Configuring Interfaces

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

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. 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.

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.

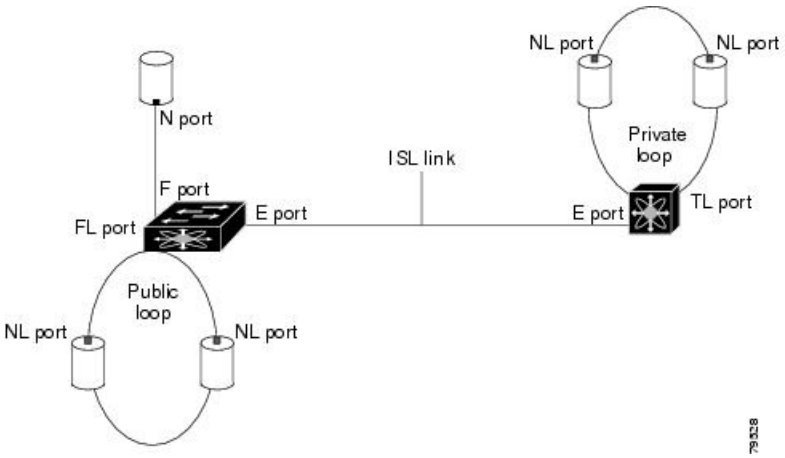
Interface Description

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, ST port, and B port (see Figure 1: Cisco MDS 9000 Series Switch Port Modes, on page 3). Besides these modes, each interface may be configured in auto or Fx port modes. These two modes determine the port type during interface initialization.

Figure 1: Cisco MDS 9000 Series Switch Port Modes



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 PortChannels.

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.

Note FL port mode is not supported on 4-port 10-Gbps switching module interfaces.

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

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.

Note ST port mode is not supported on the Cisco MDS 9124 Fabric Switch, the Cisco Fabric Switch for HP c-Class BladeSystem, and the Cisco Fabric Switch for IBM BladeCenter.

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.

B Port

While E ports typically interconnect Fibre Channel switches, some SAN extender devices, such as the Cisco PA-FC-1G Fibre Channel port adapter, implement a bridge port (B port) model to connect geographically dispersed fabrics. This model uses B ports as described in the T11 Standard FC-BB-2.

If an FCIP peer is a SAN extender device that supports only Fibre Channel B ports, you should enable the B port mode for the FCIP link. When a B port mode is enabled, the E port functionality is also enabled and they coexist. Even if the B port mode is disabled, the E port functionality remains enabled. For more details about SPAN, see the Cisco MDS 9000 Series NX-OS IP Services Configuration Guide.

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.

Note Fibre Channel interfaces on Storage Services Modules (SSMs) cannot be configured in auto mode.

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 1: Administrative States , on page 6.

Table 1: 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 2: Operational States , on page 7.

Table 2: 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 3: Reason Codes for Interface States , on page 7.

Table 3: Reason Codes for Interface States

Administrative Configuration	Operational Status	Reason Code
Up	Up	None.
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 4: Reason Codes for Nonoperational States , on page 8. Note that only some of the reason codes are listed in Table 4: Reason Codes for Nonoperational States , on page 8.

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 4: Reason Codes for Nonoperational States , on page 8.

Table 4: Reason Codes for Nonoperational States

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.	
SDM failure	A port is isolated because SDM is unable to program routes.	

Reason Code (Long Version)	Description	Applicable Modes
Isolation due to ELP failure	The port negotiation failed.	Only E ports and TE ports
Isolation due to ESC failure	The port negotiation failed.	
Isolation due to domain overlap	The Fibre Channel domains (fcdomain) 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 channel interfaces
Suspended due to incompatible speed	The interfaces belonging to a port channel have incompatible speeds.	
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.

10-Gbps Fiber Channel Mode

Some Cisco MDS Fibre Channel 8-Gbps and 16-Gbps modules and the Cisco MDS 9396S 16-Gbps Fabric Switch have the capability to run at 10-Gbps speed, and in two modes:

- 1/2/4/8-Gbps (for 8-Gbps modules) or 2/4/8/16-Gbps (for 16-Gbps modules and 9396S 16-Gbps Fabric Switch).
- 10-Gbps

Benefits of 10-Gbps Fiber Channel Mode

A 10-Gbps Fibre Channel uses a more efficient encoding and a faster clock rate than an 8-Gbps Fibre Channel. Therefore, it has an approximately 50 percent throughput advantage over an 8-Gbps Fibre Channel. Consequently, less links are needed to achieve a given bandwidth.

Supported Modules and Switches

The following modules and switches support 10-Gbps mode:

- 32-port Cisco MDS 1/2/4/8/10-Gbps Advanced Fibre Channel Module (DS-X9232-256K9)
- 48-port Cisco MDS 1/2/4/8/10-Gbps Advanced Fibre Channel Module (DS-X9248-256K9)
- 48-port Cisco MDS 2/4/8/10/16-Gbps Advanced Fibre Channel Module (DS-X9448-768K9)
- 96-port Cisco MDS 9396S 2/4/8/10/16-Gbps Fabric Switch (DS-C9396S-96EK9)

Note By default, all of the above are in their native Fibre Channel speed (1/2/4/8 Gbps or 2/4/8/16 Gbps) mode.

