GWN781x/783x Switch Firmware Release Notes

IMPORTANT UPGRADING NOTE

1. **GWN781x/783x 1.0.7.71 requires GWN Manager version to be at least 1.1.28.27 or newer.**

Table of Content

FIRMWARE FILE DOWNLOAD

Individual firmware files are available for downloading at URL below:

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

FIRMWARE VERSION 1.0.7.71

PRODUCT NAME

GWN7811, GWN7811P, GWN7812P, GWN7813, GWN7813P, GWN7830, GWN7831

DATE

08/05/2024

FIRMWARE FILE INFORMATION

- GWN781x Firmware file name: gwn781xfw.bin
  MD5 checksum: aacbc68ce57d3e5331691bc1bc16c5d1
- GWN7830 Firmware file name: gwn7830fw.bin
  MD5 checksum: aacbc68ce57d3e5331691bc1bc16c5d1
- GWN7831 Firmware file name: gwn7831fw.bin
  MD5 checksum: aacbc68ce57d3e5331691bc1bc16c5d1

ENHANCEMENTS

- 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 refresh IP address when using DHCP to get VLAN IP address.
- Added gateway priority when using DHCP to get VLAN IP address.
- Added default gateway configuration under MGMT VLAN.

- Added support for OSPFv3.
- Added IP/IPv6 unicast routing on/off (only CLI).
- 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 MAC bypass authentication.
- Added DHCPv6 Snooping.
- Added upgrade by FTP and Explicit FTPS.
- Added connection diagnostics with GWN.Cloud/Manager.
- Added DST mode for time settings.
- Added HTTPS/SSH port customization.
- Added GWN Manager takeover function.
- Added port group. (only CLI).
- Added 1588v2 P2P TC (only CLI).
- Added support to see switch clients and other information.
- Added support for 12 VTY (SSH or telnet) sessions
- 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.
- Fixed issue that network is not stable when ethernet cable is very long.
- 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.
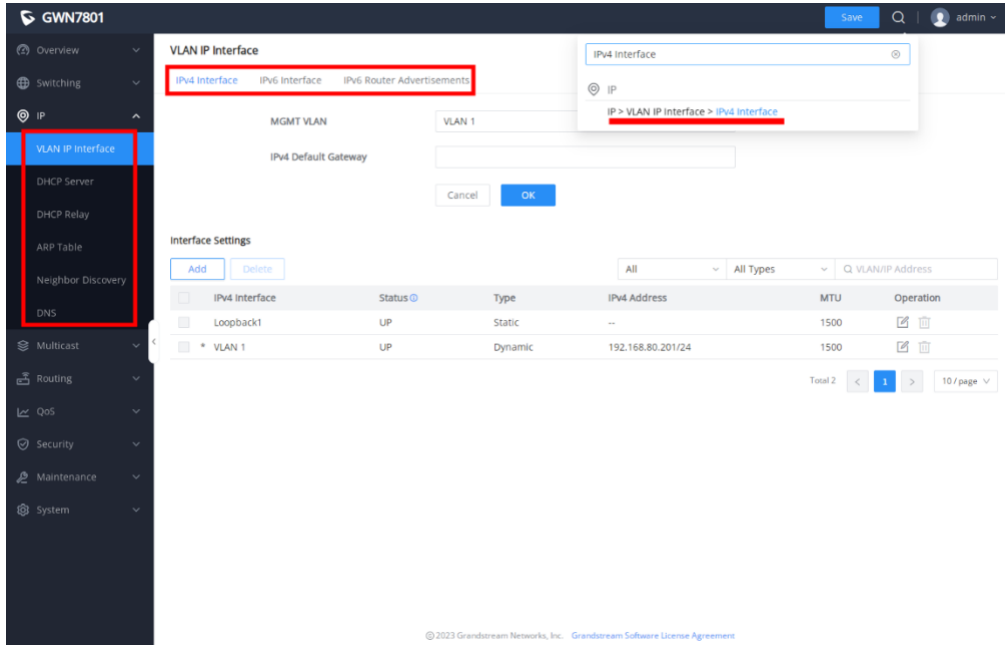
- **Optimize CPU and memory usage in Web GUI**

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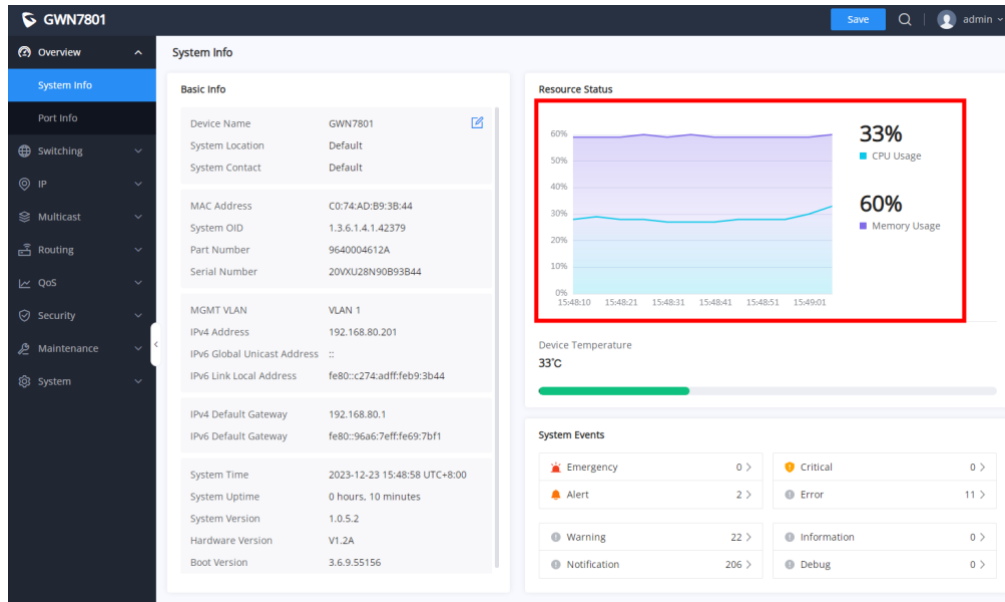

- **Optimize device IP address display**

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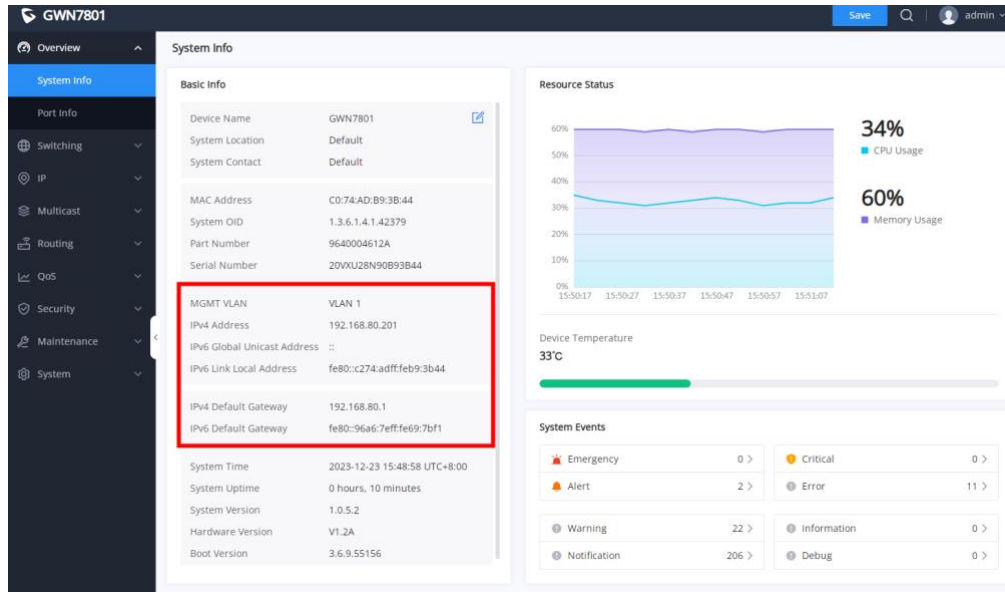
- **Add more port details such as neighbor, PoE power history info**

