QSS and QSS Pro 4.1

User Guide

Document version: 2
25/03/2025

Contents

1. Overview

About QSS and QSS Pro 4.1

QSS and QSS Pro 4.1 represent iterative advancements over QSS and QSS Pro 4.0, incorporating new features and enhancements designed for QSW managed switches.

QSS 4.1 focuses on Layer 2 (L2) features, providing essential capabilities for switching, VLAN support, and network monitoring, making it suitable for environments where efficient data flow and local management are critical.

In contrast, QSS Pro 4.1 extends capabilities to Lite Layer 3 (LL3), incorporating advanced routing features for more complex network configurations. This version supports organizations requiring dynamic IP routing and increased scalability. By utilizing QSS or QSS Pro 4.1, you can access enhanced tools for managing your network infrastructure.

Comparative overview of QSS and QSS Pro 4.1 features

Feature Category	QSS 4.1	QSS Pro 4.1
Port Management		
Management port	Yes	
Port speed	Yes	
Flow control	Yes	
Forward Error Correction (FEC)	Yes **Note** FEC is supported only on ports with speeds of 25 GbE or higher.	
Port breakout	Yes **Note** Port breakout is supported only on ports with speeds of 100 GbE or higher.	
System Settings		
System information	Yes	

Feature Category	QSS 4.1	QSS Pro 4.1
Switch password	Yes	
Time settings	Yes	
Backup and restoration	Yes	
Factory reset	Yes	
Password reset	Yes	
Secure connection (HTTPS)	Yes	
Diagnostic Logs	Yes	
Smart fan	Yes	
SNMP	Yes	
Network Settings		
IPv4 settings	Yes	
IPv6 settings	No	Yes
DNS server settings	Yes	
DHCP server settings	No	Yes
QoS	Yes	
Multichassis LAG	No	Yes
Intelligent AV streaming	Yes	
Layer 2 (L2) Features		
VLAN	Yes	
Link aggregation	Yes	
RSTP	Yes	
LLDP	Yes	
IGMP snooping	Yes	

Feature Category	QSS 4.1	QSS Pro 4.1
AV over IP	Yes	
Dynamic MAC address aging timer	Yes	
Static MAC address	Yes	
PTP transparent clock	No	Supported only on the QSW-M7308R-4X.
Lite Layer 3 (LL3) Features		
Routing	No	Yes
Address Resolution Protocol (ARP)	No	Yes
Neighbor Discovery Protocol (NDP)	No	Yes
Security		
Loop protection	Yes	
IPv4 ACL	Yes	
IPv6 ACL	Yes	
MAC ACL	Yes	
Maintenance		
Firmware update	Yes	
Port Tests	Yes **Note** Port tests is a model-specific feature and may not be available on all switch models.	
LED controls	Yes	
Port mirroring	Yes	

Feature Category	QSS 4.1	QSS Pro 4.1
Digital diagnostic monitoring (DDM)	A model-specific feature available only on models with an SFP port.	
System logs	Yes	

System requirements

Category	Details
Hardware	A QNAP QSW managed switch

Software	• Web browser:
	  • Microsoft Edge 42 or later
	  • Mozilla Firefox 60.0 or later
	  • Apple Safari 11.1 or later
	  • Google Chrome 70.0 or later
	• Qfinder Pro 6.9.2 or later

Switch access

Method	Description	Requirements
Web browser	You can access the switch using any computer on the same network if you have the following information: • Switch name (Example: http://example123/) or IP address • Login credentials of a valid user account For details, see Accessing the switch using a browser.	• Computer that is connected to the same network as the switch • Web browser

Method	Description	Requirements
Qfinder Pro	Qfinder Pro is a desktop utility that enables you to locate and access QNAP devices on a specific network. The utility supports Windows, macOS, and Linux. For details, see Accessing the switch using Qfinder Pro.	• Computer that is connected to the same network as the switch • Web browser • Qfinder Pro

Accessing the switch using a browser

You can access the switch using any computer on the network if you know its IP address and the login credentials of a valid user account. QNAP switches support DHCP client configuration by default for IP assignment. When connected to a network, the switch automatically obtains an IP address from a DHCP server.

Note

- If you do not know the IP address of the switch, you can locate it using Qfinder Pro.
- If the switch is not connected to a DHCP supported network, you can access the switch web interface by changing the IP address of the computer to 169.254.100.102.
- The default IP address of the switch is 169.254.100.101.

1. Verify that your computer is connected to the same network as the switch.
2. Open a web browser on your computer.
3. Type the IP address of the switch in the address bar.
   The login page appears.
4. Specify the username and password.

Default Username	Default Password
`admin`	For details on the default password, see this FAQ.

5. Click **Login**.

The **Overview** page appears.

Important

After setting up the switch, ensure that you change the IP address of the computer to the original configuration.

Accessing the switch using Qfinder Pro

1. Install Qfinder Pro on a computer that is connected to the same network as the switch.

   Tip
   To download Qfinder Pro, go to https://www.qnap.com/utilities.

2. Open Qfinder Pro.
   Qfinder Pro automatically searches for all QNAP devices on the network.
3. Locate the switch in the list, and then double-click the name or IP address.
   The login page appears.
4. Specify the username and password.

Default Username	Default Password
admin	For details on the default password, see this FAQ.

5. Click **Login**.

The **Overview** page appears.

Important
After setting up the switch, ensure that you change the IP address of the computer to the original configuration.

Getting started

1. Log in to the switch as an administrator.
   The default administrator account is admin.
   For details, see Switch access.
2. Configure the system settings.
   For details, see System management.
3. Configure port settings and other network settings.
   For details, see Network management.

2. System management

The **System** section of the QSS or QSS Pro navigation menus provides access to device configuration options.

Changing the switch name

1. Log in to the switch system.
2. Go to **System** > **System Settings** > **System Information**.
3. Click .
4. Specify the switch name.
   Requirements:
   - Length: 1–32 characters
   - Valid characters: A–Z, a–z, 0–9
   - Valid special characters: Hyphen (-)
5. Click to confirm the switch name.

The switch updates the device name.

Updating the switch password

1. Log in to the switch system.
2. Go to **System** > **System Settings** > **Password**.
3. Enter the following information:

   Tip

   Click to make the password visible.

Setting	User Action
Current password	Specify the current password of the device.
New password	Specify a password that contains 8 to 20 ASCII characters.
Confirm new password	Reenter the new password.

4. Click **Save**.

The switch logs you out of the interface. You can access the switch with the new password.

Configuring time settings

Note

You must configure the system time correctly to ensure the following:

- When using a web browser to connect to the device or save a file, the displayed time of the action is correct.
- Event logs reflect the exact time that events occur.
- Scheduled tasks run at the correct time.

1. Log in to the switch system.
2. Go to **System** > **System Settings** > **Time**.
3. Specify the time zone.
4. Specify the time configuration.

Setting	Description
Synchronize with internet time server	Ensure that your device is connected to the internet, and then specify the following information: **Server**: Specify the Network Time Protocol (NTP) server. Examples: time.nist.gov, time.windows.com
Manual configuration	Specify the date and time.

5. Configure the Daylight Savings Time (DST) settings.
   - **Disable**: Disables the DST settings
   - **Adjust the system clock automatically**: Allows the internal clock of the switch to configure the DST settings.
   - **Adjust the system clock manually**: Allows you to manually configure the starting time, ending time, and the offset settings.
6. Click **Save**.