The following tables contain information about each module and the port ranges that need to be configured in 10-Gbps speed:

Table 5: 32-Port Cisco MDS 1/2/4/8/10-Gbps Advanced Fibre Channel Module (DS-X9232-256K9)

ASIC Port Range	10G Port	Offline Port
1-8	2-6,8	1,7
9-16	10-14,16	9,15
17-24	18-22,24	17,23
25-32	26-30,32	25,31

Table 6: 48-Port Cisco MDS 1/2/4/8/10-Gbps Advanced Fibre Channel Module (DS-X9248-256K9)

ASIC Port Range	10G Port	Offline Port
1-12	4-8,10	1-3,9,11-12
13-24	16-20,22	13-15,21,23-24
25-36	28-32,34	25-27,33,35-36
37-48	40-44,46	37-39, 45,47-48

Table 7: 48-Port Cisco MDS 2/4/8/10/16-Gbps Advanced Fibre Channel Module (DS-X9448-768K9)

ASIC Port Range	Offline Ports
1-8	None
9-16	None
17-24	None
25-32	None
33-40	None
41-48	None

Table 8: 96-Port Cisco MDS 9396S 2/4/8/10/16-Gbps Fabric Switch (DS-C9396S-96EK9)

ASIC Port Range	Offline Port
1-8	None

ASIC Port Range	Offline Port
9-16	None
17-24	None
25-32	None
33-40	None
41-48	None
49-56	None
57-64	None
65-72	None
73-80	None
81-88	None
89-96	None

Port Administrative Speeds

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

For internal ports on the Cisco Fabric Switch for HP c_Class BladeSystem and Cisco Fabric Switch for IBM BladeCenter, a port speed of 1 Gbps is not supported. Auto negotiation is supported between 2 Gbps and 4 Gbps only. Also, if the BladeCenter is a T chassis, then port speeds are fixed at 2 Gbps, and auto negotiation is not enabled.

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.

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.

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:

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 fc** *slot/port* **transceiver** commands display both values (ID and transmitter type) for Cisco-supported SFPs. Table 9: SFP Transmitter Acronym Definitions , on page 14 defines the acronyms used in the command output. For information about how to display interface information, see the Displaying Interface Information, on page 52.

Table 9: SFP Transmitter Acronym Definitions

Definition	Acronym
Standard transmitters defined in the GBIC specifications	
Short wave laser	swl
Long wave laser	lwl
Long wave laser cost reduced	lwcr
Electrical	elec
Extended transmitters assigned to Cisco-supported SFPs	
CWDM-1470	c1470
CWDM-1490	c1490
CWDM-1510	c1510
CWDM-1530	c1530
CWDM-1550	c1550
CWDM-1570	c1570
CWDM-1590	c1590
CWDM-1610	c1610

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 or flapped when a given event threshold is reached.

Note The Port Monitor portguard is not available for absolute counters.

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

- err-pkt-from-port
- err-pkt-from-xbar
- err-pkt-to-xbar
- credit-loss-reco
- link-loss
- signal-loss
- sync-loss
- rx-datarate
- invalid-crc
- invalid-words
- link-loss
- tx-credit-not-available
- tx-datarate
- tx-discards
- tx-slowport-oper-delay
- tx-slowport-count
- txwait
- tx-discards

Port Monitor

The Port Monitor feature can be used to monitor the performance and status of ports and generate alerts 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 error count crosses these threshold values.

Table 10: Default Port Monitor Policy with Threshold Values, on page 17 displays the default port monitor policy with threshold values. The unit for threshold values (rising and falling) differs across different counters.

Note NP ports are not monitored in port monitor.

Table 10: Default Port Monitor Policy with Threshold Values

Counter	Threshold Type	Interval (Seconds)	Rising Threshold	Event	Falling Threshold	Event	Warning Threshold	Port Monitor 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
state-change	Delta	60	5	4	0	4	Not enabled	Not enabled
invalid-words	Delta	60	5	4	0	4	Not enabled	Not enabled
invalid-crc	Delta	60	5	4	1	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-available	Delta	1	10% [1]	4	0%	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-count[2]	Delta	60	5	4	0	4	Not enabled	Not enabled
tx-slowport-oper-delay[3]	Absolute	60	50 ms 80 ms (Advanced 8-Gbps modules)	4	0 ms	4	Not enabled	Not enabled
txwait[4]	Delta	60	40%	4	0%	4	Not enabled	Not enabled
err-pkt-from-port_ASIC Error Pkt from Port	—	—	—	—	—	—	—	—
err-pkt-to-xbar_ASIC Error Pkt to xbar	—	—	—	—	—	—	—	—
err-pkt-from-xbar_ASIC Error Pkt from xbar	—	—	—	—	—	—	—	—

[1] 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.

[2] For all platforms, if the default value for tx-slowport-count is modified, ISSD will be restricted. To proceed with ISSD, use the **no** form of the **counter tx-slowport-count** command to roll back to the default value.

[3]
- 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).

[4]
- 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 11: Recommended Units for Port Monitor Policy

Counter	Threshold Type	Interval (Seconds)	Rising Threshold	Event	Falling Threshold	Event	Warning Threshold
link-loss	Delta	Seconds	Number	Event ID	Number	Event ID	Number
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	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
tx-credit-not-available	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
tx-slowport-count	Delta	Seconds	Number	Event ID	Number	Event ID	Number
tx-slowport-oper-delay	Absolute	Seconds	Milliseconds	Event ID	Milliseconds	Event ID	Milliseconds
txwait	Delta	Seconds	Percentage	Event ID	Percentage	Event ID	Percentage

Note

- 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.
- tx-slowport-count is applicable only for 8-Gbps modules (DS-X9224-96K9, DS-X9248-96K9, and DS-X9248-48K9) in the Cisco MDS 9500 Series switches. In the default configuration, the port monitor sends an alert when a slow-port condition is detected 5 times in 1 second for the configured slow-port monitor timeout. (See the **system timeout slowport-monitor** command in the Cisco MDS 9000 Series Command Reference.)
- tx-slowport-oper-delay is applicable only for advanced 8 and 16-Gbps modules. There are two defaults based on the module type:
  - For advanced 8-Gbps modules, the default rising threshold is 80 ms in a 1-second polling interval.
  - For 16-Gbps modules, the default rising threshold is 50 ms in a 1-second polling interval.
- 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.)
- Portguard action for tx-slowport-oper-delay (for Absolute type counter) is not supported.
- txwait is applicable only for advanced 8 and 16-Gbps modules. 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** keywords to detect slow flow on a device. For more information, see Configuring a Port Monitor Policy, on page 44.