  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.
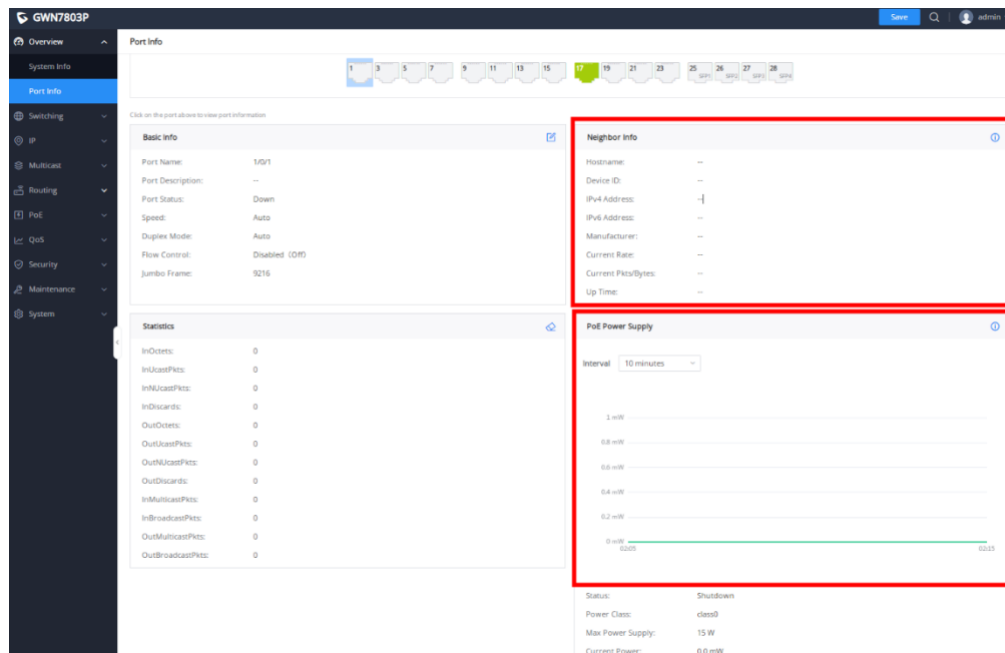
- **Add port scheduled enabling feature**

  You can customize the Scheduled enable time for a port, including physical ports and LAGs.
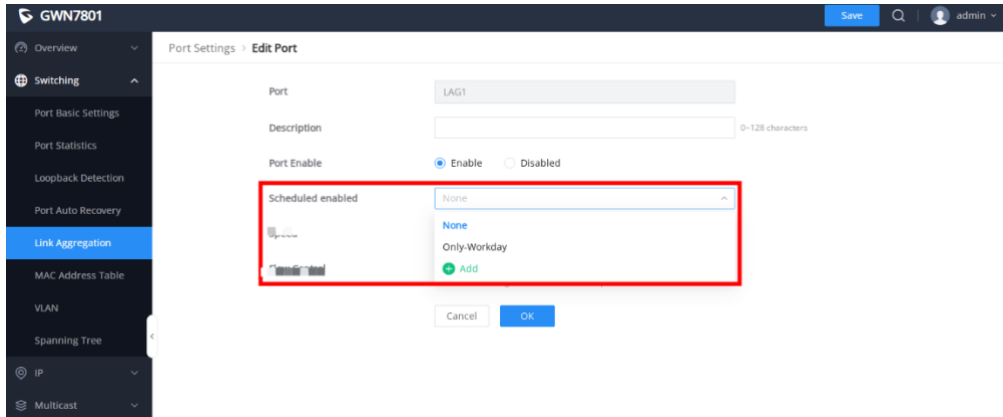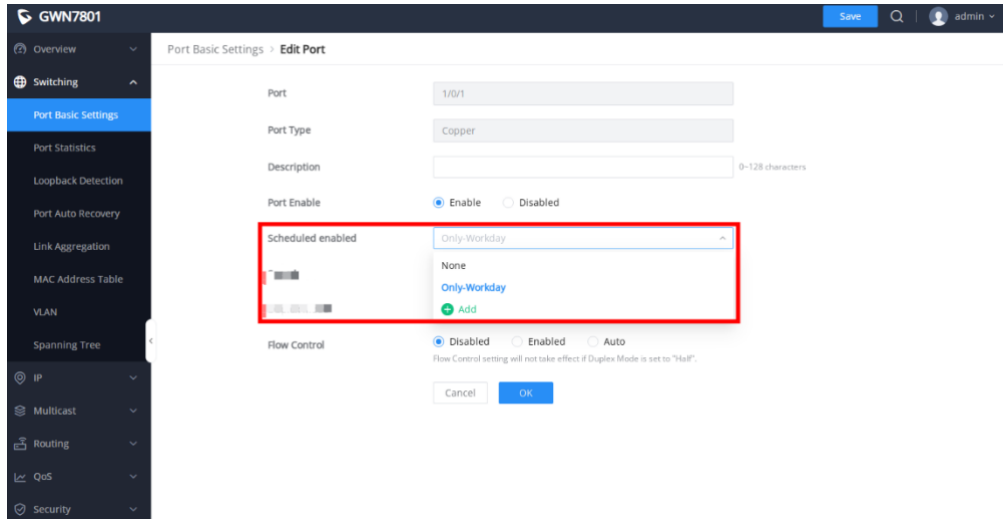
- **Add more port statistics info**

