QSS and QSS Pro CLI

User Guide

Firmware: v4.5
Published: September 2026

Table of Contents

Revision History

PUBLISH DATE	COMMENTS
September 2026	First release of the QSS CLI Manual for QSS / QSS Pro firmware 4.5.

1. Overview

This chapter introduces the QSS and QSS Pro command-line environment: what it is, the command modes it's structured into, and the conventions this manual uses to document each command.

IN THIS CHAPTER

About QSS and QSS Pro

QSS and QSS Pro are the network operating systems that run on QNAP QSW managed switches.

- **QSS** focuses on essential Layer 2 (L2) switching: VLANs, link aggregation, spanning tree, and network monitoring.
- **QSS Pro** extends QSS with Lite Layer 3 (LL3) functions — static routing, a DHCP server, DHCP relay, and related IP-layer features.

Both editions share the same command-line interface. Commands exclusive to one edition are marked **QSS only** or **QSS Pro only** throughout this manual; anything without that badge works on both.

About the command-line interface (CLI)

The CLI gives administrators direct, granular control over switch configuration, monitoring, and troubleshooting — available even when the network or web interface is unreachable, since it can be reached through the switch's console port as well as over the network.

CLI modes

The CLI is organized into modes. Each mode exposes a different set of commands and is shown by a distinct prompt.

An administrator login (console or SSH) starts directly in Privileged EXEC — there is no separate User EXEC mode or `enable` step to reach it.

MODE	PROMPT	ENTERED WITH	EXIT WITH
Privileged EXEC	`qss#`	(start of session)	`logout`
Global configuration	`qss(config)#`	`configure terminal`	`end` (Privileged EXEC)
Interface configuration	`qss(config-if)#`	`interface <interface-type> <interface-id>`	`exit` / `end`
Port-channel interface configuration	`qss(config-if)#`	`interface port-channel <n>`	`exit` / `end`
VLAN interface configuration	`qss(config-if)#`	`interface vlan <vlan-id>`	`exit` / `end`
Config-VLAN	`qss(config-vlan)#`	`vlan <vlan-id>`	`exit` / `end`
SNTP configuration	`qss(config-sntp)#`	`sntp`	`exit` / `end`
DHCP pool configuration	`qss(dhcp-config)#`	`dhcp pool <pool-index>`	`exit` / `end`
ACL extended access list configuration	`qss(config-extnacl)#`	`ip access-list extended <access-list-number>`	`exit` / `end`
ACL MAC configuration	`qss(config-extmacl)#`	`mac access-list extended <access-list-number>`	`exit` / `end`
Line configuration	`qss(config-line)#`	`line console`	`exit` / `end`

Mode navigation commands

The table above shows, for every mode, which command enters it and which leaves it — this section documents each of those commands on its own, with syntax, parameters, and an example. Entries marked **entry command** also create the thing they enter configuration mode for (a VLAN, a DHCP pool, an access list); rather than repeat that command's own full parameter reference here, each one links to its existing entry.

Session and mode transitions

Configure Terminal

Privileged EXEC

Moves from Privileged EXEC to Global configuration mode.

SYNTAX

```
configure terminal
```

PARAMETERS

No parameters.

EXAMPLE

```
qss# configure terminal
```

NOTES

- Enters Global configuration mode (prompt changes to qss(config)#).
- At the Privileged EXEC prompt, configure is listed with the description "Configures the terminal".

Exit

Any Global configuration sub-mode

Leaves the current configuration sub-mode and returns to Global configuration mode.

SYNTAX

```
exit
```

PARAMETERS

No parameters.

EXAMPLE

```
qss(config-vlan)# exit
```

NOTES

- Returns to Global configuration mode (qss(config)#) from any of these sub-modes: Interface configuration, Port-channel interface configuration, VLAN interface configuration, Config-VLAN, SNTP configuration, DHCP pool configuration, ACL extended access list configuration, ACL MAC configuration, and Line configuration.
- The exit command is also listed at qss# (Privileged EXEC), described as "Exit from EXEC mode".

End

Global configuration and its sub-modes

Returns directly to Privileged EXEC mode from Global configuration or any of its sub-modes.

SYNTAX

```
end
```

PARAMETERS

No parameters.

EXAMPLE

```
qss(config)# end
```

NOTES

- Enters Privileged EXEC mode directly (prompt changes to qss#), skipping Global configuration even from a sub-mode.
- The end command is also listed at qss# (Privileged EXEC) itself, described as "Exit to the privileged Exec (#) mode".

Logout

Privileged EXEC

Ends the CLI session.

SYNTAX

```
logout
```

PARAMETERS

No parameters.

EXAMPLE

```
qss# logout
```

NOTES

- The logout command is listed at qss# (Privileged EXEC), described as "Log out from EXEC mode".

Help

Privileged EXEC

Displays help for CLI commands.

SYNTAX

```
help
```

PARAMETERS

No parameters.

EXAMPLE

```
qss# help
```

NOTES

- The help command is listed at qss#, described as "Displays help for the command" — it prints the full command list for the current mode, paged.

Lock

Privileged EXEC

Locks the console.

SYNTAX

```
lock
```

PARAMETERS

No parameters.

EXAMPLE

```
qss# lock
```

NOTES

- The lock command is listed at qss#, described as "Lock the console".

Entering a configuration sub-mode

Interface

Global configuration

Enters Interface configuration mode for a physical port.

SYNTAX

```
interface <interface-type> <interface-id>
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
`interface-type`	`varies by model`	Interface type keyword, e.g. gigabitethernet or extreme-ethernet (see note below).	—
`interface-id`	`slot/port`	Port number in slot/port form, e.g. 0/1.	—

EXAMPLE

```
qss(config)# interface gigabitethernet 0/1
```

NOTES

- Enters Interface configuration mode (prompt changes to qss(config-if)#).
- The interface type keyword depends on the switch model and port type — for example "gigabitethernet" or "extreme-ethernet" (abbreviation "ex"); "port-channel <n>" addresses a link-aggregation group. Type "?" after the command to list the interface types available on your switch.

Interface Port-Channel

Global configuration

Enters Port-channel interface configuration mode for a link-aggregation group.

SYNTAX

```
interface port-channel <channel-group-number>
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
channel-group-number	1-N (device-dependent)	Port-channel (LACP) group number.	—

EXAMPLE

```
qss(config)# interface port-channel 1
```

NOTES

- Enters Port-channel interface configuration mode (prompt changes to qss(config-if)#).

SNTP

Global configuration

Enters SNTP configuration mode.

SYNTAX

```
sntp
```

PARAMETERS

No parameters.

EXAMPLE

```
qss(config)# sntp
```

NOTES

- Enters SNTP configuration mode (prompt changes to qss(config-sntp)#).

VLAN (entry command)

Global configuration

Creates the VLAN if it does not already exist, and enters Config-VLAN mode.

SYNTAX

```
vlan <vlan-id (1-4094)>
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
vlan-id	1-4094	ID of the VLAN to create or enter — see Set VLAN (Layer 2 Features) for the full parameter reference.	—

EXAMPLE

```
qss(config)# vlan 4
```

NOTES

- Enters Config-VLAN mode (prompt changes to qss(config-vlan)#). Also creates the VLAN if it does not already exist — see Set VLAN (Layer 2 Features) for the full parameter reference.

Interface VLAN (entry command)

Global configuration

Creates the VLAN interface (SVI) if it does not already exist, and enters VLAN interface configuration mode.

SYNTAX

```
interface vlan <vlan-id (1-4094)>
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
vlan-id	1-4094	ID of the VLAN interface (SVI) to create or enter — see Set VLAN Interface (IP Configuration) for the full parameter reference.	—

EXAMPLE

```
qss(config)# interface vlan 5
```

NOTES

- Enters VLAN interface configuration mode (prompt changes to qss(config-if)#). Also creates the VLAN interface if it does not already exist — see Set VLAN Interface (IP Configuration) for the full parameter reference.

DHCP Pool (entry command)

Global configuration QSS Pro only

Creates the DHCP address pool if it does not already exist, and enters DHCP pool configuration mode.

SYNTAX

```
dhcp pool <pool-index (1-2147483647)>
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
pool-index	1-2147483647	DHCP pool index — identifies this address pool (not a VLAN ID or subnet).	—

EXAMPLE

```
qss(config)# dhcp pool 1
```

NOTES

- Enters DHCP pool configuration mode (prompt changes to qss(dhcp-config)#). Also creates the DHCP pool if it does not already exist — see Set DHCP Server Pool (Layer 3 Features) for the full parameter reference.

IP Access List Extended (entry command)

Global configuration

Creates the extended IP access list if it does not already exist, and enters ACL extended access list configuration mode.

SYNTAX

```
ip access-list extended <access-list-number (1001-65535)>
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
access-list-number	1001-65535	Extended IP access list number to create, delete, or configure.	—

EXAMPLE

```
qss(config)# ip access-list extended 1001
```

NOTES

- Enters ACL extended access list configuration mode (prompt changes to qss(config-extnacl)#). Also creates the access list if it does not already exist — see Set IP Access List (Security) for the full parameter reference.

MAC Access List Extended (entry command)

Global configuration

Creates the extended MAC access list if it does not already exist, and enters ACL MAC configuration mode.

SYNTAX

```
mac access-list extended <access-list-number (1-65535)>
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
access-list-number	1-65535	Extended MAC access list number to create, delete, or configure.	—

EXAMPLE

```
qss(config)# mac access-list extended 1
```

NOTES

- Enters ACL MAC configuration mode (prompt changes to qss(config-extmacl)#). Also creates the access list if it does not already exist — see Set MAC Access List (Security) for the full parameter reference.

Line Console (entry command)

Global configuration

Enters Line configuration mode.

SYNTAX

```
line console
```

PARAMETERS

No parameters.

EXAMPLE

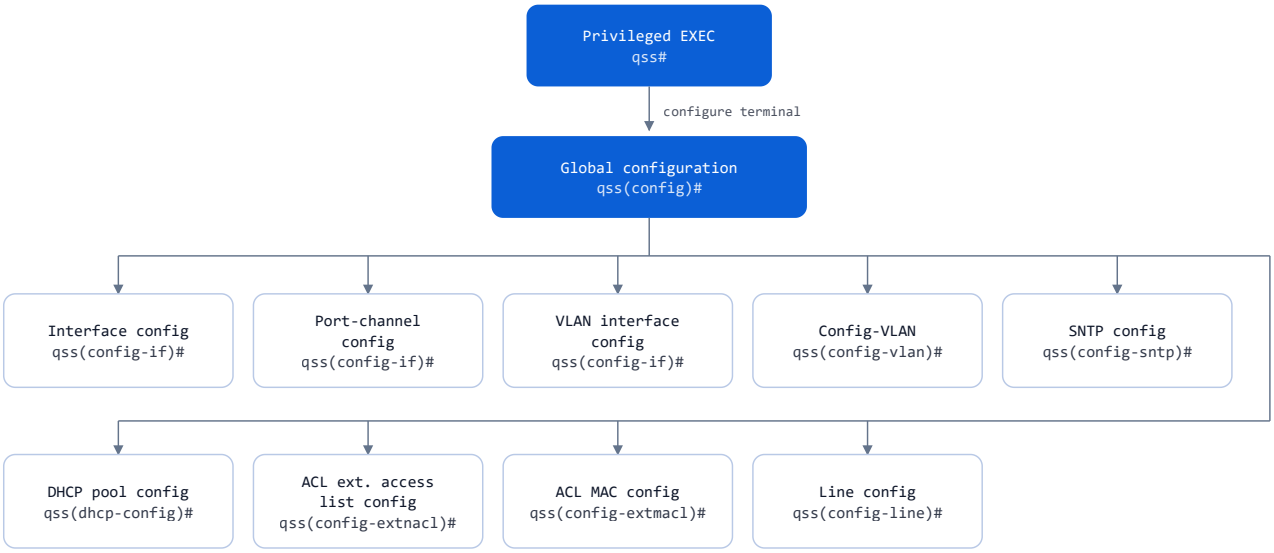
```
qss(config)# line console
```

NOTES

- Enters Line configuration mode (prompt changes to qss(config-line)#) — see Set Line Console Mode (Maintenance) for the existing full entry.

CLI hierarchy

The CLI is structured hierarchically: higher-level modes allow broad system configuration, while lower-level modes provide detailed control over an individual interface or feature.



CLI commands

This section describes what CLI commands are, how commands are organized in this manual, and how to read a command reference entry.

Where a feature has hidden dependencies — settings that must be configured elsewhere first, or a typical order to configure them in — its group opens with a **Before you begin** callout and a numbered **Configuration order** list, so you see what you need before you start instead of discovering it from a failed command. DHCP Relay (chapter 5, Layer 3 (L3) Commands) is the current example.

Every command entry in this manual uses the same structure: **Description** (purpose and notable behavior), **Syntax** (exact keywords and parameter placeholders), **Mode** (which CLI mode(s) it runs in), **Prerequisites** (shown only when the command has one — **Required** when it actually fails without it, **Typical order** when it's just the usual sequence), **Parameters** (each parameter's allowed values/range), **Example** (typical usage), and **Example output** (shown only for commands whose output was captured from a real switch — see Conventions below for masking and blank-line formatting).

Conventions used in this guide

Commands can include combinations of keywords, options, and arguments. The basic conventions for syntax elements are as follows:

CONVENTION	EXAMPLE	MEANING
Plain text	`show interfaces status`	Type it exactly as shown.
< >	`<vlan-id>`	A required value you supply yourself.

CONVENTION	EXAMPLE	MEANING
`{ }`	`{ enable | disable }`	A required choice — pick exactly one, separated by |. A single mandatory item (no |) is written bare instead.
`[ ]`	`[<gateway>]`	Optional — you may omit it.
`[{ }]`	`[{ send | receive }]`	An optional choice.
no	`no shutdown`	Reverses or removes the setting made by the positive form.

Where a command has a `no` form, it is shown in the same entry as the positive form (one Syntax block listing both) rather than as a separate command — the `no` form removes or resets the setting, as described in that entry's Notes when its effect isn't a plain opposite of the positive action.

Where an example output was captured from a real switch, device-identifying values — switch name, MAC address, and serial number — are masked to placeholders (`<switch-name>`, `<mac-address>`, `<serial-number>`); consecutive blank lines may be reduced for readability. Other output text and indentation are preserved.

Configuration commands in this manual change the running configuration; run `save` (**Save Configuration**, System Settings) to keep changes across a reboot.

Getting help

The CLI can tell you what's valid at any point, and tells you what went wrong when something isn't — you don't need to have this manual open to find out.

Context-sensitive help (`?`) — press `?` to list what's valid at the current point. After a command followed by a space, `?` also displays short descriptions of the command and available options. For example, `show loop_protection ?` lists `all`, `details`, `interface`, and `summary` with descriptions; `<CR>` indicates that pressing Enter executes the command as entered. Typed alone at a prompt, it lists every command available in the current mode (see CLI modes above — the list depends on which mode you're in); typed directly after a partial keyword, it lists the matching completions:

```
qss# show system-?
system-information
system-log-server
qss# show system-
% Ambiguous Command
```

Incomplete command hints — enter a command that's missing a required parameter, and the CLI prints that command's full syntax line instead of running it:

```
qss(config)# set port-mirr
CONFIGURE commands :  set port-mirroring {enable | disable}
qss(config)# set port-mirroring
% Incomplete command.
```

Tab completion and keyword abbreviation — press **Tab** to auto-complete a partial keyword. A keyword can also be abbreviated to the fewest characters that still identify it uniquely — if the CLI can't tell which command you mean, it reports `% Ambiguous Command`.

Reading the `^` marker — `% Invalid input detected at '^' marker` points the caret at the first token the CLI couldn't parse:

```
qss(config)# vlan 123143
vlan 123143
     ^
% Invalid input detected at '^' marker
```

See the Error Messages chapter for the general parser plus the DHCP relay, ACL, DNS, and ARP messages, or the Error Message Index to look one up by the text shown on screen.

Interface naming

Every command that takes an interface operand uses `<interface-type> <interface-id>` — e.g. `gigabitethernet 0/1`. The interface ID is always `<slot>/<port>`.

The interface type keyword depends on your switch model. This manual can't list a fixed set — the keywords your switch accepts (e.g. gigabitethernet, extreme-ethernet, abbreviated ex) depend on the model and port type; port-channel `<n>` always addresses a link-aggregation group regardless of model. Type `?` after the command to list the interface types available on your switch.

2. CLI Access

This chapter explains how to connect to the switch and log in to the CLI, and how user privilege levels control what a logged-in session can do.

IN THIS CHAPTER

Connecting the switch to a computer

Connecting the switch to a computer through the console port lets you access the CLI and configure network settings before the switch has any network connectivity of its own.

1. Insert the console cable into the console port on the switch.
2. Connect the opposite end to the serial port or USB-to-serial interface on your computer.
3. Power on the switch.
4. Confirm that the switch power and port LEDs indicate an active physical link.
5. Install and configure a terminal emulator (see below).

The CLI can also be reached over the network via **SSH** (port 22). Enable it first with:

```
qss# ssh enable
```

Check whether it's currently on with `show ssh status`.

Installing a terminal emulator

Any terminal emulator that supports a serial console session works — for example PuTTY (Windows, Linux, macOS):

Windows	Download the installer from putty.org and run it; the default install options are fine.
Linux	Install from your package manager, e.g. `sudo apt install putty` (Debian/Ubuntu) or `sudo dnf install putty` (Red Hat/CentOS/Fedora).
macOS	Install with Homebrew (`brew install putty`), or skip PuTTY entirely and use the built-in Terminal app with `ssh admin@<switch-ip>` once SSH is enabled.

Accessing the CLI

Open a console (or SSH) session with the switch and log in: open your terminal emulator and connect to the switch's console port (or its IP address, over SSH), then enter the switch username and password.

Setting	Default
Default username	`admin`
Default password	The switch's MAC address, with the separators removed (e.g. MAC `00-08-9B-F6-15-75` → password `00089BF61575`)

Change the default password. Change it as soon as possible after first login — see **Set Admin Password** and **Set User Account** in System Settings.

User authentication and privilege levels

QSS and QSS Pro use local user authentication by default; an administrator creates accounts from Global configuration mode:

```
qss(config)# username guest privilege viewer status enable password guest123
```

Each account has one of two roles:

admin	Administrator privilege: full access — every CLI mode and every command in this manual.
viewer	Command scope includes `show`, `set`, `ping`, and `list user`. Other viewer command behavior is outside this list.

This is the access model exposed by the `username` command in firmware v4.5 — a fixed choice of admin or viewer.

Saving your changes

Every configuration command in this manual changes only the switch's running configuration, not what it will load the next time it starts. Run `save` from Global configuration mode to write the running configuration to the startup configuration, so it survives a reboot — see **Save Configuration** (System Settings). The startup configuration is what the switch loads back after **Restart Switch** (`reload`, System Settings) or a power cycle — any configuration change made since the last save is lost if the switch restarts first.

```
qss(config)# save
qss# reload
```

3. System and Interface Settings

This chapter provides the commands used to configure and manage system parameters and network interfaces. It covers operations such as viewing and modifying port settings, assigning IP addresses, and adjusting key system features. These commands are fundamental for maintaining switch performance and network connectivity through the CLI.

IN THIS CHAPTER

IN THIS CHAPTER (CONTINUED)

Port Management

This section explains commands for configuring and monitoring physical network interfaces. It covers tasks such as displaying port status, modifying interface parameters, and configuring port breakout to meet deployment requirements.

Port status & statistics

These commands display an interface's current status, description, and flow-control setting, and its traffic counters, without changing any configuration.

Show Port Status

Privileged EXEC

Displays the status, description, and flow-control setting of one or all interfaces.

SYNTAX

```
show interfaces [<interface-type> <interface-id>] [{ description | flowcontrol | status }]
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
interface-type	varies by model	Interface type keyword, e.g. gigabitethernet or extreme-ethernet (see note below).	—
interface-id	slot/port	Port number in slot/port form, e.g. 0/1.	—
description | flowcontrol | status	description | flowcontrol | status	Limits the display to just this one field, instead of the full status output (optional).	—

EXAMPLE

```
qss# show interfaces extreme-ethernet 0/1
```

EXAMPLE OUTPUT

```
qss# show interfaces extreme-ethernet 0/1

Ex0/1 up, line protocol is down (not connect)
Bridge Port Type: Customer Bridge Port

Interface SubType: extremeEthernet
Interface Alias: 1

Hardware Address is <mac-address>
MTU  9216 bytes, Full duplex, 10 Gbps,  Auto-Negotiation
FEC Mode: auto(Reed-Solomon(RS))
802.3ap: Disable
HOL Block Prevention enabled.
CPU Controlled Learning disabled.
Auto-MDIX on
Input flow-control is off,output flow-control is off

Link Up Trap is disabled

Link Down Trap is disabled

Reception Counters
   Octets                   : 0
   Unicast Packets          : 0
...
```

NOTES

- The interface type keyword depends on the switch model and port type — for example "gigabitethernet" or "extreme-ethernet" (abbreviation "ex"); "port-channel <n>" addresses a link-aggregation group. Type "?" after the command to list the interface types available on your switch.

Show Port Statistics

Privileged EXEC

Displays interface traffic counters.

SYNTAX

```
show interfaces counters
```

PARAMETERS

No parameters.

EXAMPLE

```
qss# show interfaces counters
```

EXAMPLE OUTPUT

```
qss# show interfaces counters

Port      InOctet    InUcast    InMcast    InBcast    InDiscard   InErrs     InHCOctet
----      -------    -------    -------    -------    ---------   ------     ---------
Ex0/1             0          0          0          0          0          0          0
Ex0/2             0          0          0          0          0          0          0
Ex0/3             39819      0          202        156        0          0          39819
Ex0/4             0          0          0          0          0          0          0
Ex0/5             0          0          0          0          0          0          0
Ex0/6             0          0          0          0          0          0          0
Ex0/7             0          0          0          0          0          0          0
Ex0/8             0          0          0          0          0          0          0
Ex0/9             0          0          0          0          0          0          0
Ex0/10            0          0          0          0          0          0          0
Ex0/11            0          0          0          0          0          0          0
Ex0/12            0          0          0          0          0          0          0
Ex0/13            0          0          0          0          0          0          0
Ex0/14            0          0          0          0          0          0          0
Ex0/15            35061      0          176        123        0          92         35061
Ex0/16            0          0          0          0          0          0          0
Ex0/17            0          0          0          0          0          0          0
Ex0/18            0          0          0          0          0          0          0
Ex0/19            0          0          0          0          0          0          0
Ex0/20            0          0          0          0          0          0          0
...
```

Port settings

These commands configure per-interface parameters: administrative state, description, speed, pause-frame flow control, and forward error correction (FEC).

Set Port State

Interface configuration

Enables or disables (shuts down) the interface.

SYNTAX

```
shutdown
no shutdown
```

PARAMETERS

No parameters.

EXAMPLE

```
qss(config-if)# shutdown
```

Set Port Name

Interface configuration

Sets a descriptive name for the interface.

SYNTAX

```
description <description (24)>
no description
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
description	24	Descriptive name for the interface.	—

EXAMPLE

```
qss(config-if)# description myAP
```

Set Port Speed

Interface configuration

Sets the interface's speed.

SYNTAX

```
speed { 100 | 1000 | 2500 | 10000 | 25000 | 40000 | 100000 | auto }
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
speed	100 | 1000 | 2500 | 10000 | 25000 | 40000 | 100000 | auto	Interface speed, in Mbps (or auto-negotiate).	auto

EXAMPLE

```
qss(config-if)# speed 1000
```

Set Flow Control

Interface configuration

Turns pause-frame flow control on or off in each direction.

SYNTAX

```
flowcontrol { send | receive } { on | off }
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
send | receive	send | receive	Which pause-frame direction the state applies to.	—
state	on | off	Turns the selected direction's pause frames on or off.	off

EXAMPLE

```
qss(config-if)# flowcontrol send on
```

Set FEC Mode

Interface configuration

Sets the forward error correction (FEC) mode for the interface.

SYNTAX

```
fec { auto | baser | rs | disable }
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
fec	auto | baser | rs | disable	Forward error correction mode for the interface.	auto

EXAMPLE

```
qss(config-if)# fec disable
```

Breakout

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 identifies these sub-interfaces in <port-number>/<sub-interface-range> form, where the port number is the physical port and the sub-interface range shows how it has been divided.

Set Breakout

Interface configuration

Enables or disables breakout mode on a supported port.

SYNTAX

```
breakout { disable | enable }
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
breakout	disable | enable	Enables or disables breakout mode on the port.	disable

EXAMPLE

```
qss(config-if)# breakout enable
```

Show Breakout Status

Privileged EXEC

Displays the breakout status of one or all interfaces.

SYNTAX

```
show interfaces [<interface-type> <interface-id>] breakout-status
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
interface-type	varies by model	Interface type keyword, e.g. gigabitethernet or extreme-ethernet (see note below).	—
interface-id	slot/port	Port number in slot/port form, e.g. 0/1.	—

EXAMPLE

```
qss# show interfaces extreme-ethernet 0/2 breakout-status
```

EXAMPLE OUTPUT

```
qss# show interfaces extreme-ethernet 0/2 breakout-status

Model Breakout:  Enable

Port    Breakout Status    Active   Availability
----    ---------------    ------   ------------
Ex0/2   off                on       false
```

NOTES

- The interface type keyword depends on the switch model and port type — for example "gigabitethernet" or "extreme-ethernet" (abbreviation "ex"); "port-channel <n>" addresses a link-aggregation group. Type "?" after the command to list the interface types available on your switch.