The following counters were added from Cisco MDS NX-OS Release 5.2(2a) that are not included in the default policy:

Note

- Crossbar (Xbar) counters are supported only on the Cisco MDS 9700 48-Port 16-Gbps Fibre Channel Switching Module (DS-X9448-768K9) and Cisco MDS 9000 24/10-Port SAN Extension Module (DS-X9334-K9).
- Crossbar counters do not work as expected when check interval is configured.
- Crossbar counters work only when the poll-interval is set to 300 seconds.

- err-pkt-from-port_ASIC Error Pkt from port
- err-pkt-to-xbar_ ASIC Error Pkt to xbar—This counter provides information about the number of error packets that were sent from the crossbar on a module to the crossbar on a supervisor.
- err-pkt-from-xbar_ ASIC Error Pkt from xbar—This counter provides information about the number of error packets that were sent to the crossbar on a module from the crossbar on a supervisor.

Table 12: Slowdrain Port-Monitor Policy Threshold Value, on page 21 displays the threshold value of the slow-drain port-monitor policy:

Table 12: Slowdrain Port-Monitor Policy Threshold Value

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

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.

Warning Threshold

From Cisco MDS NX-OS Release 6.2(15), the warning threshold functionality is available for each counter in a Port Monitor policy.

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

From Cisco MDS NX-OS Release 6.2(15), a new functionality called check interval is introduced to check errors at a shorter time interval than the poll 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

- The port monitor check interval feature is supported only on the Cisco MDS 9710 Multilayer Director, Cisco MDS 9718 Multilayer Directors, and Cisco MDS 9706 Multilayer Directors.
- Check interval is supported on both counters, absolute and delta.
- We recommend that you configure the poll interval as a multiple of the check interval.
- Check interval is supported on the Cisco MDS 9700 Series Multilayer Directors from Cisco MDS NX-OS Release 6.2(15) onwards, and on the Cisco MDS 9250i Multiservice Fabric Switch from Cisco MDS NX-OS Release 6.2(17) onwards.
- 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 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.

Local Switching

Local switching allows traffic to be switched directly with a local crossbar when the traffic is directed from one port to another on the same line card. By using local switching, an extra switching step is avoided, which in turn decreases the latency.

When using local switching, note the following guidelines:

- All ports need to be in shared mode, which is the default state. To change a port mode to shared, use the **switchport ratemode shared** command.
- E ports are not allowed in the module because they must be in dedicated mode.

Note Local switching is not supported on the Cisco MDS 9700 Series switches.

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. You can 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 3.

Guidelines for Configuring Port Monitor Check Interval

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

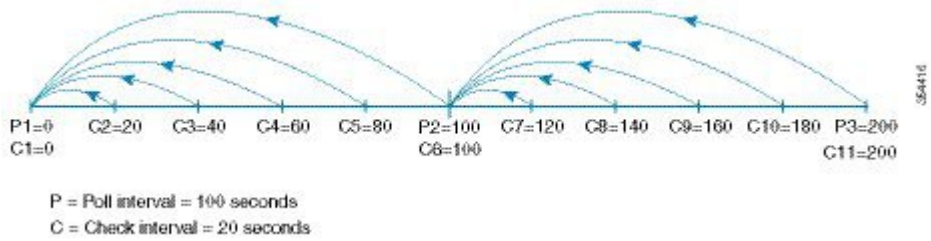
Note The value of the check interval is common across counters and policies.

- Check interval should be less than the poll 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.
- Port logical type *core* should be configured for the ports that connect a core switch to a Cisco NPV switch from port monitor and system timeout perspective. If not, port monitor and system timeout considers the operational port mode for such ports. For example, F ports are considered under edge policy in the port monitor.
- 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



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 Local Switching

- All the ports should be in shared mode, which is usually the default state. To place a port in shared mode, enter the **switchport rate-mode shared** command.
- E ports are not allowed in the module because they must be in dedicated mode.

Note Local switching is not supported on the Cisco MDS 9700 Series switches.

Guidelines for 10-Gbps Fibre Channel Mode

- For Cisco MDS 9513, the ports in the module can be configured to 10-Gbps speed only when the DS-13SLT-FAB3 (fabric 3) module bandwidth is 256 Gbps. Any other combination of fabric modules or Cisco MDS 9506 or Cisco MDS 9509 will not let the ports come up in 10 Gbps.
- When the 8-Gbps modules are in 10-Gbps mode, the ports in the module that are not 10-Gbps capable are disabled and will be in the out of service state. For DS-X9232-256K9, the ASIC range is eight ports, of which two ports will be out of service. For DS-X9248-256K9, the ASIC range is 12 ports, of which six ports will be out of service. For the 16-Gbps modules and fabric switch, all the ports have 10-G speed mode.
- The ports function only in full rate mode. They cannot be moved to shared rate mode.
- The ports cannot be configured in any other speed other than the speed values provided in the k command.
- Ports that are 10-Gbps capable and are disabled or are out of service cannot be put back in service using the **no out-of-service** command. To put these ports back in service, all the ports in the ASIC range need to be reconfigured with the **no 10g-speed-mode** command.
- Local switching must be disabled. Otherwise, ports cannot be configured in dedicated mode.