The switch updates the time settings.

Backing up system settings

1. Log in to the switch system.
2. Go to **System** > **System Settings** > **Backup & Restore**.
3. Click **Backup**.

The device exports the system settings as a BIN file and downloads the file to your computer.

Restoring system settings

Warning

If the selected backup file contains user or user group information that already exists on the device, the system will overwrite the existing information.

1. Log in to the switch system.
2. Go to **System** > **System Settings** > **Backup & Restore**.
   A file explorer window opens.
3. Navigate to **Restore System Settings**.
4. Click **Browse**.
5. Select a valid BIN file that contains the device system settings.
6. Click **Restore**.

The switch restores the settings.

Resetting the switch password

Note

- You can also reset the switch password by pressing and holding the physical reset button for 5 seconds.
- The default `admin` account is automatically enabled after a system reset.

1. Log in to the switch system.
2. Go to **System** > **System Settings** > **Backup & Restore**.
3. Click **Password Reset**.

The switch resets the password.

Note

For details on the default password, see this FAQ.

Resetting the switch to factory settings

Resetting the switch deletes the data stored on the device and restores the switch to the default factory settings.

Tip
You can also reset the switch to factory defaults by pressing and holding the physical reset button for 10 seconds.

1. Log in to the switch system.
2. Go to **System** > **System Settings** > **Backup & Restore**.
3. Click **Factory Reset**.
   A confirmation message appears.
4. Click **Yes**.

The switch resets to the factory default settings.

Note
To log in to the interface again, you must locate the device using Qfinder Pro. For details, see Switch access.

Restarting the switch

1. Log in to the switch system.
2. Click  located on the upper-right corner of the page.
3. Click **Restart Switch**.
   A confirmation message appears.
4. Click **Yes**.

The switch restarts itself.

Enabling secure connection (HTTPS)

1. Log in to the switch system.
2. Go to **System** > **System Settings** > **HTTPS**.
3. Select **Enable Secure Connection (HTTPS)**.
4. Select a TLS version.

Note
Select the latest version of TLS to maximize system security. Ensure that your system meets the TLS requirements to avoid compatibility issues.

5. Optional: Select **Force secure connections (HTTPS) only**.

> **Note**
> After enabling this setting, you can only access the web administration page via HTTPS.

6. Click **Save**.

The switch saves the secure connection settings.

Downloading diagnostic logs

You can remotely monitor switch events (including system, LLDP, and IGMP snooping events) by recording and downloading diagnostic logs.

1. Log in to the switch system.
2. Go to **System** > **System Settings** > **Diagnostic Logs**.
3. Select the services for which you wish to download logs.

> **Note**
> By default, system logs are included in the downloaded logs.

4. Specify a period for collecting logs.
5. Click **Start**.
   The switch starts collecting the logs of the selected services.
6. Click **Download**.

The switch downloads the compressed file to your device.

Configuring smart fan settings

> **Note**
> The QSW-M7308R model does not support smart fan control. This is because it is designed for industrial environments where precise temperature regulation may not be as critical. However, other switch models running firmware version QSS 4.0.x or later have adjustable fan settings. You can use these settings to optimize cooling performance based on your specific network conditions and ambient temperature.

1. Log in to the switch system.
2. Go to **System** > **System Settings** > **Smart Fan**.

3. Select the fan speed mode.

Option	Description
Normal (recommended)	Fans run on normal speed. This is the default setting.
Quiet	Fans run on low speed to decrease noise.
Full speed	Fans run on high speed to lower the system temperature. This mode is suitable for high loading systems.

4. Click **Save**.

The switch saves the smart fan settings.

Configuring SNMP settings

The Simple Network Management Protocol (SNMP) is used to collect and organize information about managed devices on a network. Enabling the SNMP service allows events (such as warnings and errors) to be immediately reported to a Network Management Station (NMS).

1. Log in to the switch system.
2. Go to **System** > **System Settings** > **SNMP**.
3. Select **Enable SNMP service**.
4. Select the SNMP version that the NMS uses.

Option	User Action
SNMPv2c	Specify an SNMP community name that contains 1 to 64 characters from any of the following groups: • Letters: A to Z, a to z • Numbers: 0 to 9 The SNMP community string functions as a password that is used to authenticate messages sent between the NMS and the device. Every packet that is transmitted between the NMS and the SNMP agent includes the community string.

Option	User Action
SNMPv3	Specify the username, authentication protocol and password, and privacy protocol and password. **a.** Specify a username. **Note** The username should contain 1 to 32 characters from any of the following groups: • Letters: A to Z, a to z • Numbers: 0 to 9 • Multi-byte characters: Chinese, Japanese, Korean, and Russian • Special characters: All except " ' / \ **b.** Optional: Select **Authentication**. **1.** Specify the authentication protocol. **Tip** You can select **HMAC-MD5** or **HMAC-SHA**. If you are unsure about this setting, QNAP recommends selecting **HMAC-SHA**. **2.** Specify an authentication password that contains 8 to 64 ASCII characters. **c.** Optional: Select **Privacy**. **1.** Specify a privacy password that contains 8 to 64 ASCII characters.

5. Select the SNMP trap.

SNMP Trap	Description
coldStart	A coldStart trap signifies that the SNMP entity is reinitializing itself so that the agent configuration or the protocol entity implementation can be altered.
warmStart	A warmStart trap signifies that the SNMP entity is reinitializing itself so that the agent configuration or the protocol entity implementation cannot be altered.

SNMP Trap	Description
linkUp	A linkUp trap signifies that the sending protocol entity recognizes that one of the communication links represented in the agent configuration has become active.
linkDown	A linkDown trap signifies that the sending protocol entity recognizes a failure in one of the communication links represented in the agent configuration.

6. Specify the trap addresses of the host or the targeted recipient.
7. Click **Save**.

The switch saves the SNMP settings.

Viewing information on the switch

To view the hardware and system information of the switch, go to **System** > **System Settings** > **System Information**.

The screen provides the following information.

Information	Description
Switch name	Displays the default or modified name of the switch
Model name	Displays the model name of the switch
MAC address	Displays the MAC address of the switch
IP address	Displays the DHCP or static IP address of the switch
System uptime	Displays how long the system has been operational
Current firmware version	Displays the firmware image version of the switch

Configuring the idle session timeout setting

The idle session timeout setting determines the maximum period of user inactivity allowed before a user's login session is automatically terminated. This security feature mitigates the risk of unauthorized access to sensitive information on unattended devices.

1. Log in to the switch system.
2. Click ⋮ located on the upper-right corner of the page.

3. Click **Idle Session Timeout**.
4. Select the timeout period.

The switch saves the idle session timeout setting.

3. Network management

Configuring and managing network settings on your QSW managed switch allows you to optimize network performance and ensure efficient data flow. You can manage traffic prioritization, bandwidth allocation, and network security. Proper network configuration enhances connectivity, reduces latency, and safeguards data integrity across the network.

Common settings

This section covers typical network configuration and management options for all QNAP QSW managed switches. These settings help you establish essential switch functions and implement comprehensive access control to secure your network.

Configuring port settings

Configuring port settings is an important step in optimizing your network's performance and ensuring data transmission. The available settings and their functions may vary depending on your QSS or QSS Pro version.

1. Log in to the switch system.
2. Go to **System** > **Port Management**.
3. Go to **Port Configuration**.
4. Identify a port or LAG.
5. Configure the settings.