Priority Flow Control (PFC)

On supported QSS Pro models, Priority Flow Control (PFC) ensures lossless transport by pausing traffic on congested queues while allowing other traffic to continue, preventing packet drops and maintaining service quality for critical applications. PFC here operates in active mode, applying flow control to individual ports based on their assigned class of service (CoS) priority, independently of the Data Center Bridging Exchange (DCBX) protocol.

Set PFC Mode

Interface configuration | QSS Pro only

Sets the priority flow control (PFC) mode for the interface.

SYNTAX

```
priority-flow-control mode { off | active }
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
mode	off | active	Priority flow control (PFC) mode for the interface.	off

EXAMPLE

```
qss(config-if)# priority-flow-control mode off
```

Set PFC Queue

Interface configuration | QSS Pro only

Sets which CoS queue priority flow control (PFC) applies to.

SYNTAX

```
priority-flow-control cos-queue <queue (0-7)>
no priority-flow-control cos-queue [<queue (0-7)>]
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
queue	0-7	Egress queue number.	—

EXAMPLE

```
qss(config-if)# priority-flow-control cos-queue 7
```

Show PFC

Privileged EXEC QSS Pro only

Displays the priority flow control (PFC) configuration for all interfaces.

SYNTAX

```
show interfaces priority-flow-control
```

PARAMETERS

No parameters.

EXAMPLE

```
qss# show interfaces priority-flow-control
```

EXAMPLE OUTPUT

```
qss# show interfaces priority-flow-control

Port    PFC mode           Queue

----    --------           -----
Ex0/1   off
Ex0/2   off
Ex0/3   off
Ex0/4   off
Ex0/5   off
Ex0/6   off
Ex0/7   off
Ex0/8   off
Ex0/9   off
Ex0/10  off
Ex0/11  off
Ex0/12  off
Ex0/13  off
Ex0/14  off
Ex0/15  off
Ex0/16  off
Ex0/17  off
Ex0/18  off
Ex0/19  off
...
```

IP Configuration

This section documents commands for configuring IPv4 and IPv6 interfaces and DNS settings. It enables administrators to manage network addressing and name resolution to maintain stable and reliable connectivity.

IPv4 address

These commands assign an IPv4 address to an interface, either as a static address and subnet mask or obtained automatically over DHCP, and show the resulting IPv4 configuration and status.

Set IP Address via DHCP

Interface configuration

Obtains the interface's IPv4 address from DHCP.

SYNTAX

```
ip address dhcp
no ip address
```

PARAMETERS

No parameters.

EXAMPLE

```
qss(config-if)# ip address dhcp
```

Set Static IP Address

Interface configuration

Sets a static IPv4 address and subnet mask on the interface.

SYNTAX

```
ip address <ip-address> <subnet-mask>
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
ip-address	IPv4 address	IPv4 address to assign to the interface.	—
subnet-mask	IPv4 subnet mask	Subnet mask for the address above.	—

EXAMPLE

```
qss(config-if)# ip address 10.0.0.3 255.255.255.0
```

Set VLAN Interface State

Interface configuration

Enables or disables (shuts down) the VLAN interface.

SYNTAX

```
shutdown
no shutdown
```

PARAMETERS

No parameters.

EXAMPLE

```
qss(config-if)# shutdown
```

Show IP Interface

Privileged EXEC

Displays IPv4 configuration and status for all interfaces.

SYNTAX

```
show ip interface all
```

PARAMETERS

No parameters.

EXAMPLE

```
qss# show ip interface all
```

EXAMPLE OUTPUT

```
qss# show ip interface all

oob is up, line protocol is up
Internet Address is <ip-address>/23
Broadcast Address  <ip-address>
IP address allocation method is dynamic
IP address allocation protocol is dhcp

vlan1 is up, line protocol is up
Internet Address is <ip-address>/16
Broadcast Address  <ip-address>
IP address allocation method is dynamic
IP address allocation protocol is dhcp
Vlan counters disabled
```

IPv6 address

These commands assign an IPv6 address to an interface, either as a static address and prefix length or obtained automatically over DHCPv6, and show the resulting IPv6 configuration and status.

Set IPv6 Address

Interface configuration

Sets a static IPv6 address and prefix length on the interface.

SYNTAX

```
ipv6 address <prefix> <prefix-len (0-128)>
no ipv6 address <prefix> <prefix-len (0-128)>
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
prefix	IPv6 address	IPv6 address to assign to the interface.	—
prefix-len	0-128	IPv6 prefix length, in bits.	—

EXAMPLE

```
qss(config-if)# ipv6 address 3333::1111 64
```

Set IPv6 Address via DHCP

Interface configuration

Obtains the interface's IPv6 address from DHCPv6.

SYNTAX

```
ipv6 address dhcp
no ipv6 address dhcp
```

PARAMETERS

No parameters.

EXAMPLE

```
qss(config-if)# ipv6 address dhcp
```

Show IPv6 Interface

Privileged EXEC

Displays IPv6 configuration and status for all interfaces.

SYNTAX

```
show ipv6 interface all
```

PARAMETERS

No parameters.

EXAMPLE

```
qss# show ipv6 interface all
```

EXAMPLE OUTPUT

```
qss# show ipv6 interface all

Forwarding operationally Enabled
Default-hop limit value is 64
RFC5095 is compatible

VRF Id  : 0
VRF Name: default
vlan1 is up, line protocol is up
    Forwarding operationally Enabled
    Link local address:
        fe80::<interface-id> [scope: Linklocal]
    Global unicast address(es):
        Not Configured.
    Joined group address(es):
        <ipv6-address> Scope:[Multicast linklocal]
        <ipv6-address> Scope:[Multicast linklocal]
        <ipv6-address> Scope:[Multicast linklocal]
    MTU is 1500
    ND DAD is enabled, Number of DAD attempts: 1
    Destination Unreachable error messages enabled
    ICMPv6 Error Rate Limiting Enabled
    ICMPv6 Error Rate-Limit Interval: 100
    ICMPv6 Error Rate-Limit Bucket Size: 10
    ICMPv6 Redirects Disabled
...
```

DNS

These commands configure the DNS server addresses the switch uses for name resolution, and show which servers are currently configured. QSS (L2) switches can use only server indexes 1–2 (IPv4 only); QSS Pro (L3) switches can use only indexes 5–8 (IPv4 or IPv6). QSS does not use 5–8, QSS Pro does not use 1–2, and indexes 3–4 and all other indexes are unavailable.

Set DNS Server (IPv4/IPv6)

Global configuration **QSS Pro only**

Sets a DNS server address on a QSS Pro (L3) switch (index 5–8), by IPv4 or IPv6 address. Indexes 1–2 and all other indexes are unavailable to this command.

SYNTAX

```
ip name-server <server-index (5-8)> { ipv4 <ucast_addr> | ipv6 <ip6_addr> }
no ip name-server <server-index (5-8)>
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
server-index	5-8	Index of the DNS server entry to set (this command manages entries 5–8).	—
ucast_addr	IPv4 address	DNS server IPv4 address.	—
ip6_addr	IPv6 address	DNS server IPv6 address.	—

EXAMPLE

```
qss(config)# ip name-server 5 ipv4 12.0.0.6
```

Set DNS Server (IPv4)

Global configuration QSS only

Sets a DNS server address on a QSS (L2) switch (index 1–2), IPv4 only. Indexes 5–8 and all other indexes are unavailable to this command.

SYNTAX

```
ip name-server <server-index (1-2)> ipv4 <ucast_addr>
no ip name-server <server-index (1-2)>
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
server-index	1-2	Index of the DNS server entry to set (this command manages entries 1–2).	—
ucast_addr	IPv4 address	DNS server IPv4 address.	—

EXAMPLE

```
qss(config)# ip name-server 1 ipv4 12.0.0.6
```

Show DNS Servers

Privileged EXEC

Displays the configured DNS server addresses.

SYNTAX

```
show ip dns name-server
```

PARAMETERS

No parameters.

EXAMPLE

```
qss# show ip dns name-server
```

EXAMPLE OUTPUT

```
qss# show ip dns name-server

  Name Server IP Table
  ====================
Index  Address-Type  State  IP-Address
=====  ============  =====  ============
5      ipv4          Static <ip-address>
6      ipv6          Static <ipv6-address>
```

Default gateway (QSS)

These commands set and display the switch's default gateway address, used to reach networks outside its directly connected subnets. This is a QSS-only alternative to configuring a default route directly.

Set Default Gateway

Global configuration QSS only

Sets the switch's default gateway address.

SYNTAX

```
ip default-gateway <ucast_addr>
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
ucast_addr	IPv4 address	Default gateway IPv4 address.	—

EXAMPLE

```
qss(config)# ip default-gateway 192.168.10.1
```

Show Default Gateway

Privileged EXEC QSS only

Displays the configured default gateway.

SYNTAX

```
show ip default-gateway
```

PARAMETERS

No parameters.

EXAMPLE

```
qss# show ip default-gateway
```

Out-of-band (OOB) management

Out-of-band (OOB) management settings allow you to control and configure the dedicated management interface that operates separately from the production data network. These settings include enabling or disabling the OOB port and assigning its IP addressing parameters. By configuring the OOB interface, you ensure reliable access to the device for monitoring, troubleshooting, and recovery, even when in-band connectivity is unavailable.

Set OOB Port State

Global configuration

Enables or disables the out-of-band (OOB) management port.

SYNTAX

```
oob { enable | disable }
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
oob	enable | disable	Enables or disables the OOB management port.	—

EXAMPLE

```
qss(config)# oob enable
```

Set OOB IP Address

Global configuration

Sets the OOB port's IP address, mask, and gateway, or obtains them from DHCP.

SYNTAX

```
oob ip address <ucast_addr> <ip_mask> [<gateway>]
oob ip address dhcp
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
ucast_addr	IPv4 address	OOB port IPv4 address.	—
ip_mask	IPv4 subnet mask	Subnet mask for the OOB port address, e.g. 255.255.255.0.	—
gateway	IPv4 address	Gateway IPv4 address.	—

EXAMPLE

```
qss(config)# oob ip address dhcp
```

NOTES

- Also available via DHCP ("oob ip address dhcp").
- Requires a switch model with an out-of-band management port.

VLAN interface

This command creates or deletes a VLAN interface (switch virtual interface, SVI) — the Layer 3 presence a VLAN needs before it can be given an IPv4 or IPv6 address.

Set VLAN Interface

Global configuration

Creates or deletes a VLAN interface (SVI).

SYNTAX

```
interface vlan <vlan-id (1-4094)>
no interface vlan <vlan-id (1-4094)>
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
vlan-id	1-4094	ID of the VLAN this command applies to.	—

EXAMPLE

```
qss(config)# no interface vlan 5
```

System Settings

This section lets administrators manage system parameters to maintain secure and reliable switch operation.

System information & hostname

These commands display the switch's identifying and status information — model, MAC address, firmware version, serial number, uptime, temperature, and fan speed — and let you set the switch's hostname.

Show System Information

Privileged EXEC

Displays the switch's model name, MAC address, firmware version, serial number, uptime, temperature, and fan speed.

SYNTAX

```
show system-information
```

PARAMETERS

No parameters.

EXAMPLE

```
qss# show system-information
```

EXAMPLE OUTPUT

```
qss# show system-information

System Information
Switch name                     : <switch-name>
Model name                      : QSW-M7230P-2X4F24T
MAC address                     : <mac-address>
Switch firmware                 : 4.5.0.847494 (20260908)
Serial number                   : <serial-number>
System up time                  : 0 Days, 5 Hrs, 19 Mins, 25 Secs
Temperature                     : 33
Fan 1 speed                     : 5273
Fan 2 speed                     : 5294
Fan 3 speed                     : 5357
Fan 4 speed                     : 5314
Fan 5 speed                     : 5357
```

FIELD	MEANING
`Switch name`	Configured device hostname.
`Model name`	Switch model name.
`MAC address`	Base MAC address of the switch.
`Switch firmware`	Running firmware version.
`Serial number`	Device serial number.
`System up time`	Time elapsed since the switch last booted.
`Temperature`	Current chassis temperature reading, in degrees Celsius.
`Fan speed`	Current fan speed reading, in RPM (one line per fan).

Set Hostname

Global configuration

Sets the switch's hostname.

SYNTAX

```
hostname <hostname (32)>
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
hostname	32	Switch hostname, shown in the CLI prompt and used to identify the device.	—

EXAMPLE

```
qss(config)# hostname switch-room101
```

User accounts & passwords

These commands manage local administrator accounts on the switch: setting the built-in admin account's password, and adding, updating, deleting, or listing additional local user accounts.

Set Admin Password

Global configuration

Sets the password for the built-in admin account.

SYNTAX

```
username admin password <passwd>
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
passwd	up to 20 characters	Password for this account/setting.	—

EXAMPLE

```
qss(config)# username admin password admin123
```

Show User Accounts

Privileged EXEC

Lists all local user accounts.

SYNTAX

```
listuser
```

PARAMETERS

No parameters.

EXAMPLE

```
qss# listuser
```

Set User Account

Global configuration

Adds, updates, or deletes a local user account.

SYNTAX

```
username <username (20)> [privilege { admin | viewer }] [status { enable | disable }] password
<password (20)>
no username <username (20)>
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
username	20	Account name to add, update, or delete.	—
privilege	admin | viewer	Account role: full-control admin, or restricted viewer.	—
status	enable | disable	Enables or disables the account without deleting it.	—
password	20	Account password.	—

EXAMPLE

```
qss(config)# username guest privilege viewer status enable password guest123
```

Time & SNTP

Time settings allow you to configure and view the system's internal clock; keeping accurate time ensures correct log timestamps, reliable event correlation, and proper operation of time-dependent features. Simple Network Time Protocol (SNTP) settings let you synchronize that clock with external time servers: you can configure unicast SNTP servers, enable or disable the SNTP client, set the device time zone, and define daylight saving time rules.

Set System Clock

Privileged EXEC

Sets the system date and time.

SYNTAX

```
clock set <hh:mm:ss> <day (1-31)> <month (01-12)> <year (2000-2037)>
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
hh:mm:ss	e.g. 09:00:00	Time of day, 24-hour clock.	—
day	1-31	Day of the month being set.	—
month	01-12	Month of the date being set.	—
year	2000-2037	Year of the date being set.	—

EXAMPLE

```
qss# clock set 09:00:00 10 10 2025
```

Show System Clock

Privileged EXEC

Displays the current system date and time.

SYNTAX

```
show clock
```

PARAMETERS

No parameters.

EXAMPLE

```
qss# show clock
```

EXAMPLE OUTPUT

```
qss# show clock

 Tue Sep 08 07:11:42 2026
```

Set SNTP Unicast Server

SNTP configuration

Sets the SNTP server to synchronize time from, by IPv4 address, IPv6 address, or domain name.

SYNTAX

```
set sntp unicast-server { ipv4 <ucast_addr> | ipv6 <ip6_addr> | domain-name <dns_host_name> }
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
server-type	ipv4 | ipv6 | domain-name	Selects whether the SNTP server below is given as an IPv4 address, an IPv6 address, or a domain name.	—
ucast_addr	IPv4 address	SNTP server IPv4 address.	—
ip6_addr	IPv6 address	SNTP server IPv6 address.	—
dns_host_name	hostname	SNTP server domain name, resolved via DNS.	pool.ntp.org

EXAMPLE

```
qss(config-sntp)# set sntp unicast-server domain-name time.google.com
```

Show SNTP Status

Privileged EXEC

Displays the SNTP unicast client status.

SYNTAX

```
show sntp unicast-mode status
```

PARAMETERS

No parameters.

EXAMPLE

```
qss# show sntp unicast-mode status
```

EXAMPLE OUTPUT

```
qss# show sntp unicast-mode status

auto discovery of sntp/ntp servers is disabled
unicast poll interval value is 1024
unicast max poll time out value is 5
unicast max retry time value is 8
unicast current mode value is SYNCHRONIZED TO PRIMARY SERVER
sntp client is up for 06:36:12
unicast primary server resolved ip address is <ip-address>
unicast primary server host name is pool.ntp.org
unicast primary server version is 4
unicast primary server port is 123
last updated time from the primary server is Tue Sep 08 2026 07:03:47
Num sntp-client req-msgs transmitted to the primary server 20
```

Set SNTP Client

SNTP configuration

Enables or disables the SNTP client.

SYNTAX

```
set sntp client { enabled | disabled }
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
client	enabled | disabled	Enables or disables the SNTP client.	enabled

EXAMPLE

```
qss(config-sntp)# set sntp client enabled
```

Set SNTP Time Zone

SNTP configuration

Sets the switch time zone from a fixed list of GMT offsets, each mapped to representative cities or regions.

SYNTAX

```
set time-zone <GMT-offset> <zone-keyword>
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
GMT-offset	GMT-1100 … GMT1400 (37 offsets; see Time zones table)	UTC offset for the time zone, e.g. GMT0800. See Notes for the full list of offsets and which zone keywords each one accepts.	—
zone-keyword	depends on GMT-offset — see Notes	A city/region name valid for the chosen GMT offset, e.g. Taipei for GMT0800.	—

EXAMPLE

```
qss(config-sntp)# set time-zone GMT0800 Taipei
```

NOTES

- Each GMT offset accepts only its own specific set of zone keywords (37 offsets in total) — see the table below.
- Use the canonical spelling shown for each time-zone keyword.

TIME ZONES

GMT OFFSET	ZONE KEYWORDS
GMT	GreenwichMeanTime_Dublin_Edinburgh_Lisbon_London | Monrovia
GMT0100	Amsterdam_Berlin_Bern_Rome_Stockholm_Vienna | Belgrade_Bratislava_Budapest_Ljubljana_Prague | Brussels_Copenhagen_Madrid_Paris | Sarajevo_Skopje_Warsaw_Zagreb | Casablanca
GMT0200	Athens_Vilnius | Bucharest | Cairo | Harare_Pretoria | Helsinki_Kyiv_Riga_Tallinn | Israel | Kaliningrad
GMT0300	Istanbul | Baghdad_Kuwait_Riyadh | Nairobi | Minsk | Moscow
GMT0330	Tehran
GMT0400	AbuDhabi_Muscat | Baku_Tbilisi | Samara
GMT0430	Kabul
GMT0500	Islamabad_Karachi_Tashkent | Yekaterinburg
GMT0530	Bombay_Calcutta_Madras_NewDelhi | Colombo
GMT0545	Nepal
GMT0600	Omsk
GMT0630	Myanmar
GMT0700	Bangkok_Hanoi_Jakarta | Krasnoyarsk
GMT0800	Beijing_Chongqing_HongKong_Urumqi | Perth | Singapore | Taipei | Irkutsk | Ulaanbaatar
GMT0845	Eucla
GMT0900	Osaka_Sapporo_Tokyo | Seoul | Yakutsk
GMT0930	Adelaide | Darwin
GMT1000	Brisbane | Canberra_Melbourne_Sydney | Guam_PortMoresby | Hobart | Vladivostok
GMT1030	LordHowels
GMT1100	Magadan | Srednekolymsk | SolomonIs | NewCaledonia | NorfolkIs
GMT1200	Auckland_Wellington | Fiji_Kamchatka_MarshallIs | Kamchatka | Kwajalein
GMT1245	ChathamIs
GMT1300	PhoenixIs | Tokelau | Samoa
GMT1400	LineIs
GMT-0100	Azores_CapeVerdeIs
GMT-0200	Mid-Atlantic
GMT-0300	Brasilia | BuenosAires_Georgetown | Greenland
GMT-0330	Newfoundland
GMT-0400	AtlanticTime | Caracas_LaPaz | PuertoRico | Santiago
GMT-0500	Bogota_Lima_Quito | EasternTime | Indiana
GMT-0600	CentralTime | MexicoCity_Tegucigalpa | Saskatchewan
GMT-0700	Arizona | MountainTime | Yukon
GMT-0800	PacificTime
GMT-0900	Alaska
GMT-0930	MarquesasIs

GMT OFFSET	ZONE KEYWORDS
GMT-1000	Hawaii
GMT-1100	MidwayIsland_Samoa

Set SNTP Daylight Saving Time

SNTP configuration

Sets daylight saving time to disabled, automatic, or a manual start/end schedule.

SYNTAX

```
set dst { disable | auto | manual <start (week-day-month,hh:mm)> <end (week-day-month,hh:mm)> [{ one-hour | half-hour | forty-five-minutes }] }
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
dst-mode	disable | auto | manual	Whether daylight saving time is off, automatically scheduled, or set manually with the fields below.	—
start	e.g. First-Sun-Mar,03:30	DST start time in week-day-month,hh:mm form (24-hour), e.g. First-Sun-Mar,03:30 — only used when dst-mode is manual.	—
end	e.g. Second-Sun-Nov,03:30	DST end time, in the same format as the start time — only used when dst-mode is manual.	—
offset	one-hour | half-hour | forty-five-minutes	How much to shift the clock during DST (optional; default one-hour) — only used when dst-mode is manual.	—

EXAMPLE

```
qss(config-sntp)# set dst disable
qss(config-sntp)# set dst auto
qss(config-sntp)# set dst manual First-Sun-Mar,03:30 Second-Sun-Nov,03:30 one-hour
```

Smart fan

These commands set and display the switch's fan speed mode — normal, quiet, or maximum — which controls the tradeoff between cooling and acoustic noise.

Show Smart Fan Mode

Privileged EXEC

Displays the current smart fan mode.

SYNTAX

```
show env fan
```

PARAMETERS

No parameters.

EXAMPLE

```
qss# show env fan
```

EXAMPLE OUTPUT

```
qss# show env fan


SmartFan mode                    : normal
```

Set Smart Fan Mode

Global configuration

Sets the fan speed mode to normal, quiet, or maximum speed.

SYNTAX

```
smartfan mode { normal | quiet | max_speed }
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
mode	normal | quiet | max_speed	Fan speed mode: normal, quiet, or maximum.	normal

EXAMPLE

```
qss(config)# smartfan mode normal
```

SNMP

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).

Set SNMP v2c Community

Global configuration

Sets the SNMPv2c community string and enables the SNMP service.

SYNTAX

```
snmp v2c community <community (31)>
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
community	31	SNMPv2c community string.	—

EXAMPLE

```
qss(config)# snmp v2c community myQnapSwitch
```

Set SNMP v3 User

Global configuration

Sets an SNMPv3 username with optional authentication and privacy settings, and enables the SNMP service.

SYNTAX

```
snmp v3 username <username (31)> [authentication { HMAC-MD5 | HMAC-SHA } <auth-password (31)>
[privacy CBC-DES <priv-password (31)>]]
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
username	up to 31 characters	SNMPv3 username.	—
authentication	HMAC-MD5 | HMAC-SHA	Authentication algorithm (optional).	—
auth-password	up to 31 characters	Authentication password.	—
privacy	CBC-DES	Privacy (encryption) algorithm (optional).	—
priv-password	up to 31 characters	Privacy (encryption) password.	—

EXAMPLE

```
qss(config)# snmp v3 username myQnapSwitch authentication HMAC-SHA <auth-password>
```

Disable SNMP

Global configuration

Disables the SNMP service.

SYNTAX

```
snmp disable
```

PARAMETERS

No parameters.

EXAMPLE

```
qss(config)# snmp disable
```

Show SNMP Configuration

Privileged EXEC

Displays the current SNMP configuration.

SYNTAX

```
show snmp
```

PARAMETERS

No parameters.

EXAMPLE

```
qss# show snmp
```

EXAMPLE OUTPUT

```
qss# show snmp

SNMP service             : Disabled
------------
```

Set SNMP Trap Target Address

Global configuration

Sets up to three SNMP trap target addresses (TagId1–3), each with its own notification parameters (Param1–3).

SYNTAX

```
snmp targetaddr TagId1 param Param1 <ip-address>
snmp targetaddr TagId2 param Param2 <ip-address>
snmp targetaddr TagId3 param Param3 <ip-address>
no snmp targetaddr TagId1
no snmp targetaddr TagId2
no snmp targetaddr TagId3
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
`TagId1 | TagId2 | TagId3`	`TagId1 | TagId2 | TagId3`	Three fixed trap-target slots — set each independently.	—
`Param1 | Param2 | Param3`	`Param1 | Param2 | Param3`	The notification parameter name associated with that slot (matches the "param" keyword argument; up to 31 characters).	—
`IP`	`IPv4 address`	Trap receiver IPv4 address for that slot.	—

EXAMPLE

```
qss(config)# snmp targetaddr TagId2 param Param2 10.1.2.3
```

Show SNMP Trap Target Address

Privileged EXEC

Displays the configured SNMP trap target addresses.

SYNTAX

```
show snmp targetaddr
```

PARAMETERS

No parameters.

EXAMPLE

```
qss# show snmp targetaddr
```

EXAMPLE OUTPUT

Prints nothing when there are no entries.

```
qss# show snmp targetaddr
```

Set Coldstart Trap

Global configuration

Enables or disables the SNMP coldstart trap.

SYNTAX

```
snmp-server enable traps coldstart
no snmp-server enable traps coldstart
```

PARAMETERS

No parameters.

EXAMPLE

```
qss(config)# snmp-server enable traps coldstart
```

Set Warmstart Trap

Global configuration

Enables or disables the SNMP warmstart trap.

SYNTAX

```
snmp-server enable traps warmstart
no snmp-server enable traps warmstart
```

PARAMETERS

No parameters.

EXAMPLE

```
qss(config)# snmp-server enable traps warmstart
```

Set Link Status Trap

Global configuration

Sets which link-status events send an SNMP trap on all ports.