  Support viewing port Private MIB information.
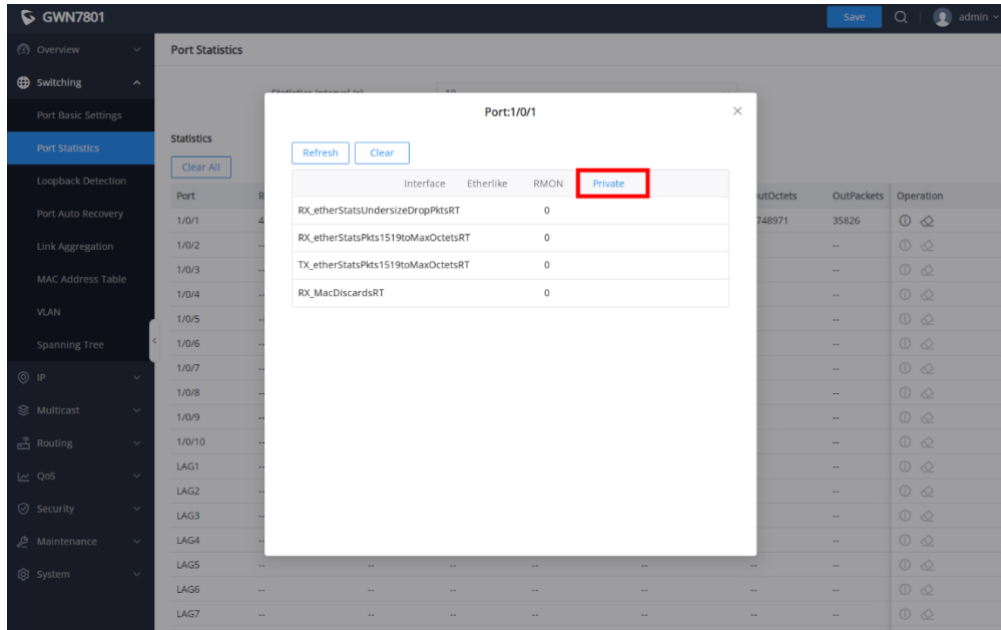
- **Add loopback detection**

  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.
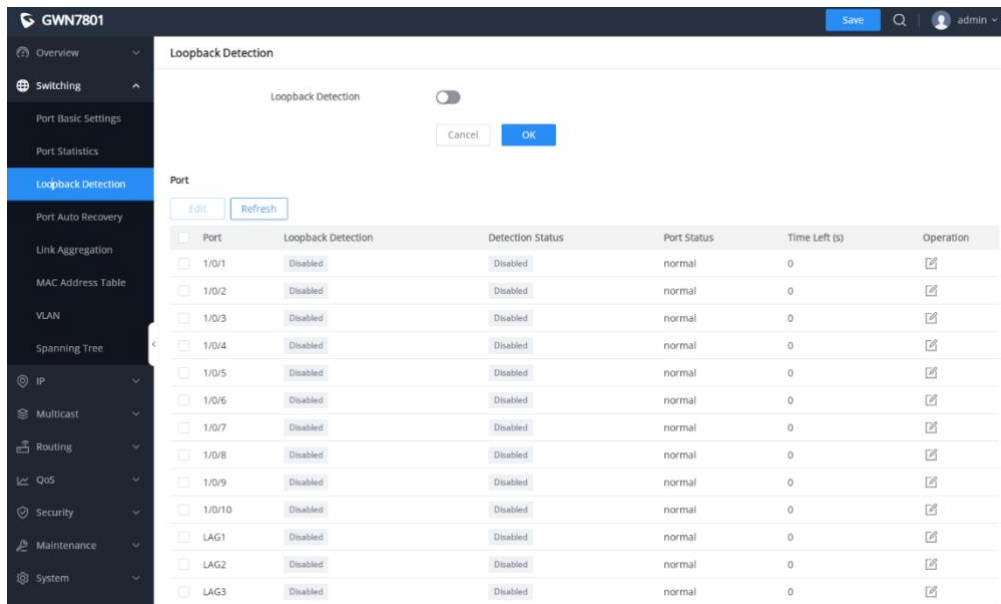
- **Add QinQ**

  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.
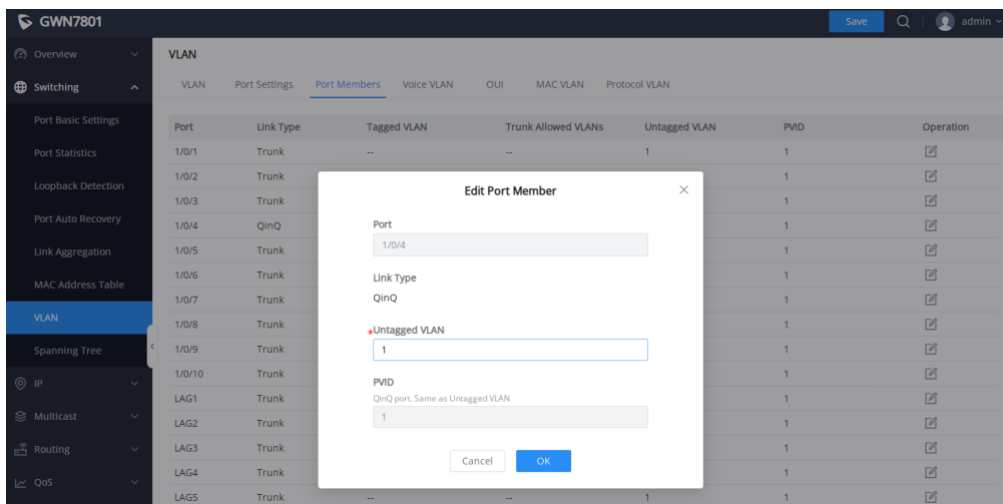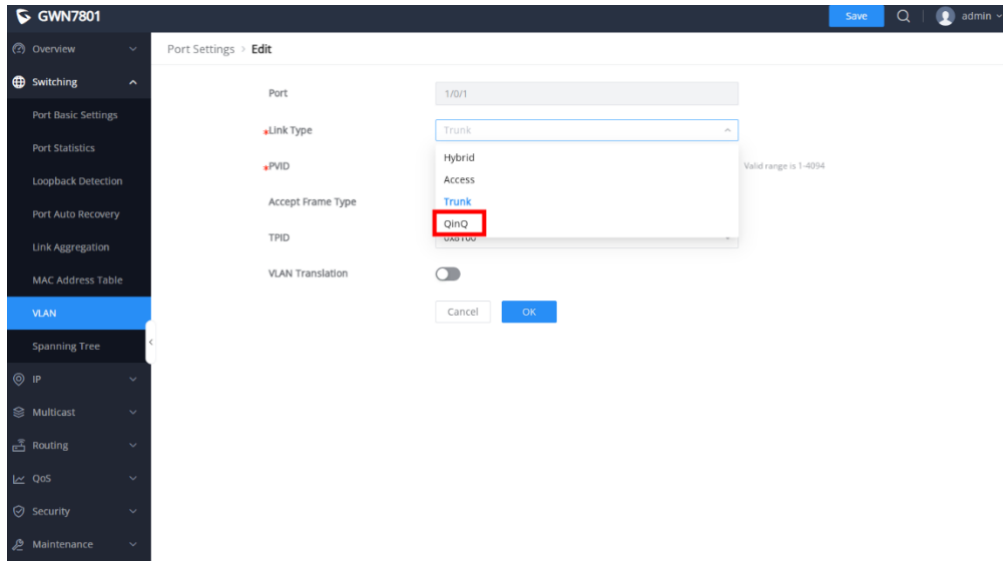
- **Optimize trunk port settings**

