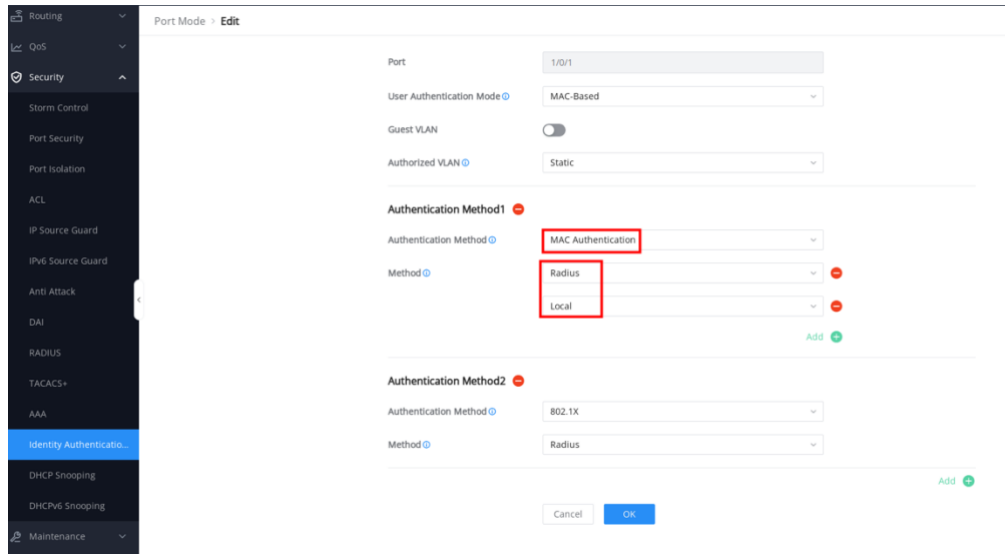


The screenshot shows the Identity Authentication Management configuration page. The left sidebar is expanded to 'Security' > 'Identity Authentication'. The main content area has four tabs: 'Port Mode' (selected), 'Port', 'Authentication Sessions', and 'Local User of MAC-based'. Under 'Port Mode', there are three toggle switches: '802.1X Authentication' (disabled), 'MAC Authentication' (highlighted with a red box and enabled), and 'Guest VLAN' (disabled). Below the toggles are 'Cancel' and 'OK' buttons. Below the configuration area is a 'Port' section with an 'Edit' button and a table with the following data:

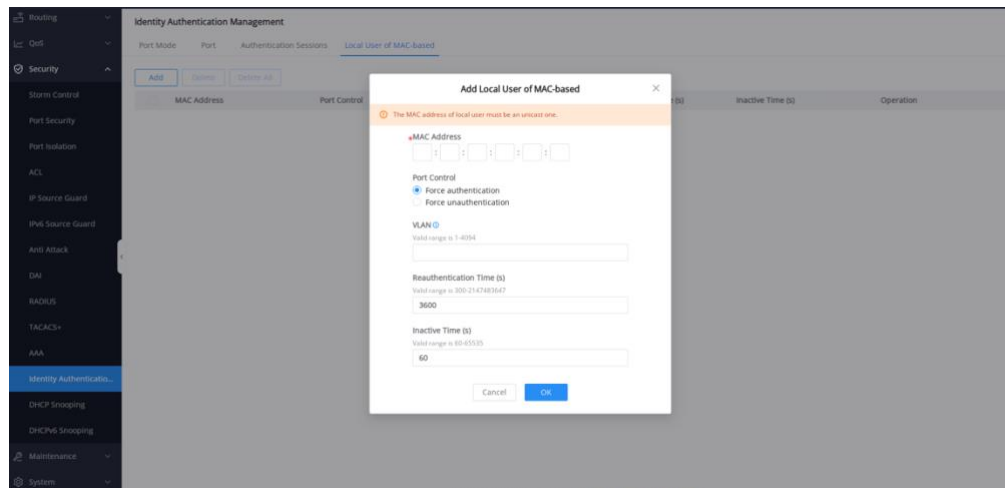
Port	User Authentication Mode	Authentication Method / Method	Guest VLAN	Authorized VLAN	Operation
<input type="checkbox"/> 1/0/1	MAC-Based	--	Disabled	Static	
<input type="checkbox"/> 1/0/2	MAC-Based	--	Disabled	Static	
<input type="checkbox"/> 1/0/3	MAC-Based	--	Disabled	Static	
<input type="checkbox"/> 1/0/4	MAC-Based	--	Disabled	Static	
<input type="checkbox"/> 1/0/5	MAC-Based	--	Disabled	Static	
<input type="checkbox"/> 1/0/6	MAC-Based	--	Disabled	Static	
<input type="checkbox"/> 1/0/7	MAC-Based	--	Disabled	Static	
<input type="checkbox"/> 1/0/8	MAC-Based	--	Disabled	Static	
<input type="checkbox"/> 1/0/9	MAC-Based	--	Disabled	Static	
<input type="checkbox"/> 1/0/10	MAC-Based	--	Disabled	Static	
<input type="checkbox"/> 1/0/11	MAC-Based	--	Disabled	Static	
<input type="checkbox"/> 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.