SYNTAX

```
snmp-server enable traps allport link-status { disable | enable | linkup-only | linkdown-only }
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
`link-status`	`disable | enable | linkup-only | linkdown-only`	Which link-status events send an SNMP trap: none, all, link-up only, or link-down only.	—

EXAMPLE

```
qss(config)# snmp-server enable traps allport link-status enable
```

Show SNMP Traps

Privileged EXEC

Displays the SNMP trap configuration.

SYNTAX

```
show snmp-server traps
```

PARAMETERS

No parameters.

EXAMPLE

```
qss# show snmp-server traps
```

EXAMPLE OUTPUT

```
qss# show snmp-server traps

Currently enabled traps:

------------------------
```

DHCP auto-configuration

These commands enable or disable, and show the status of, DHCP client auto-configuration — the switch obtaining its own management-plane settings automatically from a DHCP server.

Show DHCP Auto-Configuration

Privileged EXEC

Displays the DHCP client auto-configuration status.

SYNTAX

```
show dhcp-auto-config
```

PARAMETERS

No parameters.

EXAMPLE

```
qss# show dhcp-auto-config
```

EXAMPLE OUTPUT

```
qss# show dhcp-auto-config

Dhcp auto configuration is Enabled
```

Set DHCP Auto-Configuration

Global configuration

Enables or disables DHCP client auto-configuration.

SYNTAX

```
ip dhcp client auto-dhcp-configuration
no ip dhcp client auto-dhcp-configuration
```

PARAMETERS

No parameters.

EXAMPLE

```
qss(config)# ip dhcp client auto-dhcp-configuration
```

SSH service

These commands enable or disable the SSH service (port 22) used to reach the CLI remotely, and show whether the service is currently enabled.

Set SSH Service

Privileged EXEC

Enables or disables the SSH service (port 22).

SYNTAX

```
ssh { enable | disable }
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
ssh	enable | disable	Enables or disables the SSH service (port 22).	enable

EXAMPLE

```
qss# ssh enable
```

Show SSH Service Status

Privileged EXEC

Displays whether the SSH service is enabled.

SYNTAX

```
show ssh status
```

PARAMETERS

No parameters.

EXAMPLE

```
qss# show ssh status
```

EXAMPLE OUTPUT

```
qss# show ssh status

Port 22, Status: Enabled
```

Restart / reset

These commands restart the switch, reset it to factory defaults (erasing the configuration), or reset the admin password to its factory default.

Restart Switch

Privileged EXEC

Reloads (restarts) the switch.

SYNTAX

```
reload
```

PARAMETERS

No parameters.

EXAMPLE

```
qss# reload
```

Reset to Factory Defaults

Privileged EXEC

Erases the configuration and restores factory defaults.

SYNTAX

```
erase all-config
```

PARAMETERS

No parameters.

EXAMPLE

```
qss# erase all-config
```

Reset Password

Privileged EXEC

Resets the admin password to its factory default.

SYNTAX

```
erase user-password
```

PARAMETERS

No parameters.

EXAMPLE

```
qss# erase user-password
```

Configuration backup & restore

These commands copy the switch's running configuration to or from a remote TFTP server for backup and restore. Save Configuration is different: it writes the running configuration to the startup configuration so it survives a reboot — run it after any configuration change you want to keep, not only as part of a TFTP backup. See "Saving your changes" in CLI Access.

Back Up Configuration

Privileged EXEC

Copies the running configuration to a remote TFTP server.

SYNTAX

```
copy qsw-config tftp://<server>/<filename>
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
server	hostname or IPv4 address	TFTP server to copy the running configuration to.	—
filename	file name/path	Destination file name/path on the TFTP server.	—

EXAMPLE

```
qss# copy qsw-config tftp://192.0.2.1/qsw.config
```

Restore Configuration

Privileged EXEC

Copies a configuration file from a remote TFTP server to the switch.

SYNTAX

```
copy tftp://<server>/<filename> qsw-config
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
server	hostname or IPv4 address	TFTP server to copy the configuration file from.	—
filename	file name/path	Source file name/path on the TFTP server.	—

EXAMPLE

```
qss# copy tftp://192.0.2.1/qsw.config qsw-config
```

Save Configuration

Global configuration

Saves the running configuration as the startup configuration.

SYNTAX

```
save
```

PARAMETERS

No parameters.

EXAMPLE

```
qss(config)# save
```

NOTES

- Run after any configuration change you want to keep across a reboot.

ADRA NDR

These commands enable or disable, and show the status of, ADRA NDR integration — network detection and response for traffic analysis and threat detection.

Show ADRA NDR Mode

Privileged EXEC

Displays whether ADRA NDR integration is enabled.

SYNTAX

```
show adra-ndr-mode
```

PARAMETERS

No parameters.

EXAMPLE

```
qss# show adra-ndr-mode
```

EXAMPLE OUTPUT

```
qss# show adra-ndr-mode

NDR Mode           : Disabled
```

Set ADRA NDR Mode

Global configuration

Enables or disables ADRA NDR integration for network traffic analysis and threat detection.

SYNTAX

```
set adra-ndr-mode { enable | disable }
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
adra-ndr-mode	enable | disable	Enables or disables ADRA NDR integration.	disable

EXAMPLE

```
qss(config)# set adra-ndr-mode enable
```

4. Layer 2 (L2) Features

This chapter provides commands for configuring and managing the device's Layer 2 switching capabilities. It guides administrators in controlling traffic forwarding, link behavior, and device-to-device discovery within the network. The commands in this chapter support efficient network segmentation, enhanced link performance, rapid topology convergence, and monitoring of Layer 2 network activity.

IN THIS CHAPTER

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; these commands create and delete VLANs and manage VLAN Forwarding Instance (VFI) membership.

Set VLAN

Global configuration

Creates or deletes a VLAN.

SYNTAX

```
vlan <vlan-id (1-4094)>
no vlan <vlan-id (1-4094)>
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
vlan-id	1-4094	ID of the VLAN this command applies to.	—

EXAMPLE

```
qss(config)# vlan 4
```

Set VLAN Member Ports

Config-VLAN

Adds or removes tagged and untagged member ports on the VLAN.

SYNTAX

```
ports [add] ([<interface-type> <0/a-b, 0/c, ...>] [<interface-type> <0/a-b, 0/c, ...>] [port-channel
<a,b,c-d>]) [untagged (<interface-type> <0/a-b, 0/c, ...> [<interface-type> <0/a-b, 0/c, ...>] [port-
channel <a,b,c-d>] [all])]
no ports [<interface-type> <0/a-b, 0/c, ...>] [<interface-type> <0/a-b, 0/c, ...>] [port-channel
<a,b,c-d>] [all] [untagged ([<interface-type> <0/a-b, 0/c, ...>] [<interface-type> <0/a-b, 0/c, ...>]
[port-channel <a,b,c-d>] [all])]
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
interface-type	varies by model	Interface type keyword, e.g. gigabitethernet or extreme-ethernet (see note below).	—
add	add	Adds the listed ports/port-channels as members (optional; this is the default action when omitted).	—
0/a-b, 0/c, ...	0/a-b, 0/c, ...	One or more interface IDs (or ranges), comma-separated, e.g. 0/1-4,0/6.	—
port-channel	e.g. 1,2,3-5	One or more port-channel group numbers (or ranges), comma-separated.	—
untagged	untagged	Marks the listed ports/port-channels as untagged members, instead of tagged (optional).	—
all	all	Applies to every port on the VLAN, instead of only the ones listed (optional).	—

EXAMPLE

```
qss(config-vlan)# ports gigabitethernet 0/1 untagged all
```

NOTES

- The interface type keyword depends on the switch model and port type — for example "gigabitethernet" or "extreme-ethernet" (abbreviation "ex"); "port-channel <n>" addresses a link-aggregation group. Type "?" after the command to list the interface types available on your switch.

Set VLAN Name

Config-VLAN

Sets a name for the VLAN.

SYNTAX

```
name <vlan name string>
no name
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
vlan name string	up to 32 characters	User-assigned name for the VLAN.	—

EXAMPLE

```
qss(config-vlan)# name vlan1
```

Show VLAN

Privileged EXEC

Displays a summary of VLANs and their member ports.

SYNTAX

```
show vlan [brief | id <vlan-range> | summary | ascending] [ switch <context_name>]
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
vlan-range	e.g. 10 or 10-20	A VLAN ID, or a range of VLAN IDs.	—
context_name	switch name	Switch stack member name (single-switch systems can omit this).	—

EXAMPLE

```
qss# show vlan
```

EXAMPLE OUTPUT

```
qss# show vlan

Vlan database
-------------
Vlan ID             : 1
Member Ports        : Ex0/1, Ex0/2, Ex0/3, Ex0/4, Ex0/5, Ex0/6
                      Ex0/7, Ex0/8, Ex0/9, Ex0/10, Ex0/11, Ex0/12
                      Ex0/13, Ex0/14, Ex0/15, Ex0/16, Ex0/17, Ex0/18
                      Ex0/19, Ex0/20, Ex0/21, Ex0/22, Ex0/23, Ex0/24
                      Ex0/25, Ex0/26, Ex0/27, Ex0/28, Ex0/29, Ex0/30
                      Ex0/31, Ex0/32, Ex0/33, Ex0/34, Ex0/35, Ex0/36
                      po1, po2, po3, po4, po5, po6
                      po7, po8, po9, po10, po11, po12
                      po13, po14, po15, po16, po17, po18
                      po19, po20, po21, po22, po23, po24
                      po25, po26, po27, po28, po29, po30
                      po31, po32, po33, po34, po35, po36
                      po4093
Untagged Ports      : Ex0/1, Ex0/2, Ex0/3, Ex0/4, Ex0/5, Ex0/6
                      Ex0/7, Ex0/8, Ex0/9, Ex0/10, Ex0/11, Ex0/12
                      Ex0/13, Ex0/14, Ex0/15, Ex0/16, Ex0/17, Ex0/18
                      Ex0/19, Ex0/20, Ex0/21, Ex0/22, Ex0/23, Ex0/24
                      Ex0/25, Ex0/26, Ex0/27, Ex0/28, Ex0/29, Ex0/30
                      Ex0/31, Ex0/32, Ex0/33, Ex0/34, Ex0/35, Ex0/36

                      po1, po2, po3, po4, po5, po6
                      po7, po8, po9, po10, po11, po12
                      po13, po14, po15, po16, po17, po18
                      po19, po20, po21, po22, po23, po24
                      po25, po26, po27, po28, po29, po30
                      po31, po32, po33, po34, po35, po36
                      po4093
Forbidden Ports     : None
Name                :
Status              : Permanent
Egress Ethertype    : 0x8100
Service Loopback Status   : Disabled
AV Profile Type     : no av-type
-----------------------------------------------------
```

Show VLAN Port Membership

Privileged EXEC

Displays the VLAN membership of every port.

SYNTAX

```
show vlan port vlan-id
```

PARAMETERS

No parameters.

EXAMPLE

```
qss# show vlan port vlan-id
```

EXAMPLE OUTPUT

```
qss# show vlan port vlan-id

Port         Port Vlan ID
----         ------------
Ex0/1        1
Ex0/2        1
Ex0/3        1
Ex0/4        1
Ex0/5        1
Ex0/6        1
Ex0/7        1
Ex0/8        1
Ex0/9        1
Ex0/10       1
Ex0/11       1
Ex0/12       1
Ex0/13       1
Ex0/14       1
Ex0/15       1
Ex0/16       1
Ex0/17       1
Ex0/18       1
Ex0/19       1
Ex0/20       1
Ex0/21       1
...
```

Link aggregation (LACP / port-channel)

The Link Aggregation Control Protocol (LACP) allows you to combine multiple switching ports into a single logical network interface (a port-channel). This ensures increased throughput and provides redundancy — in case of port failure, traffic continues on the remaining ports. For link aggregation across two switches, see MC-LAG (chapter 5).

Set Port-Channel Load-Balance Policy

Global configuration

Sets the hashing policy used to distribute traffic across a port-channel's member links.

SYNTAX

```
port-channel load-balance { src-mac | dest-mac | src-dest-mac | src-ip | dest-ip | src-dest-ip | src-dest-mac-ip | src-dest-mac-ip-l4-port }
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
load-balance	src-mac | dest-mac | src-dest-mac | src-ip | dest-ip | src-dest-ip | src-dest-mac-ip | src-dest-mac-ip-l4-port	Hashing policy used to distribute traffic across the port-channel's member links (which fields of the packet decide the egress link).	src-dest-mac

EXAMPLE

```
qss(config)# port-channel load-balance src-dest-mac-ip
```

Show Port-Channel Load-Balance Policy

Privileged EXEC

Displays the port-channel load-balance policy.

SYNTAX

```
show etherchannel load-balance
```

PARAMETERS

No parameters.

EXAMPLE

```
qss# show etherchannel load-balance
```

EXAMPLE OUTPUT

```
qss# show etherchannel load-balance


                Channel Group Listing

                ---------------------

Group : 1

----------
Source and Destination MAC Address

Group : 2

----------
Source and Destination MAC Address

Group : 3

----------
Source and Destination MAC Address

Group : 4

----------
Source and Destination MAC Address

Group : 5

----------
Source and Destination MAC Address

Group : 6

----------
Source and Destination MAC Address

Group : 7

----------
...
```

Set Channel Group

Interface configuration

Assigns the interface to a port-channel (LACP or static) and sets its group number.

SYNTAX

```
channel-group <channel-group-number (1-N)> mode { static | lacp }
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
`channel-group-number`	`1-N (device-dependent)`	Port-channel (LACP) group number.	—
`mode`	`static | lacp`	Whether the group is a static port-channel or a dynamic LACP one.	—

EXAMPLE

```
qss(config-if)# channel-group 1 mode static
```

Show Port-Channel Summary

Privileged EXEC

Displays a summary of all port-channels and their member ports.

SYNTAX

```
show etherchannel summary
```

PARAMETERS

No parameters.

EXAMPLE

```
qss# show etherchannel summary
```

EXAMPLE OUTPUT

```
qss# show etherchannel summary

Port-channel Module Admin Status is enabled

Port-channel Module Oper Status is enabled

Port-channel recovery action on exceeding Threshold is None

Port-channel Independent mode is disabled

Port-channel System Identifier is  <mac-address>

LACP System Priority: 32768

LACP Error Recovery Time: 0

LACP Error Recovery Threshold: 5

LACP Recovery Triggered count: 0

LACP Error Recovery Threshold for Defaulted State : 5

LACP Error Recovery Threshold for Hardware Failure : 5

LACP Same state threshold : 5


Flags:

D - down         P - in port-channel

I - stand-alone  H - Hot-standby (LACP only)

E - ErrDisabled

U - in-use       d - default port

R - Layer3

AD - Admin Down      AU - Admin Up

OD - Operative Down  OU - Operative Up
...
```

Spanning tree

The Rapid Spanning Tree Protocol (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.

Enable Spanning Tree (Global)

Global configuration

Enables or disables spanning tree protocol switch-wide.

SYNTAX

```
spanning-tree
no spanning-tree
```

PARAMETERS

No parameters.

EXAMPLE

```
qss(config)# spanning-tree
```

Set Spanning Tree (Port)

Interface configuration

Enables or disables spanning tree on the interface.

SYNTAX

```
no spanning-tree disable
spanning-tree disable
```

PARAMETERS

No parameters.

EXAMPLE

```
qss(config-if)# no spanning-tree disable
```

Set Spanning Tree Priority

Global configuration

Sets the switch's bridge priority for spanning tree.

SYNTAX

```
spanning-tree priority <bridge-priority (0-61440)>
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
bridge-priority	0-61440	Bridge priority for spanning tree (lower values are preferred as root).	32768

EXAMPLE

```
qss(config)# spanning-tree priority 4096
```

Show Spanning Tree Priority

Privileged EXEC

Displays the switch's spanning tree bridge priority.

SYNTAX

```
show spanning-tree priority
```

PARAMETERS

No parameters.

EXAMPLE

```
qss# show spanning-tree priority
```

EXAMPLE OUTPUT

```
qss# show spanning-tree priority

Bridge Priority is 32768
```

NOTES

- The older `show spanning-tree bridge priority` form is no longer accepted — use `show spanning-tree priority` (without `bridge`).

Show Spanning Tree Summary

Privileged EXEC

Displays a summary of spanning tree port role, state, and status for every port.

SYNTAX

```
show spanning-tree ports-summary
```

PARAMETERS

No parameters.

EXAMPLE

```
qss# show spanning-tree ports-summary
```

EXAMPLE OUTPUT

```
qss# show spanning-tree ports-summary

Spanning Tree Global Status : Disabled
Spanning tree enabled protocol is RSTP
Spanning Tree port pathcost method is Long


RSTP Port Roles and States
Port-Index        Port-Role    Port-State   Port-Status
----------        ---------    ----------   -----------
Ex0/1             Disabled     Discarding   Disabled
Ex0/2             Disabled     Discarding   Disabled
Ex0/3             Disabled     Discarding   Disabled
Ex0/4             Disabled     Discarding   Disabled
Ex0/5             Disabled     Discarding   Disabled
Ex0/6             Disabled     Discarding   Disabled
Ex0/7             Disabled     Discarding   Disabled
Ex0/8             Disabled     Discarding   Disabled
Ex0/9             Disabled     Discarding   Disabled
Ex0/10            Disabled     Discarding   Disabled
Ex0/11            Disabled     Discarding   Disabled
Ex0/12            Disabled     Discarding   Disabled
Ex0/13            Disabled     Discarding   Disabled
Ex0/14            Disabled     Discarding   Disabled
...
```

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.

Set LLDP

Global configuration

Enables or disables LLDP.

SYNTAX

```
set lldp { enable | disable }
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
`lldp`	`enable | disable`	Enables or disables LLDP switch-wide.	`enable`

EXAMPLE

```
qss(config)# set lldp enable
```

Show LLDP

Privileged EXEC

Displays the LLDP configuration.

SYNTAX

```
show lldp
```

PARAMETERS

No parameters.

EXAMPLE

```
qss# show lldp
```

EXAMPLE OUTPUT

```
qss# show lldp

LLDP is enabled
LLDP Version                        : v1
Transmit Interval                   : 30
Holdtime Multiplier                 : 4
Reinitialization Delay              : 2
Tx Delay                            : 2
Notification Interval               : 5
Chassis Id SubType                  : Mac Address
Chassis Id                          : <mac-address>
LLDP Tag Status                     : disabled
Configured Management Ipv4 Address  : 0.0.0.0
Configured Management Ipv6 Address  : ::
```

Show LLDP Neighbors

Privileged EXEC

Displays LLDP-discovered neighboring devices.

SYNTAX

```
show lldp neighbors
```

PARAMETERS

No parameters.

EXAMPLE

```
qss# show lldp neighbors
```

EXAMPLE OUTPUT

Shows two real neighbor entries.

```
qss# show lldp neighbors

Capability Codes   :
(R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device,
(W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other

Chassis ID           Local Intf    Hold-time   Capability      Port Id
----------           ----------    ---------   ----------      -------
<mac-address>    Ex0/3         3601                        <mac-address>
<mac-address>    Ex0/15        3601                        <mac-address>

Total Entries Displayed : 2
```

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; these commands configure IGMP snooping behavior and show its statistics.

Set IGMP Snooping (Global)

Global configuration

Enables or disables IGMP snooping switch-wide.

SYNTAX

```
ip igmp snooping
no ip igmp snooping
```

PARAMETERS

No parameters.

EXAMPLE

```
qss(config)# ip igmp snooping
```

Set IGMP Snooping (Per VLAN)

Config-VLAN

Enables or disables IGMP snooping on the VLAN.

SYNTAX

```
ip igmp snooping
no ip igmp snooping
```

PARAMETERS

No parameters.

EXAMPLE

```
qss(config-vlan)# ip igmp snooping
```

Set IGMP Snooping Querier

Config-VLAN

Enables the IGMP snooping querier on the VLAN, optionally with a specific source address.

SYNTAX

```
ip igmp snooping querier [{ address | <ucast_addr> }]
no ip igmp snooping querier
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
address	address	Uses the VLAN interface's own IP address as the querier source (the default when no address is given).	—
ucast_addr	IPv4 address	Specific source IPv4 address to use for the IGMP snooping querier, instead of the switch's own address.	—

EXAMPLE

```
qss(config-vlan)# ip igmp snooping querier
```

Set IGMP Snooping Fast Leave

Config-VLAN

Enables or disables IGMP fast-leave processing on the VLAN.

SYNTAX

```
ip igmp snooping fast-leave
no ip igmp snooping fast-leave
```

PARAMETERS

No parameters.

EXAMPLE

```
qss(config-vlan)# ip igmp snooping fast-leave
```

Set IGMP Snooping Static Router Port

Config-VLAN

Adds or removes a static multicast router port on the VLAN.

SYNTAX

```
ip igmp snooping mrouter <interface-type> <0/a-b, 0/c, ...>
no ip igmp snooping mrouter <interface-type> <0/a-b, 0/c, ...>
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
interface-type	varies by model	Interface type keyword, e.g. gigabitethernet or extreme-ethernet (see note below).	—
0/a-b, 0/c, ...	0/a-b, 0/c, ...	One or more interface IDs (or ranges), comma-separated, e.g. 0/1-4,0/6.	—

EXAMPLE

```
qss(config-vlan)# ip igmp snooping mrouter gigabitethernet 0/1
```

NOTES

- The interface type keyword depends on the switch model and port type — for example "gigabitethernet" or "extreme-ethernet" (abbreviation "ex"); "port-channel <n>" addresses a link-aggregation group. Type "?" after the command to list the interface types available on your switch.

Show IGMP Snooping Globals

Privileged EXEC

Displays the global IGMP snooping configuration.

SYNTAX

```
show ip igmp snooping globals
```

PARAMETERS

No parameters.

EXAMPLE

```
qss# show ip igmp snooping globals
```

EXAMPLE OUTPUT

```
qss# show ip igmp snooping globals

Snooping Configuration
----------------------------
IGMP Snooping globally disabled
IGMP Snooping is operationally disabled
IGMP Snooping Enhanced mode is disabled
IGMP Snooping Sparse mode is disabled
Transmit Query on Topology Change  globally disabled
Multicast forwarding mode is MAC based
Proxy globally disabled
Proxy reporting globally disabled
Filter is disabled
Router port purge interval is 255 seconds
Port purge interval is 260 seconds
Report forward interval is 1 seconds
Group specific query interval is 2 seconds
Reports are forwarded on router ports
Queries are forwarded on all ports
Group specific query retry count is 2
Multicast VLAN disabled
Leave config level is Vlan based
Report processing config level is on non-router ports

Control Plane Driven for report message is disabled
```

Show IGMP Snooping

Privileged EXEC

Displays IGMP snooping status, optionally filtered to one VLAN.

SYNTAX

```
show ip igmp snooping [vlan <vlan-id (1-4094)>]
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
`vlan-id`	`1-4094`	ID of the VLAN this command applies to.	—

EXAMPLE

```
qss# show ip igmp snooping vlan 1
```

EXAMPLE OUTPUT

```
qss# show ip igmp snooping vlan 1

Snooping VLAN Configuration for the VLAN 1
  IGMP Snooping disabled
  IGMP configured version is V2
  Fast leave is disabled
  Snooping switch is configured as Non-Querier
  Snooping switch is acting as Non-Querier
  Elected Querier is 0.0.0.0
  Startup Query Count is 2
  Startup Query Interval is 31 seconds
  Query interval is 125 seconds
  Other Querier Present Interval is 255 seconds
  Port Purge Interval is 260 seconds
  Max Response Code is 100, Time is 10.00 seconds
  Robustness variable is 2
```

Set IGMP Snooping Sparse Mode

Global configuration

Enables or disables blocking of unregistered multicast traffic flooding (sparse mode).

SYNTAX

```
ip igmp snooping sparse-mode { enable | disable }
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
sparse-mode	enable | disable	Enables or disables blocking unregistered multicast traffic (sparse mode).	disable

EXAMPLE

```
qss(config)# ip igmp snooping sparse-mode disable
```

Show IGMP Snooping Groups

Privileged EXEC

Displays learned or static IGMP multicast groups.

SYNTAX

```
show ip igmp snooping groups [{ [[vlan <vlan-id (1-4094)> [group <mcast_addr>]] [{ static | dynamic }] [switch <switch-name (32)>]] | [summary] }]
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
vlan-id	1-4094	Limits the display to this one VLAN (optional; shows all VLANs when omitted).	—
mcast_addr	IPv4 multicast address	Limits the display to this one multicast group address (optional).	—
entry-type	static | dynamic	Limits the display to only statically configured groups, or only dynamically learned ones (optional).	—
switch	up to 32 characters	Switch stack member name (single-switch systems can omit this).	—
summary	summary	Shows a per-VLAN group-count summary instead of the full group list (optional).	—

EXAMPLE

```
qss# show ip igmp snooping groups
```

EXAMPLE OUTPUT

Output from a switch with no IGMP snooping groups learned.

```
qss# show ip igmp snooping groups

Total Num of Group Addresses [0]
```

MAC address table

The MAC address table, also known as the Content Addressable Memory (CAM) table or forwarding database, is a critical component of Layer 2 switching that maps MAC addresses to physical interfaces. The switch uses this table to make forwarding decisions, directing frames to the appropriate egress port based on the destination MAC address. These commands manage the table's dynamic and static (manually added) entries.

Show MAC Address Table

Privileged EXEC

Displays learned and static MAC address table entries.

SYNTAX

```
show mac-address-table [vlan <vlan-range>] [address <aa:aa:aa:aa:aa:aa>] [{ interface <interface-type> <interface-id> | switch <context_name> }]
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
vlan-range	e.g. 10 or 10-20	A VLAN ID, or a range of VLAN IDs.	—
aa:aa:aa:aa:aa:aa	aa:aa:aa:aa:aa:aa	Limits the display to this one MAC address (optional; shows all when omitted).	—
interface-type	varies by model	Interface type keyword, e.g. gigabitethernet or extreme-ethernet (see note below).	—
interface-id	slot/port	Port number in slot/port form, e.g. 0/1.	—
context_name	switch name	Switch stack member name (single-switch systems can omit this).	—

EXAMPLE

```
qss# show mac-address-table
```

EXAMPLE OUTPUT

Shows a dynamically learned ("Learnt") entry alongside the static CPU entries.