Setting	Description	QSS 1.x-2.x	QSS 3.x	QSS 4.x	QSS Pro 4.0 and later
State	Enables or disables the port.	Supported			
Port Name	A human-readable label for the network port.	Not supported	Supported		

Setting	Description	QSS 1.x-2.x	QSS 3.x	QSS 4.x	QSS Pro 4.0 and later
Speed	Configures the data transfer rate. **Note** When port speed is set to **Auto**, the maximum supported speed is advertised to the connected device.	Supported			
Flow Control	Regulates the data flow of the port. For details, see Enhancing data transmission using flow control.	Supported			
FEC	Forward Error Correction (FEC) recovers lost packets on a link by sending additional parity packets. For details, see Reducing data loss using FEC.	Supported on certain switch models (not dependent on QSS or QSS Pro version) Only available on ports with speeds of 25 GbE or higher			

6. Click **Save**.

The switch saves the port settings.

Enhancing data transmission using flow control

Flow control manages the data flow between devices to prevent congestion and ensure efficient data transmission. By controlling the rate at which data is sent and received, flow control helps avoid network bottlenecks and data loss, particularly in high-traffic environments.

To configure the flow control of a port, see Configuring port settings.

Note

On certain QSS and QSS Pro versions, flow control is a toggle switch that can be enabled or disabled. When enabled, it automatically configures bidirectional (TX/RX) mode for the port.

Flow Control Mode	Description
Disabled	Operate the port without any flow control mechanisms, which can be useful in scenarios where flow control might interfere with network performance.
Bidirectional (TX/RX)	Dynamically adjusts both incoming and outgoing traffic to manage network congestion, ensuring balanced data handling. This mode is ideal for environments requiring balanced control over both incoming and outgoing traffic.
Transmitting (TX)	Regulates outgoing traffic to connected devices when nearing overload, maintaining smooth data flow. This mode is suitable for high-throughput settings where outgoing data needs careful management.
Receiving (RX)	Implements congestion control by temporarily pausing data reception when nearing capacity, allowing the connected device to adjust its transmission rate. This mode is suitable for managing incoming traffic in order to prevent receiver overload.

Reducing data loss using FEC

Forward Error Correction (FEC) enhances data transmission reliability by detecting and correcting errors without requiring data retransmission. FEC works by sending additional parity packets alongside the original data, allowing the receiving device to recover lost or corrupted packets.

To configure FEC on a port, see Configuring port settings.

FEC Mode	Description
Disable	Disables FEC, which might be preferable in low-error environments or where FEC overhead could negatively impact performance.
All	Automatically selects the optimal FEC mode (excluding **Auto-Negotiation**) for transmitting and receiving data packets.

FEC Mode	Description
RS-FEC (Reed-Solomon FEC)	Provides robust error correction. Suitable for noisy environments or where data integrity is critical but may introduce higher latency. This mode is ideal for environments with significant interference or long-distance transmission where strong error correction is needed.
BASE-R-FEC (Fire-Code FEC)	Offers lower latency than RS-FEC but with weaker correction. Ideal for high-speed ports such as 25 GbE switching ports. This mode is suitable for high-speed, low-latency networks where minimal delay is essential. **Note** QSW managed switches equipped with 100 GbE ports are incompatible with the BASE-R-FEC mode.
Auto-Negotiation	Automatically determines the best FEC mode based on network conditions. This mode is suitable for dynamic networks needing automatic selection of the optimal FEC mode based on real-time conditions.

Configuring port breakout settings

The breakout configuration function allows you to segment a single high-bandwidth port into four lower-capacity sub-interfaces, increasing flexibility in network traffic management. For instance, a 100 GbE port can be divided into four separate 25 GbE ports using a breakout cable or module.

The Interface ID helps you identify these sub-interfaces. It follows the format `<port_number>/<sub-interface_range>`, where the port number represents the physical port and the sub-interface range shows how it has been divided.

- Breakout enabled
  `1(1/1-4)`: This means that port 1 is divided into four sub-interfaces—`1/1`, `1/2`, `1/3`, and `1/4`—each functioning as an independent connection.
- Breakout disabled
  `3(3/1)`: This indicates that port 3 is not divided and operates as a single 100 GbE connection.

1. Log in to the switch system.
2. Go to **System** > **Port Management** > **Breakout Configuration**.
3. Identify a port.
4. Under **Breakout State**, click  .

The switch enables port breakout, splitting the port into four sub-interfaces.

Configuring IPv4 interface and management port settings

Note

- You can add up to 32 VLAN interfaces.
- Each VLAN interface can be assigned with an IPv4 address and an IPv6 address.

1. Log in to the switch system.
2. Go to **System** > **IP Configuration** > **IPv4 Interface Settings**.
3. Optional: Configure the management port settings.
   Users can access the switch through a dedicated management port without being affected by network congestion or malfunction.
   a. Next to **Management Port**, click .
      The switch enables the management port.
   b. Under **Action**, click .
      The **Edit Management Port Interface** window appears.
   c. Select the interface type.
      - **DHCP**: The adapter automatically acquires an IPv4 address and related network settings.
      - **Static**: Manually assign a static IP address to the adapter.
        - Fixed IP address
        - Subnet mask
        - Gateway
   d. Click **Save**.
4. Optional: Configure the IPv4 interface settings.
   The IPv4 interface allows users to access the switch through the ports that are also used for network traffic management.
   a. Next to **IPv4 Interface**, click .
   b. Click **Add**.
      The **Add IPv4 Interface** window appears.
   c. Select a preconfigured VLAN ID from the drop-down list.
   d. Select the interface type.
      - **DHCP**: The adapter automatically acquires an IPv4 address and related network settings.

- **Static**: Manually assign a static IP address to the adapter.
  - Fixed IP address
  - Subnet mask
  - Gateway

e. Click **Save**.
The switch closes the configuration window.

5. Click **Save**.

The switch saves the IPv4 interface and management port settings.

Configuring IPv6 settings

> **Note**
> IPv6 configuration features are supported exclusively in QSS Pro versions.

1. Log in to the switch system.
2. Go to **System** > **IP Configuration** > **IPv6 Interface Settings**.
3. Click **Add**.
The **Add IPv6 Interface** window appears.
4. Select a VLAN ID.
5. Select an IP address assignment method.
   - **DHCP**: The adapter automatically acquires an IPv6 address and DNS settings from the DHCPv6-enabled server.
   - **Static**: Manually assign a static IP address to the adapter. You must specify the following information:
     - IPv6 address
     - Prefix length

     > **Tip**
     > Obtain the prefix length information from your network administrator.
6. Click **Save**.

The switch saves the IPv6 interface settings.

> **Tip**
> You can edit or delete IPv6 interfaces by clicking or , respectively.

Configuring DNS server settings

> **Note**
> DNS server configuration is available only in QSS Pro versions.

1. Log in to the switch system.
2. Go to **System** > **IP Configuration** > **DNS Settings**.
3. Click **Add**.
   The **Add DNS Server** window appears.
4. Select a preference number to determine the order in which the system tries to contact the DNS servers.
5. Select the IP version.
6. Specify the IP address.
7. Click **Save**.

The switch saves the DNS server settings.

Configuring MC-LAG (multichassis link aggregation group) settings

This section details the configuration options for MC-LAG on QSS Pro. MC-LAG aggregates physical links across multiple switches, appearing as a single logical LAG to connected devices, enhancing redundancy, load balancing, and simplifying network management.