Thus, for interconnecting 16-Gbps Fibre Channel modules, 16 Gbps is the preferred speed. However, for interconnecting 8-Gbps modules, or for interconnecting 16-Gbps modules and 8-Gbps modules, we recommend 10 Gbps as the preferred speed.

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.

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.

Default Settings

Table 14: Default Interface Parameters , on page 31 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:

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:

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.

For the Cisco Fabric Switch for HP c-Class BladeSystem and the Cisco Fabric Switch for IBM BladeCenter, you can configure a range of interfaces in internal ports or external ports, but you cannot mix both interface types within the same range. For example, bay 1-10 , bay 12 or ext 0 , ext 15-18 are valid ranges, but bay 1-5 , ext 15-17 is not.

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:

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 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:

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)# **no shutdown**

Configuring an Interface Mode

To configure the interface mode, perform these steps:

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**

Note 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**

Note
- TL ports and SD ports cannot be configured automatically. They must be administratively configured.
- 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:

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 4 Specify the maximum login value for this port:

switch(config-if)# **switchport max-npiv-limit 100**

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:

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 35 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:

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 10-G bps Fiber Channel Mode via the CLI

There are two ways to change the ports to the 10-Gbps speed mode:

- Using the **10g-speed mode** command, which is the recommended method.

Note When 10-G speed mode is configured in an interface mode for 16-Gbps modules, all the ports in an interface mode will be in 10-Gbps mode, whereas in 8-Gbps modules, only certain ports in an interface mode will be in 10-Gbps mode and the rest will be in the out-of-service state.

- Using the generic **switchport speed** command.

To configure the interface mode, perform these steps. The following is an example on a Cisco MDS 9396S DS-C9396S-96EK9.

Step 1 Enter configuration mode:

switch# **configure terminal**

Step 2 Select a Fibre Channel interface and enter interface configuration mode:

switch(config)# **interface fc1/1-8**

Ensure that a full ASIC range of ports is selected before executing this command. For example, fcy/1-12 for a 48-port 8-Gbps module or fcy/1-8 for an 8-Gbps 32-port, 48-port 16-Gbps module.

Step 3 Configure all the ports (1 to 8) in Fibre Channel module 1 to 10 Gbps:

switch(config-if)# **10g-speed-mode**

For the DS-X9248-256K9 module, the **10g-speed-mode** command will work only for interface ranges 1–12, 13–24, 25–36, or 37–48.

For the DS-X9232-256K9 module, the **10g-speed-mode** command will work only for interface ranges 1–8, 9–16, 17–24, or 25–32.

For the DS-X9448-768K9 module, the **10g-speed-mode** command will work only for interface ranges 1–8, 9–16, 17–24, 25–32, 33–40, or 41–48.

For the DS-C9396S-96EK9 module, the **10g-speed-mode** command will work only for interface ranges 1-8, 9-16, 17-24, 25-32, 33-40, 41-48, 49-56, 57-64, 65-72, 73-80, 81-88, or 89-96.

Step 4 (Optional) Revert the settings and put all the ports (1 to 8) in the out-of-service state and move them to the in-service state:

switch(config-if)# **no 10g-speed-mode**

Configuring the 10-Gbps Fibre Channel Mode via the Device Manager

Perform these steps to convert a defined range of interfaces to 10-G mode for a module with 2/4/8/10/16-Gbps Advanced Fibre Channel module (DS-X9448-768K9):

Step 1 Launch the Device Manager for the device supporting 10-G speed.

Step 2 Right-click the module and select **Configure bandwidth Reservation**.

Step 3 Select one or more ASIC port ranges and click **Apply**. By default, all the ports are 2/4/8 or 2/4/8/16-Gbps speed capable.

Configuring the Port Administrative Speeds

Note Changing the port administrative speed is a disruptive operation.

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

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:

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 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**

Enabling 10-Gbps Speed Mode

Cisco MDS 9000 Series Advanced 8-Gbps modules support 10-Gbps ports. However, a group of ports must be configured to 10-Gbps mode in order to use the port speed group feature. Individual ports cannot be configured to 10-Gbps mode.

- For the 48-Port Advanced 8-Gbps module, the group size is 12 ports (1-12, 13-24, and so on). When the group is configured to 10-Gbps mode, the ports 1-3, 9, and 11-12 in that group are unavailable for use and displays them as outOfServc or Out of Service in the output.
- For the 32-Port Advanced 8-Gbps module, the group size is 8 ports (1-8, 9-16, and so on). When the group is configured to 10-Gbps mode, the ports 1 and 7 in the group are unavailable for use and displays them as outOfServc or Out of Service in the output.
- For the 48-Port 16-Gbps module, in the Cisco MDS 9700 switch and the Cisco MDS 9396S switch the group size is 8 ports. When the group is configured to 10-Gbps mode, all the 8 ports are available for use.

To enable the 10-Gbps speed mode on a group of ports, perform these steps:

Step 1 Enter configuration mode:

switch# **configure terminal**

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

switch(config)# **interface fc1/1-12**

Step 3 Change the speed group to 10-Gbps:

switch(config-if)# **10g-speed-mode**

(Optional) Revert to default speed group setting:

switch(config-if)# **no 10g-speed-mode**

What to do next

Note In Cisco NX-OS Release 5.2(8c), the default speed group for the supported switching modules are 1-, 2-, 4-, and 8-Gbps.

