

# **Configuring Interfaces**

This chapter provides information about interfaces and how to configure interfaces.

- Finding Feature Information, on page 2
- Feature History for Interfaces, on page 3
- Information About Interfaces, on page 5
- Prerequisites for Interfaces, on page 32
- Guidelines and Limitations, on page 33
- Default Settings, on page 36
- Configuring Interfaces, on page 37
- Verifying Interface Configuration, on page 60
- Transmit-Wait History Graph, on page 92

## **Finding Feature Information**

Your software release might not support all the features documented in this module. For the latest caveats and feature information, see the Bug Search Tool at https://tools.cisco.com/bugsearch/ and the release notes for your software release.

#### **Guidelines and Recommendations :**

- FEC on Cisco MDS 9000 Series switches should be disabled on 16 Gbps links.
- Ensure that enough buffer credits are configured on MDS ports to cover the distance for the specific frame size.
- Use logical link bundling via port channels across DWDM links even in case of different path lengths. The superior technology of port channels to any other logical bundling solution in the industry makes this possible and provides the benefit of higher reliability without impacting FSPF routing decisions.
- Check with your DWDM vendor for specific configurations and setting, specifically for NOS/LOS propagation.

To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the New and Changed chapter or the Feature History table below.

# **Feature History for Interfaces**

Table 1: New and Changed Features, on page 3 lists the New and Changed features.

#### **Table 1: New and Changed Features**

Feature Name	Release	Feature Information		
Interfaces and Port Channels				
Display SFP power control and status	9.4(2)	Added FC SFP power control and status		
Display SFP descriptions and Parameters	9.4(2)	Added support to display SFP descriptions and Parameters for Fibre Channel ports		
Port Beaconing	8.4(1)	This feature is supported on Cisco MDS switches that are operating in Cisco NPV mode.		
Port Monitor	8.4(1)	Added support to configure a logging severity level for port monitor syslog messages.		
Interfaces	8.4(1)	Fixed the output formatting of the <b>show logging onboard txwait</b> command.		
Port Beaconing	8.3(1)	This feature can be used to identify individual switch and directly attached peer ports in a data center environment.		
		The following command was introduced:		
		beacon interface fc <i>slot/port</i> {both   local   peer} [status {normal   warning   critical}] [duration <i>seconds</i> ] [frequency <i>number</i> ]		
Interface Modes	8.1(1)	The link connecting from a core switch to a Cisco N-Port Virtualizer (NPV) switch must be treated as an ISL (core port) in interfaces and port channels. Port monitor may take portguard action on the link if it is treated as an edge port, which will result in the loss of connectivity to the devices that are connected to the Cisco NPV switch.		
		The following command was introduced:		
		switchport logical-type {auto   core   edge}		
Port Monitor				

Feature Name	Release	Feature Information
Port Monitor Policy	8.5(1)	A new port monitor portguard action (cong-isolate-recover) was introduced for the credit-loss-reco, tx-credit-not-available, tx-slowport-oper-delay, and txwait counters.
		The <i>cong-isolate-recover</i> portguard action was added to the following commands:
		• counter credit-loss-reco
		• counter tx-credit-not-available
		• counter tx-slowport-oper-delay
		• counter tx-wait
Port Monitor	8.1(1)	The <b>port-type</b> { <b>access-port</b>   <b>trunks</b>   <b>all</b> } command was replaced with the <b>logical-type</b> { <b>core</b>   <b>edge</b>   <b>all</b> } command, where <b>port-type</b> was replaced with <b>logical-type</b> , <b>access-port</b> was replaced with <b>edge</b> , and <b>trunks</b> was replaced with <b>core</b> .
		The following command was modified:
		logical-type {core   edge   all}
Port Monitor Policy	8.1(1)	A new port monitor portguard action (cong-isolate) was introduced for the credit-loss-reco, tx-credit-not-available, tx-slowport-oper-delay, and txwait counters.
		The <i>cong-isolate</i> portguard action was added to the following commands:
		• counter credit-loss-reco
		• counter tx-credit-not-available
		• counter tx-slowport-oper-delay
		• counter tx-wait

## Information About Interfaces

The main function of a switch is to relay frames from one data link to another. To relay the frames, the characteristics of the interfaces through which the frames are received and sent must be defined. The configured interfaces can be Fibre Channel interfaces, Gigabit Ethernet interfaces, the management interface (mgmt0), or VSAN interfaces.

## **Interface Description**

For Fibre Channel interfaces, you can configure the description parameter to provide a recognizable name for an interface. Using a unique name for each interface allows you to quickly identify an interface when you are looking at a listing of multiple interfaces. You can also use the description to identify the traffic or the use for a specific interface.

## **Interface Modes**

Each physical Fibre Channel interface in a switch may operate in one of several port modes: E port, F port, FL port, TL port, TE port, SD port, and ST port (see Figure 1: Cisco MDS 9000 Series Switch Port Modes, on page 5). Besides these modes, each interface may be configured in auto or Fx port modes. These two modes determine the port type during interface initialization.





**Note** Interfaces are created in VSAN 1 by default. For more information about VSAN, see the Cisco MDS 9000 Series NX-OS Fabric Configuration Guide.

Each interface has an associated administrative configuration and an operational status:

• The administrative configuration does not change unless you modify it. This configuration has various attributes that you can configure in administrative mode.

• The operational status represents the current status of a specified attribute, such as the interface speed. This status cannot be changed and is read-only. Some values, for example, operational speed, may not be valid when the interface is down.

**Note** When a module is removed and replaced with the same type of module, the original configuration is retained. If a different type of module is inserted, the original configuration is no longer retained.

#### E Port

In expansion port (E port) mode, an interface functions as a fabric expansion port. This port can be connected to another E port to create an Inter-Switch Link (ISL) between two switches. E ports carry frames between switches for configuration and fabric management. They serve as a conduit between switches for frames destined for remote N ports and NL ports. E ports support Class 2, Class 3, and Class F services.

An E port connected to another switch can also be configured to form a port channel. For more details about configuring a port channel, see Configuring Port Channels.

#### F Port

In fabric port (F port) mode, an interface functions as a fabric port. This port can be connected to a peripheral device (host or disk) operating as an N port. An F port can be attached to only one N port. F ports support Class 2 and Class 3 services.

### FL Port

In fabric loop port (FL port) mode, an interface functions as a fabric loop port. This port can be connected to one or more NL ports (including FL ports in other switches) to form a public, arbitrated loop. If more than one FL port is detected on the arbitrated loop during initialization, only one FL port becomes operational and the other FL ports enter nonparticipating mode. FL ports support Class 2 and Class 3 services.

### **NP Ports**

An NP port is a port on a device that is in NPV mode and connected to the core switch via an F port. NP ports function like N ports, except that in addition to providing N port operations, they also function as proxies for multiple physical N ports.

For more details about NP ports and NPV, see Configuring N Port Virtualization .

### TE Port

In trunking E port (TE port) mode, an interface functions as a trunking expansion port. It can be connected to another TE port to create an extended ISL (EISL) between two switches. TE ports are specific to Cisco MDS 9000 Series Multilayer Switches. These switches expand the functionality of E ports to support the following:

- VSAN trunking
- Transport quality of service (QoS) parameters
- Fibre Channel trace (fctrace) feature

I

	In TE port mode, all the frames are transmitted in EISL frame format, which contains VSAN information. Interconnected switches use the VSAN ID to multiplex traffic from one or more VSANs across the same physical link. This feature is referred to as trunking in the Cisco MDS 9000 Series Multilayer Switches. For more details about trunking, see Configuring Trunking. TE ports support Class 2, Class 3, and Class F services.
TF Port	
	In trunking F port (TF port) mode, an interface functions as a trunking expansion port. It can be connected to another trunked N port (TN port) or trunked NP port (TNP port) to create a link between a core switch and an NPV switch or an host bus adapter (HBA) in order to carry tagged frames. TF ports are specific to Cisco MDS 9000 Series Multilayer Switches. They expand the functionality of F ports to support VSAN trunking.
	In TF port mode, all the frames are transmitted in EISL frame format, which contains VSAN information. Interconnected switches use the VSAN ID to multiplex traffic from one or more VSANs across the same physical link. This feature is referred to as trunking in the Cisco MDS 9000 Series Multilayer Switches. For more details about trunking, see Configuring Trunking. TF ports support Class 2, Class 3, and Class F services.
TNP Port	
	In trunking NP port (TNP port) mode, an interface functions as a trunking expansion port. It can be connected to a trunked F port (TF port) to create a link to a core NPIV switch from an NPV switch in order to carry tagged frames.
SD Port	
	In SPAN destination port (SD port) mode, an interface functions as a switched port analyzer (SPAN). The SPAN feature is specific to switches in the Cisco MDS 9000 Series. It monitors network traffic that passes though a Fibre Channel interface. This is done using a standard Fibre Channel analyzer (or a similar switch probe) that is attached to an SD port. SD ports do not receive frames; they only transmit a copy of the source traffic. The SPAN feature is non-intrusive and does not affect switching of network traffic in SPAN source ports. For more details about SPAN, see the Cisco MDS 9000 Series NX-OS System Management Configuration Guide.
ST Port	
	In the SPAN tunnel port (ST port) mode, an interface functions as an entry point port in the source switch for the RSPAN Fibre Channel tunnel. The ST port mode and the remote SPAN (RSPAN) feature are specific to switches in the Cisco MDS 9000 Series Multilayer Switches. When configured in ST port mode, the interface cannot be attached to any device, and thus cannot be used for normal Fibre Channel traffic. For more details about SPAN, see the Cisco MDS 9000 Series NX-OS System Management Configuration Guide.
Fx Port	
	Interfaces configured as Fx ports can operate in either F port mode or FL port mode. The Fx port mode is determined during interface initialization depending on the attached N port or NL port. This administrative configuration disallows interfaces to operate in any other mode, for example, preventing an interface to connect to another switch.
Auto Mode	
	Interfaces configured in auto mode can operate in F port, FL port, E port, TE port, or TF port mode. The port mode is determined during interface initialization. For example, if the interface is connected to a node (host or disk), it operates in F port mode or FL port mode depending on the N port mode or NL port mode. If the

interface is attached to a third-party switch, it operates in E port mode. If the interface is attached to another switch in the Cisco MDS 9000 Series Multilayer Switches, it may become operational in TE port mode. For more details about trunking, see Configuring Trunking.

TL ports and SD ports are not determined during initialization and are administratively configured.

## **Interface States**

An interface state depends on the administrative configuration of the interface and the dynamic state of the physical link.

### **Administrative States**

The administrative state refers to the administrative configuration of the interface, as described in Table 2: Administrative States, on page 8.

#### Table 2: Administrative States

Administrative State	Description
Up	Interface is enabled.
Down	Interface is disabled. If you administratively disable an interface by shutting down that interface, the physical link layer state change is ignored.

#### **Operational States**

Operational state indicates the current operational state of an interface, as described in Table 3: Operational States , on page 8.

#### Table 3: Operational States

Operational State	Description
Up	Interface is transmitting or receiving traffic, as required. To be in this state, an interface must be administratively up, the interface link layer state must be up, and the interface initialization must be completed.
Down	Interface cannot transmit or receive (data) traffic.
Trunking	Interface is operational in TE mode or TF mode.

#### **Reason Codes**

Reason codes are dependent on the operational state of an interface, as described in Table 4: Reason Codes for Interface States, on page 8.

 Table 4: Reason Codes for Interface States

Administrative Configuration	Operational Status	Reason Code
Up	Up	None.

Administrative Configuration	Operational Status	Reason Code
Down	Down	Administratively down—If you administratively configure an interface as down, you disable the interface. No traffic is received or transmitted.
Up	Down	See Table 5: Reason Codes for Nonoperational States , on page 10. Note that only some of the reason codes are listed in Table 5: Reason Codes for Nonoperational States , on page 10.

**Note** Only some of the reason are listed in the table.

If the administrative state is up and the operational state is down, the reason code differs based on the nonoperational reason code, as described in Table 5: Reason Codes for Nonoperational States, on page 10.

I

Reason Code (Long Version)	Description	Applicable Modes
Link failure or not connected	The physical layer link is not operational.	All
SFP not present	The small form-factor pluggable (SFP) hardware is not plugged in.	-
Initializing	The physical layer link is operational and the protocol initialization is in progress.	-
Reconfigure fabric in progress	The fabric is currently being reconfigured.	
Offline	The Cisco NX-OS software waits for the specified R_A_TOV time before retrying initialization.	-
Inactive	The interface VSAN is deleted or is in a suspended state.	
	To make the interface operational, assign that port to a configured and active VSAN.	
Hardware failure	A hardware failure is detected.	
Error disabled	Error conditions require administrative attention. Interfaces may be error-disabled for various reasons:	
	Configuration failure	
	• Incompatible buffer-to-buffer credit configuration	
	To make the interface operational, you must first fix the error conditions causing this state, and administratively shut down or enable the interface.	
Fibre Channel redirect failure	A port is isolated because a Fibre Channel redirect is unable to program routes.	-
No port activation license available	A port is not active because it does not have a port license.	1
SDM failure	A port is isolated because SDM is unable to program routes.	

#### Table 5: Reason Codes for Nonoperational States

Reason Code (Long Version)	Description	Applicable Modes
Isolation due to ELP failure	The port negotiation failed.	Only E
Isolation due to ESC failure	The port negotiation failed.	TE ports
Isolation due to domain overlap	The Fibre Channel domains (fedomain) overlap.	
Isolation due to domain ID assignment failure	The assigned domain ID is not valid.	
Isolation due to the other side of the link E port isolated	The E port at the other end of the link is isolated.	
Isolation due to invalid fabric reconfiguration	The port is isolated due to fabric reconfiguration.	
Isolation due to domain manager disabled	The fcdomain feature is disabled.	
Isolation due to zone merge failure	The zone merge operation failed.	
Isolation due to VSAN mismatch	The VSANs at both ends of an ISL are different.	
Nonparticipating	FL ports cannot participate in loop operations. This might occur if more than one FL port exists in the same loop, in which case, all but one FL port in that loop automatically enters nonparticipating mode.	Only FL ports and TL ports
Port Channel administratively down	The interfaces belonging to a port channel are down.	Only port
Suspended due to incompatible speed	The interfaces belonging to a port channel have incompatible speeds.	interfaces
Suspended due to incompatible mode	The interfaces belonging to a port channel have incompatible modes.	
Suspended due to incompatible remote switch WWN	An improper connection is detected. All interfaces in a port channel must be connected to the same pair of switches.	

## **Graceful Shutdown**

Interfaces on a port are shut down by default (unless you modified the initial configuration).

The Cisco NX-OS software implicitly performs a graceful shutdown in response to either of the following actions for interfaces operating in the E port mode:

- If you shut down an interface.
- If a Cisco NX-OS software application executes a port shutdown as part of its function.

A graceful shutdown ensures that no frames are lost when the interface is shutting down. When a shutdown is triggered either by you or the Cisco NX-OS software, the switches connected to the shutdown link coordinate with each other to ensure that all the frames in the ports are safely sent through the link before shutting down. This enhancement reduces the chance of frame loss.

A graceful shutdown is not possible in the following situations:

- If you physically remove the port from the switch.
- If In-Order Delivery (IOD) is enabled. For more details about IOD, see Cisco MDS 9000 Series NX-OS Fabric Configuration Guide.
- If the Min\_LS\_interval interval is higher than 10 seconds. For information about Fabric Shortest Path First (FSPF) global configuration, see Cisco MDS 9000 Series NX-OS Fabric Configuration Guide

- Note
  - This feature is triggered only if both the switches at either end of the E port interface are Cisco MDS switches and are running Cisco SAN-OS Release 2.0(1b) or later, or Cisco MDS NX-OS Release 4.1(1a) or later.

### **Port Administrative Speeds**

By default, the port administrative speed for an interface is automatically calculated by the switch.

#### Autosensing

Auto sensing speed is enabled on all 4-Gbps and 8-Gbps switching module interfaces by default. This configuration enables the interfaces to operate at speeds of 1 Gbps, 2 Gbps, or 4 Gbps on 4-Gbps switching modules, and 8 Gbps on 8-Gbps switching modules. When auto sensing is enabled for an interface operating in dedicated rate mode, 4 Gbps of bandwidth is reserved even if the port negotiates at an operating speed of 1 Gbps or 2 Gbps.

To avoid wasting unused bandwidth on 48-port and 24-port 4-Gbps and 8-Gbps Fibre Channel switching modules, you can specify that only 2 Gbps of required bandwidth be reserved, not the default of 4 Gbps or 8 Gbps. This feature shares the unused bandwidth within the port group, provided the bandwidth does not exceed the rate limit configuration for the port. You can also use this feature for shared rate ports that are configured for auto sensing.

Ω

**Tip** When migrating a host that supports up to 2-Gbps traffic (that is, not 4 Gbps with auto-sensing capabilities) to the 4-Gbps switching modules, use auto sensing with a maximum bandwidth of 2 Gbps. When migrating a host that supports up to 4-Gbps traffic (that is, not 8 Gbps with auto-sensing capabilities) to the 8-Gbps switching modules, use auto sensing with a maximum bandwidth of 4 Gbps.

## **Frame Encapsulation**

The **switchport encap eisl** command applies only to SD port interfaces. This command determines the frame format for all the frames transmitted by the interface in SD port mode. If the encapsulation is set to EISL, all

outgoing frames are transmitted in the EISL frame format, regardless of the SPAN sources. For information about encapsulation, see the Cisco MDS 9000 Series NX-OS System Management Configuration Guide.

The **switchport encap eisl** command is disabled by default. If you enable encapsulation, all outgoing frames are encapsulated, and you will see a new line (Encapsulation is eisl) in the **show interface** *SD\_port\_interface* command output. For information about encapsulation, see the Cisco MDS 9000 Series NX-OS System Management Configuration Guide.

## **Debounce Timer**

Debounce timers delay the notification of link changes that can decrease traffic loss due to a network reconfiguration.

There are two types of debounce timers:

• Sync Loss: This timer applies when a link is active. A link is active after the link initialization (LR-LRR-IDLE-IDLE) is successful. If there is synchronization loss for less than 100 ms when the Fibre Channel link is active, the interface does not bounce, but remains active. The value for debounce timer link down due to synchronization loss is 100 ms for Fibre Channel interfaces. This value cannot be configured. If there is synchronization loss for 100 ms or more when the Fibre Channel link is active, the interface goes down with the following message:

%PORT-5-IF\_DOWN\_LINK\_FAILURE: %\$VSAN vsan%\$ Interface intf is down (Link failure loss of sync)

NOS/OLS: This timer applies when a Fibre Channel port is initializing prior to when it is active. A Fibre
Channel port is initializing prior to FLOGI or ACC (FLOGI) for F ports and ELP or ACC (ELP) for E
ports. During the port initialization if a Fibre Channel interface encounters multiple NOS/OLS sequences
continuously for a threshold of 10 times in 2 seconds, the interface is going to be moved to the *errDisabled*state with the following message:

%PORT-5-IF\_DOWN\_LINK\_FAILURE: %\$VSAN vsan%\$ Interface intf is down (Link failure due to NOS/OLS debounce timeout)

The value for NOS/OLS debounce timer is 2 seconds and not configurable.

## **Port Beaconing**

The Port Beaconing feature can be used to identify individual switch and directly attached peer ports in a data center environment. This feature may be used by a switch administrator to help a data center operations personnel to identify ports that need to be serviced by replacing cables or small form-factor pluggable transceivers (SFPs).

The switch administrator can specify a status, duration, and blink rate for switch port beacon LEDs. Port Beacon LEDs of any directly attached peer port may also be controlled if the peer supports the Link Cable Beaconing (LCB) Fibre Channel protocol. Port beacon LEDs on either end or both ends of a link may be controlled using a single command.

## **Bit Error Rate Thresholds**

The bit error rate (BER) threshold is used by a switch to detect an increased error rate before performance degradation seriously affects traffic.

Bit errors occur because of the following reasons:

- · Faulty or bad cable
- Faulty or bad Gigabit Interface Converter (GBIC) or Small Form-Factor Pluggable (SFP)
- GBIC or SFP is specified to operate at 1 Gbps, but is used at 2 Gbps
- GBIC or SFP is specified to operate at 2 Gbps, but is used at 4 Gbps
- Short-haul cable is used for long haul or long-haul cable is used for short haul
- Momentary synchronization loss
- · Loose cable connection at one end or both ends
- · Improper GBIC or SFP connection at one end or both ends

A BER threshold is detected when 15 error bursts occur in an interval of minimum 45 seconds and a maximum of 5-minute period with a sampling interval of 3 seconds. By default, the switch disables the interface when the threshold is reached. Use the **shutdown** and **no shutdown** command sequence to re-enable the interface.

You can configure the switch to not disable an interface when the threshold is crossed. By default, the threshold disables the interface.

#### **Disabling the Bit Error Rate Threshold**

By default, the threshold disables the interface. However, you can configure the switch to not disable an interface when the threshold is crossed.

To disable the BER threshold for an interface, perform these steps:

#### Procedure

 Step 1 Enter configuration mode: switch# configure terminal
 Step 2 Select a Fibre Channel interface and enter interface configuration submode: switch(config)# interface fc1/1
 Step 3 Prevent the detection of BER events from disabling the interface: switch(config-if)# switchport ignore bit-errors (Optional) Prevent the detection of BER events from enabling the interface: switch(config-if)# no switchport ignore bit-errors Tip Regardless of the setting of the **switchport ignore bit-errors** command, a switch generates a syslog message when the BER threshold is exceeded.

## **SFP Transmitter Types**

The SFP hardware transmitters are identified by their acronyms when displayed using the **show interface brief** command. If the related SFP has a Cisco-assigned extended ID, the **show interface** and **show interface brief** commands display the ID instead of the transmitter type. The **show interface transceiver** and **show interface f** *slot/port* **transceiver** commands display both values (ID and transmitter type) for Cisco-supported SFPs. Table 6: SFP Transmitter Acronym Definitions , on page 15 defines the acronyms used in the command output. For information about how to display interface information, see the #unique 59.

Definition	Acronym	
Standard transmitters defined in the GBIC specifications		
Short wave laser	swl	
Medium wave laser	mwl	
Extended reach wave laser	erwl	
Long wave laser	lwl	
Long wave laser cost reduced	lwcr	
Electrical	elec	

Table 6: SFP Transmitter Acronym Definitions

## **Port Monitor**

The Port Monitor feature can be used to monitor the performance and status of ports and generate alerts and syslog messages when problems occur. You can configure thresholds for various counters and enable event triggers when the values cross the threshold.

For rising and falling thresholds, a syslog is generated only when the counter value crosses these threshold values.

Table 7: Default Port Monitor Policy with Threshold Values for Releases Prior to Cisco MDS NX-OS Release 8.5(1), on page 16 displays the default port monitor policy with threshold values. The unit for threshold values (rising and falling) differs across different counters.



#### Note

The link connecting a core switch to a Cisco NPV switch should be treated as an Inter-Switch Link (ISL) (core port) in the port monitor. Previously, core ports were included as access ports and were subject to any portguard actions configured. This allows portguard actions on true access (edge) ports, while ports connecting to Cisco NPV switches remain unaffected. Use the interface level **switchport logical-type** command to change the logical type for the links between an NPIV switch and a Cisco NPV switch.

Note

From Cisco MDS NX-OS Release 8.3(1), NP ports are also monitored in port monitor.