> **Important**
> Ensure identical MC-LAG configuration across all member switches for proper operation.

1. Log in to the switch system.
2. Click **MC-LAG**.
3. Click **Settings**.
   The **MC-LAG Settings** window appears.
4. Specify the VLAN ID.
5. Specify an IP address for inter-chassis control protocol (ICCP) communication.
6. Specify the IP subnet mask.
7. Select one or more ports.
8. Select one or more link aggregation groups.

9. Click **Save**.
   The switch saves the MC-LAG configuration.

10. On the **MC-LAG** page, click  .

The switch enables MC-LAG.

Configuring QoS settings

Quality of service (QoS) enables the switch to examine incoming packets and classify them into groups to prioritize certain traffic over others. You can classify these packets based on the type of traffic, source, or destination address. You can also configure and enable traffic policies on the switch ports using two QoS classification techniques, Differentiated Services Code Point (DSCP) and class of service (CoS).

1. Log in to the switch system.
2. Go to **QoS** > **QoS**.
3. Next to **QoS**, click  .
   QoS is enabled on the switch.
4. Identify a port or LAG.
5. Under **DSCP**, click  .
   DSCP is enabled on the port or LAG.
6. Specify a CoS value to assign to incoming packets.

   Note

   - When DSCP is enabled on a port, incoming packets are tagged with the specified CoS value. The packets are then processed in order of priority according to their CoS value and which queue the CoS value is mapped to.
   - The switch uses CoS 802.1p priority tag values which range from 0 to 7. By default, they are each mapped to the queue of the same number, where queue 0 receives the lowest priority and queue 7 the highest priority. To change the default mappings, see Mapping CoS values to queues.
   - The switch does not override the CoS values of incoming packets that have already been assigned CoS values.

7. Click **Save**.

The switch saves the QoS settings.

Mapping CoS values to queues

The switch supports 8 queues for each switch port. Different queues receive different priority in the network traffic, where queue 0 receives the lowest priority and queue 7 receives the highest priority.

By default, CoS values 0-7 each map to the queue of the same number. Therefore, a data packet with CoS value 0 would be put in queue 0 and processed last, after data packets with higher CoS values have been processed. However, you can change this default mapping by assigning different queues to the CoS values. You can also assign the same queue to more than one CoS value.

1. Log in to the switch system.
2. Go to **QoS** > **CoS Mapping**.
3. Assign a queue for each CoS value.
4. Click **Save**.

The switch saves the mappings.

Mapping DSCP values to queues

Differentiated Services Code Point (DSCP) is a field in the header of an IP packet that is used to provide QoS optimization. You can map DSCP values to queues to determine the priority of incoming IP packets based on their DSCP values.

Queue 0 receives the lowest priority, while queue 7 receives the highest priority.

By default, the switch assigns the following queues to the following DSCP value ranges.

DSCP Values	Queue
0-7	0
8-15	1
16-23	2
24-31	3
32-39	4
40-47	5
48-55	6
56-63	7

1. Log in to the switch system.
2. Go to **QoS** > **DSCP Mapping**.
3. Assign a queue number to each DSCP value.
4. Click **Save**.

The switch saves the mappings.

Configuring QoS rate limits

1. Log in to the switch system.
2. Go to **QoS** > **Rate Limits**.
3. Identify a port.
4. Click .
   The **Configure Rate Limiting** window opens.
5. Specify the ingress rate between 1 and 1000 Mbps.
6. Specify the egress rate between 1 and 1000 Mbps.

   Tip
   Select **Unlimited** to allow unlimited ingress or egress traffic.
7. Click **Save**.

The switch saves the rate limit settings.

Tip
To enable rate limits on multiple ports simultaneously, click **Multiple Port Configuration**.

Optimizing intelligent AV streaming

Intelligent AV streaming optimization utilizes algorithms for dynamic bandwidth allocation and prioritization of audio/visual traffic, ensuring smooth streaming through packet classification and congestion control.

1. Log in to the switch system.
2. Go to **QoS** > **Intelligent AV Streaming Optimization**.
3. Click .
4. Click **Save**.

The switch enables intelligent AV streaming optimization.

Configuring Layer 2 (L2) settings

Layer 2 (L2) settings enable you to adjust network configurations at the data link layer, allowing devices within the same network segment to communicate effectively. These settings typically include managing VLANs, link aggregation, and MAC address tables, which help control traffic flow and improve network performance. Configuring these options enhances network security, reduces congestion, and optimizes data transmission within the local network.

This section provides detailed steps to configure L2 settings on your switch for a stable and organized network structure.

Adding a VLAN

A virtual LAN (VLAN) groups multiple network devices together and limits their broadcast domain. Members of a VLAN are isolated and network traffic is only sent between group members.

Each VLAN is assigned a specific VLAN identification number. The **VLAN** screen displays information about existing VLANs and provides access to VLAN configuration options.

1. Log in to the switch system.
2. Go to **L2 Features** > **VLAN**.
3. Click **Add**.
   The **Add VLAN** window opens.
4. Specify a VLAN ID.
5. Optional: Specify a name for the VLAN.
6. Select ports to include in the VLAN.

   Note

   - Click a port once to configure it as an untagged port or twice to configure it as a tagged port.
   - Only tagged ports can belong to multiple VLANs.
7. Click **Save**.

The switch adds the VLAN.

Adding a link aggregation group (LAG)

The Link Aggregation Control Protocol (LACP) allows you to combine multiple switching ports into a single logical network interface. This ensures increased throughput and provides redundancy. In case of port failure, traffic continues on the remaining ports.

The **Link Aggregation** page displays information about existing link aggregation groups and provides access to configuration options.

Warning
To prevent network loop errors during the LAG configuration process, do not connect the switch to other devices using more than one network cable until after you have configured LAGs on all the devices. You can enable loop protection to avoid network loops in the connected network.

1. Log in to the switch system.

2. Go to **L2 Features** > **Link Aggregation**.
3. Identify a group.
4. Click .
   The **Edit Group** window opens.
5. Configure the group settings.

Setting	Description
Mode	Controls the link aggregation mode for the group • **LACP**: Uses IEEE 802.3ad protocol to send Link Aggregation Control Protocol Data Units (LACPDUs) to connected devices to establish a link aggregation. This allows you to control the bundling of several physical links into a logical link. • **Static**: Establishes link aggregation without the LACP protocol **Important** Ensure that you configure the LAG before connecting cables to the switch to avoid creating a data loop.
Port Configu-ration	Specifies which ports are included in the group **Note** Ensure that you configure the same settings for all the member ports in a LAG.

6. Click **Save**.
   The **Edit Group** window closes.
7. Configure the load-balancing algorithm settings.
   The selected load-balancing algorithm for LAGs dictates traffic distribution across member links, influencing factors like throughput optimization and redundancy effectiveness.
   a. Next to **Load balance algorithm**, click .
      The **Load-Balancing Algorithm Settings** window appears.
   b. Select an algorithm.
   c. Click **Save**.
      The **Load balance algorithm** window closes.

The switch applies the LAG settings.

Note

When assigning a LAG to a VLAN, QNAP recommends removing individual LAG port members from the VLAN, and then adding the entire group to the VLAN as required. If individual port members are not removed, the VLAN is reset to its default settings.