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

- **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.
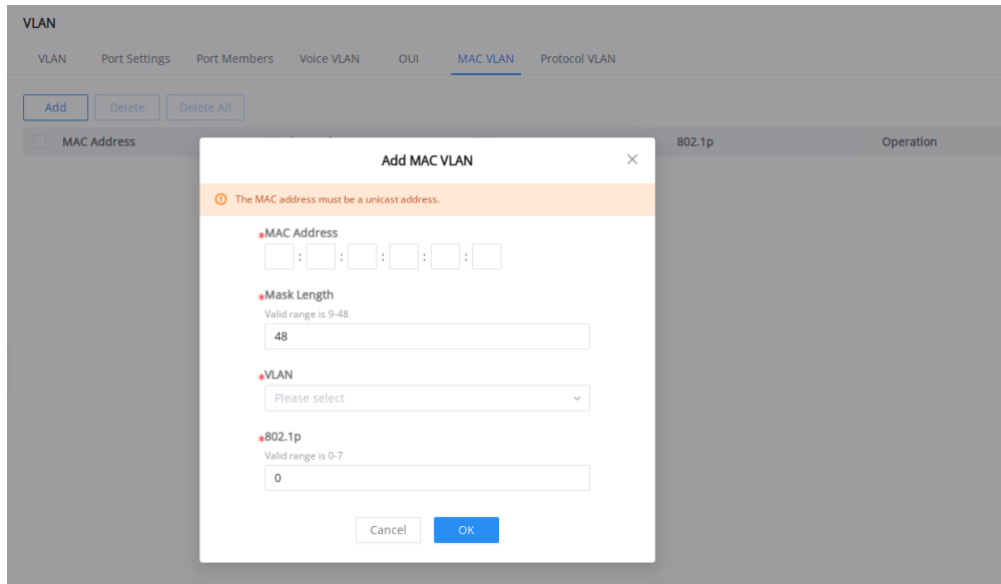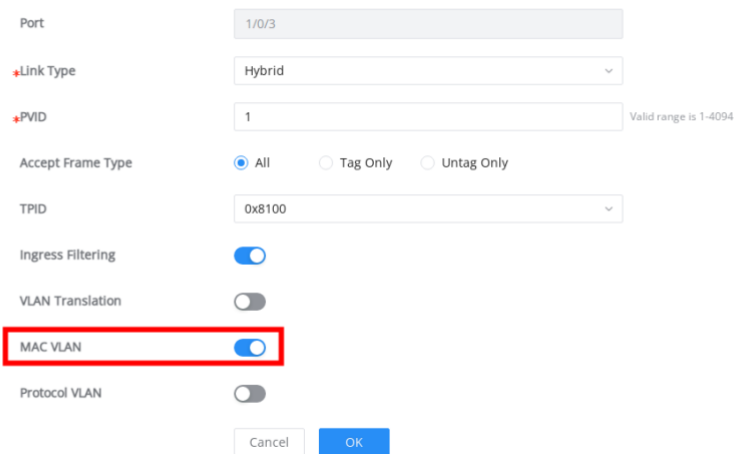
- **Add protocol-based VLAN**

  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.

- **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.

- **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.

- **Add refresh IP address when using DHCP to get VLAN IP address**

  When the VLAN IPv4 interface uses DHCP to obtain an IP address, or the VLAN IPv6 uses "Auto Generate" to obtain a link-local address, or "Stateful DHCPv6", "Stateless DHCPv6", or "Stateless Auto Configuration" to obtain a global unicast address, re-acquisition of the IP address is supported.
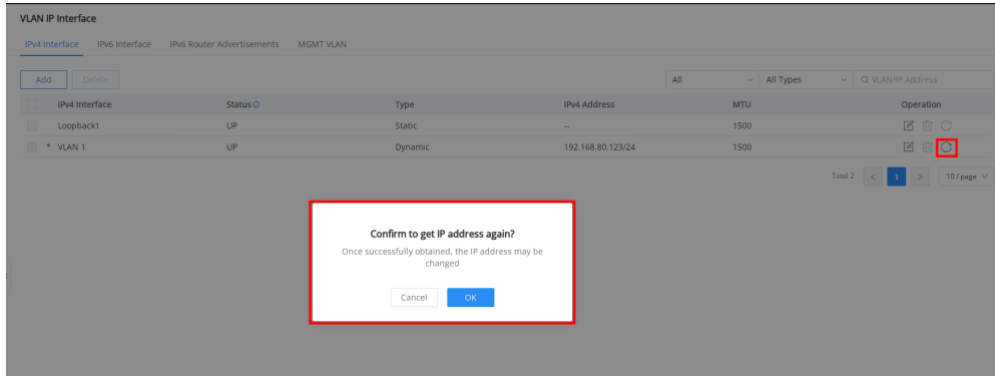
- **Add gateway priority when using DHCP to get VLAN IP address**

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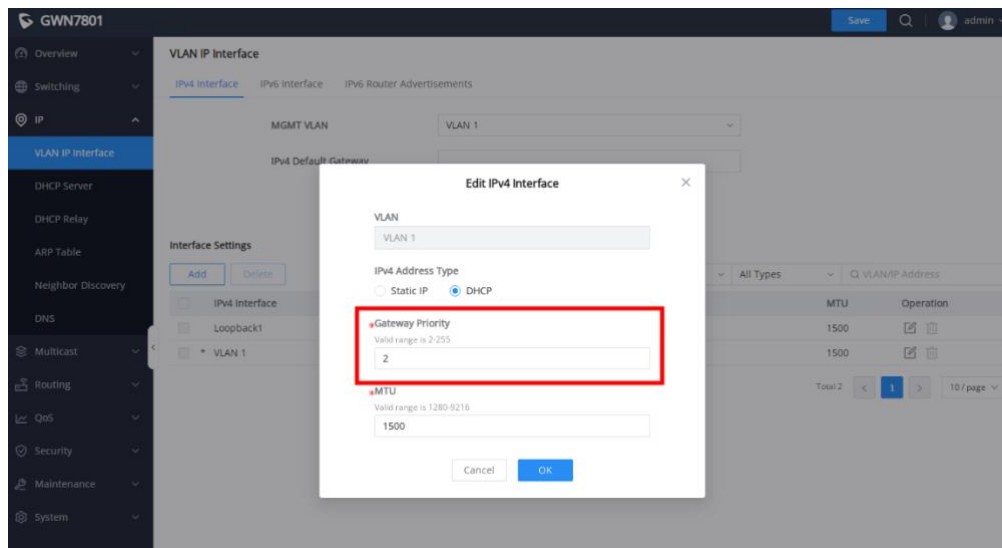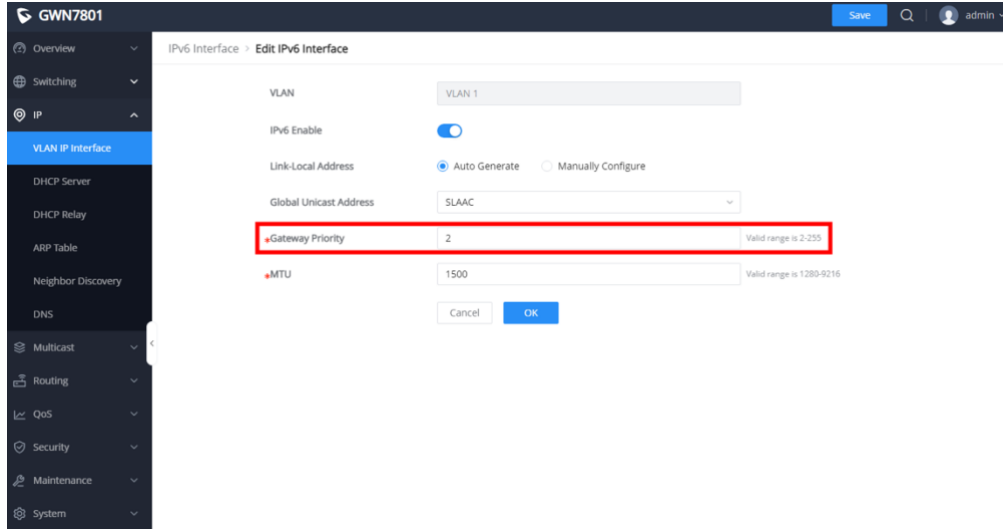
- **Add default gateway configuration under MGMT VLAN**