Counter	Threshold Type	Interval (Seconds)
link-loss	Delta	60
sync-loss	Delta	60
signal-loss	Delta	60
state-change	Delta	60
invalid-words	Delta	60
invalid-crc	Delta	60
tx-discards	Delta	60
lr-rx	Delta	60
lr-tx	Delta	60
timeout-discards	Delta	60
credit-loss-reco	Delta	60
tx-credit-not-available	Delta	1
rx-datarate	Delta	60
tx-datarate	Delta	60
tx-slowport-oper-delay	Absolute	60
2		
txwait <sup>3</sup>	Delta	60

#### Table 7: Default Port Monitor Policy with Threshold Values for Releases Prior to Cisco MDS NX-OS Release 8.5(1)

<sup>1</sup> tx-credit-not-available and TXWait are configured as a percentage of the polling interval. So, if 10% is configured with a 1 second polling interval, the tx-credit-not-available will alert when the port does not have tx credits available for 100 ms.

If the tx-credit-not-available timer and the port monitor timer do not start at the same time or if the difference between the tx-credit-not-available timer and the port monitor timer is not zero, there will be a spike of rising and falling alarms from port monitor.

- For all platforms, if the default value for tx-slowport-oper-delay is modified, ISSD to a version lower than Cisco MDS NX-OS Release 6.2(13) will be restricted. To proceed with ISSD, use the no form of the counter tx-slowport-oper-delay command to roll back to the default value.
  - This counter was introduced in Cisco NX-OS Release 6.2(13).
- <sup>3</sup> For all platforms, if the default value for txwait is modified, ISSD to a version lower than Cisco MDS NX-OS Release 6.2(13) will be restricted. To proceed with ISSD, use the **no** form of the **counter txwait** command to roll back to the default value.
  - This counter was introduced in Cisco NX-OS Release 6.2(13).

Table 8: Default Port Monitor Policy with	<b>Threshold Values for Cisco</b>	o MDS NX-OS Release 8.5(1)	and Later Releases
---	-----------------------------------	----------------------------	--------------------

Counter	Threshold	Interval	Warning	J	Thresho	Thresholds		alling ac	tions	Congesti	on-signal
	туре	(3603)	Threshold	Alerts	Rising	Falling	Event	Alerts	PortGuard	Warning	Alarm
link-loss	Delta	60	none	n/a	5	1	4	syslog, rmon	none	n/a	n/a
sync-loss	Delta	60	none	n/a	5	1	4	syslog, rmon	none	n/a	n/a
signaHoss	Delta	60	none	n/a	5	1	4	syslog, rmon	none	n/a	n/a
invaldevoods	Delta	60	none	n/a	1	0	4	syslog, rmon	none	n/a	n/a
invalidads	Delta	60	none	n/a	5	1	4	syslog, rmon	none	n/a	n/a
stædringe	Delta	60	none	n/a	5	0	4	syslog, rmon	none	n/a	n/a
tx-discards	Delta	60	none	n/a	200	10	4	syslog, rmon	none	n/a	n/a
lr-rx	Delta	60	none	n/a	5	1	4	syslog, rmon	none	n/a	n/a
lr-tx	Delta	60	none	n/a	5	1	4	syslog, rmon	none	n/a	n/a
inva tekents	Delta	60	none	n/a	200	10	4	syslog, rmon	none	n/a	n/a
actilossico	Delta	60	none	n/a	1	0	4	syslog, rmon	none	n/a	n/a
techtadle	Delta	60	none	n/a	10% 4	0%	4	syslog, rmon	none	n/a	n/a

Counter	Threshold	Interval	Warning	J	Thresho	lds	Rising/F	alling ac	tions	Congesti	on-signal
	туре	(Secs)	Threshold	Alerts	Rising	Falling	Event	Alerts	PortGuard	Warning	Alarm
rx-datarate	Delta	10	none	n/a	80%	70%	4	syslog, rmon	none	n/a	n/a
tx-datarate	Delta	10	none	n/a	80%	70%	4	syslog, rmon	none	n/a	n/a
<b>tsbygotpasity</b> <u>5</u>	Absolute	60	none	n/a	50ms	0ms	4	syslog, rmon	none	n/a	n/a
txwait <sup>6</sup>	Delta	60	none	n/a	30%	10%	4	syslog, rmon	none	n/a	n/a
rædtræbret	Delta	10	none	n/a	5@90%	1@90%	4	syslog, rmon, obfl	none	n/a	n/a
txdtræhrt	Delta	10	none	n/a	5@90%	1@90%	4	syslog, rmon, obfl	none	n/a	n/a
inputeriors	Delta	60	none	n/a	5	1	4	syslog, rmon	none	n/a	n/a

<sup>4</sup> tx-credit-not-available and TXWait are configured as a percentage of the polling interval. So, if 10% is configured with a 1 second polling interval, the tx-credit-not-available will alert when the port does not have tx credits available for 100 ms.

If the tx-credit-not-available timer and the port monitor timer do not start at the same time or if the difference between the tx-credit-not-available timer and the port monitor timer is not zero, there will be a spike of rising and falling alarms from port monitor.

- For all platforms, if the default value for tx-slowport-oper-delay is modified, ISSD to a version lower than Cisco MDS NX-OS Release 6.2(13) will be restricted. To proceed with ISSD, use the **no** form of the **counter tx-slowport-oper-delay** command to roll back to the default value.
  - This counter was introduced in Cisco NX-OS Release 6.2(13).
- For all platforms, if the default value for txwait is modified, ISSD to a version lower than Cisco MDS NX-OS Release 6.2(13) will be restricted. To proceed with ISSD, use the no form of the counter txwait command to roll back to the default value.
  - This counter was introduced in Cisco NX-OS Release 6.2(13).

Counter	Threshold Type	Interval (Seconds)	Rising Threshold	Event	Falling Threshold	Event	Warning Threshold
link-loss	Delta	Seconds	Number	Event ID	Number	Event ID	Number

5

Counter	Threshold Type	Interval (Seconds)	Rising Threshold	Event	Falling Threshold	Event	Warning Threshold
sync-loss	Delta	Seconds	Number	Event ID	Number	Event ID	Number
signal-loss	Delta	Seconds	Number	Event ID	Number	Event ID	Number
state-change	Delta	Seconds	Number	Event ID	Number	Event ID	Number
invalid-words	Delta	Seconds	Number	Event ID	Number	Event ID	Number
invalid-crc's	Delta	Seconds	Number	Event ID	Number	Event ID	Number
tx-discards	Delta	Seconds	Number	Event ID	Number	Event ID	Number
lr-rx	Delta	Seconds	Number	Event ID	Number	Event ID	Number
lr-tx	Delta	Seconds	Number	Event ID	Number	Event ID	Number
timeout-discards	Delta	Seconds	Number	Event ID	Number	Event ID	Number
credit-loss-reco	Delta	Seconds	Number	Event ID	Number	Event ID	Number
txacdimetavailable	Delta	Seconds	Percentage	Event ID	Percentage	Event ID	Percentage
rx-datarate	Delta	Seconds	Percentage	Event ID	Percentage	Event ID	Percentage
tx-datarate	Delta	Seconds	Percentage	Event ID	Percentage	Event ID	Percentage
txsbwpattapardsby	Absolute	Seconds	Milliseconds	Event ID	Milliseconds	Event ID	Milliseconds
txwait	Delta	Seconds	Percentage	Event ID	Percentage	Event ID	Percentage
err-pkt-to-xbar	Delta	Seconds	Number	Event ID	Number	Event ID	Number
er-pkt-fiom-xbar	Delta	Seconds	Number	Event ID	Number	Event ID	Number

Table 10: Recommended Units for Port Monitor Policy For Cisco MDS NX-OS Release 8.5(1) and Later Releases

Counter	Threshold Type		Warning		Thresho	lds	Rising/F	alling ac	tions	Congesti	on-signal
	iyhe	(3603)	Threshold	Alerts	Rising	Falling	Event	Alerts	PortGuard	Warning	Alarm
link-loss	Delta	Seconds	Number	syslog, rmon	Number	Number	Event ID	syslog, rmon	none	n/a	n/a
sync-loss	Delta	Seconds	Number	syslog, rmon	Number	Number	Event ID	syslog, rmon	none	n/a	n/a
signaHoss	Delta	Seconds	Number	syslog, rmon	Number	Number	Event ID	syslog, rmon	none	n/a	n/a
invalidewoods	Delta	Seconds	Number	syslog, rmon	Number	Number	Event ID	syslog, rmon	none	n/a	n/a

Counter	Threshold Turn o		Warning		Thresho	lds	Rising/F	alling ac	tions	Congestion-signal		
	туре	(Secs)	Threshold	Alerts	Rising	Falling	Event	Alerts	PortGuard	Warning	Alarm	
invalidends	Delta	Seconds	Number	syslog, rmon	Number	Number	Event ID	syslog, rmon	none	n/a	n/a	
statechange	Delta	Seconds	Number	syslog, rmon	Number	Number	Event ID	syslog, rmon	none	n/a	n/a	
tx-discards	Delta	Seconds	Number	syslog, rmon	Number	Number	Event ID	syslog, rmon	none	n/a	n/a	
lr-rx	Delta	Seconds	Number	syslog, rmon	Number	Number	Event ID	syslog, rmon	none	n/a	n/a	
lr-tx	Delta	Seconds	Number	syslog, rmon	Number	Number	Event ID	syslog, rmon	none	n/a	n/a	
ínætekæds	Delta	Seconds	Number	syslog, rmon	Number	Number	Event ID	syslog, rmon	none	n/a	n/a	
aaddassaaa	Delta	Seconds	Number	syslog, rmon	Number	Number	Event ID	syslog, rmon	none	n/a	n/a	
tachtadde	Delta	Seconds	Percentage	syslog, rmon	Percentage	Percentage	Event ID	syslog, rmon	none	n/a	n/a	
rx-datarate	Delta	Seconds	Percentage	syslog, rmon	Percentage	Percentage	Event ID	syslog, rmon	none	n/a	n/a	
tx-datarate	Delta	Seconds	Percentage	syslog, rmon	Percentage	Percentage	Event ID	syslog, rmon	none	n/a	n/a	
tstvyoepaedby	Absolute	Seconds	Milkaands	syslog, rmon	Milkaands	Milkaands	Event ID	syslog, rmon	none	n/a	n/a	
txwait	Delta	Seconds	Percentage	syslog, rmon	Percentage	Percentage	Event ID	syslog, rmon	none	Percentage	Percentage	
şêkoveb wan	Delta	Seconds	Ninhagene	syslog, rmon	Ninhagene	Ninhagene	Event ID	syslog, rmon	none	n/a	n/a	
\$\$\$\$0vdowan	Delta	Seconds	Ninhagene	syslog, rmon	Ninhagene	Ninhagene	Event ID	syslog, rmon	none	n/a	n/a	
rxdtrathrat	Delta	Seconds	Ninhagung	syslog, rmon, obfl	Ninhaging	Ninhaging	Event ID	syslog, rmon, obfl	none	n/a	n/a	
txdtatehrst	Delta	Seconds	Ninhagange	syslog, rmon, obfl	Ninhaging	Ninhaging	Event ID	syslog, rmon, obfl	none	n/a	n/a	

Counter Threshold Interval W		Warning	Narning Th		Thresholds		<b>Rising/Falling actions</b>			Congestion-signal	
	Type (Secs)		Threshold	Alerts	Rising	Falling	Event	Alerts	PortGuard	Warning	Alarm
inputencis	Delta	Seconds	Number	syslog, rmon	Number	Number	Event ID	syslog, rmon	none	n/a	n/a

Note

- From Cisco MDS NX-OS Release 8.1(1), the err-pkt-from-port—ASIC Error Pkt from Port counter is deprecated.
  - The err-pkt-from-port—ASIC Error Pkt from Port, err-pkt-to-xbar—ASIC Error Pkt to xbar, and err-pkt-from-xbar—ASIC Error Pkt from xbar counters were introduced in Cisco NX-OS Release 5.2(2a) and are not supported on one rack unit and two rack unit switches.
  - We recommend that you use the delta threshold type for all the counters except the tx-slowport-oper-delay counter which uses absolute threshold type.
  - The rx-datarate and tx-datarate are calculated using the inoctets and outoctets on an interface.
  - The unit for threshold values (rising and falling) differs across different counters.
  - The tx-slowport-oper-delay wait counter is applicable only for advanced 16-Gbps and 32-Gbps modules and switches.
  - You must configure slow-port monitoring using the **system timeout slowport-monitor** command in order to get alerts for tx-slowport-count and tx-slowport-oper-delay for a particular port type. (See the **system timeout slowport-monitor** command in the Cisco MDS 9000 Series Command Reference.)
  - Absolute counters do not support port-guard action. However, tx-slowport-oper-delay counter supports Congestion Isolation port-guard action.
  - The txwait counter is applicable only for advanced 16-Gbps and 32-Gbps modules and switches. In the default configuration, the port monitor sends an alert if the transmit credit is not available for 400 ms (40%) in 1 second.

txwait sends alerts when there are multiple slow-port events that have not hit the slow-port monitor threshold, but have together hit the txwait threshold configured. For example, if there are 40 discrete 10-ms intervals of 0 TX credits in 1 second, tx-slowport-oper-delay does not find these credits; txwait finds the credits and sends an alert.

- The state-change counter records the port down-to-port up action as one state change that is similar to *flap*. This is the reason the state-change counter does not have the portguard action set as *flap*.
- When the portguard action is set as *flap*, you will get alerts only through syslog.
- Only the credit-loss-reco, tx-credit-not-available, tx-slowport-oper-delay, and txwait counters use the **cong-isolate** and **cong-isolate-recover** keywords to detect slow flow on a device. For more information, see Configuring a Port Monitor Policy, on page 49.
- You can configure RMON alerts for rx-datarate-burst, tx-datarate-burst, sfp-rx-power-low-warn and sfp-tx-power-low-warn counters. However, RMON alerts will not be generated.

For more information on internal CRC errors and the various stages, see "Internal CRC Detection and Isolation" section in *Cisco MDS 9000 Series High Availability Configuration Guide*.

Table 11: Slowdrain Port-Monitor Policy Threshold Value For Releases Prior to Cisco MDS NX-OS Release 8.5(1), on page 22 displays the threshold value of the slow-drain port-monitor policy:

Counter	Threshold Type	Interval (Seconds)	Rising Threshold	Event	Falling Threshold	Event	Port Monitor Portguard
Credit Loss Reco	Delta	1	1	4	0	4	Not enabled
TX Credit Not Available	Delta	1	10	4	0	4	Not enabled

Table 12: Slowdrain Port-Monitor Policy Threshold Value For Cisco MDS NX-OS Release 8.5(1) and Later Releases

Counter	Counter Threshold In Type (S		Interval Warning		Thresholds		Rising/F	alling ac	tions	Congesti	on-signal
	туре	(3603)	Threshold	Alerts	Rising	Falling	Event	Alerts	PortGuard	Warning	Alarm
Credit Loss Reco	Delta	1	none	n/a	1	0	4	syslog, rmon	none	n/a	n/a
TX Credit Not Available	Delta	1	none	n/a	10	0	4	syslog, rmon	none	n/a	n/a
tx-datarate	Delta	10	none	n/a	80	70	4	syslog, obfl	none	n/a	n/a
TXWait <sup>7</sup>	Delta	1	none	n/a	30	10	4	syslog, rmon	none	n/a	n/a

<sup>7</sup> Supported with Release 9.3(1) and later



**Note** If no other port monitor policy is explicitly activated, the slowdrain policy is activated. The default policy shows only the default counter monitor values.

#### Crossbar (Xbar) Counters

The Xbar counters monitor internal CRC errors. These are CRC errors that have been caused internally by one of the forwarding *stages* in the switch. These only apply to director class FC modules.

The following are the crossbar counters:

- err-pkt-from-port
- err-pkt-to-xbar
- err-pkt-from-xbar

The above crossbar (Xbar) counters are not included in the default policy.





Note

- On the 2/4/8/10/16 Gbps Advanced FC module, DS-X9448-768K9, there are 6 FC ASICs each handling 8 ports.
- On the 1/10/40G IPS.2/4/8/10/16G FC module, DS-X9334-K9, there are 3 FC ASICs each handling 8 ports.
- On the 4/8/16/32 Gbps Advanced FC module, DS-X9648-1536K9, there are 3 FC ASICs each handling 16 ports.

#### SFP Counters

From Cisco MDS NX-OS Release 8.5(1), the SFP counters allow you to configure the low warning thresholds for Tx Power and Rx Power for SFPs so that you receive a syslog when these values drop below the configured values. SFPs are monitored once every 10 minutes (600 seconds). The rising threshold is the count of the times the Rx or Tx Power was less than or equal to the SFP's Rx or Tx Power low warning threshold multiplied by the percentage. Consequently, the rising threshold can at most increment by one, every 10 minutes.

Configuring a rising threshold value that is more than the 600 multiple of the poll interval will display an error. For example, for a polling interval of 1200, the rising threshold will be 2 (1200/600) and cannot be more than 2. The SFP counters are not included in the default policy and the only alert action that is available is syslog. You can configure the polling interval using the port monitor **counter** command.

You can configure the SFP counters as below:

- Configuring a low warning threshold percentage of 100% allows this counter to trigger when the Rx Power is less than or equal to the SFP's Rx Power low warning threshold.
- Configuring a low warning threshold percentage less than 100% allows this counter to trigger when the Rx Power is above the SFP's Rx Power low warning threshold.
- Configuring a low warning threshold percentage of greater than 100% allows this counter to trigger when the Rx Power is less than the SFP's Rx Power low warning threshold (between low warning and low alarm).



Note

- The SFP counters are not part of the default port monitor policy. You must explicitly enable them using the **monitor counter** command.
- The minimum polling interval for SFP counters is 600 seconds. The polling interval must be in multiple of 600. You can configure the polling interval using the port monitor **counter** command.

For configuring the SFP counters, see Configuring a Port Monitor Policy, on page 49.

The following are the SFP counters:

- sfp-rx-power-low-warn: Specifies the number of times a port's SFP has reached a percentage of the SFP's Rx Power's low warning threshold. This threshold varies depending on the SFP type, speed, and manufacturer and can be displayed via the **show interface transceiver details** command. Hence, this threshold is not an absolute value but a percentage of each individual SFP's Rx Power low warning threshold. This percentage can be configured in the range of 50% to 150% to allow for alerting at values less than the Rx Power low warning threshold or greater than the Rx Power low warning threshold... Hence, this is an absolute value and varies between 50% to 150%. The low warning threshold value is calculated as the actual low warning threshold value of the SFP times the specified percentage. If the Rx power is lesser than or equal to the low warning threshold value, then this counter is incremented.
- sfp-tx-power-low-warn: Specifies the number of times a port's SFP has reached a percentage of the SFP's Tx Power's low warning threshold. This threshold varies depending on the SFP type, speed, and manufacturer and can be displayed via the show interface transceiver details command. Hence, this threshold is not an absolute value but a percentage of each individual SFP's Tx Power low warning threshold. This percentage can be configured in the range of 50% to 150% to allow for alerting at values less than the Tx Power low warning threshold or greater than the Tx Power low warning threshold... Hence, this is an absolute value and varies between 50% to 100%. The low warning threshold value is calculated as the actual low warning threshold value of the SFP times the specified percentage. If the Tx power is lesser than or equal to the low warning threshold value, then this counter is incremented.

#### **Datarate Burst Counters**

From Cisco MDS NX-OS Release 8.5(1), the datarate burst counters monitor the number of times the datarate crosses the configured threshold datarate in 1 second intervals. If the number crosses the configured number for rising threshold, the configured alert actions are taken as the condition is met. Datarate burst counters are

polled every second. The datarate burst counters are not included in the default policy. For configuring the datarate burst counters, see Configuring a Port Monitor Policy, on page 49.

The following are the datarate burst counters:

- rx-datarate-burst
- tx-datarate-burst

#### Warning Threshold

Port Monitor warning thresholds can be used to generate syslog messages before rising and falling thresholds are reached. A single threshold is configurable per Port Monitor counter. A syslog is generated whenever the counter crosses the configured warning threshold in either the rising or falling direction. This allows the user to track counters that are not severe enough to hit the rising threshold, but where nonzero events are of interest.

The warning threshold must be equal or less than the rising threshold and equal or greater than the falling threshold.

The warning threshold is optional; warning syslogs are only generated when it is specified in a counter configuration.

#### **Use Case—Warning Threshold**

Let us consider two scenarios with the following configurations:

- Rising threshold is 30
- Warning threshold is 10
- Falling threshold is 0

This example displays the syslog generated when the error count is less than the rising threshold value, but has reached the warning threshold value:

#### Syslog Generated When the Error Count is Less Than the Rising Threshold Value

%PMON-SLOT2-4-WARNING\_THRESHOLD\_REACHED\_UPWARD: Invalid Words has reached warning threshold in the upward direction (port fc2/18 [0x1091000], value = 10).

%PMON-SLOT2-5-WARNING\_THRESHOLD\_REACHED\_DOWNWARD: Invalid Words has reached warning threshold in the downward direction (port fc2/18 [0x1091000], value = 5).

In the first polling interval, the errors triggered for the counter (Invalid Words) are 10, and have reached the warning threshold value. A syslog is generated, indicating that the error count is increasing (moving in the upward direction).

In the next polling interval, the error count decreases (moves in the downward direction), and a syslog is generated, indicating that the error count has decreased (moving in the downward direction).

This example displays the syslog that is generated when the error count crosses the rising threshold value:

#### Syslog Generated When the Error Count Crosses the Rising Threshold Value

%PMON-SLOT2-4-WARNING\_THRESHOLD\_REACHED\_UPWARD: Invalid Words has reached warning threshold in the upward direction (port fc2/18 [0x1091000], value = 30).

%PMON-SLOT2-3-RISING\_THRESHOLD\_REACHED: Invalid Words has reached the rising threshold (port=fc2/18 [0x1091000], value=30).

%SNMPD-3-ERROR: PMON: Rising Alarm Req for Invalid Words counter for port fc2/18(1091000), value is 30 [event id 1 threshold 30 sample 2 object 4 fcIfInvalidTxWords]

%PMON-SLOT2-5-WARNING\_THRESHOLD\_REACHED\_DOWNWARD: Invalid Words has reached warning threshold in the downward direction (port fc2/18 [0x1091000], value = 3).

%PMON-SLOT2-5-FALLING\_THRESHOLD\_REACHED: Invalid Words has reached the falling threshold (port=fc2/18 [0x1091000], value=0).

%SNMPD-3-ERROR: PMON: Falling Alarm Req for Invalid Words counter for port fc2/18(1091000), value is 0 [event id 2 threshold 0 sample 2 object 4 fcIfInvalidTxWords]

This example displays the syslog generated when the error count is more than the warning threshold value and less than the rising threshold value:

## Syslog Generated When the Error Count is More than the Warning Threshold Value and Less than the Rising Threshold Value

%PMON-SLOT2-4-WARNING\_THRESHOLD\_REACHED\_UPWARD: Invalid Words has reached warning threshold in the upward direction (port fc2/18 [0x1091000], value = 15).

%PMON-SLOT2-5-WARNING\_THRESHOLD\_REACHED\_DOWNWARD: Invalid Words has reached warning threshold in the downward direction (port fc2/18 [0x1091000], value = 3).

The errors generated for the counter (Invalid Words) are 30 when the counter has crossed both the warning and rising threshold values. A syslog is generated when no further errors are triggered.

As there are no further errors in this poll interval, the consecutive polling interval will have no errors, and the error count decreases (moves in downward direction) and reaches the falling threshold value, which is zero. A syslog is generated for the falling threshold.

#### **Port Monitor Check Interval**

Check interval polls for values more frequently within a poll interval so that the errors are detected much earlier and appropriate action can be taken.