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:

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 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**

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:

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:

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 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:

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:

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*]

(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 five times within 120 seconds due to multiple causes. The portguard controls the interface in the following manner:

- The interface will be error disabled due to link down if there are link failures due to bit errors 2 times and link failures due to credit loss 3 times in 120 seconds.
- The interface will be error disabled due to bit errors if there are link failures due to bit errors 5 times in 120 seconds.
- The interface will be error disabled due to credit loss if there are link failures due to credit loss 5 times in 120 seconds.

Example

This example shows how to configure portguard to bring a port to down state if the link flaps 5 times within 120 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 120
switch (config-if)# errdisable detect cause bit-errors num-times 5 duration 120
```

```
switch (config-if)# errdisable detect cause credit-loss num-times 5 duration 120
```

The above example sets the configuration to the following status:

- The port will be error disabled due to bit errors if the port suffers link failure due to bit errors 5 times in 120 seconds.
- The port will be error-disabled due to credit loss if the port suffers link failure due to credit loss 5 times in 120 seconds.
- The port will be error-disabled due to link down if the port suffers link failure due to bit errors 2 times and link-failure due to credit loss 3 times in 120 seconds.

This example shows the internal information about a port in down state because of 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
```

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:

Step 1 Enter configuration mode:

switch# **configure terminal**

Step 2 Enable port monitoring:

switch(config)# **port-monitor enable**

(Optional) Disable port monitoring:

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

Configuring the Check Interval

To configure the check interval, perform these steps:

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)# **port-type** {**access-port** | **trunks** | **all**}

Step 4 Specify the counter parameters:

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-count** | **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** {**errordisable** | **flap**}

Note
- 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.
- Counter **tx-slowport-count** is supported only on DS-X9224-96K9, DS-X9248-96K9, and DS-X9248-48K9 modules.

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

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-count** | **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** {**errordisable** | **flap**}

(Optional) Monitor a counter:

switch(config-port-monitor)# **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-count** | **tx-slowport-oper-delay** | **txwait**}

A port monitor currently recognizes two kinds of ports:

- Port type access ports are normally F ports with a single end device logged in. However, a port monitor considers TF ports and F ports with multiple logins to be port type access as well.
- Port type trunk ports are E ports (ISLs) regardless of whether they are actually carrying multiple VSANs (TE, trunking) or not. Some of the access port counter thresholds and portguard actions might not be appropriate on the TF ports in the port-monitor configurations. Specifically, port guard *disable* or *flap* actions can affect multiple end devices on the F ports with multiple logins. Therefore, performing disable or flap 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:

Step 1 Enter configuration mode:

switch# **configure terminal**

Step 2 Activate the specified port monitor policy:

switch(config)# **port-monitor activate** *policyname*

(Optional) Activate the default port monitor policy:

switch(config)# **port-monitor activate**

(Optional) Deactivate the specified port monitoring policy:

switch(config)# **no port-monitor activate** *policyname*

Configuring Port Monitor Portguard

To configure a port monitor portguard action, 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:

switch(config)# **no port-monitor name** *policyname*

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

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-count** | **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** {**errordisable** | **flap**}

Note

- 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.
- Counter **tx-slowport-count** is supported only on DS-X9224-96K9, DS-X9248-96K9, and DS-X9248-48K9 modules.

Configuring Port Group Monitor

Enabling a Port Group Monitor

To enable a port group monitor, perform these steps:

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:

Step 1 Enter configuration mode:

switch# **configure terminal**

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

switch(config)# **port-group-monitor name** *policyname*

(Optional) Remove the policy:

switch(config)# **no port-group-monitor name** *policyname*

Step 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 Specific Counter Monitoring.

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
TX Datarate   Delta      60        80                   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                   10
TX Datarate   Delta      60       80                   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:

Step 1 Enter configuration mode:

switch# **configure terminal**

Step 2 Activate the specified port group monitor policy:

switch(config)# **port-group-monitor activate** *policyname*

(Optional) Activate the default port group monitor policy:

switch(config)# **port-group-monitor activate**

(Optional) Deactivate the specified port group monitor policy:

switch(config)# **no port-group-monitor activate** *policyname*

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**

Step 3 Configure the IPv4 address and IPv4 subnet mask:

switch(config-if)# **ip address 10.16.1.2 255.255.255.0**

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)# **ip default-gateway 1.1.1.4**

Step 7 Return to user EXEC mode:

switch(config)# **exit**

(Optional) Save your configuration changes to the file system:

switch# **copy running-config startup-config**

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# **configure 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:

switch(config)# **interface vsan 2**

Step 3 Enable the VSAN interface:

switch(config-if)# **no shutdown**

Verifying Interfaces Configuration

Displaying Interface Information

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

The following example displays the status of interfaces:

Displays All Interfaces

```
switch# show interface

fc1/1 is up
    Hardware is Fibre Channel, SFP is short wave laser
    Port WWN is 20:0b:00:05:30:00:8d:de
    Admin port mode is F
    Port mode is F, FCID is 0x610000
    Port vsan is 2
    Speed is 2 Gbps
    Transmit B2B Credit is 3
    Receive B2B Credit is 16
    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
      134 frames input, 8468 bytes
        0 discards, 0 errors
        0 CRC, 0 unknown class
        0 too long, 0 too short
      154 frames output, 46072 bytes
        0 discards, 0 errors
      1 input OLS, 1 LRR, 0 NOS, 0 loop inits
      1 output OLS, 0 LRR, 1 NOS, 0 loop inits
      16 receive B2B credit remaining
      3 transmit B2B credit remaining.
.
.
.
fc1/9 is trunking
    Hardware is Fibre Channel, SFP is long wave laser cost reduced
    Port WWN is 20:09:00:05:30:00:97:9e
    Peer port WWN is 20:0b:00:0b:5f:a3:cc:00
    Admin port mode is E, trunk mode is on
    Port mode is TE
    Port vsan is 100
    Speed is 2 Gbps
    Transmit B2B Credit is 255
    Receive B2B Credit is 255
    Receive data field Size is 2112
    Beacon is turned off
    Trunk vsans (admin allowed and active) (1,100,3000)
    Trunk vsans (up)                       (1,100,3000)
    Trunk vsans (isolated)                 ()
    Trunk vsans (initializing)             ()
    5 minutes input rate 280 bits/sec, 35 bytes/sec, 0 frames/sec
    5 minutes output rate 176 bits/sec, 22 bytes/sec, 0 frames/sec
```

```
      4609939 frames input, 8149405708 bytes
        0 discards, 0 errors
        0 CRC, 0 unknown class
        0 too long, 0 too short
      4638491 frames output, 7264731728 bytes
        0 discards, 0 errors
      3 input OLS, 9 LRR, 1 NOS, 0 loop inits
      9 output OLS, 7 LRR, 1 NOS, 0 loop inits
      16 receive B2B credit remaining
      3 transmit B2B credit remaining.
.
.
.
fc1/13 is up
    Hardware is Fibre Channel, SFP is short wave laser
    Port WWN is 20:0d:00:05:30:00:97:9e
    Admin port mode is auto, trunk mode is on
    Port mode is F, FCID is 0x650100
    Port vsan is 100
    Speed is 2 Gbps
    Transmit B2B Credit is 3
    Receive B2B Credit is 16
    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
      8696 frames input, 3227212 bytes
        0 discards, 0 errors
        0 CRC, 0 unknown class
        0 too long, 0 too short
      16799 frames output, 6782444 bytes
        0 discards, 0 errors
      0 input OLS, 0 LRR, 0 NOS, 0 loop inits
      1 output OLS, 1 LRR, 0 NOS, 1 loop inits
      16 receive B2B credit remaining
      3 transmit B2B credit remaining.
.
.
.
sup-fc0 is up
    Hardware is Fibre Channel
    Speed is 1 Gbps
    139597 packets input, 13852970 bytes
      0 multicast frames, 0 compressed
      0 input errors, 0 frame, 0 overrun 0 fifo
    139516 packets output, 16759004 bytes, 0 underruns
      0 output errors, 0 collisions, 0 fifo
      0 carrier errors
```

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 fc3/13 , fc3/16
fc3/13 is up
    Hardware is Fibre Channel, SFP is short wave laser
    Port WWN is 20:8d:00:05:30:00:97:9e
    Admin port mode is FX
    Port mode is F, FCID is 0x7b0300
    Port vsan is 1
    Speed is 2 Gbps
    Transmit B2B Credit is 3
    Receive B2B Credit is 12
    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
      1856 frames input, 116632 bytes
        0 discards, 0 errors
        0 CRC,  0 unknown class
        0 too long, 0 too short
      1886 frames output, 887712 bytes
        0 discards, 0 errors
      0 input OLS, 0 LRR, 0 NOS, 1 loop inits
      1 output OLS, 1 LRR, 0 NOS, 1 loop inits
      16 receive B2B credit remaining
      3 transmit B2B credit remaining.
fc3/16 is up
    Hardware is Fibre Channel, SFP is short wave laser
    Port WWN is 20:90:00:05:30:00:97:9e
    Admin port mode is FX
    Port mode is F, FCID is 0x7d0100
    Port vsan is 3000
    Speed is 2 Gbps
    Transmit B2B Credit is 3
    Receive B2B Credit is 12
    Receive data field Size is 2112
    Beacon is turned off
    5 minutes input rate 504 bits/sec, 63 bytes/sec, 0 frames/sec
    5 minutes output rate 520 bits/sec, 65 bytes/sec, 0 frames/sec
      47050 frames input, 10311824 bytes
        0 discards, 0 errors
        0 CRC,  0 unknown class
        0 too long, 0 too short
      62659 frames output, 10676988 bytes
        0 discards, 0 errors
      0 input OLS, 0 LRR, 0 NOS, 0 loop inits
      1 output OLS, 1 LRR, 0 NOS, 1 loop inits
      16 receive B2B credit remaining
      3 transmit B2B credit remaining.
```

The following example displays the status of a specified interface:

Displays a Specific Interface

```
switch# show interface fc2/2
fc2/2 is trunking
    Port description is Trunk to Core-4
    Hardware is Fibre Channel, SFP is short wave laser
    Port WWN is 20:42:00:05:30:00:97:9e
    Peer port WWN is 20:cc:00:05:30:00:50:9e
```

```
    Admin port mode is E, trunk mode is on
    Port mode is TE
    Port vsan is 1
    Speed is 2 Gbps
    Transmit B2B Credit is 255
    Receive B2B Credit is 255
    Receive data field Size is 2112
    Beacon is turned off
    Belongs to port-channel 2
    Trunk vsans (admin allowed and active) (1,100,3000)
    Trunk vsans (up)                       (1)
    Trunk vsans (isolated)                 (100,3000)
    Trunk vsans (initializing)             ()
    5 minutes input rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
    5 minutes output rate 32 bits/sec, 4 bytes/sec, 0 frames/sec
      2214834 frames input, 98673588 bytes
        0 discards, 0 errors
        0 CRC, 0 unknown class
        0 too long, 0 too short
      2262415 frames output, 343158368 bytes
        0 discards, 0 errors
      1 input OLS, 1 LRR, 1 NOS, 0 loop inits
      2 output OLS, 1 LRR, 0 NOS, 0 loop inits
      16 receive B2B credit remaining
      3 transmit B2B credit remaining.
```

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 Information in a Brief Format