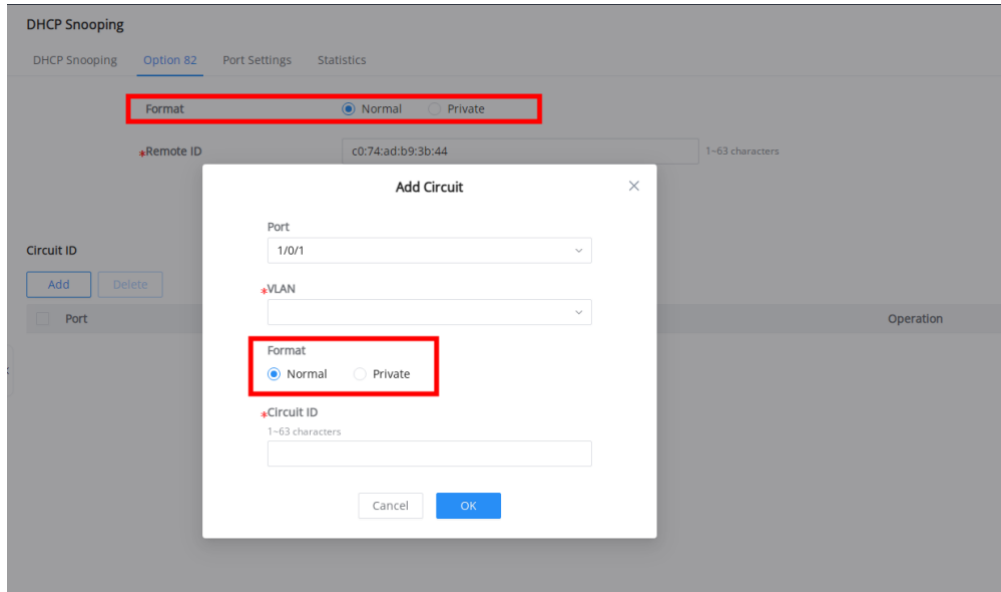
To add a MAC-based local user, you need to add the MAC address, port control mode, VLAN authorized for use after authentication, re-authentication time, and inactive time.