With the existing poll interval, it is not possible to detect errors at an early stage. Users have to wait till the completion of the poll interval to detect the errors.

By default, the check interval functionality is not enabled.

Note
 From Cisco MDS NX-OS Release 8.5(1), port monitor does *early detection* and does not require the port monitor check interval feature to be configured, as it is redundant.
 The port monitor check interval feature is supported only on the Cisco MDS 9710 Multilayer Director, Cisco MDS 9718 Multilayer Directors, Cisco MDS 9706 Multilayer Directors, Cisco MDS 9250i, Cisco

• Check interval is supported on both counters, absolute and delta.

MDS 9148T, Cisco MDS 9396T, and Cisco MDS 9132T.

- We recommend that you configure the poll interval as a multiple of the check interval.
- When a port comes up, the check interval will not provide an alert regarding invalid words for the port until the poll interval expires. We recommend that you bring up a set of ports at a given time in the module instead of all the ports.

#### **Port Monitor Early Detection**

Prior to Cisco MDS NX-OS Release 8.5(1) and without check interval configured, port-monitor checked to determine if the warning or rising thresholds were reached only after the polling interval expired. Starting with Cisco MDS NX-OS Release 8.5(1), most port monitor counters are monitored every second so that port monitor can detect warning and rising thresholds and take alert actions as soon as the threshold is detected. There is no change in the falling threshold behavior.

#### **Port Monitor Alerts**

From Cisco MDS NX-OS Release 8.5(1), port monitor allows you to configure alerts for each counter so that you can tailor the alerts that port monitor generates with each counter. By default, all counters are configured for syslog and RMON alerts. Only the rx-datarate, tx-datarate, rx-datarate-burst, and tx-datarate-burst counters allow the configuration of the OBFL alert type. OBFL indicates that these counters record their events into Onboard Failure Logging. These are disposable via the **show logging onboard datarate** command.

The following alerts are supported:

• syslog: Generates a syslog when a configured threshold is reached. You can also configure an event ID (severity-level) for the syslogs that are generated when a rising or falling threshold is detected so that you can filter the logs using the severity level.

The following severity levels are supported:

- ALERT (1)
- CRITICAL (2)
- ERROR (3)
- WARNING (4)
- NOTICE (5)
- rmon: Generates an SNMP alert when a configured threshold is reached.
- obfl: Enables OBFL logging.

Note

The OBFL alert is supported only for rx-datarate, tx-datarate, rx-datarate-burst, and tx-datarate-burst counters.

• none: Disables all alerts.

## **Port Group Monitor**

#### Note

Port Group Monitor functionality only applies to modules that support oversubscription.

The ports on a line card are divided into fixed groups called port groups that share a link of fixed bandwidth to the backplane. Since the total port bandwidth can exceed the backplane link bandwidth, frames will be queued, introducing traffic delays. The Port Group Monitor functionality can be used to monitor this oversubscription in both the transmit and receive directions to allow ports to be rebalanced between port groups before the delays become unacceptable.

When the Port Group Monitor feature is enabled and when a policy consisting of polling interval in seconds and the rising and falling thresholds in percentage are specified, the port group monitor generates a syslog if port group traffic goes above the specified percentage of the maximum supported bandwidth for that port group (for receive and for transmit). Another syslog is generated if the value falls below the specified threshold.

Table shows the threshold values for the default Port Group Monitor policy:

#### Table 13: Default Port Group Monitor Policy Threshold Values

Counter	Threshold Type	Interval (Seconds)	% Rising Threshold	% Falling Threshold
RX Datarate	Delta	60	80	20
TX Datarate	Delta	60	80	20



**Note** When a port group monitor is enabled in a 1-rack box, and if any of the thresholds is met for the receive performance and transmit performance counters, the port group monitor is not supported.

## Portguard

The Portguard feature is intended for use in environments where systems do not adapt quickly to a port going down and up (single or multiple times). For example, if a large fabric takes 5 seconds to stabilize after a port goes down, but the port actually goes up and down once per second, a severe failure might occur in the fabric, including devices becoming permanently unsynchronized.

The Portguard feature provides the SAN administrator with the ability to prevent this issue from occurring. A port can be configured to stay down after a specified number of failures in a specified time period. This allows the SAN administrator to automate fabric stabilization, thereby avoiding problems caused by the up-down cycle.

Using the Portguard feature, the SAN administrator can restrict the number of error events and bring a malfunctioning port to down state dynamically once the error events exceed the event threshold. A port can be configured such that it shuts down when specific failures occur.

There are two types of portguard, *Port Level* type and *Port Monitor* type. While the former is a basic type where event thresholds are configurable on a per port basis, the latter allows the configuration of policies that are applied to all the ports of the same type, for example, all E ports or all F ports.



Note

We recommend against the simultaneous use of both types of portguard for a given port.

#### **Port Level Portguard**

The following is the list of events that can be used to trigger port-level portguard actions:

- TrustSec violation-Link fails because of excessive TrsustSec violation events.
- Bit errors—Link fails because of excessive bit error events.
- Signal loss—Link fails because of excessive signal loss events.
- Signal synchronization loss—Link fails because of excessive signal synchronization events.
- Link reset-Link fails because of excessive link reset events.
- Link down-Link fails because of excessive link down events.
- Credit loss (Loop F ports only)—Link fails because of excessive credit loss events.

A link failure occurs when it receives two bad frames in an interval of 10 seconds and the respective interface will be error disabled. A general link failure caused by link down is the superset of all other causes. The sum of the number of all other causes equals the number of link down failures. This means that a port is brought to down state when it reaches the maximum number of allowed link failures or the maximum number of specified causes.

Port level portguard can be used to shut down misbehaving ports based on certain link event types. Event thresholds are configurable for each event type per port which makes them customizable between host, array, and tape F ports, or between intra- and inter-data center E ports, for example.

The events listed above might get triggered by certain events on a port, such as:

- Receipt of Not Operational Signal (NOS)
- Too many hardware interrupts
- The cable is disconnected
- The detection of hardware faults
- The connected device is rebooted (F ports only)
- The connected modules are rebooted (E ports only)

### **Port Monitor Portguard**

The Port Monitor Portguard feature allows a port to be automatically error disabled, flapped, congestion-isolated, and so on when a given event threshold is reached.

**Note** Absolute counters do not support portguard action. However, TX Slowport Oper Delay counter supports Congestion Isolation portguard action.



Note

From Cisco MDS NX-OS Release 8.5(1), the input errors, sfp-rx-power-low-warn, sfp-tx-power-low-warn, rx-datarate-burst, and tx-datarate-burst counters were added.

The following is the list of events that can be used to trigger the Port Monitor portguard actions:

- credit-loss-reco
- link-loss
- signal-loss
- sync-loss
- rx-datarate
- invalid-crcs
- · invalid-words
- · timeout-discards
- tx-credit-not-available
- tx-datarate
- tx-discards
- tx-slowport-oper-delay
- txwait
- input-errors
- sfp-rx-power-low-warn
- sfp-tx-power-low-warn
- state-change
- rx-datarate-burst
- tx-datarate-burst

## **Interface Types**

#### **Management Interfaces**

You can remotely configure a switch through the management interface (mgmt0). To configure a connection on the mgmt0 interface, configure either the IPv4 parameters (IP address, subnet mask, and default gateway), or the IPv6 parameters (IP address, subnet mask, and default gateway) so that the switch is reachable.

Before you configure the management interface manually, obtain the switch's IPv4 address, subnet mask, and default gateway, or the IPv6 address, depending on which IP version you are configuring.

The management port (mgmt0) auto senses and operates in full-duplex mode at a speed of 10, 100, or 1000 Mbps. Auto sensing supports both the speed mode and the duplex mode. On a Supervisor-1 module, the default speed is 100 Mbps and the default duplex mode is auto. On a Supervisor-2 module, the default speed and the default duplex mode are set to auto.



**Note** Explicitly configure a default gateway to connect to the switch and send IP packets or add a route for each subnet.

### **VSAN Interfaces**

VSANs are applicable to Fibre Channel fabrics and enable you to configure multiple isolated SAN topologies within the same physical infrastructure. Create an IP interface on top of a VSAN, and then use this interface to send frames to the corresponding VSAN. To use this feature, configure the IP address for this VSAN.



Note

VSAN interfaces cannot be created for non existing VSANs.

# **Prerequisites for Interfaces**

Before you begin configuring the interfaces, ensure that the modules in the chassis are functioning as designed. To verify the status of a module at any time, enter the **show module** command in EXEC mode. For information about verifying the module status, refer to the Cisco MDS 9000 Series NX-OS Fundamentals Configuration Guide.

## **Guidelines and Limitations**

From Cisco MDS NX-OS Release 7.3(x) or earlier, ports were classified as port type access ports, trunks, or all in the port monitor. Access ports were mode (T)F ports and trunks were mode (T)E ports (ISLs). Since ports connecting to Cisco NPV switches are mode (T)F, they were included under the port type access ports. These Cisco NPV ports behave like ISLs, but they are a multi-user connection to a switch and not an end device. Because of this, it is not preferred to take portguard actions on the access ports for port-monitor counters pertaining to slow-drain conditions.

From Cisco MDS NX-OS Release 8.1(1), the port monitor has implemented a different classification mechanism. Instead of port type access ports, trunks, or all, a logical type core, edge, or all value can be configured. Core ports are mode T(E) ports and ports connecting core switches to Cisco NPV switches. Edge ports are mode F ports connecting to end devices. With this new classification, portguard actions can safely be configured especially pertaining to slow drain type conditions such that when the problem is detected and the action is taken, it is only on the ports connected to end devices. It is still valid to configure portguard actions for logical type core ports, but this should only be done for counters pertaining to physical errors on the port (such as link loss, invalid words, invalid CRC, and so on).

The MDS NX-OS will automatically classify all F port-channels and trunking F ports as logical-type core. It will classify all non-trunking F ports, including those to both Cisco and non-Cisco NPV switches, as logical-type edge.

If a Cisco NPV switch or non-Cisco NPV switch cannot take portguard types of actions then classifying the ports connected to it as logical-type edge is appropriate.

The logical type of a port is displayed using the **show interface** and **show interface brief** commands.



Note When you use the logical-type command to define a port type, the command overrides the default port type.

In the port monitor, you can configure the policies per port type (core and edge) so that portguard action can be taken on the ports when certain criteria are met. Generally, edge policies are configured to take portguard action on ports and the core policies will not be configured with portguard action. If the link between a core switch and a Cisco NPV switch is treated as an edge port, portguard action is taken on such ports which will result in the loss of connectivity to all the devices connected to the Cisco NPV switch.

For any Cisco NPV switch that supports its own Port Monitor policies, it is best to implement these portguard actions on the Cisco NPV switch itself. Hence, we recommend that all non-trunking F ports connected to Cisco NPV switches be manually configured to a logical type of core, using the **switchport logical-type core** command. This will ensure that port monitor core policy is applied to the port connected to a Cisco NPV switch. We also recommend that Port Monitor be implemented on the Cisco NPV switch, if supported.

For more information, see Interface Modes, on page 5.

## **Guidelines for Configuring Port Monitor Check Interval**

• Check interval should be configured before activating any port monitor policies.

Note

The value of the check interval is common across counters and policies.

- We recommend that you configure the check interval to be less than the poll interval. Also, configure the poll interval as a multiple of the check interval.
- Check interval is applicable to all the active port monitor policies configured.
- Users should deactivate all the active port monitor policies before enabling, modifying, or disabling the check interval functionality.
- · Check interval cannot be enabled when an active policy is configured.
- Software downgrade to a version that does not support the check interval functionality is restricted when the check interval functionality is enabled.
- We recommend that you do not have a portguard action set to the state-change counter when an interface state is changed from down state to up state.
- We recommend that you do not use the default policy when the check interval is configured.

#### **Check Interval**

Let us consider a scenario where the poll interval, rising threshold and check interval are configured with the following values:

- Poll interval is 100 seconds
- Rising threshold is 30
- · Check interval is 20 seconds



C = Check interval = 20 seconds

The check interval starts its interval, C1, along with the poll interval at P1. If an error occurs between the check intervals C2 and C3, the check intervals C2 and C3 are higher than the configured rising threshold value of 30, an alert (syslog or trap or both) is generated at C3, alerting the user that an error has occurred at that particular port.



Note

You can configure longer poll intervals to capture events across poll intervals. For example, configure a poll interval of 24 hours with a check interval of 30 seconds, with the rising threshold value being checked cumulatively every 30 seconds.

## **Guidelines for VSAN Interface Configuration**

- Create a VSAN before creating the interface for that VSAN. If a VSAN does not exist, the interface cannot be created.
- Create the interface VSAN; it is not created automatically.
- If you delete the VSAN, the attached interface is automatically deleted.
- Configure each interface only in one VSAN.

## $\mathcal{P}$

Tip After configuring the VSAN interface, you can configure an IP address or Virtual Router Redundancy Protocol (VRRP) feature. See the Cisco MDS 9000 Series NX-OS IP Services Configuration Guide.

## **Guidelines and Limitations for Port Beaconing**

- The port beacon LED on directly attached peers can only be controlled when the link to the peer is up and operational.
- If you enable port beacon mode on a port using the **beacon interface** command and then enable beacon mode using the **switchport beacon** command, the beacon mode takes precedence and the port beacon mode will be disabled. If you disable the beacon mode, the port beacon mode will continue to be disabled until you enable the port beacon mode again.
- If you send a port beaconing request from Switch A to Switch B using the **beacon interface** command and then if you enable **switchport beacon** locally on Switch B, the **switchport beacon** command takes precedence over the port beaconing request and stops the LED activity on Switch B. However, if you run the **show interface** command on Switch A, the output will continue to show the port beaconing status for the port on Switch B until the specified duration is reached.
- If you enable port beacon mode on a port using the beacon interface command and then perform a
  system switchover using the system switchover command, the show interface command on the switch
  does not show the port beaconing status as on. However, the port LED to which the port beaconing
  request was sent continues to beacon with the specified parameters until the specified duration is reached
  or when you run the switchport beacon command to override the port beaconing request for the port.
- If you send a port beaconing request with the duration set to 0 from Switch A that is running Cisco MDS NX-OS Release 8.3(1) or later releases to Switch B and then downgrade Switch A to Cisco MDS NX-OS Release 8.2(2) or earlier releases, the port LED on Switch B to which the port beaconing request was sent continues to beacon with the specified parameters until you run the **switchport beacon** command to override the port beaconing request for the port on Switch B.
- From Cisco MDS NX-OS Release 8.4(1), this feature is supported on Cisco MDS switches that are operating in Cisco NPV mode.
- This feature is not supported on port-channel interfaces. It is supported only on individual Fibre Channel interfaces or port-channel members.

# **Default Settings**

Table 14: Default Interface Parameters , on page 36 lists the default settings for interface parameters.

#### Table 14: Default Interface Parameters

Parameters	Default
Interface mode	Auto
Interface speed	Auto
Administrative state	Shutdown (unless changed during initial setup)
Trunk mode	On (unless changed during initial setup) on non-NPV and NPIV core switches. Off on NPV switches.
Trunk-allowed VSANs or VF-IDs	1 to 4093
Interface VSAN	Default VSAN (1)
Beacon mode	Off (disabled)
EISL encapsulation	Disabled
Data field size	2112 bytes
# **Configuring Interfaces**

For more information on configuring mgmt0 interfaces, refer to the Cisco MDS 9000 Series NX-OS Fundamentals Configuration Guide and Cisco MDS 9000 Series NX-OS IP Services Configuration Guide.

For more information on configuring Gigabit Ethernet interfaces, see the Cisco MDS 9000 Series NX-OS IP Services Configuration Guide.

### **Configuring a Fibre Channel Interface**

To configure a Fibre Channel interface, perform these steps:

### Procedure

**Step 1** Enter configuration mode:

switch# configure terminal

### **Step 2** Select a Fibre Channel interface and enter interface configuration submode:

### switch(config)# interface fc 1/1

When a Fibre Channel interface is configured, it is automatically assigned a unique world wide name (WWN). If the interface's operational state is up, it is also assigned a Fibre Channel ID (FC ID).

### **Configuring a Range of Fibre Channel Interfaces**

To configure a range of interfaces, perform these steps:

### Procedure

**Step 1** Enter configuration mode:

switch# configure terminal

**Step 2** Select the range of Fibre Channel interfaces and enter interface configuration submode3:

switch(config)# interface fc1/1 - 4, fc2/1 - 3

### Note

When using this command, provide a space before and after the comma.

### Setting the Interface Administrative State

To set the interface administrative state, you must first gracefully shut down the interface and enable traffic flow.

### **Shutting Down an Interface**

To gracefully shut down an interface, perform these steps:

### Procedure

**Step 1** Enter configuration mode:

switch# configure terminal

- Step 2Select a Fibre Channel interface and enter interface configuration submode:switch(config)# interface fc1/1
- **Step 3** Gracefully shut down the interface and administratively disable the traffic flow; this is the default state switch(config-if)# **shutdown**

### **Enabling Traffic Flow**

To enable traffic flow, perform these steps:

### Procedure

Step 1	Enter configuration mode: switch# configure terminal	
Step 2	Select a Fibre Channel interface and enter interface configuration submode: switch(config)# interface fc1/1	
Step 3	Enable traffic flow to administratively allow traffic when the no prefix is used (provided the operational state is up): switch(config-if)# <b>no shutdown</b>	

## **Configuring an Interface Mode**

To configure the interface mode, perform these steps:

L

### Procedure

Step 1	Enter configuration mode:	
	switch# configure terminal	
Step 2	Select a Fibre Channel interface and enter interface configuration submode:	
	switch(config)# interface fc1/1	
Step 3	Configure the administrative mode of the port. You can set the operational state to auto, E, F, FL, Fx, TL, NP, or SD port mode:	
	switch(config-if)# switchport mode F	
	<b>Note</b> Fx ports refer to an F port or an FL port (host connection only), but not E ports.	
Step 4	Configure interface mode to auto negotiate an E, F, FL, or TE port mode (not TL or SD port modes) of operation:	
	switch(config-if)# switchport mode auto	
	<ul><li>Note</li><li>TL ports and SD ports cannot be configured automatically. They must be administratively configured.</li></ul>	
	• You cannot configure Fibre Channel interfaces on Storage Services Modules (SSM) in auto mode.	

# **Configuring the MAX NPIV Limit**



**Note** Both the **max-npiv-limit** and **trunk-max-npiv-limit** can be configured on a port or port channel. If the port or port channel becomes a trunking port, **trunk-max-npiv-limit** is used for limit checks.

To configure the maximum NPIV limit, perform these steps:

### Procedure

 

 Step 1
 Enter configuration mode: switch# configure terminal

 Step 2
 Select a Fibre Channel interface and enter interface configuration submode: switch(config)# interface fc 3/29

 Step 3
 Configure switch port mode F on the Fibre Channel interface: switch(config-if)# switchport mode F

 Step 4Specify the maximum login value for this port:<br/>switch(config-if)# switchport max-npiv-limit 100<br/>The valid range is from 1 to 256.

### **Configuring the System Default F Port Mode**

The **system default switchport mode F** command sets the administrative mode of all Fibre Channel ports to mode F, while avoiding traffic disruption caused by the formation of unwanted ISLs. This command is part of the setup utility that runs during bootup after a **write erase** or **reload** command is issued. It can also be executed from the command line in configuration mode. This command changes the configuration of the following ports to administrative mode F:

- All ports that are down and that are not out of service.
- All F ports that are up, whose operational mode is F, and whose administrative mode is not F.

The system default switchport mode F command does not affect the configuration of the following ports:

- All user-configured ports, even if they are down.
- All non-F ports that are up. However, if non-F ports are down, this command changes the administrative mode of those ports.



Note

- To ensure that ports that are a part of ISLs do not get changed to port mode F, configure the ports in port mode E, rather than in auto mode.
  - When the command is executed from the command line, the switch operation remains graceful. No ports are flapped.

To set the administrative mode of Fibre Channel ports to mode F in the CLI, perform these steps:

#### Procedure

**Step 1** Enter configuration mode:

#### switch# configure terminal

**Step 2** Sets administrative mode of Fibre Channel ports to mode F (if applicable):

#### switch(config)# system default switchport mode F

(Optional) Set the administrative mode of Fibre Channel ports to the default (unless user configured), use the following command:

#### switch(config)# no system default switchport mode F

Note

For detailed information about the switch setup utility, see the Cisco MDS 9000 Series NX-OS Fundamentals Configuration Guide.

### **Setup Utility**

Setup Utility, on page 41 shows the command in the setup utility and the command from the command line.

```
Configure default switchport mode F (yes/no) [n]: y
```

```
switch(config) # system default switchport mode F
```

### **Configuring ISL Between Two Switches**

**Note** Ensure that the Fibre Channel cable is connected between the ports and perform a no-shut operation on each port.

E-port mode is used when a port functions as one end of an ISL setting. When you set the port mode to E, you restrict the port coming up as an E port (trunking or nontrunking, depending on the trunking port mode).

To configure the port mode to E:

### Procedure

- Step 1
   Enter configuration mode:

   switch#configure terminal
- **Step 2** Select a Fibre Channel interface and enter interface configuration submode:

switch(config)# interface fc 3/29

**Step 3** Configure switch port mode E on the Fibre Channel interface:

switch(config)# switchport mode E

#### Note

Ensure that you perform the task of setting the port mode to E on both the switches between which you are attempting to bring up the ISL link.

# **Configuring the Port Administrative Speeds**

Ŵ

**Note** Changing the port administrative speed is a disruptive operation.

To configure the port speed of the interface, perform these steps:

### Procedure

**Step 1** Enter configuration mode:

switch# configure terminal

**Step 2** Select the Fibre Channel interface and enter interface configuration mode:

switch(config)# interface fc 1/1

**Step 3** Configure the port speed of the interface to 1000 Mbps:

### switch(config-if)# switchport speed 1000

All the 10-Gbps capable interfaces, except the interface that is being configured, must be in the out-of-service state. At least one other 10-Gbps capable interface must be in the in-service state.

(Optional) Revert to the factory default (auto) administrative speed of the interface:

switch(config-if)# no switchport speed

### **Configuring Port Speed Group**

To configure the port speed group of the interface, perform these steps:

#### Procedure

Step 1Enter configuration mode:

switch# **configure terminal** 

**Step 2** Select the Fibre Channel interface and enter interface configuration mode:

switch(config)# interface fc 1/1

**Step 3** Configure the port speed group to 10 Gbps:

switch(config-if)# speed group 10g

The preferred way of changing the speed group is the **10g-speed-mode** command.

(Optional) Unset the port speed group and revert to the factory default (auto) administrative speed group of the interface:

switch(config-if)# no speed group 10g

### **Configuring the Interface Description**

The interface description can be any alphanumeric string that is up to 80 characters long. To configure a description for an interface, perform these steps:

### Procedure

Step 1	Enter configuration mode: switch# configure terminal
Step 2	Select a Fibre Channel interface and enter interface configuration submode: switch(config)# <b>interface fc1/1</b>
Step 3	Configure the description of the interface: switch(config-if)# switchport description cisco-HBA2
	The string can be up to 80 characters long.
	(Optional) Clear the description of the interface:
	switch(config-if)# no switchport description

### **Configuring a Port Logical Type**

The logical port type can be used to override the default type assigned by the Cisco NX-OS to a port. Previously, point to point F and TF ports were used by a single edge device with a single login to the switch. With the adoption of the Cisco NPV technology, these types of switch ports can now have multiple logins from multiple edge devices on a single port. In such cases, the ports are no longer dedicated to a single edge device, but are shared by multiple devices similar to Inter-Switch Links (ISLs). The **switchport logical-type** command allows the you to change the port type so that port monitor and congestion timeout features apply core type policies and not the more aggressive edge type policies to such links.