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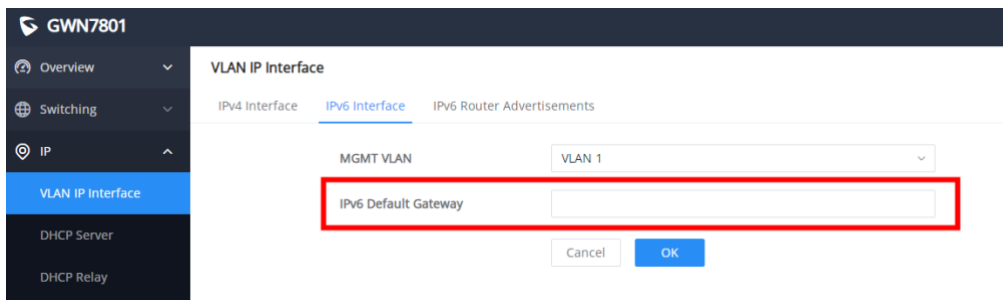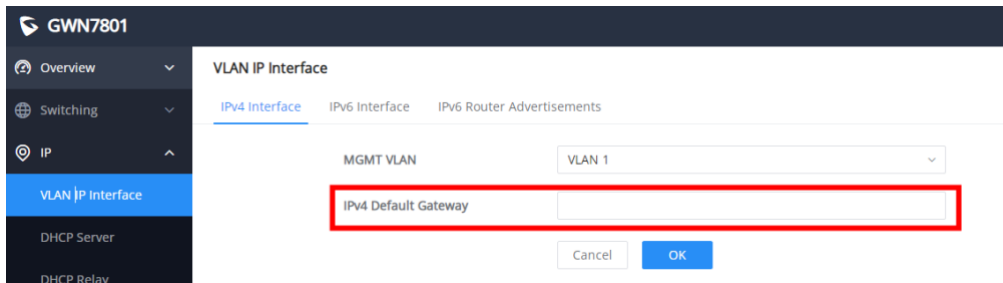
- **Optimize DHCP option 43 configurations for DHCP server**

  Supports configuring specified services for DHCP Option 43.
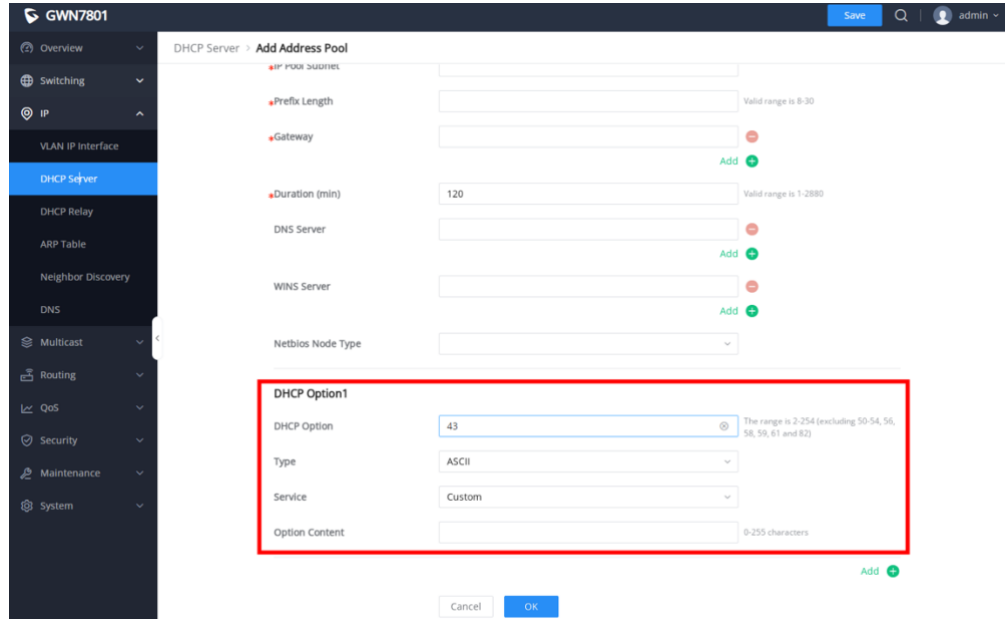
- **Optimize routing table**

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

- **Add OSPFv3**

  OSPFv3 is an OSPF routing protocol running on IPv6. It divides the autonomous system AS into one or more logical areas and publishes routes in the form of LSA.

  Globally set parameters such as router ID, SPF calculation, and LSA. After establishing a full connection with the neighbor, if the router ID is modified, the OSPFv3 process must be restarted for it to take effect again.

Set interface parameters, including the region to join, network type, etc.