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

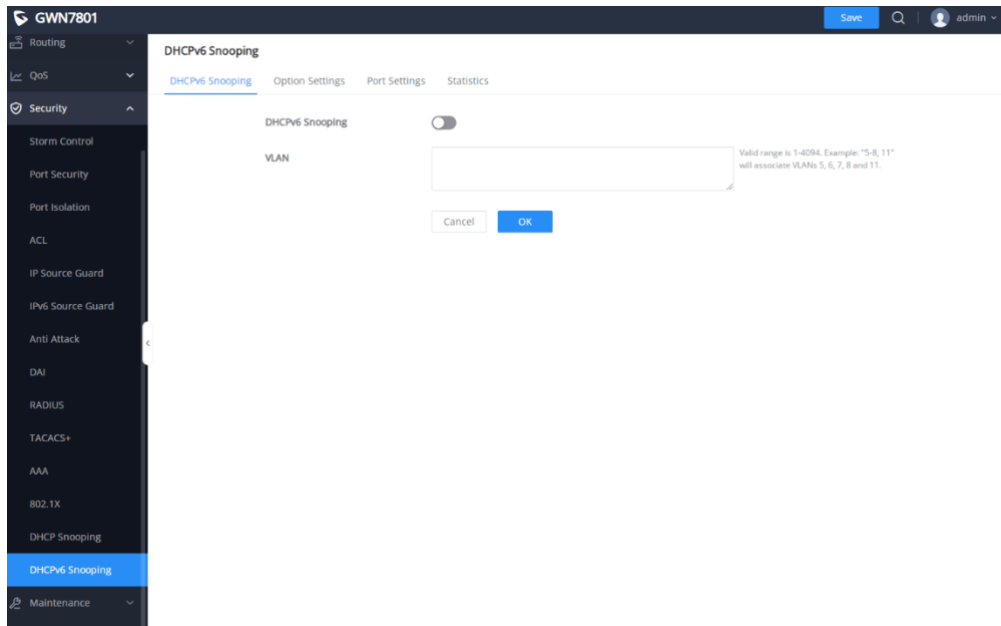
The Remote ID and Circuit ID of Option 82 can be configured in standard format and private format. Standard format: The default format is set according to TLV (type-length-value).

Private format: Only Value is used for setting.



- **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.



- **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  Supported file formats: bin