### Procedure

**Step 1** Enter configuration mode:

switch# configure terminal

# **Step 2** Select a Fibre Channel interface and enter interface configuration submode:

**Step 3** Configure a logical type for an interface:

switch(config-if)# switchport logical-type {auto | core | edge}

(Optional) Remove the logical type from an interface:

switch(config-if)# no switchport logical-type {auto | core | edge}

# **Specifying a Port Owner**

Using the Port Owner feature, you can specify the owner of a port and the purpose for which a port is used so that the other administrators are informed.



Note The Portguard and Port Owner features are available for all ports regardless of the operational mode.

To specify or remove a port owner, perform these steps:

### Procedure

**Step 1** Enter configuration mode:

switch# configure terminal

**Step 2** Select the port interface:

switch(config)# interface fc1/1

**Step 3** Specify the owner of the switch port:

switch(config)# switchport owner description

The description can include the name of the owner and the purpose for which the port is used, and can be up to 80 characters long.

(Optional) Remove the port owner description:

switch(config)# no switchport owner

(Optional) Display the owner description specified for a port, use one of the following commands:

• switch# show running interface fc module-number/interface-number

• switch# show port internal info interface fc module-number/interface-number

### **Configuring Beacon Mode**

By default, the beacon mode is disabled on all switches. The beacon mode is indicated by a flashing green light that helps you identify the physical location of the specified interface. Note that configuring the beacon mode has no effect on the operation of the interface.

To configure a beacon mode for a specified interface or range of interfaces, perform these steps:

### Procedure

**Step 1** Enter configuration mode:

### switch# configure terminal

**Step 2** Select a Fibre Channel interface and enter interface configuration submode:

switch(config)# interface fc1/1

**Step 3** Enable the beacon mode for the interface:

switch(config-if)# switchport beacon

(Optional) Disable the beacon mode for the interface:

switch(config-if)# no switchport beacon

### Tip

The flashing green light turns on automatically when an external loopback that causes the interfaces to be isolated is detected. The flashing green light overrides the beacon mode configuration. The state of the LED is restored to reflect the beacon mode configuration after the external loopback is removed.

### **Configuring the Port Beacon LED**

To configure the port beacon LEDs on one or both ends of a link, perform this step:

switch# beacon interface fc *slot/port* {both | local | peer} [status {normal | warning | critical}] [duration *seconds*] [frequency *number*]

### **Configuring a Switch Port Attribute Default Value**

You can configure default values for various switch port attributes. These attributes will be applied globally to all future switch port configurations, even if you do not individually specify them at that time.

To configure a default value for a switch port attribute, perform these steps:

### Procedure

**Step 1** Enter configuration mode:

#### switch# configure terminal

**Step 2** Configure the default setting for the administrative state of an interface as up (the factory default setting is down): switch(config)# **no system default switchport shutdown** 

#### Note

This command is applicable only to interfaces for which no user configuration exists for the administrative state.

(Optional) Configure the default setting for the administrative state of an interface as down:

switch(config)# system default switchport shutdown

#### Note

This command is applicable only to interfaces for which no user configuration exists for the administrative state.

(Optional) Configure the default setting for the administrative trunk mode state of an interface as Auto:

switch(config)# system default switchport trunk mode auto

#### Note

The default setting is On.

### **Configuring the Port-Level Portguard**

All portguard causes are monitored over a common time interval with the same start and stop times. The *link down* counter is not a specific event, but the aggregation of all other cause counters in the same time interval.

To configure a port-level portguard for a interface, perform these steps:

### Procedure

**Step 1** Enter configuration mode:

switch# configure terminal

**Step 2** Select the interface:

switch(config)# interface fc1/1

**Step 3** Enable portguard error disabling of the interface if the link goes down once:

### switch(config-if)# errdisable detect cause link-down

(Optional) Enable portguard error disabling of the interface if the link flaps a certain number of times within the specified time, in *seconds*:

switch(config-if)# errdisable detect cause link-down [num-times number duration seconds ]

#### Note

The duration range is from 45 to 2000000 seconds. The duration must be equal to or greater than **num-times** multipled by 45.

(Optional) Remove the portguard configuration for the interface:

#### switch(config-if)# no errdisable detect cause link-down

The link resumes flapping and sending error reports normally.

**Step 4** Enable portguard error disabling of the interface if the specified error occurs once:

switch(config-if)# errdisable detect cause {trustsec-violation | bit-errors | credit-loss | link-reset | signal-loss |
sync-loss}

(Optional) Enable portguard error disabling of the interface if the specified error occurs a certain number times within the specified time, in *seconds*:

switch(config-if)# errdisable detect cause {trustsec-violation | bit-errors | credit-loss | link-reset | signal-loss | sync-loss | [num-times *number* duration *seconds* ]

(Optional) Remove the portguard configuration for the interface:

switch(config-if)# no errdisable detect cause {trustsec-violation | bit-errors | credit-loss | link-reset | signal-loss | sync-loss}

The link resumes flapping and sending error reports normally.

#### Note

The portguard credit loss event is triggered only on loop interfaces; it is not triggered on point-to-point interfaces.

This example shows how to configure portguard to set an interface to error disabled state if the link flaps 5 times within 225 seconds due to multiple causes. The portguard controls the interface in the following manner:

### Example

This example shows how to configure portguard to bring a port to down state if the link flaps 5 times within 225 seconds based on multiple causes:

```
switch# configure terminal
switch(config)# interface fc1/1
switch(config-if)# errdisable detect cause link-down num-times 5 duration 225
switch(config-if)# errdisable detect cause bit-errors num-times 5 duration 225
switch(config-if)# errdisable detect cause credit-loss num-times 5 duration 225
```

The above example sets the configuration to the following status:

- The port will be error disabled due to link down if the port suffers link failure due to link down 5 times in 225 seconds.
- The port will be error-disabled due to bit errors if the port suffers link failure due to bit errors 5 times in 225 seconds.
- The port will be error-disabled due to credit loss if the port suffers link failure due to credit loss 5 times in 225 seconds.

This example shows the internal information about a port in down state because of TrustSec violation:

```
switch# show interface fc1/9
fc1/9 is trunking
Hardware is Fibre Channel, SFP is short wave laser w/o OFC (SN)
```

```
Port WWN is 20:09:54:7f:ee:eb:dc:00
Peer port WWN is 20:49:8c:60:4f:53:bb:80
Admin port mode is auto, trunk mode is on
snmp link state traps are enabled
Port mode is TE
Port vsan is 1
Admin Speed is auto max 16 Gbps
Operating Speed is 4 Gbps
Rate mode is dedicated
Port flow-control is R RDY
Transmit B2B Credit is 500
Receive B2B Credit is 500
B2B State Change Number is 14
Receive data field Size is 2112
Beacon is turned off
Logical type is core
Belongs to port-channel2
Trunk vsans (admin allowed and active) (1-2,5)
Trunk vsans (up)
                                        (1-2)
Trunk vsans (isolated)
                                        (5)
Trunk vsans (initializing)
                                        ()
5 minutes input rate 448 bits/sec, 56 bytes/sec, 0 frames/sec
5 minutes output rate 384 bits/sec,48 bytes/sec, 0 frames/sec
  783328 frames input, 58490580 bytes
    0 discards,0 errors
    0 invalid CRC/FCS,0 unknown class
    0 too long,0 too short
  783799 frames output, 51234876 bytes
    0 discards,0 errors
  56 input OLS, 63 LRR, 8 NOS, 277 loop inits
  49 output OLS, 27 LRR, 49 NOS, 43 loop inits
  500 receive B2B credit remaining
  500 transmit B2B credit remaining
  500 low priority transmit B2B credit remaining
Last clearing of "show interface" counters : never
```

$$\mathcal{P}$$

- Tip
- Link down is the superset of all other causes. A port is brought to down state if the total number of other causes equals to the number of allowed link-down failures.
- Even if the link does not flap due to failure of the link, and portguard is not enabled, the port goes into a down state if too many invalid FLOGI requests are received from the same host. Use the **shut** and the **no shut** commands consecutively to bring up the link.

### **Configuring a Port Monitor**

Configuring a portguard action is optional for each counter in a port monitor policy, and is disabled by default.

### **Enabling a Port Monitor**

To enable or disable a port monitor, perform these steps:

L

### Procedure

 Step 1
 Enter configuration mode:

 switch# configure terminal

Step 2Enable port monitoring:<br/>switch(config)# port-monitor enable<br/>(Optional) Disable port monitoring:<br/>switch(config)# no port-monitor enable

### **Configuring the Check Interval**

To configure the check interval, perform these steps:

### Procedure

 Step 1 Enter the configuration mode: switch# configure terminal
 Step 2 Configure the check interval time to 30 seconds switch# port-monitor check-interval 30 To disable check interval use the following command: switch# no port-monitor check-interval

### **Configuring a Port Monitor Policy**

To configure a port monitor policy, perform these steps:

Step 1	Enter configuration mode:
	switch# configure terminal
Step 2	Specify the policy name and enter port monitoring policy configuration mode:
	switch(config)# port-monitor name policyname
	(Optional) Remove the policy name:

switch(config)# no port-monitor name policyname

**Step 3** Apply policy type:

switch(config-port-monitor)# logical-type {core | edge | all}

**Step 4** Specify the counter parameters:

Releases prior to Cisco MDS NX-OS Release 8.5(1)

switch(config-port-monitor)# counter {credit-loss-reco | err-pkt-from-port | err-pkt-from-xbar | err-pkt-to-xbar | invalid-crc | invalid-words | link-loss | lr-rx | lr-tx | rx-datarate | signal-loss | state-change | sync-loss | timeout-discards | tx-credit-not-available | tx-datarate | tx-discards | tx-slowport-oper-delay | txwait} poll-interval seconds {absolute | delta} rising-threshold count1 event RMON-ID warning-threshold count2 falling-threshold count3 event RMON-ID portguard { cong-isolate | errordisable | flap}

Cisco MDS NX-OS Release 8.5(1) and later releases

switch(config-port-monitor)# counter {credit-loss-reco | err-pkt-from-port | err-pkt-from-xbar | err-pkt-to-xbar | input-errors | invalid-crc | invalid-words | link-loss | lr-rx | lr-tx | rx-datarate | rx-datarate-burst | sfp-rx-power-low-warn | sfp-tx-power-low-warn | signal-loss | state-change | sync-loss | timeout-discards | tx-credit-not-available | tx-datarate | tx-datarate-burst | tx-discards | tx-slowport-oper-delay | txwait [warning-signal-threshold count1 alarm-signal-threshold count2 portguard congestion-signals]} poll-interval seconds {absolute | delta} rising-threshold count3 event RMON-ID [warning-threshold count4] [alerts [obfl rmon syslog | none]] [datarate count5 ] [falling-threshold count6] [portguard {DIRL | FPIN | cong-isolate | cong-isolate-recover | errordisable | flap]}

#### Note

- A port monitor policy cannot be configured as a combination of cong-isolate, cong-isolate-recover, DIRL, and FPIN port guard actions. For example, if in a policy you configure the tx-datarate, tx-datarate-burst, and txwait with DIRL portguard action and then configure the credit-loss-reco counter with the cong-isolate portguard action, you will not be able to activate the policy.
- Port monitor polling interval must not be more than the configured recovery interval when the cong-isolate, cong-isolate-recover, DIRL, and FPIN port guard actions are configured.
- We recommend that you use the delta threshold type for all the counters except the tx-slowport-oper-delay counter which uses absolute threshold type.
- The rx-datarate and tx-datarate are calculated using the inoctets and outoctets on an interface.
- You must activate the err-pkt-from-port, err-pkt-from-xbar, and err-pkt-to-xbar counters using the monitor counter name command, before specifying the counter parameters.
- Counters err-pkt-from-xbar, err-pkt-from-port, and err-pkt-to-xbar support delta threshold type only.
- Counter tx-slowport-oper-delay supports absolute threshold type only.
- Counter tx-slowport-oper-delay does not support portguard action.
- You must first enable ER\_RDY flow-control mode using the **system fc flow-control er\_rdy** command and then enable congestion isolation using the **feature congestion-isolation** command before setting the portguard action as congestion isolate (cong-isolate) and congestion isolation recovery (cong-isolate-recover).
- From Cisco MDS NX-OS Release 8.5(1), a new default *fabricmon\_edge\_policy* is introduced where FPIN is already configured for the supported counters.

- From Cisco MDS NX-OS Release 8.5(1), switches operating in the Cisco NPV mode do not support cong-isolate, cong-isolate-recover, DIRL, and FPIN portguard actions and the default *fabricmon\_edge\_policy*.
- When you configure a policy with the cong-isolate, cong-isolate-recover, DIRL, or FPIN portguard actions, you can expect multiple rising thresholds without waiting for a falling threshold.
- You must configure Exchange Diagnostic Capabilities (EDC) interval for congestion signal before configuring the TxWait **warning-signal-threshold** and **alarm-signal-threshold** values. For more information, see Configuring EDC Congestion Signal.
- Ensure that you provide at least one minute delay between deactivation and activation of port monitor policy when configuring the portguard actions **cong-isolate**, **cong-isolate-recover**, and **FPIN**.
- The **cong-isolate**, **cong-isolate-recover**, **DIRL**, and **FPIN** portguard actions are applicable only for logical-type edge policies.
- The **cong-isolate** and **cong-isolate-recover** port monitor portguard actions are supported only for the credit-loss-reco, tx-credit-not-available, tx-slowport-oper-delay, and txwait counters.
- The **DIRL** port monitor portguard action is supported only for the tx-datarate, tx-datarate-burst, and txwait counters.
- The **FPIN** port monitor portguard action is supported only for the link-loss, sync-loss, signal-loss, invalid-words, invalid-crc, and txwait counters.
- For SFP counters, **sfp-rx-power-low-warn** and **sfp-tx-power-low-warn**, the polling interval must be configured in multiples of 600 (10 minutes) and the rising threshold value should not exceed the multiple value of the polling interval. For example, if the polling interval is configure as 1800, which is 3 times 600, then the rising threshold value should not be more than 3.
- The rx-datarate-burst and tx-datarate-burst counters are configured as the number of 1-second bursts above 90% (default) detected in a polling interval. You can change the default datarate burst threshold using the **counter tx-datarate-burst poll-interval** *seconds* **delta rising-threshold** *count* **event** *RMON-ID* **datarate** *percentage* command.

(Optional) Revert to the default values for a counter:

Releases prior to Cisco MDS NX-OS Release 8.5(1)

switch(config-port-monitor)# no counter {credit-loss-reco | err-pkt-from-port | err-pkt-from-xbar | err-pkt-to-xbar | invalid-crc | invalid-words | link-loss | lr-rx | lr-tx | rx-datarate | signal-loss | state-change | sync-loss | timeout-discards | tx-credit-not-available | tx-datarate | tx-discards | tx-slowport-oper-delay | txwait} poll-interval seconds {absolute | delta} rising-threshold count1 event RMON-ID warning-threshold count2 falling-threshold count3 event RMON-ID portguard { cong-isolate | errordisable | flap}

Cisco MDS NX-OS Release 8.5(1) and later releases

switch(config-port-monitor)# no counter {credit-loss-reco | err-pkt-from-port | err-pkt-from-xbar | err-pkt-to-xbar | input-errors | invalid-crc | invalid-words | link-loss | lr-rx | lr-tx | rx-datarate | rx-datarate-burst | sfp-rx-power-low-warn | sfp-tx-power-low-warn | signal-loss | state-change | sync-loss | timeout-discards | tx-credit-not-available | tx-datarate | tx-datarate-burst | tx-discards | tx-slowport-oper-delay | txwait [warning-signal-threshold count1 alarm-signal-threshold count2 portguard congestion-signals]} poll-interval seconds {absolute | delta} rising-threshold count3 event RMON-ID [warning-threshold count4] [alerts [obfl rmon syslog | none]] [datarate count5 ] [falling-threshold count6] [portguard {DIRL | FPIN | cong-isolate | cong-isolate-recover | errordisable | flap]}

(Optional) Monitor a counter:

Releases prior to Cisco MDS NX-OS Release 8.5(1)

switch(config-port-monitor)# monitor counter {credit-loss-reco | err-pkt-from-port | err-pkt-from-xbar | err-pkt-to-xbar | input-errors | invalid-crc | invalid-words | link-loss | lr-rx | lr-tx | rx-datarate | signal-loss | state-change | sync-loss | timeout-discards | tx-credit-not-available | tx-datarate | tx-discards | tx-slowport-count | tx-slowport-oper-delay | txwait}

Cisco MDS NX-OS Release 8.5(1) and later releases

switch(config-port-monitor)# monitor counter {credit-loss-reco | err-pkt-from-port | err-pkt-from-xbar | err-pkt-to-xbar | input-errors | invalid-crc | invalid-words | link-loss | lr-rx | lr-tx | rx-datarate | rx-datarate-burst | sfp-rx-power-low-warn | sfp-tx-power-low-warn | signal-loss | state-change | sync-loss | timeout-discards | tx-credit-not-available | tx-datarate | tx-datarate-burst | tx-discards | tx-slowport-count | tx-slowport-oper-delay | txwait}

A port monitor currently recognizes two kinds of ports:

- Logical-type edge ports are normally F ports that are connected to end devices.
- Logical-type core ports are E ports (ISLs) or (T)F ports connected to Cisco NPV switches. Some of the edge port
  counter thresholds and port-guard actions might not be appropriate on the TF ports in the port-monitor configurations.
  Specifically, portguard *disable*, *flap*, and *isolate* actions can affect multiple end devices on the F ports. Therefore,
  performing disable, flap, or isolate actions should be avoided on an N-Port Identifier Virtualization (NPIV) system.

### **Activating a Port Monitor Policy**

To activate a port monitor policy, perform these steps:

#### Procedure

Step 1	Enter configuration mode:
	switch# configure terminal
Step 2	Activate the specified port monitor policy:
	<pre>switch(config)# port-monitor activate policyname</pre>
	(Optional) Activate the default port monitor policy:
	<pre>switch(config)# port-monitor activate</pre>
	(Optional) Deactivate the specified port monitoring policy:
	<pre>switch(config)# no port-monitor activate policyname</pre>

### **Configuring Logging Level for Port Monitor**

To configure logging level for port monitor syslog messages, perform the steps below:

### Procedure

**Step 1** Enter configuration mode:

switch# configure terminal

Step 2Configure a logging level for port monitor syslog messages:<br/>switch(config)# logging level pmon severity-level<br/>(Optional) Revert to the default logging level for the port monitor syslog messages:<br/>switch(config)# no logging level pmon

### **Configuring Port Monitor Portguard**

To configure a port monitor portguard action, perform these steps:

### Procedure

**Step 1** Enter configuration mode:

switch# configure terminal

**Step 2** Specify the policy name and enter port monitoring policy configuration mode:

switch(config)# port-monitor name policyname

(Optional) Remove the policy:

switch(config)# no port-monitor name policyname

**Step 3** Specify a counter, its parameters, and a portguard action for a counter:

Releases prior to Cisco MDS NX-OS Release 8.5(1)

switch(config-port-monitor)# counter {credit-loss-reco | err-pkt-from-port | err-pkt-from-xbar | err-pkt-to-xbar | invalid-crc | invalid-words | link-loss | lr-rx | lr-tx | rx-datarate | signal-loss | state-change | sync-loss | timeout-discards | tx-credit-not-available | tx-datarate | tx-discards | tx-slowport-oper-delay | txwait} poll-interval seconds {absolute | delta} rising-threshold count1 event RMON-ID warning-threshold count2 falling-threshold count3 event RMON-ID portguard { cong-isolate | errordisable | flap}

Cisco MDS NX-OS Release 8.5(1) and later releases

switch(config-port-monitor)# counter {credit-loss-reco | err-pkt-from-port | err-pkt-from-xbar | err-pkt-to-xbar | input-errors | invalid-crc | invalid-words | link-loss | lr-rx | lr-tx | rx-datarate | rx-datarate-burst | sfp-rx-power-low-warn | sfp-tx-power-low-warn | signal-loss | state-change | sync-loss | timeout-discards | tx-credit-not-available | tx-datarate | tx-datarate-burst | tx-discards | tx-slowport-oper-delay | txwait [warning-signal-threshold *count1* alarm-signal-threshold *count2* portguard congestion-signals]} poll-interval *seconds* {absolute | delta} rising-threshold *count3* event *RMON-ID* [warning-threshold *count4*] [alerts [obf1 rmon syslog | none]] [datarate *count5* ] [falling-threshold *count6*] [portguard {DIRL + FPIN + cong-isolate | cong-isolate-recover + errordisable | flap]}

#### Note

- A port monitor policy cannot be configured as a combination of cong-isolate, cong-isolate-recover, DIRL, and FPIN port guard actions. For example, if in a policy you configure the tx-datarate, tx-datarate-burst, and txwait with DIRL portguard action and then configure the credit-loss-reco counter with the cong-isolate portguard action, you will not be able to activate the policy.
- Port monitor polling interval must not be more than the configured recovery interval when the cong-isolate, cong-isolate-recover, DIRL, and FPIN port guard actions are configured.
- We recommend that you use the delta threshold type for all the counters except the tx-slowport-oper-delay counter which uses absolute threshold type.
- The rx-datarate and tx-datarate are calculated using the inoctets and outoctets on an interface.
- You must activate the err-pkt-from-port, err-pkt-from-xbar, and err-pkt-to-xbar counters using the monitor counter name command, before specifying the counter parameters.
- Counters err-pkt-from-xbar, err-pkt-from-port, and err-pkt-to-xbar support delta threshold type only.
- Counter tx-slowport-oper-delay supports absolute threshold type only.
- Counter tx-slowport-oper-delay does not support portguard action.
- You must first enable ER\_RDY flow-control mode using the **system fc flow-control er\_rdy** command and then enable congestion isolation using the **feature congestion-isolation** command before setting the portguard action as congestion isolate (cong-isolate) and congestion isolation recovery (cong-isolate-recover).
- From Cisco MDS NX-OS Release 8.5(1), a new default *fabricmon\_edge\_policy* is introduced where FPIN is already configured for the supported counters.
- From Cisco MDS NX-OS Release 8.5(1), switches operating in the Cisco NPV mode do not support cong-isolate, cong-isolate-recover, DIRL, and FPIN portguard actions and the default *fabricmon\_edge\_policy*.
- When you configure a policy with the cong-isolate, cong-isolate-recover, DIRL, or FPIN portguard actions, you can expect multiple rising thresholds without waiting for a falling threshold.
- You must configure Exchange Diagnostic Capabilities (EDC) interval for congestion signal before configuring the TxWait **warning-signal-threshold** and **alarm-signal-threshold** values. For more information, see Configuring EDC Congestion Signal.
- Ensure that you provide at least one minute delay between deactivation and activation of port monitor policy when configuring the portguard actions **cong-isolate**, **cong-isolate-recover**, and **FPIN**.
- The **cong-isolate**, **cong-isolate-recover**, **DIRL**, and **FPIN** portguard actions are applicable only for logical-type edge policies.
- The **cong-isolate** and **cong-isolate-recover** port monitor portguard actions are supported only for the credit-loss-reco, tx-credit-not-available, tx-slowport-oper-delay, and txwait counters.
- The **DIRL** port monitor portguard action is supported only for the tx-datarate, tx-datarate-burst, and txwait counters.
- The **FPIN** port monitor portguard action is supported only for the link-loss, sync-loss, signal-loss, invalid-words, invalid-crc, and txwait counters.
- For SFP counters, **sfp-rx-power-low-warn** and **sfp-tx-power-low-warn**, the polling interval must be configured in multiples of 600 (10 minutes) and the rising threshold value should not exceed the multiple value of the polling

interval. For example, if the polling interval is configure as 1800, which is 3 times 600, then the rising threshold value should not be more than 3.