```
qss# show mac-address-table

Vlan    Mac Address         Type     ConnectionId       Ports
----    -----------         ----     ------------       -----
1       <mac-address>   Static                      CPU
1       <mac-address>   Learnt                      Ex0/15
1       <mac-address>   Learnt                      Ex0/3

Total Mac Addresses displayed: 3
```

NOTES

- The interface type keyword depends on the switch model and port type — for example "gigabitethernet" or "extreme-ethernet" (abbreviation "ex"); "port-channel <n>" addresses a link-aggregation group. Type "?" after the command to list the interface types available on your switch.

Show MAC Address Table Aging Time

Privileged EXEC

Displays the MAC address table aging time.

SYNTAX

```
show mac-address-table aging-time
```

PARAMETERS

No parameters.

EXAMPLE

```
qss# show mac-address-table aging-time
```

EXAMPLE OUTPUT

```
qss# show mac-address-table aging-time

Mac Address Aging Time: 300
```

Clear MAC Address Table

Global configuration

Clears all dynamically learned MAC address table entries.

SYNTAX

```
clear mac-address-table dynamic
```

PARAMETERS

No parameters.

EXAMPLE

```
qss(config)# clear mac-address-table dynamic
```

Set MAC Address Table Aging Time

Global configuration

Sets how long a dynamically learned MAC address entry is kept before aging out.

SYNTAX

```
mac-address-table aging-time <seconds (10-400)>
no mac-address-table aging-time
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
seconds	10-400	How long a dynamically learned entry is kept before aging out.	300

EXAMPLE

```
qss(config)# mac-address-table aging-time 200
```

Set Static MAC Address Table Entry

Global configuration

Adds or removes a static MAC address table entry.

SYNTAX

```
mac-address-table static unicast <aa:aa:aa:aa:aa:aa> vlan <vlan-id (1-4094)> [interface { <interface-type> <interface-id> | port-channel <a,b,c-d> }]
no mac-address-table static unicast <aa:aa:aa:aa:aa:aa> vlan <vlan-id (1-4094)>
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
aa:aa:aa:aa:aa:aa	MAC address	MAC address of the static entry to add or remove.	—
vlan-id	1-4094	VLAN containing the static MAC entry.	—
interface-type	one interface type and ID	One physical interface target for the static MAC entry.	—
interface-id	one interface ID	Single physical interface target.	—
port-channel	one port-channel	Single link-aggregation group target.	—
a,b,c-d	port-channel group number	Port-channel group number.	—

EXAMPLE

```
qss(config)# mac-address-table static unicast 00:11:22:33:22:11 vlan 1 interface gigabitethernet 0/1
```

NOTES

- The interface type keyword depends on the switch model and port type — for example "gigabitethernet" or "extreme-ethernet" (abbreviation "ex"); "port-channel <n>" addresses a link-aggregation group. Type "?" after the command to list the interface types available on your switch.

PTP (transparent clock / boundary clock)

Configuring Precision Time Protocol (PTP) transparent clock (TC) and boundary clock settings on a QSW managed switch enhances time synchronization by accounting for the transit time of PTP messages, improving precision across networked devices. PTP boundary clock is available only on QSW-M7230-2X4F24T and QSW-M7230P-2X4F24T; both models support it. This is important for environments needing accurate timing, such as data centers and industrial systems, since it reduces latency and network delay while maintaining compliance with PTP standards like IEEE 1588.

Set PTP Transparent Clock

Global configuration

Enables or disables PTP transparent clock (TC) mode switch-wide.

SYNTAX

```
ptp tc enable
no ptp tc enable
```

PARAMETERS

No parameters.

EXAMPLE

```
qss(config)# ptp tc enable
```

Set PTP TC Domain Number

Global configuration

Sets the PTP transparent clock domain number.

SYNTAX

```
ptp tc domain-number <domain-number (0-127)>
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
`domain-number`	`0-127`	PTP domain number — must match the domain used by other clocks on the same PTP network.	`0`

EXAMPLE

```
qss(config)# ptp tc domain-number 0
```

Set PTP Transparent Clock (Port)

Interface configuration

Enables or disables PTP transparent clock on the interface.

SYNTAX

```
ptp tc
no ptp tc
```

PARAMETERS

No parameters.

EXAMPLE

```
qss(config-if)# ptp tc
```

Show PTP Transparent Clock Summary

Privileged EXEC

Displays a summary of PTP transparent clock status.

SYNTAX

```
show ptp tc summary
```

PARAMETERS

No parameters.

EXAMPLE

```
qss# show ptp tc summary
```

EXAMPLE OUTPUT

```
qss# show ptp tc summary

PTP Transparent Clock (TC) Status
=================================
Transparent clock: Disable
clock domain     : 0
 Port 1    : Disable
 Port 2    : Disable
 Port 3    : Disable
 Port 4    : Disable
 Port 5    : Disable
 Port 6    : Disable
 Port 7    : Disable
 Port 8    : Disable
 Port 9    : Disable
 Port 10   : Disable
 Port 11   : Disable
 Port 12   : Disable
 Port 13   : Disable
 Port 14   : Disable
 Port 15   : Disable
 Port 16   : Disable
 Port 17   : Disable
 Port 18   : Disable
 Port 19   : Disable
...
```

Set PTP Boundary Clock Domain/Protocol/Step

Global configuration

Sets the PTP boundary clock's domain number, transport protocol, and one-step or two-step timestamping. Available only on QSW-M7230-2X4F24T and QSW-M7230P-2X4F24T.

SYNTAX

```
ptp bc domain-number <domain-number (0-127)> protocol { L2 | UDPv4 } sfp-step { twostep | onestep }
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
domain-number	0-127	PTP domain number.	0
protocol	L2 | UDPv4	Transport protocol used to carry PTP messages.	UDPv4
sfp-step	twostep | onestep	One-step or two-step timestamping.	twostep

EXAMPLE

```
qss(config)# ptp bc domain-number 0 protocol udpv4 sfp-step twostep
```

Enable PTP Boundary Clock

Global configuration

Enables or disables PTP boundary clock (BC) mode switch-wide. Available only on QSW-M7230-2X4F24T and QSW-M7230P-2X4F24T.

SYNTAX

```
ptp bc enable
no ptp bc enable
```

PARAMETERS

No parameters.

EXAMPLE

```
qss(config)# ptp bc enable
```

NOTES

- Before enabling the boundary clock, add 2–6 ports to it with "ptp bc vlan <vlan-id (1-4094)>".
- PTP transparent clock (TC) and boundary clock (BC) are mutually exclusive — run "no ptp tc enable" first.

Set PTP Boundary Clock (Port)

Interface configuration

Adds the port to the PTP boundary clock on the given VLAN, with optional message-interval and DSCP settings. Available only on QSW-M7230-2X4F24T and QSW-M7230P-2X4F24T.

SYNTAX

```
ptp bc vlan <vlan-id (1-4094)> [announce interval <announce-interval (-4..1)>] [delay-req interval
<delay-req-interval (-4..1)>] [sync interval <sync-interval (-4..1)>] [dscp <dscp (0..63)>]
no ptp bc
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
`vlan-id`	`1-4094`	VLAN this per-port PTP Boundary Clock setting applies to.	—
`announce-interval`	`-4 to 1`	Log2 interval between PTP Announce messages, in seconds (e.g. 0 = 1 s, 1 = 2 s, -1 = 0.5 s) (optional).	`1`
`delay-req-interval`	`-4 to 1`	Log2 interval between PTP Delay_Req messages, in seconds (optional).	`0`
`sync-interval`	`-4 to 1`	Log2 interval between PTP Sync messages, in seconds (optional).	`0`
`dscp`	`0-63`	DSCP value used for PTP messages sent on this port (optional).	`0`

EXAMPLE

```
qss(config-if)# ptp bc vlan 1 announce interval -3 delay-req interval -3 sync interval -2 dscp 6
```

NOTES

- Defaults when omitted: announce interval 1, delay-req interval 0, sync interval 0, dscp 0.

Show PTP Boundary Clock Summary

Privileged EXEC

Displays a summary of PTP boundary clock status. Available only on QSW-M7230-2X4F24T and QSW-M7230P-2X4F24T.

SYNTAX

```
show ptp bc summary
```

PARAMETERS

No parameters.

EXAMPLE

```
qss# show ptp bc summary
```

EXAMPLE OUTPUT

```
qss# show ptp bc summary

PTP Boundary Clock Status
=========================
Global Configuration:
  BC Feature:          Disabled
  Domain ID:           0
  Protocol:            UDPv4

SFP Clock Status:
  Clock Identity:      <mac-address>
  Step Mode:           Two-step
  Status:              Disabled

RJ45 Clock Status:
  Clock Identity:      <mac-address>
  Step Mode:           Two-step
  Status:              Disabled

Interfaces Status:
--------------------------------------------------------------------------------
Port  Type Status          VLAN  DSCP  Annu  Sync  DelayReq
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
* Note: Annu/Sync/DelayReq values are logarithms to base 2 (e.g., 0=1s, 1=2s, -1=0.5s).
```

5. Layer 3 (L3) Commands

This chapter describes the commands used to configure and manage Layer 3 features on the switch, including multi-chassis link aggregation (MC-LAG) and quality of service (QoS). These commands support essential routing functions that enable communication between different VLANs and IP subnets. You can configure and manage static routes, DHCP services, and neighbor-discovery state, monitor Layer 3 forwarding information, pair the switch with an MC-LAG peer, and classify and prioritize traffic with QoS.

Static routing, DHCP server, DHCP relay, ARP, IPv6 neighbors, and MC-LAG are available on QSS Pro only; QoS applies to both QSS and QSS Pro.

IN THIS CHAPTER

IN THIS CHAPTER (CONTINUED)

Static routing (IPv4/IPv6)

These commands configure and manage IPv4 and IPv6 routing on the switch. They enable the switch to forward traffic between different IP subnets and VLANs by defining static routes and viewing routing tables, supporting flexible deployment in dual-stack or transition environments.

Set Static Route

Global configuration | QSS Pro only

Adds an IPv4 static route, or a default route (0.0.0.0/0).

SYNTAX

```
ip route <prefix> <mask> <next-hop>
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
prefix	IPv4 address	Destination network address for the static route.	—
mask	IPv4 subnet mask	Subnet mask, e.g. 255.255.255.0.	—
next-hop	IPv4 address	Next-hop IPv4 address.	—

EXAMPLE

```
qss(config)# ip route 2.2.2.0 255.255.255.0 10.1.1.2
qss(config)# ip route 0.0.0.0 0.0.0.0 192.168.1.2
```

Show IP Route

Privileged EXEC | QSS Pro only

Displays the IPv4 routing table.

SYNTAX

```
show ip route
```

PARAMETERS

No parameters.

EXAMPLE

```
qss# show ip route
```

EXAMPLE OUTPUT

```
qss# show ip route

  UI IPv4 Routing Table
  IP-Address      PrefixLen       Gateway         InterfaceType   Protocol
  ================================================================
  <network>       255.255.0.0     0.0.0.0         Connected       vlan 1
```

Set IPv6 Static Route

Global configuration | QSS Pro only

Adds an IPv6 static route on a VLAN interface.

SYNTAX

```
ipv6 route <prefix> <prefix-len (0-128)> <next-hop> vlan <vlan-id (1-4094)>
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
prefix	IPv6 address	Destination network address for the static route.	—
prefix-len	0-128	IPv6 prefix length, in bits.	—
next-hop	IPv6 address	Next-hop IPv6 address.	—
vlan-id	1-4094	ID of the VLAN this command applies to.	—

EXAMPLE

```
qss(config)# ipv6 route 9999::1111 64 3333::1100 vlan 1
```

Show IPv6 Route

Privileged EXEC | QSS Pro only

Displays the IPv6 routing table.

SYNTAX

```
show ipv6 route
```

PARAMETERS

No parameters.

EXAMPLE

```
qss# show ipv6 route
```

EXAMPLE OUTPUT

Output from a switch with no IPv6 routes configured.

```
qss# show ipv6 route


* No Route entries in the table
```

DHCP server

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.

Set DHCP Server

Global configuration QSS Pro only

Enables or disables the DHCP server.

SYNTAX

```
service dhcp-server
no service dhcp-server
```

PARAMETERS

No parameters.

EXAMPLE

```
qss(config)# service dhcp-server
```

Set DHCP Server Pool

Global configuration QSS Pro only

Creates or deletes a DHCP server address pool.

SYNTAX

```
dhcp pool <pool-index (1-2147483647)>
no dhcp pool <pool-index>
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
pool-index	1-2147483647	DHCP pool index — identifies this address pool (not a VLAN ID or subnet).	—

EXAMPLE

```
qss(config)# dhcp pool 1
```

NOTES

- Entering this command switches to DHCP pool configuration mode (qss(dhcp-config)#).

Set DHCP Pool Network

DHCP pool configuration QSS Pro only

Sets the address range and mask served by the DHCP pool.

SYNTAX

```
network <start-ip> { <mask> | /<prefix-length (1-31)> } <end-ip>
no network
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
start-ip	IPv4 address	Start of the address range.	—
mask	IPv4 subnet mask	Subnet mask, e.g. 255.255.255.0.	—
prefix-length	1-31	Subnet prefix length, in bits.	—
end-ip	IPv4 address	End of the address range.	—

EXAMPLE

```
qss(dhcp-config)# network 12.0.0.0 255.0.0.0 12.0.0.100
```

Set DHCP Pool Default Router

DHCP pool configuration | QSS Pro only

Sets the default router (gateway) address handed out by the DHCP pool.

SYNTAX

```
default-router <ip-address>
no default-router
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
ip-address	IPv4 address	Default gateway IPv4 address to hand out to DHCP clients.	—

EXAMPLE

```
qss(dhcp-config)# default-router 10.23.2.99
```

Set DHCP Pool Lease Time

DHCP pool configuration | QSS Pro only

Sets how long a leased address from the DHCP pool remains valid.

SYNTAX

```
lease { days <days (0-30)> [hours <hours (0-23)> [minutes <minutes (1-59)>]] | infinite }
no lease
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
lease	days <days> [hours <hours> [minutes <minutes>]] | infinite	How long a leased address stays valid — a specific duration (days/hours/minutes below), or never expiring.	—
days	0-30	Lease duration, days component.	—
hours	0-23	Lease duration, hours component.	—
minutes	1-59	Lease duration, minutes component.	—

EXAMPLE

```
qss(dhcp-config)# lease days 1 hours 1 minutes 1
```

NOTES

- If days = 0, hours and minutes cannot both be 0.
- Maximum 32 DHCP server pools.

Set DHCP Pool DNS Servers

DHCP pool configuration | QSS Pro only

Sets up to two DNS server addresses handed out by the DHCP pool.

SYNTAX

```
dns-server <ip-address> [<ip-address>]
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
ip-address	IPv4 address	DNS server IPv4 address to hand out to DHCP clients.	—

EXAMPLE

```
qss(dhcp-config)# dns-server 1.1.1.1
```

Show DHCP Server Pools

Privileged EXEC | QSS Pro only

Displays configured DHCP server pools.

SYNTAX

```
show dhcp server pools
```

PARAMETERS

No parameters.

EXAMPLE

```
qss# show dhcp server pools
```

EXAMPLE OUTPUT

Prints nothing when there are no entries.

```
qss# show dhcp server pools
```

Show DHCP Server Binding

Privileged EXEC | QSS Pro only

Displays DHCP server address-lease bindings.

SYNTAX

```
show dhcp server binding
```

PARAMETERS

No parameters.

EXAMPLE

```
qss# show dhcp server binding
```

EXAMPLE OUTPUT

Prints nothing when there are no entries.

```
qss# show dhcp server binding
```

DHCP relay

DHCP relay forwards DHCP requests from clients to a DHCP server on a different subnet, so a single centralized server can serve multiple VLANs. These commands enable the relay agent globally and per VLAN, configure up to eight relay servers per VLAN, and manage DHCP Option 82 (relay agent information) insertion, format, and forwarding policy at both the global and per-VLAN level. Several of these commands accept an optional [vrf <vrf-name>], which selects the routing context (VRF) the command applies to. This firmware has a single context, named `default`: the option can be omitted (the command then applies to the default context), or set explicitly with `vrf default` — the only value accepted.

Before you begin

- Enable DHCP snooping globally (`ip dhcp snooping`). **REQUIRED**
- Enable DHCP snooping on the VLAN you plan to relay on (`ip dhcp snooping vlan <N>`). **REQUIRED**
- Make sure the DHCP server is disabled (`no service dhcp-server`) — relay cannot be enabled while it is active. **REQUIRED**
- Create the VLAN interface you'll relay on (`interface vlan <vlan-id (1-4094)>`). **TYPICAL ORDER**

CONFIGURATION ORDER

1. Enable DHCP snooping globally.

```
qss(config)# ip dhcp snooping
```

2. Enable DHCP snooping on the VLAN.

```
qss(config)# ip dhcp snooping vlan 10
```

3. Enable the DHCP relay agent globally.

```
qss(config)# service dhcp-relay
```

4. Enter the VLAN interface and enable relay on it.

```
qss(config)# interface vlan 10
qss(config-if)# ip dhcp relay enable
```

5. Add at least one DHCP server address for the VLAN (up to 8 per VLAN).

```
qss(config-if)# ip dhcp relay server 10.0.0.100
```

6. (Optional) Enable Option 82 and set the circuit-id format.

```
qss(config)# ip dhcp relay information option
qss(config)# ip dhcp relay circuit-id format vlan-port
```

Show DHCP Relay Information

Privileged EXEC **QSS Pro only**

Displays the DHCP relay configuration and status, globally and per VLAN — including whether each VLAN inherits the global Option 82 policy or overrides it, and a routing-pending status indicator.

SYNTAX

```
show ip dhcp relay information [vrf <vrf-name>] [vlan <vlan-id>] [<interface-type> <interface-id>]
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
`vrf-name`	`default`	Name of the routing context. This firmware has a single context named "default"; omit the option or specify "default".	—
`vlan-id`	`1-4094`	ID of the VLAN this command applies to.	—
`interface-type`	`varies by model`	Interface type keyword, e.g. gigabitethernet or extreme-ethernet (see note below).	—
`interface-id`	`slot/port`	Port number in slot/port form, e.g. 0/1.	—

EXAMPLE

```
qss# show ip dhcp relay information
```

EXAMPLE OUTPUT

Output from a switch with DHCP relay disabled and no per-VLAN relay configured.

```
qss# show ip dhcp relay information

Context Name : default
------------

Dhcp Relay                  : Disabled
Dhcp Relay Servers only     : Disabled

DHCP server                 : 0.0.0.0

Dhcp Relay RAI option       : Disabled
Option-82 Policy            : replace
Global Circuit-Id Format    : vlan-port
Global Remote-Id Format     : mac
Default Circuit Id information : router-index
Debug Level                 : 0x0

No of Packets inserted RAI option               : 0
No of Packets inserted circuit ID suboption     : 0
No of Packets inserted remote ID suboption      : 0
No of Packets inserted subnet mask suboption    : 0
No of Packets inserted Vendor Specific suboption    : 0
No of Packets dropped                           : 0
No of Packets which did not inserted RAI option : 0

Total Relay Agents in default : 0

Dhcp Vendor-specific option          : Disbled

Default Vendor-Specific Action       :   Drop

Per-VLAN DHCP Relay Configuration
---------------------------------
VLAN   Admin     Override  Policy    CktIdFmt    RemIdFmt      Routing-Pend  (inherited=global)
(no per-VLAN relay rows)

Total Relay Agents in the system : 1
```

NOTES

- The interface type keyword depends on the switch model and port type — for example "gigabitethernet" or "extreme-ethernet" (abbreviation "ex"); "port-channel <n>" addresses a link-aggregation group. Type "?" after the command to list the interface types available on your switch.

Clear DHCP Relay Statistics

Privileged EXEC QSS Pro only

Clears the DHCP relay counters.

SYNTAX

```
clear ip dhcp relay statistics [vrf <vrf-name>]
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
vrf-name	default	Name of the routing context. This firmware has a single context named "default"; omit the option or specify "default".	—

EXAMPLE

```
qss# clear ip dhcp relay statistics
```

Enable DHCP Relay

Global configuration QSS Pro only

Enables or disables the DHCP relay agent globally; enabling fails if the DHCP server is already active (disable the DHCP server first).

REQUIRES FIRST
- Enable DHCP snooping globally first.
- Make sure the DHCP server is disabled — relay cannot be enabled while it is active.

SYNTAX

```
service dhcp-relay [vrf <vrf-name>]
no service dhcp-relay [vrf <vrf-name>]
```

PREREQUISITES

- Enable DHCP snooping globally first. REQUIRED
- Make sure the DHCP server is disabled — relay cannot be enabled while it is active. REQUIRED

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
vrf-name	default	Name of the routing context. This firmware has a single context named "default"; omit the option or specify "default".	—

EXAMPLE

```
qss(config)# service dhcp-relay
```

Enable DHCP Relay Option 82

Global configuration | QSS Pro only

Enables or disables insertion of DHCP Option 82 (relay agent information) into forwarded requests.

SYNTAX

```
ip dhcp relay information option [vrf <vrf-name>]
no ip dhcp relay information option [vrf <vrf-name>]
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
vrf-name	default	Name of the routing context. This firmware has a single context named "default"; omit the option or specify "default".	—

EXAMPLE

```
qss(config)# ip dhcp relay information option
```

NOTES

- After enabling Option 82 the CLI warns that the circuit ID must be set explicitly — use "ip dhcp relay circuit-id format" (global or per-VLAN).

Set DHCP Relay Option 82 Policy

Global configuration | QSS Pro only

Sets the global forwarding policy for packets that already carry Option 82: keep, drop, or replace.

SYNTAX

```
ip dhcp relay information policy { keep | drop | replace }
no ip dhcp relay information policy
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
policy	keep | drop | replace	What to do with a packet that already carries Option 82: keep it, drop it, or replace it.	—

EXAMPLE

```
qss(config)# ip dhcp relay information policy replace
```

NOTES

- The `no` form (`no ip dhcp relay information policy`) resets the global Option 82 policy to its default.

Set DHCP Relay Circuit ID Format

Global configuration | QSS Pro only

Sets the global Circuit ID format used in Option 82: VLAN/port, or a custom literal string.

SYNTAX

```
ip dhcp relay circuit-id format { vlan-port | custom <custom-string (64)> }
no ip dhcp relay circuit-id format
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
format	vlan-port | custom <custom-string (64)>	Circuit ID format: the VLAN and port the request arrived on, or a custom literal string below.	—
custom	up to 64 characters	A literal string used as-is (no variable/token substitution) — only used when circuit-id-format is custom.	—

EXAMPLE

```
qss(config)# ip dhcp relay circuit-id format vlan-port
```

NOTES

- Free-form literal string used as-is (no variable/token substitution); maximum 64 characters. Longer strings are rejected.
- The `no` form (`no ip dhcp relay circuit-id format`) resets the global Circuit ID format to its default.

Set DHCP Relay Remote ID Format

Global configuration | QSS Pro only

Sets the global Remote ID format used in Option 82: MAC address, or a custom literal string.

SYNTAX

```
ip dhcp relay remote-id format { mac | custom <custom-string (64)> }
no ip dhcp relay remote-id format
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
format	mac | custom <custom-string (64)>	Remote ID format: the switch's own MAC address, or a custom literal string below.	—
custom	up to 64 characters	A literal string used as-is (no variable/token substitution) — only used when remote-id-format is custom.	—

EXAMPLE

```
qss(config)# ip dhcp relay remote-id format mac
```

NOTES

- Free-form literal string used as-is (no variable/token substitution); maximum 64 characters. Longer strings are rejected.
- The `no` form (`no ip dhcp relay remote-id format`) resets the global Remote ID format to its default.

Enable DHCP Relay (VLAN)

Interface configuration | QSS Pro only

Enables DHCP relay on this VLAN interface, creating the relay rule.

REQUIRES FIRST • Enable DHCP snooping on this same VLAN first.

SYNTAX

```
ip dhcp relay enable
no ip dhcp relay enable
```

PREREQUISITES

- Enable DHCP snooping on this same VLAN first. REQUIRED
- Create the VLAN interface first — this command runs in that interface's configuration mode. TYPICAL ORDER

PARAMETERS

No parameters.

EXAMPLE

```
qss(config-if)# ip dhcp relay enable
```

NOTES

- Creates the entire relay rule for this VLAN; the no form deletes the entire rule (servers/policy/option-82 settings are all removed).
- Difference from admin-status: enable/no enable controls the existence of the rule (create/remove), while admin-status only turns an existing rule on/off with configuration retained.
- The global service dhcp-relay switch takes precedence over both (global OFF stops all relay forwarding; per-VLAN settings are retained).

Set DHCP Relay Admin Status (VLAN)

Interface configuration | QSS Pro only

Turns an already-created relay rule on this VLAN on or off without deleting it.

REQUIRES FIRST • Use `ip dhcp relay enable` first to create the relay rule — this command only toggles an existing one.

SYNTAX

```
ip dhcp relay admin-status { enable | disable }
no ip dhcp relay admin-status
```

PREREQUISITES

- Use `ip dhcp relay enable` first to create the relay rule — this command only toggles an existing one.

  REQUIRED

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
admin-status	enable | disable	Turns the already-created per-VLAN relay rule on or off.	enable

EXAMPLE

```
qss(config-if)# ip dhcp relay admin-status enable
```

NOTES

- Does not create or delete the relay rule; only enables/disables an already-created rule.
- When disabled, the configuration is retained and relay forwarding stops on this VLAN only.
- Use ip dhcp relay enable first to create the relay rule.
- The `no` form (`no ip dhcp relay admin-status`) resets the per-VLAN admin status to its default (enabled).

Set DHCP Relay Server (VLAN)

Interface configuration | QSS Pro only

Adds a DHCP server address for this VLAN (up to 8 servers per VLAN).

SYNTAX

```
ip dhcp relay server <ucast_addr>
no ip dhcp relay server <ucast_addr>
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
ucast_addr	IPv4 address	DHCP server IPv4 address to add for this VLAN.	—

EXAMPLE

```
qss(config-if)# ip dhcp relay server 10.0.0.100
```

NOTES

- The `no` form (`no ip dhcp relay server <ucast_addr>`) removes a previously added server address; repeat with each address to remove more than one.