Enabling or disabling RSTP

RSTP provides rapid convergence of the spanning tree and builds a loop-free topology for the switch network. RSTP allows you to enable backup links in case an active link fails.

Note

- RSTP is disabled by default.
- The default bridge priority for the switch is 32768.

1. Log in to the switch system.
2. Go to **L2 Features** > **RSTP**.
3. Next to **RSTP**, click  to enable the RSTP function.
4. Select the RSTP bridge priority from the drop-down list.

   Note

   - The default bridge priority is 32768.
   - For root bridge priority, QNAP recommends setting the value to zero.

5. Identify a port.
6. Enable or disable RSTP on the port.

Toggle State	Description
	Click to enable the RSTP function.
	Click to disable the RSTP function.

7. Click **Save**.

The switch saves the RSTP setting.

Enabling or disabling LLDP

The Link Layer Discovery Protocol (LLDP) uses periodic broadcasts to advertise device information over the network and discover neighboring devices. This protocol operates by establishing a distributed database and gathering information from neighboring ports connected by a network link.

The **LLDP** page displays information about detected devices and allows you to enable or disable LLDP.

1. Log in to the switch system.
2. Go to **L2 Features** > **LLDP**.
3. Enable or disable LLDP.

Toggle State	User Action
	Click to enable the LLDP function.
	Click to disable the LLDP function.

4. Click **Save**.

The switch saves the LLDP setting.

Configuring IGMP snooping

The Internet Group Management Protocol (IGMP) manages IP multicast group memberships. IP hosts and adjacent multicast routers use IGMP to establish multicast group memberships.

The **IGMP Snooping** page displays information about detected IGMP groups and provides access to IGMP snooping configuration options.

1. Log in to the switch system.
2. Go to **L2 Features** > **IGMP Snooping** > **IGMP Snooping Settings**.
3. Next to **IGMP Snooping**, click  .
   The switch enables IGMP snooping.
4. Next to **Multicast Flood Blocking**, click  .
   Enable multicast flood blocking to ensure efficient forwarding of multicast traffic by directing packets only to interested devices.
5. Under **Action**, click  .
   The **Edit IGMP Snooping Settings** window appears.
6. Configure the IGMP snooping settings.
   a. Select the IGMP snooping state.
   b. Optional: Enable IGMP querier to send periodic query packets to multicast groups to avoid multicast traffic loss.

c. Optional: Enable fast leave to improve the responsiveness of multicast group membership changes.

d. Optional: Select a static route port to act as the designated router for multicast traffic.

7. Click **Save**.

The switch saves the IGMP snooping settings.

Configuring AV over IP settings

AV over IP (Audio-Visual over Internet Protocol) transmits digital audio and video streams over Ethernet networks, enabling efficient and scalable AV signal distribution by utilizing existing infrastructure. AV over IP utilizes managed switches to prioritize and secure the real-time transmission of audio and video streams over an IP network.

Important

Enabling IGMP snooping, fast leave, IGMP querier, and multicast flood blocking, and configuring appropriate VLANs are crucial first steps for configuring AV over IP on your switch.

1. Log in to the switch system.
2. Go to **L2 Features** > **IGMP Snooping** > **AV over IP**.
3. Select a preconfigured VLAN ID.
4. Next to **AV over IP**, click  .
5. Click **Save**.

The switch enables AV over IP on the switch.

Configuring the dynamic MAC address aging timer

The aging timer deletes a MAC address entry from the table if there has been no incoming traffic from that MAC address after the specified period.

1. Log in to the switch system.
2. Go to **L2 Features** > **MAC Address Table** > **Dynamic MAC Address**.
3. Specify the dynamic MAC address aging time.
4. Click **Save**.

The switch saves the dynamic MAC address aging time.

Adding a static MAC address

To improve frame forwarding efficiency between LAN ports, the network switch maintains a MAC address table that maps MAC addresses to LAN ports of connected devices. You can manually add a MAC address to the table, which allows the switch to retain the MAC entry even after a reboot.

1. Log in to the switch system.
2. Go to **L2 Features** > **MAC Address Table** > **Static MAC Address**.
3. Click **Add**.
   The **Add Static MAC Address** window opens.
4. Configure the MAC address settings.
   a. Specify a MAC address.
   b. Specify a VLAN ID.
   c. Select a switching port or LAG.
5. Click **Save**.
   The **Add Static MAC Address** window closes.

The switch adds the MAC address.

> **Tip**
> The MAC address table in QSS 4.x and QSS Pro 4.x includes a dynamic refresh function, allowing for real-time updates of the associated device list. To update the table, go to **L2 Features** > **MAC Address** > **MAC Address Table**, and then click the designated **Refresh** button.

Configuring the PTP transparent clock settings

Configuring Precision Time Protocol (PTP) transparent clock (TC) settings on a QSW managed switch enhances time synchronization by accounting for the transit time of PTP messages, improving precision across networked devices. This setup is crucial for environments needing accurate timing, such as data centers and industrial systems, as it reduces latency and network delays. Enabling transparent clock mode helps maintain compliance with PTP standards like IEEE 1588, ensuring better performance and compatibility within the network.

1. Log in to the switch system.
2. Go to **L2 Features** > **PTP** > **TC Configuration**.
3. Next to **PTP transparent clock**, click  .
4. Specify the clock domain number between 0 and 127 to define the timing synchronization domain for network devices.

5. Locate the desired ports or LAGs, and then click  under the **Action** column.
6. Click **Save**.

The switch enables the transparent clock settings on the ports and LAGs.

Configuring Lite Layer 3 (LL3) settings

Lite Layer 3 (LL3) settings enable you to manage routing and network configurations at the network layer, facilitating communication between different subnets and network segments. These settings typically include configuring static routing, setting up a DHCP server for automated IP address assignment, and managing ARP (Address Resolution Protocol) and NDP (Neighbor Discovery Protocol) to map and discover connected devices efficiently.

Configuring LL3 options helps optimize traffic flow, enhance network performance, and ensure uninterrupted communication across network segments. LL3 settings are only available on QSS Pro.

Static route settings

You can create and manage static routes in the **Routing** page. Under normal circumstances, the router automatically obtains routing information after it has been configured for internet access. Static routes are only required in special circumstances, such as having multiple IP subnets located on your network.

QSS Pro maintains distinct routing tables for IPv4 and IPv6 traffic, ensuring proper separation and handling of each type of network communication.

Adding an IPv4 static route

1. Log in to switch system.
2. Go to **L3 Features** > **Routing**.
   The **IPv4 Static Route** page appears.
3. Click **Add**.
   The **Add IPv4 Static Route** window appears.
4. Optional: Next to **Default route**, click ☐.
   The static route is selected as the default routing interface.
5. Specify a static IP address where connections are routed to.
6. Specify the IP address of the destination's subnet mask.
7. Specify the gateway IP address of the interface that will act as the next hop for this route.
8. Click **Save**.

The switch creates the IPv4 static route.

Adding an IPv6 static route

1. Log in to the switch system.
2. Go to **L3 Features** > **Routing**.
   The **IPv4 Static Route** page appears.
3. Click **IPv6 Static Route**.
4. Click **Add**.
   The **Add IPv6 Static Route** window appears.
5. Optional: Next to **Default route**, click ☐.
   The static route is selected as the default routing interface.
6. Specify a static IP address where connections are routed to.
7. Select the prefix length for IPv6 addressing.
8. Specify the gateway IP address of the interface that will act as the next hop for this route.
9. Select a preconfigured VLAN ID.
10. Click **Save**.