• The rx-datarate-burst and tx-datarate-burst counters are configured as the number of 1-second bursts above 90% (default) detected in a polling interval. You can change the default datarate burst threshold using the **counter tx-datarate-burst poll-interval** *seconds* **delta rising-threshold** *count* **event** *RMON-ID* **datarate** *percentage* command.

### **Configuring Port Group Monitor**

### **Enabling a Port Group Monitor**

To enable a port group monitor, perform these steps:

### Procedure

- Step 1
   Enter configuration mode:

   switch# configure terminal
- Step 2
   Enable port monitoring:

   switch(config)# port-group-monitor enable

   (Optional) Disable port monitoring:

   switch(config)# no port-group-monitor enable

### **Configuring a Port Group Monitor Policy**

To configure a port group monitor policy, perform these steps:

01	Enter configuration mode: switch# configure terminal
) 2	Specify the policy name and enter port group monitoring policy configuration mode: switch(config)# <b>port-group-monitor name</b> policyname
	(Optional) Remove the policy:
	<pre>switch(config)# no port-group-monitor name policyname</pre>
o 3	Specify the delta receive or transmit counter poll interval (in seconds) and thresholds (in percentage):

switch(config-port-group-monitor)# counter {rx-datarate | tx-datarate} poll-interval seconds delta rising-threshold percentage1 falling-threshold percentage2

(Optional) Revert to the default policy:

switch(config-port-group-monitor)# no counter tx-datarate

For more information on reverting to the default policy, see Reverting to the Default Policy for a Specific Counter and Port Group Monitor.

**Step 4** Turn on datarate monitoring:

switch(config-port-group-monitor)# monitor counter {rx-datarate | tx-datarate}

(Optional) Turn off datarate monitoring:

switch(config-port-group-monitor)# no monitor counter {rx-datarate | tx-datarate}

For more information on turning off transmit datarate monitoring, see Turning Off the Monitoring of Specific Counter.

#### Note

On 8-Gbps and higher speed modules, port errors are monitored using the **invalid-crc** and **invalid-words** counters. The **err-pkt-from-port** counter is supported only on 4-Gbps modules.

### **Reverting to the Default Policy for a Specific Counter**

The following examples display the default values for counters:

```
switch(config) # port-group-monitor name PGMON policy
switch (config-port-group-monitor) # counter tx-datarate poll-interval 200 delta
rising-threshold 75 falling-threshold 0 \,
switch(config)# show port-group-monitor PGMON policy
Policy Name : PGMON policy
Admin status : Not Active
Oper status : Not Active
Port type
         : All Port Groups
_____
Counter
           Threshold Interval %ge Rising Threshold %ge Falling Threshold
_____
           ______
RX Datarate Delta 200 75
                                         0
                  60
                         80
TX Datarate Delta
                                         20
switch(config-port-group-monitor)# no counter tx-datarate
switch(config) # show port-group-monitor PGMON policy
Policy Name : PGMON policy
Admin status : Not Active
Oper status : Not Active
Port type
         : All Port Groups
_____
Counter Threshold Interval %ge Rising Threshold %ge Falling Threshold
           _____ ____
_____
RX Datarate Delta 60 80
TX Datarate Delta 60 80
                                        10
                                        10
                        _____
```

### **Turning Off Specific Counter Monitoring**

The following examples display turning off counter monitoring:

```
switch(config)# port-group-monitor name PGMON_policy
switch(config-port-group-monitor)# no monitor counter rx-datarate
switch(config)# show port-group-monitor PGMON_policy
Policy Name : PGMON_policy
Admin status : Not Active
Oper status : Not Active
Port type : All Port Groups
------
Counter Threshold Interval %ge Rising Threshold %ge Falling Threshold
------
TX Datarate Delta 60 100 80
```

### **Activating a Port Group Monitor Policy**

To activate a port group monitor policy, perform these steps:

### Procedure

Step 1	1 Enter configuration mode:	
	switch# configure terminal	
Step 2	Activate the specified port group monitor policy:	
	<pre>switch(config)# port-group-monitor activate policyname</pre>	
	(Optional) Activate the default port group monitor policy:	
	<pre>switch(config)# port-group-monitor activate</pre>	
	(Optional) Deactivate the specified port group monitor policy:	
	<pre>switch(config)# no port-group-monitor activate policyname</pre>	

# **Configuring Management Interfaces**

### **Configuring the Management Interface Over IPv4**

To configure the mgmt0 Ethernet interface to connect over IPv4, perform these steps:

Step 1	Enter configuration mode:		
	switch# configure terminal		
Step 2	Select the management Ethernet interface on the switch and enter interface configuration submode:		
	switch(config)# interface mgmt0		

I

Step 3	Configure the IPv4 address and IPv4 subnet mask: switch(config-if)# <b>ip address 10.16.1.2 255.255.255.0</b>	
Step 4	Enable the interface: switch(config-if)# no shutdown	
Step 5	Return to configuration mode: switch(config-if)# exit	
Step 6	Configure the default gateway IPv4 address: switch(config)# <b>ip default-gateway 1.1.1.4</b>	
Step 7	Return to user EXEC mode: switch(config)# <b>exit</b> (Optional) Save your configuration changes to the file system: switch# <b>copy running-config startup-config</b>	

### **Configuring the Management Interface Over IPv6**

To configure the mgmt0 Ethernet interface to connect over IPv6, perform these steps:

Step 1	Enter configuration mode:		
	switch# conligure terminal		
Step 2	Select the management Ethernet interface on the switch and enter interface configuration submode:		
	switch(config)# interface mgmt0		
Step 3	Enable IPv6 and assign a link-local address on the interface:		
	switch(config-if)# ipv6 enable		
Step 4	Specify an IPv6 unicast address and prefix length on the interface:		
	switch(config-if)# ipv6 address 2001:0db8:800:200c::417a/64		
Step 5	Enable the interface:		
	switch(config-if)# no shutdown		
Step 6	Return to user EXEC mode:		
	switch(config)# exit		
	(Optional) Save your configuration changes to the file system:		

switch# copy running-config startup-config

# **Creating VSAN Interfaces**

To create a VSAN interface, perform these steps:

Step 1	Enter configuration mode:
	switch# configure terminal
Step 2	Configure a VSAN with the ID 2:
	<pre>switch(config)# interface vsan 2</pre>
Step 3	Enable the VSAN interface:
	switch(config-if)# no shutdown

# **Verifying Interface Configuration**

### **Display interface information**

Run the **show interface** command to display physical interface related information. Without any arguments, this command displays the information for all the configured interfaces in the switch.

The command output format has evolved over time. Outputs may differ if not running the latest release of Cisco MDS NX-OS

#### **Displays all interfaces**

```
switch#show interface
fc1/1 is up
   Hardware is Fibre Channel, SFP is short wave laser w/o OFC (SN)
    Port WWN is 20:01:00:2a:6a:26:a1:e0
    Peer port WWN is 21:10:00:24:ff:98:01:01
    Admin port mode is F, trunk mode is on
   snmp link state traps are enabled
    Port mode is F, FCID is 0xe90c00
   Port vsan is 1
   Admin Speed is auto
    Operating Speed is 4 Gbps
   Rate mode is dedicated
   Port flow-control is R RDY
   Transmit B2B Credit is 16
   Receive B2B Credit is 64
    B2B State Change: Admin(on), Oper(down)
   Receive data field Size is 2112
   Beacon is turned off
   Logical type is edge
    5 minutes input rate 0 bits/sec,0 bytes/sec, 0 frames/sec
    5 minutes output rate 0 bits/sec,0 bytes/sec, 0 frames/sec
      16 frames input, 1312 bytes, 82 bytes/frame average frame size
        0 discards,0 errors
        0 invalid CRC/FCS, 0 unknown class
        0 too long,0 too short
      17 frames output, 1232 bytes, 72 bytes/frame average frame size
        0 discards,0 errors
      0 input OLS, 0 LRR, 0 NOS, 0 loop inits
      1 output OLS,1 LRR, 0 NOS, 0 loop inits
    64 receive B2B credit remaining
    16 transmit B2B credit remaining
    16 low priority transmit B2B credit remaining
    0 timeout discards, 0 credit loss
    O link failures, O sync losses, O signal losses
    Percentage TxWait for last 1s/1m/1h/72h: 0%/0%/0%/0%
    Interface last changed at Sat Apr 19 17:08:22 2025
   Last clearing of "show interface" counters: never
    Transceiver Information:
      Serial number is FNS190413TV
      Cisco pid is DS-SFP-FC16G-SW
      Temperature 40.12 C, Voltage 3.34 V, Current 8.76 mA, TxPower -3.61 dBm, R
xPower -3.92 dBm
      Power control is not supported, Power is on
fc1/2 is trunking
   Hardware is Fibre Channel, SFP is short wave laser w/o OFC (SN)
   Port WWN is 20:03:00:2a:6a:26:a1:e0
    Peer port WWN is 20:03:00:de:fb:74:e4:60
```

```
Admin port mode is auto, trunk mode is on
    snmp link state traps are enabled
    Port mode is TE
    Port vsan is 1
   Admin Speed is auto
    Operating Speed is 4 Gbps
   Rate mode is dedicated
   Port flow-control is R RDY
    Transmit B2B Credit is 500
    Receive B2B Credit is 64
   B2B State Change: Admin(on), Oper(up), Negotiated Value(14)
    Receive data field Size is 2112
   Beacon is turned off
   Logical type is core
   Trunk vsans (admin allowed and active) (1)
   Trunk vsans (up)
                                            (1)
    Trunk vsans (isolated)
                                            ()
   Trunk vsans (initializing)
                                           ()
    5 minutes input rate 32 bits/sec, 4 bytes/sec, 0 frames/sec
    5 minutes output rate 32 bits/sec, 4 bytes/sec, 0 frames/sec
      493 frames input, 42776 bytes, 86 bytes/frame average frame size
        0 discards,0 errors
       0 invalid CRC/FCS,0 unknown class
       0 too long,0 too short
      493 frames output, 45400 bytes, 92 bytes/frame average frame size
        0 discards,0 errors
      0 input OLS, 0 LRR, 0 NOS, 0 loop inits
      1 output OLS, 2 LRR, 0 NOS, 1 loop inits
    64 receive B2B credit remaining
    500 transmit B2B credit remaining
    485 low priority transmit B2B credit remaining
    0 timeout discards, 0 credit loss
    O link failures, O sync losses, O signal losses
    Percentage TxWait for last 1s/1m/1h/72h: 0%/0%/0%
    Interface last changed at Sat Apr 19 17:08:25 2025
   Last clearing of "show interface" counters: never
    Transceiver Information:
      Serial number is FNS19130U1L
      Cisco pid is DS-SFP-FC16G-SW
     Temperature 43.41 C, Voltage 3.33 V, Current 8.62 mA, TxPower -2.50 dBm, R
xPower -3.96 dBm
      Power control is not supported, Power is on
fc1/3 is down (Link failure or not-connected)
    Hardware is Fibre Channel, SFP is short wave laser w/o OFC (SN)
    Port WWN is 20:04:00:2a:6a:26:a1:e0
   Admin port mode is auto, trunk mode is on
    snmp link state traps are enabled
    Port vsan is 1
    Receive data field Size is 2112
   Beacon is turned off
   Logical type is Unknown(0)
    5 minutes input rate 0 bits/sec,0 bytes/sec, 0 frames/sec
    5 minutes output rate 0 bits/sec,0 bytes/sec, 0 frames/sec
      0 frames input, 0 bytes, 0 bytes/frame average frame size
        0 discards,0 errors
        0 invalid CRC/FCS,0 unknown class
        0 too long,0 too short
      0 frames output, 0 bytes, 0 bytes/frame average frame size
        0 discards,0 errors
      0 input OLS, 0 LRR, 0 NOS, 0 loop inits
      0 output OLS,0 LRR, 0 NOS, 0 loop inits
    0 timeout discards, 0 credit loss
    O link failures, O sync losses, O signal losses
```

```
Percentage TxWait for last 1s/1m/1h/72h: 0%/0%/0%
    Last clearing of "show interface" counters: never
    Transceiver Information:
      Serial number is FNS18150JCU
      Cisco pid is DS-SFP-FC16G-SW
      Temperature 44.30 C, Voltage 3.32 V, Current 7.91 mA, TxPower -2.99 dBm, R
xPower -3.67 dBm
      Power control is not supported, Power is on
sup-fc0 is up
    Hardware is Fibre Channel
    Speed is 1 Gbps
    1978 packets input, 222120 bytes
      0 multicast frames, 0 compressed
      0 input errors, 0 frame
      0 overrun, 0 fifo
    1980 packets output, 252544 bytes
      0 underruns, 0 output errors
      0 collisions, 0 fifo
      0 carrier errors
IPStorage1/1 is down (SFP not present)
    Hardware is IPStorage, address is f40f.1b72.ca33
    Internet address(es):
   MTU 1500 bytes
   Port mode is IPS
    Beacon is turned off
   Auto-Negotiation is turned on
    5 minutes input rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
    5 minutes output rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
    0 packets input, 0 bytes, 0 bytes/packet average packet size
      0 multicast frames, 0 compressed
      0 input errors, 0 frame, 0 overrun 0 fifo
    0 packets output, 0 bytes, 0 bytes/packet average packet size, 0 underruns
      0 output errors, 0 collisions, 0 fifo
      0 carrier errors
fcip1 is down (Tunnel port src interface unbound)
    Hardware is IPStorage
    Port WWN is 00:00:00:00:00:00:00:00
   Admin port mode is auto, trunk mode is on
    snmp link state traps are enabled
    Port vsan is 1
    Belongs to port-channel50
    Peer Information
   Write acceleration mode is configured off
    Tape acceleration mode is configured off
    Tape Accelerator flow control buffer size is automatic
    FICON XRC Accelerator is configured off
    Ficon Load Balancer configured off for all vsans
   Ficon Tape acceleration configured off for all vsans
    IP Compression is disabled
   Maximum number of TCP connections is 2
    QOS control code point is 0
    QOS data code point is 0
    TCP Connection Information
      0 Active TCP connections
        O Attempts for active connections, O close of connections
    5 minutes input rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
    5 minutes output rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
      0 frames input, 0 bytes, 0 bytes/frame average frame size
         O Class F frames input, O bytes
         O Class 2/3 frames input, O bytes
         0 Reass frames
```

```
0 Error frames timestamp error 0
     0 frames output, 0 bytes, 0 bytes/frame average frame size
        0 Class F frames output, 0 bytes
        0 Class 2/3 frames output, 0 bytes
        0 Error frames
mgmt0 is up
   Internet address is 10.197.111.181/24
    Hardware is GigabitEthernet
   Address is f40f.1b72.ca30
   MTU 1500 bytes, BW 1000 Mbps full Duplex
    42241 packets input, 3274206 bytes
     0 multicast frames, 0 compressed
     0 input errors, 0 frame
     0 overrun, 0 fifo
    110 packets output, 24487 bytes
     0 underruns, 0 output errors
      0 collisions, 0 fifo
     0 carrier errors
Ethernet1/1 is down (SFP not inserted)
admin state is down, Dedicated Interface
  Hardware: 10000 Ethernet, address: f40f.1b72.ca35 (bia f40f.1b72.ca35)
 MTU bytes (CoS values): MTU 1500(0-2,4-7) bytes MTU 2112(3) bytes
  BW 10000000 Kbit, DLY 10 usec, reliability 255/255, txload 1/255, rxload 1/255
 Encapsulation ARPA, medium is broadcast
  Port mode is access
  auto-duplex, auto-speed
  Beacon is turned off
 Auto-Negotiation is turned on
  Input flow-control is off, output flow-control is off
 Auto-mdix is turned off
  Switchport monitor is off
  Last link flapped never
 Last clearing of "show interface" counters never
  0 interface resets
  Load-Interval #1: 30 seconds
    30 seconds input rate 0 bits/sec, 0 packets/sec
    30 seconds output rate 0 bits/sec, 0 packets/sec
   input rate 0 bps, 0 pps; output rate 0 bps, 0 pps
  Load-Interval #2: 5 minute (300 seconds)
    300 seconds input rate 0 bits/sec, 0 packets/sec
    300 seconds output rate 0 bits/sec, 0 packets/sec
    input rate 0 bps, 0 pps; output rate 0 bps, 0 pps
  RX
   0 unicast packets 0 multicast packets 0 broadcast packets
   0 input packets 0 bytes
   0 jumbo packets 0 storm suppression packets
   0 runts 0 giants 0 CRC/FCS 0 no buffer
    0 input error 0 short frame 0 overrun 0 underrun 0 ignored
   0 watchdog 0 bad etype drop 0 bad proto drop 0 if down drop
   0 input with dribble 0 input discard
   0 Rx pause
  ТΧ
   0 unicast packets 0 multicast packets 0 broadcast packets
    0 output packets 0 bytes
   0 jumbo packets
    0 output error 0 collision 0 deferred 0 late collision
    0 lost carrier 0 no carrier 0 babble 0 output discard
    0 Tx pause
port-channel7 is down (No operational members)
   Hardware is Fibre Channel
    Port WWN is 24:07:00:2a:6a:26:a1:e0
```

```
Admin port mode is auto, trunk mode is on
snmp link state traps are enabled
Port vsan is 1
Logical type is Unknown(0)
5 minutes input rate 0 bits/sec,0 bytes/sec, 0 frames/sec
5 minutes output rate 0 bits/sec,0 bytes/sec, 0 frames/sec
  0 frames input, 0 bytes, 0 bytes/frame average frame size
    0 discards,0 errors
    0 invalid CRC/FCS,0 unknown class
    0 too long,0 too short
  0 frames output, 0 bytes, 0 bytes/frame average frame size
    0 discards,0 errors
  0 input OLS, 0 LRR, 0 NOS, 0 loop inits
  0 output OLS, 0 LRR, 0 NOS, 0 loop inits
O timeout discards, O credit loss
0 link failures, 0 sync losses, 0 signal losses
Percentage TxWait for last 1s/1m/1h/72h: 0%/0%/0%
No members
```

#### Displays the counters for all interfaces

```
switch# show interface counters
fc1/1
    5 minutes input rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
    5 minutes output rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
   16 frames input, 1312 bytes, 82 bytes/frame average frame size
      0 class-2 frames, 0 bytes
     16 class-3 frames, 1312 bytes
     0 class-f frames, 0 bytes
      0 discards, 0 errors, 0 CRC/FCS
     0 unknown class, 0 too long, 0 too short
    17 frames output, 1232 bytes, 72 bytes/frame average frame size
      0 class-2 frames, 0 bytes
     17 class-3 frames, 1232 bytes
      0 class-f frames, 0 bytes
      0 discards, 0 errors
    O timeout discards, O credit loss
    0 input OLS, 0 LRR, 0 NOS, 0 loop inits
    1 output OLS, 1 LRR, 0 NOS, 0 loop inits
    0 link failures, 0 sync losses, 0 signal losses
    3 Transmit B2B credit transitions to zero
    1 Receive B2B credit transitions to zero
      0 2.5us TxWait due to lack of transmit credits
    Percentage TxWait for last 1s/1m/1h/72h: 0%/0%/0%/0%
    64 receive B2B credit remaining
    16 transmit B2B credit remaining
   16 low priority transmit B2B credit remaining
    Last clearing of "show interface" counters: never
f_{c1/2}
    5 minutes input rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
    5 minutes output rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
    14 frames input, 1124 bytes, 80 bytes/frame average frame size
     0 class-2 frames, 0 bytes
      14 class-3 frames, 1124 bytes
      0 class-f frames, 0 bytes
      0 discards, 0 errors, 0 CRC/FCS
      0 unknown class, 0 too long, 0 too short
    15 frames output, 1036 bytes, 69 bytes/frame average frame size
     0 class-2 frames, 0 bytes
      15 class-3 frames, 1036 bytes
     0 class-f frames, 0 bytes
     0 discards, 0 errors
    0 timeout discards, 0 credit loss
    0 input OLS, 0 LRR, 0 NOS, 0 loop inits
```

```
1 output OLS, 1 LRR, 0 NOS, 0 loop inits
0 link failures, 0 sync losses, 0 signal losses
3 Transmit B2B credit transitions to zero
1 Receive B2B credit transitions to zero
```

#### **Displays an particular interface**

```
switch# show interface fc1/1
fc1/1 is up
   Hardware is Fibre Channel, SFP is short wave laser w/o OFC (SN)
   Port WWN is 20:01:00:2a:6a:26:a1:e0
   Peer port WWN is 21:10:00:24:ff:98:01:01
   Admin port mode is F, trunk mode is on
   snmp link state traps are enabled
   Port mode is F, FCID is 0xe90c00
   Port vsan is 1
   Admin Speed is auto
   Operating Speed is 4 Gbps
   Rate mode is dedicated
   Port flow-control is R RDY
   Transmit B2B Credit is 16
   Receive B2B Credit is 64
   B2B State Change: Admin(on), Oper(down)
   Receive data field Size is 2112
   Beacon is turned off
   Logical type is edge
   5 minutes input rate 0 bits/sec,0 bytes/sec, 0 frames/sec
   5 minutes output rate 0 bits/sec,0 bytes/sec, 0 frames/sec
     16 frames input, 1312 bytes, 82 bytes/frame average frame size
       0 discards,0 errors
       0 invalid CRC/FCS, 0 unknown class
       0 too long,0 too short
     17 frames output, 1232 bytes, 72 bytes/frame average frame size
       0 discards,0 errors
     0 input OLS, 0 LRR, 0 NOS, 0 loop inits
     1 output OLS,1 LRR, 0 NOS, 0 loop inits
   64 receive B2B credit remaining
   16 transmit B2B credit remaining
   16 low priority transmit B2B credit remaining
   0 timeout discards, 0 credit loss
   O link failures, O sync losses, O signal losses
   Percentage TxWait for last 1s/1m/1h/72h: 0%/0%/0%/0%
   Interface last changed at Sat Apr 19 17:08:22 2025
   Last clearing of "show interface" counters: never
   Transceiver Information:
      Serial number is FNS190413TV
      Cisco pid is DS-SFP-FC16G-SW
      Temperature 39.20 C, Voltage 3.34 V, Current 8.76 mA, TxPower -3.59 dBm, R
xPower -3.92 dBm
      Power control is not supported, Power is on
```

### Displays the counters of an particular interface

```
switch# show interface fc1/1 counters
fc1/1
5 minutes input rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
5 minutes output rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
16 frames input, 1312 bytes, 82 bytes/frame average frame size
0 class-2 frames, 0 bytes
16 class-3 frames, 1312 bytes
0 class-f frames, 0 bytes
0 discards, 0 errors, 0 CRC/FCS
0 unknown class, 0 too long, 0 too short
```

0

```
17 frames output, 1232 bytes, 72 bytes/frame average frame size
 0 class-2 frames, 0 bytes
 17 class-3 frames, 1232 bytes
  0 class-f frames, 0 bytes
  0 discards, 0 errors
0 timeout discards, 0 credit loss
0 input OLS, 0 LRR, 0 NOS, 0 loop inits
1 output OLS, 1 LRR, 0 NOS, 0 loop inits
O link failures, O sync losses, O signal losses
3 Transmit B2B credit transitions to zero
1 Receive B2B credit transitions to zero
 0 2.5us TxWait due to lack of transmit credits
Percentage TxWait for last 1s/1m/1h/72h: 0%/0%/0%
64 receive B2B credit remaining
16 transmit B2B credit remaining
16 low priority transmit B2B credit remaining
Last clearing of "show interface" counters: never
```