Set the zone parameters to which the interface joins.
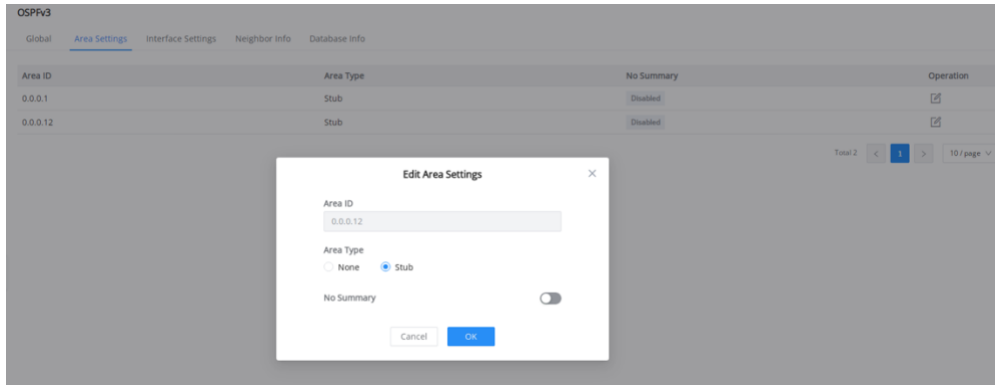
After the neighbor relationship is established, check the neighbor information and Database information.
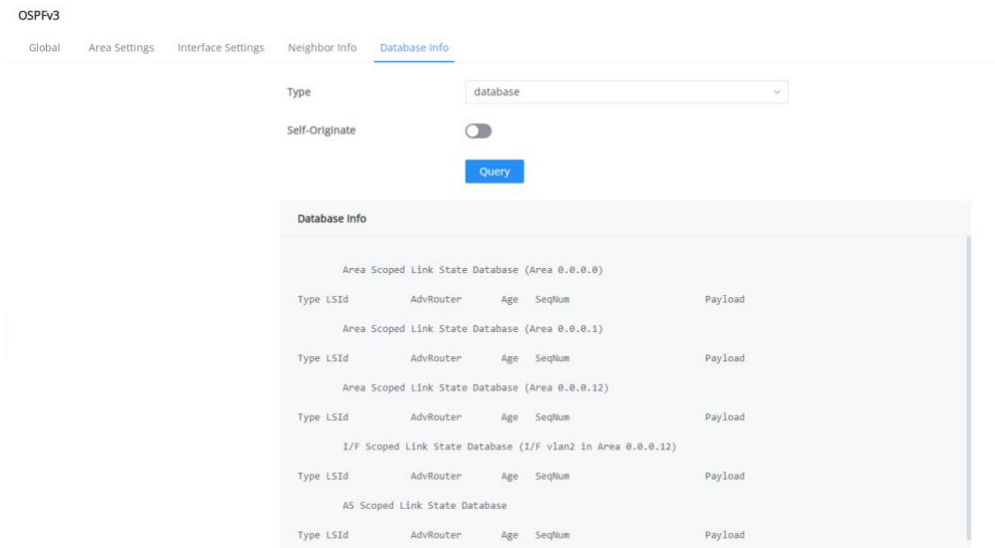
- **Add ACL advanced settings, including mirroring, statistic and priority remapping for rule**

  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.

- **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.

VLAN bind ACL：

Speed limit group settings:

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

- **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.
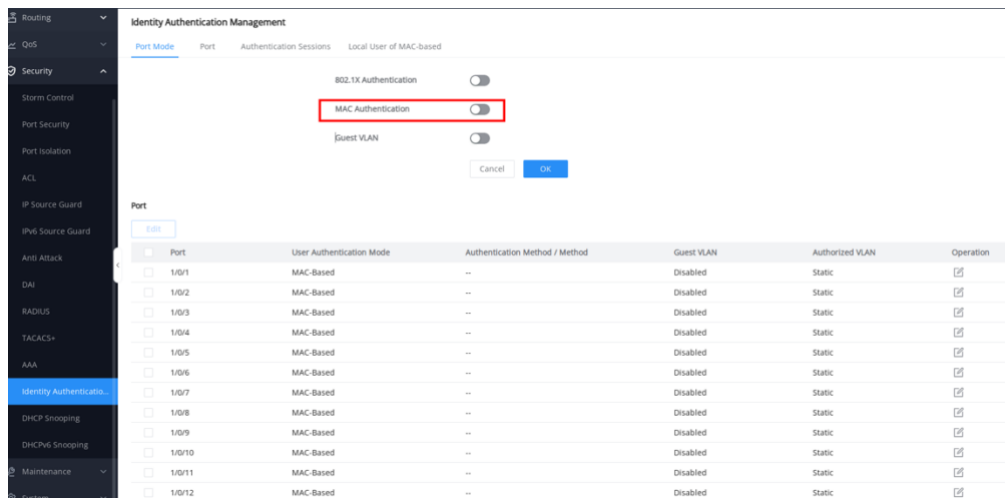
- **Add MAC bypass authentication**

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

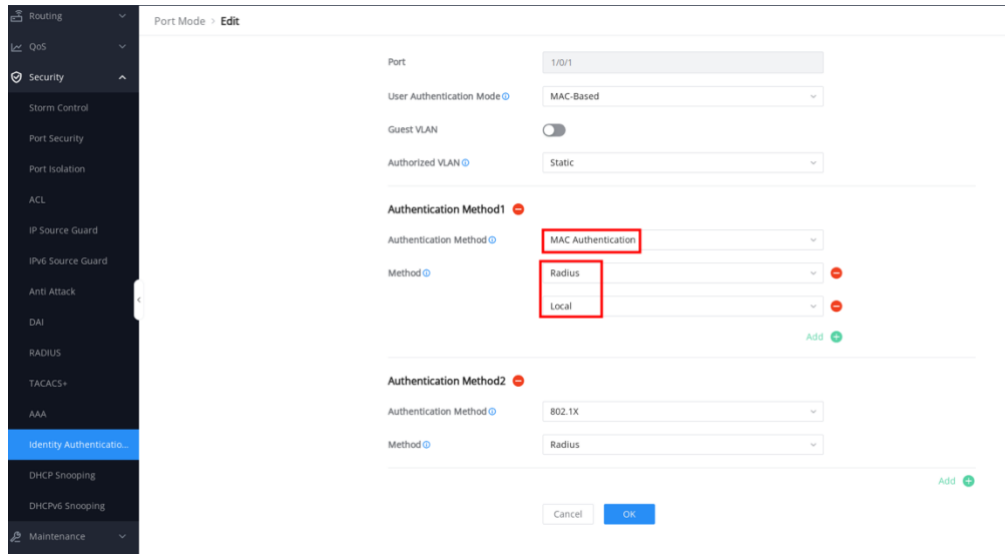   MAC authentication has been added to the port authentication method, and the authentication methods support RADIUS and Local.

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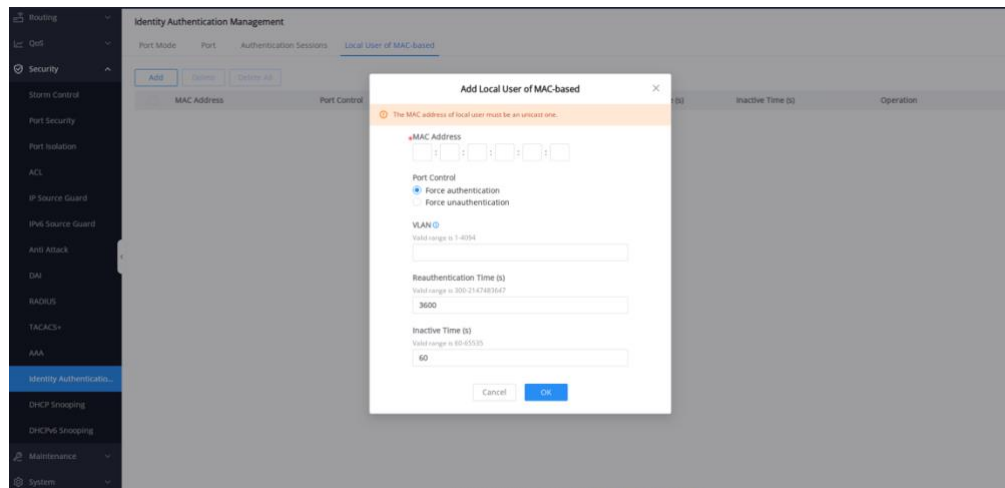
- **Optimize remote ID and Circuit ID for DHCP Snooping**