**Upgrade via Network**

Allow DHCP Option 43/160/66 to Override Server

Firmware Upgrade Protocol

Firmware Server Path

FTP/Explicit FTPS/HTTP/HTTPS Username

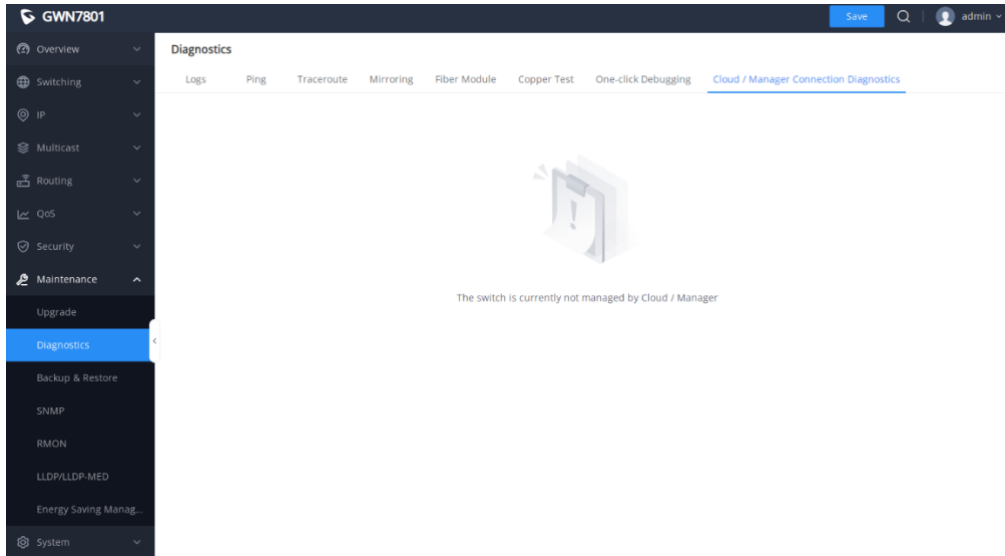
FTP/Explicit FTPS/HTTP/HTTPS Password

Check/Download New Firmware at Bootup

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

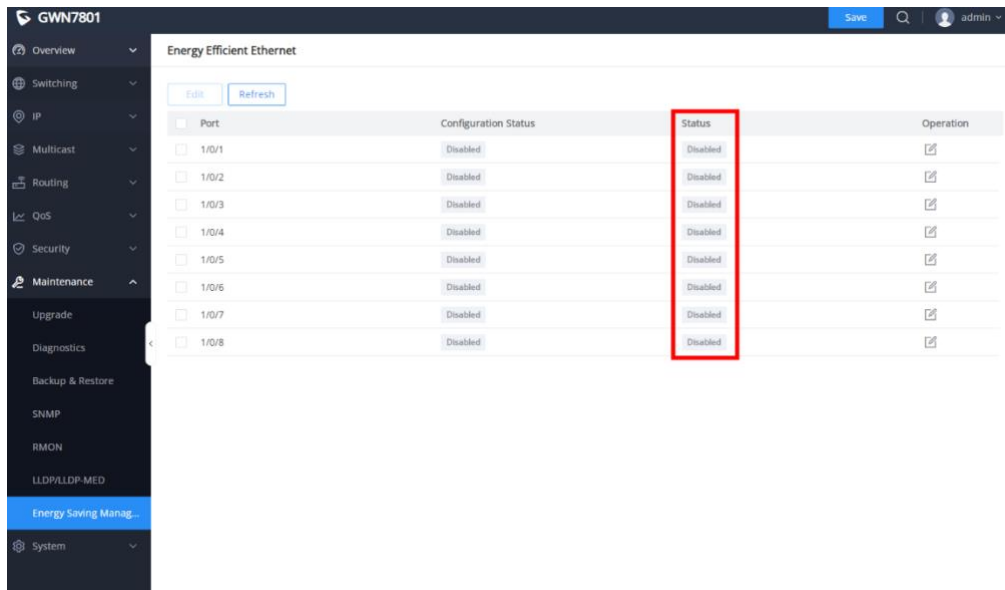
- **Add connection diagnostics with GWN.Cloud/Manager**

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.



- **Optimize EEE**

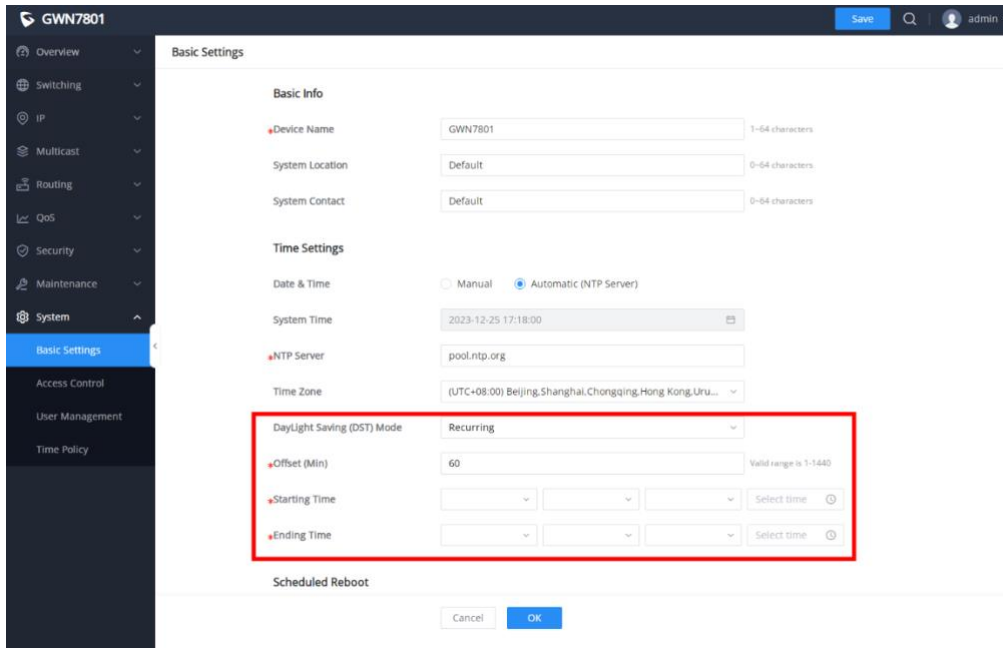
Added actual port status display.