```
switch# show interface brief
--------------------------------------------------------------------------------
Interface  Vsan   Admin  Admin   Status          SFP   Oper  Oper   Port
```

```
                Mode   Trunk                          Mode  Speed  Channel
                       Mode                                 (Gbps)
-------------------------------------------------------------------------------
fc1/1      1      E      on      trunking         swl    TE      2    1
fc1/2      1      E      on      trunking         swl    TE      2    1
fc1/3      1      auto   on      SFPAbsent       --     --           --
fc1/4      1      auto   on      SFPAbsent       --     --           --
fc1/5      3000   auto   on      up               swl    F       2    --
...
fc2/2      1      E      on      trunking         swl    TE      2    2
fc2/3      1      auto   on      down             c1610  --           --
fc2/4      1      auto   on      down             c1590  --           --
fc2/5      3000   auto   on      notConnected     lwcr   --           --
fc2/6      1      auto   on      SFPAbsent       --     --           --
...
fc3/16     3000   FX     --      up               swl    F       2    --
fc3/17     1      FX     --      SFPAbsent       --     --           --
...
-------------------------------------------------------------------------------
Interface               Status     IP Address        Speed        MTU
-------------------------------------------------------------------------------
GigabitEthernet4/1      SFPAbsent --                auto         1500
...
GigabitEthernet4/6      down       10.1.1.2/8        auto         3000
GigabitEthernet4/7      down       10.1.1.27/24      auto         1500
GigabitEthernet4/8      down       --                auto         1500
-------------------------------------------------------------------------------
Interface           Status              Oper Mode           Oper Speed
                                                            (Gbps)
-------------------------------------------------------------------------------
iscsi4/1            down                --
...
-------------------------------------------------------------------------------
Interface          Status                            Speed
                                                     (Gbps)
-------------------------------------------------------------------------------
sup-fc0            up                                1
-------------------------------------------------------------------------------
Interface               Status     IP Address        Speed        MTU
-------------------------------------------------------------------------------
mgmt0                   up         172.19.48.96/25   100 Mbps     1500
-------------------------------------------------------------------------------
Interface               Vsan     Admin    Status            Oper   Oper
                                 Trunk                      Mode   Speed
                                 Mode                              (Gbps)
-------------------------------------------------------------------------------
port-channel 1          1        on       trunking          TE     4
port-channel 2          1        on       trunking          TE     4
-------------------------------------------------------------------------------
Interface  Vsan   Admin  Admin   Status       Oper  Profile  Port-channel
                  Mode   Trunk                Mode
                         Mode
-------------------------------------------------------------------------------
fcip10     1      auto   on      notConnected --     10       --
```

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
    0 link failures, 0 sync losses, 0 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
```

Note 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# show interface counters brief
-------------------------------------------------------------------------------
Interface          Input (rate 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
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)
                   -----------------------------  -----------------------------
                   Rate     Total                 Rate     Total
                   Mbits/s  Frames                Mbits/s  Frames
-------------------------------------------------------------------------------
port-channel 1     0        0                     0        0
port-channel 2     0        3946                  0        3946
```

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, on page 59 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

```
switch# show interface brief
--------------------------------------------------------------------------------
Interface  Vsan   Admin  Admin   Status          SFP    Oper  Oper   Port
                  Mode   Trunk                         Mode  Speed  Channel
                         Mode                                (Gbps)
--------------------------------------------------------------------------------
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

```
switch# show interface brief
--------------------------------------------------------------------------------
Interface  Vsan   Admin  Admin   Status          SFP    Oper  Oper   Port
                  Mode   Trunk                         Mode  Speed  Channel
                         Mode                                (Gbps)
--------------------------------------------------------------------------------
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        --     --           --
```

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:

```
switch# show port-monitor
--------------------------------------------------------------------------------
Port Monitor : enabled
--------------------------------------------------------------------------------
Policy Name  : Sample
```

```
Admin status : Not Active
Oper status  : Not Active
Port type    : All Ports
-------------------------------------------------------------------------------------------------------
Counter        Threshold    Interval    Rising Threshold    event    Falling Threshold
event    PMON Portguard
-------------------------------------------------------------------------------------------------------
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
Available        Delta        1              10%              4           0%
 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           0ms
 4        Not enabled
TXWait           Delta        1              40%              4           0%
 4        Not enabled
-------------------------------------------------------------------------------------------------------
Policy Name  : default
Admin status : Not Active
Oper status  : Not Active
Port type    : All Ports
-------------------------------------------------------------------------------------------------------
Counter        Threshold  Interval  Rising Threshold   event  Falling Threshold     event
    PMON Portguard
-------------------------------------------------------------------------------------------------------
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
Available        Delta       1            10%           4            0%            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            0ms           4
       Not enabled
TXWait           Delta       1            40%           4            0%            4
       Not enabled
-------------------------------------------------------------------------------------------------------------
```

```
switch# show port-monitor
-------------------------------------------------------------------------------------------------
Port Monitor : enabled
-------------------------------------------------------------------------------------------------
Policy Name  : Sample
Admin status : Not Active
Oper status  : Not Active
Port type    : All Ports
-------------------------------------------------------------------------------------------------
Counter        Threshold    Interval    Rising Threshold    event    Falling Threshold
event    PMON Portguard
-------------------------------------------------------------------------------------------------
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
Available        Delta        1             10%              4           0%
```

```
 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            0ms
 4        Not enabled
TXWait           Delta        1              40%              4            0%
 4        Not enabled
--------------------------------------------------------------------------------------------------------
Policy Name  : default
Admin status : Not Active
Oper status  : Not Active
Port type    : All Ports
--------------------------------------------------------------------------------------------------------
Counter        Threshold  Interval  Rising Threshold   event  Falling Threshold     event
    PMON Portguard
--------------------------------------------------------------------------------------------------------
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
Available        Delta       1            10%            4            0%               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            0ms              4
       Not enabled
TXWait           Delta       1            40%            4            0%               4
       Not enabled
--------------------------------------------------------------------------------------------------------
```

```
switch# show port-monitor active
Policy Name  : sample
```

```
Admin status : Active
Oper status  : Active
Port type    : All Access Ports
-------------------------------------------------------------------------------------------------------------
Counter          Threshold  Interval  Rising Threshold  event  Falling Threshold   event
portguard
-------------------------------------------------------------------------------------------------------------
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
Available         Delta        1         10%              4            0%              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            0ms             4
   Not enabled
TXWait            Delta        1         40%              4            0%              4
   Not enabled
-------------------------------------------------------------------------------------------------------------
```

```
switch# show port-monitor sample
Policy Name  : sample
Admin status : Active
Oper status  : Active
Port type    : All Access Ports
-------------------------------------------------------------------------------------------------------------
Counter          Threshold  Interval Rising Threshold  event Falling Threshold  event
portgurard
-------------------------------------------------------------------------------------------------------------
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
Available         Delta        1             10%         4            0%          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            0ms         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    event  Falling     event  Warning
PMON
                                       Threshold        Threshold           Threshold
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    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     0ms          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  : slowdrain
Admin status : Not Active
Oper status  : Not Active
Port type    : All Access Ports
_________________________________________________________________________________________________
Counter            Threshold    Interval    Rising Threshold    event    Falling Threshold
    event    PMON Portguard
_________________________________________________________________________________________________
Credit Loss Reco     Delta           1            1               4            0
       4         Not enabled
TX Credit Not
Available            Delta           1            10%             4            0%
       4         Not enabled
_________________________________________________________________________________________________
```