  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.
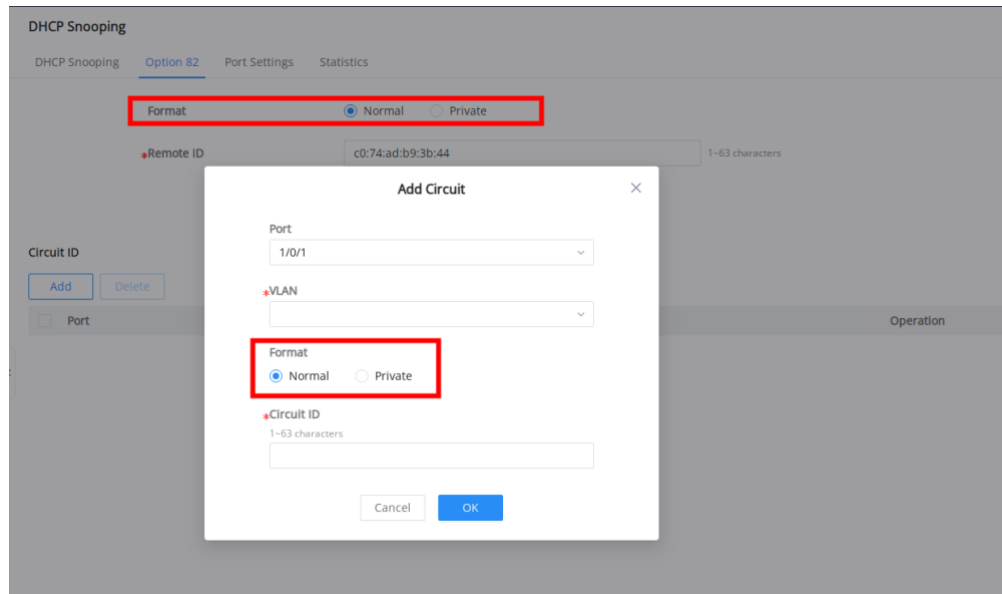
- **Add DHCPv6 Snooping**

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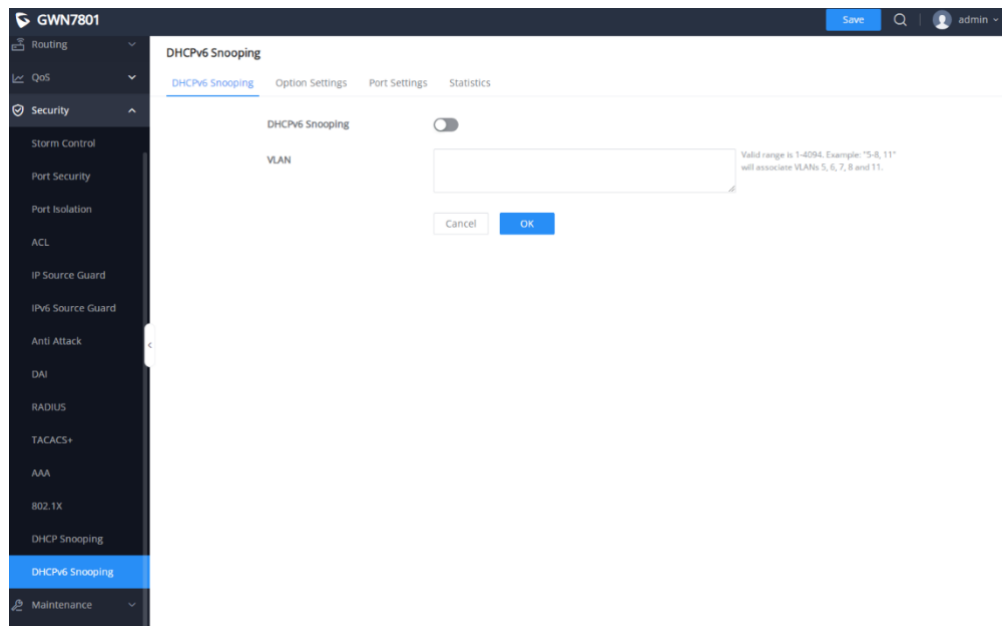
- **Add upgrade by FTP and Explicit FTPS**

  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.

- **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.
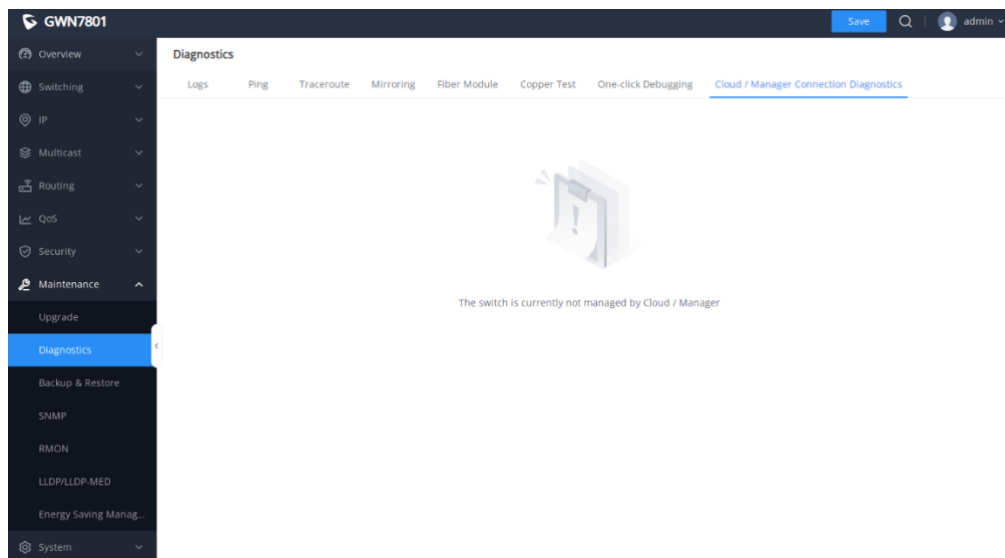
- **Optimize EEE**

  Added actual port status display.
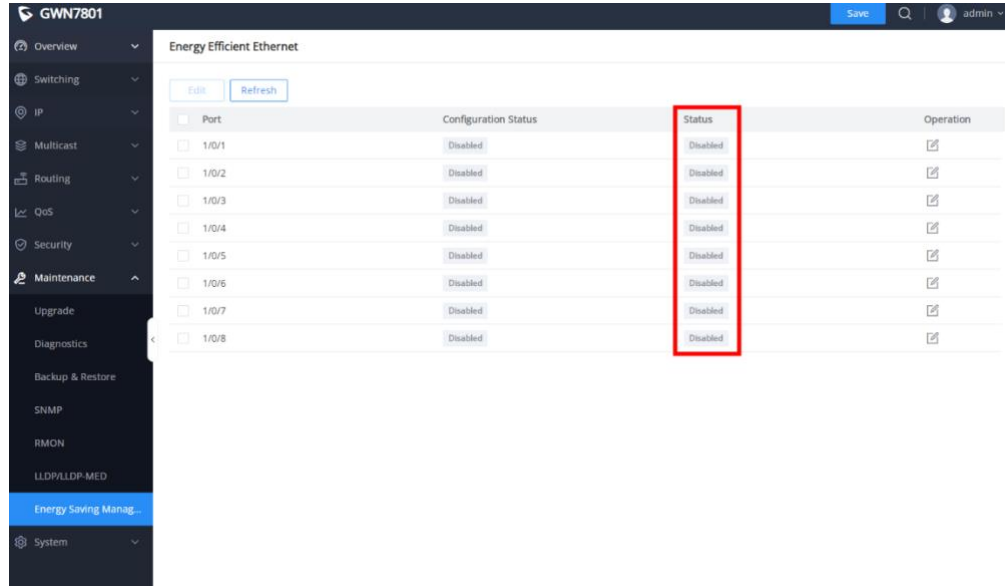
- **Add DST mode for time settings**