#### Displays the details of counters of an particular interface

```
switch# show interface fc1/1 counters detailed
fc1/1
Rate Stats:
 Rx 5 min rate bit/sec:
                                                                                0
 Tx 5 min rate bit/sec:
                                                                                Ω
                                                                                0
 Rx 5 min rate bytes/sec:
 Tx 5 min rate bytes/sec:
                                                                                0
 Rx 5 min rate frames/sec:
                                                                                0
 Tx 5 min rate frames/sec:
                                                                                0
Total Stats:
 Rx total frames:
                                                                               16
 Tx total frames:
                                                                               17
                                                                             1312
 Rx total bytes:
                                                                             1232
 Tx total bytes:
 Rx bytes/frame average frame size:
                                                                               82
                                                                               72
 Tx bytes/frame average frame size:
 Rx total multicast:
                                                                                0
 Tx total multicast:
                                                                                0
 Rx total broadcast:
                                                                                0
 Tx total broadcast:
                                                                                0
 Rx total unicast:
                                                                               16
 Tx total unicast:
                                                                               17
 Rx total discards:
                                                                                0
 Tx total discards:
                                                                                0
 Rx total errors:
                                                                                0
 Tx total errors:
                                                                                0
 Rx class-2 frames:
                                                                                0
 Tx class-2 frames:
                                                                                0
 Rx class-2 bytes:
                                                                                0
 Tx class-2 bytes:
                                                                                0
 Rx class-2 frames discards:
                                                                                0
                                                                                0
 Rx class-2 port reject frames:
 Rx class-3 frames:
                                                                               16
 Tx class-3 frames:
                                                                               17
 Rx class-3 bytes:
                                                                             1312
 Tx class-3 bytes:
                                                                             1232
 Rx class-3 frames discards:
                                                                                0
 Rx class-f frames:
                                                                                0
 Tx class-f frames:
                                                                                0
 Rx class-f bytes:
                                                                                0
 Tx class-f bytes:
                                                                                0
 Rx class-f frames discards:
```

Link	Stats:	
Rx	Link failures:	0
Rx	Sync losses:	0
Rx	Signal losses:	0
Rx	Primitive sequence protocol errors:	0
Rx	Invalid transmission words:	0
Rx	Invalid CRCs:	0
Rx	Delimiter errors:	0
Rx	fragmented frames:	0
Rx	frames with EOF aborts:	0
Rx	unknown class frames:	0
Rx	Runt frames:	0
Rx	Jabber frames:	0
Rx	too long:	0
Rx	too short:	0
Rx	Link Reset(LR) while link is active:	0
Τx	Link Reset(LR) while link is active:	0
Rx	Link Reset Responses(LRR):	0
Τx	Link Reset Responses(LRR):	1
Rx	Offline Sequences(OLS):	0
Τx	Offline Sequences(OLS):	1
Rx	Non-Operational Sequences(NOS):	0
Τx	Non-Operational Sequences (NOS):	0
BB_	SCs credit resend actions:	0
BB_	SCr Tx credit increment actions:	0
Loop	Stats:	
Rx	F8 type LIP sequence errors:	0
Τx	F8 type LIP sequence errors:	0
Rx	Non F8 type LIP sequence errors:	0
Τx	Non F8 type LIP sequence errors:	0
Conc	gestion Stats:	
Τx	Timeout discards:	0
Τx	Credit loss:	0
Tx₩	Nait 2.5us due to lack of transmit credits:	0
Per	ccentage TxWait for last 1s/1m/1h/72h:	0%/0%/0%/0%
Rx	B2B credit remaining:	0
Τx	B2B credit remaining:	0
Τx	Low Priority B2B credit remaining:	0
Rx	B2B credit transitions to zero:	1
Τx	B2B credit transitions to zero:	3
Last	clearing of "show interface" counters :	never

### **Displays the FCIP interface**

```
switch# show interface fcip 1
fcip1 is down (Tunnel port src interface unbound)
   Hardware is IPStorage
   Port WWN is 00:00:00:00:00:00:00:00
   Admin port mode is auto, trunk mode is on
   snmp link state traps are enabled
   Port vsan is 1
   Belongs to port-channel50
   Peer Information
   Write acceleration mode is configured off
   Tape acceleration mode is configured off
   Tape Accelerator flow control buffer size is automatic
   FICON XRC Accelerator is configured off
   Ficon Load Balancer configured off for all vsans
   Ficon Tape acceleration configured off for all vsans
   IP Compression is disabled
   Maximum number of TCP connections is 2
```

```
QOS control code point is 0
QOS data code point is 0
TCP Connection Information
 0 Active TCP connections
   O Attempts for active connections, O close of connections
5 minutes input rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
5 minutes output rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
  0 frames input, 0 bytes, 0 bytes/frame average frame size
     O Class F frames input, O bytes
     0 Class 2/3 frames input, 0 bytes
     0 Reass frames
    0 Error frames timestamp error 0
  0 frames output, 0 bytes, 0 bytes/frame average frame size
     O Class F frames output, O bytes
     0 Class 2/3 frames output, 0 bytes
     0 Error frames
```

#### **Displays the counters of a FCIP interface**

```
switch# show interface fcip 1 counters
fcip1
   TCP Connection Information
     0 Active TCP connections
       O Attempts for active connections, O close of connections
   5 minutes input rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
   5 minutes output rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
      0 frames input, 0 bytes, 0 bytes/frame average frame size
         O Class F frames input, O bytes
        0 Class 2/3 frames input, 0 bytes
        0 Reass frames
        0 Error frames timestamp error 0
      0 frames output, 0 bytes, 0 bytes/frame average frame size
         O Class F frames output, O bytes
        O Class 2/3 frames output, O bytes
         0 Error frames
```

#### Displays the details of the counters for a FCIP interface

```
switch# show interface fcip 1 counters detailed
fcip1
    TCP Connection Information
      0 Active TCP connections
        O Attempts for active connections, O close of connections
    5 minutes input rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
    5 minutes output rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
      0 frames input, 0 bytes, 0 bytes/frame average frame size
        0 Class F frames input, 0 bytes
         O Class 2/3 frames input, O bytes
         0 Reass frames
         0 Error frames timestamp error 0
      0 frames output, 0 bytes, 0 bytes/frame average frame size
         O Class F frames output, O bytes
         0 Class 2/3 frames output, 0 bytes
         0 Error frames
```

### **Displays the IPS interface**

```
switch# show interface ipstorage 1/1
IPStorage1/1 is down (SFP not present)
Hardware is IPStorage, address is f40f.1b72.ca33
Internet address(es):
MTU 1500 bytes
Port mode is IPS
```

```
Beacon is turned off
Auto-Negotiation is turned on
5 minutes input rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
5 minutes output rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
0 packets input, 0 bytes, 0 bytes/packet average packet size
0 multicast frames, 0 compressed
0 input errors, 0 frame, 0 overrun 0 fifo
0 packets output, 0 bytes, 0 bytes/packet average packet size, 0 underruns
0 output errors, 0 collisions, 0 fifo
0 carrier errors
```

#### Displays the counters of an IPS interface

```
switch# show interface ipstorage 1/1 counters
IPStorage1/1
5 minutes input rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
5 minutes output rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
0 packets input, 0 bytes, 0 bytes/packet average packet size
0 multicast frames, 0 broadcast frames
0 errors, 0 queue drops, 0 if-down drops, 0 RED drops
0 bad ether type drop, 0 bad protocol drops
0 packets output, 0 bytes, 0 bytes/packet average packet size, 0 underruns
0 multicast, 0 broadcast
0 errors, 0 collisions, 0 arp drops, 0 if-down drops
```

#### Displays the details of counters for an IPS interface

```
switch# show interface ipstorage 1/1 counters detailed
IPStorage1/1
Rate Stats:
 Rx 5 minutes input rate bits/sec:
                                                                                0
 Rx 5 minutes input rate bytes/sec:
                                                                                0
                                                                                0
 Rx 5 minutes input rate packets/sec:
                                                                                0
 Tx 5 minutes input rate bits/sec:
 Tx 5 minutes input rate bytes/sec:
                                                                                0
 Tx 5 minutes input rate packets/sec:
                                                                                0
 Total Stats:
 Rx packets input:
                                                                                0
 Rx bytes:
                                                                                0
                                                                                0
 Rx bytes/frame average frame size:
                                                                                0
 Rx multicast frames:
 Rx broadcast frames:
                                                                                0
                                                                                0
 Tx packets output:
 Tx bytes:
                                                                                0
                                                                                0
 Tx bytes/packet average packet size:
 Tx multicast frames:
                                                                                0
 Tx broadcast frames:
                                                                                0
 Tx errors:
                                                                                0
MAC Error Stats:
                                                                                0
 Rx errors:
 Rx queue drops:
 Rx if-down drops:
                                                                                0
 Rx RED drops:
                                                                                0
 Rx bad ether type drops:
                                                                                0
                                                                                0
 Rx bad protocol drops:
  Rx packets with FCS or align errors:
                                                                                0
  Rx packets with length < min:
                                                                                0
  Rx packets with length < min & FCS error:
                                                                                0
  Rx packets with length > max:
                                                                                0
  Rx packets with length > max & FCS error:
                                                                                0
                                                                                0
  Rx packets with PCI error:
```

Rx	packets with GMX/SPX/PCI error:	0
Rx	packets dropped by RED buffer exhaustion:	0
Rx	L2 multicast packets:	0
Rx	L2 broadcast packets:	0
Тx	underruns:	0
Тx	collisions:	0
Тx	ARP drops:	0
Тx	if-down drops:	0

#### **Displays the port channel interface**

```
switch# show interface port-channel50
port-channel50 is down (No operational members)
   Hardware is IPStorage
    Port WWN is 24:32:00:2a:6a:26:a1:e0
   Admin port mode is auto, trunk mode is on
    snmp link state traps are enabled
   Port vsan is 1
   Logical type is Unknown(0)
    5 minutes input rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
    5 minutes output rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
      O frames input, O bytes, O bytes/frame average frame size
         0 Class F frames input, 0 bytes
         O Class 2/3 frames input, O bytes
         0 Reass frames
         0 Error frames timestamp error 0
      0 frames output, 0 bytes, 0 bytes/frame average frame size
         O Class F frames output, O bytes
         0 Class 2/3 frames output, 0 bytes
         0 Error frames
    Member[1] : fcip1
                          [down]
   Member[2] : fcip2
                          [down]
```

### Displaying interface information for other 9.x releases

The following examples are for releases prior to 9.4(4)

Displays the status of interfaces.

```
switch# show interface
fc1/1 is up
   Hardware is Fibre Channel, SFP is short wave laser w/o OFC (SN)
   Port WWN is 20:01:54:7f:ee:de:c5:00
   Admin port mode is SD
   snmp link state traps are enabled
   Port mode is SD
   Port vsan is 1
   Admin Speed is 8 Gbps
   Operating Speed is 8 Gbps
   Rate mode is dedicated
   Beacon is turned off
   Logical type is Unknown(0)
    5 minutes input rate 0 bits/sec,0 bytes/sec, 0 frames/sec
    5 minutes output rate 0 bits/sec,0 bytes/sec, 0 frames/sec
      4 frames input, 304 bytes
       0 discards,0 errors
       0 invalid CRC/FCS,0 unknown class
        0 too long,0 too short
      4 frames output, 304 bytes
       0 discards,0 errors
      0 input OLS, 0 LRR, 0 NOS, 0 loop inits
      0 output OLS,0 LRR, 0 NOS, 0 loop inits
```

```
1 receive B2B credit remaining
     0 transmit B2B credit remaining
     0 low priority transmit B2B credit remaining
   Interface last changed at Mon Apr 24 23:10:49 2017
   Last clearing of "show interface" counters : never
٠
fc3/8 is trunking
   Hardware is Fibre Channel, SFP is short wave laser w/o OFC (SN)
   Port WWN is 20:88:54:7f:ee:de:c5:00
   Admin port mode is auto, trunk mode is on
   snmp link state traps are enabled
   Port mode is TF
   Port vsan is 1
   Admin Speed is auto max 32 Gbps
   Operating Speed is 16 Gbps
   Rate mode is dedicated
   Port flow-control is R RDY
   Transmit B2B Credit is 64
   Receive B2B Credit is 32
   Receive data field Size is 2112
   Beacon is turned off
   Logical type is core
   Trunk vsans (admin allowed and active) (1-7,200,400)
   Trunk vsans (up)
                                           (1-2)
   Trunk vsans (isolated)
                                           (6-7,200,400)
   Trunk vsans (initializing)
                                           (3-5)
   5 minutes input rate 13438472736 bits/sec,1679809092 bytes/sec, 779072 frames/sec
   5 minutes output rate 13438477920 bits/sec,1679809740 bytes/sec, 779073 frames/sec
      99483764407 frames input,213691124011124 bytes
       0 discards,0 errors
       0 invalid CRC/FCS,0 unknown class
       0 too long,0 too short
      99485576094 frames output,213695013798564 bytes
       0 discards,0 errors
     0 input OLS, 0 LRR, 0 NOS, 0 loop inits
     1 output OLS,1 LRR, 0 NOS, 0 loop inits
     32 receive B2B credit remaining
     62 transmit B2B credit remaining
      62 low priority transmit B2B credit remaining
   Interface last changed at Mon Apr 24 23:11:47 2017
   Last clearing of "show interface" counters : never
fc3/15 is up
   Hardware is Fibre Channel, SFP is short wave laser w/o OFC (SN)
   Port WWN is 20:8f:54:7f:ee:de:c5:00
   Admin port mode is F, trunk mode is off
   snmp link state traps are enabled
   Port mode is F, FCID is 0xe003c0
   Port vsan is 1
   Admin Speed is auto max 32 Gbps
   Operating Speed is 16 Gbps
   Rate mode is dedicated
   Port flow-control is R_RDY
   Transmit B2B Credit is 80
   Receive B2B Credit is 32
   Receive data field Size is 2112
```

```
Beacon is turned off
Logical type is edge
5 minutes input rate 0 bits/sec,0 bytes/sec, 0 frames/sec
5 minutes output rate 0 bits/sec,0 bytes/sec, 0 frames/sec
  29 frames input, 2600 bytes
    0 discards, 0 errors
    0 invalid CRC/FCS,0 unknown class
    0 too long,0 too short
  36 frames output, 2948 bytes
    0 discards,0 errors
  0 input OLS, 0 LRR, 0 NOS, 0 loop inits
  1 output OLS,1 LRR, 0 NOS, 0 loop inits
  32 receive B2B credit remaining
  80 transmit B2B credit remaining
  80 low priority transmit B2B credit remaining
Interface last changed at Mon Apr 24 23:11:50 2017
Last clearing of "show interface" counters : never
```

You can also specify arguments (a range of interfaces or multiple specified interfaces) to display interface information. You can specify a range of interfaces by issuing a command in the following format:

interface fc1/1 - 5, fc2/5 - 7



```
Note
```

The spaces are required before and after the dash ( - ) and before and after the comma ( , ).

The following example displays the status of a range of interfaces:

#### **Displays Multiple, Specified Interfaces**

```
switch# show interface fc3/9 , fc3/12
fc3/9 is trunking
    Hardware is Fibre Channel, SFP is short wave laser w/o OFC (SN)
   Port WWN is 20:89:54:7f:ee:de:c5:00
   Peer port WWN is 20:09:00:2a:6a:a4:0b:00
   Admin port mode is E, trunk mode is on
   snmp link state traps are enabled
    Port mode is TE
   Port vsan is 1
   Admin Speed is auto
   Operating Speed is 32 Gbps
   Rate mode is dedicated
   Port flow-control is ER RDY
   Transmit B2B Credit for vl0 is 15
   Transmit B2B Credit for vll is 15
   Transmit B2B Credit for vl2 is 40
   Transmit B2B Credit for vl3 is 430
   Receive B2B Credit for vl0 is 15
   Receive B2B Credit for vll is 15
   Receive B2B Credit for v12 is 40
   Receive B2B Credit for vl3 is 430
   B2B State Change Number is 14
   Receive data field Size is 2112
```
```
Beacon is turned off
    fec is enabled by default
    Logical type is core
    FCSP Status: Successfully authenticated
   Trunk vsans (admin allowed and active) (1-7, 200, 400)
    Trunk vsans (up)
                                           (1 - 7)
    Trunk vsans (isolated)
                                            (200, 400)
   Trunk vsans (initializing)
                                            ()
    5 minutes input rate 1175267552 bits/sec,146908444 bytes/sec, 67007 frames/sec
    5 minutes output rate 1175268256 bits/sec,146908532 bytes/sec, 67005 frames/sec
     8563890817 frames input, 18703349820904 bytes
        0 discards, 0 errors
        0 invalid CRC/FCS,0 unknown class
        0 too long,0 too short
     8563735031 frames output, 18703009725636 bytes
       0 discards,0 errors
     0 input OLS, 0 LRR, 0 NOS, 0 loop inits
      1 output OLS, 3 LRR, 0 NOS, 0 loop inits
     70 receive B2B credit remaining
     500 transmit B2B credit remaining
     485 low priority transmit B2B credit remaining
    Interface last changed at Mon Apr 24 23:11:49 2017
   Last clearing of "show interface" counters : never
fc3/12 is trunking
   Hardware is Fibre Channel, SFP is short wave laser w/o OFC (SN)
    Port WWN is 20:8c:54:7f:ee:de:c5:00
    Peer port WWN is 20:0c:00:2a:6a:a4:0b:00
    Admin port mode is E, trunk mode is on
    snmp link state traps are enabled
   Port mode is TE
    Port vsan is 1
    Admin Speed is auto
   Operating Speed is 32 Gbps
   Rate mode is dedicated
    Port flow-control is ER RDY
   Transmit B2B Credit for vl0 is 15
    Transmit B2B Credit for vl1 is 15
   Transmit B2B Credit for vl2 is 40
   Transmit B2B Credit for vl3 is 430
   Receive B2B Credit for vl0 is 15
   Receive B2B Credit for vll is 15
    Receive B2B Credit for vl2 is 40
   Receive B2B Credit for vl3 is 430
   B2B State Change Number is 14
    Receive data field Size is 2112
   Beacon is turned off
    fec is enabled by default
    Logical type is core
   FCSP Status: Successfully authenticated
   Trunk vsans (admin allowed and active) (1-7,200,400)
   Trunk vsans (up)
                                            (1 - 7)
   Trunk vsans (isolated)
                                            (200, 400)
    Trunk vsans (initializing)
                                            ()
    5 minutes input rate 1175267840 bits/sec,146908480 bytes/sec, 67008 frames/sec
    5 minutes output rate 1175265056 bits/sec,146908132 bytes/sec, 67007 frames/sec
     8564034952 frames input, 18703367929364 bytes
       0 discards,0 errors
        0 invalid CRC/FCS,0 unknown class
        0 too long,0 too short
      8563736100 frames output, 18703012026724 bytes
        0 discards,0 errors
```

```
1 input OLS,1 LRR,1 NOS,0 loop inits
1 output OLS,2 LRR, 0 NOS, 0 loop inits
70 receive B2B credit remaining
500 transmit B2B credit remaining
485 low priority transmit B2B credit remaining
Interface last changed at Mon Apr 24 23:11:50 2017
Last clearing of "show interface" counters : never
```

The following example displays the status of a specified interface:

#### **Displays a Specific Interface**

```
switch# show interface fc3/9
fc3/9 is trunking
   Hardware is Fibre Channel, SFP is short wave laser w/o OFC (SN)
   Port WWN is 20:89:54:7f:ee:de:c5:00
    Peer port WWN is 20:09:00:2a:6a:a4:0b:00
   Admin port mode is E, trunk mode is on
   snmp link state traps are enabled
    Port mode is TE
   Port vsan is 1
   Admin Speed is auto
   Operating Speed is 32 Gbps
   Rate mode is dedicated
   Port flow-control is ER RDY
   Transmit B2B Credit for vl0 is 15
   Transmit B2B Credit for vll is 15
   Transmit B2B Credit for vl2 is 40
   Transmit B2B Credit for vl3 is 430
    Receive B2B Credit for vl0 is 15
   Receive B2B Credit for vll is 15
   Receive B2B Credit for vl2 is 40
   Receive B2B Credit for vl3 is 430
   B2B State Change Number is 14
   Receive data field Size is 2112
   Beacon is turned off
   fec is enabled by default
   Logical type is core
   FCSP Status: Successfully authenticated
   Trunk vsans (admin allowed and active) (1-7,200,400)
                                            (1 - 7)
    Trunk vsans (up)
   Trunk vsans (isolated)
                                            (200, 400)
   Trunk vsans (initializing)
                                            ()
   5 minutes input rate 1175263296 bits/sec,146907912 bytes/sec, 67007 frames/sec
    5 minutes output rate 1175266272 bits/sec,146908284 bytes/sec, 67007 frames/sec
      8570830922 frames input, 18718506849280 bytes
        0 discards,0 errors
       0 invalid CRC/FCS,0 unknown class
        0 too long,0 too short
     8570675128 frames output, 18718166747180 bytes
       0 discards,0 errors
      0 input OLS, 0 LRR, 0 NOS, 0 loop inits
      1 output OLS, 3 LRR, 0 NOS, 0 loop inits
      70 receive B2B credit remaining
     500 transmit B2B credit remaining
      485 low priority transmit B2B credit remaining
    Interface last changed at Mon Apr 24 23:11:49 2017
```

Last clearing of "show interface" counters : never

The following example displays a summary of information:

### **Displays Interface Information in a Brief Format**

### switch# show interface brief

Interface	Vsan	Admin Mode	Admin Trunk	Status	SFP	Oper Mode	Oper Speed	Port Channel	Logical Type
			Mode				(Gbps)		
fc1/1	1	Ε	on	up	swl	Е	8		core
fc1/2	1	auto	on	sfpAbsent					
fc1/3	1	F	on	up	swl	F	8		core

### switch# show interface brief

Interface	Vsan	Admin Mode	Admin Trunk Mode	Status	SFP	Oper Mode	Oper Speed (Gbps)	Port Channel	Logical Type	
fc1/1	1	auto	on	down	swl					
$f_{c1}/2$	1	auto	on	down	swl					
fc1/3	1	auto	on	down	swl					
fc1/4	1	auto	on	down	swl					
fc1/5	1	auto	on	down	swl					
fc1/6	1	auto	on	down	swl					
fc1/7	1	auto	on	down	swl					
fc1/8	1	auto	on	down	swl					
fc1/9	1	auto	on	down	swl					
fc1/10	1	auto	on	down	swl					
fc1/11	1	auto	on	down	swl					
fc1/12	1	auto	on	sfpAbsent						
Interface							Sneed			
INCELIACE			Status				(Gbps)			
sup-fc0			up				1			
Interface		 S	tatus	IP Add:	ress	Sp	eed	MTU		
IPStorage1	./1	c	utOfServ	rc 10.1.1	.32/24	1	Gbps	1500		
IPStorage1	/2	С	utOfServ	7C		1	Gbps	1500		
IPStorage1	/3	С	utOfServ	7C		1	Gbps	1500		
IPStorage1	/4	e	rrDisabl	.ed		1	Gbps	1500		
IPStorage1	/5	i	nit			2	5 Gbps	1500		
TPStorage1	/6	C	utOfServ	/C		4	0 Gbps	1500		

The following example displays the description of interfaces:

### **Displays Port Description**

```
switch# show interface description
```

Interface	Description
fc3/1	test intest
fc3/2	
fc3/3	
fc3/4	TE port
fc3/5	
fc3/6	
fc3/10	Next hop switch 5
fc3/11	
fc3/12	
fc3/16	
Interface	Description
port-channel 1	
- port-channel 5	
port-channel 6	

The following example displays a summary of information:

### **Displays Interface Counters**

```
switch# show interface counters
fc3/1
    5 minutes input rate 24 bits/sec, 3 bytes/sec, 0 frames/sec
    5 minutes output rate 16 bits/sec, 2 bytes/sec, 0 frames/sec
   3502 frames input, 268400 bytes
      0 discards, 0 CRC, 0 unknown class
      0 too long, 0 too short
    3505 frames output, 198888 bytes
      0 discards
   1 input OLS, 1 LRR, 1 NOS, 0 loop inits
   2 output OLS, 1 LRR, 1 NOS, 0 loop inits
    1 link failures, 1 sync losses, 1 signal losses
.
fc9/8
    5 minutes input rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
    5 minutes output rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
   0 frames input, 0 bytes
      0 class-2 frames, 0 bytes
      0 class-3 frames, 0 bytes
      0 class-f frames, 0 bytes
      0 discards, 0 CRC, 0 unknown class
      0 too long, 0 too short
    0 frames output, 0 bytes
      0 class-2 frames, 0 bytes
      0 class-3 frames, 0 bytes
      0 class-f frames, 0 bytes
      0 discards
    0 input OLS, 0 LRR, 0 NOS, 0 loop inits
```

```
0 output OLS, 0 LRR, 0 NOS, 0 loop inits
    O link failures, O sync losses, O signal losses
      16 receive B2B credit remaining
      3 transmit B2B credit remaining.
sup-fc0
    114000 packets input, 11585632 bytes
      0 multicast frames, 0 compressed
      0 input errors, 0 frame, 0 overrun 0 fifo
    113997 packets output, 10969672 bytes, 0 underruns
      0 output errors, 0 collisions, 0 fifo
      0 carrier errors
mgmt0
    31557 packets input, 2230860 bytes
      0 multicast frames, 0 compressed
      0 input errors, 0 frame, 0 overrun 0 fifo
    26618 packets output, 16824342 bytes, 0 underruns
      0 output errors, 0 collisions, 7 fifo
      0 carrier errors
vsan1
    0 packets input, 0 bytes, 0 errors, 0 multicast
    0 packets output, 0 bytes, 0 errors, 0 dropped
port-channel 1
    5 minutes input rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
    5 minutes output rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
    0 frames input, 0 bytes
      0 class-2 frames, 0 bytes
      0 class-3 frames, 0 bytes
      0 class-f frames, 0 bytes
      0 discards, 0 CRC, 0 unknown class
      0 too long, 0 too short
    0 frames output, 0 bytes
      0 class-2 frames, 0 bytes
      0 class-3 frames, 0 bytes
      0 class-f frames, 0 bytes
      0 discards
    0 input OLS, 0 LRR, 0 NOS, 0 loop inits
    0 output OLS, 0 LRR, 0 NOS, 0 loop inits
    0 link failures, 0 sync losses, 0 signal losses
```

```
Ń
```

Note Inter

Interfaces 9/8 and 9/9 are not trunking ports and display Class 2, 3, and F information as well.