The switch creates the IPv6 static route.

Configuring DHCP server settings

The Dynamic Host Configuration Protocol (DHCP) server on a managed switch automatically assigns IP addresses, subnet masks, and other configuration parameters to devices requesting them on the network. This simplifies network management and ensures consistent IP address allocation.

> **Note**
> The DHCP server maintains a table of DHCP bindings, which are associations between assigned IP addresses and device MAC addresses.
> To clear the table, go to **L3 Features** > **DHCP Server** > **DHCP Bindings**, and then click **Clear**.

1. Log in to the switch system.
2. Go to **L3 Features** > **DHCP Server**.
3. Click **Add**.
   The **Add DHCP Server** window appears.
4. Select a preconfigured VLAN ID.
5. Enter the first IP address in the pool that will be assigned to DHCP clients.

6. Enter the last IP address in the pool that will be assigned to DHCP clients.

   Note
   Ensure this address falls within the same subnet as the starting IP address.

7. Specify the subnet mask for the network segment where DHCP clients reside.
8. Enter the IP address of the default gateway for the DHCP clients.
9. Enter the IP address of the primary DNS server for DHCP clients.
10. Optional: Enter the IP address of the secondary DNS server for DHCP clients
11. Enter the desired lease time in days, hours, or minutes.

    Note

    - This determines how long a DHCP client can retain its assigned IP address before needing to renew it.
    - Select **Infinite lease** if you want DHCP clients to retain their assigned IP addresses indefinitely.

12. Click **Save**.
    The switch saves the DHCP server settings.
13. On the **DHCP Server** page, enable the DHCP server by clicking  .

The switch enables the DHCP server on the switch.

Adding a static ARP entry

A static Address Resolution Protocol (ARP) entry is a manually configured link between an IP address and a MAC address in a network device, ensuring consistent device identification. It helps users enhance network stability and security by preventing ARP spoofing, where attackers trick the network into sending data to the wrong device, and by avoiding address conflicts, making it crucial for reliable communication in managed switches.

1. Log in to the switch system.
2. Go to **L3 Features** > **ARP Table** > **Static ARP**.
3. Click **Add**.
   The **Add Static ARP Entry** window opens.
4. Specify the IP address that you want to associate with a MAC address for static mapping.
5. Select a VLAN ID that corresponds to the network domain of the specified IP address to ensure proper routing within the same segment.

6. Enter the MAC address to complete the static mapping.
7. Click **Save**.

The switch saves the static ARP entry.

Configuring the dynamic ARP aging timer

The aging timer removes an ARP entry from the table if no traffic is received from the associated IP-MAC address within the specified period.

1. Log in to the switch system.
2. Go to **L3 Features** > **ARP Table** > **Dynamic ARP**.
3. Specify the dynamic ARP aging timer.
4. Click **Save**.

The switch saves the dynamic ARP aging time.

Adding a static NDP entry

A static NDP (Neighbor Discovery Protocol) entry is a user-defined association between an IPv6 address and a MAC address in a network device. Unlike dynamic NDP entries, which are automatically discovered, static entries remain unchanged unless manually modified or deleted. These static mappings help maintain network stability and security by preventing unauthorized devices from altering the associations between IP and MAC addresses. This is essential in networks where reliable and secure device communication is required.

1. Log in to the switch system.
2. Go to **L3 Features** > **IPv6 NDP Table** > **Static NDP**.
3. Click **Add**.
   The **Add Static NDP Entry** window opens.
4. Specify the IPv6 address that you want to associate with a MAC address for static mapping.
5. Select a VLAN ID that corresponds to the network domain of the specified IPv6 address to ensure proper routing within the same segment.
6. Enter the MAC address to complete the static mapping.
7. Click **Save**.

The switch saves the static NDP entry.

> **Tip**
> To refresh or clear the NDP entries, navigate to **L3 Features** > **IPv6 NDP Table** > **IPv6 NDP Cache**, then click **Refresh** to update the entries or click **Clear Table** to remove them.

.

4. Security Management

To create a reliable network environment that supports organizational operations and minimizes risks, you can implement effective security measures, including loop protection to block harmful loops and access control lists (ACLs) to filter traffic and prevent unauthorized access.

Configuring loop protection settings

A loop occurs when data packets are continually forwarded between ports. Network loops often lead to a significant drop in network performance. Enabling loop protection allows you to disable the affected interface temporarily to avoid network degradation.

1. Log in to the switch system.
2. Go to **Security** > **Loop Protection**.
3. Next to **Loop protection**, click  .
4. Specify how much time after detecting a loop to disable the port.

   Note

   - The default shutdown time is 180 seconds.
   - The value must be from 0 to 604800 seconds.

5. Under **Action**, click  to enable loop protection on specific ports or all ports.
6. Click **Save**.

The switch saves the loop protection settings.

Managing access control list (ACL) entries

ACLs allow you to handle network traffic in a switch by using controlled rule sets. Each ACL rule is a user-created set of conditions that the switch uses to determine whether a data packet can pass through the network. If the data packet matches an existing ACL rule, the switch then uses the rule to determine whether to permit or deny the packet. If there is no matching ACL rule or there are no ACL rules, the switch applies a default rule.

You can use ACLs to control host access to different parts of a network or to control traffic forwarding or blocking at the switch level.

Adding an IPv4 address–based ACL rule

1. Log in to the switch system.
2. Go to **Security** > **ACL** > **By IPv4 Address**.

3. Click **Add**.
   The **Add ACL - IPv4 Address** window opens.

4. Configure the ACL settings.

Setting	User Action
ACL No.	This value must be from 1 to 255.
Protocol	Select the type of traffic affected by the ACL entry.
TCP Flag	Select one or more connection states to filter the TCP traffic.
Source	
IP Address	Specify the IP address of an incoming connection.
Subnet Mask	Specify the subnet mask used by an incoming connection.
Service Port	Specify the port number used by an incoming connection.
Destination	
IP Address	Specify the IP address being accessed by a source connection.
Subnet Mask	Specify the subnet mask being accessed by a source connection. **Important** Specifying a subnet mask other than 255.255.255.255 broadcasts traffic to the entire subnet, potentially affecting unintended hosts. For example, using 255.255.255.0 broadcasts to the entire 256-address subnet.
Service Port	Specify the port number being accessed by a source connection.

5. Select the switching ports to apply the ACL rule.

6. Specify the type of permission type used for the ACL entry.

   - **Allow**: Allows access for the configured IP addresses.
   - **Deny**: Restricts access for the configured IP addresses.
   - **Mirror**: Forwards a copy of the matching traffic to a designated monitoring port for analysis without affecting the original flow.

> **Note**
> If the source or destination field is left blank, the permission setting is applied to all connections.

7. Click **Save**.

The switch adds the IPv4 address–based ACL rule.