Set DHCP Relay Source Address (VLAN)

Interface configuration | QSS Pro only

Selects whether the relay's source (giaddr) address comes from the egress interface or the relay's own giaddr value.

SYNTAX

```
ip dhcp relay source-address { egress-interface | giaddr }
no ip dhcp relay source-address
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
source-address	egress-interface | giaddr	Where the relay's source (giaddr) address comes from: the egress interface's own address, or the relay's configured giaddr value.	—

EXAMPLE

```
qss(config-if)# ip dhcp relay source-address egress-interface
```

NOTES

- The `no` form (`no ip dhcp relay source-address`) resets the per-VLAN source-address selection to its default.

Set DHCP Relay Option 82 Override (VLAN)

Interface configuration | QSS Pro only

Overrides the global Option 82 policy with a per-VLAN setting.

SYNTAX

```
ip dhcp relay information override
no ip dhcp relay information override
```

PARAMETERS

No parameters.

EXAMPLE

```
qss(config-if)# ip dhcp relay information override
```

NOTES

- The `no` form (`no ip dhcp relay information override`) disables the per-VLAN override, so the VLAN reverts to inheriting the global Option 82 policy.

Set DHCP Relay Option 82 Policy (VLAN)

Interface configuration | QSS Pro only

Sets the per-VLAN Option 82 forwarding policy.

SYNTAX

```
ip dhcp relay information policy { keep | drop | replace }
no ip dhcp relay information policy
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
`policy`	`keep | drop | replace`	What to do with a packet that already carries Option 82, for this VLAN only.	—

EXAMPLE

```
qss(config-if)# ip dhcp relay information policy keep
```

NOTES

- The `no` form (`no ip dhcp relay information policy`) resets the per-VLAN Option 82 policy so the VLAN inherits the global policy.

Set DHCP Relay Circuit ID Format (VLAN)

Interface configuration | QSS Pro only

Sets the per-VLAN Circuit ID format: VLAN/port, or a custom literal string.

SYNTAX

```
ip dhcp relay circuit-id format { vlan-port | custom <custom-string (64)> }
no ip dhcp relay circuit-id format
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
`format`	`vlan-port | custom <custom-string (64)>`	Circuit ID format: the VLAN and port the request arrived on, or a custom literal string below.	—
`custom`	`up to 64 characters`	A literal string used as-is (no variable/token substitution) — only used when circuit-id-format is custom.	—

EXAMPLE

```
qss(config-if)# ip dhcp relay circuit-id format custom site-A-vlan10
```

NOTES

- The `no` form (`no ip dhcp relay circuit-id format`) resets the per-VLAN Circuit ID format so the VLAN inherits the global format.

Set DHCP Relay Remote ID Format (VLAN)

Interface configuration | QSS Pro only

Sets the per-VLAN Remote ID format: MAC address, or a custom literal string.

SYNTAX

```
ip dhcp relay remote-id format { mac | custom <custom-string (64)> }
no ip dhcp relay remote-id format
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
format	mac | custom <custom-string (64)>	Remote ID format: the switch's own MAC address, or a custom literal string below.	—
custom	up to 64 characters	A literal string used as-is (no variable/token substitution) — only used when remote-id-format is custom.	—

EXAMPLE

```
qss(config-if)# ip dhcp relay remote-id format custom Floor3-Edge
```

NOTES

- The `no` form (`no ip dhcp relay remote-id format`) resets the per-VLAN Remote ID format so the VLAN inherits the global format.

Show DHCP Relay Statistics

Privileged EXEC | QSS Pro only

Displays six DHCP relay counters: Requests Relayed, Replies Relayed, Relay Dropped, MTU Dropped, Option 82 Inserted, and Option 82 Stripped.

SYNTAX

```
show ip dhcp relay statistics
```

PARAMETERS

No parameters.

EXAMPLE

```
qss# show ip dhcp relay statistics
```

EXAMPLE OUTPUT

```
qss# show ip dhcp relay statistics

DHCP Relay Per-VLAN Statistics
--------------------------------
VLAN     Requests   Replies    RelayDrop    MtuDrop      Opt82-Ins    Opt82-Str
(no per-VLAN relay rows)
```

FIELD	MEANING
`VLAN`	VLAN the row's counters apply to.
`Requests`	DHCP client requests the relay agent forwarded to a server.
`Replies`	DHCP server replies the relay agent forwarded back to clients.
`RelayDrop`	Packets the relay agent discarded outright.
`MtuDrop`	Packets discarded because they exceeded the relay interface's MTU.
`Opt82-Ins`	Packets to which relay agent information (Option 82) was added.
`Opt82-Str`	Packets from which Option 82 was removed before forwarding.

NOTES

- Takes no optional parameters.

ARP

The Address Resolution Protocol (ARP) maps IP addresses to MAC addresses, enabling communication between devices on the same network segment. A static ARP entry is a manually configured link between an IP address and a MAC address, helping prevent ARP spoofing and address conflicts. These commands configure static ARP entries, set the aging timer that removes dynamic entries with no recent traffic, and view the ARP table.

Show ARP Table

Privileged EXEC | QSS Pro only

Displays the ARP table.

SYNTAX

```
show ip arp table
```

PARAMETERS

No parameters.

EXAMPLE

```
qss# show ip arp table
```

EXAMPLE OUTPUT

Prints nothing when there are no entries.

```
qss# show ip arp table
```

Show ARP Settings

Privileged EXEC QSS Pro only

Displays ARP retry and timeout settings.

SYNTAX

```
show ip arp information
```

PARAMETERS

No parameters.

EXAMPLE

```
qss# show ip arp information
```

EXAMPLE OUTPUT

```
qss# show ip arp information

ARP Configurations:
-------------------
VRF Name:  default

 Maximum number of ARP request retries is 3
 ARP cache timeout is 14400 seconds
```

Clear ARP Table

Global configuration QSS Pro only

Clears all dynamically learned ARP entries.

SYNTAX

```
clear ip arp
```

PARAMETERS

No parameters.

EXAMPLE

```
qss(config)# clear ip arp
```

Set ARP Timeout

Global configuration QSS Pro only

Sets how long a dynamically learned ARP entry is kept before aging out.

SYNTAX

```
arp timeout <seconds (60-86400)>
no arp timeout
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
seconds	60-86400	How long a dynamically learned ARP entry is kept before aging out.	14400

EXAMPLE

```
qss(config)# arp timeout 3600
```

Set Static ARP Entry

Global configuration | QSS Pro only

Adds a static ARP entry mapping an IP address to a MAC address on a VLAN.

SYNTAX

```
arp <ip-address> <hardware-address> vlan <vlan-id (1-4094)>
no arp <ip-address>
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
ip-address	IPv4 address	IPv4 address to map.	—
hardware-address	aa:aa:aa:aa:aa:aa	MAC address to map the IPv4 address to.	—
vlan-id	1-4094	ID of the VLAN this command applies to.	—

EXAMPLE

```
qss(config)# arp 10.0.0.13 24:5E:BE:03:04:05 vlan 1
```

NOTES

- The `no` form (`no arp <ip-address>`) deletes the entry by IP address alone — no MAC address or VLAN needed.

IPv6 neighbors

The Neighbor Discovery Protocol (NDP) is an IPv6 protocol used to determine the link-layer (MAC) address of neighboring devices, discover other network nodes, and maintain connectivity information. NDP replaces ARP in IPv4 networks and enables devices to identify and communicate with directly connected IPv6 neighbors, through both dynamic discovery and manually configured static neighbor entries.

Show IPv6 Neighbors

Privileged EXEC | QSS Pro only

Displays the IPv6 neighbor discovery table.

SYNTAX

```
show ipv6 neighbors
```

PARAMETERS

No parameters.

EXAMPLE

```
qss# show ipv6 neighbors
```

EXAMPLE OUTPUT

Prints nothing when there are no entries.

```
qss# show ipv6 neighbors
```

Clear IPv6 Neighbors

Privileged EXEC | QSS Pro only

Clears the IPv6 neighbor discovery table.

SYNTAX

```
clear ipv6 neighbors
```

PARAMETERS

No parameters.

EXAMPLE

```
qss# clear ipv6 neighbors
```

Set IPv6 Neighbor

Global configuration | QSS Pro only

Adds or removes a static IPv6 neighbor entry mapping a prefix to a MAC address on a VLAN.

SYNTAX

```
ipv6 neighbor <prefix> vlan <vlan-id (1-4094)> <mac-address (xx:xx:xx:xx:xx:xx)>
no ipv6 neighbor <prefix> vlan <vlan-id (1-4094)> <mac-address (xx:xx:xx:xx:xx:xx)>
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
`prefix`	`IPv6 address`	Neighbor's IPv6 address.	—
`vlan-id`	`1-4094`	ID of the VLAN this command applies to.	—
`mac-address`	`aa:aa:aa:aa:aa:aa`	MAC address to map the IPv6 address to.	—

EXAMPLE

```
qss(config)# ipv6 neighbor 3333::1111 vlan 1 24:5E:BE:33:44:55
```

MC-LAG

Multi-chassis link aggregation (MC-LAG) allows two separate switches to appear as a single logical device to connected downstream systems. This configuration provides redundancy and load balancing by distributing traffic across multiple physical links while maintaining link aggregation. If one switch or link fails, traffic automatically switches to the remaining active links without disruption, improving network resiliency and uptime.

These commands configure MC-LAG membership and behavior — pairing the switch with its peer, assigning ports to the MC-LAG, and controlling failover behavior.

Show MC-LAG Peer-Link Info

Privileged EXEC | QSS Pro only

Displays MC-LAG peer-link (ICCL) status.

SYNTAX

```
show mc-lag-peerlink info
```

PARAMETERS

No parameters.

EXAMPLE

```
qss# show mc-lag-peerlink info
```

EXAMPLE OUTPUT

```
qss# show mc-lag-peerlink info

 MC-LAG Instance 0

 ----------------

 Node IP Address        : 0.0.0.0

 Node Subnet mask       : 255.255.0.0

 Peer Node IP Address   : 0.0.0.0

 MC-LAG Peer-link Interface : po4093

 MC-LAG VLAN            : 0

 Node State             : INIT

 Requires system reboot : No

 Socket Conn Status     : NOT CONNECTED

 Peer Firmware Version  : N/A

 MC-LAG Sync            : Disabled
```

Enable MC-LAG (Global)

Global configuration | QSS Pro only

Enables or disables MC-LAG switch-wide.

SYNTAX

```
set mc-lag { enable | disable }
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
mc-lag	enable | disable	Enables or disables MC-LAG switch-wide.	disable

EXAMPLE

```
qss(config)# set mc-lag enable
```

Enable MC-LAG (Port-Channel)

Interface configuration | QSS Pro only

Enables or disables MC-LAG on the port-channel.

SYNTAX

```
set mc-lag { enable | disable }
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
mc-lag	enable | disable	Enables or disables MC-LAG on this port-channel.	disable

EXAMPLE

```
qss(config-if)# set mc-lag enable
```

Reset MC-LAG

Global configuration QSS Pro only

Resets the MC-LAG configuration to its default.

SYNTAX

```
reset mc-lag
```

PARAMETERS

No parameters.

EXAMPLE

```
qss(config)# reset mc-lag
```

Set MC-LAG IP Address

Global configuration QSS Pro only

Sets the IP address, mask, and VLAN for the MC-LAG peer-link (ICCL) interface.

SYNTAX

```
set mc-lag ip address <ip-address> <subnet-mask> vlan <vlan-id (2-4094)>
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
ip-address	IPv4 address	MC-LAG peer-link (ICCL) interface IPv4 address.	—
subnet-mask	IPv4 subnet mask	Subnet mask, e.g. 255.255.255.0.	—
vlan-id	2-4094	VLAN carried over the MC-LAG peer-link (ICCL).	—

EXAMPLE

```
qss(config)# set mc-lag ip address 192.168.10.1 255.255.255.0 vlan 10
```

Set MC-LAG Peer-Link Member Port

Interface configuration QSS Pro only

Adds or removes the interface from the MC-LAG peer-link (ICCL).

SYNTAX

```
mc-lag-peerlink
no mc-lag-peerlink
```

PARAMETERS

No parameters.

EXAMPLE

```
qss(config-if)# mc-lag-peerlink
```

QoS

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 packets by traffic type, source, or destination, and configure traffic policies on switch ports using two QoS classification techniques: Differentiated Services Code Point (DSCP) and class of service (CoS).

Scheduler & trust

These commands control the QoS scheduler globally and per interface: enabling the scheduler, choosing between strict priority (SP) and weighted round robin (WRR), trusting the DSCP value of incoming packets, and setting the default CoS priority for untagged ingress traffic. A summary command shows the scheduler, CoS map, and DSCP map configuration together.

Set QoS Scheduler State

Global configuration

Enables or disables the QoS scheduler.

SYNTAX

```
qos scheduler { disable | enable }
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
scheduler	disable | enable	Enables or disables the QoS scheduler switch-wide.	disable

EXAMPLE

```
qss(config)# qos scheduler enable
```

Set QoS Scheduler Algorithm

Global configuration

Sets the queue scheduling algorithm to strict priority (SP) or weighted round robin (WRR).

SYNTAX

```
qos scheduler sched-algo { sp | wrr }
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
sched-algo	sp | wrr	Queue scheduling algorithm: strict priority (SP) or weighted round robin (WRR).	wrr

EXAMPLE

```
qss(config)# qos scheduler sched-algo wrr
```

Set QoS Trust DSCP

Interface configuration

Enables or disables trusting the DSCP value of incoming packets on the interface.

SYNTAX

```
qos trust dscp
no qos trust dscp
```

PARAMETERS

No parameters.

EXAMPLE

```
qss(config-if)# qos trust dscp
```

Set QoS Default User Priority

Interface configuration

Sets the default CoS priority applied to untagged ingress traffic on the interface.

SYNTAX

```
qos default-user-priority <cos (0-7)>
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
cos	0-7	Default CoS priority applied to untagged ingress traffic on the interface.	0

EXAMPLE

```
qss(config-if)# qos default-user-priority 7
```

Show QoS Scheduler Summary

Privileged EXEC

Displays a summary of the QoS scheduler, CoS map, and DSCP map configuration.

SYNTAX

```
show qos summary
```

PARAMETERS

No parameters.

EXAMPLE

```
qss# show qos summary
```

EXAMPLE OUTPUT

```
qss# show qos summary

QoS Global Configuration
----------------------
Scheduler Profile            : 2 (QoS Disable)
Scheduler algorithm          : weightedRoundRobin

QoS Default Pbit Preference Entries
---------------------------------
IfIndex  Pbit preference over DSCP
-------- ------------------------
Ex0/1    Enabled
Ex0/2    Enabled
Ex0/3    Enabled
Ex0/4    Enabled
Ex0/5    Enabled
Ex0/6    Enabled
Ex0/7    Enabled
Ex0/8    Enabled
Ex0/9    Enabled
Ex0/10   Enabled
Ex0/11   Enabled
Ex0/12   Enabled
Ex0/13   Enabled
Ex0/14   Enabled
...
```

Queue mapping

These commands map CoS priority values and DSCP values to the switch's egress queues, and show the resulting mappings.

Set CoS-to-Queue Map

Global configuration

Maps a CoS priority value to an egress queue.

SYNTAX

```
qos cos-queue-map cos <cos (0-7)> queue <queue (0-7)>
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
cos	0-7	CoS priority value.	—
queue	0-7	Egress queue number.	—

EXAMPLE

```
qss(config)# qos cos-queue-map cos 2 queue 3
```

Set DSCP-to-Queue Map

Global configuration

Maps a DSCP value to an egress queue.

SYNTAX

```
qos dscp-queue-map dscp <dscp (0-63)> queue <queue (0-7)>
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
dscp	0-63	DSCP value used to classify or match traffic.	—
queue	0-7	Egress queue number.	—

EXAMPLE

```
qss(config)# qos dscp-queue-map dscp 56 queue 6
```

Show CoS-to-Queue Map

Privileged EXEC

Displays the CoS-to-queue mapping.

SYNTAX

```
show qos cos-queue-map
```

PARAMETERS

No parameters.

EXAMPLE

```
qss# show qos cos-queue-map
```

EXAMPLE OUTPUT

```
qss# show qos cos-queue-map

QoS CoS-queue-map (Class 10 ~ 17)
---------------------------------
CoS      Mapped Queue
-------- ------------------------
0        1
1        0
2        2
3        3
4        4
5        5
6        6
7        7
```

Show DSCP-to-Queue Map

Privileged EXEC

Displays the DSCP-to-queue mapping.

SYNTAX

```
show qos dscp-queue-map
```

PARAMETERS

No parameters.

EXAMPLE

```
qss# show qos dscp-queue-map
```

EXAMPLE OUTPUT

```
qss# show qos dscp-queue-map

QoS DSCP-queue-map (Class 100 ~ 163)
---------------------------------
DSCP     Mapped Queue
-------- ------------------------
0        0
1        0
2        0
3        0
4        0
5        0
6        0
7        0
8        1
9        1
10       1
11       1
12       1
13       1
14       1
15       1
16       2
17       2
18       2
...
```

Rate limiting

These commands set an interface's maximum ingress and egress rate — further capped by the port's own maximum speed — and show the configured limits for all interfaces.

Set Egress Rate Limit

Interface configuration

Sets the interface's maximum egress rate; the configurable value is further capped by the port's maximum speed.

SYNTAX

```
rate-limit output rate-value <mbps (1-100000)> Mbps
no rate-limit output
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
`mbps`	`1-100000`	Maximum egress rate, in Mbps (further capped by the port's own maximum speed).	`0 (no limit)`

EXAMPLE

```
qss(config-if)# rate-limit output rate-value 5000 Mbps
```

NOTES

- The configurable upper bound is further limited by the port's maximum speed (e.g. a 10G port accepts up to 10000 Mbps); values exceeding the port speed are rejected with "% Rate limit <n> Mbps exceeds the port maximum speed (<m> Mbps)".

Set Ingress Rate Limit

Interface configuration

Sets the interface's maximum ingress rate; the configurable value is further capped by the port's maximum speed.

SYNTAX

```
rate-limit input rate-value <mbps (1-100000)> Mbps
no rate-limit input
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
`mbps`	`1-100000`	Maximum ingress rate, in Mbps (further capped by the port's own maximum speed).	`0` (no limit)

EXAMPLE

```
qss(config-if)# rate-limit input rate-value 5000 Mbps
```

NOTES

- The configurable upper bound is further limited by the port's maximum speed (e.g. a 10G port accepts up to 10000 Mbps); values exceeding the port speed are rejected with "% Rate limit <n> Mbps exceeds the port maximum speed (<m> Mbps)".

Show Interface Rate Limit

Privileged EXEC

Displays the ingress and egress rate limit for all interfaces.

SYNTAX

```
show interface rate-limit
```

PARAMETERS

No parameters.

EXAMPLE

```
qss# show interface rate-limit
```

EXAMPLE OUTPUT

```
qss# show interface rate-limit

Ex0/1
Ingress Rate Limit : Unlimited

Egress Rate Limit  : Unlimited


Ex0/2
Ingress Rate Limit : Unlimited

Egress Rate Limit  : Unlimited


Ex0/3
Ingress Rate Limit : Unlimited

Egress Rate Limit  : Unlimited


Ex0/4
Ingress Rate Limit : Unlimited

Egress Rate Limit  : Unlimited
...
```

Intelligent AV Streaming

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

Set Intelligent AV Streaming

Global configuration

Enables or disables intelligent AV streaming, which prioritizes audio/video traffic for low-latency playback.

SYNTAX

```
qos intelligent-av-streaming
no qos intelligent-av-streaming
```

PARAMETERS

No parameters.

EXAMPLE

```
qss(config)# qos intelligent-av-streaming
```

Show Intelligent AV Streaming

Privileged EXEC

Displays the intelligent AV streaming configuration.

SYNTAX

```
show qos intelligent-av-streaming
```

PARAMETERS

No parameters.

EXAMPLE

```
qss# show qos intelligent-av-streaming
```

EXAMPLE OUTPUT

```
qss# show qos intelligent-av-streaming

Intelligent AV Streaming     : None (2)
```

ECN

Explicit Congestion Notification (ECN) allows you to mark packets instead of dropping them when congestion is detected. By enabling ECN on an interface, you let the device signal congestion early, improving queue stability and reducing packet loss for ECN-capable traffic.

Set ECN

Interface configuration

Enables or disables Explicit Congestion Notification (ECN) on the interface.

SYNTAX

```
qos ecn { disable | enable }
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
ecn	disable | enable	Enables or disables Explicit Congestion Notification on the interface.	disable

EXAMPLE

```
qss(config-if)# qos ecn enable
```

Show ECN

Privileged EXEC

Displays the ECN configuration.

SYNTAX

```
show qos ecn
```

PARAMETERS

No parameters.

EXAMPLE

```
qss# show qos ecn
```

EXAMPLE OUTPUT

```
qss# show qos ecn

QoS Explicit Congestion Notification
---------------------------------
IfIndex  ECN
-------- -------------------------
Ex0/1    Disable
Ex0/2    Disable
Ex0/3    Disable
Ex0/4    Disable
Ex0/5    Disable
Ex0/6    Disable
Ex0/7    Disable
Ex0/8    Disable
Ex0/9    Disable
Ex0/10   Disable
Ex0/11   Disable
Ex0/12   Disable
Ex0/13   Disable
Ex0/14   Disable
Ex0/15   Disable
Ex0/16   Disable
Ex0/17   Disable
Ex0/18   Disable
Ex0/19   Disable
...
```

Queue / VLAN statistics

These commands display and clear per-queue egress statistics for an interface and per-VLAN ingress statistics, and set whether each is reported in packets or bytes.

Show QoS Queue Statistics

Privileged EXEC

Displays per-queue egress statistics for an interface.

SYNTAX

```
show qos queue-statistics interface <interface-type> <interface-id>
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
`interface-type`	`varies by model`	Interface type keyword, e.g. gigabitethernet or extreme-ethernet (see note below).	—
`interface-id`	`slot/port`	Port number in slot/port form, e.g. 0/1.	—

EXAMPLE

```
qss# show qos queue-statistics interface extreme-ethernet 0/1
```

EXAMPLE OUTPUT

```
qss# show qos queue-statistics interface extreme-ethernet 0/1

Queue Statistics
Port   Queue    Transmitted Packets  Tail Dropped Packets Transmitted Bytes    Tail Dropped Bytes
-------------------------------------------------------------------------------------------------
1      0        0                    0                    0                    0
1      1        0                    0                    0                    0
1      2        0                    0                    0                    0
1      3        0                    0                    0                    0
1      4        0                    0                    0                    0
1      5        0                    0                    0                    0
1      6        0                    0                    0                    0
1      7        0                    0                    0                    0
```

NOTES

- The interface type keyword depends on the switch model and port type — for example "gigabitethernet" or "extreme-ethernet" (abbreviation "ex"); "port-channel <n>" addresses a link-aggregation group. Type "?" after the command to list the interface types available on your switch.

Clear QoS Queue Statistics

Privileged EXEC

Clears per-queue egress counters for one interface or all interfaces.

SYNTAX

```
clear qos queue-statistics [{ interface <interface-type> <interface-id> | all }]
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
`interface-type`	`varies by model`	Interface type keyword, e.g. gigabitethernet or extreme-ethernet (see note below).	—
`interface-id`	`slot/port`	Port number in slot/port form, e.g. 0/1. Together with interface-type, identifies the one interface to clear per-queue counters for.	—
`all`	`all`	Clears per-queue counters for every interface, instead of just one.	—

EXAMPLE

```
qss# clear qos queue-statistics interface extreme-ethernet 0/1
```

NOTES

- The interface type keyword depends on the switch model and port type — for example "gigabitethernet" or "extreme-ethernet" (abbreviation "ex"); "port-channel <n>" addresses a link-aggregation group. Type "?" after the command to list the interface types available on your switch.

Set Egress Queue Counter Unit

Global configuration

Sets whether egress queue counters are reported in packets or bytes.

SYNTAX

```
qos egress-queue-cnc-type { packet | byte }
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
egress-queue-cnc-type	packet | byte	Unit egress queue counters are reported in: packets or bytes.	—

EXAMPLE

```
qss(config)# qos egress-queue-cnc-type packet
```

Show QoS VLAN Ingress Statistics

Privileged EXEC

Displays ingress statistics for a VLAN.

SYNTAX

```
show qos vlan-ingress-statistics <vlan-id>
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
vlan-id	1-4094	ID of the VLAN this command applies to.	—

EXAMPLE

```
qss# show qos vlan-ingress-statistics 1
```

EXAMPLE OUTPUT

```
qss# show qos vlan-ingress-statistics 1

VLAN Ingress Statistics
VLAN ID    Ingress Packets      Ingress Bytes
--------------------------------------------------
1          2702                 0
```

Clear QoS VLAN Ingress Statistics

Privileged EXEC

Clears ingress counters for one VLAN or all VLANs.