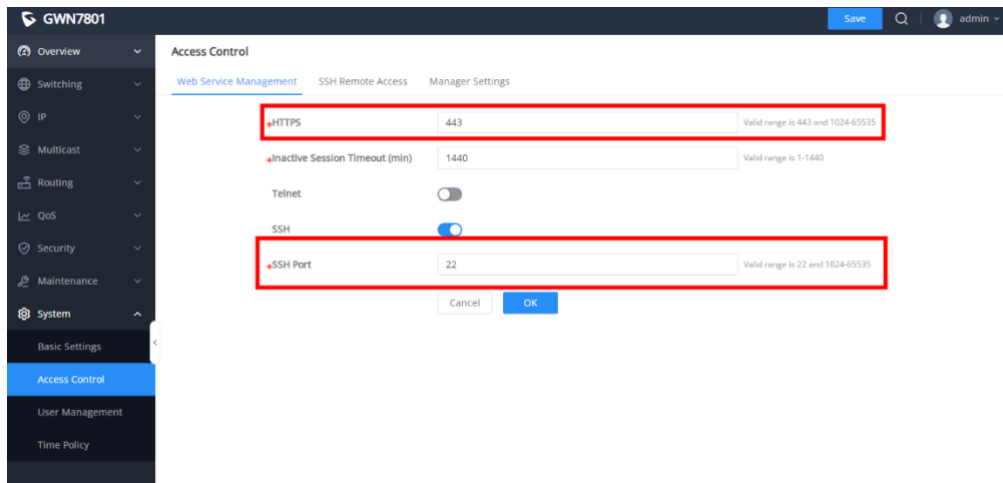
- **Add DST mode for time settings**

Added daylight saving time offset setting and automated time configuration.

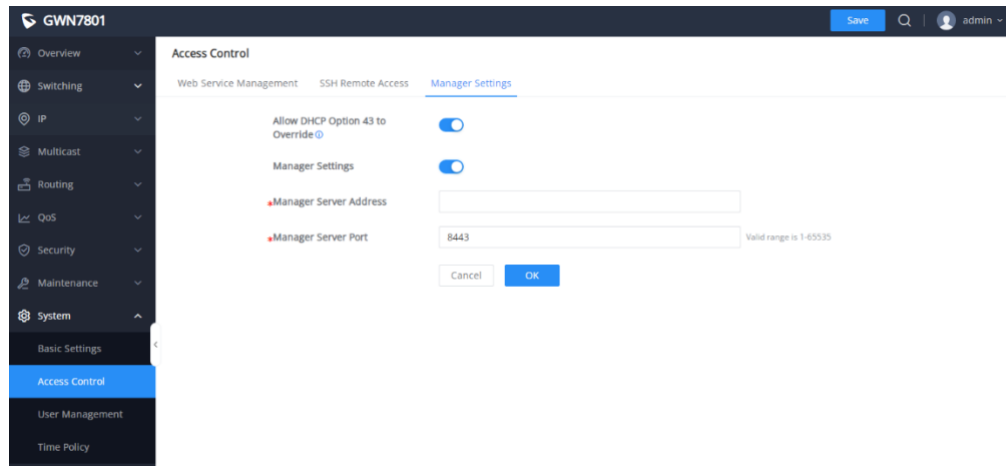


- **Add HTTPS/SSH port customization**

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



- **Optimize Manager settings**



- **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 1.0.3.8**

### **PRODUCT NAME**

GWN7816(P)

### **DATE**

12/4/2023

### **FIRMWARE FILE INFORMATION**

- GWN7816(P) Firmware file name: gwn7816fw.bin  
MD5 checksum: b568755fddd4286ba98d423e920e9bcf

### **CHANGES/ENHANCEMENT**

- This is the initial firmware for GWN7816(P)

## **FIRMWARE VERSION 1.0.3.3**

### **PRODUCT NAME**

GWN7832

### **DATE**

10/17/2023

### **FIRMWARE FILE INFORMATION**

- GWN7832 Firmware file name: gwn7832fw.bin  
MD5 checksum: f4fef887515210fd74574aebd7f55bdd

### **CHANGES/ENHANCEMENT**

- This is the initial firmware for GWN7832

## **FIRMWARE VERSION 1.0.1.14**

### **PRODUCT NAME**

GWN7806(P)

### **DATE**

8/12/2023

### **FIRMWARE FILE INFORMATION**

- GWN7806(P) Firmware file name: gwn7806fw.bin  
MD5 checksum: 68748aa8734a8979dff9b8692f1d37e3

### **CHANGES/ENHANCEMENT**

- This is the initial firmware for GWN7806