The following example displays the brief counter information of interfaces:

### **Displays Interface Counters in Brief Format**

Switch# snow inter		cers brief		
Interface	Input (r	ate is 5 min avg)	Output (	rate is 5 min avg)
	Rate	Total	Rate	Total
	Mbits/s	Frames	Mbits/s	Frames
fc3/1	0	3871	0	3874
fc3/2	0	3902	0	4232

### switch# show interface counters brief

fc3/3	0	3901	0	4138
fc3/4	0	3895	0	3894
fc3/5	0	3890	0	3897
fc9/8	0	0	0	0
fc9/9	0	5	0	4
fc9/10	0	4186	0	4182
fc9/11	0	4331	0	4315
Interface	Input (	rate is 5 min avg)	Output (	rate is 5 min avg)
Interface	Input (  Rate Mbits/s	rate is 5 min avg) Total Frames	Output ( Rate Mbits/s	rate is 5 min avg) Total Frames
Interface	Input (  Rate Mbits/s	rate is 5 min avg) Total Frames	Output ( Rate Mbits/s	rate is 5 min avg) Total Frames
Interface	Input (  Rate Mbits/s 0	Total Frames	Output ( Rate Mbits/s	rate is 5 min avg) Total Frames 0

You can run the **show interface transceiver** command only on a switch in the Cisco MDS 9100 Series if the SFP is present, as show in the following example:

#### **Displays Transceiver Information**

switch# show interface transceiver

```
fc1/1 SFP is present
   name is CISCO-AGILENT
    part number is QFBR-5796L
    revision is
    serial number is A00162193
    fc-transmitter type is short wave laser
    cisco extended id is unknown (0x0)
. . .
fc1/9 SFP is present
   name is FINISAR CORP.
    part number is FTRJ-1319-7D-CSC
    revision is
    serial number is H11A6ER
    fc-transmitter type is long wave laser cost reduced
    cisco extended id is unknown (0x0)
. . .
```

The following example displays the entire running configuration, with information about all the interfaces. The interfaces have multiple entries in the configuration files to ensure that the interface configuration commands execute in the correct order when the switch reloads.

### **Displays the Running Configuration for All Interfaces**

```
switch# show running-config
...
interface fc9/1
  switchport speed 2000
...
interface fc9/1
  switchport mode E
...
interface fc9/1
  channel-group 11 force
  no shutdown
```

The following example displays the running configuration information for a specified interface. The interface configuration commands are grouped together:

### Displays the Running Configuration for a Specified Interface

```
switch# show running-config interface fc1/1
interface fc9/1
switchport speed 2000
switchport mode E
channel-group 11 force
no shutdown
```

Displays the running configuration after the system default switchport mode F command is executed.

The following example displays the running configuration after the **system default switchport mode F** command is executed:

Displays the Running Configuration after the System Default Switchport Mode F Command is Executed

```
switch# show running-config
version 3.1(3)
system default switchport mode F
interface fc4/1
interface fc4/2
interface fc4/3
interface fc4/4
interface fc4/5
interface fc4/6
interface fc4/7
interface fc4/8
interface fc4/9
interface fc4/10
```

The following example displays the running configuration after two interfaces are individually configured for FL mode:

Displays the Running Configuration after Two Interfaces are Individually Configured for Mode FL

```
switch# show running-config
version 3.1(3)
system default switchport mode F
interface fc4/1
switchport mode FL
interface fc4/2
interface fc4/3
switchport mode FL
interface fc4/4
interface fc4/5
interface fc4/6
interface fc4/7
interface fc4/8
interface fc4/9
interface fc4/1
```

The following example displays interface information in a brief format after the **system default switchport mode F** command is executed:

# Displays Interface Information in a Brief Format after the System Default Switchport Mode F Command is Executed

Interface	Vsan	Admin Mode	Admin Trunk Mode	Status	SFP	Oper Mode	Oper Speed (Gbps)	Port Channel	Logical Type
fc4/1	1	F		notConnected	swl				
fc4/2	1	F		notConnected	swl				
fc4/3	1	F		notConnected	swl				
fc4/4	1	F		notConnected	swl				
fc4/5	1	F		sfpAbsent					
fc4/6	1	F		sfpAbsent					
fc4/7	1	F		sfpAbsent					
fc4/8	1	F		sfpAbsent					
fc4/9	1	F		sfpAbsent					

The following example displays interface information in a brief format after two interfaces are individually configured for FL mode:

# Displays Interface Information in a Brief Format after Two Interfaces Are Individually Configured for Mode FL

Interface	Vsan	Admin Mode	Admin Trunk Mode	Status	SFP	Oper Mode	Oper Speed (Gbps)	Port Channel	Logical Type
fc4/1	1	FL		notConnected	swl				
fc4/2	1	F		notConnected	swl				
fc4/3	1	FL		notConnected	swl				
fc4/4	1	F		notConnected	swl				
fc4/5	1	F		sfpAbsent					
fc4/6	1	F		sfpAbsent					
fc4/7	1	F		sfpAbsent					
fc4/8	1	F		sfpAbsent					
fc4/9	1	F		sfpAbsent					
fc4/10	1	F		sfpAbsent					

### switch# show interface brief

switch# show interface brief

## **Displaying Interface Statistics**

Run the **ShowIntStats** command from user EXEC mode. This command displays the interface statistics. Without any arguments, this command displays the statistics for all the configured interfaces in the switch.

The following example displays the statistics of interfaces:

### switch# ShowIntStats

2023/07/21 18:27:15 Link Stats:

											-+	• • • • • • • • •
	Link		Sync	Signal	Invalid	Invalid	I	NOS	NOS	OLS	I	OLS
Intf	Failu	ires	Loss	Loss	Words	CRCs	I	Rx	Tx	Rx		Tx
Rx   Tx	Corrected	Unco	rrected	BB_SCs	BB_SCr							
fc1/1		3	0	0	0	0		0	3	3		4
0   4	0		0	0	0	I						
fc1/2		0	0	0	0	0	I	0	0	0	Ι	1
0   2     fc1/3	1	1	0	0	0	I 0	I	0	1	1	T	2
2   2	. 0	'	0	0	0							
fc1/4		1	0	0	3051	0	Ι	0	1	1	Ι	2
2   2     fc1/5		1	0	0	0	I 0	I	0	1	1	I	2
	0	'	0	0	0							
fc1/6		1	0	0	0	0	Ι	1	1	2	Ι	2
2   2     fc1/7	1	0	0	0	0	I 0	I	0	0	0	ī	0
	. 0	'	0	0	0					-		
fc1/8		0	0	0	0	0	Ι	0	0	0	Ι	0
U   U     fc1/9	1	0	0	0	0	I 0	I	0	0	0	ī	0
	0		0	0	0						'	
fc1/10		0	0	0	0	0	Ι	0	0	0	Ι	0
0   0     fc1/11	1	0	0	0	0	I 0	I	0	0	0	ī	1
	0		0	0	0			0	Ū	1 0	'	-
fc1/12		0	0	0	0	0	Ι	0	0	0	Ι	1
0   2     fc1/13	0		0		0	   0	ī	0	0	I 0	ī	1
	0		0	1 0	0			0	Ū	1 0		-
fc1/14	I	1	0	1	0	0	Ι	4	3	2	Ι	2
4   0	1	1 1	2	0 1	0	   0	1	2	2	1 2	ī	2
4   0	0	- 1	2	0	0			-	-			2
fc1/16	I	1	1	0	0	0	Ι	1	1	1	Ι	2
3   1	0		2		0		1	0	0	۱ O	ī	0
	0		0	1 0	0			0	Ū	1 0		0
fc1/18		0	0	0	0	0	I	0	0	0	Ι	0
0   0	0		0		0	   0	ī	1	0	ı 1	ī	1
	44222135		0	1 0	0			-	Ū	-	'	-
fc1/20		0	0	0	0	0	Ι	0	0	0	Ι	1
_   _   _     fc1/21	58311348		0		0	   0	ī	0	0	I 0	ī	1
	2776734		0	0	0			0	0	1 0	'	-
fc1/22		0	0	0	0	0	Ι	0	0	0	Ι	1
1   1	32918274		0		0		1	0	0	ı 1	ī	1
2 0	52394		0		0		1	0	U	ι <u>τ</u>	I	Ŧ
fc1/24		3	0	0	0	0	I	0	3	3	Ι	4
0   4	0	ן ג ו	0		0	   ∩	I	Ο	2	। २	ī	Д
0 4	0	ן כ 	0	1 0	0		1	U	5	, ,	1	т
fc1/26	1	3	0	0	0	0	I	0	3	3	Ι	4
0   4	0	 	0		0		I	Ο	2	1 2	ī	Л
	0	ן כ 	0		0		1	0	5	, ,	I	T

fc1/28	0	0	0	0	0	0	0	0	1
		0		0					
fc1/29	0	0	0	0	0	0	0	0	1
0   2   48458710		0	0	0	I				
fc1/30	0	0	0	0	0	0	0	0	1
		0		0				0 1	0
	0			0	1 0	1 0	1 0 1	0 1	0
fc1/32	0		0	0	I 0	0	0	0	1
		0		0					
fc1/33	0	0	0	0	0	0	0	0	1
0   2   0	1	0	0	0	I				
fc1/34	1	0	0	0	0	0	1	1	2
2   2   0	1	ı ∩ ı		0	I 0	۱ O	1 1 1	1 1	2
2   2   1930	1	0		0	1	1 0	1 1	± 1	2
fc1/36	1	0	0	0	I 0	0	1	1	2
2   2   53	1	0	0	0	I				
fc1/37	1	0	0	0	0	0	1	1	2
2   2   0	1	0		0		. 0	. 1.	1 1	2
	1	0		0	1 0	1 0	_	1	2
fc1/39	0	I 0 I	0	0	0	0	0	0	1
	L	0	0	0	İ				
fc1/40	0	0	0	0	0	0	0	0	1
		0		0				0 1	1
tcl/41	0			0	0	0	0	0	Ţ
1   1   0	0	I 0 I	0	0	I 0	0	0	0	1
1   1   460053		0		0					
fc1/43	0	12	0	0	0	0	0	0	1
0   2   39898	1	0	0	0	I				
fc1/44	62	11386	1	62	6	0	62	0	67
58   72   45455329	1	23		0		I 0	I 0 I	0 1	1
	1	0		0	1	1 0	1 0 1	0 1	T
fc1/46	0	0	0	0	I 0	0	0	0	1
0   2   0	1	0	0	0	I				
fc1/47	0	0	0	0	0	0	0	0	1
1   1   154536	1			0		. 0		0 1	1
	1	0		0	1	1 0	1 0 1	0 1	T
port-channel21	0	0	0	0	I 0	0	0	0	3
0   6   0	1	0	0	0	I				
port-channel22	62	11386	1	62	6	0	62	0	71
61   77   45600392		23		0				0 1	0
port-channel31	1			0	1 0	1 0	1 0 1	0 1	0
port-channel32	0	12	0	0	0	0	0	0	5
-   3   7   499951		0	0	0	I				
port-channel41	4	0	0	3051	0	1	4	5	8
		0		0				10 .	1 0
port-channel42     21   11   1004	8	ء د	2	0	I U	1 7	11	TO	16
port-channel131	0	0		0	, I 0	1		2 1	5
7   3   104595439		0		Ũ	, j	-		2 1	Ũ
port-channel132	0	0	0	0	0	0	0	0	0
0   0   0		0	0	0					

You can also specify arguments (a range of interfaces or multiple specified interfaces) to display interface statistics. You can specify a range of interfaces by issuing a command in the following format:

-stats fc1/1 - 5 , fc2/5 - 7

Note The spaces are required before and after the dash ( - ) and before and after the comma ( , ).

The following example displays the link statistics of a specified interface:

```
switch# ShowIntStats --link-stats fc1/1
2023/07/21 18:27:24 Link Stats:
```

					I		I			+		+		 
Link	Sync   Signa	l   Inva	lid	In	valid		NOS	NOS	I	OLS	OLS	1	LRR	LRR
FEC   FEC		1		1										
Intf   Failures	Loss   Loss	Word	ls	CR	Cs	1	Rx	Tx		Rx	Tx		Rx	Τx
Corrected   Uncorr	ected   BB S	Cs   BB	SCr	1										
+										I				 +
fc1/1   3	0   0	0	0		0		0	3		3	4		0	4
0	0	0	0	1										
										+		+	+	

The following example displays the link statistics for a range of interfaces:

```
switch# ShowIntStats --link-stats fc1-10
2023/07/21 18:27:37 Link Stats:
```

	+			-+-				I				+-			-+-		 							+	
L			L	in	k		Sy	nc   :	Signal	Invali	.d	In	vali	d	]	NOS	NOS		OLS	(	OLS		LRR	I	LRR
	FEC				FE(	С		- I																	
	Intf		F	'ai	lur	es	Lo	oss	Loss	Words	1	CF	Cs			Rx	Τx		Rx		Τx		Rx		Tx
	Co	rre	ecte	d	U1	nco	orred	cted	BB SCs	BB S	Cr														
+		+								+					-+-		 	-+			1				+
L	fc1/	1	1			3		0	0		0			0		0	3		3			1		0	
4				0				0	0	1	0														
	fc1/	2	1			0		0	0		0			0		0	0		0			1		0	
2				0				0	0		0														
	fc1/	3	1			1		0	0		0			0		0	1		1		-	2		2	
2	1			0				0	0	1	0														
	fc1/	4	1			1		0	0	30	51			0		0	1		1			2		2	1
2	1			0				0	0	1	0														
	fc1/	5				1		0	0		0			0		0	1		1		1	2		2	1
2	1			0				0	0	1	0														
	fc1/	6	1			1		0	0		0			0		1	1		2		-	2		2	
2				0	1			0	0		0														
	fc1/	7	1			0		0	0		0			0		0	0		0		(	C		0	1
0	1			0				0	0	1	0														
	fc1/	8	1			0		0	0		0			0		0	0		0		(	C		0	
0	1			0				0	0	1	0														
	fc1/	9	1			0		0	0		0			0		0	0		0		(	C		0	1
0	1			0				0	0	1	0														
	fc1/	10	1			0		0	0		0			0		0	0		0		(	C		0	
0				0				0	0		0														
_				_				h		I					-			-						-	

The following example displays the general statistics for a range of interfaces:

switch# ShowIntStats --general-stats fc1/1-4
2023/07/21 18:27:57 General Stats:

_												
I	· .	Frames	Frames	C3	Frames	C3	Frames	C2	Frames	C2 F	rames   C	CF Frames
L	CF Frame	es   Mcast	:   Mc	ast	Bca	st	Bca	st	Ucas	st	Ucast	I.
	Intf	Rx	Tx	Rx		Tx		Rx		Tx	F	Rx
I.	Tx	Frame	es Rx   Fr	ames Tz	k   Fra	mes R>	k   Fra	mes Tx	Fran	nes Rx	Frames	Tx
+	fc1/1	29819972	4471699	4   29	9819972	44	716994		0		0	0
i		0	0	. (		C	)	. 0	298	319972	447169	994
	fc1/2	71	11	2	71	1	112	1	0	1	0	0
		0	0	(		C	)	0		71	1	.12
	fc1/3	314596	30950	0	0		0		0		0	314596
	30950	0 0	0	(		C	)	0		314596	3095	500
	fc1/4	45	304	5	0		0		0		0	45
L	304	15	0	(		C	)	0	I	45	30	945
-												

The following example displays the congestion statistics for a range of interfaces:

switch# ShowIntStats --congestion-stats fcl/1-4
2023/07/21 18:28:32 Congestion Stats:

_	+		+		+		+		+				+		_+		_+	+-	
I	י ססד ו		1	I	I	I	I	Ι	TxWait % last	Ι	Timeout	Ι	Credit	<i>P</i>	Active	Ι	Active		LRR
I	Intf   Tx	   	TBBZ		RBBZ		TxWait	I	ls/1m/1h/72h	Ι	Discards	I	Loss	1	LR Rx		LR Tx	Ι	Rx
+	fc1/1	+-   	9	+	+ 4		0		0%/0%/0%/0%		0		0		.+0		0		+ 0
	fc1/2	 	5		2	Ι	0	Ι	0%/0%/0%/0%	Ι	0	Ι	0	I	1	Ι	0	Ι	0
	fc1/3	 	5		4	I	0	Ι	0%/0%/0%/0%	Ι	0	Ι	0	I	0	Ι	2	I	2
	fc1/4   2		5		4		0	I	0%/0%/0%/0%	Ι	0	I	0	I	0		2	Ι	2
									1										

The following example displays the details of the transceiver (SFP) statistics for a range of interfaces:

switch# ShowIntStats --transceiver-stats fc1/1-15
2023/07/21 18:29:06 Transceiver(SFP) Detail Stats:

			de la companya de la						1	1
			Cisco		Serial			Nominal		
	1	Tx	Rx	T>	K					
Intf	Name	1	PID		Number	Syr	nc	Bit Rate	Temp	
Voltag	e   Curren	t   Power	Power		Fault					
+	+	+					+			+
fc1/	1   CISCO	-FINISAR	DS-SFP-FC1	6G-SW	FNS18150XH6	i	.n	14000Mb/s	45.34C	
3.33V	7.71mA	-2.81dBm	-2.90	dBm	0					
fc1/	2   CIS	CO-AVAGO	DS-SFP-FC3	2G-SW	AVD2101W00P	i	n	28000Mb/s	43.39C	1
3.30V	7.50mA	0.23dBm	-1.00	dBm	0					

fc1/3	CISCO-FINISAR	DS-SFP-FC16G-SW		FNS18283Q6Z		in	14000Mb/s		54.66C
3.30V	8.54mA   -3.51dBm	-3.00dBm		0					
fc1/4	CISCO-FINISAR	DS-SFP-FC16G-SW		FNS18150RLK		in	14000Mb/s		53.76C
3.32V	7.97mA   -2.90dBm	-11.78dBm		0					
fc1/5	CISCO-FINISAR	DS-SFP-FC16G-SW		FNS18400JV0		in	14000Mb/s	I.	49.35C
3.32V	8.10mA   -3.10dBm	-2.72dBm		0					
fc1/6	CISCO-FINISAR	DS-SFP-FC16G-SW		FNS18020AJZ		in	14000Mb/s	L	52.11C
3.31V	7.85mA   -2.83dBm	-4.45dBm		0					
fc1/7	CISCO-FINISAR	DS-SFP-FC16G-SW		FNS18400DD0	1	no	14000Mb/s	L	54.80C
3.33V	8.01mA   -3.20dBm	-28.24dBm		0					
fc1/8	CISCO-FINISAR	DS-SFP-FC16G-SW		FNS180116DQ	1	no	14000Mb/s	L	52.80C
3.31V	8.07mA   -2.98dBm	-27.45dBm		0					
fc1/9	CISCO-FINISAR	DS-SFP-FC16G-SW		FNS18400EC5	1	no	14000Mb/s	L	53.55C
3.32V	8.06mA   -3.32dBm	-25.09dBm		0					
fc1/10	CISCO-FINISAR	DS-SFP-FC16G-SW		FNS18021LXY	1	no	14000Mb/s	L	54.33C
3.31V	8.04mA   -3.17dBm	-27.96dBm		0					
fc1/11	CISCO-FINISAR	DS-SFP-FC16G-SW		FNS18021KTD	1	in	14000Mb/s	L	53.63C
3.31V	7.94mA   -3.24dBm	-3.01dBm		0					
fc1/12	CISCO-FINISAR	DS-SFP-FC16G-SW		FNS180116E6	1	in	14000Mb/s	L	54.29C
3.31V	8.02mA   -2.89dBm	-2.62dBm		0					
fc1/13	CISCO-FINISAR	DS-SFP-FC16G-SW	Ι	FNS18400JVS	1	in	14000Mb/s	L	52.54C
3.31V	7.85mA   -3.10dBm	-4.02dBm		0					
fc1/14	CISCO-FINISAR	DS-SFP-FC32G-SW	T	FNS21240LWJ	1	in	28000Mb/s	L	53.53C I
3.32V I	7.67mA   -1.38dBm	-1.29dBm		0					
1 fc1/15	L CISCO-AVAGO	DS-SFP-FC32G-SW	T	AVD2101W02S	1	in l	28000Mb/s	I.	48.12C
3.29V I	7.50mA   -0.30dBm	-1.41dBm	1	0					
	, trevable								