Adding an IPv6 address-based ACL rule

1. Log in to the switch system.
2. Go to **Security** > **ACL** > **By IPv6 Address**.
3. Click **Add**.
   The **Add ACL - IPv6 Address** window opens.
4. Configure the ACL settings:

Setting	User Action
ACL No.	This value must be from 1 to 255.
Protocol	Select the type of traffic affected by the ACL entry. • **TCP**: A connection-oriented protocol that ensures reliable data transmission. • **UDP**: A connectionless protocol that provides fast but unreliable data transfer. • **ICMPv6**: A protocol used for network diagnostics and error messages. • **IP**: A general option that applies to all IPv6 traffic.
TCP Flag	Select one or more connection states to filter TCP traffic. • **FIN**: Indicates the sender wants to end the connection. • **RST**: Resets the connection immediately. • **ACK**: Confirms receipt of data. • **SYN**: Initiates a new connection. • **PSH**: Requests immediate data processing. • **URG**: Marks data as urgent for priority handling.
Source	
IP Address	Specify the IPv6 address of an incoming connection.

Setting	User Action
Prefix Length	Specify the prefix length used by an incoming connection.
Service Port	Specify the port number used by an incoming connection.
Destination	
IP Address	Specify the IPv6 address being accessed by a source connection.
Prefix Length	Specify the prefix length being accessed by a source connection.
Service Port	Specify the port number being accessed by a source connection.

Note
If a field is left blank, the system displays `Any` to indicate no specific restriction.

5. Select the switching ports to apply the ACL rule.
6. Specify the permission type for the ACL entry.
   - **Allow**: Grants access to the configured IPv6 addresses.
   - **Deny**: Restricts access to the configured IPv6 addresses.
   - **Mirror**: Forwards a copy of the matching traffic to a designated monitoring port for analysis without affecting the original flow.
7. Click **Save**.

The switch adds the IPv6 address–based ACL rule.

Adding a MAC address–based ACL rule

1. Log in to the switch system.
2. Go to **Security** > **ACL** > **By MAC Address**.
3. Click **Add**.
   The **Add ACL - MAC Address** window opens.
4. Configure the ACL settings.

Setting	User Action
ACL No.	Specify a number between 1 and 255.
Source	

Setting	User Action
MAC address	Specify the source MAC address.
Destination	
MAC address	Specify the destination MAC address.
Port	Select specific ports to apply the ACL rule, or select **All** to apply the rule to all ports.

5. Specify the permission type for the ACL entry.
   - **Allow**: Grants access to the configured MAC addresses.
   - **Deny**: Restricts access to the configured MAC addresses.
   - **Mirror**: Forwards a copy of the matching traffic to a designated monitoring port for analysis without affecting the original flow.
6. Click **Save**.

The switch adds the MAC address–based ACL rule.

5. System Maintenance and Diagnostics

This chapter outlines essential procedures for ensuring optimal system performance and reliability. It covers key topics such as log management, Digital Diagnostic Monitoring (DDM), port diagnostics, port mirroring, and firmware updates. These maintenance practices are crucial for optimizing system functions and preventing potential operational disruptions.

Firmware management

QNAP recommends keeping your device firmware up to date. This ensures that your device can benefit from new software features, security updates, enhancements, and bug fixes.

You can update the switch firmware using one of the following methods:

Update Method	Description
Using **Live Update**	Firmware updates are automatically detected and installed onto your device. For details, see Checking for live updates.
Using **Manual Update**	You can check for firmware updates on the QNAP website, download updates to a computer, and manually install updates onto your device. For details, see Updating the firmware manually.

Firmware update requirements

Your device must meet the following requirements to perform a firmware update:

Requirement	Description
Hardware equipment	• A computer • Ethernet cables **Note** • A computer is required when updating the firmware manually or using Qfinder Pro. • QNAP recommends updating the firmware using wired Ethernet connections to ensure your network connection remains stable during the firmware update process.
Back up system settings	QNAP recommends backing up the system settings to your computer before updating the firmware. For details, see Backing up system settings.

Requirement	Description
Administrator privileges	You must be a switch administrator or have administrator privileges to update the firmware.
Stop switch operations	Updating the firmware may disrupt ongoing switch services and operations. QNAP recommends stopping all switch operations before the firmware update. The switch must be restarted for the firmware update to take effect.
Device model name	Ensure that you have the correct switch model name. You can find the switch model name using one of the following methods: • Locate the model name on a sticker on the bottom or rear of your device. • View the model name on the top banner. • Go to **Maintenance** > **Firmware Update** > **Live Update** > **Model name**.
Firmware version	If you are manually updating the firmware using **Firmware Update** or Qfinder Pro, ensure the selected firmware version is correct for your device model.

Checking for live updates

Warning

- To prevent data loss, QNAP recommends backing up all data on your device before updating the firmware. For details, see Backing up system settings.
- Do not power off your device during the firmware update process.
- QNAP devices configured exclusively on IPv6 networks may not receive automatic live updates due to current server limitations.

Important

- Make sure you review Firmware update requirements before updating the firmware.
- The update may require several minutes or longer, depending on your hardware configuration and network connection.

1. Log in to the switch system.
2. Go to **Maintenance** > **Firmware Update** > **Live Update**.
3. Click **Check for update**.
   The switch checks for available firmware updates. You can choose to update the firmware if there is an available update.

4. Click **Update System**.
   A confirmation message appears.
5. Click **Update**.

The switch updates the firmware.

Updating the firmware manually

Warning

- To prevent data loss, QNAP recommends backing up all data on your device before updating the firmware. For details, see Backing up system settings.
- Do not power off your device during the firmware update process.

Important

- Make sure you review Firmware update requirements before updating the firmware.
- The update may require several minutes or longer, depending on your hardware configuration and network connection.

1. Download the device firmware.
   a. Go to http://www.qnap.com/download.
   b. Select the product type.
   c. Select your device model.
   d. Read the release notes and confirm the following:
      - The device model matches the firmware version.
      - Updating the firmware is necessary.
      - Check for any additional firmware update setup instructions.
2. Ensure that the product model and firmware are correct.
3. Select the download server based on your location.
4. Download the firmware package.
5. Click **Browse**.
6. Select a folder.
7. Save the downloaded firmware package.
8. Extract the firmware image file.
9. Log in to the switch system.
10. Go to **Maintenance** > **Firmware Update** > **Firmware Update**.

11. Click **Browse** and then select the extracted firmware image file.
12. Click **Update System**.
    A confirmation message window appears.
13. Click **Update**.

The switch updates the firmware and restarts automatically.

Performing and viewing port diagnostics

You can use built-in port diagnostics on your network switch to conduct comprehensive functionality tests on the RJ45 ports, aiding in the isolation of connectivity problems and guaranteeing proper network operation.

> **Note**
> Port test is a model-specific feature available only on switches with RJ45 ports.

1. Log in to the switch system.
2. Go to **Maintenance** > **Port Diagnostics** > **Port Tests**.
3. Select a port number.
4. Click **Test**.

The switch displays the port test results.

> **Note**
> If a pair status is `Open`, it indicates that there is a break in the cable. The cable length and cable fault distance can be used to identify the location of the break.

Configuring switch LED behavior

There are two configuration options for switch LEDs:

- Locator LED activation: Enable the locator LED to simplify switch identification within a rack or dense environment. When activated, the locator LED will flash for a user-defined duration.
- LED mode selection: Choose the desired LED mode to control the behavior of the locator LED and the LEDs on the front panel. These modes determine whether the LEDs are enabled or disabled, allowing you to customize the level of visual indication for switch activity and potential issues.

> **Note**
> LED behavior configuration is a model-specific feature and may not be available on all switch models. In QSS 4.1, it is available on all supported models running QSS 4.0 or later. In QSS Pro 4.1, LED behavior configuration remains model-specific.