SYNTAX

```
clear qos vlan-ingress-statistics [{ <vlan-id> | all }]
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
vlan-id	1-4094	Clears ingress counters for this one VLAN.	—
all	all	Clears ingress counters for every VLAN, instead of just one.	—

EXAMPLE

```
qss# clear qos vlan-ingress-statistics 1
```

Set Ingress VLAN Counter Unit

Global configuration

Sets whether VLAN ingress counters are reported in packets or bytes.

SYNTAX

```
qos ingress-vlan-cnc-type { packet | byte }
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
ingress-vlan-cnc-type	packet | byte	Unit VLAN ingress counters are reported in: packets or bytes.	—

EXAMPLE

```
qss(config)# qos ingress-vlan-cnc-type packet
```

Drop monitor

These commands start, stop, and show the status of drop monitoring on a VLAN, which watches for packet drops so you can identify congestion or misconfiguration.

Show QoS VLAN Drop Monitor

Privileged EXEC

Displays the current drop-monitor status.

SYNTAX

```
show qos vlan-drop-monitor
```

PARAMETERS

No parameters.

EXAMPLE

```
qss# show qos vlan-drop-monitor
```

EXAMPLE OUTPUT

```
qss# show qos vlan-drop-monitor

VLAN Drop Monitor Status
--------------------------------------------------
Status: Disabled
```

Start QoS VLAN Drop Monitor

Global configuration

Starts monitoring packet drops on a VLAN.

SYNTAX

```
qos vlan-drop-monitor start <vlan-id>
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
vlan-id	1-4094	VLAN to monitor.	—

EXAMPLE

```
qss(config)# qos vlan-drop-monitor start 1
```

Stop QoS VLAN Drop Monitor

Global configuration

Stops monitoring packet drops.

SYNTAX

```
qos vlan-drop-monitor stop
```

PARAMETERS

No parameters.

EXAMPLE

```
qss(config)# qos vlan-drop-monitor stop
```

6. Security

Security-related configuration allows you to control network access, enforce traffic policies, and safeguard system resources. These commands support the implementation of measures that prevent unauthorized connections, maintain data integrity, and ensure stable and secure network operations.

IN THIS CHAPTER

Loop protection

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.

Show Loop Protection Details

Privileged EXEC

Displays detailed loop protection status for every port.

SYNTAX

```
show loop_protection details
```

PARAMETERS

No parameters.

EXAMPLE

```
qss# show loop_protection details
```

EXAMPLE OUTPUT

```
qss# show loop_protection details

LOOP PROTECTION is disabled
Shutdown Time                      : 180
------------------------------------------------------------------------
Port        Active        Loops      Looping           Last Loop
   1      Disabled          0           -                  -
   2      Disabled          0           -                  -
   3      Disabled          0           -                  -
   4      Disabled          0           -                  -
   5      Disabled          0           -                  -
   6      Disabled          0           -                  -
   7      Disabled          0           -                  -
   8      Disabled          0           -                  -
   9      Disabled          0           -                  -
  10      Disabled          0           -                  -
  11      Disabled          0           -                  -
  12      Disabled          0           -                  -
  13      Disabled          0           -                  -
  14      Disabled          0           -                  -
  15      Disabled          0           -                  -
  16      Disabled          0           -                  -
  17      Disabled          0           -                  -
  18      Disabled          0           -                  -
...
```

Set Loop Protection (Global)

Global configuration

Enables or disables loop protection switch-wide.

SYNTAX

```
set loop_protection { enable | disable }
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
protection	enable | disable	Enables or disables loop protection switch-wide.	disable

EXAMPLE

```
qss(config)# set loop_protection enable
```

Set Loop Protection (Port)

Interface configuration

Enables or disables loop protection on the interface.

SYNTAX

```
loop_protection { enable | disable }
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
protection	enable | disable	Enables or disables loop protection on the interface.	disable

EXAMPLE

```
qss(config-if)# loop_protection enable
```

Set Loop Protection Shutdown Period

Global configuration

Sets how long a port stays shut down after loop protection trips it.

SYNTAX

```
loop_protection shutdown-period <seconds (0-604800)>
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
seconds	0-604800	How long the port stays shut down after loop protection trips it, in seconds.	180

EXAMPLE

```
qss(config)# loop_protection shutdown-period 200
```

Clear Loop Protection Status

Global configuration

Clears the loop protection status/counters.

SYNTAX

```
clear loop_protection status
```

PARAMETERS

No parameters.

EXAMPLE

```
qss(config)# clear loop_protection status
```

ACL (IP / IPv6 / MAC, ACL mirroring)

Access control list (ACL) settings provide mechanisms for defining and enforcing packet filtering policies on network interfaces. These settings allow administrators to control traffic flow based on parameters such as source and destination addresses, MAC addresses, or protocol types. IPv4-based, IPv6-based, and MAC-based ACLs can each be configured and viewed, and matching traffic can be mirrored to a monitoring port, to ensure accurate policy enforcement.

Show Access Lists

Privileged EXEC

Displays IP or MAC access lists.

SYNTAX

```
show access-lists [{ ip <access-list-number (1-65535)> | mac <access-list-number (1-65535)> }]
```

RELATED COMMANDS

Set ACL Mirror Destination, Set ACL Mirror Source, Show ACL Mirroring Session

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
`ip | mac`	`ip | mac`	Selects whether the number below identifies an IP or a MAC access list (optional; shows all lists of both kinds when the whole bracketed group is omitted).	—
`access-list-number`	`1-65535`	Limits the display to this one access list (optional; shows all when omitted).	—

EXAMPLE

```
qss# show access-lists
```

EXAMPLE OUTPUT

Output from a switch with no access lists configured.

```
qss# show access-lists

IP ACCESS LISTS
----------------

 %No IP Access Lists have been configured

MAC ACCESS LISTS
----------------

 %No MAC Access Lists have been configured


USER DEFINED LISTS
----------------------

 %No User Defined Lists have been configured
```

NOTES

- IP access lists use numbers 1001–65535 when created with ip access-list extended; MAC access lists use 1–65535.

Set IP Access List

Global configuration

Creates or deletes an extended IP access list and enters its configuration mode.

SYNTAX

```
ip access-list extended <access-list-number (1001-65535)>
no ip access-list extended <access-list-number (1001-65535)>
```

RELATED COMMANDS

Set ACL Rule (ICMPv4), Set ACL Rule (IPv6 ICMP), Set ACL Rule (IPv6 TCP), Set ACL Rule (IPv6 UDP), Set ACL Rule (TCP), Set ACL Rule (UDP)

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
access-list-number	1001-65535	Extended IP access list number to create, delete, or configure.	—

EXAMPLE

```
qss(config)# ip access-list extended 1001
```

Set ACL Rule (TCP)

ACL extended access list configuration

Adds a permit or deny rule matching TCP traffic to the IP access list.

SYNTAX

```
{ permit | deny } tcp { any | host <src-ip-address> | <src-ip-address> <src-mask> }
[eq <port-number (1-65535)>]
{ any | host <dest-ip-address> | <dest-ip-address> <dest-mask> }
[eq <port-number (1-65535)>]
[ack][rst][fin][syn][psh][urg] priority <value (1-255)>
```

RELATED COMMANDS

Set IP Access Group, Set IP Access List

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
action	permit | deny	"permit" forwards matching packets; "deny" drops them.	—
any | host <src-ip-address> | <src-ip-address> <src-mask>	any | host <ip> | <ip> <mask>	"any" matches every address; "host <ip>" matches one address; "<ip> <mask>" matches a subnet. Applies to both the source and destination operand.	—
src-ip-address	IPv4 address	Source IPv4 address to match.	—
src-mask	IPv4 wildcard mask	Source address wildcard mask.	—
port-number	1-65535	TCP/UDP port number.	—
dest-ip-address	IPv4 address	Destination IPv4 address to match.	—
dest-mask	IPv4 wildcard mask	Destination address wildcard mask.	—
ack	ack	Matches only TCP segments with the ACK flag set (optional; flags follow the documented order).	—
rst	rst	Matches only TCP segments with the RST flag set (optional; flags follow the documented order).	—
fin	fin	Matches only TCP segments with the FIN flag set (optional; flags follow the documented order).	—
syn	syn	Matches only TCP segments with the SYN flag set (optional; flags follow the documented order).	—
psh	psh	Matches only TCP segments with the PSH flag set (optional; flags follow the documented order).	—
urg	urg	Matches only TCP segments with the URG flag set (optional; flags follow the documented order).	—
priority	1-255	Rule priority (lower numbers match first).	—

EXAMPLE

```
qss(config-extnacl)# permit tcp host 192.168.100.100 any ack priority 1
qss(config-extnacl)# permit tcp any host 192.168.100.200 fin syn priority 5
qss(config-extnacl)# deny tcp any host 192.168.100.200 eq 23 rst psh urg priority 10
```

Set ACL Rule (ICMPv4)

ACL extended access list configuration

Adds a permit or deny rule matching ICMPv4 traffic to the IP access list.

SYNTAX

```
{ permit | deny } icmp { any | host <src-ip-address> | <src-ip-address> <mask> }
{ any | host <dest-ip-address> | <dest-ip-address> <mask> }
[ message-type <message-type (0-255)>] [ message-code <message-code (0-255)>]
priority <priority (1-255)>
```

RELATED COMMANDS

Set IP Access Group, Set IP Access List

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
action	permit | deny	"permit" forwards matching packets; "deny" drops them.	—
any | host <src-ip-address> | <src-ip-address> <mask>	any | host <ip> | <ip> <mask>	"any" matches every address; "host <ip>" matches one address; "<ip> <mask>" matches a subnet. Applies to both the source and destination operand.	—
src-ip-address	IPv4 address	Source IPv4 address to match.	—
mask	IPv4 subnet mask	Subnet mask for the source or destination address match, e.g. 255.255.255.0.	—
dest-ip-address	IPv4 address	Destination IPv4 address to match.	—
message-type	0-255	ICMP message type.	—
message-code	0-255	ICMP message code.	—
priority	1-255	Rule priority (lower numbers match first).	—

EXAMPLE

```
qss(config-extnacl)# permit icmp host 192.168.100.100 any priority 1
qss(config-extnacl)# permit icmp 192.168.1.0 255.255.255.0 any priority 1
qss(config-extnacl)# deny icmp any host 192.168.100.200 priority 5
```

Set ACL Rule (UDP)

ACL extended access list configuration

Adds a permit or deny rule matching UDP traffic to the IP access list.

SYNTAX

```
{ permit | deny } udp { any | host <src-ip-address> | <src-ip-address> <src-mask> }
[eq <port-number (1-65535)>]
{ any | host <dest-ip-address> | <dest-ip-address> <dest-mask> }
[eq <port-number (1-65535)>]
priority <priority (1-255)>
```

RELATED COMMANDS

Set IP Access Group, Set IP Access List

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
action	permit | deny	"permit" forwards matching packets; "deny" drops them.	—
any | host <src-ip-address> | <src-ip-address> <src-mask>	any | host <ip> | <ip> <mask>	"any" matches every address; "host <ip>" matches one address; "<ip> <mask>" matches a subnet. Applies to both the source and destination operand.	—
src-ip-address	IPv4 address	Source IPv4 address to match.	—
src-mask	IPv4 wildcard mask	Source address wildcard mask.	—
port-number	1-65535	TCP/UDP port number.	—
dest-ip-address	IPv4 address	Destination IPv4 address to match.	—
dest-mask	IPv4 wildcard mask	Destination address wildcard mask.	—
priority	1-255	Rule priority (lower numbers match first).	—

EXAMPLE

```
qss(config-extnacl)# permit udp host 192.168.100.100 any priority 1
qss(config-extnacl)# deny udp any host 192.168.100.200 eq 69 priority 5
```

Set IP Access Group

Interface configuration

Applies (or removes) an IP access list to the interface, inbound.

SYNTAX

```
ip access-group <access-list-number (1001-65535)> in
no ip access-group <access-list-number (1001-65535)> in
```

RELATED COMMANDS

Set ACL Mirror Destination, Set ACL Mirror Source, Set ACL Rule (ICMPv4), Set ACL Rule (IPv6 ICMP), Set ACL Rule (IPv6 TCP), Set ACL Rule (IPv6 UDP), Set ACL Rule (TCP), Set ACL Rule (UDP), Show ACL Mirroring Session

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
access-list-number	1001-65535	IP access list number to apply to (or remove from) the interface.	—

EXAMPLE

```
qss(config-if)# ip access-group 11001 in
```

Set ACL Mirror Source

Global configuration

Sets the IP or MAC access list whose matched traffic is mirrored.

SYNTAX

```
monitor session <session-id (2-7)> source { ip-acl <acl-id> | mac-acl <acl-id> }
```

RELATED COMMANDS

Set IP Access Group, Set MAC Access Group, Show Access Lists

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
session-id	2-7	Mirroring session ID.	—
ip-acl | mac-acl	ip-acl | mac-acl	Selects whether the mirrored traffic is matched by an IP or a MAC access list.	—
acl-id	1001-65535 (ip-acl) / 1-65535 (mac-acl)	Access list number whose matched traffic is mirrored — extended IP ACL number (1001-65535) when the selection above is ip-acl, MAC ACL number (1-65535) when it is mac-acl.	—

EXAMPLE

```
qss(config)# monitor session 2 source ip-acl 1001
```

Set ACL Mirror Destination

Global configuration

Sets the interface that receives mirrored ACL traffic for the session.

SYNTAX

```
monitor session <session-id (2-7)> destination interface <interface-type> <interface-id>
no monitor session <session-id (2-7)> destination interface <interface-type> <interface-id>
```

RELATED COMMANDS

Set IP Access Group, Show Access Lists

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
session-id	2-7	Mirroring session ID.	—
interface-type	varies by model	Interface type keyword, e.g. gigabitethernet or extreme-ethernet (see note below).	—
interface-id	slot/port	Port number in slot/port form, e.g. 0/1.	—

EXAMPLE

```
qss(config)# monitor session 2 destination interface gigabitethernet 0/1
```

NOTES

- The interface type keyword depends on the switch model and port type — for example "gigabitethernet" or "extreme-ethernet" (abbreviation "ex"); "port-channel <n>" addresses a link-aggregation group. Type "?" after the command to list the interface types available on your switch.

Set ACL Rule (IPv6 TCP)

ACL extended access list configuration

Adds a permit or deny rule matching IPv6 TCP traffic to the IP access list.

SYNTAX

```
{ permit | deny } ipv6-tcp { any | host <src-ipv6-address> <prefix-length (0-128)> }
[eq <port-number (1-65535)>]
{ any | host <dest-ipv6-address> <prefix-length (0-128)> }
[eq <port-number (1-65535)>]
[{ ack | rst }] priority <priority (1-255)>
```

RELATED COMMANDS

Set IP Access Group, Set IP Access List

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
action	permit | deny	"permit" forwards matching packets; "deny" drops them.	—
any | host <src-ipv6-address> <prefix-length>	any | host <ipv6> <prefix-len>	"any" matches every address; "host <ipv6> <prefix-len>" matches one address/prefix. Applies to both the source and destination operand.	—
src-ipv6-address	IPv6 address	Source IPv6 address to match.	—
dest-ipv6-address	IPv6 address	Destination IPv6 address to match.	—
prefix-length	0-128	IPv6 prefix length, in bits (applies to both the source and destination operand).	—
port-number	1-65535	TCP/UDP port number.	—
ack | rst	ack | rst	Matches only TCP segments with the ACK or RST flag set (optional).	—
priority	1-255	Rule priority (lower numbers match first).	—

EXAMPLE

```
qss(config-extnacl)# permit ipv6-tcp host 2222::4444 64 any priority 1
qss(config-extnacl)# permit ipv6-tcp host 2222::4444 64 host 3333::1 64 eq 443 priority 2
qss(config-extnacl)# deny ipv6-tcp any host 3333::1 64 eq 23 priority 5
```

Set ACL Rule (IPv6 ICMP)

ACL extended access list configuration

Adds a permit or deny rule matching IPv6 ICMP traffic to the IP access list.

SYNTAX

```
{ permit | deny } ipv6-icmp { any | host <src-ipv6-address> <prefix-length (0-128)> }
{ any | host <dest-ipv6-address> <prefix-length (0-128)> }
[ message-type <message-type (0-255)>] [ message-code <message-code (0-255)>]
priority <priority (1-255)>
```

RELATED COMMANDS

Set IP Access Group, Set IP Access List

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
action	permit | deny	"permit" forwards matching packets; "deny" drops them.	—
any | host <src-ipv6-address> <prefix-length>	any | host <ipv6> <prefix-len>	"any" matches every address; "host <ipv6> <prefix-len>" matches one address/prefix. Applies to both the source and destination operand.	—
src-ipv6-address	IPv6 address	Source IPv6 address to match.	—
dest-ipv6-address	IPv6 address	Destination IPv6 address to match.	—
prefix-length	0-128	IPv6 prefix length, in bits (applies to both the source and destination operand).	—
message-type	0-255	ICMP message type.	—
message-code	0-255	ICMP message code.	—
priority	1-255	Rule priority (lower numbers match first).	—

EXAMPLE

```
qss(config-extnacl)# permit ipv6-icmp host 2222::4444 64 any priority 1
qss(config-extnacl)# permit ipv6-icmp host 2222::4444 64 host 3333::1 64 message-type 128 priority 2
qss(config-extnacl)# deny ipv6-icmp any host 3333::1 64 priority 5
```

Set ACL Rule (IPv6 UDP)

ACL extended access list configuration

Adds a permit or deny rule matching IPv6 UDP traffic to the IP access list.

SYNTAX

```
{ permit | deny } ipv6-udp { any | host <src-ipv6-address> <prefix-length (0-128)> }
[eq <port-number (1-65535)>]
{ any | host <dest-ipv6-address> <prefix-length (0-128)> }
[eq <port-number (1-65535)>]
priority <priority (1-255)>
```

RELATED COMMANDS

Set IP Access Group, Set IP Access List

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
action	permit | deny	"permit" forwards matching packets; "deny" drops them.	—
any | host <src-ipv6-address> <prefix-length>	any | host <ipv6> <prefix-len>	"any" matches every address; "host <ipv6> <prefix-len>" matches one address/prefix. Applies to both the source and destination operand.	—
src-ipv6-address	IPv6 address	Source IPv6 address to match.	—
dest-ipv6-address	IPv6 address	Destination IPv6 address to match.	—
prefix-length	0-128	IPv6 prefix length, in bits (applies to both the source and destination operand).	—
port-number	1-65535	TCP/UDP port number.	—
priority	1-255	Rule priority (lower numbers match first).	—

EXAMPLE

```
qss(config-extnacl)# permit ipv6-udp host 2222::4444 64 any priority 1
qss(config-extnacl)# permit ipv6-udp host 2222::4444 64 host 3333::1 64 eq 443 priority 2
qss(config-extnacl)# deny ipv6-udp any host 3333::1 64 eq 69 priority 5
```

Set MAC Access List

Global configuration

Creates or deletes an extended MAC access list and enters its configuration mode.

SYNTAX

```
mac access-list extended <access-list-number (1-65535)>
no mac access-list extended <access-list-number (1-65535)>
```

RELATED COMMANDS

Set ACL Rule (MAC)

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
access-list-number	1-65535	Extended MAC access list number to create, delete, or configure.	—

EXAMPLE

```
qss(config)# mac access-list extended 1
```

Set ACL Rule (MAC)

ACL MAC configuration

Adds a permit or deny rule matching source/destination MAC addresses to the MAC access list.

SYNTAX

```
{ permit | deny } { any | host <mac-address> } { any | host <mac-address> } priority <priority (1-255)>
```

RELATED COMMANDS

Set MAC Access Group, Set MAC Access List

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
action	permit | deny	"permit" forwards matching packets; "deny" drops them.	—
source	any | host	Source MAC address to match: "any" matches all addresses, or "host" matches a single MAC address (see the note below for its format).	—
destination	any | host	Destination MAC address to match: "any" matches all addresses, or "host" matches a single MAC address (see the note below for its format).	—
priority	1-255	Rule priority (lower numbers match first).	—

EXAMPLE

```
qss(config-extmacl)# permit host 24:5e:be:00:00:15 any priority 1
qss(config-extmacl)# deny host 24:5e:be:00:00:15 any priority 2
```

NOTES

- `host` takes a MAC address in aa:aa:aa:aa:aa:aa form.

Set MAC Access Group

Interface configuration

Applies (or removes) a MAC access list to the interface, inbound.

SYNTAX

```
mac access-group <access-list-number (1-65535)> in
no mac access-group [<access-list-number (1-65535)>] in
```

RELATED COMMANDS

Set ACL Mirror Source, Set ACL Rule (MAC)

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
access-list-number	1-65535	MAC access list number to apply to (or remove from) the interface.	—

EXAMPLE

```
qss(config-if)# mac access-group 1 in
```

Set ACL Rule (IP)

ACL extended access list configuration

Adds a permit or deny rule using IP source and destination address matches.

SYNTAX

```
{ permit | deny } ip { any | host <src-ip-address> | <src-ip-address> <src-mask> } [eq <port-number
(1-65535)>] { any | host <dest-ip-address> | <dest-ip-address> <dest-mask> } [eq <port-number (1-
65535)>] priority <value (1-255)>
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
action	permit | deny	Chooses whether matching packets are permitted or denied.	—
address-form	any | host	Address form used by either operand: any address or one host.	—
src-ip-address	IPv4 address	Source IP address to match.	—
src-mask	IPv4 mask	Mask paired with the source IP address.	—
port-number	1-65535	Optional source or destination port number.	—
dest-ip-address	IPv4 address	Destination IP address to match.	—
dest-mask	IPv4 mask	Mask paired with the destination IP address.	—
priority	1-255	Required rule priority.	—

EXAMPLE

```
qss(config-extnacl)# permit ip host 192.0.2.10 any priority 10
qss(config-extnacl)# deny ip any host 198.51.100.20 priority 20
```

Set ACL Rule (IPv6)

ACL extended access list configuration

Adds a permit or deny rule using IPv6 source and destination address matches.

SYNTAX

```
{ permit | deny } ipv6 { any | host <src-ip-address> | <src-ip-address> <src-mask> } [eq <port-number (1-65535)>] { any | host <dest-ip-address> | <dest-ip-address> <dest-mask> } [eq <port-number (1-65535)>] priority <value (1-255)>
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
`action`	`permit | deny`	Chooses whether matching packets are permitted or denied.	—
`address-form`	`any | host`	Address form used by either operand: any address or one host.	—
`src-ip-address`	`IPv6 address`	Source IPv6 address to match.	—
`src-mask`	`unspecified type and range`	Mask paired with the source IPv6 address.	—
`port-number`	`1-65535`	Optional source or destination port number.	—
`dest-ip-address`	`IPv6 address`	Destination IPv6 address to match.	—
`dest-mask`	`unspecified type and range`	Mask paired with the destination IPv6 address.	—
`priority`	`1-255`	Required rule priority.	—

EXAMPLE

```
qss(config-extnacl)# permit ipv6 host 2001:db8::10 any priority 10
qss(config-extnacl)# deny ipv6 any host 2001:db8::20 priority 20
```

DoS prevention

These commands enable or disable DoS attack prevention switch-wide, turn individual attack-prevention checks on or off, and show the current DoS prevention configuration.

Set DoS Prevention

Global configuration

Enables or disables DoS attack prevention switch-wide (master switch).

SYNTAX

```
dos-prevention { enable | disable }
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
`dos-prevention`	`enable | disable`	Enables or disables DoS attack prevention switch-wide.	`disable`

EXAMPLE

```
qss(config)# dos-prevention enable
```

Set DoS Prevention Types

Global configuration

Enables or disables one or more specific DoS attack-prevention checks.

SYNTAX

```
dos-prevention type [tcp-syn-data] [tcp-over-bc] [null-scan] [xmas-scan] [tcp-syn-fin] [tcp-syn-rst] [tcp-udp-port-zero] [frag-ip] [arp-mac-sa-mismatch] [land] [tcp-without-full-header] [tcp-fin-without-ack] [blat] [tcp-syn-low-port]
no dos-prevention type [tcp-syn-data] [tcp-over-bc] [null-scan] [xmas-scan] [tcp-syn-fin] [tcp-syn-rst] [tcp-udp-port-zero] [frag-ip] [arp-mac-sa-mismatch] [land] [tcp-without-full-header] [tcp-fin-without-ack] [blat] [tcp-syn-low-port]
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
attack type	tcp-syn-data | tcp-over-bc | null-scan | xmas-scan | tcp-syn-fin | tcp-syn-rst | tcp-udp-port-zero | frag-ip | arp-mac-sa-mismatch | land | tcp-without-full-header | tcp-fin-without-ack | blat | tcp-syn-low-port	One or more attack-detection checks to enable or disable (space-separated).	none (all 14 types Off)

EXAMPLE

```
qss(config)# dos-prevention type tcp-syn-data null-scan tcp-syn-fin
```

Show DoS Prevention

Privileged EXEC

Displays the DoS attack prevention configuration.

SYNTAX

```
show dos-prevention
```

PARAMETERS

No parameters.

EXAMPLE

```
qss# show dos-prevention
```

EXAMPLE OUTPUT

```
qss# show dos-prevention

DoS Prevention            : Disabled
  TCP SYN with Data       : Off
  TCP over MAC MC/BC      : Off
  Null Scan               : Off
  XMAS Scan               : Off
  TCP SYN-FIN             : Off
  TCP SYN-RST             : Off
  TCP/UDP Port Zero       : Off
  IP/ICMP Fragmentation   : Off
  ARP MAC SA Mismatch     : Off
  Land Attack             : Off
  TCP Without Full Header : Off
  TCP FIN without ACK     : Off
  Blat (TCP/UDP)          : Off
  TCP-SYN (Source < 1024) : Off
```

DHCP snooping

DHCP snooping is a security feature that monitors DHCP messages on the network and builds a binding table that associates client MAC addresses, IP addresses, VLANs, and interface information. This helps prevent malicious or rogue DHCP servers from assigning unauthorized IP addresses, ensures the validity of DHCP traffic, and enables features such as IP Source Guard (IPSG) and Dynamic ARP Inspection (DAI) to validate network clients.