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
-------------------------------------------------------------------------------------------------
Counter      Threshold  Interval %ge Rising Threshold %ge Falling Threshold
-------      ---------  -------- -------------------- ----------------------
RX Datarate   Delta      60       50                   10
TX Datarate   Delta      60       50                   10
-------------------------------------------------------------------------------------------------
Policy Name  : pgm2
Admin status : Active
Oper status  : Active
Port type    : All Port Groups
-------------------------------------------------------------------------------------------------
Counter       Threshold  Interval %ge Rising Threshold %ge Falling Threshold
```

```
-------      ---------  -------- -------------------- ----------------------
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
--------------------------------------------------------------------------------
Counter       Threshold  Interval %ge Rising Threshold %ge Falling Threshold
-------      ---------  -------- -------------------- ----------------------
RX Datarate   Delta      60       80                   20
TX Datarate   Delta      60       80                   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 Datarate   Delta      60       80                   10
TX Datarate   Delta      60       80                   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
--------------------------------------------------------------------------------
Counter      Threshold  Interval %ge Rising Threshold %ge Falling Threshold
-------      ---------  -------- -------------------- ----------------------
RX Datarate   Delta      26       450                  250
TX Datarate   Delta      60       100                  80
--------------------------------------------------------------------------------
```

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 advanced 8-Gbps and 16-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 fc*x/y* counters**

The following example displays the transmit-wait history graph, in seconds, for advanced 8-Gbps modules and 16-Gbps modules:

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

TxWait history for port fc1/81:
===============================

   455555555455554555554555599999999999999999999999999999999999
     900000000800009000008100011111231922322211321121112112113111
     433799991899990359909838608935137962088988254848894870461938
1000                                  #
900                             ####################################
800                             ####################################
700                             ####################################
600                             ####################################
500 ############################################################
400 ############################################################
300 ############################################################
200 ############################################################
100 ############################################################
    0....5....1....1....2....2....3....3....4....4....5....5....6
```

```
              0    5    0    5    0    5    0    5    0    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 advanced 8-Gbps modules and 16-Gbps modules:

```
   55555555555555555555555555555555555555555555555555555555555555555
   05555555555555555555555555555555555555555555555555555555555555555
   ...........................................................
   03544444544444544545444444444563536353437543445334355454534 4
60
54  ############################################################
48 ############################################################
42 ############################################################
36 ############################################################
30 ############################################################
24 ############################################################
18 ############################################################
12 ############################################################
6 ############################################################
  0....5....1....1....2....2....3....3....4....4....5....5....6
            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 advanced 8-Gbps modules and 16-Gbps modules:

```
  33333333333333333333333333333333333333333
  33333333333333333333333333333333333333332
     22222222222222222222222222222222222222229
     77778877777787787777877787767777777787679000000000000000000000000000000000
3600
3240 ##########################################
2880 ##########################################
2520 ##########################################
2160 ##########################################
1800 ##########################################
1440 ##########################################
1080 ##########################################
 720 ##########################################
 360 ##########################################
    0....5....1....1....2....2....3....3....4....4....5....5....6....6....7.7
              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 advanced 8-Gbps modules and 16-Gbps modules:

```
switch# show logging onboard txwait
Notes:
    - sampling period is 20 seconds
    - only txwait delta value >= 100 ms are logged
---------------------------------
 Module: 1 txwait count
---------------------------------
```

```
-------------------------------------------------------------------------------
| Interface | Delta TxWait Time     | Congestion | Timestamp                |
|           | 2.5us ticks | seconds |            |                          |
-------------------------------------------------------------------------------
|   fc1/11  |  3435973    | 08      |      42%   | Sun Sep 30 05:23:05 2001 |
|   fc1/11  |  6871947    | 17      |      85%   | Sun Sep 30 05:22:25 2001 |
```