1. Log in to the switch system.
2. Go to **Maintenance** > **Port Diagnostics** > **LED Controls**.

   Note
   On switches without RJ45 ports, go to **Maintenance** > **LED Controls**.

3. Specify the LED activity duration for the locator LED.
4. Click **Start**.
   The switch activates the locator LED.
5. Optional: Select an LED mode.

LED Mode	Description
Normal	All LEDs behave in accordance with their corresponding system state. This is the default mode.
Locator LED always on	The locator LED displays solid green. Other switch LEDs behave in accordance with their corresponding system state. This mode can be used to easily identify the switch in a rack or other environment.
Locator LED always off	The locator LED is disabled. Other switch LEDs behave in accordance with their corresponding system state. This mode can be used to reduce visual distractions.
Disable all LEDs	All LEDs are disabled. This mode can be used to conserve power or to reduce visual distractions.

6. Click **Save**.

The switch saves the selected LED mode.

Configuring port mirroring

Port mirroring is a network monitoring technique that copies data packets from one or more source ports and transmits them to a dedicated destination port for analysis and troubleshooting.

1. Log in to the switch system.
2. Go to **Maintenance** > **Port Mirroring**.
3. Next to **Port Mirroring**, click  .
   The switch enables port mirroring.
4. Select a destination port.

5. For each source port, select the traffic mirroring direction.

Mirroring Direction	Description
Both	Mirrors all packets to the destination port
Egress	Mirrors only outgoing packets to the destination port
Ingress	Mirrors only incoming packets to the destination port
Disabled	Mirroring is disabled on the port

6. Click **Save**.

The switch saves the port mirroring settings.

Configuring digital diagnostic monitoring (DDM) settings

Digital diagnostic monitoring (DDM) provides real-time monitoring and diagnostics of the optical transceiver parameters of your managed switch. DDM helps maintain network health by setting threshold alerts when parameter values exceed or fall below expected ranges.

1. Log in to the switch system.
2. Go to **Maintenance** > **DDM**.
3. Select one of the following parameter settings:
   - **Temperature Settings**
   - **Voltage Settings**
   - **Bias Current Settings**
   - **TX Power Settings**
   - **RX Power Settings**
4. Identify the desired port.
5. Under the **Action** column, click .
   The threshold configuration window appears.
6. Specify the threshold values for the following.

Criteria	Description
High Alarm	The upper critical threshold, beyond which the parameter value indicates a severe issue that requires immediate attention.

Criteria	Description
High Warning	A high but non-critical threshold, signaling that the parameter value is nearing potentially problematic levels.
Low Warning	A low but non-critical threshold, indicating that the parameter value is approaching potentially problematic levels.
Low Alarm	The lower critical threshold, below which the parameter value indicates a serious issue that requires immediate attention.

7. Click **Save**.
   The threshold configuration window closes.
8. Under **Threshold Control**, click  .

   Note
   Enabling the threshold toggle button activates the specified threshold values and triggers a system log when these values are reached. Disabling the toggle prevents the threshold values from triggering a system log, even if they are exceeded.
   You can edit the threshold values regardless of the state of the toggle button.
9. Click **Save**.

The switch saves the DDM parameter setting and enables DDM on the configured ports.

Switch log management

You can filter logs based on their severity level, search for specific log files, or delete them altogether. These logs can be used to diagnose issues or monitor switch operations.

1. Log in to the switch system.
2. Go to **Maintenance** > **Log**.
3. Perform any of the following tasks.

Task	User Action
Search log files	**a.** Locate the **Search** field. **b.** Enter search terms.
Delete log files	**a.** Click **Clear**. The **Clear Logs** window opens. **b.** Click **Clear**.

The switch performs the specified task.

6. AMIZcloud Management

By integrating QNAP QSW managed switch with AMIZcloud, you can add your device using a join key or hardware details, enabling streamlined monitoring, configuration, and deployment. This integration enhances network management efficiency, providing real-time insights and remote access to optimize your IT infrastructure.

About AMIZcloud

AMIZcloud (https://amizcloud.qnap.com) is a centralized cloud management platform designed for remotely deploying, managing, and monitoring QNAP devices located in various places in your organization. After creating an organization and specifying user roles, you can add devices to your organization by using an AMIZcloud join key or specifying hardware information.

Owners and administrators in your organization can manage, operate, and configure connected devices and also deploy virtual machines or containers on these devices. You can create alert policies to receive notifications for specific events and view the comprehensive dashboard to monitor the status of your devices. Providing deployment flexibility and facilitating device management, AMIZcloud helps you build a robust IT infrastructure to boost your productivity.

Registering your switch with AMIZcloud

1. Log in to your switch system.
2. Click  .
3. Click **Begin Setup**.
   The **Connect Your Switch to AMIZcloud** window appears.
4. Click **Get Started Using your QNAP ID**.
   The **Register to AMIZcloud** wizard appears.
5. Select your device's region from the drop-down menu.
6. Click **Next**.
   The **QNAP Account Center** login page appears on a new browser tab.
7. Enter your QNAP ID and password.
8. Click **Sign in**.
   The **QNAP Account Center** page closes.
9. Go back to the AMIZcloud configuration page.
   The **Device Registration** window opens.
10. Specify a device name.

11. Optional: Next to **Join an organization**, click .

> **Note**
> When registering your device with AMIZcloud, joining an organization allows organization administrators to manage your device. Once you join, your device will be automatically assigned to the default organization and site.

12. Select an organization from the drop-down list.
13. Select a site.
14. Click **Register**.
    AMIZcloud registers the device.
15. Optional: Click **Go to AMIZcloud**.

The AMIZcloud web page opens in a new tab.

For details on managing your QSW managed switch with AMIZcloud, see Managing your switch with AMIZcloud.

> **Tip**
>
> - Once the device is registered with AMIZcloud, appears to indicate a successful registration.
> - indicates that the device either failed to register with AMIZcloud or lost its connection. To restore connectivity, select the drop-down menu next to the icon, and then click under **AMIZCloud Status**.

Managing your switch with AMIZcloud

Once your switch is registered with AMIZcloud, you can access management features directly through the AMIZcloud portal. You can monitor device performance, apply configuration changes, and manage firmware updates to maintain optimal network operations.

1. Log in to AMIZcloud.
   The **Dashboard** page appears.

> **Note**
> If you did not join an organization during the device registration process with AMIZcloud, click next to the AMIZcloud logo to access and manage your switch settings.
> For details, see Switching between QNAP ID and QNAP organization device management mode.

2. Click **QSW Switches**.

3. Click your switch name.
   The **General** page opens.

4. Perform any of the following tasks.

Task	User Action
Unregister the device from AMIZcloud	**a.** Under **Action**, click **Unregister**. **b.** On the confirmation page, click **Confirm**. AMIZcloud unregisters the device. This action will deactivate all AMIZcloud services associated with the device.
Edit the asset number	Editing a device's asset number allows you to keep accurate and up-to-date records of your device within AMIZcloud. **a.** Under **Action**, click **Edit Asset Number**. The **Edit Device Asset Number** window opens. **b.** Enter an asset code containing 1-32 characters. **Note** Use any combination of letters (A-Z, a-z), numbers (0-9), or special characters. **c.** Click **Apply**.

7. Support and other resources

QNAP provides the following resources:

Resource	URL
Documentation	https://download.qnap.com
Service Portal	https://service.qnap.com
Downloads	https://download.qnap.com
QNAP Community	https://community.qnap.com