Before you begin

- Enable DHCP snooping globally (`ip dhcp snooping`). **REQUIRED**
- Enable DHCP snooping on the VLANs where it should operate (`ip dhcp snooping vlan <N>`). **REQUIRED**

CONFIGURATION ORDER

1. Optionally enable existing-Option-82 verification when packets carrying Option 82 from untrusted ports must be rejected.

```
qss(config)# ip dhcp snooping verify information
```

2. Alternative: to skip this specific check instead of enabling it, use the `no` form. Packets continue to subsequent processing and may still be subject to other checks.

```
qss(config)# no ip dhcp snooping verify information
```

Show DHCP Snooping Global Settings

Privileged EXEC

Displays the global DHCP snooping configuration.

SYNTAX

```
show ip dhcp snooping globals
```

PARAMETERS

No parameters.

EXAMPLE

```
qss# show ip dhcp snooping globals
```

EXAMPLE OUTPUT

```
qss# show ip dhcp snooping globals

DHCP Snooping Global information
--------------------------------

Switch : default
-------  -------
Layer 2 DHCP Snooping is globally disabled
Information verification is disabled
MAC Address verification is disabled
```

Show DHCP Snooping Port Settings

Privileged EXEC

Displays the per-interface DHCP snooping configuration.

SYNTAX

```
show ip dhcp snooping interface
```

PARAMETERS

No parameters.

EXAMPLE

```
qss# show ip dhcp snooping interface
```

EXAMPLE OUTPUT

```
qss# show ip dhcp snooping interface

DHCP Snooping Interface Information
-----------------------------------

Port     Port Security State   Rate Limit
----     -------------------   ----------
Ex0/1          untrusted          0 Kbps
Ex0/2          untrusted          0 Kbps
Ex0/3          untrusted          0 Kbps
Ex0/4          untrusted          0 Kbps
Ex0/5          untrusted          0 Kbps
Ex0/6          untrusted          0 Kbps
Ex0/7          untrusted          0 Kbps
Ex0/8          untrusted          0 Kbps
Ex0/9          untrusted          0 Kbps
Ex0/10         untrusted          0 Kbps
Ex0/11         untrusted          0 Kbps
Ex0/12         untrusted          0 Kbps
Ex0/13         untrusted          0 Kbps
Ex0/14         untrusted          0 Kbps
Ex0/15         untrusted          0 Kbps
Ex0/16         untrusted          0 Kbps
Ex0/17         untrusted          0 Kbps
...
```

Show DHCP Snooping VLAN Settings

Privileged EXEC

Displays the per-VLAN DHCP snooping configuration.

SYNTAX

```
show ip dhcp snooping
```

PARAMETERS

No parameters.

EXAMPLE

```
qss# show ip dhcp snooping
```

EXAMPLE OUTPUT

Prints only the header when nothing is configured.

```
qss# show ip dhcp snooping

DHCP Snooping Vlan information
------------------------------
```

Set DHCP Snooping Binding Entry

Global configuration

Adds a static entry to the DHCP snooping binding table.

SYNTAX

```
ip source binding <mac> vlan <vlan-id> <ip> interface <interface-type> <interface-id>
```

RELATED COMMANDS

Show IP Source Guard Binding Table

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
mac	aa:aa:aa:aa:aa:aa	MAC address of the bound client.	—
vlan-id	1-4094	ID of the VLAN this command applies to.	—
ip	IPv4 address	IPv4 address for this entry.	—
interface-type	varies by model	Interface type keyword, e.g. gigabitethernet or extreme-ethernet (see note below).	—
interface-id	slot/port	Port number in slot/port form, e.g. 0/1.	—

EXAMPLE

```
qss(config)# ip source binding 00:11:22:33:44:55 vlan 10 192.168.1.100 interface ex 0/1
```

NOTES

- The interface type keyword depends on the switch model and port type — for example "gigabitethernet" or "extreme-ethernet" (abbreviation "ex"); "port-channel <n>" addresses a link-aggregation group. Type "?" after the command to list the interface types available on your switch.

Set DHCP Snooping (Global)

Global configuration

Enables or disables DHCP snooping switch-wide.

SYNTAX

```
ip dhcp snooping
no ip dhcp snooping
```

PARAMETERS

No parameters.

EXAMPLE

```
qss(config)# ip dhcp snooping
```

Set DHCP Snooping Trusted Sources

Global configuration

Enables or disables checking for an existing DHCP Option 82 field on packets received from untrusted ports; when enabled, the switch rejects such packets, and when disabled, it skips this specific check.

SYNTAX

```
ip dhcp snooping verify information
no ip dhcp snooping verify information
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
`form`	`ip dhcp snooping verify information | no ip dhcp snooping verify information`	The enabled form rejects packets that already contain Option 82 when they arrive on an untrusted port; the no form skips this specific check.	—

EXAMPLE

```
qss(config)# ip dhcp snooping verify information
```

NOTES

- When enabled, the switch rejects packets that already contain DHCP Option 82 when they arrive on an untrusted port.
- The `no` form skips this specific existing-Option-82 check. Packets continue to subsequent processing and may still be rejected by other checks.

Set DHCP Snooping Source MAC Verification

Global configuration

Enables or disables verification that a DHCP packet's source MAC matches its client hardware address.

SYNTAX

```
ip dhcp snooping verify mac-address
no ip dhcp snooping verify mac-address
```

PARAMETERS

No parameters.

EXAMPLE

```
qss(config)# ip dhcp snooping verify mac-address
```

Set DHCP Snooping Trusted Port

Interface configuration

Marks the interface as a trusted DHCP snooping port.

SYNTAX

```
ip dhcp snooping trust
```

PARAMETERS

No parameters.

EXAMPLE

```
qss(config-if)# ip dhcp snooping trust
```

Set DHCP Snooping Rate Limit

Interface configuration

Sets the maximum DHCP snooping rate in kilobits per second (kbps) on the interface before excess packets are dropped.

SYNTAX

```
ip dhcp snooping rate-limit <rate (1-500)>
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
rate	1-500	Maximum DHCP snooping rate, in kilobits per second (kbps), on the interface before excess packets are dropped.	0 (no limit)

EXAMPLE

```
qss(config-if)# ip dhcp snooping rate-limit 100
```

Set DHCP Snooping VLANs

Global configuration

Enables or disables DHCP snooping on specific VLANs.

SYNTAX

```
ip dhcp snooping vlan <vlan-id (1-4094)>
no ip dhcp snooping vlan <vlan-id (1-4094)>
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
vlan-id	1-4094	VLAN to enable or disable DHCP snooping on.	—

EXAMPLE

```
qss(config)# ip dhcp snooping vlan 1
```

IP Source Guard

IP Source Guard (IPSG) is a Layer 2 security feature that prevents IP address spoofing by filtering traffic based on valid IP–MAC bindings. When enabled on an interface, the switch permits only traffic that matches an authorized binding. IPSG can use static bindings, DHCP snooping bindings, or port-level verification rules to protect the network from malicious or misconfigured hosts.

Show IP Source Guard Binding Table

Privileged EXEC

Displays the IP Source Guard binding table.

SYNTAX

```
show ip source binding
```

RELATED COMMANDS

Set DHCP Snooping Binding Entry

PARAMETERS

No parameters.

EXAMPLE

```
qss# show ip source binding
```

EXAMPLE OUTPUT

Prints only the header when nothing is configured.

```
qss# show ip source binding

                          Host Binding Information

                          ------------------------
```

NOTES

- This is also the DHCP snooping binding table — there is no separate "show ip dhcp snooping binding" command.

Set IP Source Guard Static Binding

Interface configuration

Adds or removes a static IP Source Guard binding entry on the interface.

SYNTAX

```
ip-source-guard static-binding <ip> <mac> vlan <vlan-id (1-4094)>
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
ip	IPv4 address	IPv4 address for this entry.	—
mac	aa:aa:aa:aa:aa:aa	MAC address of the bound client.	—
vlan-id	1-4094	VLAN the static IP Source Guard binding applies to.	—

EXAMPLE

```
qss(config-if)# ip-source-guard static-binding 192.168.1.10 00:11:22:33:44:55 vlan 1
```

Set IP Source Guard

Interface configuration

Enables or disables IP Source Guard on the interface.

SYNTAX

```
ip verify source port-security
no ip verify source port-security
```

PARAMETERS

No parameters.

EXAMPLE

```
qss(config-if)# ip verify source port-security
```

Show IP Source Guard

Privileged EXEC

Displays IP Source Guard port settings.

SYNTAX

```
show ip verify source [interface <interface-type> <interface-id>]
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
interface-type	varies by model	Interface type keyword, e.g. gigabitethernet or extreme-ethernet (see note below).	—
interface-id	slot/port	Port number in slot/port form, e.g. 0/1.	—

EXAMPLE

```
qss# show ip verify source
```

EXAMPLE OUTPUT

```
qss# show ip verify source

Interface          IP Source guard Status
---------          ----------------------
Ex0/1         Disable
Ex0/2         Disable
Ex0/3         Disable
Ex0/4         Disable
Ex0/5         Disable
Ex0/6         Disable
Ex0/7         Disable
Ex0/8         Disable
Ex0/9         Disable
Ex0/10        Disable
Ex0/11        Disable
Ex0/12        Disable
Ex0/13        Disable
Ex0/14        Disable
Ex0/15        Disable
Ex0/16        Disable
Ex0/17        Disable
Ex0/18        Disable
Ex0/19        Disable
Ex0/20        Disable
...
```

NOTES

- The interface type keyword depends on the switch model and port type — for example "gigabitethernet" or "extreme-ethernet" (abbreviation "ex"); "port-channel <n>" addresses a link-aggregation group. Type "?" after the command to list the interface types available on your switch.

Dynamic ARP Inspection (DAI)

Dynamic ARP Inspection (DAI) protects the network against ARP spoofing attacks by validating ARP packets received on untrusted interfaces. The switch inspects ARP requests and responses and verifies their consistency against trusted bindings. Interfaces can be marked as trusted or untrusted, VLANs can be selectively enabled for inspection, and rate limits help prevent excessive ARP traffic from affecting switch performance.

Show DAI Statistics

Privileged EXEC

Displays Dynamic ARP Inspection (DAI) statistics and port settings.

SYNTAX

```
show arp spoofing [interface <interface-type> <interface-id>]
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
`interface-type`	`varies by model`	Interface type keyword, e.g. gigabitethernet or extreme-ethernet (see note below).	—
`interface-id`	`slot/port`	Port number in slot/port form, e.g. 0/1.	—

EXAMPLE

```
qss# show arp spoofing
```

EXAMPLE OUTPUT

```
qss# show arp spoofing

Arp Spoofing table
------------------
Port     Security State  Rate limit  Arp forward  Arp drop  SA drop  DA drop  IP drop
----     --------------  ----------  -----------  --------  -------  -------  -------
Ex0/1       trusted          0 pps       0          0         0        0        0
Ex0/2       trusted          0 pps       0          0         0        0        0
Ex0/3       trusted          0 pps       0          0         0        0        0
Ex0/4       trusted          0 pps       0          0         0        0        0
Ex0/5       trusted          0 pps       0          0         0        0        0
Ex0/6       trusted          0 pps       0          0         0        0        0
Ex0/7       trusted          0 pps       0          0         0        0        0
Ex0/8       trusted          0 pps       0          0         0        0        0
Ex0/9       trusted          0 pps       0          0         0        0        0
Ex0/10      trusted          0 pps       0          0         0        0        0
Ex0/11      trusted          0 pps       0          0         0        0        0
Ex0/12      trusted          0 pps       0          0         0        0        0
Ex0/13      trusted          0 pps       0          0         0        0        0
Ex0/14      trusted          0 pps       0          0         0        0        0
Ex0/15      trusted          0 pps       0          0         0        0        0
Ex0/16      trusted          0 pps       0          0         0        0        0
Ex0/17      trusted          0 pps       0          0         0        0        0
Ex0/18      trusted          0 pps       0          0         0        0        0
...
```

NOTES

- The interface type keyword depends on the switch model and port type — for example "gigabitethernet" or "extreme-ethernet" (abbreviation "ex"); "port-channel <n>" addresses a link-aggregation group. Type "?" after the command to list the interface types available on your switch.
- This output also covers: show DAI port settings (the CLI returns both from the same table).

Show DAI VLAN Settings

Privileged EXEC

Displays which VLANs have Dynamic ARP Inspection (DAI) enabled.

SYNTAX

```
show mac force forwarding
```

PARAMETERS

No parameters.

EXAMPLE

```
qss# show mac force forwarding
```

EXAMPLE OUTPUT

Output from a switch with no DAI-related entries configured.

```
qss# show mac force forwarding


% No entries to display
```

Show DAI Additional Settings

Privileged EXEC

Displays additional Dynamic ARP Inspection (DAI) global settings.

SYNTAX

```
show arp inspection globals
```

PARAMETERS

No parameters.

EXAMPLE

```
qss# show arp inspection globals
```

EXAMPLE OUTPUT

```
qss# show arp inspection globals

Dynamic ARP Inspection information
---------------------------------

Source MAC verification is disabled
Destination MAC verification is disabled
IP address verification is disabled
```

Set DAI VLANs

Config-VLAN

Enables or disables Dynamic ARP Inspection (DAI) on the current VLAN.

SYNTAX

```
mac force forwarding { enable | disable }
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
forwarding	enable | disable	Enables or disables Dynamic ARP Inspection on the current VLAN.	—

EXAMPLE

```
qss(config-vlan)# mac force forwarding enable
```

Set DAI Trusted Port

Interface configuration

Allows (trusted) or drops (untrusted) downstream broadcast ARP replies on the interface.

SYNTAX

```
downstream arp-bcast { allow | drop }
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
arp-bcast	allow | drop	Allows or drops downstream broadcast ARP replies received on the interface.	—

EXAMPLE

```
qss(config-if)# downstream arp-bcast allow
```

Set DAI Rate Limit

Interface configuration

Sets the maximum ARP packet rate on the interface before excess packets are dropped.

SYNTAX

```
ip arp inspection rate-limit <rate (1-300)>
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
rate	1-300	Maximum Dynamic ARP Inspection (DAI) rate, in kilobits per second (kbps), on the interface before excess packets are dropped.	0 (no limit)

EXAMPLE

```
qss(config-if)# ip arp inspection rate-limit 100
```

Set DAI Verification

Global configuration

Enables or disables source-MAC, destination-MAC, and/or IP verification for Dynamic ARP Inspection.

SYNTAX

```
arp inspection validate [src-mac][dst-mac][ip]
no arp inspection validate [src-mac][dst-mac][ip]
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
src-mac	src-mac	Also validates the ARP packet's source MAC address against the binding table (optional).	—
dst-mac	dst-mac	Also validates the ARP reply's destination MAC address against the binding table (optional).	—
ip	ip	Also validates the ARP packet's IP address against the binding table (optional).	—

EXAMPLE

```
qss(config)# arp inspection validate src-mac dst-mac ip
```

802.1X

IEEE 802.1X provides port-based network access control that authenticates devices before allowing them to send or receive traffic. These commands let administrators configure global 802.1X behavior, define authentication methods, specify RADIUS server settings, create local authentication entries, and control authentication behavior at the interface level.

Show 802.1X Global Settings

Privileged EXEC

Displays the global 802.1X configuration.

SYNTAX

```
show dot1x global
```

PARAMETERS

No parameters.

EXAMPLE

```
qss# show dot1x global
```

EXAMPLE OUTPUT

```
qss# show dot1x global

 Sysauthcontrol                  = Disabled
 Module Oper Status              = Disabled
 Dot1x Protocol Version          = 2
 Dot1x Authentication Method     = Radius
 Nas ID                          = fsNas1
```

Show 802.1X Port Settings

Privileged EXEC

Displays the 802.1X configuration for one port or all ports.

SYNTAX

```
show dot1x ports [{ <interface-type> <interface-id> | all }]
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
interface-type	varies by model	Interface type keyword, e.g. gigabitethernet or extreme-ethernet (see note below).	—
interface-id	slot/port	Port number in slot/port form, e.g. 0/1.	—
all	all	Shows every port's 802.1X configuration, instead of just one.	—

EXAMPLE

```
qss# show dot1x ports
```

EXAMPLE OUTPUT

```
qss# show dot1x ports

Dot1x Info for Ex0/1

---------------------

AuthMode              = PORT-BASED
AuthPaeStatus         = ENABLED
PortStatus            = AUTHORIZED
AuthPortStatus        = AUTHORIZED
AdminControlDirection = BOTH
MaxReq                = 2
Port Control          = Force Authorized
QuietPeriod           = 60 Seconds
ReAuthPeriod          = 3600 Seconds
ServerTimeout         = 30 Seconds
SuppTimeout           = 30 Seconds
Tx Period             = 30 Seconds

Dot1x Info for Ex0/2

---------------------

AuthMode              = PORT-BASED
AuthPaeStatus         = ENABLED
PortStatus            = AUTHORIZED
...
```

NOTES

- The interface type keyword depends on the switch model and port type — for example "gigabitethernet" or "extreme-ethernet" (abbreviation "ex"); "port-channel <n>" addresses a link-aggregation group. Type "?" after the command to list the interface types available on your switch.

Show 802.1X Authenticated Sessions

Privileged EXEC

Displays MAC addresses currently authenticated by 802.1X.

SYNTAX

```
show dot1x authentication session
```

PARAMETERS

No parameters.

EXAMPLE

```
qss# show dot1x authentication session
```

EXAMPLE OUTPUT

Prints nothing when there are no entries.

```
qss# show dot1x authentication session
```

Set 802.1X

Global configuration

Enables or disables 802.1X port-based authentication switch-wide.

SYNTAX

```
dot1x system-auth-control
no dot1x system-auth-control
```

PARAMETERS

No parameters.

EXAMPLE

```
qss(config)# dot1x system-auth-control
```

Set 802.1X RADIUS Server

Global configuration

Sets the RADIUS server address and authentication parameters for 802.1X.

SYNTAX

```
radius-server host <ipv4-address> [auth-port <auth-port (1-65535)>] [acct-port <acct-port (1-65535)>]
[timeout <timeout (1-120)>] [retransmit <retransmit (1-254)>] [key <secret-key-string>]
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
ipv4-address	IPv4 address	RADIUS server IPv4 address.	—
auth-port	1-65535	RADIUS authentication UDP port.	1812
acct-port	1-65535	RADIUS accounting UDP port.	1813
timeout	1-120 seconds	Timeout, in seconds.	10
retransmit	1-254	Number of retransmission attempts.	3
secret-key-string	text string	Shared secret key.	—

EXAMPLE

```
qss(config)# radius-server host 192.0.2.10 auth-port 12345 acct-port 10000 timeout 60 retransmit 100
key mysecretekey
```

Set 802.1X Control Direction

Interface configuration

Sets whether unauthorized traffic is blocked in one direction or both directions on the port.

SYNTAX

```
dot1x control-direction { in | both }
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
control-direction	in | both	Whether unauthorized traffic is blocked in one direction only, or both directions, on the port.	both

EXAMPLE

```
qss(config-if)# dot1x control-direction both
```

Set 802.1X Port Control

Interface configuration

Sets the port's 802.1X authorization mode: automatic, forced-authorized, or forced-unauthorized.

SYNTAX

```
dot1x port-control { auto | force-authorized | force-unauthorized }
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
port-control	auto | force-authorized | force-unauthorized	802.1X authorization mode for the port: automatic, forced-authorized, or forced-unauthorized.	force-authorized

EXAMPLE

```
qss(config-if)# dot1x port-control auto
```

Set 802.1X Max Request

Interface configuration

Sets how many times the switch retries an authentication request before giving up.

SYNTAX

```
dot1x max-req <count (1-10)>
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
max-req	1-10	How many times the switch retries an authentication request before giving up.	2

EXAMPLE

```
qss(config-if)# dot1x max-req 3
```

Set 802.1X Timeout

Interface configuration

Sets the server, supplicant, or retransmission timeout for 802.1X authentication.

SYNTAX

```
dot1x timeout { server-timeout | supp-timeout | tx-period } <seconds (1-65535)>
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
timeout type	server-timeout | supp-timeout | tx-period	Which timeout to set: RADIUS server response, supplicant response, or retransmission period.	—
seconds	1-65535	Timeout, in seconds.	30

EXAMPLE

```
qss(config-if)# dot1x timeout server-timeout 300
```

Set 802.1X Authentication Mode

Interface configuration

Sets whether 802.1X authenticates by port or by individual MAC address.

SYNTAX

```
dot1x auth-mode { port-based | mac-based }
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
auth-mode	port-based | mac-based	Whether 802.1X authenticates by port, or by individual MAC address.	port-based

EXAMPLE

```
qss(config-if)# dot1x auth-mode port-based
```

7. PoE

Power over Ethernet (PoE) commands let you monitor and control power delivery to connected powered devices (PDs) on each port. You can set the power class and priority a port supplies, watch for an unresponsive PD and automatically recover it, and keep PoE power available to connected devices across a switch reboot.

IN THIS CHAPTER

PoE power & priority

These commands show a port's PoE power status, set the PoE power class it can supply, set its power priority (used when total demand exceeds the power budget), and enable or disable PoE on the port.

Show PoE Power Status

Privileged EXEC

Displays PoE power status for one or all interfaces.

SYNTAX

```
show power inline [<interface-type> <interface-id>]
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
`interface-type`	`varies by model`	Interface type keyword, e.g. gigabitethernet or extreme-ethernet (see note below).	—
`interface-id`	`slot/port`	Port number in slot/port form, e.g. 0/1.	—

EXAMPLE

```
qss# show power inline extreme-ethernet 0/1
```

EXAMPLE OUTPUT

```
qss# show power inline extreme-ethernet 0/1

PoE Port Info
-------------
Port Number       : 1
PoeAdminStatus    : Up
PoeStatus         : 0xa8
PowerConsumption  : 0.0 Watt
class             : NA
Operation mode    : PoE++
LegacyDetection   : Disable
Priority          : low
```

NOTES

- The interface type keyword depends on the switch model and port type — for example "gigabitethernet" or "extreme-ethernet" (abbreviation "ex"); "port-channel <n>" addresses a link-aggregation group. Type "?" after the command to list the interface types available on your switch.

Set PoE Power Mode

Interface configuration

Sets the PoE power class the interface can supply.

SYNTAX

```
power inline operationmode { poe | poe+ | poe++ }
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
operationmode	poe | poe+ | poe++	PoE power class the interface is allowed to supply.	poe++

EXAMPLE

```
qss(config-if)# power inline operationmode poe++
```

Set PoE Power Priority

Interface configuration

Sets the interface's PoE power priority, used when total demand exceeds the power budget.

SYNTAX

```
power inline priority { critical | high | low }
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
priority	critical | high | low	PoE power priority for this port, used when total demand exceeds the power budget.	low

EXAMPLE

```
qss(config-if)# power inline priority critical
```

Set Per-Port PoE

Interface configuration

Enables or disables PoE on the interface.

SYNTAX

```
power inline { auto | never }
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
inline	auto | never	Whether PoE is supplied automatically when a device is detected, or never supplied.	auto

EXAMPLE

```
qss(config-if)# power inline auto
```

PD alive

PD-alive monitoring watches whether the powered device (PD) connected to a PoE port is still responsive, and can automatically recover it. These commands configure the detection mode, recovery action, retry count, and recovery interval, and show the current PD-alive status.

Show PoE PD Alive Status

Privileged EXEC

Displays PoE PD-alive monitoring status for one or all interfaces.

SYNTAX

```
show poe pd-alive [<interface-type> <interface-id>]
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
interface-type	varies by model	Interface type keyword, e.g. gigabitethernet or extreme-ethernet (see note below).	—
interface-id	slot/port	Port number in slot/port form, e.g. 0/1.	—

EXAMPLE

```
qss# show poe pd-alive extreme-ethernet 0/1
```

EXAMPLE OUTPUT

```
qss# show poe pd-alive extreme-ethernet 0/1

PD Alive
--------
state    mode  neighbor                              status      action  reboot    recovery
                                                                         count     interval
-----    ----  --------                              ----------  ------  ------    --------
Disable  LLDP  No Neighbors                          Unprepared  Reboot  3         120
```

NOTES

- The interface type keyword depends on the switch model and port type — for example "gigabitethernet" or "extreme-ethernet" (abbreviation "ex"); "port-channel <n>" addresses a link-aggregation group. Type "?" after the command to list the interface types available on your switch.

Set PoE PD Alive

Interface configuration

Configures PD-alive monitoring: detection mode, action, retry count, and recovery interval.