Note: Only ports having transceiver are displayed

The following example displays the breif details such as device alias for a range of interfaces:

#### switch# ShowIntStats --brief fc1/1-4

2023/07/21 18:31:20 Interface Brief + Device-alias + Peer PWWN + Description:

		······			+				
I I I		Admin	· · ·	·		Oper	·		1
Device-alias		1			I		1		
	Admin	Trunk	1	1	Oper	Speed	Port	logical	Name
or	F	Port		1		I			
Intf   VSAN	Mode	Mode	Status	SFP	Mode	(Gbps)	Channel	Туре	
Switchname		Peer	PWWN		Des	scription	1		
+									
fc1/1   1000	F	off	up	swl	FI	16		edge	
	NA I		1	NA I				2	
fc1/2   1000	F	off	up	swl	F	32		edge	. 1
M9148V-N24 init	t qle2742 1	21:00	:34:80:0d:0	6d:72:5	52		1	2	
fc1/3   1	– E	on	trunking	swl	TE	16	41	core	
	NA			NA					
fc1/4   1	E	on	trunking	swl	TE	16	41	core	
	NA			NA					

Note: Only upto 64 characters of discription are displayed

The following example displays the error statistics for a range of interfaces:

```
switch# ShowIntStats --errorsonly fc1/44-48
2023/07/21 18:34:37 Link Stats:
```

								+	t
Link	Sync   Si	gnal   Inv	alid   In	valid	NOS	NOS	OLS   0	LS   LI	RR
LRR   FEC   FEC									
Intf   Failures	Loss   Lo	ss   Wor	ds   CR	Cs	Rx	Τx	Rx   T	x   R.	x
Tx   Corrected   Unco	rrected	BB_SCs   B	B_SCr						
fc1/44   62	11386	1	62	6	0	62	0	67   !	58
72   45470689	23	0	0						
fc1/45   0	0	0	0	0	0	0	0	1	1
1   56593	0	0	0						
fc1/46   0	0	0	0	0	0	0	0	1	0
2   0	0	0	0						
fc1/47   0	0	0	0	0	0	0	0	1	1
1   154611	0	0	0						
fc1/48   0	0	0	0	0	0	0	0	1	1
1   0	0	0	0						
								II	

The following example displays the port channel statistics of the specified port channel:

```
switch# ShowIntStats port-channel144
2023/07/21 18:38:19 Link Stats:
```

		Link	Syn	c   Signa	l   Inva	alid	Invali	d	NOS		NOS		OLS		OLS	
LRR   LRR	FEC	FE					ana -		D		<b>—</b>		D		<b>—</b>	
RX   TX	 Correc	ted   Un	s   Los correct	ed   BB S	Cs   BB	SCr	CRUS	1	КX	1	.T.X	I	КX	I	ΤX	1
+				·		-++							ŀ	+		-
port-channe	1144	627		0				0	2		0		2	I	2	I
2   2	100	02, 1		0 1	0	0 1										

### **Displaying the Port-Level Portguard**

The following command displays information about an interface that is set to error-disabled state by the portguard because of a TrustSec violation:

```
switch# show interface fc8/3
```

fc8/3 is down (Error disabled - port down due to trustsec violation) Hardware is Fibre Channel, SFP is short wave laser w/o OFC (SN) Port WWN is 21:c3:00:0d:ec:10:57:80 Admin port mode is E, trunk mode is on snmp link state traps are enabled Port vsan is 1 Receive data field Size is 2112 Beacon is turned off 5 minutes input rate 0 bits/sec, 0 bytes/sec, 0 frames/sec 5 minutes output rate 0 bits/sec, 0 bytes/sec, 0 frames/sec 11274 frames input, 1050732 bytes 0 discards, 0 errors 0 CRC, 0 unknown class 0 too long, 0 too short 11242 frames output, 971900 bytes 0 discards, 0 errors 11 input OLS, 34 LRR, 10 NOS, 0 loop inits 72 output OLS, 37 LRR, 2 NOS, 0 loop inits Interface last changed at Sun Nov 27 07:34:05 1988

An interface may be error disabled for several reasons. To recover an error-disabled interface, use the **shutdown** and **no shutdown** commands in interface configuration mode to re-enable the link.

# **Displaying Port Monitor Status and Policies**

The following commands display information about the Port Monitor feature:

**Note** The port *Logical type* is displayed as the *Port type*.

switch# <b>show</b>	port-monitor	r						
Port Monitor	enabled							
Congestion-Is	plation : en	nabled						
Policy Name Admin status Oper status Port type	default Not Active Not Active All Ports	9						
Counter	Threshold	Interval	Rising Threshold	event	Falling Threshold	event	Warning Threshold	PMON Portguard
Link Loss	Delta	60	5	4	1	4	Not enabled	Not enabled
Sync Loss	Delta	60	5	4	1	4	Not enabled	Not enabled
Signal Loss	Delta	60	5	4	1	4	Not enabled	Not enabled
Invalid Words	Delta	60	1	4	0	4	Not enabled	Not enabled
Invalid CRC's	Delta	60	5	4	1	4	Not enabled	Not enabled
State Change	Delta	60	5	4	0	4	Not enabled	Not enabled
TX Discards	Delta	60	200	4	10	4	Not enabled	Not enabled
LR RX	Delta	60	5	4	1	4	Not enabled	Not enabled
LR TX	Delta	60	5	4	1	4	Not enabled	Not enabled
Timeout								
Discards Credit	Delta	60	200	4	10	4	Not enabled	Not enabled
Loss Reco TX Credit	Delta	60	1	4	0	4	Not enabled	Not enabled
Not Available	Delta	60	10%	4	08	4	Not enabled	Not enabled
RX Datarate	Delta	60	80%	4	20%	4	Not enabled	Not enabled
TX Datarate	Delta	60	80%	4	20%	4	Not enabled	Not enabled
TX-Slowport-								
Oper-Delay	Absolute	60	50ms	4	Oms	4	Not enabled	Not enabled
TXWait	Delta	60	40%	4	0%	4	Not enabled	Not enabled

### switch# show port-monitor active

Policy Name : sample Admin status : Active Oper status : Active Port type : All Ports

Counter	Threshold	Interval	Rising Threshold	event	Falling Threshold	event	Warning Threshold	PMON Portguard
Link Loss	Delta	60	5	4	1	4	Not enabled	Not enabled
Sync Loss	Delta	60	5	4	1	4	Not enabled	Not enabled
Signal Loss	Delta	60	5	4	1	4	Not enabled	Not enabled
Invalid Words	Delta	60	5	4	1	4	Not enabled	Not enabled
Invalid CRC's	Delta	60	5	4	1	4	Not enabled	Not enabled
State Change	Delta	60	5	4	0	4	Not enabled	Not enabled
TX Discards	Delta	60	50	4	0	4	Not enabled	Not enabled
LR RX	Delta	60	5	4	1	4	Not enabled	Not enabled
LR TX	Delta	60	5	4	1	4	Not enabled	Not enabled
Timeout								

\_\_\_\_\_

Discards Credit	Delta	60	200	4	10	4	Not enabled	Not enabled
Loss Reco TX Credit	Delta	1	1	4	0	4	Not enabled	Cong-isolate
Not Available	Delta	1	10%	4	0%	4	Not enabled	Cong-isolate
RX Datarate	Delta	60	80%	4	70%	4	Not enabled	Not enabled
TX Datarate ASIC Error	Delta	60	80%	4	70%	4	Not enabled	Not enabled
Pkt from Port ASIC Error	Delta	60	50	4	10	4	Not enabled	Not enabled
Pkt to xbar ASIC Error	Delta	60	50	4	10	4	Not enabled	Not enabled
Pkt from xbar TX-Slowport-	Delta	60	50	4	10	4	Not enabled	Not enabled
Oper-Delay	Absolute	1	50ms	4	Oms	4	Not enabled	Cong-isolate
TXWait	Delta	1	40%	4	0%	4	Not enabled	Cong-isolate

Policy Name : sample Admin status : Active Oper status : Active Port type : All Edge Ports

Counter	Threshold	Interval	Rising Threshold	event	Falling Threshold	event	port	gurard
Link Loss	Delta	60	5	4	1	4	Not	enabled
Sync Loss	Delta	60	5	4	1	4	Not	enabled
Signal Loss	Delta	60	5	4	1	4	Not	enabled
Invalid Words	Delta	60	1	4	0	4	Not	enabled
Invalid CRC's	Delta	60	5	4	1	4	Not	enabled
TX Discards	Delta	60	200	4	10	4	Not	enabled
LR RX	Delta	60	5	4	1	4	Not	enabled
LR TX	Delta	60	5	4	1	4	Not	enabled
Timeout Discards	Delta	60	200	4	10	4	Not	enabled
Credit Loss Reco	Delta	1	1	4	0	4	Not	enabled
TX Credit Not	D - 1	1	100	4	0.0	4	N7 - 1	1. 1
Available	Delta	1	108	4	08	4	Not	enabled
RX Datarate	Delta	60	80%	4	20%	4	Not	enabled
TX Datarate	Delta	60	80%	4	20%	4	Not	enabled
TX-Slowport-Count	Delta	1	5	4	0	4	Not	enabled
TX-Slowport-Oper								
-Delay	Absolute	1	50ms	4	Oms	4	Not	enabled
TXWait	Delta	1	40%	4	0%	4	Not	enabled

### switch# show port-monitor default

Policy Name : default Admin status : Not Active Oper status : Not Active Port type : All Ports

Counter	Threshold	Interval	Rising Threshold	event	Falling Threshold	event	Warning Threshold	PMON Portguard
Link Loss	Delta	60		4	1	4	Not enabled	Not enabled
Sync Loss	Delta	60	5	4	1	4	Not enabled	Not enabled
Signal Loss	Delta	60	5	4	1	4	Not enabled	Not enabled
Invalid Words	Delta	60	1	4	0	4	Not enabled	Not enabled
Invalid CRC's	Delta	60	5	4	1	4	Not enabled	Not enabled
State Change	Delta	60	5	4	0	4	Not enabled	Not enabled
TX Discards	Delta	60	200	4	10	4	Not enabled	Not enabled
LR RX	Delta	60	5	4	1	4	Not enabled	Not enabled
LR TX	Delta	60	5	4	1	4	Not enabled	Not enabled

Timeout Discards	Delta	60	200	4	10	4	Not enabled	Not enabled
Credit Loss Reco	Delta	60	1	4	0	4	Not enabled	Not enabled
TX Credit Not	Delta	60	10%	4	0%	4	Not enabled	Not enabled
Available								
RX Datarate	Delta	60	80%	4	20%	4	Not enabled	Not enabled
TX Datarate	Delta	60	80%	4	20%	4	Not enabled	Not enabled
TX-Slowport-	Absolute	60	50ms	4	Oms	4	Not enabled	Not enabled
Oper-Delay								
TXWait	Delta	60	40%	4	0%	4	Not enabled	Not enabled

#### switch# show port-monitor slowdrain

Policy Name Admin status Oper status Port type	: slo : Not : Not : All	wdrain Active Active Edge Ports						
Counter		Threshold	Interval	Rising Threshold	event	Falling Threshold	event	PMON Portguard
Credit Loss Reco		Delta	1	1	4	0	4	Not enabled
Available								

#### switch# show port-monitor slowportdetect

Policy Name : Admin status : Oper status : Port type :	: slowportde : Not Active : Not Active : All Ports	tect								
Counter	Threshold	Interval	Rising	event	Falling Threshold	event	Warning Threshold	PMON Portguard		
Credit Loss Reco TX Credit	Delta	1	2	2	0	2	Not enabled	Cong-isolate		
Not Available TX-Slowport-	Delta	1	2%	2	0%	2	Not enabled	Cong-isolate		
Oper-Delay TXWait	Absolute Delta	1 1	2ms 2%	2 2	Oms O%	2 2	Not enabled Not enabled	Cong-isolate Cong-isolate		

switch# <b>show</b>	logging level pmon	
Facility	Default Severity	Current Session Severity
PMon	4	4



Note

The port monitor process does not display in the list of processes when you run the **show logging level** command. The **show logging level pmon** command must be issued to determine the logging level of port monitor.

# **Displaying Port Group Monitor Status and Policies**

The following examples display information about the port group monitor:

```
switch# show port-group-monitor status
Port Group Monitor : Enabled
```

Active Policies : pgm2 Last 100 logs : switch# switch# show port-group-monitor Port Group Monitor : enabled \_\_\_\_\_ \_\_\_\_\_ Policy Name : pgm1 Admin status : Not Active Oper status : Not Active Port type : All Port Groups \_\_\_\_\_ Threshold Interval %ge Rising Threshold %ge Falling Threshold Counter \_\_\_\_\_ \_\_\_\_\_ 60 50 60 50 RX Datarate Delta 10 TX Datarate Delta 60 10 -----\_\_\_\_\_ Policy Name : pgm2 Admin status : Active Oper status : Active Port type : All Port Groups \_\_\_\_\_ Threshold Interval %ge Rising Threshold %ge Falling Threshold Counter \_\_\_\_\_ \_\_\_\_\_ \_ \_\_\_\_\_ RX Datarate Delta 60 80 10 TX Datarate Delta 60 80 10 \_\_\_\_\_ \_\_\_\_\_ Policy Name : default Admin status : Not Active Oper status : Not Active Port type : All Port Groups -----\_\_\_\_\_ Threshold Interval %ge Rising Threshold %ge Falling Threshold Counter \_\_\_\_\_ ----- ----- ------60 80 20 RX Datarate Delta 60 80 TX Datarate Delta 20 \_\_\_\_\_ switch# show port-group-monitor active Policy Name : pgm2 Admin status : Active Oper status : Active Port type : All Port Groups \_\_\_\_\_ \_\_\_\_\_ Counter Threshold Interval %ge Rising Threshold %ge Falling Threshold \_\_\_\_\_ RX DatarateDelta6080TX DatarateDelta6080 10 10 \_\_\_\_\_ switch# show port-group-monitor PGMON policy PPolicy Name : PGMON\_policy Admin status : Not Active Oper status : Not Active Port type : All Port Groups \_\_\_\_\_ Threshold Interval %ge Rising Threshold %ge Falling Threshold Counter \_\_\_\_\_ \_\_\_\_\_ \_\_\_\_ RX Datarate Delta 26 TX Datarate Delta 60 450 250 100 80 \_\_\_\_\_ \_\_\_\_\_ \_\_\_\_\_ \_\_\_\_\_

L

## **Displaying the Management Interface Configuration**

The following command displays the management interface configuration:

```
switch# show interface mgmt 0
mgmt0 is up
Hardware is FastEthernet
Address is 000c.30d9.fdbc
Internet address is 10.16.1.2/24
MTU 1500 bytes, BW 100 Mbps full Duplex
26388 packets input, 6101647 bytes
0 multicast frames, 0 compressed
0 input errors, 0 frame, 0 overrun 0 fifo
10247 packets output, 2389196 bytes, 0 underruns
0 output errors, 0 collisions, 0 fifo
0 carrier errors
```

## **Displaying VSAN Interface Information**

To following example displays the VSAN interface information:

```
switch# show interface vsan 2
vsan2 is up, line protocol is up
WWPN is 10:00:00:05:30:00:59:1f, FCID is 0xb90100
Internet address is 10.1.1.1/24
MTU 1500 bytes, BW 1000000 Kbit
0 packets input, 0 bytes, 0 errors, 0 multicast
0 packets output, 0 bytes, 0 errors, 0 dropped
```

# **Transmit-Wait History Graph**

The transmit-wait history for the slow ports on 16-Gbps and 32-Gbps modules and switches can be displayed in the form of a graph over a period of time. The total transmit-wait time for each time period is displayed as a column of #. The actual value appears above each column as a vertically printed number. The following graphs can be displayed:

- Seconds scale—The transmit-wait history for the port over the last 60 seconds. The Y-axis value is the total transmit-wait time for each second, in milliseconds.
- Minutes scale—The transmit-wait history for the port over the last 60 seconds. The Y-axis value is the total transmit-wait time for each minute, in seconds, to one decimal place.
- Hours scale—The transmit-wait history for the port over the last 60 seconds. The Y-axis value is the total transmit-wait time for each hour, in minutes.

To display the transmit-wait history for a given interval of time, use the following commands:

Display the transmit-wait history graph for the period when transmit credit is not available for a given interval of time (seconds, minutes, or hours):

```
switch# show process creditmon txwait-history [module x [port y]]
```

Display the transmit-wait time in 2.5 microsecond units, as well as in seconds:

switch# show logging onboard txwait



**Note** The transmit-wait delta values are logged periodically (every 20 seconds) into the OBFL when transmit wait increases by at least 100 ms in the 20-second interval.

Display the total transmit-wait value for a particular interface in 2.5-microsecond units:

switch# show interface fcx/y counters

The following example displays the transmit-wait history graph, in seconds, for 16-Gbps modules:

switch(config)# show process creditmon txwait-history module 1 port 81

TxWait history for port fc1/81:

	45	55	5	55	55	5	54	15	5	5	54	15	55	55	55	4	55	55	5	99	99	9	99	99	9	99	9	99	9	99	99	99	99	99	99	9	99	99	9	99	9	99	99	3	
		9	00	0 0	0	0	00	00	8	0	00	0 (	9(	) (	00	0	08	31	0	00	)1	1:	11	.1	2	31	9	22	23	22	22	11	.3	21	11	2	11	.1	2	11	2	11	31	11	1
		4	3	37	9	9	99	91	8	9	99	99	03	35	59	9	09	8	3	86	50	8	93	35	1	37	9	62	20	88	39	88	32	54	18	4	88	39	4	87	04	16	19	33	8
100	0																										#																		
900																				ŧ	ŧ#	# :	##	#	#	# #	#	# #	#	# #	#	# #	ŧ#	# ‡	##	#	# #	#	#:	# #	# :	##	# #	ŧ #	
800																				ŧ	ŧ#	# :	##	#	#	# #	#	# #	#	# #	#	# #	ŧ#	# ‡	##	#	# #	#	#:	# #	# :	##	# #	ŧ #	
700																				ŧ	ŧ#	# :	##	#	#	# #	#	# #	#	# #	#	# #	ŧ#	# ‡	##	#	# #	#	#:	# #	# :	##	# #	ŧ #	
600																				ŧ	ŧ#	# :	##	#	#	# #	#	# #	#	# #	#	# #	ŧ#	# #	##	#	# #	#	# :	# #	# :	##	# #	ŧ #	
500	1	##	# :	##	#	#	# #	ŧ#	#	#:	# #	#	# :	# #	ŧ#	#	# †	ŧ#	#	# #	ŧ#	# :	##	#	#	# #	#	# #	#	# #	#	# #	ŧ#	# #	##	#	# #	#	# :	# #	# :	##	# #	ŧ #	
400	ŧ	##	# :	##	#	#	# #	ŧ#	#	#:	# #	#	# 1	# #	ŧ#	#	# ‡	ŧ#	#	# #	ŧ #	# :	##	#	#	# #	#	# #	#	# #	#	# #	ŧ#	# #	##	#	# #	#	# :	# #	# :	##	# #	ŧ#	
300	1	##	# :	##	#	#	# #	ŧ#	#	#:	# #	#	# :	# #	ŧ#	#	# †	ŧ#	#	# #	ŧ#	# :	##	#	#	# #	#	# #	#	# #	#	# #	ŧ#	# #	##	#	# #	#	# :	# #	# :	##	# #	ŧ #	
200	1	##	# :	##	#	#	# #	ŧ#	#	#:	# #	#	# :	# #	ŧ#	#	# †	ŧ#	#	# #	ŧ#	# :	##	#	#	# #	#	# #	#	# #	#	# #	ŧ#	# #	##	#	# #	#	# :	# #	# :	##	# #	ŧ #	
100	1	##	# :	##	#	#	# #	ŧ#	#	#:	# #	+#	# 1	# #	ŧ#	#	# ‡	ŧ#	#	# ŧ	ŧ #	# :	##	#	#	# #	#	# #	#	# #	#	# #	ŧ#	# ŧ	##	#	# #	#	#:	# #	# :	##	# #	ŧ #	
	(	).	•		5	•		•	1	•			1	• •	• •	•	2.	•	•	• 2	2.	•		3	•		•	3.	•		4		•	• 4	1.	•		5	•		•	5.	• •		6
									0				5				0			ç	5			0				5			0			ç	5			0			ļ	5			0

```
Tx Credit Not Available per second (last 60 seconds)
    # = TxWait (ms)
```

The following example displays the transmit-wait history graph, in minutes, for 16-Gbps modules:

```
60
****
54
0
 5
  0
  5
   0
   5 0 5 0
      5
      0
 Tx Credit Not Available per minute (last 60 minutes)
 # = TxWait (secs)
```

The following example displays the transmit wait history graph, in hours, for 16-Gbps modules:

```
3600
0 5 0 5 0 5 0 5 0 5 0 5 0 2
 Tx Credit Not Available per hour (last 72 hours)
  # = TxWait (secs)
```

The following example displays the transmit-wait OBFL logging for 16-Gbps modules:

module-4# show logging onboard txwait

-----Notes:

Sampling period is 20 secondsOnly txwait delta >= 100 ms are logged

														_
 	Interface	 	Delta TxWa 2.5us ticl	ait ks	Time seconds	 s	Congestion	 	Time	estar	np			 
	Eth4/1(VL3)		2758526		6		34%	1	Mon	Nov	26	14:32:28	2018	-
i	Eth4/1(VL3)	i	7982000	i	19	i	99%	i	Mon	Nov	26	14:32:08	2018	i
i	Eth4/1(VL3)	i	7976978	i	19	i	99%	i	Mon	Nov	26	14:31:48	2018	i
i	Eth4/1(VL3)	i	7974588	i	19	i	99%	i	Mon	Nov	26	14:31:28	2018	i
Ì	Eth4/1(VL3)	Ì	7970818	Í	19	Ì	99%	Ì	Mon	Nov	26	14:31:08	2018	Ì
İ.	Eth4/1(VL3)	Ì	7965766	Í	19	Ì	99%	Ì	Mon	Nov	26	14:30:48	2018	Ì
1	Eth4/1(VL3)	Ι	7976161		19		99%	I	Mon	Nov	26	14:30:28	2018	I
1	Eth4/1(VL3)	Ι	7538726		18		94%	I	Mon	Nov	26	14:30:08	2018	I
1	Eth4/1(VL3)		7968258		19		99%	L	Mon	Nov	26	14:29:48	2018	
1	fc4/9		7987745		19		99%	L	Mon	Nov	26	14:33:08	2018	
1	fc4/9		7991818		19		99%	L	Mon	Nov	26	14:32:48	2018	
1	fc4/9		7992774		19		99%	L	Mon	Nov	26	14:32:28	2018	
1	fc4/9		7992052		19		99%	L	Mon	Nov	26	14:32:08	2018	
	fc4/9		7991918		19		99%	L	Mon	Nov	26	14:31:48	2018	
1	fc4/9		7991993		19		99%	L	Mon	Nov	26	14:31:28	2018	
	fc4/9		7987967		19		99%	L	Mon	Nov	26	14:31:08	2018	
	fc4/9		7992034		19		99%	L	Mon	Nov	26	14:30:48	2018	
	fc4/9		7991966		19		99%	L	Mon	Nov	26	14:30:28	2018	
	fc4/9		7990076		19	- 1	99%	L	Mon	Nov	26	14:30:08	2018	
	fc4/9		7991890		19	1	99%	L	Mon	Nov	26	14:29:48	2018	