  Added daylight saving time offset setting and automated time configuration.
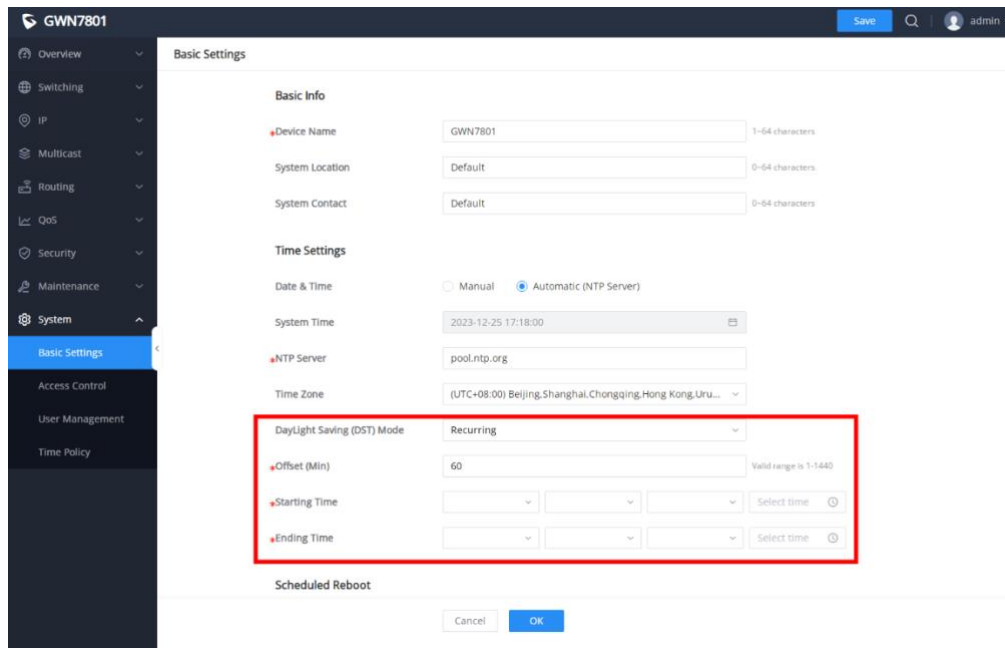
- **Add HTTPS/SSH port customization**

Users use customized HTTPS and SSH ports to access and configure device.
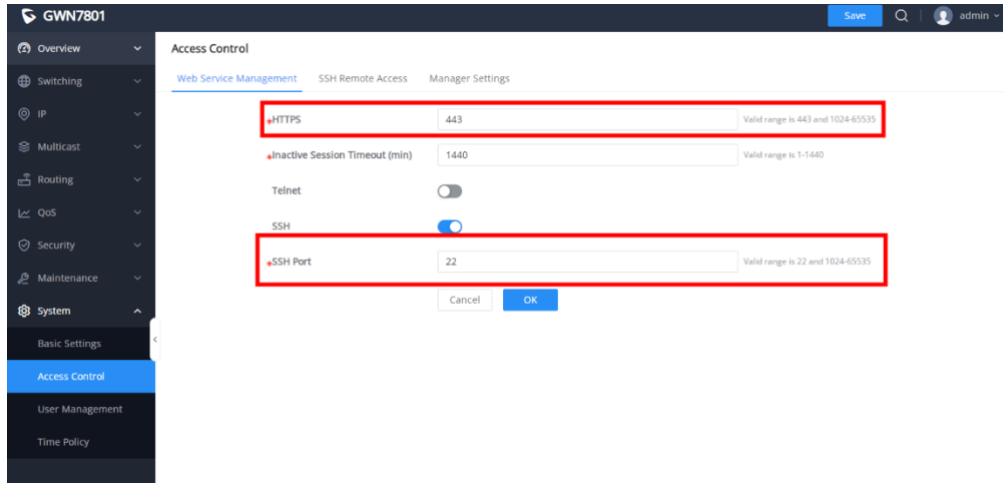
- **Optimize Manager settings**
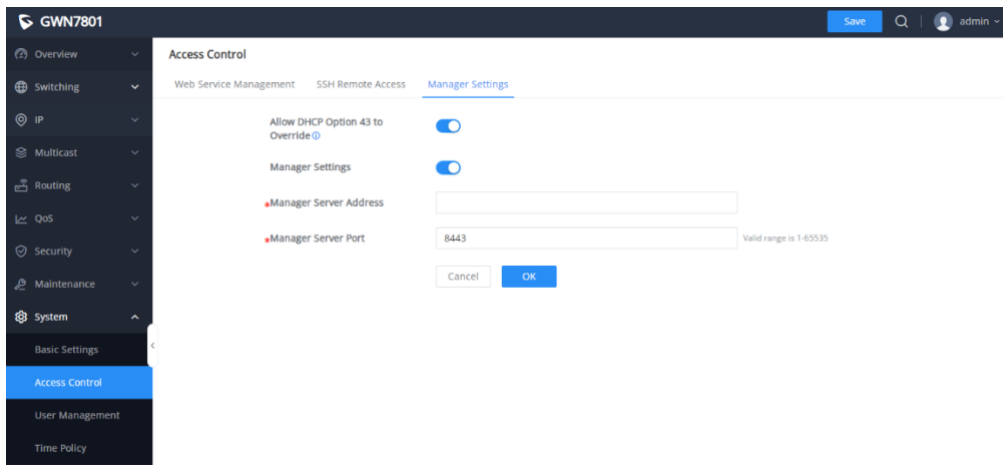
- **Add GWN Manager takeover function**

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

FIRMWARE VERSION 1.0.1.20

PRODUCT NAME

GWN7811, GWN7811P, GWN7812P, GWN7813, GWN7813P

DATE

11/07/2023

FIRMWARE FILE INFORMATION

- GWN781x Firmware file name: gwn781xfw.bin
  MD5 checksum: 70d00f61ebe58d9ad79e707f81b0256e

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 SNTP GWN Cloud interface.
- Added GWN Cloud time sync interface.
- Added support EXEC CLI config command by GWN Cloud.
- 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 in plain text, and an error message is displayed.
- Fixed some issues when work with GWN Cloud.
- Internal bug fixes.

FIRMWARE VERSION 1.0.1.8

PRODUCT NAME

GWN7811, GWN7811P, GWN7812P, GWN7813, GWN7813P

DATE

08/04/2023

FIRMWARE FILE INFORMATION

- GWN781x Firmware file name: gwn781xfw.bin
  MD5 checksum: c4393865767f3b042086515b75029db6

CHANGES/ENHANCEMENT

- This is the first release of GWN781x.