SYNTAX

```
pd-alive [ state { enable | disable } ] [ mode { lldp | icmp <ip_addr> } ] [ action { alarm | reboot } ] [ reboot-count { unlimited | count <count (1-5)> } ] [ recovery-interval <recovery-interval (30-600)> ]
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
`state`	`enable | disable`	Enables or disables PD-alive monitoring on the interface.	`disable`
`mode`	`lldp | icmp`	Detection method: LLDP-based liveness, or ICMP ping to the PD's IP address (icmp requires the address below).	`lldp`
`ip_addr`	`IPv4 address`	IPv4 address to ping for ICMP-based PD-alive detection (used only when mode is icmp).	—
`action`	`alarm | reboot`	What to do when the PD is detected as unresponsive: raise an alarm, or reboot PoE power to the port.	`alarm`
`reboot-count`	`unlimited | count <1-5>`	How many failed detection attempts to allow before taking the configured action — "unlimited" never gives up, or set an exact count below.	`count (see below)`
`count`	`1-5`	How many failed detection attempts to allow before taking the configured action (used only when reboot-count is a specific count, not unlimited).	`3`
`recovery-interval`	`30-600`	How long to wait, in seconds, before retrying after taking the recovery action.	`120`

EXAMPLE

```
qss(config-if)# pd-alive state enable mode icmp 192.168.5.5 action reboot reboot-count count 3
recovery-interval 360
```

Continuous PoE

These commands enable or disable continuous PoE, which keeps power supplied to connected devices during a switch reboot, and show whether it is currently enabled.

Show Continuous PoE

Privileged EXEC

Displays whether continuous PoE (power retained during reboot) is enabled.

SYNTAX

```
show poe continuous-power
```

PARAMETERS

No parameters.

EXAMPLE

```
qss# show poe continuous-power
```

EXAMPLE OUTPUT

```
qss# show poe continuous-power

Continuous PoE : Disabled
```

Set Continuous PoE

Global configuration

Enables or disables continuous PoE power during a switch reboot.

SYNTAX

```
poe continuous-power
no poe continuous-power
```

PARAMETERS

No parameters.

EXAMPLE

```
qss(config)# poe continuous-power
```

8. Maintenance

This section provides commands used to monitor and maintain the system's operational status. These tools help users verify hardware functionality, perform diagnostic checks on network ports, and configure monitoring features to observe traffic behavior and interface activity.

IN THIS CHAPTER

LED

These commands set the front-panel LED mode, blink the locator LED for a set number of minutes to help identify a physical unit, and show the current LED configuration.

Set LED Mode

Global configuration

Sets the front-panel LED mode.

SYNTAX

```
led mode { normal | disabled | locator_on | locator_off }
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
mode	normal | disabled | locator_on | locator_off	Front-panel LED behavior: normal operation, disabled, or forced on/off as a locator.	normal

EXAMPLE

```
qss(config)# led mode normal
```

Set LED Blink

Global configuration

Blinks the front-panel locator LED for a set number of minutes.

SYNTAX

```
led blink <minute (1-30)>
no led blink
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
minute	1-30	How many minutes to blink the locator LED for.	30

EXAMPLE

```
qss(config)# led blink 1
```

Show LED Configuration

Privileged EXEC

Displays the current LED mode configuration.

SYNTAX

```
show env led
```

PARAMETERS

No parameters.

EXAMPLE

```
qss# show env led
```

EXAMPLE OUTPUT

```
qss# show env led


LED mode                        : normal

LED Blink Interval              : 30

LED Blink Enable                : 2
```

Cable diagnostics

This command runs cable diagnostics on an interface and displays the results, helping identify cabling faults without physical access to the link.

Show Cable Diagnostics

Privileged EXEC

Runs and displays cable diagnostics for an interface.

SYNTAX

```
show interface cable-diag <interface-type> <interface-id>
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
interface-type	varies by model	Interface type keyword, e.g. gigabitethernet or extreme-ethernet (see note below).	—
interface-id	slot/port	Port number in slot/port form, e.g. 0/1.	—

EXAMPLE

```
qss# show interface cable-diag extreme-ethernet 0/1
```

EXAMPLE OUTPUT

```
qss# show interface cable-diag extreme-ethernet 0/1

Local Pair  Pair length      Pair status
----------  -----------      -----------
    A           0            OPEN
    B           0            OPEN
    C           0            OPEN
    D           0            OPEN
```

NOTES

- The interface type keyword depends on the switch model and port type — for example "gigabitethernet" or "extreme-ethernet" (abbreviation "ex"); "port-channel <n>" addresses a link-aggregation group. Type "?" after the command to list the interface types available on your switch.

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.

Set Port Mirroring Source

Global configuration

Sets the source interface and traffic direction for port mirroring.

SYNTAX

```
monitor port-mirroring source interface <interface-type> <interface-id> [{ rx | tx | both }]
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
interface-type	varies by model	Interface type keyword, e.g. gigabitethernet or extreme-ethernet (see note below).	—
interface-id	slot/port	Port number in slot/port form, e.g. 0/1.	—
direction	rx | tx | both	Which direction of traffic on the source interface to mirror (optional).	—

EXAMPLE

```
qss(config)# monitor port-mirroring source interface gigabitethernet 0/2
```

NOTES

- The interface type keyword depends on the switch model and port type — for example "gigabitethernet" or "extreme-ethernet" (abbreviation "ex"); "port-channel <n>" addresses a link-aggregation group. Type "?" after the command to list the interface types available on your switch.

Set Port Mirroring Destination

Global configuration

Sets the destination interface that receives mirrored traffic.

SYNTAX

```
monitor port-mirroring destination interface <interface-type> <interface-id>
no monitor port-mirroring destination interface <interface-type> <interface-id>
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
interface-type	varies by model	Interface type keyword, e.g. gigabitethernet or extreme-ethernet (see note below).	—
interface-id	slot/port	Port number in slot/port form, e.g. 0/1.	—

EXAMPLE

```
qss(config)# monitor port-mirroring destination interface gigabitethernet 0/1
```

NOTES

- The interface type keyword depends on the switch model and port type — for example "gigabitethernet" or "extreme-ethernet" (abbreviation "ex"); "port-channel <n>" addresses a link-aggregation group. Type "?" after the command to list the interface types available on your switch.

Set Port Mirroring

Global configuration

Enables or disables port mirroring switch-wide.

SYNTAX

```
set port-mirroring { enable | disable }
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
port-mirroring	enable | disable	Enables or disables port mirroring switch-wide.	—

EXAMPLE

```
qss(config)# set port-mirroring enable
```

Show ACL Mirroring Session

Privileged EXEC

Displays the ACL mirroring session configuration.

SYNTAX

```
show monitor session <session-id (2-7)>
```

RELATED COMMANDS

Set IP Access Group, Show Access Lists

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
session-id	2-7	Mirroring session ID.	—

EXAMPLE

```
qss# show monitor session 2
```

EXAMPLE OUTPUT

Output from a switch with no port-mirroring session configured.

```
qss# show monitor session 2

Mirroring is globally Enabled.
% Session 2 does not exist
```

NOTES

- ACL mirroring rules themselves are configured under Security → ACL, not here.

Show Port Mirroring Status

Privileged EXEC

Displays the port mirroring configuration and status.

SYNTAX

```
show monitor port-mirroring
```

PARAMETERS

No parameters.

EXAMPLE

```
qss# show monitor port-mirroring
```

EXAMPLE OUTPUT

Output from a switch with no port-mirroring sessions configured.

```
qss# show monitor port-mirroring

% Session 1 does not exist
```

DDM

Digital diagnostic monitoring (DDM) enables per-port optical/transceiver health monitoring by reading physical sensor values (such as temperature, voltage, current, and optical power) and applying configured thresholds so the switch can report or alarm when conditions exceed safe limits.

Show DDM Status

Privileged EXEC

Displays digital diagnostic monitoring (DDM) status for one or all interfaces.

SYNTAX

```
show interfaces ddm status [<interface-type> <interface-id>]
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
`interface-type`	`varies by model`	Interface type keyword, e.g. gigabitethernet or extreme-ethernet (see note below).	—
`interface-id`	`slot/port`	Port number in slot/port form, e.g. 0/1.	—

EXAMPLE

```
qss# show interfaces ddm status extreme-ethernet 0/1
```

EXAMPLE OUTPUT

```
qss# show interfaces ddm status extreme-ethernet 0/1

Port      Temperature(C)    Voltage(V)    BiasCurrent(mA)    TxPower(mW)    RxPower(mW)
----      --------------    ----------    ---------------    -----------    -----------
Ex0/1     0.000             0.000         0.000              0.000          0.000
```

NOTES

- The interface type keyword depends on the switch model and port type — for example "gigabitethernet" or "extreme-ethernet" (abbreviation "ex"); "port-channel <n>" addresses a link-aggregation group. Type "?" after the command to list the interface types available on your switch.

Show DDM Configuration

Privileged EXEC

Displays digital diagnostic monitoring (DDM) threshold configuration.

SYNTAX

```
show interfaces ddm config [<interface-type> <interface-id>]
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
`interface-type`	`varies by model`	Interface type keyword, e.g. gigabitethernet or extreme-ethernet (see note below).	—
`interface-id`	`slot/port`	Port number in slot/port form, e.g. 0/1.	—

EXAMPLE

```
qss# show interfaces ddm config extreme-ethernet 0/1
```

EXAMPLE OUTPUT

```
qss# show interfaces ddm config extreme-ethernet 0/1

Port      Monitoring    Type      LoAlarm    LoWarn    HiWarn    HiAlarm
----      ----------    ----      -------    ------    ------    -------
Ex0/1     Disabled      TEMP      -          -         -         -
                        VCC       -          -         -         -
                        TX_BIAS   -          -         -         -
                        TX_POWER  -          -         -         -
                        RX_POWER  -          -         -         -
```

NOTES

- The interface type keyword depends on the switch model and port type — for example "gigabitethernet" or "extreme-ethernet" (abbreviation "ex"); "port-channel <n>" addresses a link-aggregation group. Type "?" after the command to list the interface types available on your switch.

Set DDM

Interface configuration

Enables or disables digital diagnostic monitoring (DDM) on the interface.

SYNTAX

```
ddm { disable | enable }
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
ddm	disable | enable	Enables or disables digital diagnostic monitoring on the interface.	disable

EXAMPLE

```
qss(config-if)# ddm enable
```

Set DDM Thresholds

Interface configuration

Sets high-alarm, high-warning, low-warning, and low-alarm thresholds for a monitored DDM parameter.

SYNTAX

```
ddm { Temperature | Voltage | Current | Tx_power | Rx_power } <HiAlarm (float)> <HiWarn (float)>
<LoWarn (float)> <LoAlarm (float)>
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
monitored value	Temperature | Voltage | Current | Tx_power | Rx_power	Which transceiver reading the thresholds apply to.	—
HiAlarm	float	High-alarm threshold.	not set
HiWarn	float	High-warning threshold.	not set
LoWarn	float	Low-warning threshold.	not set
LoAlarm	float	Low-alarm threshold.	not set

EXAMPLE

```
qss(config-if)# ddm Temperature 80 70 0 -10
```

NOTES

- Value ranges depend on the monitored type: Temperature -128 to 128°C (negative values allowed); Voltage 0 to 6.5535 V; Current 0 to 131 mA; Tx_power and Rx_power 0 to 6.5535 mW each.
- Negative values are rejected for Voltage, Current, Tx_power, and Rx_power.

Console timeout

These commands enter line console configuration mode and set how long an idle console session stays open before it times out.

Set Line Console Mode

Global configuration

Enters line console configuration mode.

SYNTAX

```
line console
```

PARAMETERS

No parameters.

EXAMPLE

```
qss(config)# line console
```

Set Console Timeout

Line configuration

Sets how long the console session stays open before it times out.

SYNTAX

```
exec-timeout <seconds (1-18000)>
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
seconds	1-18000	How long the console session stays open before it times out, in seconds.	—

EXAMPLE

```
qss(config-line)# exec-timeout 300
```

Dual image & firmware upgrade

The switch keeps two firmware images so it can fail over or be rolled back. These commands show which image is active and which will boot next, set the next-boot image, and upgrade the firmware from a remote FTP or HTTP server.

Show Boot Image

Privileged EXEC

Displays both firmware images' version, status (Active/Disabled), created date, and which image boots next.

SYNTAX

```
show boot image [{ image1 | image2 }]
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
image	image1 | image2	Limits the display to one firmware image slot (optional; shows both when omitted).	—

EXAMPLE

```
qss# show boot image
```

EXAMPLE OUTPUT

```
qss# show boot image

Firmware Image Information
==========================
Image   Status    NextBoot  Version         Created Date
--------------------------------------------------------------------------
image1  Active    yes       4.5.0           Tue, 08 Sep 2026 01:21:09 +0800
image2  Disabled  -         4.4.5           Tue, 16 Jun 2026 06:16:40 +0800
```

FIELD	MEANING
Image	Firmware image slot: image1 or image2.
Status	"Active" if this slot is the one currently running; "Disabled" for the standby slot.
NextBoot	"yes" if this slot is set to boot next (see "boot system"); "-" otherwise.
Version	Firmware version installed in this slot.
Created Date	Date and time this firmware image was installed.

Set Boot Image

Privileged EXEC

Sets which firmware image the switch boots next.

SYNTAX

```
boot system { image1 | image2 }
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
system	image1 | image2	Which firmware image to boot from next.	—

EXAMPLE

```
qss# boot system image2
```

Upgrade Firmware

Privileged EXEC

Upgrades the switch firmware from an FTP or HTTP server.

SYNTAX

```
firmware upgrade { ftp://<user-name>:<pass-word>@<ip_addr>/<filename> | http://<user-name>:<pass-word>@<ip_addr>/<filename> } [image { image1 | image2 }]
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
user-name	up to 20 characters	Username for the FTP/HTTP upgrade server.	—
pass-word	up to 20 characters	Password for the FTP/HTTP upgrade server.	—
ip_addr	IPv4 address	IPv4 address of the FTP/HTTP upgrade server.	—
filename	file name/path	File name/path on the server.	—
image	image1 | image2	Firmware slot to write the upgrade to; if omitted, the standby (inactive) slot is used.	—

EXAMPLE

```
qss# firmware upgrade http://test:pswd@192.0.2.1/QSW-FW.img image image2
```

NOTES

- If [image] is omitted, the firmware is written to the standby slot (the image not currently booted): when booting from image2 it writes image1, and vice versa.
- After a successful upgrade, boot defaults to the newly written (backup) partition, so the switch boots the new firmware on next reboot.
- Use "show boot image" to check the current boot image and "boot system" to change it.

NIC compatibility

These commands enable or disable NIC compatibility mode on an interface, which raises the inter-packet gap to work around a dropped-packet issue on some Intel NICs, and show the current setting.

Show NIC Compatibility

Privileged EXEC

Displays NIC compatibility mode status for one or all interfaces.

SYNTAX

```
show interfaces nic-compatibility [<interface-type> <interface-id>]
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
interface-type	varies by model	Interface type keyword, e.g. gigabitethernet or extreme-ethernet (see note below).	—
interface-id	slot/port	Port number in slot/port form, e.g. 0/1.	—

EXAMPLE

```
qss# show interfaces nic-compatibility extreme-ethernet 0/1
```

EXAMPLE OUTPUT

```
qss# show interfaces nic-compatibility extreme-ethernet 0/1

Port            IPG    NIC-Compatibility
----            ---    -----------------
Ex0/1           12     Disabled
```

NOTES

- The interface type keyword depends on the switch model and port type — for example "gigabitethernet" or "extreme-ethernet" (abbreviation "ex"); "port-channel <n>" addresses a link-aggregation group. Type "?" after the command to list the interface types available on your switch.

Set NIC Compatibility

Interface configuration

Enables or disables NIC compatibility mode, which raises the inter-packet gap to work around a dropped-packet issue on the Intel i219 NIC.

SYNTAX

```
nic-compatibility { enable | disable }
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
nic-compatibility	enable | disable	Enables or disables NIC compatibility mode on the interface.	disable

EXAMPLE

```
qss(config-if)# nic-compatibility enable
```

Syslog server

These commands add, update, remove, and show remote syslog server entries, including optional protocol, port, facility, severity filter, and timestamp settings, so switch log messages can be centralized on an external server.

Show Syslog Servers

Privileged EXEC

Displays all configured remote syslog server entries: address, host name, protocol, port, facility, severity, and timestamp setting.

SYNTAX

```
show system-log-server
```

PARAMETERS

No parameters.

EXAMPLE

```
qss# show system-log-server
```

EXAMPLE OUTPUT

Output from a switch with no syslog server configured — no column headers are shown in this state; the expected fields are address, host name, protocol, port, facility, severity, and timestamp.

```
qss# show system-log-server

System Log Server (0/5 configured)
No system log server configured.
```

Set Syslog Server

Global configuration

Adds or updates a remote syslog server, with optional protocol, port, facility, severity filter, and timestamp settings.

SYNTAX

```
system-log-server { ipv4 <ucast_addr> | ipv6 <ip6_addr> } host-name <host-name (20)> [protocol { udp | tcp | tls }] [port <port (1-65535)>] [facility { local0 | local1 | local2 | local3 | local4 | local5 | local6 | local7 }] [severity { info | warning | error }] [timestamp { enable | disable }]
no system-log-server { ipv4 <ucast_addr> | ipv6 <ip6_addr> }
```

PARAMETERS

PARAMETER	VALUES / RANGE	MEANING	DEFAULT
ucast_addr	IPv4 address	Syslog server IPv4 address.	—
ip6_addr	IPv6 address	Syslog server IPv6 address.	—
host-name	20	A label identifying this syslog server entry (shown in the server list; not resolved as a DNS name).	—
protocol	udp | tcp | tls	Transport protocol used to send log messages to the server.	—
port	1-65535	UDP/TCP port the syslog server listens on.	—
facility	local0 | local1 | local2 | local3 | local4 | local5 | local6 | local7	Syslog facility value tagged on messages sent to this server.	—
severity	info | warning | error	Minimum severity to send: this level and everything more severe (e.g. "warning" also sends "error").	info
timestamp	enable | disable	Includes a timestamp in each message sent to this server.	—

EXAMPLE

```
qss(config)# system-log-server ipv4 10.10.20.5 host-name CentralLog protocol udp port 514 facility local0 severity info timestamp enable
```

NOTES

- Severity acts as a threshold filter: logs at the specified level and above are sent (e.g. severity warning sends warning and error).
- When severity is omitted, the default is info, which sends logs of every severity level.
- The `no` form (`no system-log-server { ipv4 <ucast_addr> | ipv6 <ip6_addr> }`) removes a previously configured server entry, identified by address alone.

9. Error Messages

This chapter covers the messages of the general command parser and of the DHCP relay, ACL, DNS and ARP subsystems, each table in the order the tables are documented (not alphabetical). If you already have the on-screen message text, use the Error Message Index instead — it lists every message alphabetically.

IN THIS CHAPTER

General CLI Errors

These four messages can appear from any CLI mode, whenever the input itself is malformed.

MESSAGE	TRIGGER	EXAMPLE

`% Invalid input detected at '^' marker`	The command does not match the expected input format.	`qss(config)# vlan 123143`
		`vlan 123143`
		`^`
		`% Invalid input detected at '^' marker`

`% Ambiguous Command`	More than one command could match; the input is too ambiguous to resolve automatically.	`qss# show system-?`
		`system-information`
		`system-log-server`
		`qss# show system-`
		`% Ambiguous Command`

`% Incomplete command.`	A required parameter is missing.	`qss(config)# set port-mirr`
		`CONFIGURE commands :  set port-mirroring {enable | disable}`
		`qss(config)# set port-mirroring`
		`% Incomplete command.`

`% Invalid Command`	The command is invalid (no close match found).	`qss# showww` `% Invalid Command`

DHCP Relay Errors and Warnings

These messages are specific to configuring and operating the DHCP relay agent, both globally and per VLAN.

These per-VLAN settings give no message if they fail to apply: Set DHCP Relay Admin Status (VLAN), Set DHCP Relay Source Address (VLAN), Set DHCP Relay Option 82 Override (VLAN), Set DHCP Relay Option 82 Policy (VLAN), Set DHCP Relay Circuit ID Format (VLAN) and Set DHCP Relay Remote ID Format (VLAN).

MESSAGE	TRIGGER	COMMAND	MODE	RELATED
`% errCode 3324: DHCP server is active; disable dhcp-server before enabling relay`	DHCP server is still enabled when relay is enabled (server/relay mutual-exclusion pre-check).	`service dhcp-relay`	Global Configuration Mode	Set DHCP Server
`% Failed to start the DHCP Relay on this context.`	Global relay startup failed (for example, a hard dependency such as DHCP Snooping not being ready).	`service dhcp-relay`	Global Configuration Mode	
`% DHCP Relay requires global DHCP Snooping. Enable it with "ip dhcp snooping" first.`	Global relay startup failed because global DHCP Snooping is not enabled.	`service dhcp-relay`	Global Configuration Mode	Set DHCP Snooping (Global)
`% Maximum relay instances reached; Relay configurations cannot be done on this context`	The maximum number of relay context instances has been reached.	`service dhcp-relay`	Global Configuration Mode	
`% Failed to Disable the DHCP Relay on this context.`	Global relay disable failed.	`no service dhcp-relay`	Global Configuration Mode	
`WARNING: When RAI is enabled, the circuit-id needs to be configured explicitly by user`	Shown after enabling RAI (Option 82) as a reminder to configure circuit-id manually (warning only, not blocking). "Configure circuit-id" corresponds to the "ip dhcp relay circuit-id format" command (global or per-VLAN).	`ip dhcp relay information option`	Global Configuration Mode	
`% Failed to set global policy`	Global Option 82 policy configuration failed.	`ip dhcp relay information policy { keep | drop | replace }`	Global Configuration Mode	
`% Failed to set global circuit-id format`	Global circuit-id format configuration failed.	`ip dhcp relay circuit-id format { vlan-port | custom <custom-string (64)> }`	Global Configuration Mode	
`% Failed to set global remote-id format`	Global remote-id format configuration failed.	`ip dhcp relay remote-id format { mac | custom <custom-string (64)> }`	Global Configuration Mode	

MESSAGE	TRIGGER	COMMAND	MODE	RELATED
`% Invalid VRF`	The named context does not exist — only "default" exists.	`Any relay command carrying [vrf <vrf-name>]`	Global Configuration Mode	
`% This command applies to VLAN interfaces only`	The command was entered on a physical port; it applies to VLAN interfaces only.	`ip dhcp relay enable`	Interface Configuration Mode (VLAN)	
`% Invalid Command`	The command was entered on a LAG (port-channel) interface; it is not registered in port-channel mode, so the CLI returns a generic message.	`ip dhcp relay enable`	Interface Configuration Mode (port-channel)	
`% Failed to enable DHCP relay on VLAN <N>`	Per-VLAN relay enable failed (for example, a relay rule already exists on this VLAN).	`ip dhcp relay enable`	Interface Configuration Mode (VLAN)	
`% DHCP Relay on VLAN <N> requires DHCP Snooping on the same VLAN. Enable it with "ip dhcp snooping vlan <N>" first.`	Per-VLAN relay enable failed because DHCP Snooping is not enabled on this VLAN.	`ip dhcp relay enable`	Interface Configuration Mode (VLAN)	Set DHCP Snooping VLANs
`% Failed to disable DHCP relay on VLAN <N>`	Per-VLAN relay disable (rule deletion) failed.	`no ip dhcp relay enable`	Interface Configuration Mode (VLAN)	
`% Failed to add server on VLAN <N>`	Adding a per-VLAN DHCP server failed.	`ip dhcp relay server <ucast_addr>`	Interface Configuration Mode (VLAN)	
`% Failed to remove server on VLAN <N>`	Removing a per-VLAN DHCP server failed.	`no ip dhcp relay server <ucast_addr>`	Interface Configuration Mode (VLAN)	

ACL Errors

These messages appear when creating or applying IPv4, IPv6, or MAC access control lists.

MESSAGE	TRIGGER	COMMAND	MODE
`% Access-list 9999 does not exist.`	The access-list number is within the valid range but does not exist.	`no ip access-list extended 9999`	Global Configuration Mode
`% Access-list <n> rule redefined`	A rule already exists for this access-list number; the new rule overwrites the previous one.	`permit/deny ...`	ACL Extended Access List Configuration Mode

DNS Errors

This message appears when removing a DNS server entry that isn't configured.

MESSAGE	TRIGGER	COMMAND	MODE	RELATED
`% Name Server entry does not exist.`	The specified name-server entry does not exist.	`no ip name-server 8`	Global Configuration Mode	Set DNS Server (IPv4/IPv6), Set DNS Server (IPv4)

ARP Errors

These messages appear when configuring static ARP entries or Dynamic ARP Inspection (DAI).

MESSAGE	TRIGGER	COMMAND	MODE
`% ARP entry addition failed`	Static ARP IP configuration failed.	`arp <ip-address> <hardware-address> vlan <vlan-id (1-4094)>`	Global Configuration Mode
`% Invalid next hop address specified`	The static ARP IP address is not within the specified VLAN's subnet.	`arp <ip-address> <hardware-address> vlan <vlan-id (1-4094)>`	Global Configuration Mode

10. Customer Support

Contact QNAP Customer Service when you need help diagnosing or resolving a problem with your switch.

Contact QNAP Support

Go to the QNAP Customer Service portal, sign in with your QNAP ID, and select **Service Portal** to create and submit a support ticket.

Before You Submit a Ticket

Include the following information so QNAP Support can understand and reproduce the problem:

- Switch model and serial number
- Firmware version and build number
- A clear description of the problem and its effect
- The exact steps and CLI commands that reproduce it
- The complete error message or unexpected output
- Relevant configuration details, logs, and screenshots

> **Protect credentials.** Remove passwords, private keys, access tokens, and other credentials before attaching command output, configuration files, logs, or screenshots.

Appendix A. Command Index

An alphabetical index of every CLI command's syntax, by its primary (positive) form, with the page where it's documented in this manual.

F

G

No commands.

H

I

J

No commands.

K

No commands.

L

M

N

O

P

Q

R

S

T

No commands.

U

V

W

No commands.

X

No commands.

Y

No commands.

Z

No commands.

Appendix B. Error Message Index

An alphabetical index of every message in the Error Messages chapter (chapter 9), sorted by the on-screen Message string — ignoring its leading `%`, `%%`, or `WARNING:` marker — with the command that triggers it and the page where its row is documented.

P

No messages.

Q

No messages.

R

No messages.

S

No messages.

T

U

No messages.

V

No messages.

W

X

No messages.

Y

No messages.

Z

No messages.